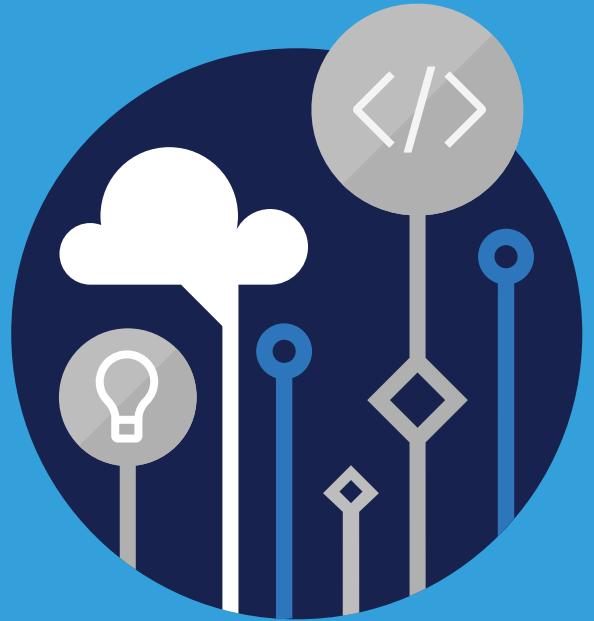


Microsoft
Official
Course



SC-200T00

Microsoft Security
Operations Analyst

SC-200T00

**Microsoft Security Operations
Analyst**

II Disclaimer

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The names of manufacturers, products, or URLs are provided for informational purposes only and Microsoft makes no representations and warranties, either expressed, implied, or statutory, regarding these manufacturers or the use of the products with any Microsoft technologies. The inclusion of a manufacturer or product does not imply endorsement of Microsoft of the manufacturer or product. Links may be provided to third party sites. Such sites are not under the control of Microsoft and Microsoft is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. Microsoft is not responsible for webcasting or any other form of transmission received from any linked site. Microsoft is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of Microsoft of the site or the products contained therein.

© 2019 Microsoft Corporation. All rights reserved.

Microsoft and the trademarks listed at <http://www.microsoft.com/trademarks>¹ are trademarks of the Microsoft group of companies. All other trademarks are property of their respective owners.

¹ <http://www.microsoft.com/trademarks>

MICROSOFT LICENSE TERMS

MICROSOFT INSTRUCTOR-LED COURSEWARE

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to your use of the content accompanying this agreement which includes the media on which you received it, if any. These license terms also apply to Trainer Content and any updates and supplements for the Licensed Content unless other terms accompany those items. If so, those terms apply.

**BY ACCESSING, DOWNLOADING OR USING THE LICENSED CONTENT, YOU ACCEPT THESE TERMS.
IF YOU DO NOT ACCEPT THEM, DO NOT ACCESS, DOWNLOAD OR USE THE LICENSED CONTENT.**

If you comply with these license terms, you have the rights below for each license you acquire.

1. DEFINITIONS.

1. "Authorized Learning Center" means a Microsoft Imagine Academy (MSIA) Program Member, Microsoft Learning Competency Member, or such other entity as Microsoft may designate from time to time.
2. "Authorized Training Session" means the instructor-led training class using Microsoft Instructor-Led Courseware conducted by a Trainer at or through an Authorized Learning Center.
3. "Classroom Device" means one (1) dedicated, secure computer that an Authorized Learning Center owns or controls that is located at an Authorized Learning Center's training facilities that meets or exceeds the hardware level specified for the particular Microsoft Instructor-Led Courseware.
4. "End User" means an individual who is (i) duly enrolled in and attending an Authorized Training Session or Private Training Session, (ii) an employee of an MPN Member (defined below), or (iii) a Microsoft full-time employee, a Microsoft Imagine Academy (MSIA) Program Member, or a Microsoft Learn for Educators – Validated Educator.
5. "Licensed Content" means the content accompanying this agreement which may include the Microsoft Instructor-Led Courseware or Trainer Content.
6. "Microsoft Certified Trainer" or "MCT" means an individual who is (i) engaged to teach a training session to End Users on behalf of an Authorized Learning Center or MPN Member, and (ii) currently certified as a Microsoft Certified Trainer under the Microsoft Certification Program.
7. "Microsoft Instructor-Led Courseware" means the Microsoft-branded instructor-led training course that educates IT professionals, developers, students at an academic institution, and other learners on Microsoft technologies. A Microsoft Instructor-Led Courseware title may be branded as MOC, Microsoft Dynamics, or Microsoft Business Group courseware.
8. "Microsoft Imagine Academy (MSIA) Program Member" means an active member of the Microsoft Imagine Academy Program.
9. "Microsoft Learn for Educators – Validated Educator" means an educator who has been validated through the Microsoft Learn for Educators program as an active educator at a college, university, community college, polytechnic or K-12 institution.
10. "Microsoft Learning Competency Member" means an active member of the Microsoft Partner Network program in good standing that currently holds the Learning Competency status.
11. "MOC" means the "Official Microsoft Learning Product" instructor-led courseware known as Microsoft Official Course that educates IT professionals, developers, students at an academic institution, and other learners on Microsoft technologies.
12. "MPN Member" means an active Microsoft Partner Network program member in good standing.

13. "Personal Device" means one (1) personal computer, device, workstation or other digital electronic device that you personally own or control that meets or exceeds the hardware level specified for the particular Microsoft Instructor-Led Courseware.
 14. "Private Training Session" means the instructor-led training classes provided by MPN Members for corporate customers to teach a predefined learning objective using Microsoft Instructor-Led Courseware. These classes are not advertised or promoted to the general public and class attendance is restricted to individuals employed by or contracted by the corporate customer.
 15. "Trainer" means (i) an academically accredited educator engaged by a Microsoft Imagine Academy Program Member to teach an Authorized Training Session, (ii) an academically accredited educator validated as a Microsoft Learn for Educators – Validated Educator, and/or (iii) a MCT.
 16. "Trainer Content" means the trainer version of the Microsoft Instructor-Led Courseware and additional supplemental content designated solely for Trainers' use to teach a training session using the Microsoft Instructor-Led Courseware. Trainer Content may include Microsoft PowerPoint presentations, trainer preparation guide, train the trainer materials, Microsoft One Note packs, classroom setup guide and Pre-release course feedback form. To clarify, Trainer Content does not include any software, virtual hard disks or virtual machines.
2. **USE RIGHTS.** The Licensed Content is licensed, not sold. The Licensed Content is licensed on a **one copy per user basis**, such that you must acquire a license for each individual that accesses or uses the Licensed Content.
- 2.1 Below are five separate sets of use rights. Only one set of rights apply to you.
 1. **If you are a Microsoft Imagine Academy (MSIA) Program Member:**
 1. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
 2. For each license you acquire on behalf of an End User or Trainer, you may either:
 1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User who is enrolled in the Authorized Training Session, and only immediately prior to the commencement of the Authorized Training Session that is the subject matter of the Microsoft Instructor-Led Courseware being provided, **or**
 2. provide one (1) End User with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
 3. provide one (1) Trainer with the unique redemption code and instructions on how they can access one (1) Trainer Content.
 3. For each license you acquire, you must comply with the following:
 1. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
 2. you will ensure each End User attending an Authorized Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Authorized Training Session,
 3. you will ensure that each End User provided with the hard-copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End

User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,

4. you will ensure that each Trainer teaching an Authorized Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Authorized Training Session,
5. you will only use qualified Trainers who have in-depth knowledge of and experience with the Microsoft technology that is the subject of the Microsoft Instructor-Led Courseware being taught for all your Authorized Training Sessions,
6. you will only deliver a maximum of 15 hours of training per week for each Authorized Training Session that uses a MOC title, and
7. you acknowledge that Trainers that are not MCTs will not have access to all of the trainer resources for the Microsoft Instructor-Led Courseware.

2. If you are a Microsoft Learning Competency Member:

1. Each license acquire may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
2. For each license you acquire on behalf of an End User or MCT, you may either:
 1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User attending the Authorized Training Session and only immediately prior to the commencement of the Authorized Training Session that is the subject matter of the Microsoft Instructor-Led Courseware provided, **or**
 2. provide one (1) End User attending the Authorized Training Session with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
 3. you will provide one (1) MCT with the unique redemption code and instructions on how they can access one (1) Trainer Content.
3. For each license you acquire, you must comply with the following:
 1. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
 2. you will ensure that each End User attending an Authorized Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Authorized Training Session,
 3. you will ensure that each End User provided with a hard-copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,

4. you will ensure that each MCT teaching an Authorized Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Authorized Training Session,
5. you will only use qualified MCTs who also hold the applicable Microsoft Certification credential that is the subject of the MOC title being taught for all your Authorized Training Sessions using MOC,
6. you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and
7. you will only provide access to the Trainer Content to MCTs.

3. If you are a MPN Member:

1. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
2. For each license you acquire on behalf of an End User or Trainer, you may either:
 1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User attending the Private Training Session, and only immediately prior to the commencement of the Private Training Session that is the subject matter of the Microsoft Instructor-Led Courseware being provided, **or**
 2. provide one (1) End User who is attending the Private Training Session with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
 3. you will provide one (1) Trainer who is teaching the Private Training Session with the unique redemption code and instructions on how they can access one (1) Trainer Content.
3. For each license you acquire, you must comply with the following:
 1. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
 2. you will ensure that each End User attending an Private Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Private Training Session,
 3. you will ensure that each End User provided with a hard copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,
 4. you will ensure that each Trainer teaching an Private Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Private Training Session,

5. you will only use qualified Trainers who hold the applicable Microsoft Certification credential that is the subject of the Microsoft Instructor-Led Courseware being taught for all your Private Training Sessions,
6. you will only use qualified MCTs who hold the applicable Microsoft Certification credential that is the subject of the MOC title being taught for all your Private Training Sessions using MOC,
7. you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and
8. you will only provide access to the Trainer Content to Trainers.

4. If you are an End User:

For each license you acquire, you may use the Microsoft Instructor-Led Courseware solely for your personal training use. If the Microsoft Instructor-Led Courseware is in digital format, you may access the Microsoft Instructor-Led Courseware online using the unique redemption code provided to you by the training provider and install and use one (1) copy of the Microsoft Instructor-Led Courseware on up to three (3) Personal Devices. You may also print one (1) copy of the Microsoft Instructor-Led Courseware. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.

5. If you are a Trainer.

1. For each license you acquire, you may install and use one (1) copy of the Trainer Content in the form provided to you on one (1) Personal Device solely to prepare and deliver an Authorized Training Session or Private Training Session, and install one (1) additional copy on another Personal Device as a backup copy, which may be used only to reinstall the Trainer Content. You may not install or use a copy of the Trainer Content on a device you do not own or control. You may also print one (1) copy of the Trainer Content solely to prepare for and deliver an Authorized Training Session or Private Training Session.

2. If you are an MCT, you may customize the written portions of the Trainer Content that are logically associated with instruction of a training session in accordance with the most recent version of the MCT agreement.
3. If you elect to exercise the foregoing rights, you agree to comply with the following: (i) customizations may only be used for teaching Authorized Training Sessions and Private Training Sessions, and (ii) all customizations will comply with this agreement. For clarity, any use of "customize" refers only to changing the order of slides and content, and/or not using all the slides or content, it does not mean changing or modifying any slide or content.

- 2.2 **Separation of Components.** The Licensed Content is licensed as a single unit and you may not separate their components and install them on different devices.
- 2.3 **Redistribution of Licensed Content.** Except as expressly provided in the use rights above, you may not distribute any Licensed Content or any portion thereof (including any permitted modifications) to any third parties without the express written permission of Microsoft.
- 2.4 **Third Party Notices.** The Licensed Content may include third party code that Microsoft, not the third party, licenses to you under this agreement. Notices, if any, for the third party code are included for your information only.
- 2.5 **Additional Terms.** Some Licensed Content may contain components with additional terms, conditions, and licenses regarding its use. Any non-conflicting terms in those conditions and licenses also apply to your use of that respective component and supplements the terms described in this agreement.

3. **LICENSED CONTENT BASED ON PRE-RELEASE TECHNOLOGY.** If the Licensed Content's subject matter is based on a pre-release version of Microsoft technology ("Pre-release"), then in addition to the other provisions in this agreement, these terms also apply:
 1. **Pre-Release Licensed Content.** This Licensed Content subject matter is on the Pre-release version of the Microsoft technology. The technology may not work the way a final version of the technology will and we may change the technology for the final version. We also may not release a final version. Licensed Content based on the final version of the technology may not contain the same information as the Licensed Content based on the Pre-release version. Microsoft is under no obligation to provide you with any further content, including any Licensed Content based on the final version of the technology.
 2. **Feedback.** If you agree to give feedback about the Licensed Content to Microsoft, either directly or through its third party designee, you give to Microsoft without charge, the right to use, share and commercialize your feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft technology, Microsoft product, or service that includes the feedback. You will not give feedback that is subject to a license that requires Microsoft to license its technology, technologies, or products to third parties because we include your feedback in them. These rights survive this agreement.
 3. **Pre-release Term.** If you are an Microsoft Imagine Academy Program Member, Microsoft Learning Competency Member, MPN Member, Microsoft Learn for Educators – Validated Educator, or Trainer, you will cease using all copies of the Licensed Content on the Pre-release technology upon (i) the date which Microsoft informs you is the end date for using the Licensed Content on the Pre-release technology, or (ii) sixty (60) days after the commercial release of the technology that is the subject of the Licensed Content, whichever is earliest ("Pre-release term"). Upon expiration or termination of the Pre-release term, you will irretrievably delete and destroy all copies of the Licensed Content in your possession or under your control.
4. **SCOPE OF LICENSE.** The Licensed Content is licensed, not sold. This agreement only gives you some rights to use the Licensed Content. Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the Licensed Content only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the Licensed Content that only allows you to use it in certain ways. Except as expressly permitted in this agreement, you may not:
 - access or allow any individual to access the Licensed Content if they have not acquired a valid license for the Licensed Content,
 - alter, remove or obscure any copyright or other protective notices (including watermarks), branding or identifications contained in the Licensed Content,
 - modify or create a derivative work of any Licensed Content,
 - publicly display, or make the Licensed Content available for others to access or use,
 - copy, print, install, sell, publish, transmit, lend, adapt, reuse, link to or post, make available or distribute the Licensed Content to any third party,
 - work around any technical limitations in the Licensed Content, or
 - reverse engineer, decompile, remove or otherwise thwart any protections or disassemble the Licensed Content except and only to the extent that applicable law expressly permits, despite this limitation.
5. **RESERVATION OF RIGHTS AND OWNERSHIP.** Microsoft reserves all rights not expressly granted to you in this agreement. The Licensed Content is protected by copyright and other intellectual property

laws and treaties. Microsoft or its suppliers own the title, copyright, and other intellectual property rights in the Licensed Content.

6. **EXPORT RESTRICTIONS.** The Licensed Content is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the Licensed Content. These laws include restrictions on destinations, end users and end use. For additional information, see www.microsoft.com/exporting.
7. **SUPPORT SERVICES.** Because the Licensed Content is provided "as is", we are not obligated to provide support services for it.
8. **TERMINATION.** Without prejudice to any other rights, Microsoft may terminate this agreement if you fail to comply with the terms and conditions of this agreement. Upon termination of this agreement for any reason, you will immediately stop all use of and delete and destroy all copies of the Licensed Content in your possession or under your control.
9. **LINKS TO THIRD PARTY SITES.** You may link to third party sites through the use of the Licensed Content. The third party sites are not under the control of Microsoft, and Microsoft is not responsible for the contents of any third party sites, any links contained in third party sites, or any changes or updates to third party sites. Microsoft is not responsible for webcasting or any other form of transmission received from any third party sites. Microsoft is providing these links to third party sites to you only as a convenience, and the inclusion of any link does not imply an endorsement by Microsoft of the third party site.
10. **ENTIRE AGREEMENT.** This agreement, and any additional terms for the Trainer Content, updates and supplements are the entire agreement for the Licensed Content, updates and supplements.
11. **APPLICABLE LAW.**
 1. United States. If you acquired the Licensed Content in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.
 2. Outside the United States. If you acquired the Licensed Content in any other country, the laws of that country apply.
12. **LEGAL EFFECT.** This agreement describes certain legal rights. You may have other rights under the laws of your country. You may also have rights with respect to the party from whom you acquired the Licensed Content. This agreement does not change your rights under the laws of your country if the laws of your country do not permit it to do so.
13. **DISCLAIMER OF WARRANTY. THE LICENSED CONTENT IS LICENSED "AS-IS" AND "AS AVAILABLE." YOU BEAR THE RISK OF USING IT. MICROSOFT AND ITS RESPECTIVE AFFILIATES GIVES NO EXPRESS WARRANTIES, GUARANTEES, OR CONDITIONS. YOU MAY HAVE ADDITIONAL CONSUMER RIGHTS UNDER YOUR LOCAL LAWS WHICH THIS AGREEMENT CANNOT CHANGE. TO THE EXTENT PERMITTED UNDER YOUR LOCAL LAWS, MICROSOFT AND ITS RESPECTIVE AFFILIATES EXCLUDES ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.**
14. **LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES. YOU CAN RECOVER FROM MICROSOFT, ITS RESPECTIVE AFFILIATES AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO US\$5.00. YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES.**

This limitation applies to

- anything related to the Licensed Content, services, content (including code) on third party Internet sites or third-party programs; and
- claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

It also applies even if Microsoft knew or should have known about the possibility of the damages. The above limitation or exclusion may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential, or other damages.

Please note: As this Licensed Content is distributed in Quebec, Canada, some of the clauses in this agreement are provided below in French.

Remarque : Ce le contenu sous licence étant distribué au Québec, Canada, certaines des clauses dans ce contrat sont fournies ci-dessous en français.

EXONÉRATION DE GARANTIE. Le contenu sous licence visé par une licence est offert « tel quel ». Toute utilisation de ce contenu sous licence est à votre seule risque et péril. Microsoft n'accorde aucune autre garantie expresse. Vous pouvez bénéficier de droits additionnels en vertu du droit local sur la protection dues consommateurs, que ce contrat ne peut modifier. La ou elles sont permises par le droit locale, les garanties implicites de qualité marchande, d'adéquation à un usage particulier et d'absence de contrefaçon sont exclues.

LIMITATION DES DOMMAGES-INTÉRÊTS ET EXCLUSION DE RESPONSABILITÉ POUR LES DOMMAGES. Vous pouvez obtenir de Microsoft et de ses fournisseurs une indemnisation en cas de dommages directs uniquement à hauteur de 5,00 \$ US. Vous ne pouvez prétendre à aucune indemnisation pour les autres dommages, y compris les dommages spéciaux, indirects ou accessoires et pertes de bénéfices.

Cette limitation concerne:

- tout ce qui est relié au le contenu sous licence, aux services ou au contenu (y compris le code) figurant sur des sites Internet tiers ou dans des programmes tiers; et.
- les réclamations au titre de violation de contrat ou de garantie, ou au titre de responsabilité stricte, de négligence ou d'une autre faute dans la limite autorisée par la loi en vigueur.

Elle s'applique également, même si Microsoft connaissait ou devrait connaître l'éventualité d'un tel dommage. Si votre pays n'autorise pas l'exclusion ou la limitation de responsabilité pour les dommages indirects, accessoires ou de quelque nature que ce soit, il se peut que la limitation ou l'exclusion ci-dessus ne s'appliquera pas à votre égard.

EFFET JURIDIQUE. Le présent contrat décrit certains droits juridiques. Vous pourriez avoir d'autres droits prévus par les lois de votre pays. Le présent contrat ne modifie pas les droits que vous confèrent les lois de votre pays si celles-ci ne le permettent pas.

Revised April 2019



Contents

■	Module 0 Course Introduction	1
	Welcome to Microsoft Security Operations Analyst	1
■	Module 1 Mitigate threats using Microsoft Defender for Endpoint	3
	Protect against threats with Microsoft Defender for Endpoint	3
	Deploy the Microsoft Defender for Endpoint environment	11
	Implement Windows 10 security enhancements	17
	Manage alerts and incidents	23
	Perform device investigations	39
	Perform actions on a device	49
	Perform evidence and entities investigations	59
	Configure and manage automation	69
	Configure for alerts and detections	76
	Utilize Threat and Vulnerability Management	84
	Knowledge check	90
	Lab - Mitigate threats using Defender for Endpoint	93
■	Module 2 Mitigate threats using Microsoft 365 Defender	99
	Introduction to threat protection with Microsoft 365	99
	Mitigate incidents using Microsoft 365 Defender	103
	Protect your identities with Azure AD Identity Protection	112
	Remediate risks with Microsoft Defender for Office 365	123
	Safeguard your environment with Microsoft Defender for Identity	129
	Microsoft Cloud App Security	135
	Respond to data loss prevention alerts	143
	Manage insider risk in Microsoft 365	149
	Knowledge check	157
	Lab - Mitigate threats using Microsoft 365 Defender	159
■	Module 3 Mitigate threats using Azure Defender	163
	Plan for cloud workload protections using Azure Defender	163
	Explain cloud workload protections in Azure Defender	176
	Connect Azure assets to Azure Defender	189
	Connect non-Azure resources to Azure Defender	198
	Remediate security alerts using Azure Defender	208
	Knowledge check	227

Lab - Mitigate threats using Azure Defender	230
Module 4 Create queries for Azure Sentinel using Kusto Query Language	235
Construct KQL statements for Azure Sentinel	235
Analyze query results using KQL	242
Build multi-table statements using KQL	248
Work with string data using KQL statements	251
Knowledge check	260
Lab - Create queries for Azure Sentinel using KQL	262
Module 5 Configure your Azure Sentinel environment	267
Introduction to Azure Sentinel	267
Create and manage Azure Sentinel workspaces	274
Query logs in Azure Sentinel	281
Use watchlists in Azure Sentinel	284
Utilize threat intelligence in Azure Sentinel	286
Knowledge check	289
Lab - Configure your Azure Sentinel environment	291
Module 6 Connect logs to Azure Sentinel	295
Connect data to Azure Sentinel using data connectors	295
Connect Microsoft services to Azure Sentinel	300
Connect Microsoft 365 Defender to Azure Sentinel	304
Connect Windows hosts to Azure Sentinel	309
Connect Common Event Format logs to Azure Sentinel	313
Connect syslog data sources to Azure Sentinel	316
Connect threat indicators to Azure Sentinel	321
Knowledge check	325
Lab - Connect logs to Azure Sentinel	329
Module 7 Create detections and perform investigations using Azure Sentinel	335
Threat detection with Azure Sentinel analytics	335
Threat response with Azure Sentinel playbooks	348
Security incident management in Azure Sentinel	358
Use entity behavior analytics in Azure Sentinel	365
Query, visualize, and monitor data in Azure Sentinel	372
Knowledge check	382
Lab - Create detections and perform investigations	383
Module 8 Perform threat hunting in Azure Sentinel	385
Threat hunting concepts in Azure Sentinel	385
Threat hunting with Azure Sentinel	388
Hunt for threats using notebooks in Azure Sentinel	396
Knowledge check	401
Lab - Threat hunting in Azure Sentinel	403

Module 0 Course Introduction

Welcome to Microsoft Security Operations Analyst

About this course

Course Description

Learn how to investigate, respond to, and hunt for threats using Microsoft Azure Sentinel, Azure Defender, and Microsoft 365 Defender. In this course you will learn how to mitigate cyberthreats using these technologies. Specifically, you will configure and use Azure Sentinel as well as utilize Kusto Query Language (KQL) to perform detection, analysis, and reporting. The course was designed for people who work in a Security Operations job role and helps learners prepare for the exam SC-200: Microsoft Security Operations Analyst.

Level

Intermediate

Audience

The Microsoft Security Operations Analyst collaborates with organizational stakeholders to secure information technology systems for the organization. Their goal is to reduce organizational risk by rapidly remediating active attacks in the environment, advising on improvements to threat protection practices, and referring violations of organizational policies to appropriate stakeholders.

Responsibilities include threat management, monitoring, and response by using a variety of security solutions across their environment. The role primarily investigates, responds to, and hunts for threats using Microsoft Azure Sentinel, Azure Defender, Microsoft 365 Defender, and third-party security products. Since the Security Operations Analyst consumes the operational output of these tools, they are also a critical stakeholder in the configuration and deployment of these technologies.

Prerequisites

- Basic understanding of Microsoft 365
- Fundamental understanding of Microsoft security, compliance, and identity products

- Intermediate understanding of Windows 10
- Familiarity with Azure services, specifically Azure SQL Database and Azure Storage
- Familiarity with Azure virtual machines and virtual networking
- Basic understanding of scripting concepts.

Expected learning

- Explain how Microsoft Defender for Endpoint can remediate risks in your environment
- Create a Microsoft Defender for Endpoint environment
- Configure Attack Surface Reduction rules on Windows 10 devices
- Perform actions on a device using Microsoft Defender for Endpoint
- Investigate domains and IP addresses in Microsoft Defender for Endpoint
- Investigate user accounts in Microsoft Defender for Endpoint
- Configure alert settings in Microsoft Defender for Endpoint
- Explain how the threat landscape is evolving
- Conduct advanced hunting in Microsoft 365 Defender
- Manage incidents in Microsoft 365 Defender
- Explain how Microsoft Defender for Identity can remediate risks in your environment
- Investigate DLP alerts in Microsoft Cloud App Security
- Explain the types of actions you can take on an insider risk management case
- Configure auto-provisioning in Azure Defender
- Remediate alerts in Azure Defender
- Construct KQL statements
- Filter searches based on event time, severity, domain, and other relevant data using KQL
- Extract data from unstructured string fields using KQL
- Manage an Azure Sentinel workspace
- Use KQL to access the watchlist in Azure Sentinel
- Manage threat indicators in Azure Sentinel
- Explain the Common Event Format and Syslog connector differences in Azure Sentinel

Module 1 Mitigate threats using Microsoft Defender for Endpoint

Protect against threats with Microsoft Defender for Endpoint

Lesson introduction

Learn how Microsoft Defender for Endpoint can help your organization stay secure.

Learning objectives

After completing this lesson, you should be able to:

- Define the capabilities of Microsoft Defender for Endpoint.
- Describe how to hunt threats within your network.
- Explain how Microsoft Defender for Endpoint can remediate risks in your environment.

Microsoft Defender for Endpoint explained

Microsoft Defender for Endpoint is a platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats on their endpoints.



The following capabilities are enabled with Microsoft Defender for Endpoint:

- Threat and vulnerability management provides real-time visibility and helps identify ways to improve your security posture.
- Attack surface reduction eliminates risky or unnecessary surface areas and restricts dangerous code from running.
- Advanced protection uses machine learning and deep analysis to protect against file-based malware.
- Endpoint detection and response monitors behaviors and attacker techniques to detect and respond to advanced attacks.
- Leverage artificial intelligence to automatically investigate alerts and remediate complex threats in minutes.
- Microsoft threat experts bring deep knowledge and proactive threat hunting to your security operations Center.

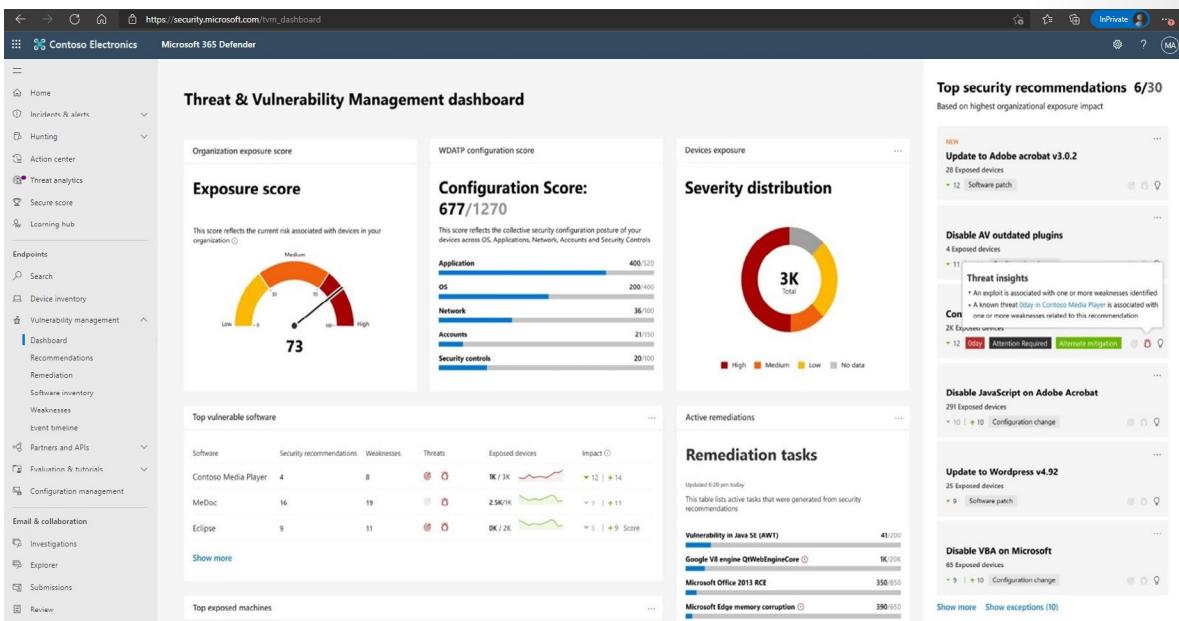
Microsoft Defender for Endpoint uses the following combination of technologies built into Windows 10 and Microsoft's robust cloud service:

- **Endpoint behavioral sensors.** Embedded in Windows 10, these sensors collect and process behavioral signals from the operating system. The sensors send the data to your private, isolated cloud instance of Microsoft Defender for Endpoint.
- **Cloud security analytics.** Leveraging big data, machine learning, and unique Microsoft optics across the Windows ecosystem, enterprise cloud products (such as Office 365), and online assets, behavioral signals are translated into insights, detections, and recommended responses to advanced threats.
- **Threat intelligence.** Generated by Microsoft hunters and security teams, and augmented by threat intelligence provided by partners, threat intelligence enables Microsoft Defender for Endpoint to identify attacker tools, techniques, and procedures, and generate alerts when these are observed in collected sensor data.

Practice security administration

You can use the Microsoft 365 Defender portal (<https://security.microsoft.com>¹) to manage Microsoft Defender for Endpoint.

Threat and vulnerability management



Effectively identifying, assessing, and remediating endpoint weaknesses is pivotal to running a healthy security program and reducing organizational risk. Threat and vulnerability management serves as an infrastructure for reducing organizational exposure, hardening endpoint surface area, and increasing organizational resilience.

This infrastructure helps organizations discover vulnerabilities and misconfigurations in real time, based on sensors, without the need of agents or periodic scans. It prioritizes issues based on a number of factors. Those factors include the threat landscape, detections in your organization, sensitive information on vulnerable devices, and business context.

Threat and vulnerability management is built-in, real-time, cloud-powered, fully integrated with the Microsoft endpoint security stack, the Microsoft Intelligent Security Graph, and the application analytics knowledge base. It can create a security task or ticket through integration with Microsoft Intune and Microsoft Endpoint Manager.

It provides the following solutions to gaps across security operations, security administration, and IT administration:

- Real-time endpoint detection and response (EDR) insights correlated with endpoint vulnerabilities
- Linked machine vulnerability and security configuration assessment data in the context of exposure discovery
- Built-in remediation processes through Microsoft Intune and Microsoft Endpoint Manager

For example, using the security recommendations present in the portal, an administrator could request that an application be updated, which would then notify the Intune team to remediate the request.

¹ <https://security.microsoft.com/?azure-portal=true>

The screenshot shows the Microsoft 365 Defender interface under the 'Vulnerability management' section. On the left, a sidebar lists various security features like Home, Incidents & alerts, Hunting, Action center, Threat analytics, Secure score, Learning hub, Endpoints, Search, Device inventory, and more. The main pane displays a table titled 'Security recommendations' with columns: Security recommendation, Weaknesses, Related component, Threats, and Exposed machines. One item is highlighted: 'Update VLC Media Player to version 3.0.8.0'. To the right, a modal window titled 'Request remediation for: Update VLC Media Player to version 3.0.8.0' is open. It includes fields for 'Exposed machines' (1/1), 'Action' (set to 'Update'), 'IT service and device management tools' (choose ServiceNow), 'Due date' (set to Tue Nov 05 2019), and 'Add notes (optional)' (with the note 'Please update to the latest version'). At the bottom of the modal is a 'Submit request' button.

Attack surface reduction

The attack surface reduction set of capabilities provides the first line of defense in the stack by ensuring configuration settings are properly set and exploit mitigation techniques are applied.

- **Hardware-based isolation** protects and maintains the integrity of the system as it starts and while it's running, and validates system integrity through local and remote attestation. Container isolation for Microsoft Edge helps protect the host operating system from malicious websites.
- **Application control** moves away from the traditional application trust model where all applications are assumed trustworthy by default to one where applications must earn trust in order to run.
- **Exploit protection** applies mitigation techniques to apps your organization uses, both individually and organization-wide.
- **Network protection** extends the malware and social engineering protection offered by Microsoft Defender SmartScreen in Microsoft Edge to cover network traffic and connectivity on your organization's devices.
- **Controlled folder access** helps protect files in key system folders from changes made by malicious and suspicious apps, including file-encrypting ransomware malware.
- **Attack surface reduction** reduces the attack surface of your applications with intelligent rules that stop the vectors used by Office-, script- and mail-based malware.
- **Network firewall** uses host-based, two-way network traffic filtering that blocks unauthorized network traffic flowing into or out of the local device.

The below screenshot shows a chart of detections against an attack surface reduction rule that is protecting office applications:

The screenshot shows the Microsoft 365 Defender Detections interface. The left sidebar includes sections like Home, Incidents & alerts, Hunting, Action center, Threat analytics, Secure score, Learning hub, Endpoints, Email & collaboration, and Policies & rules. The main content area is titled 'Attack surface reduction rules' and displays a bar chart showing activity over time. Below the chart is a table titled 'Block all Office applications from creating child processes (12)'.

Detected file	Detected on	Blocked/Audited?	Rule	Source app	Device	User	Publisher
FinanceWordDoc.docm	November 3, 2019 5:29 PM	Blocked	Block all Office applications from creat...	WINWORD.EXE	ignite-2	ignite	
FinanceWordDoc.docm	November 3, 2019 5:26 PM	Blocked	Block all Office applications from creat...	WINWORD.EXE	ignite-2	ignite	
FinanceWordDoc.docm	November 3, 2019 5:25 PM	Blocked	Block all Office applications from creat...	WINWORD.EXE	ignite-2	ignite	
FinanceWordDoc.docm	November 1, 2019 7:01 PM	Audited	Block all Office applications from creat...	WINWORD.EXE	desktop-b78tdkr	avalev	
FinanceWordDoc.docm	November 1, 2019 6:37 PM	Blocked	Block all Office applications from creat...	WINWORD.EXE	ignite-2	ignite	

Next generation protection

Microsoft Defender Antivirus is a built-in antimalware solution that provides next generation protection for desktops, portable computers, and servers. Microsoft Defender Antivirus includes:

- Cloud-delivered protection for near-instant detection and blocking of new and emerging threats. Along with machine learning and the Intelligent Security Graph, cloud-delivered protection is part of the next-gen technologies that power Microsoft Defender Antivirus.
- Always-on scanning, using advanced file and process behavior monitoring and other heuristics (also known as "real-time protection").
- Dedicated protection updates based on machine-learning, human and automated big-data analysis, and in-depth threat resistance research.

The following proxy and network settings should be considered:

- The Microsoft Defender for Endpoint sensor requires Microsoft Windows HTTP (WinHTTP) to report sensor data and communicate with the Microsoft Defender for Endpoint service.
- The embedded Microsoft Defender for Endpoint sensor runs in system context using the LocalSystem account. The sensor uses Microsoft Windows HTTP Services (WinHTTP) to enable communication with the Microsoft Defender for Endpoint cloud service.
- The WinHTTP configuration setting is independent of the Windows Internet (WinINet) internet browsing proxy settings and can only discover a proxy server by using the following auto discovery methods:
 - Transparent proxy
 - Web Proxy Auto-discovery Protocol (WPAD)

Endpoint detection and response

Microsoft Defender for Endpoint endpoint detection and response capabilities provide advanced attack detections that are near real-time and actionable. Security analysts can prioritize alerts effectively, gain visibility into the full scope of a breach, and take response actions to remediate threats.

When a threat is detected, alerts are created in the system for an analyst to investigate. Alerts with the same attack techniques or attributed to the same attacker are aggregated into an entity called an **incident**. Aggregating alerts in this manner makes it easy for analysts to collectively investigate and respond to threats.

Inspired by the “assume breach” mindset, Microsoft Defender for Endpoint continuously collects behavioral cyber telemetry. This includes process information, network activities, deep optics into the kernel and memory manager, user login activities, registry and file system changes, and others. The information is stored for six months, enabling an analyst to travel back in time to the start of an attack. The analyst can then pivot using various views and approach an investigation through multiple vectors.

Action Center

Microsoft Defender for Endpoint offers a wide breadth of visibility on multiple machines. With this kind of optics, the service generates a multitude of alerts. The volume of alerts generated can be challenging for a typical security operations team to individually address. To address this challenge, Microsoft Defender for Endpoint uses Action center to manage the alerts that must be investigated individually.

Action center shows you the investigations created by automated investigation and response capabilities. This automated, self-healing in Microsoft 365 Defender can help security teams by automatically responding to specific events.

The automated investigation feature uses various inspection algorithms, and processes used by analysts (such as playbooks) to examine alerts and take immediate remediation action to resolve breaches. This significantly reduces alert volume, allowing security operations experts to focus on more sophisticated threats and other high value initiatives.

Hunt threats within your network

Advanced hunting within Microsoft 365 Defender allows you to hunt for possible threats across your organization using a powerful search and query tool. You can proactively inspect events in your network in order to locate interesting indicators and entities. The flexible access to data aids unconstrained hunting for both known and potential threats.

Explore how to hunt for threats with Microsoft 365 Defender

These rules run automatically to check for and respond to various events and system states, including suspected breach activity and misconfigured machines.

The screenshot shows the Azure Kusto Query Editor interface. The title bar says "Advanced hunting". Below it, there are two tabs: "Get started" and "Query", with "Query" being the active tab. A toolbar with buttons for "Run query", "Save query", "Copy query to clipboard", and "Last 30 days" is visible. On the right side of the toolbar are "Help" and a refresh icon. The main area contains a Kusto query:

```
1 //Finds PowerShell execution events that could involve a download
2 ProcessCreationEvents
3 where EventTime > ago(7d)
4 where FileName > ("powershell.exe", "POWERSHELL.EXE", "powershell_ise.exe", "POWERSHELL_ISE.EXE")
5 where ProcessCommandLine has "Net.WebClient"
6 or ProcessCommandLine has "DownloadFile"
7 or ProcessCommandLine has "Invoke-WebRequest"
8 or ProcessCommandLine has "Invoke-Shellcode"
9 or ProcessCommandLine contains "http:"
10 project EventTime, ComputerName, InitiatingProcessFileName, Filename, ProcessCommandLine
11 top 100 by EventTime
12
```

Advanced hunting is based on the Kusto query language. The following operators are allowed:

- **where**. Filter a table to the subset of rows that satisfy a predicate.
- **summarize**. Produce a table that aggregates the content of the input table.
- **join** Merge the rows of two tables to form a new table by matching values of the specified column(s) from each table.
- **count**. Return the number of records in the input record set.
- **top**. Return the first N records sorted by the specified columns.
- **limit**. Return up to the specified number of rows.
- **project**. Select the columns to include, rename or drop, and insert new computed columns.
- **extend**. Create calculated columns and append them to the result set.
- **makeset()**. Return a dynamic (JSON) array of the set of distinct values that Expr takes in the group.
- **find**. Find rows that match a predicate across a set of tables.

In the screenshot above, the following filters have been written:

- Time filter to review only records from the previous seven days.
- Filter on the FileName to contain only instances of powershell.exe.
- Filter on the ProcessCommandLine.
- Project only the columns you're interested in exploring and limit the results to 100.

Best practices

The following best practices can be followed to ensure query performance:

- Apply filters first - Azure Kusto is highly optimized to utilize time filters.
- Use the **has** keyword over **contains** when looking for full tokens.
- Use **looking in specific column** rather than using full text search across all columns.
- When joining between two tables, choose the table with less rows to be the first one (left-most).
- When joining between two tables, project only needed columns from both sides of the join.

Here's an example of a Kusto query for process creation with suspicious file endings:

```
ProcessCreationEvents
| where EventTime > ago(7d)
| where FileName endswith ".pdf.exe"
    or FileName endswith ".doc.exe"
    or FileName endswith ".docx.exe"
    or FileName endswith ".jpg.exe"
    or FileName endswith ".jpeg.exe"
| project EventTime, ComputerName, FileName, AccountSid, AccountName,
AccountDomain
| top 100 by EventTime
```

Deploy the Microsoft Defender for Endpoint environment

Lesson introduction

Deploying the Microsoft Defender for Endpoint environment involves configuring your tenant, onboard-ing your devices, and configuring security team access.

You are a Security Operations Analyst working at a company that is implementing Microsoft Defender for Endpoint. Your manager plans to onboard a few devices to provide insight into required changes to the SecOps team response procedures.

You start by initializing the Defender for Endpoint environment—next, you onboard the initial devices for your deployment by running the onboarding script on the devices. You configure security for the environment. Next, you create Device groups and assign the appropriate devices.

Learning objectives

After completing this lesson, you should be able to:

- Create a Microsoft Defender for Endpoint environment
- Onboard devices to be monitored by Microsoft Defender for Endpoint

Create your environment

When accessing your Microsoft 365 Defender portal (<https://security.microsoft.com>²) for the first time, a wizard will guide you through some initial steps. You must be a global administrator or security administrator for the tenant. On the Set up preferences page, you can set the:

Data storage location - Determine where you want your tenant to be primarily hosted. You cannot change the location after this set up and Microsoft will not transfer the data from the specified geolocation.

Data retention - The default is six months.

Enable preview features - The default is on, can be changed later.

At the end of the setup wizard, there will be a dedicated cloud instance of Defender for Endpoint created.

Network configuration

If the organization does not require the endpoints to use a Proxy to access the Internet, the following configuration is not required.

The Microsoft Defender for Endpoint sensor requires Microsoft Windows HTTP (WinHTTP) to report sensor data and communicate with the Microsoft Defender for Endpoint service. The embedded Microsoft Defender for Endpoint sensor runs in the system context using the LocalSystem account. The sensor uses Microsoft Windows HTTP Services (WinHTTP) to enable communication with the Microsoft Defender for Endpoint cloud service. The WinHTTP configuration setting is independent of the Windows Internet (WinINet) internet browsing proxy settings and can only discover a proxy server by using the following discovery methods:

² <https://security.microsoft.com/?azure-portal=true>

Autodiscovery methods:

- Transparent proxy
- Web Proxy Autodiscovery Protocol (WPAD)

If a Transparent proxy or WPAD has been implemented in the network topology, there is no need for special configuration settings.

Onboard devices

You'll need to go to the onboarding section of the Microsoft 365 Defender portal to onboard any of the supported devices. Depending on the device, you'll be guided with appropriate steps and provided management and deployment tool options suitable for the device.

In general, to onboard devices to the service:

- Verify that the device fulfills the minimum requirements
- Depending on the device, follow the configuration steps provided in the onboarding section of the Defender for Endpoint portal
- Use the appropriate management tool and deployment method for your devices
- Run a detection test to verify that the devices are properly onboarded and reporting to the service

In the Microsoft 365 Defender portal select **Settings**, and then select **Endpoints**, under Device Management select **Onboarding** and then select **Select operating system...** dropdown to see the supported options.

The screenshot shows the Microsoft 365 Defender portal interface. The left sidebar is collapsed, and the main area shows the 'Endpoints' section. Under 'Onboarding', a dropdown menu is open, titled 'Select operating system to start onboarding process'. The 'Windows 10' option is selected. Below the dropdown, there is a note about deploying at scale and a link to 'Configure devices using a local script'. A 'Download package' button is visible. To the right, there is a section for 'Run a detection test' with a note about verifying device status and a command-line script for PowerShell. A 'Copy' button is present next to the script. At the bottom, a message indicates success will mark the detection test as completed.

After selecting the operating system option, the supported deployment options are outlined. Here is a list of the Windows 10 supported deployment options:

- Group Policy
- Microsoft Endpoint Configuration Manager
- Mobile Device Management (including Microsoft Intune)
- Local script

- VDI onboarding script for non-persistent devices

Select operating system to start onboarding process: Windows 10

1. Onboard a device

First device onboarded: Incomplete

Onboard devices to Microsoft Defender for Endpoint using the onboarding configuration package that matches your preferred deployment method. For other device preparation instructions, read [Onboard and set up](#).

Deployment method:

- Local Script (for up to 10 devices) **(selected)**
- Group Policy
- Microsoft Endpoint Configuration Manager current branch and later
- System Center Configuration Manager 2012 / 2012 R2 / 1511 / 1602
- Mobile Device Management / Microsoft Intune
- VDI onboarding scripts for non-persistent devices

2. Run a detection test

First device detection test Incomplete

To verify that the device is properly onboarded and reporting to the service, run the detection script on the newly onboarded device:

- Open a Command Prompt window
- At the prompt, copy and run the command below. The Command Prompt window will close automatically.

```
powershell.exe -NoExit -ExecutionPolicy Bypass -WindowStyle Hidden $ErrorActionPreference='SilentlyContinue';(New-Object System.Net.WebClient).DownloadFile('http://127.0.0.1/test.exe', 'C:\test-HQATP-test\Invoice.exe')|Start-Process 'C:\test-HQATP-test\Invoice.exe'
```

If successful, the detection test will be marked as completed and a new alert will appear in few minutes.

As you can see, there are many configuration options.

Offboarding devices

In Settings, Device Management, Offboarding, select **operating system** dropdown to see the direction to offboard devices.

Manage access

Using role-based access control (RBAC), you can create roles and groups within your security operations team to grant appropriate access to the portal. Based on the roles and groups you create, you have fine-grained control over what users with access to the portal can see and do.

Defender for Endpoint RBAC is designed to support your tier- or role-based model of choice and gives you granular control over what roles can see, devices they can access, and actions they can take. The RBAC framework is centered around the following controls:

- Control who can take specific actions:
 - Create custom roles and control what Defender for Endpoint capabilities they can access with granularity.
- Control who can see information on a specific device group or groups:
 - Create device groups by specific criteria such as names, tags, domains, and others, then grant role access to them using a specific Azure Active Directory (Azure AD) user group.

To implement role-based access, you'll need to define admin roles, assign corresponding permissions, and assign Azure AD user groups assigned to the roles.

Before using RBAC, you should understand the roles that can grant permissions and the consequences of turning on RBAC. When you first sign-in to Microsoft 365 Defender portal, you're granted either full access or read-only access. Full access rights are granted to users with Security Administrator or Global Administrator roles in Azure AD. read-only access is granted to users with a Security Reader role in Azure

AD. Someone with a Defender for Endpoint Global administrator role has unrestricted access to all devices, regardless of their device group association and the Azure AD user groups assignments

Create and manage roles for role-based access control

The following steps guide you on how to create roles in the Microsoft 365 Defender portal. It assumes that you have already created Azure Active Directory user groups.

1. Access the Microsoft 365 Defender portal using an account with a Security administrator or Global administrator role assigned.
2. In Microsoft 365 Defender portal, select **Permissions & roles**.
3. In the **Permissions & roles** screen under Endpoints roles & groups, select **Roles**.
4. Select **+ Add item**.
5. Enter the role name, description, and permissions you'd like to assign to the role.
6. On the **Assigned user groups** tab assign the role to an Azure AD Security group.
7. Use the filter to select the Azure AD group that you'd like to add to this role to.
8. Save and close.
9. Apply the configuration settings.

Important: After creating roles, you'll need to create a device group and provide access to the device group by assigning it to a role that you just created.

Permission options

The permission options:

- View data
 - Security operations - View all security operations data in the portal
 - Threat and vulnerability management - View threat and vulnerability management data in the portal
- Active remediation actions
 - Security operations - Take response actions, approve or dismiss pending remediation actions, manage allowed/blocked lists for automation and indicators
 - Threat and vulnerability management - Exception handling - Create new exceptions and manage active exceptions
 - Threat and vulnerability management - Remediation handling - Submit new remediation requests, create tickets, and manage existing remediation activities
- Alerts investigation - Manage alerts, start automated investigations, run scans, collect investigation packages, manage device tags, and download only portable executable (PE) files
- Manage security settings in Security Center - Configure alert suppression settings, manage folder exclusions for automation, onboard and offboard devices, and manage email notifications, manage evaluation lab

- Live response capabilities
 - Basic commands:
 - Start a live response session
 - Perform read-only live response commands on remote device (excluding file copy and execution)
 - Advanced commands:
 - Download a file from the remote device via live response
 - Download PE and non-PE files from the file page
 - Upload a file to the remote device
 - View a script from the files library
 - Execute a script on the remote device from the files library

Configure device groups

In an enterprise scenario, security operation teams are typically assigned a set of devices. These devices are grouped together based on a set of attributes such as their domains, computer names, or designated tags.

In Microsoft Defender for Endpoint, you can create device groups and use them to:

- Limit access to related alerts and data to specific Azure AD user groups with assigned RBAC roles
- Configure different auto-remediation settings for different sets of devices
- Assign specific remediation levels to apply during automated investigations
- In an investigation, filter the Devices list to just specific device groups by using the Group filter.

You can create device groups in the context of role-based access (RBAC) to control who can take specific action or see information by assigning the device group(s) to a user group.

As part of the process of creating a device group, you'll:

- Set the automated remediation level for that group.
- Specify the matching rule that determines which device group belongs to the group based on the device name, domain, tags, and OS platform. If a device is also matched to other groups, it is added only to the highest ranked device group.
- Select the Azure AD user group that should have access to the device group.
- Rank the device group relative to other groups after it is created.

Create a device group

To create a device group:

1. In the Microsoft 365 Defender portal, select **Settings**, and then select **Endpoints**, then under Permissions select **Device groups**.
2. Select **+ Add device group**.
3. Enter the device group name and automation settings and specify the matching rule that determines which devices belong to the group. See How the automated investigation starts.

4. Preview several devices that will be matched by this rule. If you are satisfied with the rule, select the User access tab.
5. Assign the user groups that can access the device group you created. You can only grant access to Azure AD user groups that have been assigned to RBAC roles.
6. Select **Done**. The configuration changes are applied.

Implement Windows 10 security enhancements

Lesson introduction

Microsoft Defender for Endpoint gives you various tools to eliminate risks by reducing the surface area for attacks without blocking user productivity.

You are a Security Operations Analyst working at a company that is implementing Microsoft Defender for Endpoint. You are responsible for working with the Endpoint management team to provide security configuration recommendations for Windows 10 devices.

You first review each Attack Surface Reduction component to understand the attack vector the component was designed to mitigate. You then work with the Endpoint management team to create a custom security baseline for the Windows 10 devices.

Learning objectives

After completing this lesson, you should be able to:

- Explain Attack Surface Reduction in Windows 10
- Enable Attack Surface Reduction rules on Windows 10 devices
- Configure Attack Surface Reduction rules on Windows 10 devices

Understand attack surface reduction

Attack Surface Reduction is hardening the places where a threat is likely to attack. As a Security Analyst, it is your role to understand the protection options and provide recommendations. While you are performing alert investigations, you should know the events generated by Attack Surface Reduction on the host, which might provide forensics evidence.

The following is a list of the Attack Surface Reduction components:

Solution	Description
Attack surface reduction	Reduce vulnerabilities (attack surfaces) in your applications with intelligent rules that help stop malware. (Requires Microsoft Defender Antivirus).
Hardware-based isolation	Protect and maintain the integrity of a system as it starts and while it's running. Validate system integrity through local and remote attestation. And, use container isolation for Microsoft Edge to help guard against malicious websites.
Application control	Use application control so that your applications must earn trust in order to run.
Exploit protection	Help protect operating systems and apps your organization uses from being exploited. Exploit protection also works with third-party antivirus solutions.

Solution	Description
Network protection	Extend protection to your network traffic and connectivity on your organization's devices. (Requires Microsoft Defender Antivirus).
Web protection	Secure your devices against web threats and help you regulate unwanted content.
Controlled folder access	Help prevent malicious or suspicious apps (including file-encrypting ransomware malware) from making changes to files in your key system folders (Requires Microsoft Defender Antivirus)
Network firewall	Prevent unauthorized traffic from flowing to or from your organization's devices with two-way network traffic filtering.

Enable attack surface reduction rules

Your attack surface includes all the places where an attacker could compromise your organization's devices or networks. Reducing your attack surface means protecting your organization's devices and network, which leaves attackers with fewer ways to perform attacks.

Attack surface reduction rules target certain software behaviors that are often abused by attackers. Such behaviors include:

- Launching executable files and scripts that attempt to download or run files
- Running obfuscated or otherwise suspicious scripts
- Performing behaviors that apps don't usually initiate during normal day-to-day work.

Such software behaviors are sometimes seen in legitimate applications; however, these behaviors are often considered risky because they are commonly abused by malware. Attack surface reduction rules can constrain risky behaviors and help keep your organization safe.

Each Attack Surface Reduction rule contains one of three settings:

- **Not configured:** Disable the attack surface reduction rule
- **Block:** Enable the Attack Surface Reduction rule
- **Audit:** Evaluate how the attack surface reduction rule would impact your organization if enabled

Attack surface reduction rules

Attack Surface Reduction rules currently supports all of the rules below:

- Block executable content from email client and webmail
- Block all Office applications from creating child processes
- Block Office applications from creating executable content
- Block Office applications from injecting code into other processes
- Block JavaScript or VBScript from launching downloaded executable content
- Block execution of potentially obfuscated scripts
- Block Win32 API calls from Office macro
- Use advanced protection against ransomware

- Block credential stealing from the Windows local security authority subsystem (lsass.exe)
- Block process creations originating from PSEexec and WMI commands
- Block untrusted and unsigned processes that run from USB
- Block executable files from running unless they meet a prevalence, age, or trusted list criteria
- Block Office communication applications from creating child processes
- Block Adobe Reader from creating child processes
- Block persistence through WMI event subscription

Exclude files and folders from attack surface reduction rules

You can exclude files and folders from being evaluated by most attack surface reduction rules. This means that even if an attack surface reduction rule determines the file or folder contains malicious behavior, it will not block the file from running, which also means potentially unsafe files are allowed to run and infect your devices.

You exclude attack surface reduction rules from triggering based on certificate and file hashes by allowing specified Defender for Endpoint file and certificate indicators.

You can specify individual files or folders (using folder paths or fully qualified resource names), but you can't specify which rules the exclusions apply to. An exclusion is applied only when the excluded application or service starts. For example, if you add an exclusion for an update service that is already running, the update service will continue to trigger events until the service is stopped and restarted.

Audit mode for evaluation

Use audit mode to evaluate how attack surface reduction rules would impact your organization if they were enabled. It's best to run all rules in audit mode first so you can understand their impact on your line-of-business applications. Many line-of-business applications are written with limited security concerns, and they may perform tasks in ways that seem similar to malware. By monitoring audit data and adding exclusions for necessary applications, you can deploy attack surface reduction rules without impacting productivity.

Notifications when a rule is triggered

Whenever a rule is triggered, a notification will be displayed on the device. You can customize the notification with your company details and contact information. The notification also displays within the Microsoft Defender Security Center and the Microsoft 365 security center.

Configure attack surface reduction rules

You can set these rules for devices running any of the following editions and versions of Windows:

- Windows 10 Pro, version 1709 or later
- Windows 10 Enterprise, version 1709 or later
- Windows Server, version 1803 (Semi-Annual Channel) or later
- Windows Server 2019

You can enable attack surface reduction rules by using any of these methods:

- Microsoft Intune
- Mobile Device Management (MDM)
- Microsoft Endpoint Configuration Manager
- Group Policy
- PowerShell

Enterprise-level management such as Intune or Microsoft Endpoint Configuration Manager is recommended. Enterprise-level management will overwrite any conflicting Group Policy or PowerShell settings on startup.

Mobile device management

To manage the attack surface reduction rules in mobile device management:

- Use the ./Vendor/MSFT/Policy/Config/Defender/AttackSurfaceReductionRules configuration service provider (CSP) to individually enable and set the mode for each rule.
- Follow the mobile device management reference in **Attack surface reduction rules**³ for using GUID values.
- OMA-URI path: ./Vendor/MSFT/Policy/Config/Defender/AttackSurfaceReductionRules
- Value: 75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84=2|3B576869-A4EC-4529-8536-B80A7769E899=1|D4F940AB-401B-4EFC-AADC-AD5F3C50688A=2|D3E037E1-3EB8-44C8-A917-57927947596D=1|5BEB7EFE-FD9A-4556-801D-275E5FFC04CC=0|BE9BA2D9-53EA-4CDC-84E5-9B1EEEE46550=1
- The values to enable, disable, or enable in audit mode are:
 - Disable = 0
 - Block (enable attack surface reduction rule) = 1
 - Audit = 2
- Use the ./Vendor/MSFT/Policy/Config/Defender/AttackSurfaceReductionOnlyExclusions configuration service provider (CSP) to add exclusions.

Example:

- OMA-URI path: ./Vendor/MSFT/Policy/Config/Defender/AttackSurfaceReductionOnlyExclusions
- Value: c:\path|e:\path|c:\wlisted.exe

Microsoft Endpoint Manager

To manage the attack surface reduction rules in Microsoft Endpoint Manager:

1. In Microsoft Endpoint Manager, go to **Endpoint security** and then under Manage area select **Attack surface reduction**.
2. Select + **Create Policy**.
3. Select a Platform and select **Attack surface reduction rules** from the drop-down menu.

³ <https://docs.microsoft.com/windows/security/threat-protection/microsoft-defender-atp/attack-surface-reduction#attack-surface-reduction-rules?azure-portal=true>

4. Select **Create**.
5. Follow the instructions in the profile creation wizard.

Group policy

To manage the attack surface reduction rules in Group Policy:

Warning: If you manage your computers and devices with Intune, Configuration Manager, or another enterprise-level management platform, the management software will overwrite any conflicting Group Policy settings on startup.

1. On your Group Policy management computer, open the Group Policy Management Console, right-click the Group Policy Object you want to configure, and select **Edit**.
2. In the Group Policy Management Editor, go to Computer configuration and select Administrative templates.
3. Expand the tree to **Windows components > Microsoft Defender Antivirus > Windows Defender Exploit Guard > Attack surface reduction**.
4. Select **Configure Attack surface reduction rules** and select **Enabled**. You can then set the individual state for each rule in the options section.
5. Select **Show...** and enter the rule ID in the Value name column and your chosen state in the Value column as follows:
 - Disable = 0
 - Block (enable attack surface reduction rule) = 1
 - Audit = 2
6. To exclude files and folders from attack surface reduction rules, select the **Exclude files and paths from Attack surface reduction rules** setting and set the option to **Enabled**. Select **Show** and enter each file or folder in the Value name column. Enter **0** in the Value column for each item.

PowerShell

To manage the attack surface reduction rules with PowerShell:

Warning: If you manage your computers and devices with Intune, Configuration Manager, or another enterprise-level management platform, the management software will overwrite any conflicting PowerShell settings on startup. To allow users to define the value using PowerShell, use the "User Defined" option for the rule in the management platform.

1. Type `powershell` in the Start menu, right-click Windows PowerShell, and select Run as administrator.
2. Enter the following cmdlet:
`Set-MpPreference -AttackSurfaceReductionRules_Ids <rule ID> -AttackSurfaceReductionRules_Actions Enabled`
3. To enable attack surface reduction rules in audit mode, use the following cmdlet:
`Add-MpPreference -AttackSurfaceReductionRules_Ids <rule ID> -AttackSurfaceReductionRules_Actions AuditMode`

4. To turn off attack surface reduction rules, use the following cmdlet:

```
Add-MpPreference -AttackSurfaceReductionRules_Ids <rule ID> -AttackSurfaceReductionRules_Actions Disabled
```

5. You must specify the state individually for each rule, but you can combine rules and states in a comma-separated list.
6. In the following example, the first two rules will be enabled, the third rule will be disabled, and the fourth rule will be enabled in audit mode:

```
Set-MpPreference -AttackSurfaceReductionRules_Ids <rule ID 1>,<rule ID 2>,<rule ID 3>,<rule ID 4>  
-AttackSurfaceReductionRules_Actions Enabled, Enabled, Disabled, AuditMode
```

7. You can also use the Add-MpPreference PowerShell verb to add new rules to the existing list.
8. Set-MpPreference will always overwrite the existing set of rules. If you want to add to the existing set, you should use Add-MpPreference instead. You can obtain a list of rules and their current state by using Get-MpPreference.
9. To exclude files and folders from attack surface reduction rules, use the following cmdlet:

```
Add-MpPreference -AttackSurfaceReductionOnlyExclusions "<fully qualified path or resource>"
```

10. Continue to use Add-MpPreference -AttackSurfaceReductionOnlyExclusions to add more files and folders to the list.

Important: Use Add-MpPreference to append or add apps to the list. Using the Set-MpPreference cmdlet will overwrite the existing list.

List of attack surface reduction events

All attack surface reduction events are located under Applications and Services Logs > Microsoft > Windows in the Windows Event viewer.

Manage alerts and incidents

Lesson introduction

Microsoft Defender for Endpoint provides a purpose-driven user interface to manage and investigate security incidents and alerts.

You are a Security Operations Analyst working at a company that has implemented Microsoft Defender for Endpoint, and your job is to remediate incidents. You are assigned an incident with alerts related to a suspicious PowerShell command line.

You start by reviewing the incident and understand all the related alerts, devices, and evidence. You open the alert page to review the Alert Story. This alert looks to be a typical attack vector that Defender for Endpoint identified and has performed an automated investigation. Defender is now waiting for the remediation action approval. You approve the action and close the case.

Learning objectives

After completing this lesson, you should be able to:

- Investigate incidents in Microsoft Defender for Endpoint
- Investigate alerts in Microsoft Defender for Endpoint
- Perform advanced hunting in Microsoft Defender for Endpoint

Explain security operations in Microsoft Defender for Endpoint

Microsoft Defender for Endpoint detection and response capabilities provide advanced attack detections that are near real-time and actionable. Security analysts can prioritize alerts effectively, gain visibility into the full scope of a breach, and take response actions to remediate threats.

When a threat is detected, alerts are created in the system for an analyst to investigate. Alerts with the same attack techniques or attributed to the same attacker are aggregated into an entity called an incident. Aggregating alerts in this manner makes it easy for analysts to investigate and respond to threats collectively.

Inspired by the “assume breach” mindset, Defender for Endpoint continuously collects behavioral cyber telemetry. This includes process information, network activities, deep optics into the kernel and memory manager, user sign in activities, registry and file system changes, and others. The information is stored for six months, enabling an analyst to travel back in time to the start of an attack. The analyst can then pivot in various views and approach an investigation through multiple vectors.

The response capabilities give you the power to promptly remediate threats by acting on the affected entities.

Defender for Endpoint terminology

It is important for you to understand the different components and how they work together.

Device

To start with, each endpoint is considered a Device.

Evidence

Microsoft Defender for Endpoint collects forensics information on artifacts, including accounts, processes, network information, and others.

Alert

Defender for Endpoint uses detection rules based on Microsoft expertise and that are continually updated, looks for suspicious activities. If found, then will generate an Alert.

Incident

Based on the Alerts generated, Defender for Endpoint groups the Alerts into Incidents. An Incident displays a rollup of Alerts, Evidence, and Investigations.

Investigation

Automated Investigation performed by Defender for Endpoint

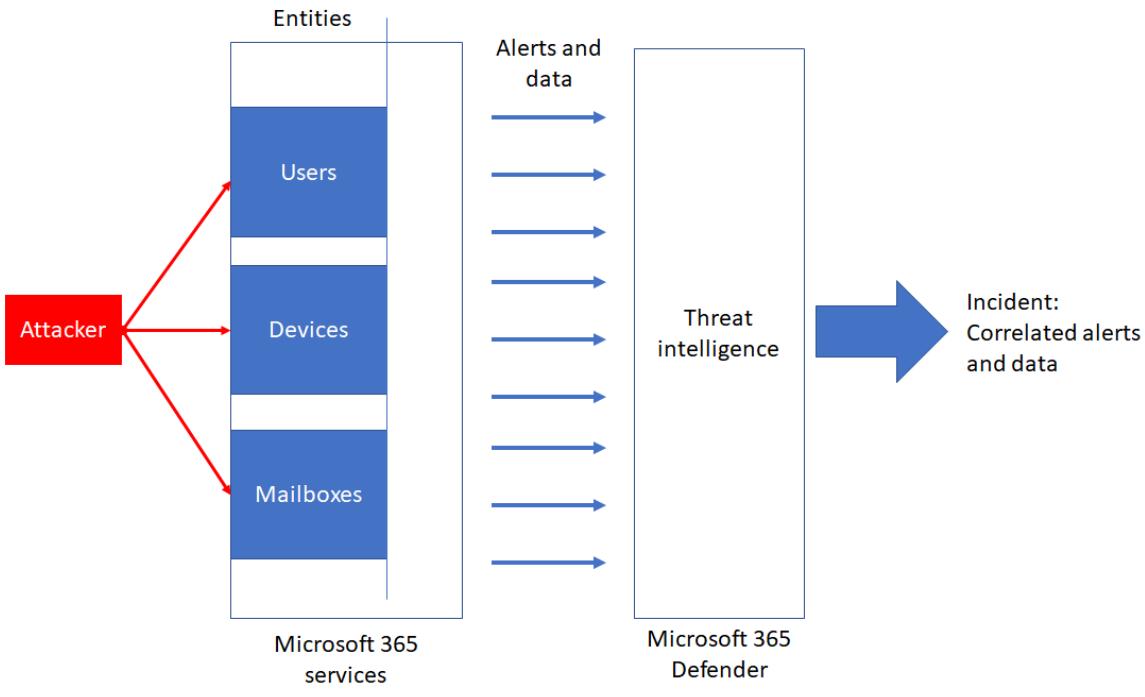
Manage and investigate incidents

You manage incidents for Microsoft Defender for Endpoint in Microsoft 365 Defender portal from **Incidents & alerts > Incidents** on the quick launch of the Microsoft 365 Defender portal (security.microsoft.com). You will learn more about managing incidents in the Microsoft 365 Defender portal in the next module.

An incident in Microsoft 365 Defender is a collection of correlated alerts and associated data that make up the story of an attack.

Microsoft 365 services and apps create alerts when they detect a suspicious or malicious event or activity. Individual alerts provide valuable clues about a completed or ongoing attack. However, attacks typically employ various techniques against different types of entities, such as devices, users, and mailboxes. The result is multiple alerts for multiple entities in your tenant.

Because piecing the individual alerts together to gain insight into an attack can be challenging and time-consuming, Microsoft 365 Defender automatically aggregates the alerts and their associated information into an incident.



Grouping related alerts into an incident gives you a comprehensive view of an attack. For example, you can see:

- Where the attack started.
- What tactics were used.
- How far the attack has gone into your tenant.
- The scope of the attack, such as how many devices, users, and mailboxes were impacted.
- All of the data associated with the attack.

If enabled, Microsoft 365 Defender can automatically investigate and resolve alerts through automation and artificial intelligence. You can also perform additional remediation steps to resolve the attack.

Incident name	Severity	Investigation state
Activity from infrequent country involving one user	Medium	N/A
Logon from a risky IP address involving one user	High	N/A
Activity from infrequent country involving one user	Medium	N/A
M365D (MTP) - 03/03/2021 - Multi-stage incident involving Initial access & Exfiltration on multiple en...	High	5 investigation states
Bad email to endpoint	Medium	N/A

Manage and investigate alerts

Alerts are the basis of all incidents and indicate the occurrence of malicious or suspicious events in your environment. Alerts are typically part of a broader attack and provide clues about an incident.

In Microsoft 365 Defender, related alerts are aggregated together to form incidents. Incidents will always provide the broader context of an attack, however, analyzing alerts can be valuable when deeper analysis is required.

The Alerts queue shows the current set of alerts. You get to the alerts queue from Incidents & alerts > Alerts on the quick launch of the Microsoft 365 Defender portal.

Alert name	Tags	Severity	Investigation state	Status	Category	Detection source	Impacted assets	First activity
Email reported by ...	Informational	Informational	In progress	Others	MDO	Jenny Sivalingam	Apr 14, 2021	
Admin action sub...	Informational	Informational	Remediated	New	Suspicious activity	Automated investigation	msdo@sdf3p1.on...	Apr 14, 2021
Custom detection -...	Medium	Medium	New	Execution	Custom detection	cont-denmarks	Apr 14, 2021	
><img src=x oner...	+5	High	No threats found	New	Exploit	Custom detection	cont-mikebarde...	Apr 14, 2021
><img src=x oner...	+2	High	No threats found	New	Exploit	Custom detection	bbsecadmin	Apr 14, 2021
Unfamiliar sign-in ...	Low	Low	New	Initial access	AAD Identity Protection	Clare Love	Apr 14, 2021	
Admin action sub...	Informational	Informational	Remediated	New	Suspicious activity	Automated investigation	Apr 14, 2021	
Test email custom ...	Medium	Medium	New	Execution	Custom detection	Clare Love	Apr 14, 2021	

Alerts from different Microsoft security solutions like Microsoft Defender for Endpoint, Microsoft Defender for Office 365, and Microsoft 365 Defender appear here.

By default, the alerts queue in the Microsoft 365 Defender portal displays the new and in progress alerts from the last 30 days. The most recent alert is at the top of the list so you can see it first.

You can filter alerts according to these criteria:

- Severity
- Status
- Category
- Detection source
- Tags
- Policy
- Impacted assets

View more alert information on the details page

The details page shows the details of the selected alert, with details and actions related to it. If you select any of the affected assets or entities in the alert story, the details page changes to provide contextual information and actions for the selected object.

Once you've selected an entity of interest, the details page changes to display information about the selected entity type, historic information when it's available, and options to take action on this entity directly from the alert page.

Alerts

Export 30 Days Manage alerts

Filters: Status: New +1

Alert name	Tags	Severity	Investigation state	Status
Email reported by ...	+5	Informational	New	<input checked="" type="radio"/> New
"><img src=x oner...	+5	High	No threats found	<input type="radio"/> New
Test email and mac...	+3	Medium		<input type="radio"/> New
Admin action sub...	+3	Informational	Remediated	<input type="radio"/> New
Custom detection -...	+3	Medium		<input type="radio"/> New
Custom detection -...	+3	Medium		<input type="radio"/> New
Admin action sub...	+3	Informational	Remediated	<input type="radio"/> New
"><img src=x oner...	+2	High	No threats found	<input type="radio"/> New
Unfamiliar sign-in ...	+2	Low		<input type="radio"/> New

Email reported by user as malware or phish

Informational • New

Classify this alert True alert False alert

Alert state

Classification Not Set Assigned to
Set Classification Unassigned
Assign to me

Alert details

Category Open alert page
Consult a threat expert
View submission
Link alert to another incident

MITRE ATT&CK Techniques

Detection technology

Manage alert

Resolve an alert

Once you're done analyzing an alert and it can be resolved, go to the Manage alert pane for the alert and mark the its status as Resolved and classify it as either a False alert or True alert. For true alerts, specify the alert's threat type in the Determination field.

Classifying alerts and specifying their determination helps tune Microsoft 365 Defender to provide more true alerts and less false alerts.

Manage automatic investigations

Your security operations team receives an alert whenever Microsoft Defender detects a malicious or suspicious artifact for Endpoint. Security operations teams face challenges in addressing the multitude of alerts that arise from the seemingly never-ending flow of threats. Microsoft Defender for Endpoint includes automated investigation and remediation (AIR) capabilities that can help your security operations team address threats more efficiently and effectively.

The technology in automated investigation uses various inspection algorithms and is based on processes that are used by security analysts. AIR capabilities are designed to examine alerts and take immediate action to resolve breaches. AIR capabilities significantly reduce alert volume, allowing security operations to focus on more sophisticated threats and other high-value initiatives. The Action center keeps track of all the investigations that were initiated automatically, along with details, such as investigation status, detection source, and any pending or completed actions.

How the automated investigation starts

When an alert is triggered, a security playbook goes into effect. Depending on the security playbook, an automated investigation can start. For example, suppose a malicious file resides on a device. When that file is detected, an alert is triggered, and the automated investigation process begins. Microsoft Defender for Endpoint checks to see if the malicious file is present on any other devices in the organization. Details from the investigation, including verdicts (Malicious, Suspicious, and No threats found) are available during and after the automated investigation.

Details of an automated investigation

During and after an automated investigation, you can view details about the investigation. Select a triggering alert to view the investigation details. From there, you can go to the Investigation graph, Alerts, Devices, Evidence, Entities, and Log tabs.

- **Alerts** - The alert(s) that started the investigation.
- **Devices** - The device(s) where the threat was seen.
- **Evidence** - The entities that were found to be malicious during an investigation.
- **Entities** - Details about each analyzed entity, including a determination for each entity type (Malicious, Suspicious, or No threats found).
- **Log** - The chronological, detailed view of all the investigation actions taken on the alert.
- **Pending actions** - If there are any actions awaiting approval as a result of the investigation, the Pending actions tab is displayed. On the Pending actions tab, you can approve or reject each action.

How an automated investigation expands its scope

While an investigation is running, any other alerts generated from the device are added to an ongoing automated investigation until that investigation is completed. In addition, if the same threat is seen on other devices, those devices are added to the investigation.

If an incriminated entity is seen in another device, the automated investigation process expands its scope to include that device, and a general security playbook starts on that device. If ten or more devices are found during this expansion process from the same entity, then that expansion action requires approval and is visible on the Pending actions tab.

How threats are remediated

As alerts are triggered and an automated investigation runs, a verdict is generated for each piece of evidence investigated. Verdicts can be Malicious, Suspicious, or No threats found.

As verdicts are reached, automated investigations can result in one or more remediation actions. Examples of remediation actions include sending a file to quarantine, stopping a service, removing a scheduled task, and more. (See Remediation actions.)

Depending on the level of automation set for your organization, as well as other security settings, remediation actions can occur automatically or only upon approval by your security operations team. Additional security settings that can affect automatic remediation include protection from potentially unwanted applications (PUA).

All remediation actions, whether pending or completed, can be viewed in the Action Center <https://security.microsoft.com/action-center/pending>⁴. If necessary, your security operations team can undo a remediation action.

Automation levels in automated investigation and remediation capabilities

Automated investigation and remediation (AIR) capabilities in Microsoft Defender for Endpoint can be configured to one of several levels of automation. Your automation level affects whether remediation actions following AIR investigations are taken automatically or only upon approval.

- Full automation (recommended) means remediation actions are taken automatically on artifacts determined to be malicious.
- Semi-automation means some remediation actions are taken automatically, but other remediation actions await approval before being taken.
- All remediation actions, whether pending or completed, are tracked in the Action Center

Levels of automation

Full - remediate threats automatically (also referred to as full automation)

With full automation, remediation actions are performed automatically. All remediation actions that are taken can be viewed in the Action Center on the History tab. If necessary, a remediation action can be undone.

Semi - require approval for any remediation (also referred to as semi-automation)

With this level of semi-automation, approval is required for any remediation action. Such pending actions can be viewed and approved in the Action Center, on the Pending tab.

Semi - require approval for core folders remediation (also a type of semi-automation)

With this level of semi-automation, approval is required for any remediation actions needed on files or executables that are in core folders. Core folders include operating system directories, such as the Windows (\windows*).

Remediation actions can be taken automatically on files or executables that are in other (non-core) folders.

⁴ <https://security.microsoft.com/action-center/pending?azure-portal=true>

Pending actions for files or executables in core folders can be viewed and approved in the Action Center, on the Pending tab.

Actions that were taken on files or executables in other folders can be viewed in the Action Center, on the History tab.

Semi - require approval for non-temp folders remediation (also a type of semi-automation)

With this level of semi-automation, approval is required for any remediation actions needed on files or executables that are not in temporary folders.

Temporary folders can include the following examples:

- \users*\appdata\local\temp*
- \documents and settings*\local settings\temp*
- \documents and settings*\local settings\temporary*
- \windows\temp*
- \users*\downloads*
- \program files\
- \program files (x86)*
- \documents and settings*\users*

Remediation actions can be taken automatically on files or executables that are in temporary folders.

Pending actions for files or executables that are not in temporary folders can be viewed and approved in the Action Center, on the Pending tab.

Actions that were taken on files or executables in temporary folders can be viewed and approved in the Action Center on the History tab.

No automated response (also referred to as no automation)

With no automation, the automated investigation does not run on your organization's devices. As a result, no remediation actions are taken or pending as a result of an automated investigation. However, other threat protection features, such as protection from potentially unwanted applications, can be in effect, depending on how your antivirus and next-generation protection features are configured.

Using the no automation option is not recommended because it reduces the security posture of your organization's devices. Consider setting up your automation level to full automation (or at least semi-automation).

Important points about automation levels

Full automation has proven to be reliable, efficient, and safe, and is recommended for all customers. Full automation frees up your critical security resources so they can focus more on your strategic initiatives. If your security team has defined device groups with a level of automation, those settings are not changed by the new default settings that are rolling out.

Investigation graph

The investigation graph provides a graphical representation of an automated investigation. All investigation-related information is simplified and arranged in specific sections. Clicking on any of the icons brings you the relevant section where you can view more information.

A progress ring shows two status indicators:

- Orange ring - shows the pending portion of the investigation
- Green ring - shows the running time portion of the investigation
- Image of start, end, and pending time for an automated investigation

Alerts

The Alerts tab for an automated investigation shows details such as a short description of the alert that initiated the automated investigation, severity, category, the device associated with the alert, user, time in queue, status, investigation state, and to whom the investigation is assigned.

Additional alerts seen on a device can be added to an automated investigation as long as the investigation is ongoing.

Selecting an alert using the check box brings up the alerts details pane where you can open the alert page, manage the alert by changing its status, see alert details, automated investigation details, related device, logged-on users, and comments and history.

Clicking on an alert title brings you to the alert page.

Devices

The Devices tab Shows details of the device name, IP address, group, users, operating system, remediation level, investigation count, and when it was last investigated. Devices that show the same threat can be added to an ongoing investigation and will be displayed in this tab. If ten or more devices are found during this expansion process from the same entity, then that expansion action will require approval and will be seen in the Pending actions view.

Selecting a device using the checkbox brings up the device details pane where you can see more information such as device details and logged-on users. Clicking on a device name brings you to the device page.

Evidence

The Evidence tab shows details related to threats associated with this investigation.

Entities

The Entities tab shows details about entities such as files, processes, services, drives, IP addresses, and the table details, such as the number of entities that were analyzed. You'll gain insight into details such as how many are remediated, suspicious, or had no threats found.

Log

The Log tab gives a detailed, chronological view of all the investigation actions taken on the alert. You'll see the action type, action, status, device name, description of the action, comments entered by analysts who may have worked on the investigation, execution start time, duration, pending duration.

As with other sections, you can customize columns, select the number of items to show per page, and filter the log. Available filters include action type, action, status, device name, and description. You can also click on an action to bring up the details pane where you'll see information such as the summary of the action and input data.

Pending actions

When you select the pending actions link, you'll be taken to the Action center. You can also access the page from the navigation page by going to automated investigation > Action center.

Use the Action Center

The unified Action center of the Microsoft 365 Defender portal lists pending and completed remediation actions for your devices, email & collaboration content, and identities in one location.

The unified Action center brings together remediation actions across Defender for Endpoint and Defender for Office 365. It defines a common language for all remediation actions and provides a unified investigation experience. Your security operations team has a "single pane of glass" experience to view and manage remediation actions.

The Action Center consists of pending and historical items:

- **Pending** displays a list of ongoing investigations that require attention. Recommended actions are presented that your security operations team can approve or reject. The Pending tab appears only if there are pending actions to be approved (or rejected).
- **History** as an audit log for all of the following items:
 - Remediation actions that were taken as a result of an automated investigation
 - Remediation actions that were approved by your security operations team (some actions, such as sending a file to quarantine, can be undone)
 - Commands that were run and remediation actions that were applied in Live Response sessions (some actions can be undone)
 - Remediation actions that were applied by Microsoft Defender Antivirus (some actions can be undone)

Select Automated Investigations, then Action center.

Action update time	Investigation ID	Action type	Details
1/26/21, 4:11 AM	57491	Stop process	2dd2c2011C
1/26/21, 4:11 AM	57491	Quarantine file	c:\windows\

When an automated investigation runs, a verdict is generated for each piece of evidence investigated. Verdicts can be Malicious, Suspicious, or No threats found depending on:

- Type of threat
- Resulting verdict
- How your organization's device groups are configured

Remediation actions can occur automatically or only upon approval by your organization's security operations team.

Review pending actions

To approve or reject a pending action:

- Select any item on the Pending tab.
- Select an investigation from any of the categories to open a panel where you can approve or reject remediation actions.

Other details, such as file or service details, investigation details, and alert details are displayed. From the panel, you can select the Open investigation page link to see the investigation details. You can also select multiple investigations to approve or reject actions on multiple investigations.

Review completed actions

To review completed actions:

- Select the History tab. (If need be, expand the time period to display more data.)
- Select an item to view more details about that remediation action.

Undo completed actions

If you've determined that a device or a file is not a threat, you can undo remediation actions that were taken, whether those actions were taken automatically or manually. You can undo any of the following actions:

- Source
 - Automated investigation
 - Microsoft Defender Antivirus
 - Manual response actions
- Supported Actions
 - Isolate device
 - Restrict code execution
 - Quarantine a file
 - Remove a registry key
 - Stop a service
 - Disable a driver
 - Remove a scheduled task

Remove a file from quarantine across multiple devices

To remove a file from quarantine across multiple devices:

- On the History tab, select a file that has the Action type Quarantine file.

- In the pane on the right side of the screen, select Apply to X more instances of this file, and then select Undo.

Perform advanced hunting

Advanced hunting is a query-based threat-hunting tool that lets you explore up to 30 days of raw data. You can proactively inspect events in your network to locate threat indicators and entities. The flexible access to data enables unconstrained hunting for both known and potential threats.

Data freshness and update frequency

Advanced hunting data can be categorized into two distinct types, each consolidated differently.

Event or activity data—populates tables about alerts, security events, system events, and routine assessments. Advanced hunting receives this data almost immediately after the sensors that collect them successfully transmit them to Defender for Endpoint.

Entity data—populates tables with consolidated information about users and devices. This data comes from both relatively static data sources and dynamic sources, such as Active Directory entries and event logs. To provide fresh data, tables are updated with any new information every 15 minutes, adding rows that might not be fully populated. Every 24 hours, data is consolidated to insert a record that contains the latest, most comprehensive data set about each entity.

Data Schema

The following reference lists all the tables in the advanced hunting schema.

- **DeviceAlertEvents** - Alerts on Microsoft Defender Security Center
- **DeviceInfo** - Device information, including OS information
- **DeviceNetworkInfo** - Network properties of devices, including adapters, IP and MAC addresses, as well as connected networks and domains
- **DeviceProcessEvents** - Process creation and related events
- **DeviceNetworkEvents** - Network connection and related events
- **DeviceFileEvents** - File creation, modification, and other file system events
- **DeviceRegistryEvents** - Creation and modification of registry entries
- **DeviceLogonEvents** - Sign-ins and other authentication events
- **DeviceImageLoadEvents** - DLL loading events
- **DeviceEvents** - Multiple event types, including events triggered by security controls such as Microsoft Defender Antivirus and exploit protection
- **DeviceFileCertificateInfo** - Certificate information of signed files obtained from certificate verification events on endpoints
- **DeviceTvmSoftwareInventoryVulnerabilities** - Inventory of software on devices and any known vulnerabilities in these software products
- **DeviceTvmSoftwareVulnerabilitiesKB** - Knowledge base of publicly disclosed vulnerabilities, including whether exploit code is publicly available
- **DeviceTvmSecureConfigurationAssessment** - Threat & Vulnerability Management assessment events, indicating the status of various security configurations on devices

- **DeviceTvmSecureConfigurationAssessmentKB** - Knowledge base of various security configurations used by Threat & Vulnerability Management to assess devices; includes mappings to various standards and benchmarks

Custom detections

With custom detections, you can proactively monitor for and respond to various events and system states, including suspected breach activity and misconfigured devices. You can do this with customizable detection rules that automatically trigger alerts and response actions.

Custom detections work with advanced hunting, which provides a powerful, flexible query language that covers a broad set of event and system information from your network. You can set them to run at regular intervals, generate alerts, and take response actions whenever there are matches.

Custom detections provide:

- Alerts for rule-based detections built from advanced hunting queries
- Automatic response actions that apply to files and devices

Create detection rules

To create detection rules:

1. Prepare the query.

In Microsoft Defender Security Center, go to Advanced hunting and select an existing query or create a new query. When using a new query, run the query to identify errors and understand possible results.

Important: To prevent the service from returning too many alerts, each rule is limited to generating only 100 alerts whenever it runs. Before creating a rule, tweak your query to avoid alerting for normal, day-to-day activity.

To use a query for a custom detection rule, the query must return the following columns:

- Timestamp
- Deviceld
- ReportId

Simple queries, such as those that don't use the project or summarize operator to customize or aggregate results, typically return these common columns.

There are various ways to ensure more complex queries return these columns. For example, if you prefer to aggregate and count by Deviceld, you can still return Timestamp and ReportId by getting them from the most recent event involving each device.

The sample query below counts the number of unique devices (Deviceld) with antivirus detections and uses this to find only those devices with more than five detections. To return the latest Timestamp and the corresponding ReportId, it uses the summarize operator with the arg_max function.

```
DeviceEvents
| where Timestamp > ago(7d)
| where ActionType == "AntivirusDetection"
| summarize (Timestamp, ReportId)=arg_max(Timestamp, ReportId), count() by
DeviceId
| where count_ > 5
```

2. Create a new rule and provide alert details.

With the query in the query editor, select Create detection rule and specify the following alert details:

- Detection name—name of the detection rule
- Frequency—interval for running the query and taking action. See additional guidance below
- Alert title—title displayed with alerts triggered by the rule
- Severity—potential risk of the component or activity identified by the rule.
- Category—type of threat component or activity, if any.
- MITRE ATT&CK techniques—one or more attack techniques identified by the rule as documented in the MITRE ATT&CK framework. This section is not available with certain alert categories, such as malware, ransomware, suspicious activity, and unwanted software
- Description—more information about the component or activity identified by the rule
- Recommended actions—additional actions that responders might take in response to an alert

Rule frequency

When saved, a new custom detection rule immediately runs and checks for matches from the past 30 days of data. The rule then runs again at fixed intervals and lookback durations based on the frequency you choose:

- Every 24 hours—runs every 24 hours, checking data from the past 30 days
- Every 12 hours—runs every 12 hours, checking data from the past 24 hours
- Every 3 hours—runs every 3 hours, checking data from the past 6 hours
- Every hour—runs hourly, checking data from the past 2 hours

Select the frequency that matches how closely you want to monitor detections, and consider your organization's capacity to respond to the alerts.

3. Choose the impacted entities.

Identify the columns in your query results where you expect to find the main affected or impacted entity. For example, a query might return both device and user IDs. Identifying which of these columns represents the main impacted entity helps the service aggregate relevant alerts, correlate incidents, and target response actions.

You can select only one column for each entity type. Columns that are not returned by your query cannot be selected.

4. Specify actions.

Your custom detection rule can automatically take actions on files or devices that are returned by the query.

Actions on devices

These actions are applied to devices in the DeviceId column of the query results:

- Isolate device—applies full network isolation, preventing the device from connecting to any application or service, except for the Defender for Endpoint service.
- Collect investigation package—collects device information in a ZIP file.

- Run antivirus scan—performs a full Microsoft Defender Antivirus scan on the device
- Initiate investigation—starts an automated investigation on the device

Actions on files

These actions are applied to files in the SHA1 or the InitiatingProcessSHA1 column of the query results:

- Allow/Block—automatically adds the file to your custom indicator list so that it is always allowed to run or blocked from running. You can set the scope of this action so that it is taken only on selected device groups. This scope is independent of the scope of the rule.
- Quarantine file—deletes the file from its current location and places a copy in quarantine

5. Set the rule scope.

Set the scope to specify which devices are covered by the rule:

- All devices
- Specific device groups

Only data from devices in scope will be queried. Also, actions will be taken only on those devices.

6. Review and turn on the rule.

After reviewing the rule, select Create to save it. The custom detection rule immediately runs. It runs again based on configured frequency to check for matches, generate alerts, and take response actions.

Consult Microsoft Threat Experts

Microsoft Threat Experts - Targeted Attack Notifications is a managed threat hunting service. Once you apply and are accepted, you'll receive targeted attack notifications from Microsoft threat experts, so you won't miss critical threats to your environment. These notifications will help you protect your organization's endpoints, email, and identities. Microsoft Threat Experts – Experts on Demand lets you get expert advice about threats your organization is facing. You can reach out for help on threats your organization is facing. It's available as a subscription service.

Targeted attack notification

Microsoft Threat Experts provides proactive hunting for the most important threats to your network, including human adversary intrusions, hands-on-keyboard attacks, or advanced attacks like cyberespionage. The managed hunting service includes:

- Threat monitoring and analysis, reducing dwell time and risk to the business
- Hunter-trained artificial intelligence to discover and prioritize both known and unknown attacks
- Identifying the most important risks, helping SOCs maximize time and energy
- Scope of compromise and as much context as can be quickly delivered to enable fast SOC response.

Collaborate with experts, on demand

Customers can engage our security experts directly from within Microsoft Defender Security Center for timely and accurate response. Experts provide insights needed to better understand the complex threats affecting your organization, from alert inquiries, potentially compromised devices, root cause of a

suspicious network connection, to more threat intelligence regarding ongoing advanced persistent threat campaigns. With this capability, you can:

- Get more clarification on alerts including root cause or scope of the incident
- Gain clarity into suspicious device behavior and next steps if faced with an advanced attacker
- Determine risk and protection regarding threat actors, campaigns, or emerging attacker techniques
- Seamlessly transition to Microsoft Incident Response (IR) or other third-party Incident Response services when necessary

If you already have Microsoft Defender for Endpoint and Microsoft 365 Defender, you can apply for Microsoft Threat Experts – Targeted Attack Notifications through their Microsoft 365 Defender portal. Go to **Settings > Endpoints > General > Advanced features > Microsoft Threat Experts – Targeted Attack Notifications**, and select **Apply**.

The option to Consult a threat expert is available in several places in the portal so you can engage with experts in the context of your investigation:

- Help and support menu
- Device page actions menu
- Alerts page actions menu
- File page actions menu

The screenshot shows the Microsoft Defender for Endpoint portal. On the left, there's a sidebar with sections like 'Device summary', 'Tags' (No tags found), 'Security Info', 'Open incidents' (1), and 'Active alerts'. The main area displays 'Overview' with a 'Risk level: High' summary. It shows '1 active alert in 1 incident' with a red bar chart indicating 'High (1)'. To the right, there are sections for 'Alerts' (No data to show), 'Timeline', 'Security assessments' (No data to show), and 'Logged' (2 logs). A context menu is open on the right side, listing options like 'Manage tags', 'Isolate device', 'Restrict app execution', 'Run antivirus scan', 'Collect investigation package', 'Initiate Live Response Session', 'Initiate Automated Investigation', and 'Consult a threat expert'. The 'Consult a threat expert' option is highlighted with a red box.

Perform device investigations

Lesson introduction

Microsoft Defender for Endpoint provides detailed device information, including forensics information.

You are a Security Operations Analyst working at a company that has implemented Microsoft Defender for Endpoint, and your primary job is to remediate incidents. You are assigned an incident with alerts related to a suspicious PowerShell command line. You start by reviewing the incident and understand all the related alerts, devices, and evidence. You open the alert page to review the Alert Story and decide to perform further analysis on the device.

You open the Device page to provide more context to the incident. The overview tab on the Device page immediately provides concerning information such as the Risk level and Exposure level. You select the Alerts tab to see a history of alerts for the device. Next, you choose the Timeline tab to see a list of events from the device. You see many suspicious events.

Learning objectives

After completing this lesson, you should be able to:

- Use the device page in Microsoft Defender for Endpoint
- Describe device forensics information collected by Microsoft Defender for Endpoint
- Describe behavioral blocking by Microsoft Defender for Endpoint

Use the device inventory list

The Device inventory page shows a list of the devices in your network where alerts were generated. By default, the queue displays devices with alerts seen in the last 30 days. Select a device to open the Device page. The Device page is also accessed from various investigation pages like Incidents and Alerts.

Devices list							
		30 days		Customize columns			
Device name	Domain	Risk level	Exposure level	OS platform	Windows 10 vers...	Health state	Last seen
[REDACTED]	[REDACTED]	■■■ High	⚠ Medium	Windows 10	Future	Active	6/15/20, 12:01 PM
[REDACTED]	[REDACTED]	■■■ High	⚠ Low	Windows 10	Future	Active	6/15/20, 4:52 AM
[REDACTED]	[REDACTED]	■■■ High	⚠ High	Windows 10	1903	Active	6/14/20, 10:51 PM
[REDACTED]	[REDACTED]	■■■ High	No data available	Windows 10	Future	Inactive	6/8/20, 4:38 AM
[REDACTED]	[REDACTED]	■■■ High	No data available	Windows 10	Future	Inactive	6/8/20, 4:47 AM
[REDACTED]	[REDACTED]	■■■ High	No data available	Windows 10	Future	Inactive	6/8/20, 4:50 AM

At a glance, you'll see information such as domain, risk level, OS platform, and other details for easy identification of devices most at risk.

During the onboarding process, the Devices list is gradually populated with devices as they begin to report sensor data. Use this view to track your onboarded endpoints as they come online, or download the complete endpoint list as a CSV file for offline analysis.

Risk level

The risk level reflects the overall risk assessment of the device based on a combination of factors, including the types and severity of active alerts on the device. Resolving active alerts, approving remediation activities, and suppressing subsequent alerts can lower the risk level.

Exposure level

The exposure level reflects the current exposure of the device based on the cumulative impact of its pending security recommendations. The possible levels are low, medium, and high. Low exposure means your devices are less vulnerable to exploitation.

If the exposure level says, "No data available," there are a few reasons why this may be the case:

- The device stopped reporting for more than 30 days – in that case, it is considered inactive, and the exposure isn't computed
- The device OS is not supported - see minimum requirements for Microsoft Defender for Endpoint
- The device has a stale agent (very unlikely)

Health state

The following device health states:

- Active – Devices that are actively reporting sensor data to the service.
- Inactive – Devices that have stopped sending signals for more than seven days.
- Misconfigured – Devices that have impaired communications with service or are unable to send sensor data. Misconfigured devices can further be classified to:
 - No sensor data
 - Impaired communications

Antivirus status

The antivirus status for Windows 10 devices only:

- Disabled - Virus & threat protection is turned off.
- Not reporting - Virus & threat protection is not reporting.
- Not updated - Virus & threat protection is not up to date.

Investigate the device

Investigate the details of an alert raised on a specific device to identify other behaviors or events that might be related to the alert or the potential scope of the breach.

You can select affected devices whenever you see them in the portal to open a detailed report about that device. Affected devices are identified in the following areas:

- Devices list
- Alerts queue
- Security operations dashboard

- Any individual alert
- Any individual file details view
- Any IP address or domain details view

When you investigate a specific device, you'll see:

- Device details
- Response actions
- Tabs (overview, alerts, timeline, security recommendations, software inventory, discovered vulnerabilities, missing KBS)
- Cards (active alerts, logged on users, security assessment)

Device details

The device details section provides information such as the device's domain, OS, and health state. If there's an investigation package available on the device, you'll see a link that allows you to download the package.

Response actions

Response actions run along the top of a specific device page and include:

- Manage tags
- Isolate device
- Restrict app execution
- Run antivirus scan
- Collect investigation package
- Initiate Live Response Session
- Initiate automated investigation
- Consult a threat expert
- Action center

You can take response actions in the Action center, on a specific device page, or on a specific file page.

Tabs

Overview

The Overview tab displays the cards for active alerts, logged on users, and security assessment.

Active alerts

The Azure Defender card will display a high-level overview of active alerts related to the device and their risk level if you have enabled the Azure ATP feature. More information is available in the "Alerts" drill-down.

Logged on users

The Logged on users card shows how many users have logged on in the past 30 days, and the most and least frequent users. Selecting the "See all users" link opens the details pane, which displays user type, sign-in type, and when the user was first and last seen.

Security assessments

The Security assessments card shows the overall exposure level, security recommendations, installed software, and discovered vulnerabilities. A device's exposure level is determined by the cumulative impact of its pending security recommendations.

Alerts

The Alerts tab provides a list of alerts that are associated with the device. This list is a filtered version of the Alerts queue, and shows a short description of the alert, severity (high, medium, low, informational), status in the queue (new, in progress, resolved), classification (not set, false alert, true alert), investigation state, category of alert, who is addressing the alert, and last activity. You can also filter the alerts.

Timeline

The Timeline tab provides a chronological view of the events and associated alerts that have been observed on the device. This can help you correlate any events, files, and IP addresses related to the device.

The timeline also enables you to selectively drill down into events that occurred within a given time period. You can view the temporal sequence of events that occurred on a device over a selected time period. To further control your view, you can filter by event groups or customize the columns.

Some of the functionality includes:

- Search for specific events:
 - Use the search bar to look for specific timeline events.
- Filter events from a specific date:
 - Select the calendar icon in the upper left of the table to display events in the past day, week, 30 days, or a custom range. By default, the device timeline is set to display the events from the past 30 days.
 - Use the timeline to jump to a specific moment in time by highlighting the section. The arrows on the timeline pinpoint automated investigations
- Export detailed device timeline events:
 - Export the device timeline for the current date or a specified date range up to seven days.

More details about certain events are provided and vary depending on the type of event, for example:

- Contained by Application Guard - the web browser event was restricted by an isolated container
- Active threat detected - the threat detection occurred while the threat was running
- Remediation unsuccessful - an attempt to remediate the detected threat was invoked but failed
- Remediation successful - the detected threat was stopped and cleaned
- Warning bypassed by user - the Windows Defender SmartScreen warning was dismissed and overridden by a user
- Suspicious script detected - a potentially malicious script was found running

- The alert category - if the event led to the generation of an alert, the alert category ("Lateral Movement", for example) is provided

Flag an event

While navigating the device timeline, you can search and filter for specific events. You can set event flags by:

- Highlighting the most important events
- Marking events that require a deep dive
- Building a clean breach timeline

Find the event that you want to flag. Select the flag icon in the Flag column.

View flagged events

In the timeline Filters section, enable Flagged events. Select Apply. Only flagged events are displayed. You can apply more filters by clicking the time bar. This will only show events prior to the flagged event.

Event details

Select an event to view relevant details about that event. A panel displays to show general event information. When applicable and data is available, a graph showing related entities and their relationships are also shown.

To further inspect the event and related events, you can quickly run an advanced hunting query by selecting Hunt for related events. The query will return the selected event and the list of other events that occurred around the same time on the same endpoint.

Security recommendations

Security recommendations are generated from Microsoft Defender for Endpoint's Threat & Vulnerability Management capability. Selecting a recommendation will show a panel where you can view relevant details such as the description of the recommendation and the potential risks associated with not enacting it.

Software inventory

The Software inventory tab lets you view software on the device, along with any weaknesses or threats. Selecting the name of the software will take you to the software details page, where you can view security recommendations, discovered vulnerabilities, installed devices, and version distribution.

Discovered vulnerabilities

The Discovered vulnerabilities tab shows the name, severity, and threat insights of discovered vulnerabilities on the device. Selecting specific vulnerabilities will show a description and details.

Missing knowledge bases

The Missing KBs tab lists the missing security updates for the device.

Use behavioral blocking

Today's threat landscape is overrun by fileless malware that lives off the land, highly polymorphic threats that mutate faster than traditional solutions can keep up with, and human-operated attacks that adapt to what adversaries find on compromised devices. Traditional security solutions are not sufficient to stop such attacks. You need artificial intelligence (AI) and machine learning (ML) backed capabilities, such as behavioral blocking and containment, included in Defender for Endpoint.

Behavioral blocking and containment capabilities can help identify and stop threats based on their behaviors and process trees even when the threat has already started. Next-generation protection, EDR, and Defender for Endpoint components and features work together in behavioral blocking and containment capabilities.

Behavioral blocking and containment capabilities work with multiple components and features of Defender for Endpoint to stop attacks immediately and prevent attacks from progressing.

- Next-generation protection (which includes Microsoft Defender Antivirus) can detect threats by analyzing behaviors and stop threats that have started running.
- Endpoint detection and response (EDR) receives security signals across your network, devices, and kernel behavior. As threats are detected, alerts are created. Multiple alerts of the same type are aggregated into incidents, which makes it easier for your security operations team to investigate and respond.
- Defender for Endpoint has a wide range of optics across identities, email, data, and apps, as well as the network, endpoint, and kernel behavior signals received through EDR. A component of Microsoft 365 Defender, Defender for Endpoint processes and correlates these signals, raises detection alerts, and connects related alerts in incidents.

With these capabilities, more threats can be prevented or blocked, even if they start running. Whenever suspicious behavior is detected, the threat is contained, alerts are created, and threats are stopped in their tracks.

The following image shows an example of an alert that was triggered by behavioral blocking and containment capabilities:

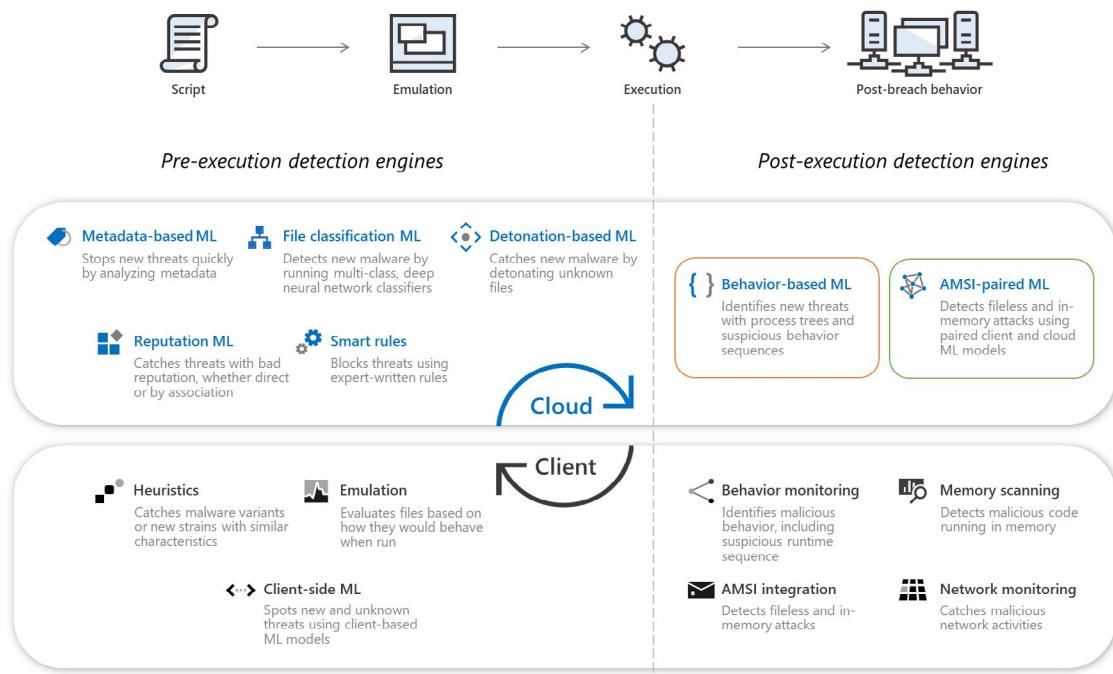
Alerts > **Initial Access behavior was detected**

Initial Access behavior was detected This alert is part of incident (1630)	Alert context nt authority\system	Status State: Resolved Classification: Not set
Severity: Low Category: Initial Access Detection source: EDR	First activity: 07.12.2019 21:31:19 Last activity: 07.12.2019 22:35:05	Assigned to:
Description Malware and unwanted software are undesirable applications that perform annoying, disruptive, or harmful actions on affected devices. Some of these undesirable applications can replicate and spread from one machine to another. Others are able to receive commands from remote attackers and perform activities associated with cyber attacks.		
Recommended actions <ol style="list-style-type: none"> Validate the alert and scope the suspected breach. Find related devices, network addresses, and files in the incident graph. Check for other suspicious activities in the device timeline. Locate unfamiliar processes in the process tree. Check files for prevalence, their locations, and digital signatures. Show more		
Alert process tree <pre> graph TD Owininit[Owininit.exe] --> Oservices[Oservices.exe] Oservices --> Osvhost[Osvhost.exe] Osvhost --> Oeqnedt32[Oeqnedt32.exe] Oeqnedt32 --> Olinks1[Olinks.exe] Olinks1 --> Olinks2[Olinks.exe] Olinks2 --> O17A21B[O17A21B.exe] O17A21B --> Raja[raja.com] O17A21B --> Ruta[ruta.com] </pre> <p>Detailed description of the process tree: The process tree starts with Owininit.exe, which spawns Oservices.exe. Oservices.exe spawns Osvhost.exe, which then spawns Oeqnedt32.exe. Oeqnedt32.exe spawns Olinks.exe, which is detected as Behavior:Win32/InitialAccess.STIm by Windows Defender AV. This Olinks.exe then spawns O17A21B.exe, which is also detected as Behavior:Win32/InitialAccess.STIm by Windows Defender AV. O17A21B.exe creates file 17A21B.exe and establishes connections to raja.com (port 80) and ruta.com (port 443), both of which are detected as Behavior:Win32/InitialAccess.STIm by Antivirus. </p>		

This alert is also related to 4 detection events and 2 other events not displayed here.
 Last event time is 07.12.2019 | 22:35:05.
 Click [here](#) to see all related events in the device timeline.

Client behavioral blocking

Client behavioral blocking is a component of behavioral blocking and containment capabilities in Defender for Endpoint. As suspicious behaviors are detected on devices (also referred to as clients or endpoints), artifacts (such as files or applications) are blocked, checked, and remediated automatically.



How client behavioral blocking works

Microsoft Defender Antivirus can detect suspicious behavior, malicious code, fileless and in-memory attacks, and more on a device. When suspicious behaviors are detected, Microsoft Defender Antivirus monitors and sends those suspicious behaviors and their process trees to the cloud protection service. Machine learning differentiates between malicious applications and good behaviors within milliseconds and classifies each artifact. As soon as an artifact is found to be malicious, it's blocked on the device.

Whenever a suspicious behavior is detected, an alert is generated and is visible in the Microsoft Defender Security Center

Client behavioral blocking is effective because it not only helps prevent an attack from starting, but it can help stop an attack that has begun executing. With feedback-loop blocking (another capability of behavioral blocking and containment), attacks are prevented on other devices in your organization.

Behavior-based detections

Behavior-based detections are named according to the MITRE ATT&CK Matrix for Enterprise. The naming convention helps identify the attack stage where malicious behavior was observed:

Tactic	Detection threat name
Initial Access	Behavior:Win32/InitialAccess.*!ml
Execution	Behavior:Win32/Execution.*!ml
Persistence	Behavior:Win32/Persistence.*!ml
Privilege Escalation	Behavior:Win32/PrivilegeEscalation.*!ml
Defense Evasion	Behavior:Win32/DefenseEvasion.*!ml
Credential Access	Behavior:Win32/CredentialAccess.*!ml
Discovery	Behavior:Win32/Discovery.*!ml

Tactic	Detection threat name
Lateral Movement	Behavior:Win32/LateralMovement.*!ml
Collection	Behavior:Win32/Collection.*!ml
Command and Control	Behavior:Win32/CommandAndControl.*!ml
Exfiltration	Behavior:Win32/Exfiltration.*!ml
Impact	Behavior:Win32/Impact.*!ml
Uncategorized	Win32/Generic.*!ml

Feedback-loop blocking

Feedback-loop blocking, also referred to as rapid protection, is a component of behavioral blocking and containment capabilities in Microsoft Defender for Endpoint. With feedback-loop blocking, devices across your organization are better protected from attacks.

How feedback-loop blocking works

When a suspicious behavior or file is detected, such as by Microsoft Defender Antivirus, information about that artifact is sent to multiple classifiers. The rapid protection loop engine inspects and correlates the information with other signals to arrive at a decision as to whether to block a file. Checking and classifying artifacts happens quickly. It results in rapid blocking of confirmed malware and drives protection across the entire ecosystem.

With rapid protection in place, an attack can be stopped on a device, other devices in the organization, and devices in other organizations, as an attack attempts to broaden its foothold.

Endpoint detection and response in block mode

When endpoint detection and response (EDR) in block mode is turned on, Defender for Endpoint blocks malicious artifacts or behaviors that are observed through post-breach protection. EDR in block mode works behind the scenes to remediate malicious artifacts that are detected post-breach.

EDR in block mode is also integrated with threat & vulnerability management. Your organization's security team will get a security recommendation to turn EDR in block mode on if it isn't already enabled.

What happens when something is detected?

When EDR in block mode is turned on and a malicious artifact is detected, blocking and remediation actions are taken. You'll see detection status as Blocked or Prevented as completed actions in the Action Center.

The following image shows an instance of unwanted software that was detected and blocked through EDR in block mode:

An active 'CVE-2012-0217' exploit malware was blocked

The screenshot shows a security alert story for an active exploit malware. The alert story details a file creation event:

- File create:** [23820] MalwareTest0.exe
- SHA1:** bd4dbe981192cf5945814de11c53f2b08085b921s3
- Path:** C:\Users\[REDACTED]\AppData\Local\Temp\[REDACTED]

The alert story also lists other processes and their details:

- [1028] userinit.exe**
 - Process id:** 1028
 - Creation time:** Aug 4, 2020, 9:48:29 PM
 - Image file path:** C:\Windows\explorer.exe
 - Image file SHA1:** 18a62cd1d5544a7dc881b118476c730ea83c6ec8
 - Image file created:** Jul 31, 2020, 12:18:43 AM
 - Elevation:** Limited
 - Integrity level:** Medium
 - User:** [REDACTED]
 - PE metadata:** explorer.exe
- [1808] explorer.exe**
 - Process id:** 1808
 - Creation time:** Aug 4, 2020, 9:48:29 PM
 - Image file path:** C:\Windows\explorer.exe
 - Image file SHA1:** 18a62cd1d5544a7dc881b118476c730ea83c6ec8
 - Image file created:** Jul 31, 2020, 12:18:43 AM
 - Elevation:** Limited
 - Integrity level:** Medium
 - User:** [REDACTED]
 - PE metadata:** explorer.exe

Details

An active 'CVE-2012-0217' exploit malware was blocked

Risk level: Medium **New**

See in timeline [Link to another incident](#) [Assign to me](#) ...

Manage alert

Alert details

Incident	Exploit incident on one endpoint
Detection source	Antivirus
Detection technology	Client
Detection status	Blocked
Category	Exploit
First activity	Aug 5, 2020, 10:19:34 PM
Last activity	Aug 12, 2020, 3:47:16 PM
Generated on	Aug 5, 2020, 10:21:22 PM
Assigned to	(Unassigned)
Threat found	CVE-2012-0217

Perform actions on a device

Lesson introduction

Microsoft Defender for Endpoint provides the remote capability to contain devices and collect forensics data. The Live Response feature allows for a restricted remote access shell on the device.

You are a Security Operations Analyst working at a company that has implemented Microsoft Defender for Endpoint, and your primary job is to remediate incidents. You are assigned an incident with alerts related to a suspicious PowerShell command line. You start by reviewing the incident and understand all the related alerts, devices, and evidence.

You open the alert page to review the Alert Story and decide to perform further analysis on the device. You open the Device page and decide that you need remote access to the device to run a custom PowerShell script to collect more forensics information.

You initiate a Live Response session from the Device page and execute a PowerShell script from your script library. You download the file for use with forensics tools. After reviewing the forensics data, you perform the device isolation action from the Device page.

Learning objectives

After completing this lesson, you should be able to:

- Perform actions on a device using Microsoft Defender for Endpoint
- Conduct forensics data collection using Microsoft Defender for Endpoint
- Access devices remotely using Microsoft Defender for Endpoint

Explain device actions

When investigating a device, you can perform actions, collect data, or remotely access the machine. Defender for Endpoint provides the device control required.

You can perform the following containment actions:

- Isolate Device
- Restrict app execution
- Run antivirus scan

You can perform the following investigation actions:

- Initiate Automated Investigation
- Collect investigation package
- Initiate Live Response Session

The Action center provides information on actions that were taken on a device or file.

Isolate devices from networks

Depending on the severity of the attack and the sensitivity of the device, you might want to isolate the device from the network. This action can help prevent the attacker from controlling the compromised device and performing further activities such as data exfiltration and lateral movement.

This device isolation feature disconnects the compromised device from the network while retaining connectivity to the Defender for Endpoint service, which continues to monitor the device.

On Windows 10, version 1709 or later, you'll have another control over the network isolation level. You can also choose to enable Outlook, Microsoft Teams, and Skype for Business connectivity (a.k.a 'Selective Isolation').

Once you have selected Isolate device on the device page, type a comment and select Confirm. The Action center will show the scan information and the device timeline will include a new event.

When a device is being isolated, a notification is displayed to inform the user that the device is being isolated from the network.

Restrict app execution

In addition to containing an attack by stopping malicious processes, you can also lock down a device and prevent subsequent attempts of potentially malicious programs from running.

Important: This action is available for devices on Windows 10, version 1709 or later. This feature is available if your organization uses Microsoft Defender Antivirus. This action needs to meet the Windows Defender Application Control code integrity policy formats and signing requirements.

To restrict an application from running, a code integrity policy is applied that only allows files to run if they are signed by a Microsoft issued certificate. This method of restriction can help prevent an attacker from controlling compromised devices and performing further malicious activities.

You'll be able to reverse the restriction of applications from running at any time. The button on the device page will change to say Remove app restrictions, and then you take the same steps as restricting app execution.

Once you have selected Restrict app execution on the device page, type a comment and select Confirm. The Action center will show the scan information, and the device timeline will include a new event.

When an app is restricted, a notification is displayed to inform the user that an app is being restricted from running.

Collect investigation package from devices

As part of the investigation or response process, you can collect an investigation package from a device. By collecting the investigation package, you can identify the current state of the device and further understand the tools and techniques used by the attacker.

To download the package (Zip file) and investigate the events that occurred on a device

- Select Collect investigation package from the row of response actions at the top of the device page.
- Specify in the text box why you want to do this action. Select Confirm.
- The zip file will download

Alternate way:

- Select Action center from the response actions section of the device page.
- In the Action center fly-out, select Package collection package available to download the zip file.

The package contains the following folders:

Autoruns

Contains set of files that each represent the content of the registry of a known auto start entry point (ASEP) to help identify attacker's persistency on the device. If the registry key is not found, the file will contain the following message: "ERROR: The system was unable to find the specified registry key or value."

Installed programs

This .CSV file contains the list of installed programs that can help identify what is currently installed on the device. For more information, see Win32_Product class.

Network connections

This folder contains a set of data points related to the connectivity information, which can help identify connectivity to suspicious URLs, attacker's command and control (C&C) infrastructure, any lateral movement, or remote connections.

- ActiveNetConnections.txt – Displays protocol statistics and current TCP/IP network connections. It provides the ability to look for suspicious connectivity made by a process.
- Arp.txt – Displays the current address resolution protocol (ARP) cache tables for all interfaces.
- ARP cache can reveal other hosts on a network that have been compromised or suspicious systems on the network that might have been used to run an internal attack.
- DnsCache.txt - Displays the contents of the DNS client resolver cache, which includes both entries preloaded from the local Hosts file and any recently obtained resource records for name queries resolved by the computer. This can help in identifying suspicious connections.
- IpConfig.txt – Displays the full TCP/IP configuration for all adapters. Adapters can represent physical interfaces, such as installed network adapters, or logical interfaces, such as dial-up connections.
- FirewallExecutionLog.txt and pfirewall.log

Prefetch files

Windows Prefetch files are designed to speed up the application startup process. It can be used to track all the files recently used in the system and find traces for applications that might have been deleted but can still be found in the prefetch file list.

- Prefetch folder – Contains a copy of the prefetch files from %SystemRoot%\Prefetch. It is suggested to download a prefetch file viewer to view the prefetch files.
- PrefetchFilesList.txt – Contains the list of all the copied files that can be used to track if there were any copy failures to the prefetch folder.

Processes

Contains a .CSV file listing the running processes, which provide the ability to identify current processes running on the device. This can be useful when identifying a suspicious process and its state.

Scheduled tasks

Contains a .CSV file listing the scheduled tasks, which can be used to identify routines performed automatically on a chosen device to look for suspicious code that was set to run automatically.

Security event log

Contains the security event log, which contains records of login or logout activity or other security-related events specified by the system's audit policy. You can open the event log file using the Event viewer.

Services

Contains a .CSV file that lists services and their states.

Windows Server Message Block (SMB) sessions

Lists shared access to files, printers, serial ports, and miscellaneous communications between nodes on a network. This can help identify data exfiltration or lateral movement. It also contains files for SMBInboundSessions and SMBOutboundSession. If there are no sessions (inbound or outbound), you'll get a text file that tells you that there are no SMB sessions found.

System information

Contains a SystemInformation.txt file that lists system information such as OS version and network cards.

Temp directories

Contains a set of text files that lists the files located in %Temp% for every user in the system. This can help to track suspicious files that an attacker may have dropped on the system. If the file contains the following message: "The system cannot find the path specified", it means that there is no temp directory for this user, and might be because the user didn't sign in to the system.

Users and groups

Provides a list of files that each represent a group and its members.

WdSupportLogs

Provides the MpCmdRunLog.txt and MPSupportFiles.cab.

CollectionSummaryReport.xls

This file is a summary of the investigation package collection, it contains the list of data points, the command used to extract the data, the execution status, and the error code if there is failure. You can use this report to track if the package includes all the expected data and identify if there were any errors.

Initiate live response session

Live response gives security operations teams instantaneous access to a device (also referred to as a machine) using a remote shell connection. This gives you the power to do in-depth investigative work and take immediate response actions to promptly contain identified threats in real time.

Live response is designed to enhance investigations by enabling your security operations team to collect forensic data, run scripts, send suspicious entities for analysis, remediate threats, and proactively hunt for emerging threats.

With live response, analysts can do all of the following tasks:

- Run basic and advanced commands to do investigative work on a device.
- Download files such as malware samples and outcomes of PowerShell scripts.
- Download files in the background (new).
- Upload a PowerShell script or executable to the library and run it on a device from a tenant level.
- Take or undo remediation actions.

Prerequisites

Before you can initiate a session on a device, make sure you fulfill the following requirements:

Verify that you're running a supported version of Windows 10

Enable live response from the settings page. You'll need to enable the live response capability in the Advanced features settings page.

Only users with manage security or global admin roles can edit these settings.

Ensure that the device has an Automation Remediation level assigned to it

You'll need to enable, at least, the minimum Remediation Level for a given Device Group. Otherwise you won't be able to establish a Live Response session to a member of that group.

Enable live response unsigned script execution (optional)

Allowing the use of unsigned scripts may increase your exposure to threats. Running unsigned scripts is not recommended as it can increase your exposure to threats. If you must use them however, you'll need to enable the setting in the Advanced features settings page.

Ensure that you have the appropriate permissions

Only users who have been provisioned with the appropriate permissions can initiate a session. The option to upload a file to the library is only available to those with the appropriate RBAC permissions. The button is greyed out for users with only delegated permissions. Depending on the role that's been granted to you, you can run basic or advanced live response commands. Users' permissions are controlled by RBAC custom role.

Live response dashboard overview

When you initiate a live response session on a device, a dashboard opens. The dashboard provides information about the session like:

- Who created the session
- When the session started
- The duration of the session

The dashboard also gives you access to:

- Disconnect session
- Upload files to the library
- Command console
- Command log

Live response commands

Depending on the role that's been granted to you, you can run basic or advanced live response commands. User permissions are controlled by RBAC custom roles. Live response is a cloud-based interactive shell; as such, specific command experience may vary in response time depending on network quality and system load between the end user and the target device.

Basic commands

The following commands are available for user roles that are granted the ability to run basic live response commands.

Command	Description
cd	Changes the current directory.
cls	Clears the console screen.
connect	Initiates a live response session to the device.
connections	Shows all the active connections.
dir	Shows a list of files and subdirectories in a directory.
download file_path	Downloads a file in the background.
drivers	Shows all drivers installed on the device.
fg command ID	Returns a file download to the foreground.
fileinfo	Get information about a file.
findfile	Locates files by a given name on the device.
help	Provides help information for live response commands.
persistence	Shows all known persistence methods on the device.
processes	Shows all processes running on the device.
registry	Shows registry values.
scheduledtasks	Shows all scheduled tasks on the device.
services	Shows all services on the device.
trace	Sets the terminal's logging mode to debug.

Advanced commands

The following commands are available for user roles that are granted the ability to run advanced live response commands.

Command	Description
analyze	Analyses the entity with various incrimination engines to reach a verdict.
getfile	Gets a file from the device. This command has a prerequisite command. You can use the -auto command with getfile to automatically run the prerequisite command.
run	Runs a PowerShell script from the library on the device.
library	Lists files that were uploaded to the live response library.
putfile	Puts a file from the library to the device. Files are saved in a working folder and are deleted when the device restarts by default.
remediate	Remediates an entity on the device. The remediation action will vary depending on the entity type. This command has a prerequisite command. You can use the -auto command with remediate to automatically run the prerequisite command.
Undo	Restores an entity that was remediated.

Use live response commands

The commands that you can use in the console follow similar principles as Windows Commands. The advanced commands offer a more robust set of actions that allow you to take more powerful actions such as download and upload a file, run scripts on the device, and take remediation actions on an entity.

Get a file from the device

For scenarios when you'd like to get a file from a device you're investigating, you can use the [getfile] command. This allows you to save the file from the device for further investigation.

The following file size limits apply:

- getFile limit: 3 GB
- fileInfo limit: 10 GB
- library limit: 250 MB

Download a file in the background

To enable your security operations team to continue investigating an impacted device, files can now be downloaded in the background.

- To download a file in the background, in the live response command console, type **download file_path &**.
- If you are waiting for a file to be downloaded, you can move it to the background by using **Ctrl + Z**.
- To bring a file download to the foreground, in the live response command console, type **fg command_id**.

Put a file in the library

Live response has a library where you can put files in. The library stores files (such as scripts) that can be run in a live response session at the tenant level. Live response allows PowerShell scripts to run. However, you must first put the files into the library before you can run them. You can have a collection of PowerShell scripts that can run on devices that you initiate live response sessions with.

To upload a file in the library:

1. Select **Upload file to library**.
2. Select **Browse** and select the file.
3. Provide a brief description.
4. Specify if you'd like to overwrite a file with the same name.
5. If you'd like to be, know what parameters are needed for the script, select the script parameters check box. In the text field, enter an example and a description.
6. Select **Confirm**.
7. (Optional) To verify that the file was uploaded to the library, run the library command.

Cancel a command

Anytime during a session, you can cancel a command by pressing CTRL + C.

Automatically run prerequisite commands

Some commands have prerequisite commands to run. If you don't run the prerequisite command, you'll get an error. For example, running the download command without *fileinfo* will return an error. You can use the *auto* flag to automatically run prerequisite commands, for example:

```
getfile c:\Users\user\Desktop\work.txt -auto
```

Run a PowerShell script

Before you can run a PowerShell script, you must first upload it to the library. After uploading the script to the library, use the **run** command to run the script. If you plan to use an unsigned script in the session, you'll need to enable the setting in the Advanced features settings page.

Apply command parameters

View the console help to learn about command parameters. To learn about an individual command, run:

```
help <command name>
```

When applying parameters to commands, parameters are handled based on a fixed order:

```
<command name> param1 param2
```

When specifying parameters outside of the fixed order, specify the name of the parameter with a hyphen before providing its value:

```
<command name> -param2_name param2
```

When using commands that have prerequisite commands, you can use flags:

```
<command name> -type file -id <file path> - auto or remediate file <file path>  
- auto.
```

Supported output types

Live response supports table and JSON format output types. For each command, there's a default output behavior. You can modify the output in your preferred output format using the following commands:

- output json
- output table

Supported output pipes

Live response supports output piping to CLI and file. CLI is the default output behavior.

View the command log

Select the Command log tab to see the commands used on the device during a session. Each command is tracked with full details such as:

- ID
- Command line
- Duration
- Status and input or output side bar

Command examples

The following is a command example, which demonstrates the use of the live response commands.

analyze

```
# Analyze the file malware.txt  
  
analyze file c:\Users\user\Desktop\malware.txt  
  
# Analyze the process by PID  
  
analyze process 1234
```

Limitations

Live response has the following limitations:

- Live response sessions are limited to 10 live response sessions at a time.
- Large-scale command execution is not supported.
- Live response session inactive timeout value is 5 minutes.
- A user can only initiate one session at a time.
- A device can only be in one session at a time.
- The following file size limits apply:
 - getFile limit: 3 GB
 - fileInfo limit: 10 GB
 - library limit: 250 MB

Perform evidence and entities investigations

Lesson introduction

Microsoft Defender for Endpoint provides information about forensic artifacts found in the environment. There are specific observable pages for Files, User Accounts, IP Addresses, and Domains.

You are a Security Operations Analyst working at a company that has implemented Microsoft Defender for Endpoint, and your primary job is to remediate incidents. You are assigned an incident with alerts related to a suspicious PowerShell command line.

You start by reviewing the incident and understand all the related alerts, devices, and evidence. The evidence tab shows three files, six processes, and one persistence method. One of the files has a name you have never seen before. You open the file page to review everything known about the file.

The file has never been seen in the organization other than this incident. If this is malware, it is good to know whether this file impacted only this machine. You decide to submit a deep analysis on the file to see if the file performs any suspicious activities. The results show suspicious activity; you then select Add Indicator from the file page to ensure Defender for Endpoint will use the indicator for detections.

Learning objectives

After completing this lesson, you should be able to:

- Investigate files in Microsoft Defender for Endpoint
- Investigate domains and IP addresses in Microsoft Defender for Endpoint
- Investigate user accounts in Microsoft Defender for Endpoint

Investigate a file

Investigate the details of a file associated with a specific alert, behavior, or event to help determine if the file exhibits malicious activities, identify the attack motivation, and understand the potential scope of the breach.

There are many ways to access the detailed profile page of a specific file. For example, you can use the search feature, select a link from the Alert process tree, Incident graph, Artifact timeline, or select an event listed in the Device timeline. You can get information from the following sections in the file view:

File details, Malware detection, File prevalence

- Deep analysis
- Alerts
- Observed in organization
- Deep analysis
- File names

Along the top of the profile page, above the file information cards. Actions you can perform here include:

- Stop and quarantine
- Add/edit indicator
- Download file
- Consult a threat expert
- Action center

Detailed profile page

File details, malware detection, and file prevalence

The file details, incident, malware detection, and file prevalence cards display various attributes about the file. You'll see details such as the file's MD5, the Virus Total detection ratio, and Microsoft Defender AV detection if available, and the file's prevalence, both worldwide and within your organizations.

Alerts

The Alerts tab provides a list of alerts that are associated with the file. This list covers much of the same information as the Alerts queue, except for the device group that the affected device belongs to, if applicable. You can choose what kind of information is shown by selecting Customize columns from the toolbar above the column headers.

Observed in organization

The Observed in the organization tab allows you to specify a date range to see which devices have been observed with the file. This tab will show a maximum of 100 devices. To see all devices with the file, export the tab to a CSV file, by selecting Export from the action menu above the tab's column headers.

Use the slider or the range selector to quickly specify a time period that you want to check for events involving the file. You can specify a time window as small as a single day. This will allow you to see only files that communicated with that IP Address at that time, drastically reducing unnecessary scrolling and searching.

Deep analysis

The Deep analysis tab allows you to submit the file for deep analysis to uncover more details about the file's behavior and its effect within your organizations. After you submit the file, the deep analysis report will appear in this tab once the results are available. If deep analysis did not find anything, the report will be empty, and the results space will remain blank.

File names

The File names tab lists all names the file has been observed to use within your organizations.

Deep file analysis

Cyber security investigations are typically triggered by an alert. Alerts are related to one or more observed files that are often new or unknown. Clicking a file takes you to the file view, where you can see the file's metadata. To enrich the data related to the file, you can submit the file for deep analysis.

The Deep analysis feature executes a file in a secure, fully instrumented cloud environment. Deep analysis results show the file's activities, observed behaviors, and associated artifacts, such as dropped files, registry modifications, and communication with IPs. Deep analysis currently supports extensive analysis of portable executable (PE) files (including .exe and .dll files).

Deep analysis of a file takes several minutes. Once the file analysis is complete, the Deep Analysis tab will update to display the date and time of the latest results available, and a summary of the report itself.

The Deep analysis summary includes a list of observed behaviors, some of which can indicate malicious activity, and observables, including contacted IPs and files created on the disk. If nothing was found, these sections will display a brief message.

The deep analysis results are matched against threat intelligence, and any matches will generate appropriate alerts.

Use the deep analysis feature to investigate the details of any file, usually during an investigation of an alert or for any other reason where you suspect malicious behavior. This feature is available within the Deep analysis tab on the file's profile page.

Submit for deep analysis is enabled when the file is available in the Defender for Endpoint backend sample collection, or if it was observed on a Windows 10 device that supports submitting to deep analysis. You can also manually submit a sample through the Microsoft Security Center Portal if the file was not observed on a Windows 10 device and wait for Submit for deep analysis button to become available.

When the sample is collected, Defender for Endpoint runs the file in a secure environment and creates a detailed report of observed behaviors and associated artifacts, such as files dropped on devices, communication to IPs, and registry modifications.

Submit files for deep analysis:

1. Select the file that you want to submit for deep analysis. You can select or search a file from any of the following views:
 - Alerts - select the file links from the Description or Details in the Artifact timeline
 - Devices list - select the file links from the Description or Details in the Device in the organization section
 - Search box - select File from the drop-down menu and enter the file name

2. In the Deep analysis tab of the file view, select **Submit**.

Only PE files are supported, including .exe and .dll files. A progress bar is displayed and provides information on the different stages of the analysis. You can then view the report when the analysis is done.

View deep analysis reports

View the deep analysis report that Defender for Endpoint provides to see the details of the deep analysis conducted on the file you submitted. This feature is available in the file view context.

You can view the comprehensive report that provides details on the following sections:

- Behaviors
- Observables

The details provided can help you investigate if there are indications of a potential attack.

1. Select the file you submitted for deep analysis.
2. Select the Deep analysis tab. If there are any previous reports, the report summary will appear in this tab.

Troubleshoot deep analysis

If you encounter a problem when trying to submit a file, try each of the following troubleshooting steps.

1. Ensure that the file in question is a PE file. PE files typically have .exe or .dll extensions (executable programs or applications).
2. Ensure the service has access to the file, that it still exists, and has not been corrupted or modified.
3. You can wait a short while and try to submit the file again if the queue is full or there was a temporary connection or communication error.
4. If the sample collection policy is not configured, then the default behavior is to allow sample collection. If it is configured, then verify the policy setting allows sample collection before submitting the file again. When sample collection is configured, then check the following registry value:
 - Path: HKLM\SOFTWARE\Policies\Microsoft\Windows Advanced Threat Protection
 - Name: AllowSampleCollection
 - Type: DWORD
 - Hexadecimal value :
 - Value = 0 – block sample collection
 - Value = 1 – allow sample collection
5. Change the organizational unit through the Group Policy.

File response actions

Quickly respond to detected attacks by stopping and quarantining files or blocking a file. After taking action on files, you can check activity details in the Action center. Response actions are available on a file's detailed profile page.

Response actions run along the top of the file page and include:

- Stop and Quarantine File

- Add Indicator
- Download file
- Action center

Stop and quarantine file

You can contain an attack in your organization by stopping the malicious process and quarantining the file where it was observed.

You can only take this action if:

- The device you're taking action on is running Windows 10, version 1703 or later
- The file does not belong to trusted third-party publishers or not signed by Microsoft
- Microsoft Defender Antivirus must at least be running on Passive mode.

The Stop and Quarantine File action includes stopping running processes, quarantining the files, and deleting persistent data, such as any registry keys. The stop and quarantine file action is limited to a maximum of 1000 devices. To stop a file on a larger number of devices, see Add indicator to block or allow file.

Stop and quarantine files

1. Select the file you want to stop and quarantine. You can select a file from any of the following views or use the Search box:
 - Alerts - select the corresponding links from the Description or Details in the Artifact timeline
 - Search box - select File from the drop-down menu and enter the file name
2. Go to the top bar and select **Stop and Quarantine File**.
3. Specify a reason, then select **Confirm**.

The Action center shows the submission information:

- Submission time - Shows when the action was submitted.
- Success - Shows the number of devices where the file has been stopped and quarantined.
- Failed - Shows the number of devices where the action failed and details about the failure.
- Pending - Shows the number of devices where the file is yet to be stopped and quarantined from. This can take time for cases when the device is offline or not connected to the network.

Select any of the status indicators to view more information about the action. For example, select Failed to see where the action failed. When the file is removed from a device, the user receives a notification.

A new event is added for each device in the device timeline where a file was stopped and quarantined. For files widely used throughout an organization, a warning is shown before action is taken to validate that the operation is intended.

Restore file from quarantine

You can roll back and remove a file from quarantine if you've determined that it's clean after an investigation. Run the following command on each device where the file was quarantined.

1. Open an elevated command-line prompt on the device:
 - Go to Start and type *cmd*.
 - Right-click Command prompt and select **Run as administrator**.

2. Enter the following command, and press **Enter**:

```
"%ProgramFiles%\Windows Defender\MpCmdRun.exe" -Restore -Name EUS:Win32/CustomEnterpriseBlock -All
```

Add indicator to block or allow a file

You can prevent further propagation of an attack in your organization by banning potentially malicious files or suspected malware. If you know a potentially malicious portable executable (PE) file, you can block it. This operation will prevent it from being read, written, or executed on devices in your organization.

Enable the block file feature

To start blocking files, you first need to turn the Block or allow feature on in Settings.

Allow or block file

When you add an indicator hash for a file, you can choose to raise an alert and block the file whenever a device in your organization attempts to run it. Files automatically blocked by an indicator won't show up in the files' Action center, but the alerts will still be visible in the Alerts queue. See manage indicators for more details on blocking and raising alerts on files. To stop blocking a file, remove the indicator. You can do so via the Edit Indicator action on the file's profile page. This action will be visible in the same position that the *Add Indicator* action was before adding the indicator. You can also edit indicators from the Settings page, under Rules > Indicators. Indicators are listed in this area by their file's hash.

Download file

Selecting Download file from the response actions allows you to download a local, password-protected .zip archive containing your file. When you select this action, a fly-out will appear. From the fly-out, you can record a reason as to why you are downloading the file. You can also set a password to open the file. If a file is not already stored by Defender for Endpoint, you cannot download it. Instead, you will see a Collect file button in the same location. If a file has not been seen in the organization in the past 30 days, Collect file will be disabled.

Check activity details in the action center

The Action center provides information on actions that were taken on a device or file. You'll be able to view the following details:

- Investigation package collection
- Antivirus scan
- App restriction
- Device isolation

All other related details are also shown, for example, submission date/time, submitting user, and if the action succeeded or failed.

Investigate a user account

Identify user accounts with the most active alerts (displayed on the dashboard as "Users at risk") and investigate cases of potentially compromised credentials, or pivot on the associated user account when investigating an alert or device to identify possible lateral movement between devices with that user account.

You can find user account information in the following views:

- Dashboard
- Alert queue
- Device details page

A clickable user account link is available in these views, which will take you to the user account details page where more details about the user account are shown.

When you investigate a user account entity, you'll see:

- User account details, Azure Advanced Threat Protection (Azure ATP) alerts, and logged on devices, role, log-on type, and other details
- Overview of the incidents and user's devices
- Alerts related to this user
- Observed locations in the organization (devices logged on to)



User details

The User details pane on left provides information about the user, such as related open incidents, active alerts, SAM name, SID, Azure ATP alerts, number of devices the user is logged on to, when the user was first and last seen, role, and log-on types. Depending on the integration features you've enabled, you'll see other details. For example, if you enable the Skype for business integration, you'll be able to contact the user from the portal. The Azure ATP alerts section contains a link that will take you to the Azure ATP

page if you have enabled the Azure ATP feature, and there are alerts related to the user. The Azure ATP page will provide more information about the alerts.

Overview

The Overview tab shows the incident details and a list of the devices the user has logged on to. You can expand these to see details of the log-on events for each device.

Alerts

The Alerts tab provides a list of alerts that are associated with the user account. This list is a filtered view of the Alert queue and shows alerts where the user context is the selected user account, the date when the last activity was detected, a short description of the alert, the device associated with the alert, the alert's severity, the alert's status in the queue, and who is assigned the alert.

Observed in organization

The Observed in organization tab allows you to specify a date range to see a list of devices where this user was observed logged on to, the most frequent and least frequent logged on user account for each of these devices, and total observed users on each device. Selecting an item on the Observed in organization table will expand the item, revealing more details about the device. Directly selecting a link within an item will send you to the corresponding page.

Investigate an IP addresses

Examine possible communication between your devices and external internet protocol (IP) addresses.

Identifying all devices in the organization that communicated with a suspected or known malicious IP address, such as Command and Control (C2) servers, helps determine the potential scope of the breach, associated files, and infected devices.

You can find information from the following sections in the IP address view:

- IP worldwide
- Reverse DNS names
- Alerts related to this IP
- IP in organization
- Prevalence

IP Worldwide and Reverse DNS names

The IP address details section shows attributes of the IP address such as its ASN and its Reverse DNS names.

Alerts related to this IP

The Alerts related to this IP section provides a list of alerts that are associated with the IP.

IP in organization

The IP in the organization section provides details on the prevalence of the IP address in the organization.

Prevalence

The Prevalence section displays how many devices have connected to this IP address and when the IP was first and last seen. You can filter the results of this section by time period; the default period is 30 days.

Most recent observed devices with IP

The most recent observed devices with IP section provides a chronological view on the events and associated alerts that were observed on the IP address.

Investigate an external IP:

1. Select **IP** from the Search bar drop-down menu.
2. Enter the IP address in the Search field.
3. Select the search icon or press Enter.

Details about the IP address are displayed, including registration details (if available), reverse IPs (for example, domains), prevalence of devices in the organization that communicated with this IP Address (during the selected time period), and the devices in the organization that were observed communicating with this IP address.

Investigate a domain

Investigate a domain to see if devices and servers in your enterprise network have been communicating with a known malicious domain.

You can investigate a domain by using the search feature or by clicking on a domain link from the Device timeline.

You can see information from the following sections in the URL view:

- URL details, Contacts, Nameservers
- Alerts related to this URL
- URL in organization
- Most recent observed devices with URL

URL worldwide

The URL Worldwide section lists the URL, a link to further details, the number of related open incidents, and the number of active alerts.

Incident

The Incident card displays a bar chart of all active alerts in incidents over the past 180 days.

Prevalence

The Prevalence card provides details on the URL's prevalence within the organization over a specified period of time.

Although the default time period is the past 30 days, you can customize the range by selecting the downward-pointing arrow in the corner of the card. The shortest range available is for prevalence over the past day, while the longest range is over the past six months.

Alerts

The Alerts tab provides a list of alerts that are associated with the URL. The table shown here is a filtered version of the alerts visible on the Alert queue screen, showing only alerts associated with the domain, their severity, status, the associated incident, classification, investigation state, and more.

The Alerts tab can be adjusted to show more or less information by selecting Customize columns from the action menu above the column headers. The number of items displayed can also be adjusted by selecting items per page on the same menu.

Observed in organization

The Observed in organization tab provides a chronological view of the events and associated alerts observed on the URL. This tab includes a timeline and a customizable table listing event details, such as the time, device, and a brief description of what happened.

You can view events from different periods of time by entering the dates into the text fields above the table headers. You can also customize the time range by selecting different areas of the timeline.

Investigate a domain:

1. Select **URL** from the Search bar drop-down menu.
2. Enter the URL in the Search field.
3. Select the search icon or press Enter. Details about the URL are displayed. Search results will only be returned for URLs observed in communications from devices in the organization.
4. Use the search filters to define the search criteria. You can also use the timeline search box to filter the displayed results of all devices in the organization observed communicating with the URL, the file associated with the communication and the last date observed.
5. Selecting any of the device names will take you to that device's view, where you can continue to investigate reported alerts, behaviors, and events.

Configure and manage automation

Lesson introduction

Microsoft Defender for Endpoint provides automated investigation and remediation. The automation configuration options allow for control of how the automation is applied to devices.

You are a Security Operations Analyst working at a company that is implementing Microsoft Defender for Endpoint. You have different remediation automation requirements for devices. You plan to create device groups to manage remediation levels.

Device groups provide two primary functions; set the remediation level, and set security access. You meet with your Security Operations team and design device groups to meet both of these functional requirements. You then configure the Remediation Level for each device group and assign the devices.

Learning objectives

After completing this lesson, you should be able to:

- Configure advanced features of Microsoft Defender for Endpoint
- Manage automation settings in Microsoft Defender for Endpoint

Configure advanced features

In the Microsoft 365 Defender portal, select **Settings**, select **Endpoints**, and then select **Advanced features** in the General area to configure advanced features.

The Advanced features area in the General Settings area provides many an on/off switch for features within the product. The following are settings that are automation focused.

Feature	Description
Automated Investigation	Enables the automation capabilities for investigation and response.
Enable EDR in block mode	When turned on, Microsoft Defender for Endpoint uses behavioral blocking and containment capabilities by blocking malicious artifacts or behaviors observed through post-breach endpoint detection and response (EDR) capabilities. This feature doesn't change how Microsoft Defender for Endpoint performs detection, alert generation, and incident correlation.
Automatically resolve alerts	Resolves an alert if Automated investigation finds no threats or has successfully remediated all malicious artifacts.
Allow or block file	Make sure that Windows Defender Antivirus is turned on and the cloud-based protection feature is enabled in your organization to use the allow or block file feature.

Automated investigation

Turn on this feature to take advantage of the automated investigation and remediation features of the service.

Autoresolve remediated alerts

For tenants created on or after Windows 10, version 1809, the automated investigation and remediation capability is configured by default to resolve alerts where the automated analysis result status is "No threats found" or "Remediated". If you don't want to have alerts auto-resolved, you'll need to turn off the feature manually.

The result of the autoresolve action may influence the Device risk level calculation based on the active alerts found on a device. If a security operations analyst manually sets the status of an alert to "In progress" or "Resolved," the autoresolve capability will not overwrite it.

Allow or block file

Blocking is only available if your organization fulfills these requirements:

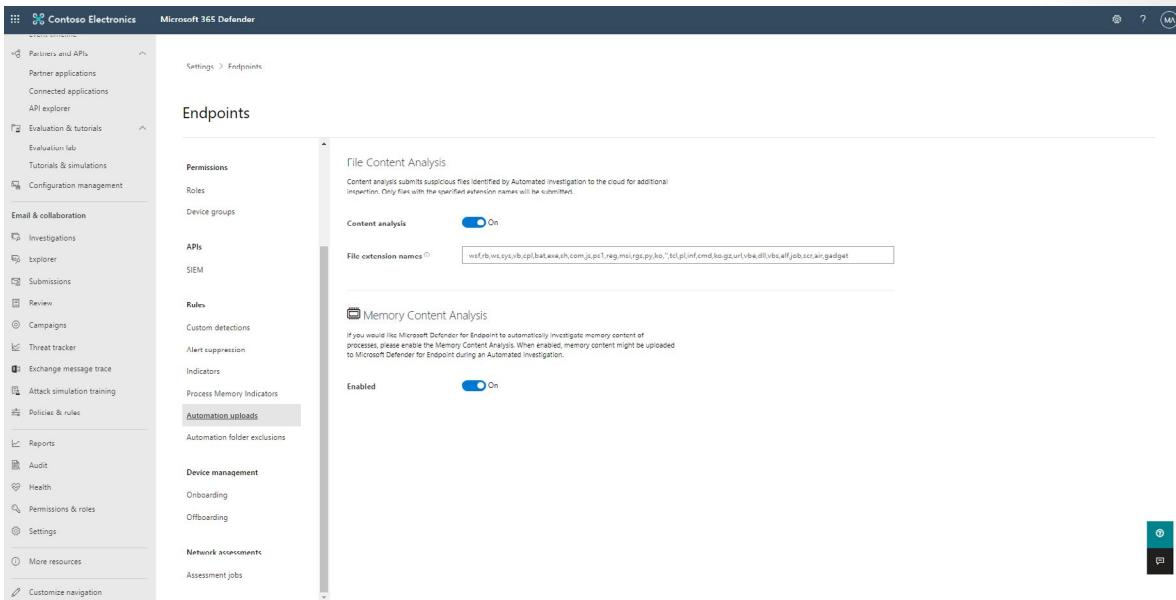
- Uses Microsoft Defender Antivirus as the active antimalware solution
- and
- The cloud-based protection feature is enabled

This feature enables you to block potentially malicious files in your network. Blocking a file will prevent it from being read, written, or executed on devices in your organization. After turning on this feature, you can block files via the Add Indicator tab on a file's profile page.

Manage automation uploads

Enable the **File Content Analysis** capability so that certain files and email attachments can automatically be uploaded to the cloud for additional inspection in Automated investigation. Identify the files and email attachments by specifying the file extension names and email attachment extension names. For example, if you add exe and bat as file or attachment extension names, then all files or attachments with those extensions will automatically be sent to the cloud for additional inspection during Automated investigation.

Enable the Memory Content Analysis capability if you would like Microsoft Defender for Endpoint to automatically investigate memory content of processes. When enabled, memory content might be uploaded to Microsoft Defender for Endpoint during an Automated investigation.



Add file extension names and attachment extension names

To configure file settings:

- In the Microsoft 365 Defender portal, select **Settings > Endpoints > Automation file uploads**.
- Toggle the content analysis setting between On and Off.
- Configure the following extension names and separate extension names with a comma:
 - File extension names - Suspicious files except email attachments will be submitted for additional inspection

Manage automation folder exclusions

Automation folder exclusions allow you to specify folders that the Automated investigation will skip. You can control the following attributes about the folder that you'd like to be skipped:

- Folders
- Extensions of the files
- File names

Folders

You can specify a folder and its subfolders to be skipped.

Extensions

You can specify the extensions to exclude in a specific directory. The extensions are a way to prevent an attacker from using an excluded folder to hide an exploit. The extensions explicitly define which files to ignore.

File names

You can specify the file names that you want to be excluded in a specific directory. The names are a way to prevent an attacker from using an excluded folder to hide an exploit. The names explicitly define which files to ignore.

Add an automation folder exclusion

To manage folder exclusions:

- In the Microsoft 365 Defender portal, select **Settings > Endpoints > Automation folder exclusions**.
- Select New folder exclusion.
- Enter the folder details:
 - Folder
 - Extensions
 - File names
 - Description
- Select **Save**.

Configure automated investigation and remediation capabilities

To configure automated investigation and remediation, turn on the features, and then set up device groups.

Turn on automated investigation and remediation

As a global administrator or security administrator:

1. In the Microsoft 365 Defender portal, select **Settings**.
2. In the Settings section, select **Endpoints** and then select **Advanced features**.
3. Turn on both Automated Investigation and Automatically resolve alerts.

Set up device groups

1. In the Microsoft 365 Defender portal, under **Permissions & roles**, select **Device groups**.
2. Select **+ Add device group**.
 - Create at least one device group, as follows:
 - Specify a name and description for the device group.
 - In the Automation level list, select a level, such as Full – remediate threats automatically. The automation level determines whether remediation actions are taken automatically or only upon approval. To learn more, see [How threats are remediated](#).
 - In the Members section, use one or more conditions to identify and include devices.
 - On the User access tab, select the Azure Active Directory groups that should have access to the device group you're creating.

-
3. Select **Done** when you're finished setting up your device group.

Automation levels

Full - remediate threats automatically (also referred to as full automation)

With full automation, remediation actions are performed automatically. All remediation actions that are taken can be viewed in the Action Center on the History tab. If necessary, a remediation action can be undone.

Semi - require approval for any remediation (also referred to as semi-automation)

With this level of semi-automation, approval is required for any remediation action. Such pending actions can be viewed and approved in the Action Center, on the Pending tab.

Semi - require approval for core folders remediation (also a type of semi-automation)

With this level of semi-automation, approval is required for any remediation actions needed on files or executables that are in core folders. Core folders include operating system directories, such as the Windows (\windows*). Remediation actions can be taken automatically on files or executables that are in other (non-core) folders. Pending actions for files or executables in core folders can be viewed and approved in the Action Center, on the Pending tab. Actions that were taken on files or executables in other folders can be viewed in the Action Center, on the History tab.

Semi - require approval for non-temp folders remediation (also a type of semi-automation)

With this level of semi-automation, approval is required for any remediation actions needed on files or executables that are not in temporary folders.

Temporary folders can include the following examples:

- \users*\appdata\local\temp*
- \documents and settings*\local settings\temp*
- \documents and settings*\local settings\temporary*
- \windows\temp*
- \users*\downloads*
- \program files\
- \program files (x86)*
- \documents and settings*\users*

Remediation actions can be taken automatically on files or executables that are in temporary folders. Pending actions for files or executables that are not in temporary folders can be viewed and approved in the Action Center, on the Pending tab. Actions that were taken on files or executables in temporary folders can be viewed and approved in the Action Center on the History tab.

No automated response (also referred to as 'no automation')

With no automation, the automated investigation does not run on your organization's devices. As a result, no remediation actions are taken or pending as a result of an automated investigation. However, other threat protection features, such as protection from potentially unwanted applications, can be in effect, depending on how your antivirus and next-generation protection features are configured.

Using the no automation option is not recommended because it reduces the security posture of your organization's devices. Consider setting up your automation level to full automation (or at least semi-automation).

Quickly configure remediation levels on device groups

Another way to set or update remediation levels on Device groups is in the Settings, General, Auto remediation page. The page provides a list of Device groups and the current remediation level for each. Select the row will allow you to adjust the remediation setting.

Block at risk devices

Contain a threat by not letting risky devices access your corporate resources through Conditional Access.

You'll need a Microsoft Intune environment, with Intune managed and Azure AD joined Windows 10 devices.

There are steps you'll need to take in Microsoft Defender Security Center, the Intune portal, and Azure AD portal.

The required roles to access these portals and implement Conditional access:

- Microsoft Defender Security Center - You'll need to sign in to the portal with a global administrator role to turn on the integration.
- Intune - You'll need to sign in to the portal with security administrator rights with management permissions.
- Azure AD portal - You'll need to sign in as a global administrator, security administrator, or Conditional Access administrator.

Take the following steps to enable Conditional Access:

1. Turn on the Microsoft Intune connection from Microsoft 365 Defender portal
2. Turn on the Defender for Endpoint integration in Intune
3. Create the compliance policy in Intune
4. Assign the policy
5. Create an Azure AD Conditional Access policy

Turn on the Microsoft Intune connection

1. In the Microsoft 365 Defender portal, select **Configuration management** and then under Connect to Intune select **Go to settings**.
2. Toggle the Microsoft Intune connection setting to **On**.
3. Select **Save preferences**.

Turn on the Defender for Endpoint integration in Endpoint Manager

1. Sign in to the Microsoft Endpoint Manager admin center <https://endpoint.microsoft.com>.
2. Select **Endpoint Security** from the left and then under Setup select **Microsoft Defender for Endpoint**.
3. Set **Connect Windows devices to Microsoft Defender for Endpoint** to **On**.

Create the compliance policy in Endpoint Manager

1. In the Microsoft Endpoint Manager admin center, select **Devices**, then select **Compliance policies**.
2. Select **+ Create policy**.
3. In Platform, select **Windows 10 and later** and then select **Create**.
4. Enter a Name and Description and select **Next**
5. In the Device Health settings, set **Require the device to be at or under the machine risk score** to your preferred level:
 - Low: The device is compliant if only low-level threats exist. Devices with medium or high threat levels are not compliant.
 - Medium: The device is compliant if the threats found on the device are low or medium. If high-level threats are detected, the device is determined as noncompliant.
 - High: This level is the least secure and allows all threat levels. So devices with high, medium, or low threat levels are considered compliant.
6. Select **Next** until you get to ***Assignments**.
7. Include or exclude your Azure AD groups to assign them the policy. Select **Next** until you can Create to save your changes (and create the policy).

Create an Azure AD Conditional Access policy

1. In the Azure portal, open Azure **Active Directory** > **Conditional Access** > **New policy**.
2. Enter a policy Name, and select **Users and groups**. Use the Include or Exclude options to add your groups for the policy, and select Done.
3. Select Cloud apps, and choose which apps to protect. For example, choose **Select apps**, and select Office 365 SharePoint Online and Office 365 Exchange Online. Select Done to save your changes.
4. Select **Conditions** > **Client apps** to apply the policy to apps and browsers. For example, select Yes, and then enable Browser and Mobile apps and desktop clients. Select Done to save your changes.
5. Select **Grant** to apply Conditional Access based on device compliance. For example, select **Grant access** > **Require device to be marked as compliant**. Choose **Select** to save your changes.
6. Select **Enable policy**, and then **Create** to save your changes.

Configure for alerts and detections

Lesson introduction

Microsoft Defender for Endpoint provides configuration options for alerts and detections. The configurations include notifications, custom indicators, and detection rules.

You are a Security Operations Analyst working at a company that has implemented Microsoft Defender for Endpoint. You are responsible for managing alert related settings in the environment. You manage Live Response settings, alert notification settings, indicators, and custom detections.

Your threat hunting team has provided you a CSV file with indicators they would like Defender for Endpoint to alert on. In the Settings page, Rules area, you select indicators and then import. After the file is imported, the indicators will be used in detections.

Your manager asks for alert notifications for a specific device group and with the severity of high. In the Settings page, General area, you select Alert notifications. You then create an alert notification rule to meet the manager's request.

Learning objectives

After completing this lesson, you should be able to:

- Configure alert settings in Microsoft Defender for Endpoint
- Manage indicators in Microsoft Defender for Endpoint

Configure advanced features

The Advance features page in the General area of the Settings - Endpoints are of the Microsoft 365 Defender portal provides the following alert and detection-related settings:

The Advanced features area in General Settings area provides many an on/off switch for features within the product. The following are settings that are alert focused.

Feature	Description
Live Response	Live Response
Live Response unsigned script execution	Enables using unsigned scripts in Live Response.
Custom network indicators	Configures devices to allow or block connections to IP addresses, domains, or URLs in your custom indicator lists.

Live response

Turn on this feature so that users with the appropriate permissions can start a live response session on devices.

Live response unsigned script execution

Enabling this feature allows you to run unsigned scripts in a live response session.

Custom network indicators

Turning on this feature allows you to create indicators for IP addresses, domains, or URLs, which determine whether they will be allowed or blocked based on your custom indicator list.

Configure Email notifications

You can configure Defender for Endpoint to send email notifications to specified recipients for new alerts. This feature enables you to identify a group of individuals who will immediately be informed and can act on alerts based on their severity.

Only users with 'Manage security settings' permissions can configure email notifications. If you've chosen to use basic permissions management, users with Security Administrator or Global Administrator roles can configure email notifications.

You can set the alert severity levels that trigger notifications. You can also add or remove recipients of the email notification. New recipients get notified about alerts encountered after they are added. For more information about alerts, see [View and organize the Alerts queue](#).

If you're using role-based access control (RBAC), recipients will only receive notifications based on the device groups that were configured in the notification rule. Users with the proper permission can only create, edit, or delete notifications limited to their device group management scope. Only users assigned to the Global administrator role can manage notification rules that were configured for all device groups.

The email notification includes basic information about the alert and a link to the portal where you can do further investigation.

Create rules for alert notifications

You can create rules that determine the devices and alert severities to send email notifications to notification recipients.

1. In the Microsoft 365 Defender portal, select **Settings** then select **Endpoints** and then select **Email notifications**.
2. Select **+ Add item**.
3. Specify the General information:
 - Rule name - Specify a name for the notification rule.
 - Include organization name - Specify the customer name that appears on the email notification.
 - Include organization-specific portal link - Adds a link with the organization's tenant ID to allow access to a specific tenant for an organization.
 - Include device information - Includes the device name in the email alert body.
 - Devices - Choose whether to notify recipients for alerts on all devices (Global administrator role only) or selected device groups. For more information, see [Create and manage device groups](#).
 - Alert severity - Choose the alert severity level.
4. Select **Next**.
5. Enter the recipient's email address, then select **+ Add**. You can add multiple email addresses.
6. Check that email recipients are able to receive the email notifications by selecting **Send test email**.
7. Select **Save** to save the rule.

Manage alert suppression

There might be scenarios where you need to suppress alerts from appearing in the portal. You can create suppression rules for specific alerts known to be innocuous, such as known tools or processes in your organization. For more information on how to manage and suppress alerts, see [Manage Microsoft Defender for Endpoint alerts⁵](#).

View existing rules

You can view a list of all the suppression rules and manage them in one place. You can also turn an alert suppression rule on or off by completing these actions:

1. In the Microsoft 365 Defender portal, select **Settings** then select **Endpoints** and then under Rules select **Alert suppression**. The list of suppression rules that users in your organization have created is displayed.
2. Select a rule by selecting the check-box beside the rule name.
3. Select **Turn rule on**, **Edit rule**, or **Delete rule**. When making changes to a rule, you can choose to release alerts that it has already suppressed, regardless of whether or not these alerts match the new criteria.

Manage indicators

Indicator of compromise (IoCs) matching is an essential feature in every endpoint protection solution. This capability gives SecOps the ability to set a list of detection indicators and for blocking (prevention and response). Create indicators that define the detection, prevention, and exclusion of entities. You can define the action to be taken, the duration for when to apply the action, and the scope of the device group to apply it to.

Currently supported sources are the cloud detection engine of Defender for Endpoint, the automated investigation and remediation engine, and the endpoint prevention engine (Microsoft Defender AV).

Cloud detection engine

The Defender for Endpoint's cloud detection engine regularly scans collected data and tries to match the indicators you set. When there is a match, action will be taken according to the IoC settings you specified.

Endpoint prevention engine

The same list of indicators is honored by the prevention agent. Meaning, if Microsoft Defender AV is the primary AV configured, the matched indicators will be treated according to the settings. For example, if the action is "Alert and Block", Microsoft Defender AV will prevent file executions (block and remediate), and a corresponding alert will be raised. Otherwise, if the Action is set to "Allow", Microsoft Defender AV will not detect nor block the file from being run.

Automated investigation and remediation engine

The automated investigation and remediation behave the same. If an indicator is set to "Allow", Automated investigation and remediation will ignore a "bad" verdict for it. If set to "Block", Automated investigation and remediation will treat it as "bad".

The current supported actions are:

- Allow
- Alert only

⁵ <https://docs.microsoft.com/microsoft-365/security/defender-endpoint/manage-alerts?view=o365-worldwide>

- Alert and block

You can create an indicator for:

- Files
- IP addresses, URLs/domains
- Certificates

There is a limit of 15,000 indicators per tenant.

To manage indicators:

- In the navigation pane, select Settings > Indicators.
- Select the tab of the entity type you'd like to manage.
- Update the indicator details and select Save or select the Delete button if you'd like to remove the entity from the list.

Create indicators for files

You can prevent further propagation of attacks in your organization by banning potentially malicious files or suspected malware. If you know a potentially malicious portable executable (PE) file, you can block it. This operation will prevent it from being read, written, or executed on machines in your organization.

There are two ways you can create indicators for files:

- By creating an indicator through the settings page
- By creating a contextual indicator using the add indicator button from the file details page

Prerequisites

Before you create indicators for files you should understand the following prerequisites:

- This feature is available if your organization uses Windows Defender Antivirus and Cloud-based protection is enabled. For more information, see [Manage cloud-based protection](#).
- The Antimalware client version must be 4.18.1901.x or later.
- It is supported on machines with Windows 10, version 1703 or later, Windows server 2016 and 2019.
- To start blocking files, you first need to turn the Block or allow feature on in Settings.
- This feature is designed to prevent suspected malware (or potentially malicious files) from being downloaded from the web. It currently supports portable executable (PE) files, including .exe and .dll files. The coverage will be extended over time.

Important: The allow or block function cannot be done on files if the file's classification exists on the device's cache prior to the allow or block action. Trusted signed files will be treated differently. Defender for Endpoint is optimized to handle malicious files. Trying to block trusted signed files, in some cases, may have performance implications. Typically, file blocks are enforced within a couple of minutes but can take upwards of 30 minutes.

Create an indicator for files

To learn more about indicators for files see [Create indicator for files⁶](#)

⁶ <https://docs.microsoft.com/microsoft-365/security/defender-endpoint/indicator-file?view=o365-worldwide>

Create a contextual indicator from the file details page

One of the options when taking response actions on a file is adding an indicator for the file. When you add an indicator hash for a file, you can choose to raise an alert and block the file whenever a machine in your organization attempts to run it. Files automatically blocked by an indicator won't show up in the file's Action center, but the alerts will still be visible in the Alerts queue.

Create indicators for IPs and URLs/domains

Defender for Endpoint can block what Microsoft deems as malicious IPs/URLs through Windows Defender SmartScreen for Microsoft browsers and through Network Protection for non-Microsoft browsers or calls made outside of a browser.

The threat intelligence data set for this has been managed by Microsoft.

By creating indicators for IPs and URLs or domains, you can now allow or block IPs, URLs, or domains based on your own threat intelligence. You can do this through the settings page or by machine groups if you deem certain groups to be more or less at risk than others. Classless Inter-Domain Routing (CIDR) notation for IP addresses is not supported.

Prerequisites

You should understand the following prerequisites prior to creating indicators for IPs, URLs, or domains:

- URL/IP allow and block relies on the Defender for Endpoint component Network Protection to be enabled in block mode. For more information on Network Protection and configuration instructions, see [Enable network protection](#).
- The Antimalware client version must be 4.18.1906.x or later.
- Supported on machines on Windows 10, version 1709 or later.
- Ensure that *Custom network indicators* are enabled in Microsoft Defender Security Center > Settings > Advanced features. For more information, see [Advanced features](#).

Only external IPs can be added to the indicator list. Indicators cannot be created for internal IPs. For web protection scenarios, we recommend using the built-in capabilities in Microsoft Edge. Microsoft Edge uses Network Protection to inspect network traffic and allows blocks for TCP, HTTP, and HTTPS (TLS). For all other processes, web protection scenarios use Network Protection for inspection and enforcement:

- IP is supported for all three protocols
- Only single IP addresses are supported (no CIDR blocks or IP ranges)
- Encrypted URLs (full path) can only be blocked on first party browsers
- Encrypted URLs (FQDN only) can be blocked outside of first party browsers
- Full URL path blocks can be applied on the domain level and all unencrypted URLs

There may be up to 2 hours of latency (usually less) between the time the action is taken and the URL and IP being blocked.

Create an indicator for IPs, URLs, or domains

To learn more about indicators for IPs and URLs/domains see [Create indicators for IPs and URLs/domains⁷](#)

Create indicators based on certificates

You can create indicators for certificates. Some common use cases include:

- Scenarios when you need to deploy blocking technologies, such as attack surface reduction rules and controlled folder access but need to allow behaviors from signed applications by adding the certificate in the allow list.
- Blocking the use of a specific signed application across your organization. By creating an indicator to block the certificate of the application, Windows Defender AV will prevent file executions (block and remediate), and the Automated Investigation and Remediation will behave the same.

Prerequisites

You should understand the following requirements prior to creating indicators for certificates:

- This feature is available if your organization uses Windows Defender Antivirus and Cloud-based protection is enabled. For more information, see [Manage cloud-based protection](#).
- The Antimalware client version must be 4.18.1901.x or later.
- Supported on machines on Windows 10, version 1703 or later, Windows server 2016 and 2019.
- The virus and threat protection definitions must be up to date.
- This feature currently supports entering .CER or .PEM file extensions.

A valid leaf certificate is a signing certificate with a valid certification path and must be chained to the Root Certificate Authority (CA) trusted by Microsoft. Alternatively, a custom (self-signed) certificate can be used as long as it's trusted by the client (Root CA certificate is installed under the Local Machine 'Trusted Root Certification Authorities'). The children or parents of the allow/block certificate IOCs are not included in the allow/block IoC functionality; only leaf certificates are supported. Microsoft signed certificates cannot be blocked.

It can take up to 3 hours to create and remove a certificate IoC.

Create an indicator for certificates:

1. In the Microsoft 365 Defender portal, select **Settings > Endpoints > Indicators**.
2. Select the Certificate tab.
3. Select **+ Add item**.
4. Specify the following details:
 - Indicator - Specify the entity details and define the expiration of the indicator.
 - Action - Specify the action to be taken and provide a description.
 - Scope - Define the scope of the machine group.
5. Review the details in the Summary tab, then select **Save**.

⁷ <https://docs.microsoft.com/microsoft-365/security/defender-endpoint/indicator-ip-domain?view=o365-worldwide>

Import a list of IoCs

You can also choose to upload a CSV file that defines the attributes of indicators, the action to be taken, and other details.

Download the sample CSV to know the supported column attributes.

1. In the Microsoft 365 Defender portal, select **Settings > Endpoints > Indicators**.
2. Select the tab of the entity type you'd like to import indicators for.
3. Select **Import > Choose file**.
4. Select **Import**. Do this for all the files you'd like to import.
5. Select **Done**.

The following table shows the supported parameters.

Parameter	Type	Description
indicatorType	Enum	Type of the indicator. Possible values are: "FileSha1", "File-Sha256", "IpAddress", "Domain-Name" and "Url". Required
indicatorValue	String	Identity of the Indicator entity. Required
action	Enum	The action that will be taken if the indicator will be discovered in the organization. Possible values are: "Alert", "AlertAnd-Block", and "Allowed". Required
title	String	Indicator alert title. Required
description	String	Description of the indicator. Required
expirationTime	DateTimeOffset	The expiration time of the indicator in the following format YYYY-MM-DDTHH:MM:SS.OZ. Optional
severity	Enum	The severity of the indicator. Possible values are: "Informational", "Low", "Medium" and "High". Optional
recommendedActions	String	TI indicator alert recommended actions. Optional
rbacGroupNames	String	Comma-separated list of RBAC group names the indicator would be applied to. Optional
category	String	Category of the alert. Examples include: Execution and credential access. Optional

Parameter	Type	Description
MITRE techniques	String	MITRE techniques code/id (comma separated). For more information, see Enterprise tactics. Optional It is recommended to add a value in category when a MITRE technique.

Manage custom detections

Custom detection rules built from advanced hunting queries let you proactively monitor various events and system states, including suspected breach activity and misconfigured devices. For more information on creating custom detections, see Create detection rules in the Manage Alerts and Incidents in Microsoft Defender for Endpoint module.

View existing rules

To view existing custom detection rules, in the Microsoft 365 Defender portal, select **Settings** then select **Endpoints** and then under Rules select **Custom detections**. The page lists all the rules with the following run information:

- Last run—when a rule was last run to check for query matches and generate alerts
- Last run status—whether a rule ran successfully
- Next run—the next scheduled run
- Status—whether a rule has been turned on or off

View rule details, modify rule, and run rule

To view comprehensive information about a custom detection rule, in the Microsoft 365 Defender portal, select **Settings** then select **Endpoints** and then under Rules select **Custom detections**. A page about the selected rule displays the following information:

- General information about the rule, including the details of the alert, run status, and scope
- List of triggered alerts
- List of triggered actions

You can also take the following actions on the rule from this page:

- Run—run the rule immediately. This action also resets the interval for the next run.
- Edit—modify the rule without changing the query
- Modify query—edit the query in advanced hunting
- Turn on / Turn off—enable the rule or stop it from running
- Delete—turn off the rule and remove it

Utilize Threat and Vulnerability Management

Lesson introduction

Microsoft Defender for Endpoint Threat and Vulnerability Management (TVM) discovers vulnerable and misconfigured devices based on known attack vectors and software vulnerabilities.

You are a Security Operations Analyst working at a company that has implemented Microsoft Defender for Endpoint. You are responsible for working with the endpoint management team to remediate weaknesses reported by Threat Vulnerability Management.

A new threat is listed in the Threat Analytics dashboard. You can quickly see that none of your devices are vulnerable to this new threat because TVM has already provided the analysis required on your devices.

Learning objectives

After completing this lesson, you should be able to:

- Describe Threat and Vulnerability Management in Microsoft Defender for Endpoint
- Identify vulnerabilities on your devices with Microsoft Defender for Endpoint
- Track emerging threats in Microsoft Defender for Endpoint

Explain Threat and Vulnerability Management

Effectively identifying, assessing, and remediating endpoint weaknesses is pivotal in running a healthy security program and reducing organizational risk. Threat and vulnerability management serves as an infrastructure for reducing organizational exposure, hardening endpoint surface area, and increasing organizational resilience.

Discover vulnerabilities and misconfigurations in real-time with sensors and without the need for agents or periodic scans. It prioritizes vulnerabilities based on the threat landscape, detections in your organization, sensitive information on vulnerable devices, and business context.

Bridging the workflow gaps

Threat and vulnerability management is built in, in real time, and cloud-powered. It's fully integrated with the Microsoft endpoint security stack, the Microsoft Intelligent Security Graph, and the application analytics knowledge base.

Vulnerability management is the industry's first solution to bridge the gap between security administration and IT administration during the remediation process. Create a security task or ticket by integrating with Microsoft Intune and Microsoft Endpoint Configuration Manager.

Real-time discovery

To discover endpoint vulnerabilities and misconfiguration, threat and vulnerability management uses the same agentless built-in Defender for Endpoint sensors to reduce cumbersome network scans and IT overhead.

It also provides:

- Real-time device inventory - Devices onboarded to Defender for Endpoint automatically report and push vulnerability and security configuration data to the dashboard.
- Visibility into software and vulnerabilities - Optics into the organization's software inventory and software changes like installations, uninstalls, and patches. Newly discovered vulnerabilities are reported with actionable mitigation recommendations for 1st and 3rd party applications.
- Application runtime context - Visibility on application usage patterns for better prioritization and decision-making.
- Configuration posture - Visibility into organizational security configuration or misconfigurations. Issues are reported in the dashboard with actionable security recommendations.

Intelligence-driven prioritization

Threat and vulnerability management helps customers prioritize and focus on the weaknesses that pose the most urgent and the highest risk to the organization. It fuses security recommendations with dynamic threat and business context:

- Exposing emerging attacks in the wild - Dynamically aligns the prioritization of security recommendations. Threat and vulnerability management focuses on vulnerabilities currently being exploited in the wild and emerging threats that pose the highest risk.
- Pinpointing active breaches - Correlates threat and vulnerability management and EDR insights to prioritize vulnerabilities being exploited in an active breach within the organization.
- Protecting high-value assets - Identify the exposed devices with business-critical applications, confidential data, or high-value users.

Seamless remediation

Threat and vulnerability management allows security administrators and IT administrators to collaborate seamlessly to remediate issues.

- Remediation requests sent to IT - Create a remediation task in Microsoft Intune from a specific security recommendation. We plan to expand this capability to other IT security management platforms.
- Alternate mitigations - Gain insights on more mitigations, such as configuration changes that can reduce the risk associated with software vulnerabilities.
- Real-time remediation status - Real-time monitoring of the status and progress of remediation activities across the organization.

Explore vulnerabilities on your devices

The Threat & Vulnerability Management area provides the following device vulnerability information

Software inventory

The Software inventory page opens with a list of software installed in your network, including the vendor name, weaknesses found, threats associated with them, exposed devices, impact to exposure score, and tags. You can filter the list view based on weaknesses found in the software, threats associated with them, and tags like whether the software has reached end-of-support.

Weaknesses

The Weaknesses page lists the software vulnerabilities your devices are exposed to by listing the Common Vulnerabilities and Exposures (CVE) ID. You can also view the severity, Common Vulnerability Scoring System (CVSS) rating, prevalence in your organization, corresponding breach, threat insights, and more.

Event timeline

The Event timeline is a risk news feed that helps you interpret how risk is introduced into the organization through new vulnerabilities or exploits. You can view events that may impact your organization's risk. For example, you can find new vulnerabilities that were introduced, vulnerabilities that became exploitable, exploits that were added to an exploit kit, and more. Event timeline also tells the story of your exposure score and Microsoft Secure Score for Devices so you can determine the cause of large changes. Events can impact your devices or your score for devices. Reduce your exposure by addressing what needs to be remediated based on the prioritized security recommendations.

Vulnerable devices report

The Reports area in the Microsoft 365 Defender portal has a Vulnerable devices report. The report shows graphs and bar charts with vulnerable device trends and current statistics. The goal is for you to understand the breadth and scope of your device exposure.

The graphs and charts include:

Severity level graphs

Each device is counted only once according to the most severe vulnerability found on that device.

Exploit availability graphs

Each device is counted only once based on the highest level of known exploit.

Vulnerability age graphs

Each device is counted only once under the oldest vulnerability publication date. Older vulnerabilities have a higher chance of being exploited.

Vulnerable devices by operating system platform graphs

The number of devices on each operating system that are exposed due to software vulnerabilities.

Vulnerable devices by Windows 10 version graphs

The number of devices on each Windows 10 version that are exposed due to vulnerable applications or OS.

Track emerging threats with Threat analytics

With more sophisticated adversaries and new threats emerging frequently and prevalently, it's critical to be able to quickly:

- Assess the impact of new threats

- Review your resilience against or exposure to the threats
- Identify the actions you can take to stop or contain the threats

Threat analytics is a set of reports from expert Microsoft security researchers covering the most relevant threats, including:

- Active threat actors and their campaigns
- Popular and new attack techniques
- Critical vulnerabilities
- Common attack surfaces
- Prevalent malware

Each report provides a detailed analysis of a threat and extensive guidance on how to defend against that threat. It also incorporates data from your network, indicating whether the threat is active and if you have applicable protections in place.

View the threat analytics dashboard

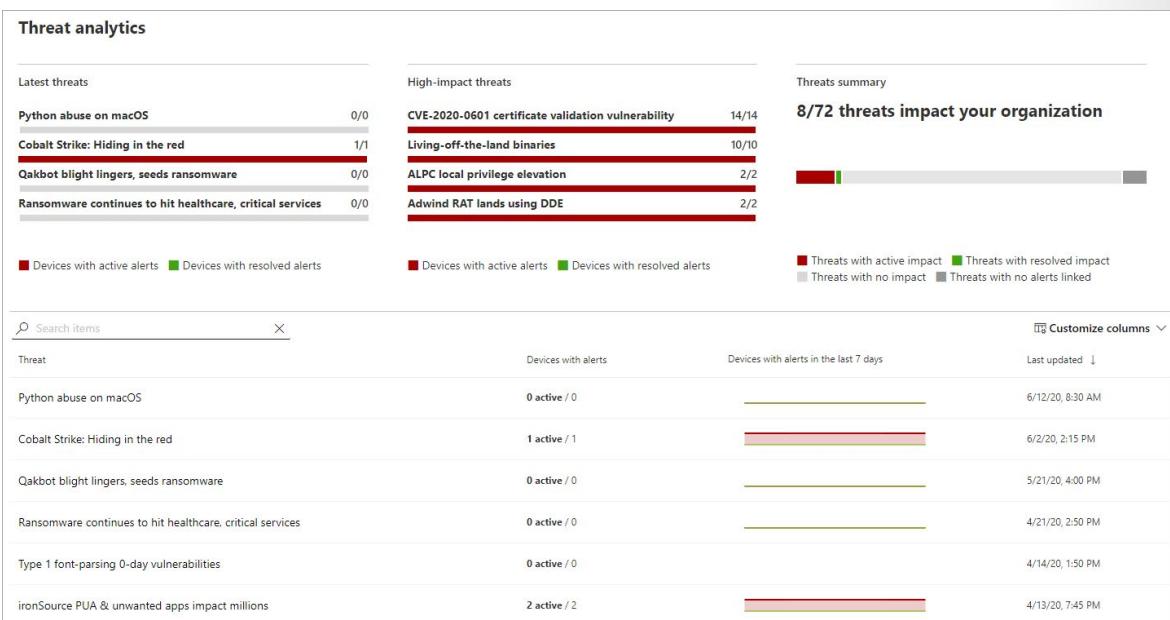
The threat analytics dashboard is a great jump-off point for getting to the reports that are most relevant to your organization. It summarizes the threats in the following sections:

Latest threats—lists the most recently published threat reports, along with the number of devices with active and resolved alerts.

High-impact threats—lists the threats that have had the highest impact on the organization. This section ranks threats by the number of devices that have active alerts.

Threat summary—shows the overall impact of tracked threats by showing the number of threats with active and resolved alerts.

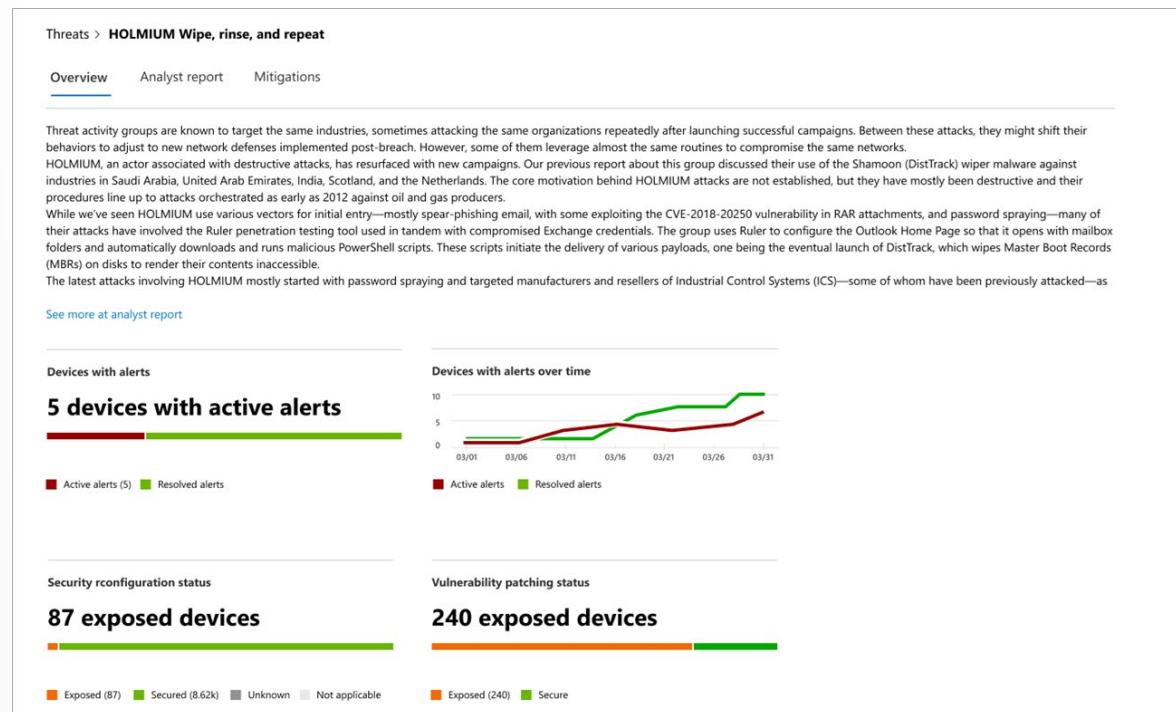
Select a threat from the dashboard to view the report for that threat.



View a threat analytics report

Each threat analytics report provides information in three sections: Overview, Analyst report, and Mitigations.

The Overview section provides a preview of the detailed analyst report. It also provides charts that highlight the impact of the threat to your organization and your exposure through misconfigured and unpatched devices.



Assess the impact on your organization

Each report includes charts designed to provide information about the organizational impact of a threat:

- Devices with alerts—shows the current number of distinct devices that have been impacted by the threat. A device is categorized as Active if there is at least one alert associated with that threat and Resolved if all alerts associated with the threat on the device have been resolved.
- Devices with alerts over time—shows the number of distinct devices with Active and Resolved alerts over time. The number of resolved alerts indicates how quickly your organization responds to alerts associated with a threat. Ideally, the chart should be showing alerts resolved within a few days.

Review security resilience and posture

Each report includes charts that provide an overview of how resilient your organization is against a given threat:

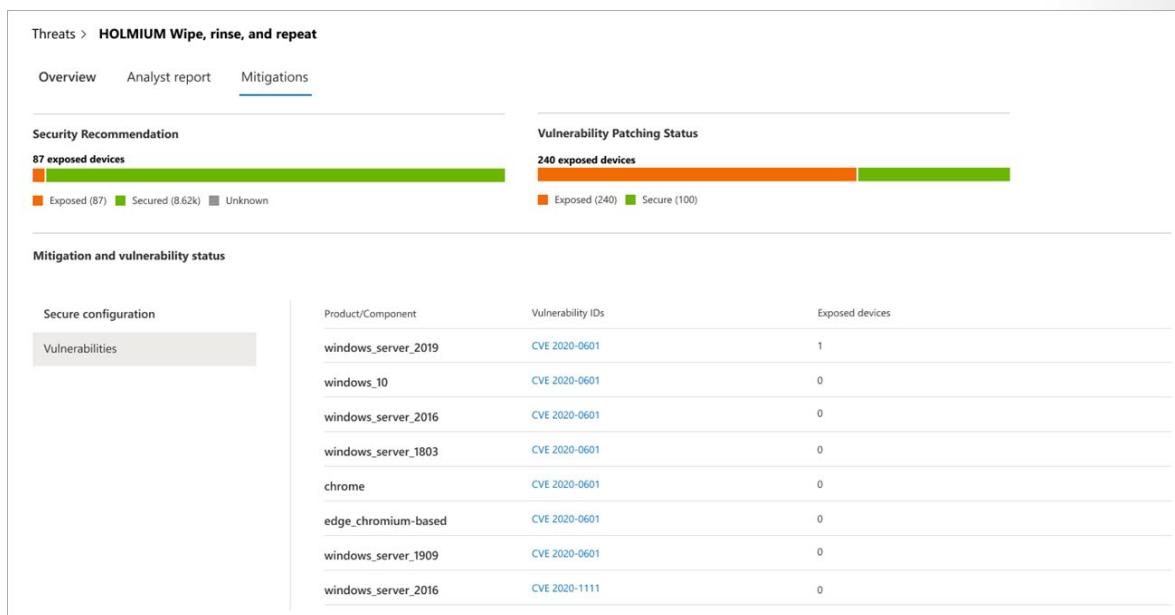
- Security configuration status—shows the number of devices that have applied the recommended security settings that can help mitigate the threat. Devices are considered Secure if they have applied all the tracked settings.
- Vulnerability patching status—shows the number of devices that have applied security updates or patches that address vulnerabilities exploited by the threat.

Mitigations: Review list of mitigations and the status of your devices

In the Mitigations section, review the list of specific, actionable recommendations that can help you increase your organizational resilience against the threat. The list of tracked mitigations includes:

- Security updates—deployment of security updates or patches for vulnerabilities
- Microsoft Defender Antivirus settings
 - Security intelligence version
 - Cloud-delivered protection
 - Potentially unwanted application (PUA) protection
 - Real-time protection

Mitigation information in this section incorporates data from threat and vulnerability management, which also provides detailed drill-down information from various links in the report.



Knowledge check

Check your Knowledge

Multiple choice

Item 1. In the Vulnerable Devices Report, which graphs show each device counted only once based on the highest level of known exploit?

- Vulnerability age graphs
- Exploit availability graphs
- Severity level graphs

Multiple choice

Item 2. Which report lists the software vulnerabilities your devices are exposed to by listing the Common Vulnerabilities and Exposures (CVE) ID?

- Event Timeline
- Weakness
- Software Inventory

Multiple choice

Item 3. Which report or dashboard provides a list of the most recently published threat reports?

- Vulnerable devices report
- Threat protection
- Threat Analytics

Multiple choice

Item 4. Which file type can be used to upload Indicators?

- JSON
- XML
- CSV

Multiple choice

Item 5. Which type is an accepted indicator type?

- Certificates
- Email subject line
- Code data

Multiple choice

Item 6. Which filter is included as part of an Alert notification rule?

- Alert Severity
- Account
- Subject IDs

Multiple choice

Item 7. Which is a valid remediation level?

- Semi - require approval for any remediation
- Semi - user accounts only
- Semi - files only

Multiple choice

Item 8. A security operations analyst needs to exclude a custom executable file c:\myapp\myapp.exe, which exclusion type should they use?

- File
- Extension
- Folder

Multiple choice

Item 9. In advanced features, which setting should be turned on to block files even if a third-party antivirus is used?

- Enable EDR in block mode
- Allow or block file
- Automated Investigation

Multiple choice

Item 10. Which of the following artifact types has an investigation page?

- Domain
- Hunter
- Threat Actor

Multiple choice

Item 11. What information is provided by a deep file analysis?

- Command history
- Registry Modifications
- Code change history

Multiple choice

Item 12. Which information is provided on the user account page?

- Associated alerts
- Security groups
- Threat hunt ID

Multiple choice

Item 13. The alert severity field contains which option?

- Informational
- Not Applicable
- Testing

Multiple choice

Item 14. A security operations analyst can create a custom detection from which of the following?

- Advanced Hunting
- An Alert
- An Incident

Multiple choice

Item 15. Which option can't be performed in the Action center?

- Manage pending actions.
- Review completed actions.
- Configure action email notifications.

Multiple choice

Item 16. Which is a deployment option for Windows 10?

- Group policy
- Microsoft Store
- General install package

Multiple choice

Item 17. Which security permission allows the configuration of storage settings?

- Manage security settings in Security Center
- Manage portal system settings
- Advanced commands

Lab - Mitigate threats using Defender for Endpoint

Lab: Mitigate threats using Microsoft Defender for Endpoint

To download the most recent version of this lab, please visit the SC-200 [GitHub repository⁸](#).

Note: Depending on the lab hosting solution used for your class delivery, the lab instructions may display directly in the virtual lab environment, in addition to being available in the GitHub repository. In that case, follow guidance from your instructor as to where you will access the lab steps from. Even if the GitHub version is not used for your class, you may still find it useful to be able to reference the lab instructions on GitHub after class is over.

Lab scenario

You are a Security Operations Analyst working at a company that is implementing Microsoft Defender for Endpoint. Your manager plans to onboard a few devices to provide insight into required changes to the SecOps team response procedures.

You start by initializing the Defender for Endpoint environment. Next, you onboard the initial devices for your deployment by running the onboarding script on the devices. You configure security for the environment. Lastly, you create Device groups and assign the appropriate devices.

Objectives

After you complete this lab, you will be able to:

- Deploy Microsoft Defender for Endpoint.
- Mitigate Attacks using Defender for Endpoint.

Lab setup

- Estimated time: 45 minutes

⁸ <https://github.com/MicrosoftLearning/SC-200T00A-Microsoft-Security-Operations-Analyst>

Answers

Multiple choice

Item 1. In the Vulnerable Devices Report, which graphs show each device counted only once based on the highest level of known exploit?

- Vulnerability age graphs
- Exploit availability graphs
- Severity level graphs

Explanation

The exploit graphs show this information.

Multiple choice

Item 2. Which report lists the software vulnerabilities your devices are exposed to by listing the Common Vulnerabilities and Exposures (CVE) ID?

- Event Timeline
- Weakness
- Software Inventory

Explanation

This report is listed by the CVE ID.

Multiple choice

Item 3. Which report or dashboard provides a list of the most recently published threat reports?

- Vulnerable devices report
- Threat protection
- Threat Analytics

Explanation

This dashboard provides a list of the most recently published threats.

Multiple choice

Item 4. Which file type can be used to upload Indicators?

- JSON
- XML
- CSV

Explanation

CSV file format is supported.

Multiple choice

Item 5. Which type is an accepted indicator type?

- Certificates
- Email subject line
- Code data

Explanation

Certificates are an indicator type.

Multiple choice

Item 6. Which filter is included as part of an Alert notification rule?

- Alert Severity
- Account
- Subject IDs

Explanation

Alert Severity is a filter option for the rule.

Multiple choice

Item 7. Which is a valid remediation level?

- Semi - require approval for any remediation
- Semi - user accounts only
- Semi - files only

Explanation

Correct. This is a valid remediation level.

Multiple choice

Item 8. A security operations analyst needs to exclude a custom executable file c:\myapp\myapp.exe, which exclusion type should they use?

- File
- Extension
- Folder

Explanation

File will exclude this specific file from automation

Multiple choice

Item 9. In advanced features, which setting should be turned on to block files even if a third-party antivirus is used?

- Enable EDR in block mode
- Allow or block file
- Automated Investigation

Explanation

EDR in block mode is used with 3rd party antivirus.

Multiple choice

Item 10. Which of the following artifact types has an investigation page?

- Domain
- Hunter
- Threat Actor

Explanation

There is an investigation page for Domain.

Multiple choice

Item 11. What information is provided by a deep file analysis?

- Command history
- Registry Modifications
- Code change history

Explanation

Registry modifications are reported.

Multiple choice

Item 12. Which information is provided on the user account page?

- Associated alerts
- Security groups
- Threat hunt ID

Explanation

Associate alerts are provided.

Multiple choice

Item 13. The alert severity field contains which option?

- Informational
- Not Applicable
- Testing

Explanation

Informational is an option.

Multiple choice

Item 14. A security operations analyst can create a custom detection from which of the following?

- Advanced Hunting
- An Alert
- An Incident

Explanation

Advanced hunting provides an option to save a query as a detection.

Multiple choice

Item 15. Which option can't be performed in the Action center?

- Manage pending actions.
- Review completed actions.
- Configure action email notifications.

Explanation

You can't configure Action notification in the Action center.

Multiple choice

Item 16. Which is a deployment option for Windows 10?

- Group policy
- Microsoft Store
- General install package

Explanation

Group policy is a valid deployment option.

Multiple choice

Item 17. Which security permission allows the configuration of storage settings?

- Manage security settings in Security Center
- Manage portal system settings
- Advanced commands

Explanation

This permission allows the configuration of storage settings.

Module 2 Mitigate threats using Microsoft 365 Defender

Introduction to threat protection with Microsoft 365

Lesson Introduction

Threats are the potential weakness that attackers can use to infiltrate your organization. Attackers will cross multiple domains like email, identity, endpoints, and applications to find a point of least resistance.

Today's defense solutions have been designed to protect, detect, and block threats for each domain separately, allowing attackers to exploit the seams and threshold differences between solutions—leaving the business vulnerable to attack. While one facet of an attack may be caught and blocked in email, the same threat actor may have also compromised identities by exploiting weak passwords or leaked credentials, or by fooling people into providing their passwords or authorization tokens. It's also possible for point solutions to overlook critical signals entirely because, in isolation, they failed to register as significant.

Learn about cybersecurity threats and how the new threat protection tools from Microsoft protect your organization's users, devices, and data.

Learning objectives

After completing this lesson, you should be able to:

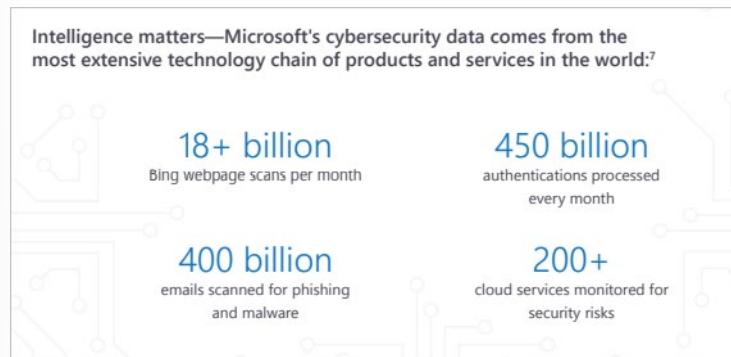
- Define security threats.
- Understand common threats.
- Explain how the threat landscape is evolving.

Introduction to threat protection

In today's cyberthreat environment, security teams are up against a constant flood of incoming risks. But with advanced security analytics, machine learning, and their own intuition, security experts are fighting back with agile, adaptable defense systems. While security teams comb through tens of thousands of cybersecurity alerts—trying to separate legitimate risks from the noise—attacks can slip through the cracks unnoticed and do significant damage.

There's too much to handle:

- The average large organization has to sift through 17,000 malware warnings each week.
- 99 days are the median amount of time for an organization to discover a security breach.
- It takes less than 48 hours for attackers to have complete control of a network.
- 4 million dollars is the average cost of a data breach to a company.



Microsoft 365 Defender is an integrated, cross-domain threat detection and response solution. It provides organizations with the ability to prevent, detect, investigate, and remediate sophisticated cross-domain attacks within their Microsoft 365 environments. Microsoft 365 Defender leverages raw signal data from individual service domains - user identity, endpoints, applications, email, and collaboration tools, normalizing the data at the ingestion point.

The data is analyzed and low-level signals that may otherwise be missed as well as individual alerts are correlated into incidents. This gives a complete view of an attack that can be responded to in its entirety. Powerful workflows and AI autoheal affected assets. Advanced hunting capabilities mean organizations can use their proprietary knowledge to uncover sophisticated breaches and customize their responses. But, Microsoft 365 Defender requires no specific expertise or customization, so defenders can immediately use the integrated console and combined incident views.

With Microsoft 365 Defender, security teams can:

- Automatically block attacks and eliminate their persistence to keep them from starting again.
- Prioritize incidents for investigation and response.
- Autoheal assets.
- Focus unique expertise on cross-domain hunting.

Microsoft 365 Defender suite protects:

- Endpoints with Microsoft Defender for Endpoint - Microsoft Defender for Endpoint is a unified endpoint platform for preventative protection, post-breach detection, automated investigation, and response.

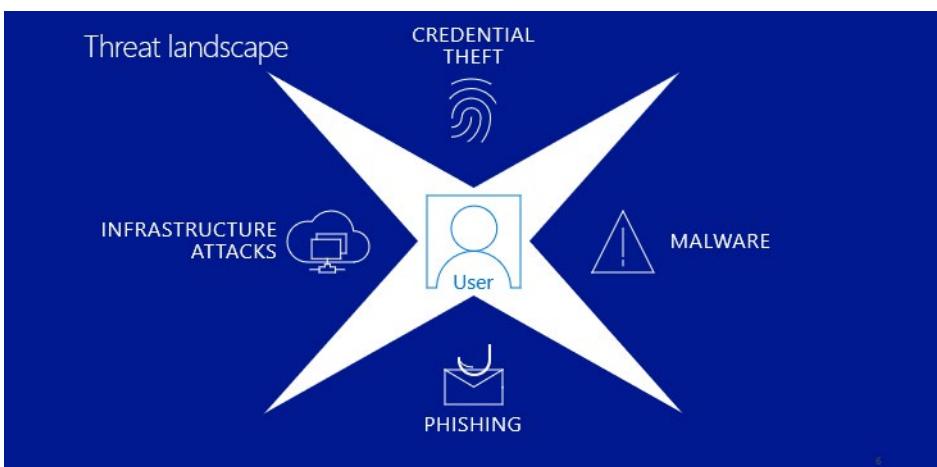
- Email and collaboration with Microsoft Defender for Office 365 - Microsoft Defender for Office 365 safeguards your organization against malicious threats posed by email messages, links (URLs) and collaboration tools.
- Identities with Microsoft Defender for Identity and Azure Active Directory (AD) Identity Protection - Microsoft Defender for Identity uses Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.
- Applications with Microsoft Cloud App security - Microsoft Cloud App security is a comprehensive cross-SaaS solution bringing deep visibility, strong data controls, and enhanced threat protection to your cloud apps.

Explore how to protect your organization with Microsoft 365 Defender

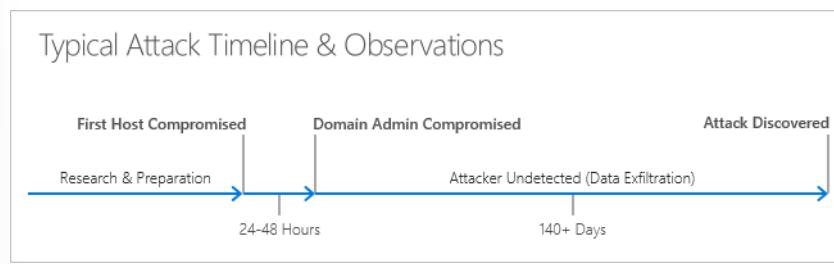
To dynamically identify new threats, Windows Defender Antivirus (part of Microsoft Defender for Endpoint) works with large sets of interconnected data in the Microsoft Intelligent Security Graph and powerful artificial intelligence (AI) systems driven by advanced machine learning models.

The Microsoft Graph Security API is a unified API that provides a standard interface and uniform schema to integrate security alerts and threat intelligence from multiple sources, enrich alerts and data with contextual information, and automate security operations. The security API is part of the Microsoft Graph, which is a unified REST API for integrating data and intelligence from Microsoft and partner products and services. Using Microsoft Graph, customers and partners can rapidly build solutions that authenticate once and use a single API call to access or act on security insights from multiple security solutions. Additional value is uncovered when you explore the other Microsoft Graph entities (Office 365, Azure Active Directory, Intune, and more) to tie business context with your security insights.

Common threats



Users face multiple threats—from credential theft to malware to phishing to infrastructure attacks. Examples of credential theft are Mimikatz, password spray, or breach harvesting. Examples of malware are viruses, ransomware, and the like. Phishing means gaining access to a user's computer and credentials, while infrastructure attacks include improperly secured virtual machines and resources in Azure.



Targeted attacks usually follow a timeline similar to the above image with:

- Research on company (Using social media, open-source intelligence sources, data from previous attacks) and preparing for the attack.
- Elevation of privilege attack (typically using credential theft, but also abuse of administrative/management tools and configuration weaknesses).
- Attackers typically extracting data for illicit purposes and going undetected for 200+ days. This is a general observation based on our incident response team's experience, which is similar to what is reported by others in the industry. Precise numbers are difficult to produce because evidence of the initial "Patient 0" host is frequently lost after such a long period of time.

Because most attacks are discovered by external parties, the variance in "time to discover" usually depends on the industry. As an example, the retail industry usually discovers attacks more quickly as credit cards are put into the market. The loss of other intellectual property such as technical designs takes longer to be apparent.

Guided Demonstration - Microsoft 365 Defender

A guided demonstration is a recorded click-through simulation. You do not use your lab tenant for this demonstration. Instead simply click the link [here¹](#) to launch this demonstration. A focus will appear in the demonstration showing you the next place to click to advance the demonstration.

In this experience you will do the following:

1. Detect security risks.
2. Investigate attacks.
3. Prevent harmful activities.

Time required: 19 minutes

¹ <https://aka.ms/M365Defender-InteractiveGuide>

Mitigate incidents using Microsoft 365 Defender

Lesson Introduction

Microsoft 365 Defender provides a purpose-driven user interface to manage and investigate security incidents and alerts across Microsoft 365 services.

You are a Security Operations Analyst working at a company that implemented Microsoft 365 Defender solutions, including Defender for Endpoint, Defender for Identity, Defender for Office 365, and Cloud App Security.

You need to see related alerts across all the solutions as one incident to see the incident's full impact and do a root cause investigation. The Microsoft Security center portal is a unified view of incidents and actions taken.

Learning objectives

After completing this lesson, you should be able to:

- Manage incidents in Microsoft 365 Defender
- Investigate incidents in Microsoft 365 Defender
- Conduct advanced hunting in Microsoft 365 Defender

Use the Microsoft 365 Defender portal

The Microsoft 365 Defender portal (<https://security.microsoft.com/>²) is a specialized workspace designed to meet the needs of security teams. These solutions are integrated across Microsoft 365 services and provide actionable insights to help reduce risks and safeguard your digital estate.

You can investigate the alerts that affect your network, understand what they mean, and collate evidence associated with the incidents so that you can devise an effective remediation plan.

The Home page shows many of the common cards that security teams need. The composition of cards and data is dependent on the user's role. Because the Microsoft 365 Defender portal uses role-based access control, different roles will see cards that are more meaningful to their day to day jobs.

This at-a-glance information helps you keep up with the latest activities in your organization. The Microsoft 365 Defender portal brings together signals from different sources to present a holistic view of your Microsoft 365 environment.

The Microsoft 365 Defender portal includes:

- Home – Get an at-a-glance view of the overall security health of your organization.
- Incidents & alerts - See the broader story of an attack by connecting the dots seen on individual alerts on entities. You'll know exactly where an attack started, what devices are impacted, who was affected, and where the threat has gone.
- Action center - Reduce the volume of alerts your security team must address manually, allowing your security operations team to focus on more sophisticated threats and other high-value initiatives.

² <https://security.microsoft.com/?azure-portal=true>

- Threat analytics – Get the detail and information you need to better protect your users, devices, apps, and more.
- Secure score – Improve your overall security posture with Microsoft Secure Score. This page provides an all-up summary of the different security features and capabilities you've enabled and includes recommendations for areas to improve.
- Hunting – Proactively search for malware, suspicious files, and activities in your Microsoft 365 organization.
- Policies & rules - Set up policies to manage devices, protect against threats, and receive alerts about various activities in your org.
- Permissions & roles - Manage who in your organization has access to view content and perform tasks in the Microsoft 365 Defender portal. You can also assign Microsoft 365 permissions in the Azure AD Portal.

The Microsoft 365 Defender portal is the central location to manage the integrated Microsoft security solutions. The current integrated solutions include Defender for Endpoint, Defender for Office 365, Defender for Identity, and Microsoft Cloud App Security. Each of these Defender products currently has their own portals. Even though the Microsoft Security center portal is the starting point, you will end up jumping to the related portals. Over time, the Defender-related portals will be unified with the Microsoft 365 Defender portal.

The **More resources** option provides a list and links to these related portals:

Portal	Description
Microsoft 365 compliance center	Manage your compliance needs across Microsoft 365 services using integrated solutions for information governance, classification, case management, and more.
Azure Active Directory	Manage your organization's identities. Set up multi-factor authentication, track user sign-ins, edit company branding, and more.
Azure AD Identity Protection	Detect potential vulnerabilities affecting your organization's identities. Investigate suspicious incidents related to your organization's identities and set up automated responses to resolve them.
Azure Advanced Threat Protection	Identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.
Azure Information Protection	Configure and manage the Azure Information Protection client and scanner to automatically classify and protect your organization's email and docs. Use reports to monitor label usage and identify sensitive info that should be protected.
Azure Security Center	Protect your data centers and get advanced threat protection for your Azure and non-Azure workloads in the cloud and on premises. Secure your Azure services fast with autoprovisioned, native protection.

Portal	Description
Microsoft 365 Device Management	Manage device access to your organization's most important data. Set up Intune enrollment, assign apps and policies, and monitor enrolled devices.
Microsoft Cloud App Security	Get visibility into your cloud apps using sophisticated analytics to identify and protect against cyberthreats, detect Shadow IT, and control how your data travels.
Office 365 security & compliance center	Manage security and compliance for all of your organization's data across Office 365. Import and archive content, prevent data leaks, protect against threats, and more.
Microsoft 365 Defender	Monitor and respond to security alerts on devices protected by next-generation protection, endpoint detection and response, and many other Microsoft Defender advanced threat protection capabilities.

Manage incidents

Microsoft 365 Defender provides a cross domain threat correlation and purpose-driven portal to investigate threats. Incidents are based on related alerts created when a malicious event or activity is seen on your network. Individual alerts provide valuable clues about an on-going attack. However, attacks typically employ various vectors and techniques to carry out a breach. Piecing individual clues together can be challenging and time-consuming.

An incident is a collection of correlated alerts that make up the story of an attack. Microsoft 365 Defender automatically aggregates malicious and suspicious events that are found in different device, user, and mailbox entities in the network. Grouping related alerts into an incident gives security defenders a comprehensive view of an attack.

For instance, security defenders can see where the attack started, what tactics were used, and how far the attack has gone into the network. They can also see the scope of the attack, like how many devices, users, and mailboxes were impacted, how severe the impact was, and other details about affected entities.

If enabled, Microsoft 365 Defender can automatically investigate and resolve the individual alerts through automation and artificial intelligence. Security defenders can also perform more remediation steps to resolve the attack straight from the incidents view.

Incidents from the last 30 days are shown in the incident queue. From here, security defenders can see which incidents should be prioritized based on risk level and other factors.

Security defenders can also rename incidents, assign them to individual analysts, classify, and add tags to incidents for a better and more customized incident management experience.

Prioritize incidents

Microsoft 365 Defender applies correlation analytics and aggregates all related alerts and investigations from different products into one incident. Microsoft 365 Defender also triggers unique alerts on activities that can only be identified as malicious given the end-to-end visibility that Microsoft 365 Defender has across the entire estate and suite of products. This view gives your security operations analyst the broader attack story, which helps them better understand and deal with complex threats across the organization.

The Incidents queue shows a collection of flagged incidents from across devices, users, and mailboxes. It helps you sort through incidents to prioritize and create an informed cybersecurity response decision.

Incident name	Severity	Categories	Active alerts	Impacted entities	Service sources	Custom tags	Last activity
File-less attack and reconnaissance	Medium	Execution, Defense evasion, D...	2/3	2 Machines	Microsoft Defender ATP, Azure ATP		11/14/19, 2:06 PM
incident #55	Medium	Execution	1/1	user-labeller@contoso.org	Microsoft Defender ATP		11/7/19, 12:58 PM
Spearphishing leads to exfiltration	High	Initial access, Execution, Cred...	26/28	polly.barden@...	Office ATP, Microsoft Defender ATP, Azure ATP, Microsoft...	SSBR_2011	11/1/19, 10:18 AM
Suspicious login activity	Medium	Suspicious activity	3/3	securitymanager	Microsoft Cloud App Security		10/28/19, 7:09 PM
incident #30	Medium	Suspicious activity	1/1	mike.barden	Microsoft Cloud App Security	mywatchlist	10/28/19, 5:13 PM
Impossible travel	Medium	Suspicious activity	1/1	mike.barden	Microsoft Cloud App Security		10/28/19, 9:40 AM

By default, the queue in the Microsoft 365 Defender portal displays incidents seen in the last 30 days. The most recent incident is at the top of the list so that you can see it first.

The incident queue exposes customizable columns that give you visibility into different characteristics of the incident or the contained entities. This helps you make an informed decision regarding the prioritization of incidents to handle.

For more clarity at a glance, automatic incident naming generates incident names based on alert attributes such as the number of endpoints affected, users affected, detection sources, or categories. This allows you to quickly understand the scope of the incident.

Available filters

Assigned to

You can choose to show alerts that are assigned to you or those handled by automation.

Categories

Choose categories to focus on specific tactics, techniques, or attack components seen.

Classification

Filter incidents based on the set classifications of the related alerts. The values include true alerts, false alerts, or not set.

Data sensitivity

Some attacks focus on targeting to exfiltrate sensitive or valuable data. By applying a filter to see if sensitive data is involved in the incident, you can quickly determine if sensitive information has potentially been compromised and prioritize addressing those incidents. Only applicable if Microsoft Information Protection is turned on.

Device group

Filter by defined device groups.

Investigation state

Filter incidents by the status of the automated investigation.

Multiple categories

You can choose to see only incidents that have mapped to multiple categories and can thus potentially cause more damage.

Multiple service sources

Filter to only see incidents that contain alerts from different sources (Microsoft Defender for Endpoint, Microsoft Cloud App Security, Microsoft Defender for Identity, Microsoft Defender for Office 365).

OS platform

Limit the incident queue view by operating system.

Service sources

By choosing a specific source, you can focus on incidents that contain at least one alert from that chosen source.

Severity

The severity of an incident is indicative of the impact it can have on your assets. The higher the severity, the bigger the impact and typically requires the most immediate attention.

Status

You can choose to limit the list of incidents shown based on their status to see which ones are active or resolved.

Preview incidents

The portal pages provide preview information for most list related data.

In this screenshot, the three highlighted areas are the circle, the greater than symbol, and the actual link.

The screenshot shows the Microsoft 365 Defender Incidents page. On the left, there's a navigation sidebar with options like Home, Incidents (which is selected and highlighted in blue), Action center, Reports, Secure score, Attack simulation training, Hunting, Classification, Policies, Permissions, Settings, More resources, and Customize navigation. The main area is titled 'Incidents' and displays a list of incidents. One incident is highlighted with a red box, showing its details: 'Incident name: Multi-stage incident involving Initial access & Persistence on one endpoint'. To the left of the incident name are two small circular icons, also highlighted with a red box. The rest of the page includes a toolbar with filters, sorting, and search options, and a footer with links for 'Need help?' and 'Give feedback'.

Circle

Selecting the circle will open a blade on the right side of the page with a preview of the line item with an option to open the full page of information.

The screenshot shows the Microsoft 365 Defender interface. On the left is a navigation sidebar with options like Home, Incidents (which is selected), Action center, Reports, Secure score, Attack simulation training, Hunting (with Advanced hunting and Custom detection rules), Classification (with Sensitivity labels, Retention labels, Sensitive info types, and Label analytics), Policies, Permissions, Settings, More resources, and Customize navigation. The main area is titled 'Incidents' and shows a list of incidents. One incident is selected, and its details are displayed in a large pane on the right. The details include:

- Multi-stage incident involving Initial access & Persistence on one endpoint**
- Status: Active
- Assigned to: Unassigned
- Severity: Medium
- Incident ID: 33
- Classification: (Not set) Set status and classification
- Categories: Initial access, Execution, Persistence
- Activity time: First - Nov 6, 2020, 12:23:39 PM, Last - Nov 6, 2020, 12:24:30 PM
- Impacted entities**: desktop-p7avz2p (Risk level: High, Exposure level: Medium)

Greater than symbol

If there are related records that can be displayed, selecting the greater than sign will display the records below the current record.

The screenshot shows the Microsoft 365 Defender interface, similar to the previous one but with more detailed incident data. The navigation sidebar is identical. The main area is titled 'Incidents' and shows a list of incidents. One incident is selected, and its details are displayed in a large pane on the right. The details are the same as in the previous screenshot. Below the main list, a series of related records are shown, each preceded by a greater than symbol (>). These records represent additional incidents or alerts related to the selected one. The interface includes standard navigation controls like back, forward, and search at the top, and pagination, column selection, and item per page settings at the bottom.

Link

The link will navigate you to the full page for the line item.

Managing incidents is critical in ensuring that threats are contained and addressed. In Microsoft 365 Defender, you have access to managing incidents on devices, users, and mailboxes. You can manage incidents by selecting an incident from the Incidents queue.

You can edit the name of an incident, resolve it, set its classification and determination. You can also assign the incident to yourself, add incident tags and comments.

In cases where you would like to move alerts from one incident to another while investigating, you can also do so from the Alerts tab, thus creating a larger or smaller incident that includes all relevant alerts.

Edit incident name

Incidents are automatically assigned a name based on alert attributes such as the number of endpoints affected, users affected, detection sources, or categories. This allows you to quickly understand the scope of the incident. You can modify the incident name to better align with your preferred naming convention.

Assign incidents

If an incident has not yet been assigned, you can select Assign to me to assign the incident to yourself. Doing so assumes ownership of not just the incident but also all the alerts associated with it.

Set status and classification

Incident status

You can categorize incidents (as Active, or Resolved) by changing their status as your investigation progresses. This helps you organize and manage how your team can respond to incidents.

For example, your SOC analyst can review the urgent Active incidents for the day and decide to assign them to herself for investigation.

Alternatively, your SOC analyst might set the incident as Resolved if the incident has been remediated. Resolving an incident will automatically close all open alerts that are part of the incident.

Classification and determination

You can choose not to set a classification or decide to specify whether an incident is true alert or false alert. Doing so helps the team see patterns and learn from them.

Add comments

You can add comments and view historical events about an incident to see previous changes made to it.

Whenever a change or comment is made to an alert, it is recorded in the Comments and history section.

Added comments instantly appear on the pane.

Add incident tags

You can add custom tags to an incident, for example, to flag a group of incidents with common characteristics. You can later filter the incidents queue for all incidents that contain a specific tag.

Investigate incidents

The incident page provides the following information and navigation links.

Incident overview

The overview page gives you a snapshot glance into the top things to notice about the incident.

The screenshot shows the Microsoft 365 Defender Incident Overview page. At the top, it displays 'Contoso Electronics' and 'Microsoft 365 Defender'. Below this, there are tabs for 'Overview', 'Alerts (38)', 'Machines (3)', 'Users (2)', 'Mailboxes (1)', 'Investigations (6)', and 'Evidence (57)'. The 'Alerts' tab is selected.

Alerts and categories:

- 36/30 active alerts
- 6 MITRE attack categories
- 2 other alert categories

Scope:

- 3 affected devices
- 2 affected users
- 1 affected mailbox

Top affected assets:

Entity type	Risk level/investigation priority	Tags
cont-pollyharre	High	
cont-mikehardin	High	High Value Asset
cont-dc1	No known risks	
adrian.bard	No data available	
mike.barden	No data available	Office 365 administrator
polly.harrel@mtv1.onmicrosoft.co...	No data available	

Evidence:

57 entities found

Evidence remediation status:

- Remediated
- Not Found
- Unremediated
- Other

Incident information:

- Tags summary: Incident tag - SSRP 2011
- Data sensitivity: Machine groups
- User groups: Office 365 administrator
- Incident details: Status - Active, Severity - High, First activity - Nov 1, 2019, 7:52:09 AM, Last activity - Nov 1, 2019, 10:18:49 AM, Classification - (Not set), Assigned to - Unassigned

The attack categories give you a visual and numeric view of how advanced the attack has progressed against the kill chain. As with other Microsoft security products, Microsoft 365 Defender is aligned to the MITRE ATT&CK™ framework.

The scope section gives you a list of top impacted assets that are part of this incident. If there is specific information regarding this asset, such as risk level, investigation priority, and any tagging on the assets, it will also surface in this section.

The alerts timeline provides a sneak peek into the chronological order in which the alerts occurred and the reasons that these alerts linked to this incident.

And last - the evidence section provides a summary of how many different artifacts were included in the incident and their remediation status, so you can immediately identify if any action is needed on your end.

This overview can help the initial triage of the incident by providing insight into the top characteristics of the incident that you should be aware of.

Alerts

You can view all the alerts related to the incident and other information about them such as severity, entities that were involved in the alert, the source of the alerts (Microsoft Defender for Identity, Microsoft Defender for Endpoint, Microsoft Defender for Office 365), and the reason they were linked together.

By default, the alerts are ordered chronologically to allow you to first view how the attack played out over time. Clicking on each alert will lead you to the **relevant alert page**, where you can conduct an in-depth investigation of that alert.

Users

See users that have been identified to be part of or related to a given incident.

Clicking the username navigates you to the **user's Cloud App Security page**, where further investigation can be conducted.

Mailboxes

Investigate mailboxes that have been identified to be part of or related to an incident. To do further investigative work, selecting the mail-related alert will open **Microsoft Defender for Office 365**, where you can take remediation actions.

Investigations

Select Investigations to see all the automated investigations triggered by alerts in this incident. The investigations will perform remediation actions or wait for analyst approval of actions, depending on how you configured your automated investigations to run in **Microsoft Defender for Endpoint and Defender for Office 365**.

Select an investigation to navigate to its Investigation details page to get full information on the investigation and remediation status. If any actions are pending for approval as part of the investigation, they will appear in the Pending actions tab.

Evidence

Microsoft 365 Defender automatically investigates all the incidents' supported events and suspicious entities in the alerts, providing you with autoreponse and information about the important files, processes, services, emails, and more. This helps quickly detect and block potential threats in the incident.

Each of the analyzed entities will be marked with a verdict (Malicious, Suspicious, Clean) and a remediation status. This helps you understand the remediation status of the entire incident and the next steps to further remediate.

Protect your identities with Azure AD Identity Protection

Lesson Introduction

Azure Active Directory (Azure AD) Identity Protection gives you advanced detection and remediation of identity-based risks to protect your Azure AD identities and applications.

You work for a retail organization that has its identities stored in Azure AD. There have been several recent incidents where identities were compromised. It's possible that sensitive customer information was exposed. You'd like to use Azure native services to protect your company from any future incidents. You've decided to use Identity Protection to protect your identity infrastructure.

In this module, you'll explore what Identity Protection is, and how to use it. You'll detect risks by using risk policies. Then, you'll investigate detected risks, and remediate them.

By the end of this module, you'll know how to protect your organization's identities from identity-based risks by using Identity Protection.

Learning objectives

After completing this lesson, you should be able to:

- Describe the features of Azure AD Identity Protection.
- Describe the investigation and remediation features of Azure AD Identity Protection.

Azure AD Identity Protection explained

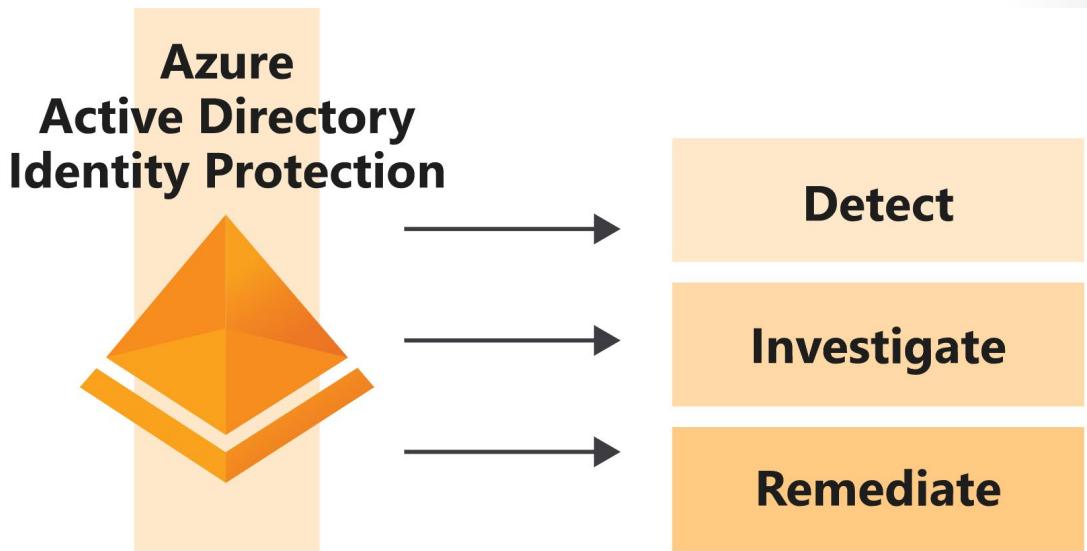
Azure Active Directory (Azure AD) Identity Protection helps you to automatically detect, remediate, and investigate identity-based risks for your organization.

The retail company you work for is conscious about its reputation. Compromised identities have previously enabled malicious users to obtain customer information fraudulently. These attacks have affected your organization's reputation, and ultimately its profitability. Your manager has asked you to investigate Identity Protection as a solution. You've been asked to report back on what the service does and how it's used.

In this unit, you'll learn what Identity Protection is, and the risks involved in using it. You'll explore the different workflows you can use in Identity Protection to protect your identities.

What is Azure Active Directory Identity Protection?

Identity Protection is a solution built into Azure AD that's designed to protect your identities through a three-part process.



Your company's specialist expertise is in retail, not in identity protection. It wants to continue to focus on its areas of strength, but still ensure that it's protected against identity risks. Your organization can use Identity Protection to automate the detection, investigation, and remediation of risks related to users' identities without hiring expensive security experts.

What are risks?

Risks can be described as suspicious activity and actions by users when they sign in, or when they take actions after signing in. That's why risks are categorized in two ways: as user risks and sign-in risks.

User risk

A user risk is caused when a user's identity or account is compromised. User risks can include:

Risk	Description
Unusual behavior	The account showed unusual activity or the patterns of usage are similar to those patterns that Microsoft systems and experts have identified as attacks.
Leaked credentials	The user's credentials could have been leaked. For example, Microsoft might have found a list of leaked credentials on the dark web, which could affect your user accounts.

Sign-in risk

Here, Identity Protection scrutinizes each authentication request to judge whether it was authorized by the owner of the identity. Sign-in risks can include:

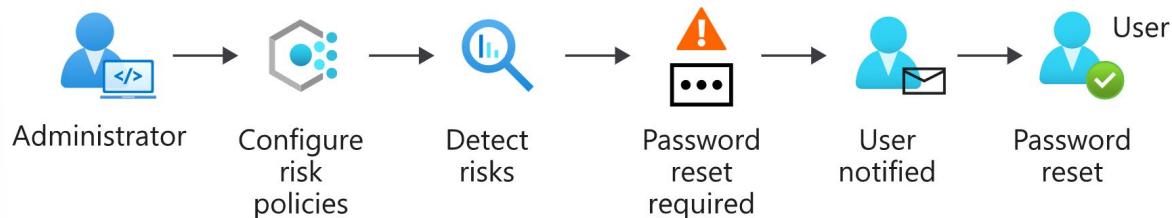
Risk	Description
Unfamiliar sign-in properties	Identity Protection remembers and learns a particular user's sign-in history. For example, when a sign-in occurs from a location that's unusual for the user, a risk detection is triggered.
Atypical travel	For example, when two or more sign-ins occur from distant locations in an unrealistically short time period, a risk detection is raised.
Malware-linked IP address	For example, if the IP address where the sign-in originates is known to have been in contact with an active bot server, a risk detection is raised.
Anonymous IP address	For example, a sign-in originates from an anonymous IP address. Because these details can be used by attackers to hide their real IP address or location, a risk detection is raised.

Azure Active Directory Identity Protection workflow

There are two different ways to detect and handle identity risks: self-remediation workflow and administrator remediation workflow.

- **Self-remediation workflow**

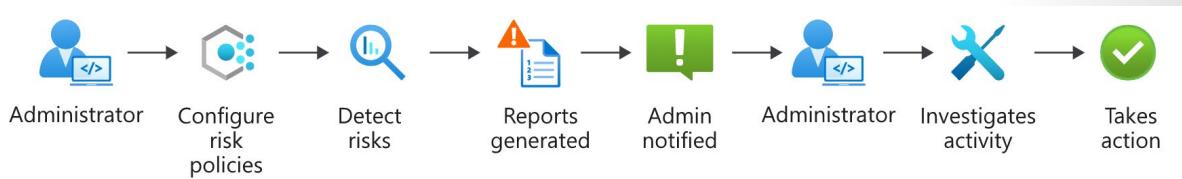
Identity Protection uses risk policies to automatically respond to detected threats for you. You configure a risk policy to decide how you want Identity Protection to respond to a particular type of risk. You then choose the action the user is asked to complete. The action could be a self-service password reset or multifactor authentication enforcement. Using policies in this way helps save time and gives you peace of mind.



In this workflow, the administrator first configures the risk policies that then monitor for identity risks. When a risk is detected, the policies enforce measures to remediate it. A policy might, for example, prompt a user to reset their password in response to a risk detected. The user then resets their password, and the risk is remediated.

- **Administrator remediation workflow**

You can also have admins decide how a risk should be remediated when it's been detected by your risk policies. This type of remediation workflow helps you make more tailored decisions. The admin understands the context in which the risks were detected.



In this workflow, the admin configures risk policies. The policies then monitor for identity risks. The admin is notified of risks in a report. The admin views the detailed report and takes appropriate action to remediate the risks. For example, the admin might decide a sign-in is safe, and accept the risk.

Detect risks with Azure AD Identity Protection policies

Risk policies make it possible for your organization to respond more appropriately to identity risk.

Previously, your retail company's IT team didn't have security skills in-house and had to hire external contractors to protect identities. Your manager wants to avoid the same situation going forward. Your company needs to be able to respond to threats in a controlled and more cost-effective manner, without weakening security.

You've been asked to investigate how identity risks are detected in Azure AD Identity Protection. You've been asked to look into risk policies and how to use them.

In this unit, you'll investigate what risk policies are. You'll also learn what each type of risk policy is used for, and how to configure and enable them. Then, you'll see what the user experience is like for each risk policy type.

What is a risk policy?

You configure a risk policy to decide how you want Identity Protection to respond to a particular type of risk. Do you want to block or allow access? Do you want to make users go through additional authentication before you allow access? Risk policies help you respond to risks rapidly. Your company can leverage risk policies, and avoid hiring external contractors to handle identity-based risks.

Different risk policies are available based on the type of identity risk. You can use a sign-in risk policy or a user risk policy.

Sign-in risk policy

A sign-in risk policy scrutinizes every sign-in, and gives it a risk score. This score indicates the probability that the sign-in was attempted by the person whose credentials are used. You decide which level of risk is acceptable by choosing a threshold of low, medium, or high. Based on the risk level, you choose whether to allow access, automatically block, or allow access only after additional requirements are met. For example, users might be asked to go through multifactor authentication to remediate detected risks that are considered to be at the medium level. Users could be blocked entirely if the risk is considered high.

You use a form to configure a sign-in risk policy in the Azure portal. You specify settings such as:

- The users this policy should target.
- The conditions that must be met, such as how high a score triggers the policy.
- How you want to respond.

Make sure users are already registered for Azure AD Multi-Factor Authentication before you apply this policy.

The screenshot shows the configuration of a 'Sign-in risk remediation policy'. It includes sections for 'Assignments' (targeting 'All users'), 'Controls' (requiring 'Require multi-factor authentication'), 'Review' (monitoring 'Number of sign-ins impacted'), and an 'Enforce Policy' toggle switch set to 'On'.

Policy name
Sign-in risk remediation policy

Assignments

- Users > All users
- Conditions > Sign-in risk

Controls

- Access > Require multi-factor authentication

Review

- Estimated impact > Number of sign-ins impacted

Enforce Policy

On Off

After a sign-in risk is identified, the user is asked to take action to remediate the risk. They're told what triggered the risk, and what they need to provide to resolve the issue. For example, the user might see this notification.

The notification from Office 365 informs the user about a detected sign-in risk, asking them to verify their identity. It includes a 'Next' button.

Office 365

Help us protect your account

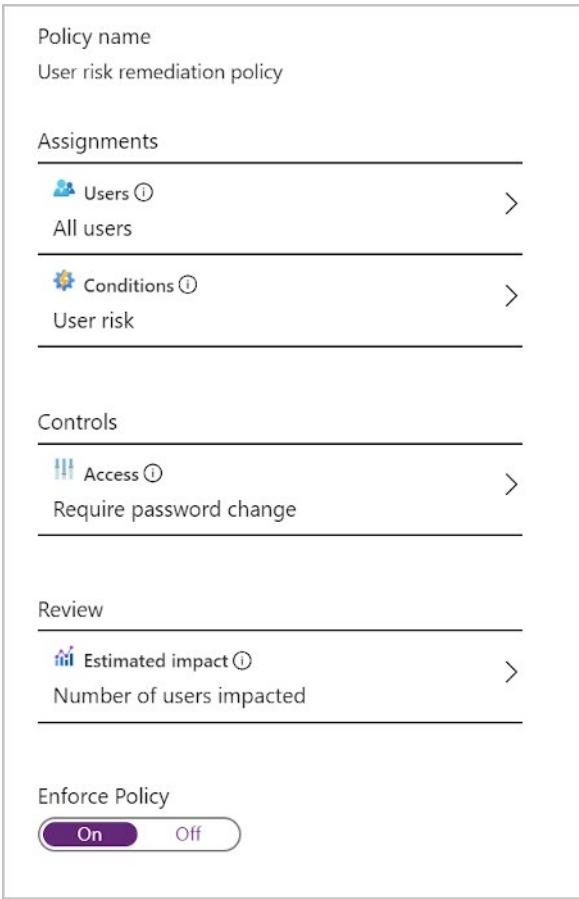
We've detected something unusual about this sign-in. For example, you might be signing in from a new location, device, or app. Before you can continue, we need to verify your identity.

Next

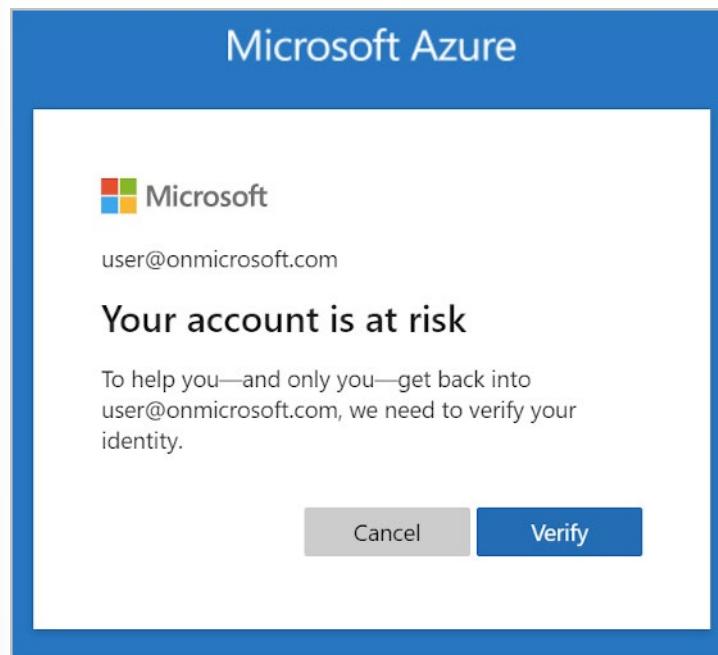
User risk policy

Here, Identity Protection learns the user's normal behavioral patterns. Identity Protection then uses this knowledge to calculate the likely risk that the user's identity was compromised. Based on this risk, the admin can decide whether to allow access, block it, or allow access only after additional requirements are met. The user could, for example, be asked to change their password by using self-service password reset before they're allowed access.

You use a form to configure a user risk policy in the Azure portal. You specify settings such as the users this policy should target, the conditions that must be met, and how you'll respond. Make sure users are already registered for self-service password reset before you apply this policy.



After a user risk is identified, the user is asked to take action to remediate that risk. They're told what triggered the risk, and what they need to provide to resolve the issue. For example, the user might see this notification.

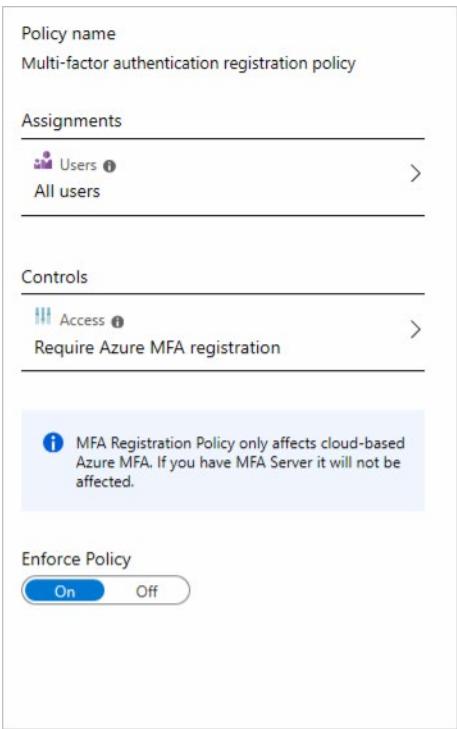


Multifactor authentication (MFA) registration policy

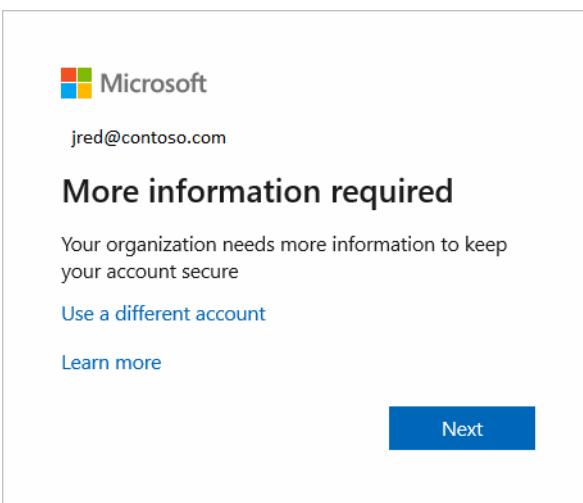
Multifactor authentication (MFA) adds a second layer of protection to your users' identities. With multi-factor authentication, the user has to go through an additional verification step after they successfully provide their username and password.

You can use an MFA registration policy to make sure all users are registered for MFA from the first time they use their account. You also configure this policy so you can enforce sign-in risk policies. This way, you let users self-remediate after a sign-in risk is detected.

You fill in a form to configure an MFA registration policy by using the Azure portal. You'll need to provide details about which users the policy targets, and whether it should be enabled or disabled.



After you configure an MFA registration policy, the user is asked to register when they sign in. The user sees this notification.



Users must complete the registration within 14 days, but they can choose to skip signing in during that period. After 14 days, they'll have to complete registration before they're allowed to sign in again.

Remediate risks detected by Azure AD Identity Protection

Investigations help you understand how you can improve your identity security posture, make it possible for you to respond to risks better, and help you avoid risks in the future.

In your retail company, you've configured Azure AD Identity Protection policies, and risks are being detected. Your manager has asked you to investigate and remediate all the risks detected, and share a report with the project manager. The team will use it to understand the company's identity-based risks better.

In this unit, you'll learn how to investigate risks by using reports. You'll see how to remediate different types of risks, and deal with any user accounts that might be blocked.

Investigate risks

Identity Protection provides reports you can use to investigate identity-based risks detected for your organization's users. These reports come in different types. Each kind of report gives the admin information about certain risks. The admin can then take specific actions to address those risks.

Report	Information included	Actions the admin can take	Period covered
Risky sign-ins	Location details, device details, sign-ins confirmed as safe, or with dismissed or remediated risks.	Confirm that sign-ins are safe or confirm that they're compromised.	Last 30 days
Risky users	Lists of users at risk, and users with dismissed or remediated risks. User history of risky sign-ins.	Reset user passwords, dismiss user risk, block user sign-ins, and confirm user accounts as compromised.	Not applicable

You use these reports to investigate risks detected by Identity Protection. The reports help you understand how to better prevent risks and improve your security stance for identities.

You can also access *risk detection type reports*, which combine information about risky user detections and sign-in detections. Use these reports to see how different risk types are related and take appropriate action.

You can view and download all reports from the Azure portal.

The screenshot shows the 'Risky sign-ins' blade in the Microsoft Azure portal. The table lists several risk events for user 'Alain Charon'. One event is highlighted in blue, showing details such as Request ID (29e08ac8-xxxx-xxxx-xxxx-4a65c26ab00), Correlation ID (44f76a8-xxxx-xxxx-xxxx-41bea9d5be5d), User (Alain Charon), Username (alain.charon@contoso.com), User ID (bab8ae07-xxxx-xxxx-xxxx-49c3f6880f05e), Application (Microsoft Office 365 Portal), Application ID (00000000-0000-0000-0000-000000000000), Resource (Windows Azure Active Directory), and Resource ID (00000002-0000-0000-0000-000000000000). The status for this event is 'Interrupted'.

Remediate risks

When your investigation is complete, you'll want to remediate the risks if you're not already using risk policies to automatically deal with them. Always address detected risks quickly.

There are different ways to remediate risks. The methods you use depend on your organization's needs.

Remediation method	Description
Self-remediation	If you configure risk policies, you can let users self-remediate. When Identity Protection has detected a risk, users either reset their password or go through multifactor authentication to unblock themselves. After self-remediation, these detected risks are considered closed. In your risk policies, the lower the acceptable risk level that triggers the policy, the more users will be affected. In general, we recommend that you set the threshold for user risk policies at <i>high</i> , and set sign-in risk policies to <i>medium and above</i> .
Reset passwords manually	For some organizations, automated password reset might not be an option. In this case, the admin can manually enforce password resets. For example, the admin can generate a temporary password and advise the user. The user can then change their password.

Remediation method	Description
Dismiss user risk detections	Sometimes, password reset isn't possible. For example, perhaps the affected user account was deleted. In this case, you can dismiss the risk detections for this user. If you choose to dismiss user risk detections, all associated risk detections for the user are closed.
Close individual detections	All detected risks contribute to an overall risk score for a user. This risk score represents the probability that a user account is compromised. The admin can also choose to close individual risk detections, and lower the overall risk of a user's account. For example, the admin can determine from a user that a particular risk detection is no longer needed and dismiss it. The overall risk that a user account was compromised is lowered.

Unblock users

User accounts can be blocked by risk policies or manually by the admin after an investigation. How these user accounts are unblocked depends on the type of risk that caused the blockage:

- **Accounts blocked because of sign-in risk**

An account blocked because of sign-in risk can be unblocked by excluding the user from the policy. The account might be unblocked if the admin asks the user to sign in from a familiar location or device. Sometimes, sign-ins are blocked from unfamiliar locations or devices. There might be an alert for suspicious behavior based on what's known about the user account's sign-in patterns. The policy can also be disabled if the admin found issues with it.

- **Accounts blocked because of user risk**

An account might be blocked if the user was flagged because of possible risky behavior. The admin can reset the password for the user to unblock the account. To remove the block, the admin might dismiss the activity identified as risky or exclude the user from the policy. If the policy is causing problems for many users, the admin can completely disable the policy.

Remediate risks with Microsoft Defender for Office 365

Lesson Introduction

Learn about the Microsoft Defender for Office 365 component of Microsoft 365 Defender.

Learning objectives

After completing this lesson, you should be able to:

- Define the capabilities of Microsoft Defender for Endpoint.
- Understand how to simulate attacks within your network.
- Explain how Microsoft Defender for Endpoint can remediate risks in your environment.

Microsoft Defender for Office 365 explained

Microsoft Defender for Office 365 is a cloud-based email filtering service that helps protect your organization against unknown malware and viruses by providing robust zero-day protection. It includes features to safeguard your organization from harmful links in real time. Microsoft Defender for Office 365 has rich reporting and URL trace capabilities that give administrators insight into the kind of attacks happening in your organization.

Microsoft Defender for Office 365 provides the following benefits:

- **Industry-leading Protection.** Microsoft Defender for Office 365 leverages 6.5 trillion signals daily from email alone to quickly and accurately detect threats and protect users against sophisticated attacks such as phishing and zero-day malware. Microsoft Defender for Office 365 blocked 5 billion phish emails and analyzed 300k phish campaigns in 2018 protecting 4 million unique users from advanced threats.
- **Actionable Insights.** Actionable insights are presented to security administrators by correlating signals from a broad range of data to help identify, prioritize, and provide recommendations on how to address potential problems. The recommendations include remediation actions empowering administrators to proactively secure their organization.
- **Automated response.** Investigation and remediation in post-breach scenarios can be difficult, expensive, and time-consuming. Most organizations lack the expertise and resources needed for rapid investigation and effective remediation. Microsoft Defender for Office 365 provides advanced automated response options that security operators can leverage saving a significant amount of time, money, and resources.
- **Training & awareness.** Social engineering attacks such as phishing often look legitimate and are hard to spot for busy users. It's critical to train end users to make the right decisions in the event of an attack. In-product notifications help users understand the risks of performing an action such as clicking on a suspicious link. Features such as attack simulator help administrators launch realistic threat simulations to train users to be more aware and vigilant. User reporting capabilities empower users to notify Microsoft of suspicious content.

The following are the primary ways you can use Microsoft Defender for Office 365 for message protection:

- In an Microsoft Defender for Office 365 filtering-only scenario, Microsoft Defender for Office 365 provides cloud-based email protection for your on-premises Exchange Server environment or any other on-premises SMTP email solution.
- Microsoft Defender for Office 365 can be enabled to protect Exchange Online cloud-hosted mailboxes.
- In a hybrid deployment, Microsoft Defender for Office 365 can be configured to protect your messaging environment and control mail routing when you have a mix of on-premises and cloud mailboxes with Exchange Online Protection for inbound email filtering.

Automate, investigate, and remediate

When you are investigating a potential cyberattack, time is of the essence. The sooner you identify and mitigate threats, the better off your organization will be. Automated investigation and response (AIR) capabilities include a set of security playbooks that can be launched automatically, such as when an alert is triggered, or manually, such as from a view in Explorer. AIR can save your security operations team time and effort in mitigating threats effectively and efficiently.

At a high level, the AIR flow works like this:

Phase	What's involved
1	An alert that is triggered, and a security playbook initiates.
2	Depending on the particular alert and security playbook, automated investigation begins immediately . (Alternately, a security analyst can start an automated investigation manually , from a value in a report such as Explorer .)
3	While an automated investigation runs, its scope can increase as new, related alerts are triggered.
4	During and after an automated investigation, details and results are available to view. Results include recommended actions that can be taken to respond and remediate any threats that were found. In addition, a playbook log is available that tracks all investigation activity. If your organization is using a custom reporting solution or a third-party solution, you can use the Office 365 Management Activity API to view information about automated investigations and threats.
5	Your security operations team reviews the results and recommendations, and approves remediation actions. In Office 365, remediation actions are taken only upon approval by your organization's security team.

Let's start with a native alert generated by Office 365. These alerts are typically investigated manually today – this is where AIR comes in. Attackers frequently send through benign URLs in emails to bypass notice from security solutions, then they weaponize them after delivery to activate their attack. Notice in the following screenshot that the alert identifies that a URL that was recently weaponized was detected by Microsoft Defender for Office 365 through Safe Links URL detonation (under **Details** on the right-hand side).

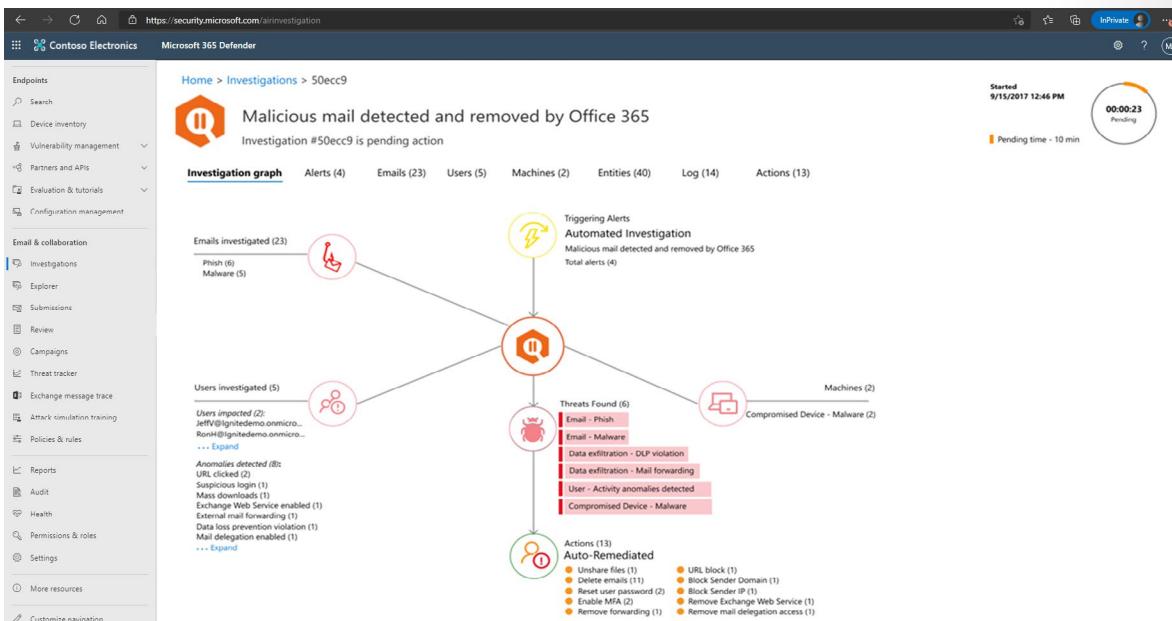
The screenshot shows the Microsoft Defender for Office 365 interface. On the left, a 'View Alerts' page lists various security incidents with columns for Severity (High, Low, Medium), Alert Name, Status (Resolved, Active), and Category (Threat Manage, Threat Monitor, Data Loss Prev, Data Governor, Permissions, Threat Manage, Mail flow). A specific alert is selected: 'Malicious mail removed by Office 365'. The right pane provides detailed information about this alert, including:

- Severity:** High
- Time:** Sep 19, 2018 1:29:49 PM
- Threat type:** Phish
- Hit count:** 1
- Details:** Office 365 has detected and removed emails with malicious URLs that were previously delivered to users.
- User(s) impacted:** JeffV@igniteddemo.onmicrosoft.com, RonH@igniteddemo.onmicrosoft.com
- Investigation:** #50ecc9
- Status:** Resolved
- Last updated by:** Office 365 Threat Intel
- Comments:** Auto-resolved by Office 365 Threat Intelligence
- Alert policy:** Office 365 Phish ZAP alert

Buttons at the bottom include 'View messages in Explorer' and 'Close'.

Microsoft Defender for Office 365 triggered an AIR playbook based on this alert and resolved the alert given the auto investigation having completed.

Clicking into the investigation deep link from the alert brings us into the Office 365 Threat Intelligence Summary Investigation Graph. This graph shows all the different entities – emails, users (and their activities), and devices that have been automatically investigated as part of the triggered alert.



Specifically, note that:

- Several emails (23) that were identified as being relevant to this investigation (based on sender, IP, domain, URL and other email attributes) and a subset of them (6) were identified as being malicious, sent from an internal user in the organization which itself is a strong indicator of a compromised user.

- A user pivot on this investigation also identifies anomalies for 1 user (Jeff) with respect to a suspicious login and mass downloads of documents.
- With the compromised user, user anomalies and compromised device threats identified in this investigation, Microsoft Defender for Office 365 has also taken some auto remediations such as blocking the URL, deleting any emails in mailboxes related to this URL, and triggering the AAD workflows for password reset and MFA for the compromised user. The ability to take automatic action or drive remediations with manual approval, based on policy, are core elements of AIR.

AIR in Microsoft Defender for Office 365 includes certain remediation actions. Whenever an automated investigation is running or has completed, you'll typically see one or more remediation actions that require approval by your security operations team to proceed. Such remediation actions include the following:

- Soft delete email messages or clusters
- Block URL (time-of-click)
- Turn off external mail forwarding
- Turn off delegation

These actions can be found in the **Actions** tab under the selected investigation, as shown in the following screenshot:

The screenshot shows the 'Actions' tab of an investigation titled 'Email investigation for 'URGENT: Please review and appro...'' with ID 'Investigation #bd4c2e is Pending Action'. The tab displays a list of recommended actions:

Action	Entity type	Entity value	Description	Threats	Status	Execution time
<input checked="" type="checkbox"/> Soft delete emails	Email clusters	{(IP2SenderDomainHost...}	For malicious emails, y...	Malware, Phish	Pending approval	2/16/19 4:53 PM
<input checked="" type="checkbox"/> Soft delete emails	Email clusters	{(SenderIp:104.47.53.1...}	For malicious emails, y...	Phish	Pending approval	2/16/19 4:53 PM
<input type="checkbox"/> Soft delete emails	Email clusters	{(Subject:'URGENT: Pl...}	For malicious emails, y...	Phish	Pending approval	2/16/19 4:53 PM
<input type="checkbox"/> Soft delete emails	Email clusters	{(Subject:'URGENT: Pl...}	For malicious emails, y...	Phish	Pending approval	2/16/19 4:53 PM

Annotations with callouts explain various parts of the interface:

- 'With the appropriate permissions, Actions can be submitted directly for remediation.' points to the 'Approve' button.
- 'The Action status, such as, Pending Approval, Approved et al.' points to the 'Status' column.
- 'Actions the investigation play book is recommending.' points to the first two rows in the table.
- 'The entity values that were used to determine the recommended Action.' points to the 'Entity value' column.
- A green circle highlights the 'Pending Action' status in the top right corner.

Guided Demonstration - Defender for Office 365

A guided demonstration is a recorded click-through simulation. You do not use your lab tenant for this demonstration. Instead simply click the link [here³](#) to launch this demonstration. A focus will appear in the demonstration showing you the next place to click to advance the demonstration.

In this experience you will do the following:

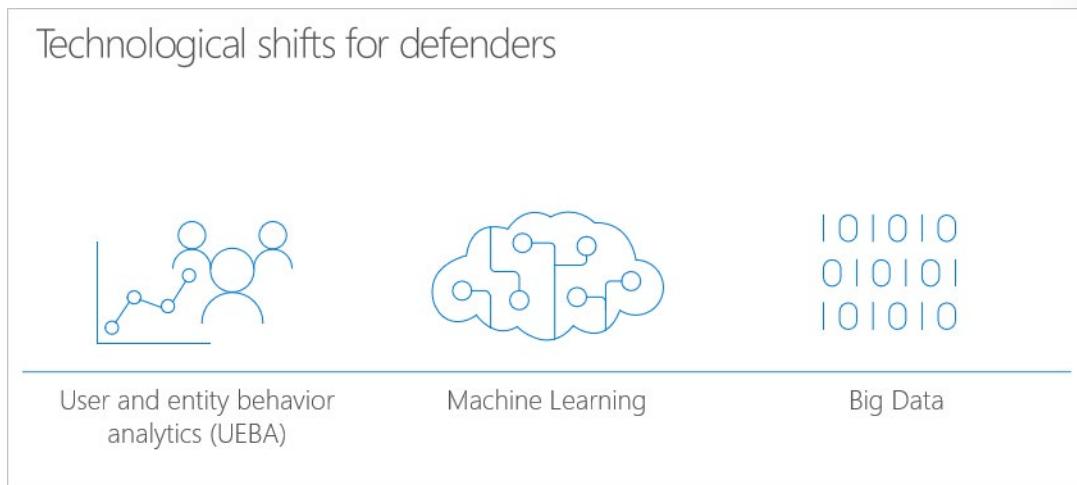
1. Configure policies.

³ <https://aka.ms/MSDO-IG>

2. Analyze threats.
3. Respond to attacks.

Time required: 28 minutes

Simulate attacks

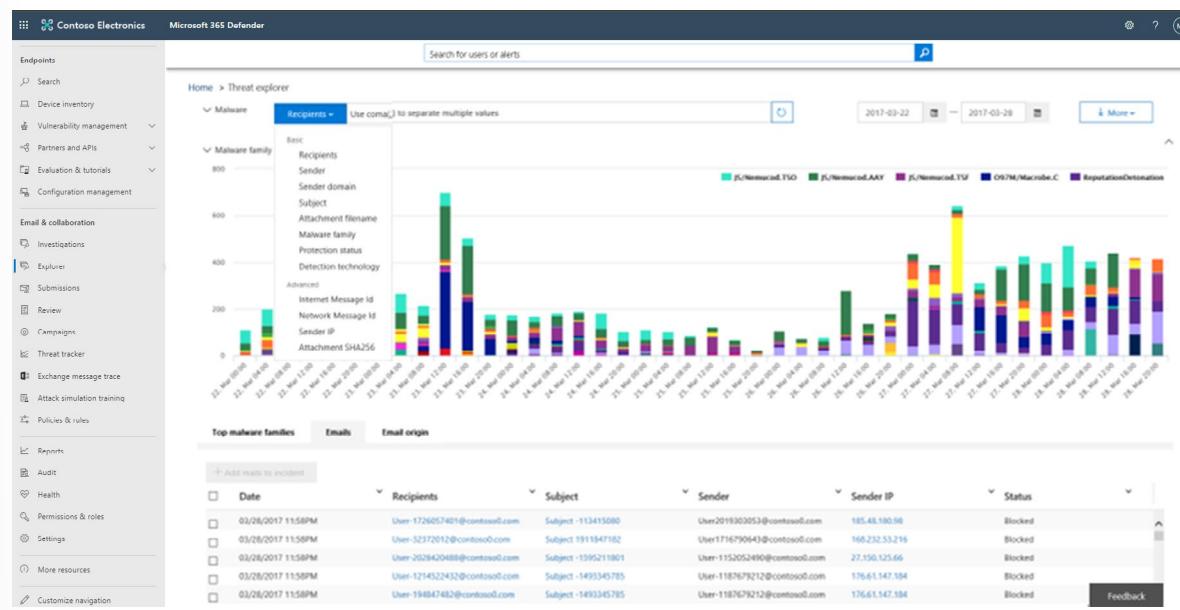


Microsoft Defender for Office 365 includes best-of-class threat investigation and response tools that enable your organization's security team to anticipate, understand, and prevent malicious attacks.

- **Threat trackers** provide the latest intelligence on prevailing cybersecurity issues. For example, you can view information about the latest malware, and take countermeasures before it becomes an actual threat to your organization. Available trackers include Noteworthy trackers, Trending trackers, Tracked queries, and Saved queries.
- **Threat Explorer** (or real-time detections) (also referred to as Explorer) is a real-time report that allows you to identify and analyze recent threats. You can configure Explorer to show data for custom periods.
- **Attack Simulator** allows you to run realistic attack scenarios in your organization to identify vulnerabilities. Simulations of current types of attacks are available, including spear phishing, credential harvest and attachment attacks, and password spray and brute force password attacks.

Threat Explorer enables you to begin delving into granular data for your organization. Inside Threat Explorer, you are first shown the variety of threat families impacting our organization over time. Additionally, you are shown the top threats and top targeted users inside the organization.

You can also change the category for the graph. In this case, the malware family is shown, but you can filter the Threat Explorer graph through several options including sender email, recipient email, and even the detection technology used to stop a threat. The detection technology piece highlights the issue if an email was blocked by Microsoft Defender's sandboxing or through an EOP filter. The graph adjusts to reflect the category being examined.



Threat Explorer allows a deeper look into a threat, beginning with a thorough description of this malware family's behavior. Threat Explorer provides a definition of the threat, the message traces of emails delivering the threat, technical details of the threat, global details of the threat, and advanced analysis.

On the **Users** tab, you can see each instance that a user in the organization was sent an attachment containing the Nemucod malware threat. You can not only see the specific recipients and subject, but the sender domain and the sender IP as well. The **Status** column tells you if the email was caught and blocked before it ever reached the user, or if it was delivered as spam.

If a user had actually received and opened the email, that would also appear under **Status**, enabling you to reach out to the user and take the appropriate remediation steps, such as scanning their device.

Safeguard your environment with Microsoft Defender for Identity

Lesson Introduction

Learn about the Microsoft Defender for Identity component of Microsoft 365 Defender.

Learning objectives

After completing this lesson, you should be able to:

- Define the capabilities of Microsoft Defender for Identity.
- Describe how to configure Microsoft Defender for Identity sensors.
- Explain how Microsoft Defender for Identity can remediate risks in your environment.

Microsoft Defender for Identity explained

Microsoft Defender for Identity is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

Microsoft Defender for Identity provides the following benefits:

- Monitor users, entity behavior, and activities with learning-based analytics
- Protect user identities and credentials stored in Active Directory
- Identify and investigate suspicious user activities and advanced attacks throughout the kill chain
- Provide clear incident information on a simple timeline for fast triage

Monitor and profile user behavior and activities

Microsoft Defender for Identity monitors and analyzes user activities and information across your network, such as permissions and group membership. It then creates a behavioral baseline for each user. Microsoft Defender for Identity then identifies anomalies with adaptive built-in intelligence, giving you insights into suspicious activities and events, revealing the advanced threats, compromised users, and insider threats facing your organization. Microsoft Defender for Identity's proprietary sensors monitor organizational domain controllers, providing a comprehensive view for all user activities from every device.

The screenshot shows a log entry in the Microsoft Defender for Identity interface. The entry details the addition of a user named 'InsertedUser' to the 'Administrators' group. Key fields include:

Field	Value
Description	Add: user InsertedUser to group Administrators
Type	Add > Add
Type (in app)	Group Membership changed
Source	App Connector
ID	/1a079ee-00b4-48dc-9/b1-116f361b16aa_105846196_158...
Matched policies	—
Investigation priority	—
User	—
User organizational unit	—
User groups	—
Activity objects	Count: 3. <i>Administrators, InsertedUser</i>
Date	Mar 30, 2020, 6:53 PM
Device type	—
User agent tags	—
App	Active Directory
Location	—
IP address	—
IP category	—
Tags	—
ISP	—

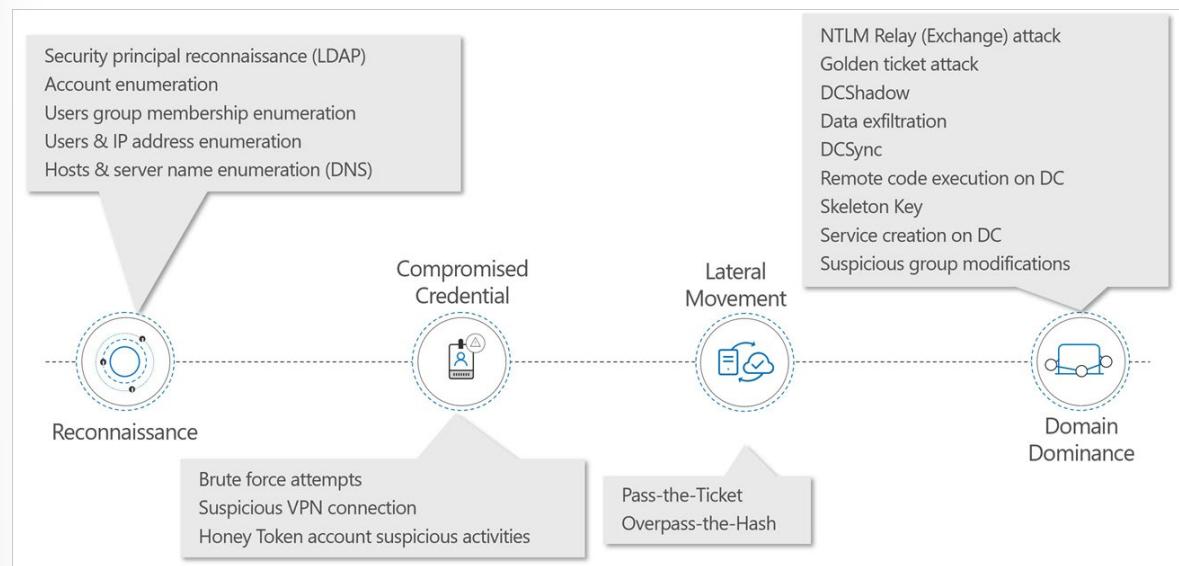
Protect user identities and reduce the attack surface

Microsoft Defender for Identity provides you invaluable insights on identity configurations and suggested security best-practices. Through security reports and user profile analytics, Microsoft Defender for Identity helps dramatically reduce your organizational attack surface, making it harder to compromise user credentials and advance an attack. Microsoft Defender for Identity's visual Lateral Movement Paths help you quickly understand exactly how an attacker can move laterally inside your organization to compromise sensitive accounts and assists in preventing those risks in advance. Microsoft Defender for Identity security reports help you identify users and devices that authenticate using clear-text passwords and provide additional insights to improve your organizational security posture and policies.

Improvement action	Related entities	Security assessment report	Urgency	Resolution
Stop clear text credentials exposure	0	Entities exposing credentials in clear text	—	COMPLETED
Stop legacy protocols communication	0	Legacy protocols usage	—	COMPLETED
Stop weak cipher usage	0	Weak cipher usage	—	COMPLETED
Modify unsecure Kerberos delegations	0	Unsecure Kerberos delegation	—	COMPLETED
Disable Print spooler service on domain controllers	2	Domain controllers with Print Spooler service available	■■■ High	OPEN
Remove dormant entities from sensitive groups	0	Dormant entities in sensitive groups	—	COMPLETED
Install Azure ATP sensors on all Domain Controllers	0	Unmonitored domain controllers	—	COMPLETED

Identify suspicious activities and advanced attacks across the cyber-attack kill-chain

Typically, attacks are launched against any accessible entity, such as a low-privileged user, and then quickly move laterally until the attacker gains access to valuable assets – such as sensitive accounts, domain administrators, and highly sensitive data. Microsoft Defender for Identity has a large range of detections across the Kill-chain from **reconnaissance** through to **compromised credentials** to **lateral movements** and **domain dominance**.



For example, in the reconnaissance stage, LDAP reconnaissance is used by attackers to gain critical information about the domain environment. Information that helps attackers map the domain structure, as well as identify privileged accounts for use later. This detection is triggered based on computers performing suspicious LDAP enumeration queries or queries targeting sensitive groups.

Brute force attacks are a common way to compromise credentials. This is when an attacker attempts to authenticate with multiple passwords on different accounts until a correct password is found or by using one password in a large-scale password spray that works for at least one account. Once found, the attacker logs in using the authenticated account. Microsoft Defender for Identity can detect this when it notices multiple authentication failures occurring using Kerberos, NTLM, or use of a password spray.

The next stage is when attackers attempt to move laterally through your environment, using pass-the-ticket, for example. Pass-the-ticket is a lateral movement technique in which attackers steal a Kerberos ticket from one computer and use it to gain access to another computer by reusing the stolen ticket. In this detection, a Kerberos ticket is being used on two (or more) different computers.

Ultimately, attackers want to establish domain dominance. One method, for example is the DCShadow attack. This attack is designed to change directory objects using malicious replication. This attack can be performed from any machine by creating a rogue domain controller using a replication process. If this occurs, Microsoft Defender for Identity triggers an alert when a machine in the network tries to register as a rogue domain controller.

This is not the complete set of detections, but it shows the breadth of detections Microsoft Defender for Identity covers.

Guided Demonstration - Microsoft Defender for Identity

A guided demonstration is a recorded click-through simulation. You do not use your lab tenant for this demonstration. Instead simply click the link [here⁴](#) to launch this demonstration. A focus will appear in the demonstration showing you the next place to click to advance the demonstration.

In this experience you will do the following:

1. Identify attacks.
2. Investigate behavior.
3. Reduce vulnerabilities.

Time required: 30 minutes

Configure Microsoft Defender for Identity sensors

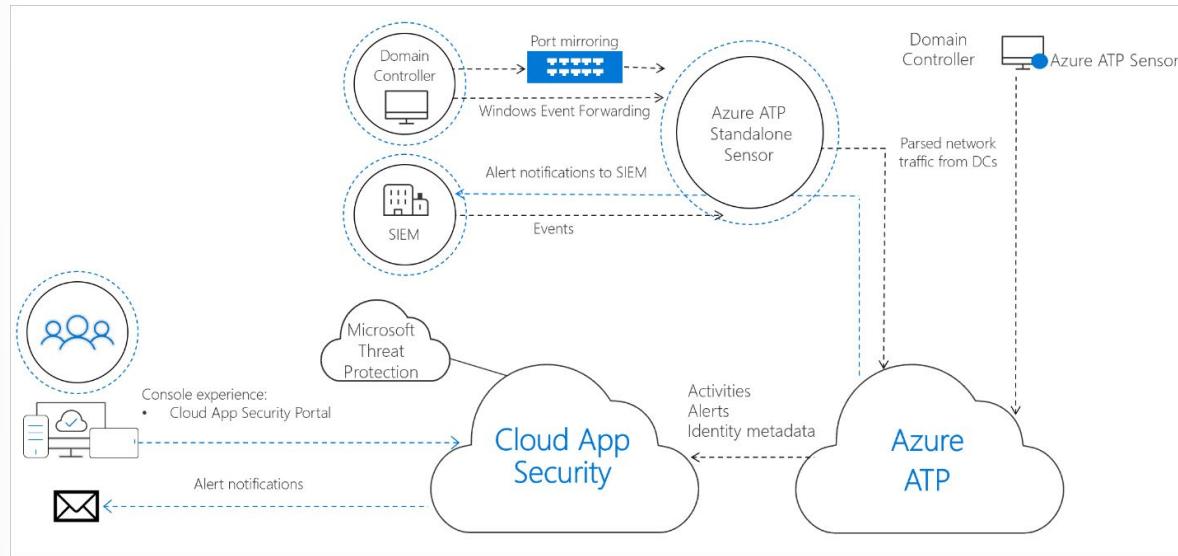
At a high level, the following steps are required to enable Microsoft Defender for Identity:

1. Create an instance on Microsoft Defender for Identity management portal.
2. Specify an on-premises AD service account in the Microsoft Defender for Identity portal.
3. Download and install the sensor package.
4. Install the Microsoft Defender for Identity sensor on all domain controllers.
5. Integrate your VPN solution (optional).

⁴ <https://aka.ms/MSDefenderforIdentity-IG>

6. Exclude the sensitive accounts you've listed during the design process.
7. Configure the required permissions for the sensor to make SAM-R calls.
8. Configure integration with Microsoft Cloud App Security.
9. Configure integration with Microsoft 365 Defender (optional).

The following diagram shows the Microsoft Defender for Identity architecture. In this unit, we will discuss how to configure the Microsoft Defender for Identity Sensor.



Installed directly on your domain controllers, the Microsoft Defender for Identity sensor accesses the event logs it requires directly from the domain controller. After the logs and network traffic are parsed by the sensor, Microsoft Defender for Identity sends only the parsed information to the Microsoft Defender for Identity cloud service (only a percentage of the logs are sent).

The Microsoft Defender for Identity sensor has the following core functionality:

- Capture and inspect domain controller network traffic (local traffic of the domain controller)
- Receive Windows events directly from the domain controllers
- Receive RADIUS accounting information from your VPN provider
- Retrieve data about users and computers from the Active Directory domain
- Perform resolution of network entities (users, groups, and computers)
- Transfer relevant data to the Microsoft Defender for Identity cloud service

The Microsoft Defender for Identity sensor has the following requirements:

- KB4487044 is installed on Server 2019. Microsoft Defender for Identity sensors already installed on 2019 servers without this update will be automatically stopped.
- The Microsoft Defender for Identity sensor supported domain controller OS list:
 - Windows Server 2008 R2 SP1 (not including Server Core)
 - Windows Server 2012
 - Windows Server 2012 R2
 - Windows Server 2016 (including Windows Server Core but not Windows Nano Server)

- Windows Server 2019 (including Windows Core but not Windows Nano Server)
- The domain controller can be a read-only domain controller (RODC).
- 10 GB of disk space is recommended. This includes space needed for the Microsoft Defender for Identity binaries, Microsoft Defender for Identity logs, and performance logs.
- The Microsoft Defender for Identity sensor requires a minimum of 2 cores and 6 GB of RAM installed on the domain controller.
- Power option of the Microsoft Defender for Identity sensor to high performance.
- Microsoft Defender for Identity sensors can be deployed on domain controllers of various loads and sizes, depending on the amount of network traffic to and from the domain controllers, and the amount of resources installed.
- When running as a virtual machine, dynamic memory or any other memory ballooning feature is not supported.

To install the Microsoft Defender for Identity sensor:

1. Download and extract the sensor file. Run **Microsoft Defender for Identity sensor setup.exe** and follow the setup wizard.
2. On the Welcome page, select your language and click **Next**.
3. The installation wizard automatically checks if the server is a domain controller or a dedicated server. If it's a domain controller, the Microsoft Defender for Identity sensor is installed. If it's a dedicated server, the Microsoft Defender for Identity standalone sensor is installed. For example, for an Microsoft Defender for Identity sensor, the following screen is displayed to let you know that an Microsoft Defender for Identity sensor is installed on your dedicated server:
4. Under **Configure the sensor**, enter the installation path and the access key, based on your environment:
 - **Installation path:** The location where the Microsoft Defender for Identity sensor is installed. By default, the path is **%programfiles%\Microsoft Defender for Identity sensor**. Leave the default value.
 - **Access key:** Retrieved from the Microsoft Defender for Identity portal.
5. Click **Install**.

After the Microsoft Defender for Identity sensor is installed, do the following to configure Microsoft Defender for Identity sensor settings:

1. Click **Launch** to open your browser and sign into the Microsoft Defender for Identity portal.
2. In the Microsoft Defender for Identity portal, go to **Configuration**. Under the System section, select **Sensors**.

The screenshot shows the 'Sensors' section of the Microsoft Defender for Identity interface. On the left, a sidebar lists various settings like System, Sensors, Updates, Data Sources, etc. The main area displays a table with one row for 'Contoso-DC'. The columns are NAME, TYPE, DOMAIN CONTROLLERS, VERSION, SERVICE STATUS, and HEALTH. The 'NAME' column shows 'Contoso-DC', 'TYPE' shows 'Sensor', 'DOMAIN CONTROLLERS' shows 'Contoso-DC.contoso.com', 'VERSION' shows '1.18.3944', 'SERVICE STATUS' shows 'Running', and 'HEALTH' is partially visible.

3. Click on the sensor you want to configure and enter the following information:

- **Description:** Enter a description for the Microsoft Defender for Identity sensor (optional).
- **Domain Controllers** (FQDN) (required for the Microsoft Defender for Identity standalone sensor, this can't be changed for the Microsoft Defender for Identity sensor): Enter the complete FQDN of your domain controller and click the **plus sign** to add it to the list. For example, dc01.contoso.com.

The following information applies to the servers you enter in the Domain Controllers list:

- All domain controllers whose traffic is being monitored via port mirroring by the Microsoft Defender for Identity standalone sensor must be listed in the Domain Controllers list. If a domain controller isn't listed in the Domain Controllers list, detection of suspicious activities might not function as expected.
- At least one domain controller in the list should be a global catalog. This enables Microsoft Defender for Identity to resolve computer and user objects in other domains in the forest.
- **Capture Network adapters** (required):
 - For Microsoft Defender for Identity sensors, all network adapters that are used for communication with other computers in your organization.
 - For Microsoft Defender for Identity standalone sensor on a dedicated server, select the network adapters that are configured as the destination mirror port. These network adapters receive the mirrored domain controller traffic.

This is a configuration dialog for the 'Contoso-DC' sensor. It has fields for 'Description' (empty), 'Domain Controller (FQDN)' set to 'Contoso-DC.contoso.com', and 'Capture network adapters' which includes two checked options: 'Ethernet' and 'Ethernet 2'. At the bottom are 'Save' and 'Cancel' buttons.

4. Click **Save**.

Microsoft Cloud App Security

Lesson Introduction

Microsoft Cloud App Security is a Cloud Access Security Broker (CASB) that operates on multiple clouds. It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your cloud services. Learn how to use Cloud App Security in your organization.

Learning objectives

After completing this lesson, you should be able to:

- Define the Cloud App Security framework
- Explain how Cloud Discovery helps you see what's going on in your organization
- Describe how to use Conditional Access App Control policies to control access to the apps in your organization

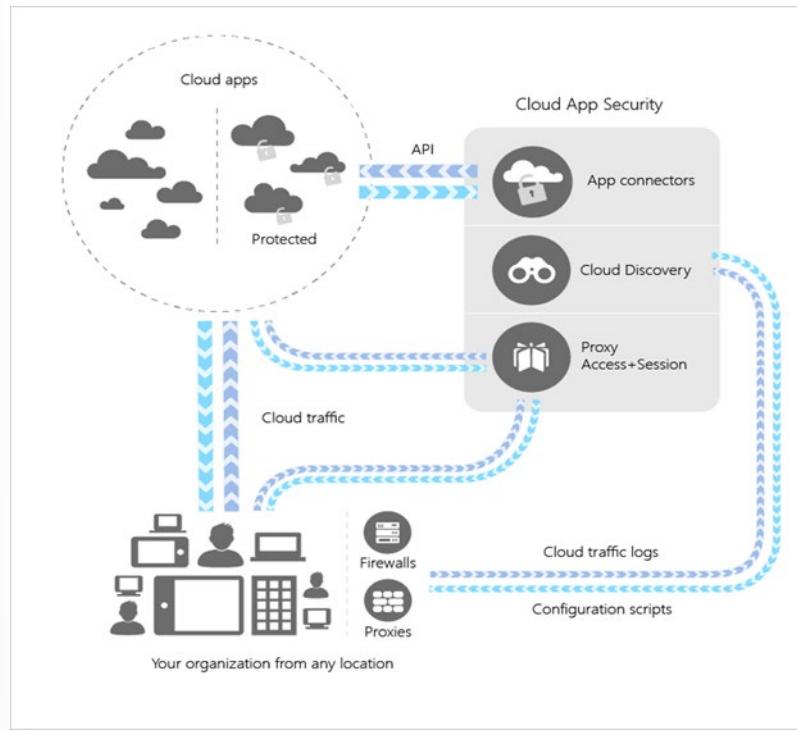
The Cloud App Security Framework

Cloud App Security Brokers (CASBs) are defined by Gartner as security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement.

In other words, CASBs are the intermediaries between your users and all of the cloud services they access. CASBs help you to apply monitoring and security controls over your users and data. CASBs for cloud services are like firewalls to corporate networks.

Microsoft Cloud App Security is a CASB that helps you identify and combat cyberthreats across Microsoft and third-party cloud services. Microsoft Cloud App Security integrates with Microsoft solutions, providing simple deployment, centralized management, and innovative automation capabilities.

The following graphic shows the flow of information around your organization. You can see how Cloud App Security functions as an intermediary between apps, data, and users.



There are four elements to the Cloud App Security framework:

- **Discover and control the use of Shadow IT:** Identify the cloud apps, IaaS, and PaaS services used by your organization. How many cloud apps do you think are used by your users? The apps you don't know about, on average totaling more than 1,000, are your "Shadow IT". When you know which apps are being used, you'll better understand and control your risk.
- **Protect your sensitive information anywhere in the cloud:** Understand, classify, and protect sensitive information at rest. To help you avoid accidental data exposure, Cloud App Security provides data loss prevention (DLP) capabilities that cover the various data leak points that exist in organizations.
- **Protect against cyberthreats and anomalies:** Detect unusual behavior across apps, users, and potential ransomware. Cloud App Security combines multiple detection methods, including anomaly, user entity behavioral analytics (UEBA), and rule-based activity detections, to show who is using the apps in your environment, and how they're using them.
- **Assess the compliance of your cloud apps:** Assess if your cloud apps comply with regulations and industry standards specific to your organization. Cloud App Security helps you compare your apps and usage against relevant compliance requirements, prevent data leaks to noncompliant apps, and limit access to regulated data.

Explore your cloud apps with Cloud Discovery

You can use Cloud Discovery to see what's happening in your network. You'll see both the cloud apps you expect and the ones you don't, signs of Shadow IT, and nonsanctioned apps that might not be compliant with your security and compliance policies. Cloud Discovery analyzes your traffic logs against a catalog of more than 16,000 cloud apps. Cloud Discovery ranks each app and scores it based on more than 80 risk factors to give you visibility into cloud use, Shadow IT, and the risk it poses in your organization.

The Cloud Discovery dashboard provides an at-a-glance overview of what kinds of apps are being used, your open alerts, and the risk levels of the apps in your organization. You can also see who your top app users are and where each app comes from (on an App Headquarters map). You can filter the data collected by Cloud Discovery to generate specific views depending on what interests you most.

Review the Cloud Discovery Dashboard

Your first step is to get a general picture of your cloud apps. Start at the Cloud Discovery dashboard then move through its elements in the following order to understand what's happening in your organization.

1. Start with the **High-level usage overview** to see the overall cloud app use. You can see the **top users** and **source IP addresses**. Based on this information, identify which users in your organization use cloud apps the most. You'll want to pay attention to these users going forward.
2. Dive one level deeper to see which category of apps your organization uses most. See how much of this usage is in **Sanctioned** apps.
3. Go even deeper on the **Discovered apps** tab. See all the apps in a specific category.
4. Review the risk score for the discovered apps in the **App risk overview**. Each discovered app is assessed against risk factors like security and compliance and regulatory measures. Apps are given a risk score between 1 and 10.
5. View where discovered apps are located (based on their headquarters) in the **App Headquarters map**.
6. If you find an app that poses a risk to your organization, you can flag it as **Unsanctioned** in the **Discovered apps** pane.

If your organization is using Microsoft Defender for Endpoint (or a similar solution), any unsanctioned app is automatically blocked.

If you don't have a threat protection solution, you can run a script against the data source to block the app. Then users will see a notification that the application is blocked when they try to access it.

Protect your data and apps with Conditional Access App Control

Cloud Discovery helps you understand what's happening in your cloud environment after the fact. While this process is important, your primary goal is to stop breaches and leaks in real time, before they put your organization at risk. You also need a way to enable users to bring their own devices to work while still protecting your organization from data leaks and data theft. Microsoft Cloud App Security integrates with identity providers (IdPs) to protect your data and devices with access and session controls through **Conditional Access App Control**. If you're using Azure Active Directory (Azure AD) as your IdP, these controls are integrated directly into Cloud App Security.

Conditional Access App Control lets you monitor and control user app access and sessions in real time. By integrating with Azure AD Conditional Access, it's easy to configure apps to work with Conditional Access App Control. It lets you selectively enforce access and session controls on your organization's apps based on any condition in Conditional Access. You can use conditions that define who (user or group of users), what (which cloud apps), and where (which locations and networks) a Conditional Access policy is applied. After you determine the conditions, you can route users to Cloud App Security where you protect data with Conditional Access App Control by applying access and session controls.

Azure AD includes built-in policies that you can configure for an easy deployment. After you configure the conditions of a Conditional Access policy in Azure AD, select **Session** under **Access controls**, and

click **Use Conditional Access App Control**. If you choose to **use custom controls**, you'll define them in the Cloud App Security portal.

You can use access and session policies in the Cloud App Security portal to further refine filters and set actions to be taken on a user. With the access and session policies, you can:

- **Prevent data exfiltration:** Block the download, cut, copy, and print of sensitive documents on, for example, unmanaged devices.
- **Protect on download:** Instead of blocking the download of sensitive documents, you can require them to be labeled and protected with Azure Information Protection. This action ensures that the document is protected and that user access is restricted in a potentially risky session.
- **Prevent upload of unlabeled files:** Enforce the use of labeling. Before a sensitive file is uploaded, distributed, and used by others, it's important to make sure that it has the right label and protection. You can block a file upload until the content is classified.
- **Monitor user sessions for compliance:** Monitor risky users when they sign in to apps and log their actions from within the session. You can investigate and analyze user behavior to understand where, and under what conditions, to apply session policies in the future.
- **Block access:** You can block access for specific apps and users depending on several risk factors. For example, you can block a user if they're using a client certificate as a form of device management.
- **Block custom activities:** Some apps have unique scenarios that carry risk; for example, sending messages with sensitive content in apps like Microsoft Teams or Slack. In these kinds of scenarios, you can scan messages for sensitive content and block them in real time.

For example, let's create a session policy in Microsoft Teams that blocks IM messages containing sensitive content. Assuming we previously created a Conditional Access policy with **Use custom controls** set under **Use Conditional Access App Control**, we start by creating a new session policy in Microsoft Cloud App Security.

We'll use an existing template for our new session policy. Select the **Block sending of messages based on real-time content inspection** policy template.

Under **Activity source** for the session policy, select **Send Teams message** as the application.

You then enable **Content Inspection**, where you'll define the sensitive information as matching a present expression, a custom expression, or any regular expression. When the expressions are defined, select **Block** under **Actions** to block the message, and to create alerts to notify administrators.

Now, when a user tries to send a sensitive message in Teams, they'll see a notification.

Classify and protect sensitive information

One of the key elements of the Cloud App Security framework is protecting your sensitive information. Sensitivity is a subjective phrase, as this can vary from one organization to another.

Here, you'll understand how to find which apps are accessing your data, how to classify which information is sensitive, how to protect it from illegal access, and how to monitor and report on the overall health of your environment.

What is Information Protection?

An employee might accidentally upload a file to the wrong place. Or they could send confidential information to someone who shouldn't have it. As a result, information could be lost or made accessible to the wrong person. Any lost or wrongfully exposed information can have serious legal, financial, or

reputational consequences for your organization. Information is vital to any modern organization, and you want to ensure that it's protected at all times.

To help you, Microsoft Cloud App Security natively integrates with Azure Information Protection, a cloud-based service that helps classify and protect files and emails across your organization.

Note: You have to enable the app connector for Microsoft 365 to take advantage of Azure Information Protection

You enforce information protection with Microsoft Cloud App Security through phases:

Phase 1: Discover data

During this phase, you make sure apps are connected to Microsoft Cloud App Security so it can scan for and classify data, then apply policies and controls. You can do this in two different ways: use an app connector, or use Conditional Access App Control.

Phase 2: Classify sensitive information

In this phase, you'll do the following:

1. Decide what counts as sensitive in the context of your organization. Microsoft Cloud App Security includes more than 100 predefined sensitive information types, and default labels in Azure Information Protection. Sensitive information types and labels define how to handle, for example, passport numbers and national identity numbers. You can also use default labels in Azure Information Protection. These labels will be used by Microsoft Cloud App Security when scanning, to classify information. The labels are:
 - **Personal:** Data for personal, nonbusiness use only.
 - **Public:** Data that can be shared for public consumption, such as marketing posters and blog posts.
 - **General:** Data that can't be shared for public consumption, but can be shared with external partners. For example, project timelines and organizational charts.
 - **Confidential:** Data that could damage the organization if it's shared with unauthorized people. For example, sales account data and forecasts.
 - **Highly confidential:** Very sensitive data that will cause serious damage if shared with unauthorized people. For example, customer details, passwords and source code.
2. Enable Azure Information Protection integration in Microsoft Cloud App Security by selecting **Automatically scan new files for Azure Information Protection classification labels** in the **Settings** pane:

The screenshot shows the Microsoft Cloud App Security interface. On the left, there's a sidebar with various settings options like Snapshot reports, Continuous reports, and Admin quarantine. The 'Azure Information Protection' option is highlighted with a red box. The main pane displays 'Azure Information Protection settings' with two checkboxes: 'Automatically scan new files for Azure Information Protection classification labels and content inspection warnings' (which is checked) and 'Only scan files for Azure Information Protection classification labels and content inspection warnings from this tenant'. Below these are sections for 'Inspect protected files' and a 'Save' button.

Phase 3: Protect data

There are different types of policies you can create to detect sensitive information and act accordingly. For example, you can create a **File policy** to scan the content of files in your apps in real time, and for data at rest. File policies let you apply governance actions. You can then automatically:

- Trigger alerts and email notifications.
- Change sharing access for files.
- Quarantine files.
- Remove file or folder permissions.
- Move files to a trash folder.

To create a file policy

1. Open Microsoft Cloud App Security
2. Select the **Control** pane
3. Select **Policies > Create policy**
4. Select **File policy**

When the form that appears, you'll fill in the following fields:

Field	Description
Policy severity	Defines how important the policy is and whether to trigger a notification. The severity of the policy can be customized to quickly identify the risk associated with a policy match.
Category	This is an informative label that you assign to the policy to help locate it later. By default, for File policies is DLP.

Field	Description
Create a filter for the files this policy will act on	It is used to decide which apps will trigger the policy. Ideally this should be defined to be as narrow as possible to avoid false positives.
Apply to (1st)	Select which discovered apps will trigger the policy. There are two choices: <ul style="list-style-type: none"> All files excluding selected folders: to apply the policy to all files. Selected folders: to apply the policy to apps like Box, SharePoint, OneDrive, and Dropbox.
Apply to (2nd)	Select which users and groups should be included in this policy. There are three options: <ul style="list-style-type: none"> All file owners File owners from selected user groups All file owners excluding selected groups
Content inspection method	Select how you want files to be inspected. There are two options: <ul style="list-style-type: none"> Built-in DLP Data Classification Services (DCS) Microsoft recommends DCS as this will allow you to use a unified labeling experience across M365, Azure Information Protection, and Microsoft Cloud App Security.
Governance	Select which governance actions you want Microsoft Cloud App Security to perform when a match is detected.

5. When you're done, select **Create** to create your file policy.

Phase 4: Monitor and report

Check your dashboard to monitor for alerts and the overall health of your environment. For example, to review file-related alerts, go to the **Alerts** pane, and select **DLP** in the **Category** field.

The screenshot shows the 'Alerts' section of the Microsoft Cloud App Security interface. On the left, there's a sidebar with icons for Home, Alerts, Threats, Policies, and Help. The main area has a title 'Alerts' with a search bar. Below it is a filter bar with dropdowns for 'RESOLUTION STATUS' (OPEN, DISMISSED, RESOLVED), 'CATEGORY' (DLP), 'SEVERITY' (Low, Medium, High), 'APP' (Select apps...), 'USER NAME' (Select users...), and 'POLICY' (Select policy...). A 'T' icon indicates 1 - 20 of 63 alerts. The alert list table has columns for Alert, App, Resolution, Severity, and Date. One alert is highlighted: 'Externally shared' from Box, with resolution 'OPEN', severity 'Low', and date '8/10/20, 4:55 PM'.

You can investigate a file-related alert to better understand what caused it to be triggered. Or you can dismiss an alert that you determine could be ignored. You can also export your alerts to a CSV file for further analysis.

Guided demonstration - Cloud App Security

A guided demonstration is a recorded click-through simulation. You do not use your lab tenant for this demonstration. Instead simply click the link [here⁵](https://aka.ms/DetectThreats-ManageAlerts-MCAS_InteractiveGuide) to launch this demonstration. A focus will appear in the demonstration showing you the next place to click to advance the demonstration.

⁵ https://aka.ms/DetectThreats-ManageAlerts-MCAS_InteractiveGuide

In this experience you will do the following:

1. Identify suspicious activities.
2. Investigate risks.
3. Take appropriate action.

Time required: 11 minutes

Respond to data loss prevention alerts

Lesson Introduction

As a Security Operations Analyst, you need to understand compliance related terminology and alerts. Learn how the data loss prevention alerts will help in your investigation to find the full scope of the incident.

Microsoft 365 provides data loss prevention (DLP) protection to identify, monitor, and automatically protect sensitive information.

You are a Security Operations Analyst working at a company that implemented Microsoft 365 compliance solutions. Based on recent security incidents in your organization, you have been assigned the responsibility to advise the compliance team on the types of information they should protect.

To work with the compliance team, you need to learn about the data loss prevention components, including sensitive info types, sensitivity labels, DLP policies, and policy alerts.

Learning objectives

After completing this lesson, you should be able to:

- Describe data loss prevention (DLP) components in Microsoft 365
- Investigate DLP alerts in the Microsoft 365 compliance center
- Investigate DLP alerts in Microsoft Cloud App Security

Describe data loss prevention alerts

As a Security Operations Analyst, you need to understand Compliance-related terminology and alerts. The Data loss prevention (DLP) alerts will help you in your investigation to find the full scope of the incident. DLP alerts can be generated from Microsoft 365 Compliance or Microsoft Cloud App Security. You might not be the person creating the DLP Policies, but it is important for you to understand them so you can recommend changes.

To comply with business standards and industry regulations, organizations must protect sensitive information and prevent its inadvertent disclosure. Sensitive information can include financial data or personal information such as credit card numbers, social security numbers, or health records.

With a DLP policy, you can:

- Identify sensitive information across many locations, such as Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft Teams.
 - For example, you can identify any document containing a credit card number that's stored in any OneDrive for Business site, or you can monitor just the OneDrive sites of specific people.
 - Prevent the accidental sharing of sensitive information.
 - For example, you can identify any document or email containing a health record that's shared with people outside your organization, and then automatically block access to that document or block the email from being sent.
 - Monitor and protect sensitive information in the desktop versions of Excel, PowerPoint, and Word.

- Just like in Exchange Online, SharePoint Online, and OneDrive for Business, these Office desktop programs include the same capabilities to identify sensitive information and apply DLP policies. DLP provides continuous monitoring when people share content in these Office programs.
- Help users learn how to stay compliant without interrupting their workflow.
- You can educate your users about DLP policies and help them remain compliant without blocking their work. For example, if a user tries to share a document containing sensitive information, a DLP policy can send them an email notification and show them a policy tip in the context of the document library that allows them to override the policy if they have a business justification. The same policy tips also appear in Outlook on the web, Outlook, Excel, PowerPoint, and Word.
- View DLP alerts and reports showing content that matches your organization's DLP policies.

Data loss prevention components

If you have not worked with DLP, it is important to understand the underlying components.

Sensitive information types

A sensitive information type is defined by a pattern that can be identified by a regular expression or a function. In addition, corroborative evidence such as keywords and checksums can be used to identify a sensitive information type. Confidence level and proximity are also used in the evaluation process.

Microsoft 365 compliance comes with built-in Sensitive information types like Credit Card Numbers, Bank Accounts, and more. You can also create a custom sensitive info type matched on regular expressions, keywords, or an uploaded dictionary.

Sensitivity labels

Sensitivity labels specify the classification of a document. These could be terms like public, private, or classified. With these labels, more functionality can be applied to the document, like encryption. Labels are applied to documents either manually by the user or automatically based on sensitive info types.

Data loss prevention policy

A DLP policy contains a few basic things:

- Where to protect the content: locations such as Exchange Online, SharePoint Online, and OneDrive for Business sites, as well as Microsoft Teams chat and channel messages.
- When and how to protect the content by enforcing rules comprised of:
 - Conditions the content must match before the rule is enforced. For example, a rule might be configured to look only for content containing Social Security numbers that have been shared with people outside your organization.
 - Actions that you want the rule to take automatically when content matching the conditions is found. For example, a rule might be configured to block access to a document and send both the user and compliance officer an email notification.

Cloud App Security file policy

File policies can be set to provide continuous compliance scans, legal eDiscovery tasks, DLP for sensitive content shared publicly, and many more use cases. Cloud App Security can monitor any file type based on more than 20 metadata filters.

Investigate DLP alerts in Microsoft 365 compliance

To view DLP Alerts from DLP Policies created in Microsoft 365 Compliance do the following:

1. In the Microsoft 365 compliance center [https://compliance.microsoft.com⁶](https://compliance.microsoft.com), go to **Data Loss Prevention**.
2. Select the **Alerts** tab to view the DLP alerts dashboard.
3. Choose filters to refine the list of alerts. Choose Customize columns to list the properties you want to see. You can also choose to sort the alerts in ascending or descending order in any column.
4. Select an alert to see details.
5. Select the **Events** tab to view all of the events associated with the alert. You can choose a particular event to view its details.
6. Select the **Sensitive Info Types** tab to view details about the sensitive information types detected in the content. Details include confidence and count.
7. After you investigate the alert, choose Manage alert to change the status (Active, Investigating, Dismissed, or Resolved). You can also add comments and assign the alert to someone in your organization.
8. To see the history of workflow management, choose Management log.
9. After you take the required action for the alert, set the status of the alert to **Resolved**.

Investigate DLP alerts in Microsoft Cloud App Security

After a Cloud App Security File policy is created with a DLP-related configuration, file policy violation alerts are investigated in the Alerts area of Cloud App Security.

To manage alerts:

From the Alerts page, select **Open** for the Resolution Status.

This section of the dashboard provides full visibility into any suspicious activity or violation of your established policies. It can help you safeguard the security posture you defined for your cloud environment.

⁶ <https://compliance.microsoft.com?azure-portal=true>

Alert	App	Resolution	Severity	Date
test! BOX_INV06079044.pdf	Test2	OPEN	Medium	40 minutes ago
test! RG.jpg	Box for Micr...	OPEN	Medium	40 minutes ago
test! test.gdoc	Box for Micr...	OPEN	Medium	an hour ago
test! test.boxnote	Box for Micr...	OPEN	Medium	an hour ago
test! .Test	Box for Micr...	OPEN	Medium	an hour ago
System alert: DLP Connector error Test dlp 127.0.0.1:1223	—	OPEN	Medium	7 hours ago

For each alert, you need to investigate and determine the nature of the violation and the required response.

- You can filter the alerts by Alert type or by Severity to process the most important ones first.
- Select a specific alert. Depending on what type of alert it is, you'll see various actions that can be taken before resolving the alert.
- You can filter based on App - The apps listed are ones for which activities were detected by Cloud App Security.
- There are three types of violations you'll need to deal with when investigating alerts:
 - **Serious violations** - Serious violations require an immediate response.
 - Examples:
 - For a suspicious activity alert, you might want to suspend the account until the user changes their password.
 - For a data leak, you might want to restrict permissions or quarantine the file.
 - If a new app is discovered, you might want to block access to the service on your proxy or firewall.
 - **Questionable violations** - Questionable violations require further investigation.
 - You can contact the user or the user's manager about the nature of the activity.
 - Leave the activity open until you have more information.
 - **Authorized violations or anomalous behavior** - Authorized violations or anomalous behavior can result from legitimate use.
 - You can dismiss the alert.

Anytime you dismiss an alert, it's important to submit feedback about why you're dismissing the alert. The Cloud App Security team uses this feedback as an indication of the accuracy of the alert. This infor-

mation is then used to fine-tune our machine learning models for future alerts. You can follow these guidelines in deciding how to categorize the alert:

- If legitimate use triggered the alert and it isn't a security issue, it could be one of these types:
 - Benign positive: The alert is accurate, but the activity is legitimate. You can dismiss the alert and set the reason to Actual severity is lower or Not interesting.
 - False positive: The alert is inaccurate. Dismiss the alert and set the reason to Alert is not accurate.
- If there's too much noise to determine the legitimacy and accuracy of an alert, dismiss it and set the reason to Too many similar alerts.
- True positive: If the alert is related to an actual risky event that was either committed maliciously or unintentionally by an insider or outsider, you should set the event to Resolve after all appropriate action has been taken to remediate the event.

Even though you are interested in File policy alerts for DLP, the alerts list will show many different alert types. It is important to understand the different alert types because these non-DLP alerts could also provide insight into a security incident.

The following table provides a list of the types of alerts that can be triggered and recommends ways you can resolve them.

Alert type	Description	Recommended resolution
Activity policy violation	This type of alert is the result of a policy you created.	To work with this type of alert in bulk, we recommend that you work in the Policy center to mitigate them. Fine-tune the policy to exclude noisy entities by adding more filters and more granular controls. If the policy is accurate, the alert is warranted, and it's a violation you want to stop immediately, consider adding automatic remediation in the policy.
File policy violation	This type of alert is the result of a policy you created.	To work with this type of alert in bulk, we recommend that you work in the Policy center to mitigate them. Fine-tune the policy to exclude noisy entities by adding more filters and more granular controls. Fine-tune the policy to exclude noisy entities by adding more filters and more granular controls.
Compromised account	This type of alert is triggered when Cloud App Security identifies an account that was compromised. This means there's a high probability that the account was used in an unauthorized way.	We recommend that you suspend the account until you can reach the user and make sure they change their password.

Alert type	Description	Recommended resolution
Inactive account	This alert is triggered when an account hasn't been used in 60 days in one of your connected cloud apps.	Contact the user and the user's manager to determine whether the account is still active. If not, suspend the user and terminate the license for the app.
New admin user	Alerts you to changes in your privileged accounts for connected apps.	Confirm that the new admin permissions are required for the user. If they aren't, recommend revoking admin privileges to reduce exposure.
New admin location	Alerts you to changes in your privileged accounts for connected apps.	Confirm that the sign-in from this anomalous location was legitimate. If it's not, recommend revoking admin permissions or suspending the account to reduce exposure.
New location	An informative alert about access to a connected app from a new location, and it's triggered only once per country/region.	Investigate the specific user's activity.
New discovered service	This alert is an alert about Shadow IT. A new app was detected by Cloud Discovery.	Assess the risk of the service based on the app catalog.
Suspicious activity	This alert lets you know that anomalous activity has been detected that isn't aligned with expected activities or users in your organization.	Investigate the behavior and confirm it with the user. This type of alert is a great place to start learning more about your environment and creating new policies with these alerts. For example, if someone suddenly uploads a large amount of data to one of your connected apps, you can set a rule to govern that type of anomalous behavior.
Use of personal account	This alert lets you know that a new personal account has access to resources in your connected apps.	Remove the user's collaborations in the external account.

Manage insider risk in Microsoft 365

Lesson Introduction

Insider risk management in Microsoft 365 helps organizations address internal risks, such as IP theft, fraud, and sabotage. Learn about insider risk management and how Microsoft technologies can help you detect, investigate, and take action on risky activities in your organization.

Learning objectives

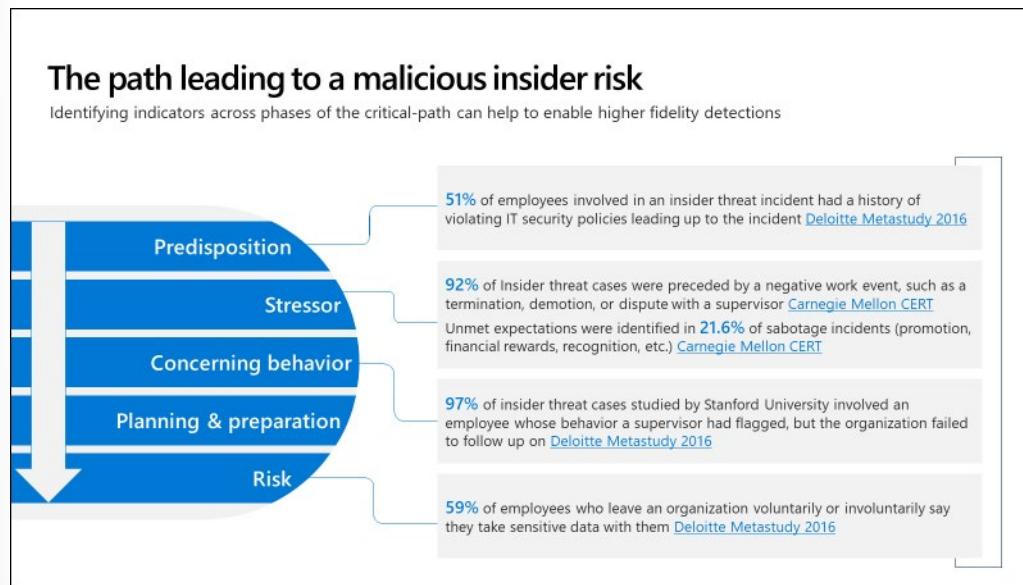
After completing this lesson, you should be able to:

- Explain how insider risk management in Microsoft 365 can help prevent, detect, and contain internal risks in an organization.
- Describe the types of built-in, pre-defined policy templates.
- List the prerequisites that need to be met before creating insider risk policies.
- Explain the types of actions you can take on an insider risk management case.

Insider risk management explained

In March of 2019, a large auto manufacturer with state-of-the-art, proprietary operations and technology filed a lawsuit against four former employees and a competitor for corporate espionage. The lawsuit was filed after discovering that the employees had downloaded proprietary warehouse schematics and operational procedures before leaving the company and shared them with the competitor.

Trusting employees is key to fostering a dynamic and productive workplace. But with trust also comes risk. Companies need to be able to quickly identify and manage risk from insiders (employees or contractors with corporate access) to minimize the negative impact to their business. Insider threats and risks from illegal, inappropriate, unauthorized, or unethical behavior and actions are a major issue for all companies and can easily go undetected until it is too late. A survey by Crowd Research Partners in 2018 indicated that 90% of organizations feel vulnerable to insider risks and 53% confirmed insider risks against their organization in the previous 12 months. According to a Carnegie Mellon CERT study, 92% of insider threat cases were preceded by a negative work event, such as a termination, demotion, or dispute with a supervisor. And in 2016, Deloitte reported that 59% of employees who leave an organization voluntarily or involuntarily say they take sensitive data with them and that 51% of employees involved in an insider threat incident had a history of violating IT security policies leading up to the incident.



The financial impact of insider threats is substantial, as companies suffer market, legal, reputational and productivity losses. According to the Ponemon Institute, the average cost of an insider incident arising from negligence is over USD307,000. If the insider is malicious, it's over USD750,000. Aside from financial loss, the impacts of insider risk can include damage to brand and reputation, competitive disadvantage, noncompliance with regulations, and loss of market share.

Traditional approaches to identifying insider risks such as user behavior analytics, monitoring user activity, and data loss prevention can suffer from limitations such as complex deployment scenarios, limited insights, and a lack of workload integration beyond SecOps.

The insider risk management solution in Microsoft 365 leverages the Microsoft Graph, security services and connectors to human resources (HR) systems like SAP, to obtain real-time native signals such as file activity, communications sentiment, abnormal user behaviors, and resignation date. A set of configurable policy templates tailored specifically for risks – such as digital IP theft, confidentiality breach, and HR violations – use machine learning and intelligence to correlate these signals to identify hidden patterns and risks that traditional or manual methods might miss. These built-in policy templates allow you to identify and mitigate risky activities while balancing employee privacy versus organization risk with privacy-by-design architecture. Finally, end-to-end integrated workflows ensure that the right people across security, HR, legal, and compliance are involved to quickly investigate and take action once a risk has been identified.

Note: Please review **Microsoft 365 licensing guidance for security & compliance⁷** to identify required licenses for your organization.

Risk Pain Points in the Modern Workplace

Managing and minimizing risk in your organization starts with understanding the types of risks found in the modern workplace. Some risks are driven by external factors such as bad actors who try to steal employee credentials through brute force or phishing attacks. Other risks are driven by internal events and employee activities that can be eliminated and avoided. Some examples of internal risks from employees include:

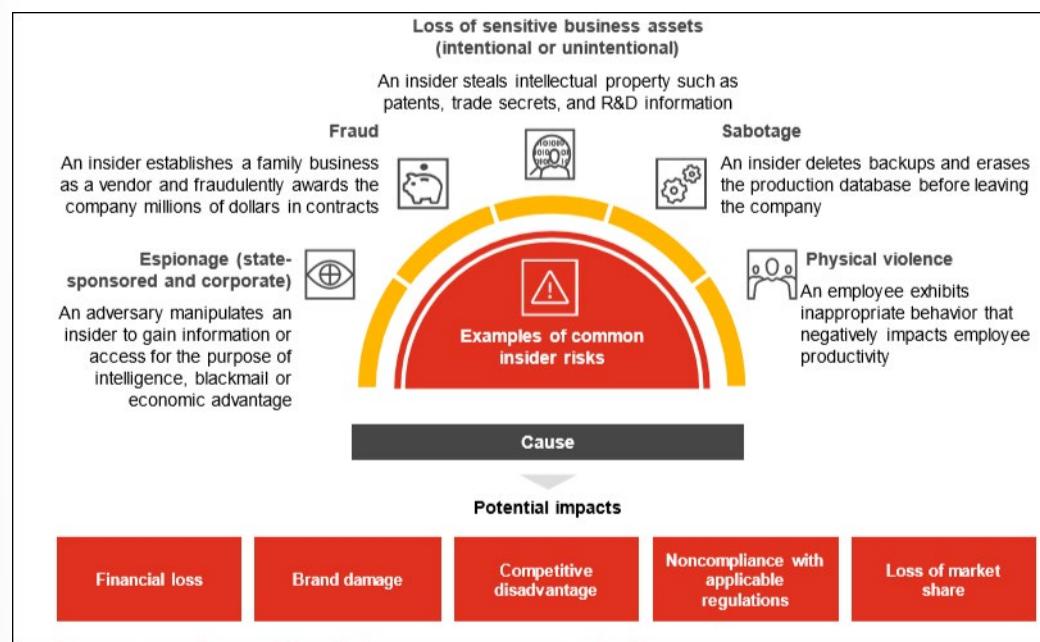
⁷ <https://docs.microsoft.com/office365/servicedescriptions/microsoft-365-service-descriptions/microsoft-365-tenantlevel-services-licensing-guidance/microsoft-365-security-compliance-licensing-guidance?azure-portal=true>



- Intellectual property (IP) theft
- Espionage
- Leaks of sensitive business assets
- Confidentiality violations
- Sabotage
- Fraud
- Insider trading
- Code-of-conduct violations
- Regulatory compliance violations

Insider risks vary by industry. In healthcare, internal fraud is the most frequently cited type of risk, while sabotage represents the greatest risk to IT businesses.

The path leading to a malicious insider risk varies. It may be an employee who has a history of violating IT security policies, a negative work event such as termination or a dispute with a supervisor, or employees who take sensitive data before leaving the company voluntarily or involuntarily.



Common insider risk scenarios

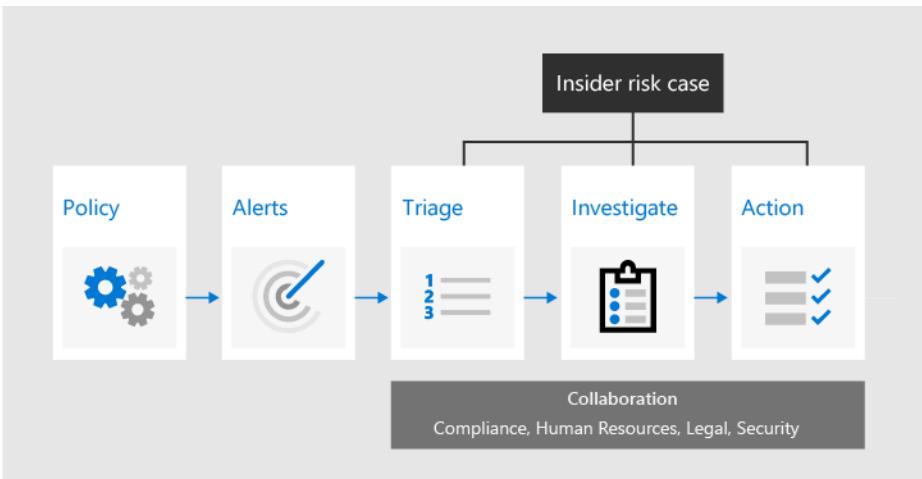
The insider risk management solution in Microsoft 365 can help you detect, investigate, and take action to mitigate internal risks in your organization in common scenarios, such as:

- **Data theft by departing employee.** When employees leave an organization, either voluntarily or as the result of termination, there is often legitimate concerns that company, customer, and employee data are at risk. Employees may innocently assume that project data isn't proprietary, or they may be tempted to take company data for personal gain and in violation of company policy and legal standards.
- **Leak of sensitive or confidential information.** In most cases, employees try their best to properly handle sensitive or confidential information. But occasionally employees make mistakes and information is accidentally shared outside your organization or in violation of your information protection policies. Sometimes employees may intentionally leak or share sensitive and confidential information with malicious intent and for potential personal gain.
- **Actions and behaviors that violate corporate policies.** Employee-to-employee communications are often a source of inadvertent or malicious violations of corporate policies. These violations can include offensive language, threats, and cyber-bullying between employees. This type of activity contributes to a hostile work environment and can result in legal actions against both employees and the larger organization.

Insider risk management workflow

Using policy templates with pre-defined conditions and comprehensive activity signaling across the Microsoft 365 service, you can use actionable insights to quickly identify and resolve risky behavior.

Identifying and resolving internal risk activities and compliance issues with insider risk management in Microsoft 365 uses the following workflow:



- 1. Policies.** Insider risk management policies determine which employees are in-scope and which types of risk indicators are configured for alerts.
- 2. Alerts.** Insider risk management alerts are automatically generated by risk indicators defined in insider risk management policies. These alerts give compliance analysts and investigators an all-up view of the current risk status and allow your organization to triage and take actions for discovered risks.
- 3. Triage.** Reviewers can quickly identify insider risk alerts and examine each to evaluate and triage. Alerts are resolved by opening a new case, assigning the alert to an existing case, or dismissing the alert.
- 4. Investigate.** Cases are manually created from alerts in the situations where further action is needed to address an issue for an employee.
- 5. Action.** After investigating the details of a case, you can take action by sending the employee a notice, resolving the case as benign, or escalating to a data or employee investigation.

Learn more

- [Crowd Research Partners, Insider Threat Report⁸](#)
- [Carnegie Mellon CERT study: The “Big Picture” of Insider IT Sabotage Across U.S. Critical Infrastructures⁹](#)
- [Carnegie Mellon University: Insider Threats in Healthcare¹⁰](#)

Prerequisites & permissions

Before you can begin creating insider risk policies, there are several requirements that need to be met.

Turn on audit logging

Insider risk management uses audit logs for user insights and activities configured in policies. The audit logs are a summary of all activities associated with an insider risk management policy or anytime a policy is modified. For step-by-step instructions to turn on auditing, see [Turn Office 365 audit log search on](#)

⁸ <https://crowdresearchpartners.com/portfolio/insider-threat-report/?azure-portal=true>

⁹ https://resources.sei.cmu.edu/asset_files/TechnicalReport/2008_005_001_14981.pdf?azure-portal=true

¹⁰ <https://insights.sei.cmu.edu/insider-threat/2019/02/insider-threats-in-healthcare-part-7-of-9-insider-threats-across-industry-sectors.html?azure-portal=true>

or off¹¹. After you turn on auditing, a message is displayed that says the audit log is being prepared and that you can run a search in a couple of hours after the preparation is complete.

Assign permissions

A global administrator will need to assign you and other compliance officers to the **Insider Risk Management** or **Insider Risk Management Admin** role group by using the **Permissions** module in the Microsoft 365 compliance center. Once you have been assigned to one of these roles, you have the ability to assign additional users to specific role groups to manage different sets of insider risk management features.

Depending on the structure of your compliance management team, you have options to assign users to specific role groups to manage different sets of insider risk management features. You have the ability to choose from the following role group options when configuring insider risk management:

- **Insider Risk Management.** Use this role group to manage insider risk management for your organization in a single group. By adding all user accounts for designated administrators, analysts, and investigators, you can configure insider risk management permissions in a single group. This role group contains all the insider risk management permission roles. This is the easiest way to quickly get started with insider risk management and is a good fit for organizations that do not need separate permissions defined for separate groups of users.
- **Insider Risk Management Admin.** Use this role group to initially configure insider risk management and later to segregate insider risk administrators into a defined group. Users in this role group can create, read, update, and delete insider risk management policies, global settings, and role group assignments.
- **Insider Risk Management Analysts.** Use this group to assign permissions to users that will act as insider risk case analysts. Users in this role group can access all insider risk management alerts, cases, and notices templates. They cannot access the insider risk Content Explorer.
- **Insider Risk Management Investigators.** Use this group to assign permissions to users that will act as insider risk data investigators. Users in this role group can access all insider risk management alerts, cases, notices templates, and the Content Explorer for all cases.

Potential dependencies

Two of the insider risk management templates have dependencies that must be configured for policy indicators to generate relevant activity alerts. This step might be optional depending on the policy you plan to configure for your organization.

Departing employee data theft template

If you configure a policy using the Departing employee data theft template, you'll need to configure a Microsoft 365 Human Resources (HR) data connector so that you can import user and log data from 3rd-party risk management and human resources platforms. HR connectors allow you to pull in human resources data from CSV files, including user termination and last employment dates. This data helps drive alert indicators in insider risk management policies and is an important part of configuring full risk

¹¹ <https://docs.microsoft.com/microsoft-365/compliance/turn-audit-log-search-on-or-off?view=o365-worldwide&azure-portal=true>

management coverage in your organization.

The following requirements must be met before you can set up an HR connector:

- A global administrator will need to consent to allow the Office 365 Import service to access data in your organization.
- The user who creates the HR connector will need to be assigned the Mailbox Import Export role in Exchange Online.
- You have to have a system in place for retrieving and exporting the data from your organization's HR system and add it to a CSV file.

Once the requirements have been met, you can set up your HR connector.

Briefly, the steps for creating the connector involve the following:

1. Creating an app in Azure Active Directory.
2. Generating the CSV file from your organization's HR system.
3. Creating an HR connector in the Microsoft 365 compliance center.
4. Running a script that will upload the HR data in the CSV file to the Microsoft cloud.

For more details, see the [Set up a connector to import HR data¹²](#) topic.

Data leaks template

Insider risk management supports using DLP policies to help identify the intentional or accidental exposure of sensitive information to unwanted parties. When configuring an insider risk management policy with the Data leaks template, you have to assign a specific DLP policy. This policy helps drive the alert indicators for sensitive information and is an important part of configuring full risk management coverage in your organization.

Note: To reduce noise, alerts will only fire when a high volume DLP policy qualifying event is triggered.

For example, an alert will fire if the policy detects 10 or more credit card numbers in an email or document, but not less. See the [Create, test, and tune a DLP policy¹³](#) topic to learn how to configure DLP policies for your organization.

Creating a new insider risk policy

Insider risk management policies include assigned users and define which types of risk indicators are configured for alerts. Before activities can trigger alerts, a policy must be configured.

To create a new insider risk management policy, you use the policy wizard in the **Insider risk management** solution in the Microsoft 365 compliance center. Briefly, you create a new policy by stepping through the policy wizard and policy settings to configure the following items:

- **Policy template**
- **Users or groups** the policy will apply to (optionally, assign higher risk scores to detected activity based on where the related content is located, what sensitive info is included, and what sensitivity labels are applied)
- **Alert indicators (Indicators)** need to be enabled under **Policy Settings** before they can be selected when creating a policy)
- **Duration** (time frame) for monitoring

¹² <https://docs.microsoft.com/microsoft-365/compliance/import-hr-data?view=o365-worldwide&azure-portal=true>

¹³ <https://docs.microsoft.com/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide&azure-portal=true>

For more information, see [Create an insider risk policy¹⁴](#).

Learn more

- [Compare Microsoft 365 Enterprise Plans¹⁵](#)
- [Enable permissions for insider risk management¹⁶](#)
- [Create, test, and tune a DLP policy¹⁷](#)

Guided demonstration - Insider risk management

A guided demonstration is a recorded click-through simulation. You do not use your lab tenant for this demonstration. Instead simply click the link [here¹⁸](#) to launch this demonstration. A focus will appear in the demonstration showing you the next place to click to advance the demonstration.

In this experience you will do the following:

1. Detect risky activities.
2. Investigate alerts.
3. Address potential threats.

Time required: 17 minutes

¹⁴ <https://docs.microsoft.com/microsoft-365/compliance/insider-risk-management-configure?view=o365-worldwide#step-5-required-create-an-insider-risk-management-policy?azure-portal=true>

¹⁵ <https://www.microsoft.com/microsoft-365/compare-microsoft-365-enterprise-plans?rtc=1?azure-portal=true>

¹⁶ <https://docs.microsoft.com/microsoft-365/compliance/insider-risk-management-configure?view=o365-worldwide#step-1-required-enable-permissions-for-insider-risk-management?azure-portal=true>

¹⁷ <https://docs.microsoft.com/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide?azure-portal=true>

¹⁸ <https://mslearn.cloudguides.com/guides/Minimize%20internal%20risks%20with%20insider%20risk%20management%20in%20Microsoft%20365>

Knowledge check

Check your Knowledge

Multiple choice

Item 1. When reviewing a specific incident, which tab is contained on the incident page?

- Networks
- Machines
- Mailboxes

Multiple choice

Item 2. You can classify an Incident as which of the following?

- True alert
- High alert
- Test alert

Multiple choice

Item 3. The Devices page shows information from which Defender product?

- Microsoft Cloud App Security
- Microsoft Defender for Identity
- Microsoft Defender for Endpoint

Multiple choice

Item 4. Which DLP component is used to classify a document?

- Sensitive info types
- Retention Policy
- Sensitivity label

Multiple choice

Item 5. In Cloud App Security, which types of Policy is used for DLP?

- Access Policy
- File Policy
- Activity Policy

Multiple choice

Item 6. Which DLP component has the logic to protect content in locations such as SharePoint Online?

- Sensitive info types
- DLP Policy
- Sensitivity label

Lab - Mitigate threats using Microsoft 365 Defender

Lab: Mitigate threats using Microsoft 365 Defender

To download the most recent version of this lab, please visit the SC-200 [GitHub repository¹⁹](#).

Note: Depending on the lab hosting solution used for your class delivery, the lab instructions may display directly in the virtual lab environment, in addition to being available in the GitHub repository. In that case, follow guidance from your instructor as to where you will access the lab steps from. Even if the GitHub version is not used for your class, you may still find it useful to be able to reference the lab instructions on GitHub after class is over.

Lab scenario

You are a Security Operations Analyst working at a company that is implementing Microsoft 365 Defender. You start by exploring the features of the Microsoft 365 security portal.

Objectives

After you complete this lab, you will be able to:

- Explain and navigate the Microsoft 365 security portal.

Lab setup

- Estimated time: 15 minutes

¹⁹ <https://github.com/MicrosoftLearning/SC-200T00A-Microsoft-Security-Operations-Analyst>

Answers

Multiple choice

Item 1. When reviewing a specific incident, which tab is contained on the incident page?

- Networks
- Machines
- Mailboxes

Explanation

The incident page has a tab for mailboxes.

Multiple choice

Item 2. You can classify an Incident as which of the following?

- True alert
- High alert
- Test alert

Explanation

Alert is an option.

Multiple choice

Item 3. The Devices page shows information from which Defender product?

- Microsoft Cloud App Security
- Microsoft Defender for Identity
- Microsoft Defender for Endpoint

Explanation

Devices are based on Defender for Endpoint.

Multiple choice

Item 4. Which DLP component is used to classify a document?

- Sensitive info types
- Retention Policy
- Sensitivity label

Explanation

The Sensitivity label is applied to a document.

Multiple choice

Item 5. In Cloud App Security, which types of Policy is used for DLP?

- Access Policy
- File Policy
- Activity Policy

Explanation

File Policy is used for DLP.

Multiple choice

Item 6. Which DLP component has the logic to protect content in locations such as SharePoint Online?

- Sensitive info types
- DLP Policy
- Sensitivity label

Explanation

The DLP Policy specifies the location.

Module 3 Mitigate threats using Azure Defender

Plan for cloud workload protections using Azure Defender

Lesson Introduction

Azure Defender, integrated with Azure Security Center, provides Azure and hybrid cloud workload protection and security.

You are a Security Operations Analyst working at a company that uses Azure Security Center for Cloud Security Posture Management. You are responsible for implementing cloud workload protections provided by Azure Defender.

You need an overview of what resources can be protected by Azure Defender. As Azure Defender is integrated with Azure Security Center, you also want to have a basic understanding of the features provided by Azure Security Center.

Learn the purpose of Azure Defender, Azure Defender's relationship to Azure Security Center, and how to enable Azure Defender.

Learning objectives

After completing this lesson, you should be able to:

- Describe Azure Defender features
- Explain Azure Security Center features
- Enable Azure Defender

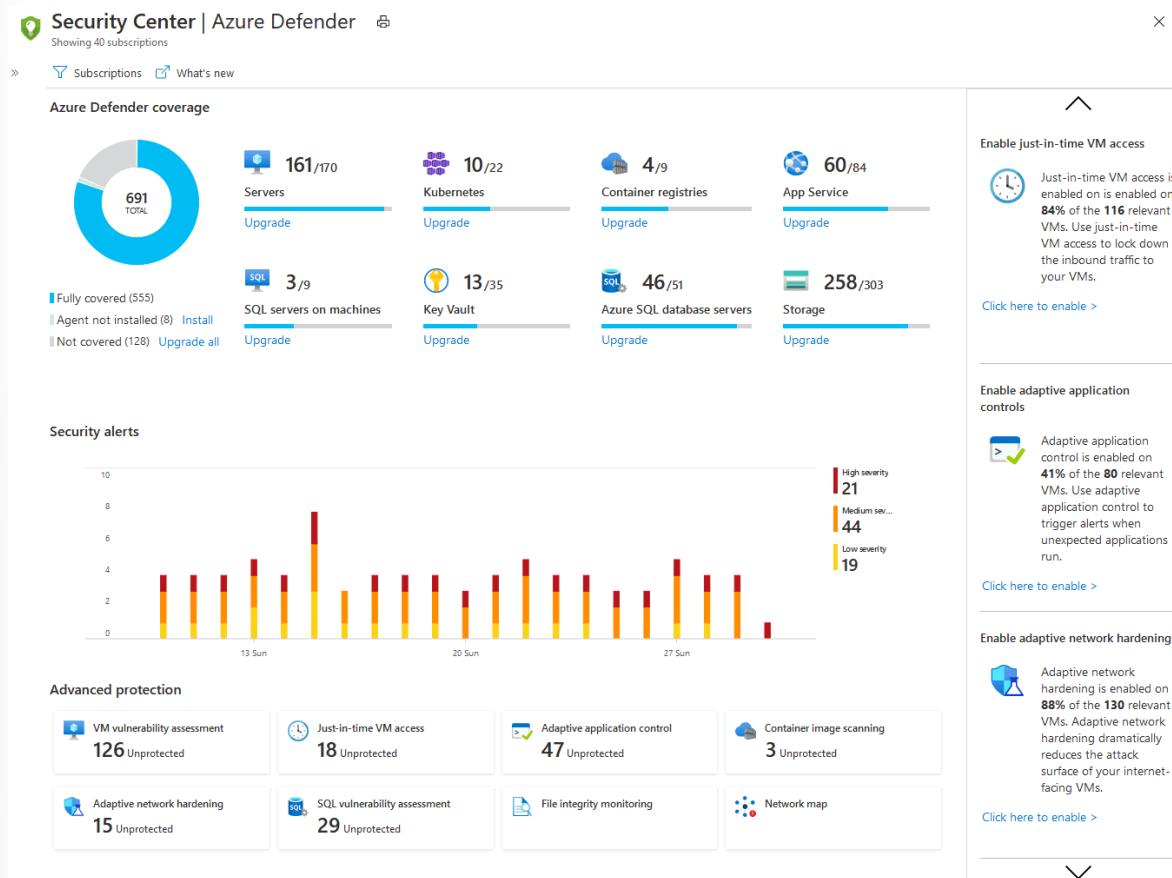
Explain Azure Defender

Azure Defender is the Cloud workload protection feature of Azure Security Center. Azure Security Center's features cover the two broad pillars of cloud security:

Cloud Security Posture Management (CSPM) - Security Center is available for free to all Azure users. The free experience includes CSPM features such as secure score, detection of security misconfigurations in your Azure machines, asset inventory, and more. Use these CSPM features to strengthen your hybrid cloud posture and track compliance with built-in policies.

Cloud Workload Protection (CWP) - Security Center's integrated cloud workload protection platform (CWPP), Azure Defender, brings advanced, intelligent protection to your Azure and hybrid resources and workloads. Enabling Azure Defender brings a range of extra security features. In addition to the built-in policies, when you've enabled any Azure Defender plan, you can also add custom policies and initiatives.

The Azure Defender dashboard in Security Center provides visibility and control of the CWP features for your environment:



What resource types can Azure Defender secure?

Azure Defender provides security alerts and advanced threat protection for virtual machines, SQL databases, containers, web applications, your network, and more.

When you enable Azure Defender from the Pricing and settings area of Azure Security Center, the following Defender plans are all enabled simultaneously and provide comprehensive defenses for the compute, data, and service layers of your environment:

- Azure Defender for servers
- Azure Defender for App Service
- Azure Defender for Storage

- Azure Defender for SQL
- Azure Defender for Kubernetes
- Azure Defender for container registries
- Azure Defender for Key Vault
- Azure Defender for Resource Manager
- Azure Defender for DNS

Hybrid cloud protection

In addition to defending your Azure environment, you can add Azure Defender capabilities to your hybrid cloud environment:

- Protect your non-Azure servers
- Protect your virtual machines in other clouds (such as AWS and GCP)

You'll get customized threat intelligence and prioritized alerts according to your specific environment so that you can focus on what matters the most.

To extend protection to virtual machines and SQL databases in other clouds or on-premises, deploy Azure Arc and enable Azure Defender. Azure Arc for servers is a free service, but services used on Arc enabled servers, such as Azure Defender, will be charged as per the pricing for that service. Learn more in Add non-Azure machines with Azure Arc.

Azure Defender security alerts

When Azure Defender detects a threat in any area of your environment, it generates a security alert. These alerts describe details of the affected resources, suggested remediation steps, and in some cases, an option to trigger a logic app in response.

Whether an alert is generated by Security Center or received by Security Center from an integrated security product, you can export it. To export your alerts to Azure Sentinel, any third-party SIEM, or any other external tool, follow the instructions in Stream alerts to a SIEM, SOAR, or IT Service Management solution.

Azure Defender advanced protection capabilities

Azure Defender uses advanced analytics for tailored recommendations related to your resources.

Protections include securing the management ports of your VMs with just-in-time access and adaptive application controls to create allow lists for what apps should and shouldn't run on your machines.

Use the advanced protection tiles in the Azure Defender dashboard to monitor and configure each of these protections.

Vulnerability assessment and management

Azure Defender includes vulnerability scanning for your virtual machines and container registries at no extra cost. The scanners are powered by Qualys, but you don't need a Qualys license or even a Qualys account - everything's handled seamlessly inside Security Center.

Review the findings from these vulnerability scanners and respond to them all from within Security Center. This brings Security Center closer to being the single pane of glass for all of your cloud security efforts.

Explain Azure Security Center

To start with Azure Defender, you need to start with Azure Security Center.

Azure Security Center is a unified infrastructure security management system that strengthens the security posture of your data centers and provides advanced threat protection across your hybrid workloads in the cloud - whether they're in Azure or not - and on-premises.

Keeping your resources safe is a joint effort between your cloud provider, Azure, and you, the customer. You have to make sure your workloads are secure as you move to the cloud. At the same time, when you move to IaaS (infrastructure as a service), there is more customer responsibility than there was in PaaS (platform as a service) and SaaS (software as a service). Azure Security Center provides you the tools needed to harden your network, secure your services, and make sure you're on top of your security posture.

Azure Security Center addresses the three most urgent security challenges:

- **Rapidly changing workloads** – It's both a strength and a challenge of the cloud. On the one hand, end users are empowered to do more. On the other, how do you make sure that the ever-changing services people are using and creating are up to your security standards and follow security best practices?
- **Increasingly sophisticated attacks** - Wherever you run your workloads, the attacks keep getting more sophisticated. You have to secure your public cloud workloads, which are, in effect, an Internet facing workload that can leave you even more vulnerable if you don't follow security best practices.
- **Security skills are in short supply** - The number of security alerts and alerting systems far outnumbers the number of administrators with the necessary background and experience to make sure your environments are protected. Staying up to date with the latest attacks is a constant challenge, making it impossible to stay in place while the world of security is an ever-changing front.

To help you protect yourself against these challenges, Security Center provides you with the tools to:

- Strengthen security posture: Security Center assesses your environment and enables you to understand the status of your resources and whether they are secure.
- Protect against threats: Security Center assesses your workloads and raises threat prevention recommendations and security alerts.
- Get secure faster: In Security Center, everything is done in cloud speed. Because it is natively integrated, deployment of Security Center is easy, providing you with autoprotection and protection with Azure services.

Architecture

Because Security Center is natively part of Azure, PaaS services in Azure - including Service Fabric, SQL Database, SQL Managed Instance, and storage accounts - are monitored and protected by Security Center without necessitating any deployment.

In addition, Security Center protects non-Azure servers and virtual machines in the cloud or on-premises, for both Windows and Linux servers, by installing the Log Analytics agent on them. Azure virtual machines are autoprotected in Security Center.

The events collected from the agents and Azure are correlated in the security analytics engine to provide you tailored recommendations (hardening tasks) that you should follow to ensure your workloads are secure. You should investigate such alerts as soon as possible to make sure malicious attacks aren't taking place on your workloads.

When you enable Security Center, the security policy built-in to Security Center is reflected in Azure Policy as a built-in initiative under the Security Center category. The built-in initiative is automatically assigned to all Security Center registered subscriptions (regardless of whether or not they have Azure Defender enabled). The built-in initiative contains only Audit policies. For more information about Security Center policies in Azure Policy, see [Working with security policies](#).

Strengthen security posture

Azure Security Center enables you to strengthen your security posture. This means it helps you identify and perform the hardening tasks recommended as security best practices and implement them across your machines, data services, and apps. This includes managing and enforcing your security policies and ensuring your Azure virtual machines, non-Azure servers, and Azure PaaS services are compliant. Security Center provides you with the tools you need to have a bird's eye view on your workloads, with focused visibility on your network security estate.

Manage organization security policy and compliance

It's a security basic to know and make sure your workloads are secure, and it starts with having tailored security policies in place. Because all the Security Center policies are built on top of Azure Policy controls, you're getting the full range and flexibility of a world-class policy solution. In Security Center, you can set your policies to run on management groups, across subscriptions, and even for a whole tenant.

 Policy Management

Choose a subscription or management group from the list below to perform the following tasks:

- View and edit the default ASC policy
- Add a custom policy
- Add regulatory compliance standards to your compliance dashboard

[Click here to learn more >](#)

16 MANAGEMENT GROUPS 40 SUBSCRIPTIONS

Search by name

Name

 72f988bf-86f1-41af-91ab-2d7cd011db47 (12 of 12 subscriptions)
>  BKG (1 of 1 subscriptions)
 CnAI Orchestration Service Public Corp prod (4 of 4 subscriptions)
 Demonstration (2 of 2 subscriptions)
 Contoso Hotels
 Contoso Hotels - Dev

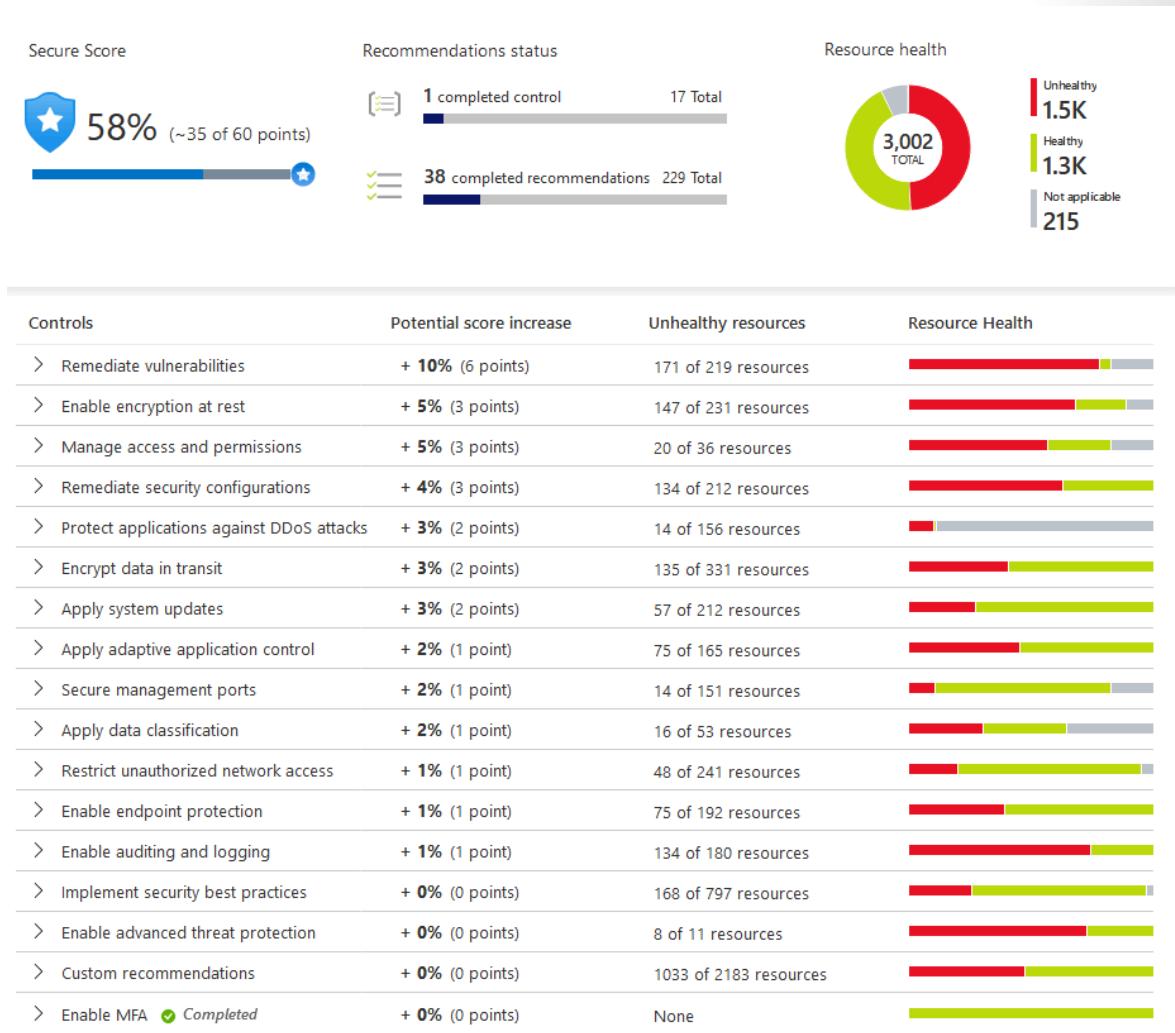
Security Center helps you identify Shadow IT subscriptions. By looking at subscriptions labeled not covered in your dashboard, you can immediately know when there are newly created subscriptions and make sure they are covered by your policies and protected by Azure Security Center.



Continuous assessments

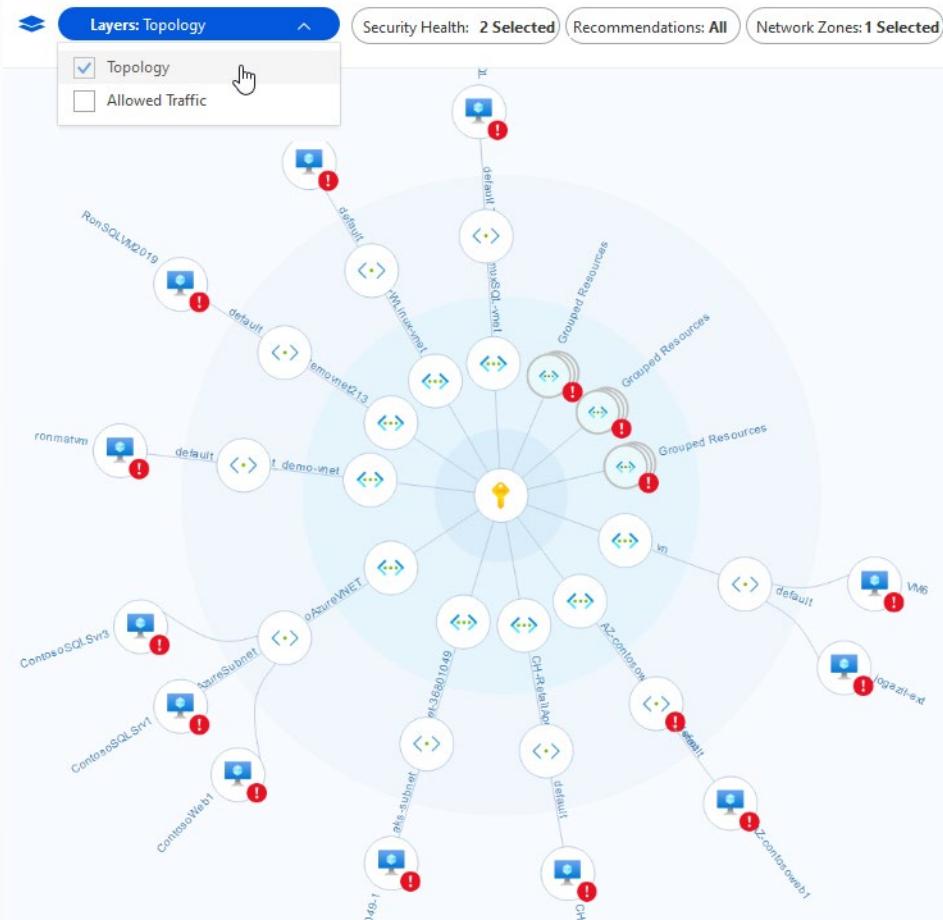
Security Center continuously discovers new resources being deployed across your workloads and assesses whether they are configured according to security best practices. If not, they're flagged, and you get a prioritized list of recommendations for what you need to fix in order to protect your machines.

To help you understand how important each recommendation is to your overall security posture, Security Center groups the recommendations into security controls and adds a secure score value to each control. This is crucial in enabling you to prioritize your security work.



Network map

One of the most powerful tools Security Center provides for continuously monitoring your network's security status is the Network map. The map enables you to see the topology of your workloads, so you can see if each node is properly configured. You can see how your nodes are connected, which helps you block unwanted connections that could potentially make it easier for an attacker to creep along your network.



Optimize and improve security by configuring recommended controls

The heart of Azure Security Center's value lies in its recommendations. The recommendations are tailored to the particular security concerns found on your workloads, and Security Center does the security admin work for you by not only finding your vulnerabilities but providing you with specific instructions for how to get rid of them.

In this way, Security Center enables you not just to set security policies but to apply secure configuration standards across your resources.

The recommendations help you to reduce the attack surface across each of your resources. That includes Azure virtual machines, non-Azure servers, and Azure PaaS services such as SQL and Storage accounts and more - where each type of resource is assessed differently and has its own standards.

Management ports of virtual machines should be protected with just-in-time network access control

×

Severity Freshness interval
High  24 Hours

^ **Description**
Azure Security Center has identified some overly-permissive inbound rules for management ports in your Network Security Group. Enable just-in-time access control to protect your VM from internet-based brute-force attacks. [Learn more.](#)

▼ **Remediation steps**

^ **Affected resources**

Unhealthy resources (3) Healthy resources (70) Not applicable resources (40)

Search virtual machines

<input type="checkbox"/> Name	↑↓ Subscription
<input type="checkbox"/> YVM	ASC DEMO
<input type="checkbox"/> vm1	ASC DEMO
<input type="checkbox"/> Barracuda	ASC DEMO

Protect against threats

Security Center's threat protection enables you to detect and prevent threats at the Infrastructure as a Service (IaaS) layer, non-Azure servers, and for Platforms as a Service (PaaS) in Azure.

Security Center's threat protection includes fusion kill-chain analysis, which automatically correlates alerts in your environment based on cyber kill-chain analysis, to help you better understand the full story of an attack campaign, where it started, and what kind of impact it had on your resources.

Integration with Microsoft Defender for Endpoint

Security Center includes automatic, native integration with Microsoft Defender for Endpoint. This means that without any configuration, your Windows and Linux machines are fully integrated with Security Center's recommendations and assessments.

In addition, Security Center lets you automate application control policies on server environments. The adaptive application controls in Security Center enable end-to-end app approval listing across your Windows servers. You don't need to create the rules and check violations. It's all done automatically for you.

Protect PaaS

Security Center helps you detect threats across Azure PaaS services. You can detect threats targeting Azure services, including Azure App Service, Azure SQL, Azure Storage Account, and more data services. You can also take advantage of the native integration with Microsoft Cloud App Security's User and Entity Behavioral Analytics (UEBA) to perform anomaly detection on your Azure activity logs.

Block brute force attacks

Security Center helps you limit exposure to brute force attacks. By reducing access to virtual machine ports, using the just-in-time VM access, you can harden your network by preventing unnecessary access. You can set secure access policies on selected ports for only authorized users, allowed source IP address ranges or IP addresses, and for a limited amount of time.

Protect data services

Security Center includes capabilities that help you perform automatic classification of your data in Azure SQL. You can also get assessments for potential vulnerabilities across Azure SQL and Storage services and recommendations for how to mitigate them.

Get secure faster

Native Azure integration (including Azure Policy and Azure Monitor logs) combined with seamless integration with other Microsoft security solutions, such as Microsoft Cloud App Security and Microsoft Defender for Endpoint, helps make sure your security solution is comprehensive and simple to onboard and roll out.

In addition, you can also extend the full solution beyond Azure to workloads running on other clouds and in on-premises data centers.

Automatically discover and onboard Azure resources with automatic provisioning

Security Center provides seamless, native integration with Azure and Azure resources. That means that you can pull together a complete security story involving Azure Policy and built-in Security Center policies across all your Azure resources and make sure that the whole thing is automatically applied to newly discovered resources as you create them in Azure.

Guided Demonstration - Azure Security Center

A guided demonstration is a recorded click-through simulation. You do not use your lab tenant for this demonstration. Instead simply click the link [here¹](#) to launch this demonstration. A focus will appear in the demonstration showing you the next place to click to advance the demonstration.

In this experience you will do the following:

1. Manage cloud security posture.
2. Protect against threats.
3. Get advanced insights.

Time required: 19 minutes

Enable Azure Defender

To enable Azure Defender, you first enable Azure Security Center, then Azure Defender, and finally configure your coverage type.

¹ <https://mslearn.cloudguides.com/guides/Protect%20your%20hybrid%20cloud%20with%20Azure%20Security%20Center>

Prerequisites

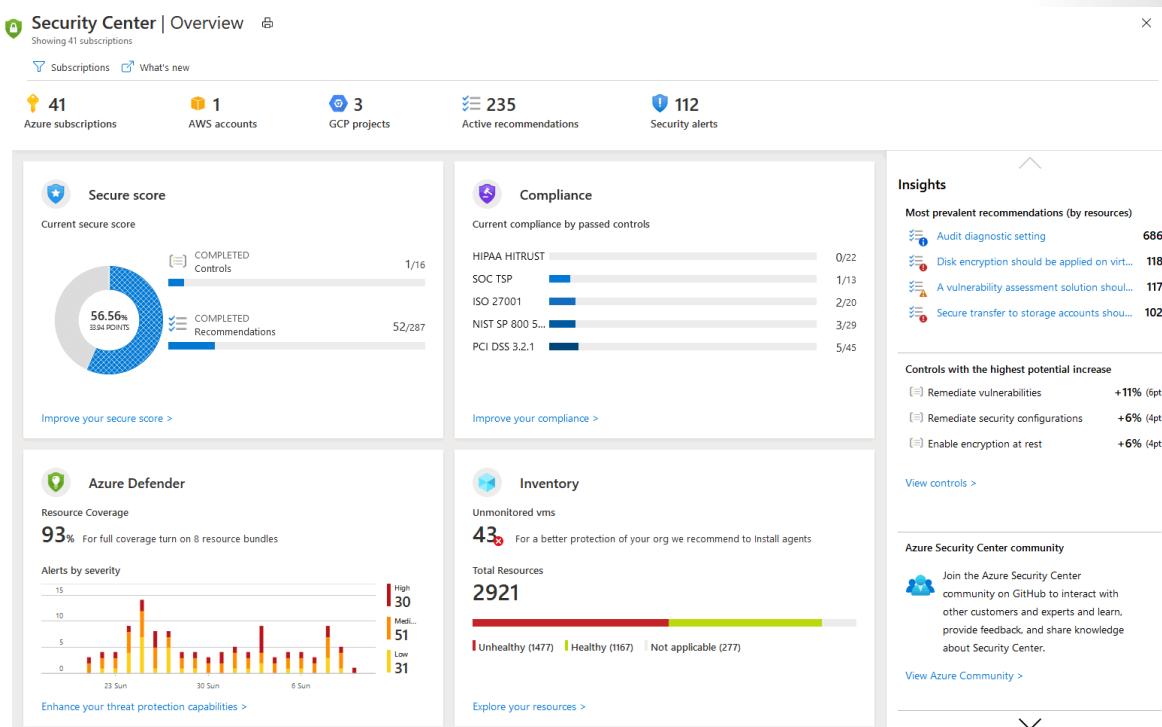
To get started with Security Center, you must have a subscription to Microsoft Azure. If you do not have a subscription, you can sign up for a free account. To enable Azure Defender on a subscription, you must be assigned the role of Subscription Owner, Subscription Contributor, or Security Admin.

Azure Security Center

To start Azure Security Center:

1. Sign in to the Azure portal.
2. From the portal's menu, select **Security Center**.

The Security Center's overview page opens.



Security Center – Overview provides a unified view into the security posture of your hybrid cloud workloads, enabling you to discover and assess the security of your workloads and identify and mitigate risk. Security Center automatically, at no cost, enables any of your Azure subscriptions not previously onboarded by you or another subscription user.

You can view and filter the list of subscriptions by selecting the Subscriptions menu item. Security Center will adjust the display to reflect the security posture of the selected subscriptions.

Within minutes of launching Security Center the first time, you might see:

- Recommendations for ways to improve the security of your connected resources.
- An inventory of your resources that are now being assessed by Security Center, along with the security posture of each.

To take full advantage of Security Center, you need to complete the steps below to enable Azure Defender and install the Log Analytics agent.

Azure Defender

From Security Center's sidebar, select Getting started:

The screenshot shows the Azure Security Center interface with the 'Getting started' section selected. At the top, there is a header with a cloud icon, the text 'Security Center | Getting started', and a 'Showing 41 subscriptions' message. Below the header are three navigation links: 'Upgrade' (underlined), 'Install Agents', and 'Get Started'. The main content area has a heading 'Enable Azure Defender on your subscriptions.' followed by a 'Get started with 30-day free trial' button and a brief description. Below this, there are three circular cards: 'Cloud security posture management' (with a shield icon), 'Cloud workload protection for machines' (with a laptop and padlock icon), and 'Advanced threat protection for PaaS' (with a binary code icon). Further down, there is a section titled 'Select workspaces to enable Azure Defender on' with a table listing workspaces. A red box highlights the first workspace, 'vademo'. To the right of the table is a summary box titled 'Total: 0 resources' containing a list of resource types and their counts. At the bottom of the page is a large blue 'Upgrade' button.

Name	Total resources	Azure Defender Plan
vademo	0	
TrafficWS	0	
Test100	0	
tddemo...	0	
samplecr...	0	
SQLBITS2...	0	
sqlauditin...	0	

Total: 0 resources

Resource Type	Count	Unit
0 machines	0	Server/Month
0 App service instances	0	Instance/Month
0 Azure SQL database servers	0	Server/Month
0 Storage accounts	0	10k transactions
0 Kubernetes cores	0	VM core/Month
0 Container registries	0	Image
0 Key Vaults (Preview)	0	10k transactions
0 SQL servers on machines (Preview)	0	

Upgrade

The Upgrade tab lists subscriptions and workspaces eligible for onboarding. To upgrade a workspace do the following:

1. From the Select workspaces to enable Azure Defender on list, select the workspaces to upgrade.
 - If you select subscriptions and workspaces that aren't eligible for trial, the next step will upgrade them, and charges will begin.
 - If you select a workspace that's eligible for a free trial, the next step will begin a trial.
2. Select **Upgrade** to enable Azure Defender.

You can protect an entire Azure subscription with Azure Defender, and all resources will inherit the protections within the subscription.

Below is the pricing page for an example subscription. You'll notice that each plan in Azure Defender is priced separately and can be individually set to on or off.

The screenshot shows the Microsoft Azure Security Center Settings page for Azure Defender plans. The left sidebar lists settings like Auto provisioning, Email notifications, Threat detection, Workflow automation, Continuous export, and Cloud connectors (Preview). The main content area has a heading 'Enable Azure Defender for enhanced security. Try it free for the first 30 days. Learn more >'. It compares 'Azure Defender off' (which is currently selected) and 'Azure Defender on'. Under 'Azure Defender off', features listed with green checkmarks are: Continuous assessment and security recommendations, Azure Secure Score, Just in time VM Access, Adaptive application controls and network hardening, Regulatory compliance dashboard and reports, Threat protection for Azure VMs and non-Azure servers (including Server EDR), and Threat protection for supported PaaS services. Features listed with red X marks are: Just in time VM Access, Adaptive application controls and network hardening, Regulatory compliance dashboard and reports, Threat protection for Azure VMs and non-Azure servers (including Server EDR), and Threat protection for supported PaaS services. Under 'Azure Defender on', features listed with green checkmarks are: Continuous assessment and security recommendations, Azure Secure Score, Just in time VM Access, Adaptive application controls and network hardening, Regulatory compliance dashboard and reports, Threat protection for Azure VMs and non-Azure servers (including Server EDR), and Threat protection for supported PaaS services. A note below says 'Azure Defender plan will apply to: 0 resources in this subscription'. At the bottom, there's a section to 'Select Azure Defender plan by resource type' with options for Servers, App Service, Azure SQL Database, and SQL servers on machines, each with an 'On' or 'Off' switch.

Explain cloud workload protections in Azure Defender

Lesson Introduction

Azure Defender brings advanced intelligent protection for your Azure and hybrid resources and workloads. Enabling Azure Defender provides a range of extra security features.

You are a Security Operations Analyst working at a company that is in the process of implementing cloud workload protection with Azure Defender.

You are the security operations team member working with the application and infrastructure teams designing the resource architecture for the new web application that uses containers and Azure SQL. You are responsible for ensuring the workloads are protected with Azure Defender and provide options for non-protected workloads.

Learn about the protections and detections provided by Azure Defender for each cloud workload.

Learning objectives

After completing this lesson, you should be able to:

- Explain which workloads are protected by Azure Defender
- Describe the benefits of the protections offered by Azure Defender
- Explain how Azure Defender protections function

Azure Defender for servers

Azure Defender for servers adds threat detection and advanced defenses for your Windows and Linux machines.

For Windows, Azure Defender integrates with Azure services to monitor and protect your Windows-based machines. Security Center presents the alerts and remediation suggestions from all of these services in an easy-to-use format.

For Linux, Azure Defender collects audit records from Linux machines by using auditd, one of the most common Linux auditing frameworks. auditd lives in the mainline kernel.

What are the benefits of Azure Defender for servers?

The threat detection and protection capabilities provided with Azure Defender for servers include:

- **Integrated license for Microsoft Defender for Endpoint (Windows only)** - Azure Defender for servers includes Microsoft Defender for Endpoint. Together, they provide comprehensive endpoint detection and response (EDR) capabilities.
 - When Defender for Endpoint detects a threat, it triggers an alert. The alert is shown in Security Center. From Security Center, you can also pivot to the Defender for Endpoint console and perform a detailed investigation to uncover the scope of the attack. Learn more about Microsoft Defender for Endpoint.
 - The Microsoft Defender for Endpoint sensor is automatically enabled on Windows servers that use Security Center.

- **Vulnerability assessment scanning for VMs** - The vulnerability scanner included with Azure Security Center is powered by Qualys.
 - Qualys' scanner is one of the leading tools for real-time identification of vulnerabilities in your Azure Virtual Machines. You don't need a Qualys license or even a Qualys account - everything's handled seamlessly inside Security Center.
- **Just-in-time (JIT) virtual machine (VM) access** - Threat actors actively hunt accessible machines with open management ports, like RDP or SSH. All of your virtual machines are potential targets for an attack. When a VM is successfully compromised, it's used as the entry point to attack further resources within your environment.
 - When you enable Azure Defender for servers, you can use just-in-time VM access to lock down the inbound traffic to your VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.
- **File integrity monitoring (FIM)** - File integrity monitoring (FIM), also known as change monitoring, examines files and registries of the operating system, application software, and others for changes that might indicate an attack. A comparison method is used to determine if the file's current state is different from the last scan of the file. You can use this comparison to determine if valid or suspicious modifications have been made to your files.
 - When you enable Azure Defender for servers, you can use FIM to validate the integrity of Windows files, your Windows registries, and Linux files.
- **Adaptive application controls (AAC)** - Adaptive application controls are an intelligent and automated solution for defining allow lists of known-safe applications for your machines.
 - When you've enabled and configured adaptive application controls, you'll get security alerts if any application runs other than the ones you've defined as safe.
- **Adaptive network hardening (ANH)** - Applying network security groups (NSG) to filter traffic to and from resources improves your network security posture. However, there can still be some cases in which the actual traffic flowing through the NSG is a subset of the NSG rules defined. In these cases, further improving the security posture can be achieved by hardening the NSG rules based on the actual traffic patterns.
 - Adaptive Network Hardening provides recommendations to further harden the NSG rules. It uses a machine learning algorithm that factors in actual traffic, known trusted configuration, threat intelligence, and other indicators of compromise. It then provides recommendations to allow traffic only from specific IP/port tuples.
- **Docker host hardening** - Azure Security Center identifies unmanaged containers hosted on IaaS Linux VMs, or other Linux machines running Docker containers. Security Center continuously assesses the configurations of these containers. It then compares them with the Center for Internet Security (CIS) Docker Benchmark. Security Center includes the entire ruleset of the CIS Docker Benchmark and alerts you if your containers don't satisfy any of the controls.
- **Fileless attack detection (Windows only)** - Fileless attacks inject malicious payloads into memory to avoid detection by disk-based scanning techniques. The attacker's payload then persists within the memory of compromised processes and performs a wide range of malicious activities.
 - With fileless attack detection, automated memory forensic techniques identify fileless attack toolkits, techniques, and behaviors. This solution periodically scans your machine at runtime, and extracts insights directly from the memory of processes. Specific insights include the identification of:
 - Well-known toolkits and crypto mining software

- Shellcode, a small piece of code typically used as the payload in the exploitation of a software vulnerability.
- Injected malicious executable in process memory
- Fileless attack detection generates detailed security alerts containing the descriptions with more process metadata, such as network activity. This accelerates alert triage, correlation, and downstream response time. This approach complements event-based EDR solutions and provides increased detection coverage.
- **Linux auditd alerts and Log Analytics agent integration (Linux only)** - The auditd system consists of a kernel-level subsystem responsible for monitoring system calls. It filters them by a specified rule set and writes messages for them to a socket. Security Center integrates functionalities from the auditd package within the Log Analytics agent to enable the collection of auditd events in all supported Linux distributions, without any prerequisites.
 - Auditd records are collected, enriched, and aggregated into events by using the Log Analytics agent for Linux agent. Security Center continuously adds new analytics that use Linux signals to detect malicious behaviors on cloud and on-premises Linux machines. Similar to Windows capabilities, these analytics span across suspicious processes, dubious sign-in attempts, kernel module loading, and other activities. These activities can indicate a machine is either under attack or has been breached.

Azure Defender for app service

Azure App Service is a fully managed platform for building and hosting your web apps and APIs without worrying about having to manage the infrastructure. It provides management, monitoring, and operational insights to meet enterprise-grade performance, security, and compliance requirements. For more information, see Azure App Service.

Azure Defender for App Service uses the scale of the cloud to identify attacks targeting applications running over App Service. Attackers probe web applications to find and exploit weaknesses. Before being routed to specific environments, requests to applications running in Azure go through several gateways, where they're inspected and logged. This data is then used to identify exploits and attackers and learn new patterns that will be used later.

By using the visibility that Azure has as a cloud provider, Security Center analyzes App Service internal logs to identify attack methodology on multiple targets. For example, methodology includes widespread scanning and distributed attacks. This type of attack typically comes from a small subset of IPs and shows patterns of crawling to similar endpoints on multiple hosts. The attacks are searching for a vulnerable page or plugin and can't be identified from the standpoint of a single host.

What does Azure Defender for App Service protect?

With the App Service plan enabled, Security Center assesses the resources covered by your App Service plan and generates security recommendations based on its findings. Security Center protects the VM instance in which your App Service is running and the management interface. It also monitors requests and responses sent to and from your apps running in App Service.

If you're running a Windows-based App Service plan, Security Center also has access to the underlying sandboxes and VMs. Together with the log data mentioned above, the infrastructure can tell the story, from a new attack circulating in the wild to compromises in customer machines. Therefore, even if Security Center is deployed after a web app has been exploited, it might be able to detect ongoing attacks.

Protect your Azure App Service web apps and APIs

To protect your Azure App Service plan with Azure Defender for App Service:

- Ensure you have a supported App Service plan that is associated with dedicated machines. Supported plans are listed above in Availability.
- Enable Azure Defender on your subscription (you can optionally enable only the Azure Defender for App Service plan).

Security Center is natively integrated with App Service, eliminating the need for deployment and on-boarding - the integration is transparent.

Azure Defender for Storage

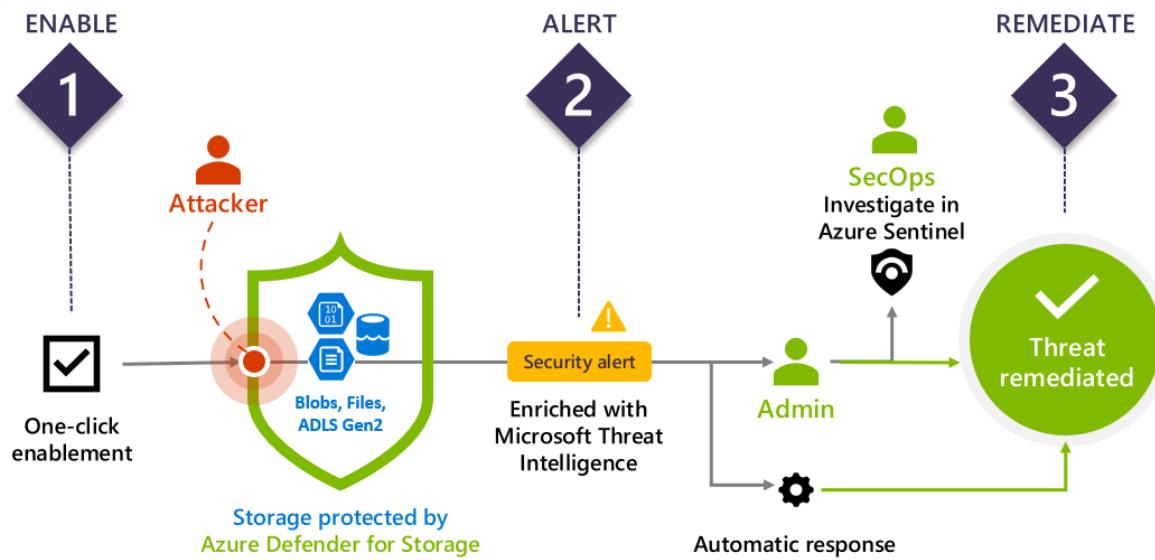
Azure Defender for Storage is an Azure-native layer of security intelligence that detects unusual and potentially harmful attempts to access or exploit your storage accounts. It utilizes the advanced capabilities of security AI and Microsoft Threat Intelligence to provide contextual security alerts and recommendations.

Security alerts are triggered when anomalies in activity occur. These alerts are integrated with Azure Security Center and sent via email to subscription administrators with details of suspicious activity and recommendations on how to investigate and remediate threats.

What are the benefits of Azure Defender for Storage?

Azure Defender for Storage provides:

- **Azure-native security** - With 1-click enablement, Defender for Storage protects data stored in Azure Blob, Azure Files, and Data Lakes. As an Azure-native service, Defender for Storage provides centralized security across all data assets managed by Azure and is integrated with other Azure security services such as Azure Sentinel.
- **Rich detection suite** - Powered by Microsoft Threat Intelligence, the detections in Defender for Storage cover the top storage threats such as anonymous access, compromised credentials, social engineering, privilege abuse, and malicious content.
- **Response at scale** - Security Center's automation tools make it easier to prevent and respond to identified threats. Learn more in Automate responses to Security Center triggers.



What kind of alerts does Azure Defender for Storage provide?

Security alerts are triggered when there's:

- **Suspicious access patterns** - such as successful access from a Tor exit node or from an IP considered suspicious by Microsoft Threat Intelligence
- **Suspicious activities** - such as anomalous data extraction or unusual change of access permissions
- **Uploads of malicious content** - such as potential malware files (based on hash reputation analysis) or hosting of phishing content

Alerts include details of the incident that triggered them, and recommendations on how to investigate and remediate threats. Alerts can be exported to Azure Sentinel or any other third-party SIEM or any other external tool.

What is hash reputation analysis for malware?

To determine whether an uploaded file is suspicious, Azure Defender for Storage uses hash reputation analysis supported by Microsoft Threat Intelligence. The threat protection tools don't scan the uploaded files. Rather they examine the storage logs and compare the hashes of newly uploaded files with those of known viruses, trojans, spyware, and ransomware.

When a file is suspected of containing malware, Security Center displays an alert and can optionally email the storage owner for approval to delete the suspicious file. To set up this automatic removal of files containing malware indicated by hash reputation analysis, deploy a workflow automation to trigger on alerts containing "Potential malware uploaded to a storage account".

Azure Defender for SQL

Azure Defender for SQL includes two Azure Defender plans that extend Azure Security Center's data security package to secure your databases and their data wherever they're located.

What does Azure Defender for SQL protect?

Azure Defender for SQL comprises two separate Azure Defender plans:

- **Azure Defender for Azure SQL database servers** protects:
 - Azure SQL Database
 - Azure SQL Managed Instance
 - Dedicated SQL pool in Azure Synapse
- **Azure Defender for SQL servers on machines** extends the protections for your Azure-native SQL Servers to fully support hybrid environments and protect SQL servers (all supported version) hosted in Azure, other cloud environments, and even on-premises machines:
 - SQL Server on Virtual Machines
 - On-premises SQL servers:
 - Azure Arc enabled SQL Server (preview)
 - SQL Server running on Windows machines without Azure Arc

What are the benefits of Azure Defender for SQL?

These two plans include functionality for identifying and mitigating potential database vulnerabilities and detecting anomalous activities that could indicate threats to your databases:

- Vulnerability assessment - The scanning service to discover, track, and help you remediate potential database vulnerabilities. Assessment scans provide an overview of your SQL machines' security state and details of any security findings.
- Advanced threat protection - The detection service that continuously monitors your SQL servers for threats such as SQL injection, brute-force attacks, and privilege abuse. This service provides action-oriented security alerts in Azure Security Center with details of the suspicious activity, guidance on how to mitigate the threats and options for continuing your investigations with Azure Sentinel.
- What kind of alerts does Azure Defender for SQL provide?

Threat intelligence enriched security alerts are triggered when there's:

- **Potential SQL injection attacks** - including vulnerabilities detected when applications generate a faulty SQL statement in the database
- **Anomalous database access and query patterns** - for example, an abnormally high number of failed sign-in attempts with different credentials (a brute force attempt)
- **Suspicious database activity** - for example, a legitimate user accessing a SQL Server from a breached computer that communicated with a crypto-mining C&C server

Alerts include details of the incident that triggered them, and recommendations on how to investigate and remediate threats.

Azure Defender for Key Vault

Azure Key Vault is a cloud service that safeguards encryption keys and secrets like certificates, connection strings, and passwords.

Enable Azure Defender for Key Vault for Azure-native, advanced threat protection for Azure Key Vault, providing an extra layer of security intelligence.

What are the benefits of Azure Defender for Key Vault?

Azure Defender detects unusual and potentially harmful attempts to access or exploit Key Vault accounts. This layer of protection allows you to address threats without being a security expert and without the need to manage third-party security monitoring systems.

When anomalous activities occur, Azure Defender shows alerts and optionally sends them via email to relevant members of your organization. These alerts include the details of the suspicious activity and recommendations on how to investigate and remediate threats.

Azure Defender for Key Vault alerts

When you get an alert from Azure Defender for Key Vault, we recommend investigating and responding to the alert as described in Respond to Azure Defender for Key Vault. Azure Defender for Key Vault protects applications and credentials, so even if you're familiar with the application or user that triggered the alert, it's important to check the situation surrounding every alert.

The alerts appear on Key Vault's Security page, the Azure Defender dashboard, and Security Center's alerts page.

Azure Defender for Resource Manager

Azure Resource Manager is the deployment and management service for Azure. It provides a management layer that enables you to create, update, and delete resources in your Azure account. You use management features, like access control, locks, and tags, to secure and organize your resources after deployment.

The cloud management layer is a crucial service connected to all your cloud resources. Because of this, it is also a potential target for attackers. So, we recommend security operations teams monitor the resource management layer closely.

Azure Defender for Resource Manager automatically monitors the resource management operations in your organization, whether they're performed through the Azure portal, Azure REST APIs, Azure CLI, or other Azure programmatic clients. Azure Defender runs advanced security analytics to detect threats and alert you about suspicious activity.

What are the benefits of Azure Defender for Resource Manager?

Azure Defender for Resource Manager protects against issues including:

- **Suspicious resource management operations**, such as operations from suspicious IP addresses, disabling antimalware and suspicious scripts running in VM extensions
- **Use of exploitation toolkits** like Microburst or PowerZure
- **Lateral movement** from the Azure management layer to the Azure resources data plane

How to investigate alerts from Azure Defender for Resource Manager

Security alerts from Azure Defender for Resource Manager are based on threats detected by monitoring Azure Resource Manager operations. Azure Defender uses internal log sources of Azure Resource

Manager and Azure Activity log, a platform sign in Azure that provides insight into subscription-level events.

To investigate security alerts from Azure Defender for Resource Manager:

1. Open Azure Activity log.
2. Filter the events to:
 - The subscription mentioned in the alert
 - The timeframe of the detected activity
 - The related user account (if relevant)
3. Look for suspicious activities.

Azure Defender for DNS

Azure DNS is a hosting service for DNS domains that provides name resolution by using Microsoft Azure infrastructure. By hosting your domains in Azure, you can manage your DNS records by using the same credentials, APIs, tools, and billing as your other Azure services.

Azure Defender for DNS provides an extra layer of protection for your cloud resources by:

- Continuously monitoring all DNS queries from your Azure resources
- Running advanced security analytics to alert you about suspicious activity

What are the benefits of Azure Defender for DNS?

Azure Defender for DNS protects against issues including:

- Data exfiltration from your Azure resources using DNS tunneling
- Malware communicating with C&C server
- Communication with malicious domains as phishing and crypto mining
- DNS attacks - communication with malicious DNS resolvers

Azure Defender for Kubernetes

Azure Kubernetes Service (AKS) is Microsoft's managed service for developing, deploying, and managing containerized applications.

Azure Security Center and AKS form the best cloud-native Kubernetes security offering, and together they provide environment hardening, workload protection, and runtime protection as outlined below.

For threat detection for your Kubernetes clusters, enable Azure Defender for Kubernetes. Host-level threat detection for your Linux AKS nodes is available if you enable Azure Defender for servers.

What are the benefits of Azure Defender for Kubernetes?

Through continuous analysis of the following AKS sources, Security Center provides real-time threat protection for your containerized environments and generates alerts for threats and malicious activity detected at the host and AKS cluster level. You can use this information to quickly remediate security issues and improve the security of your containers.

Security Center provides threat protection at different levels:

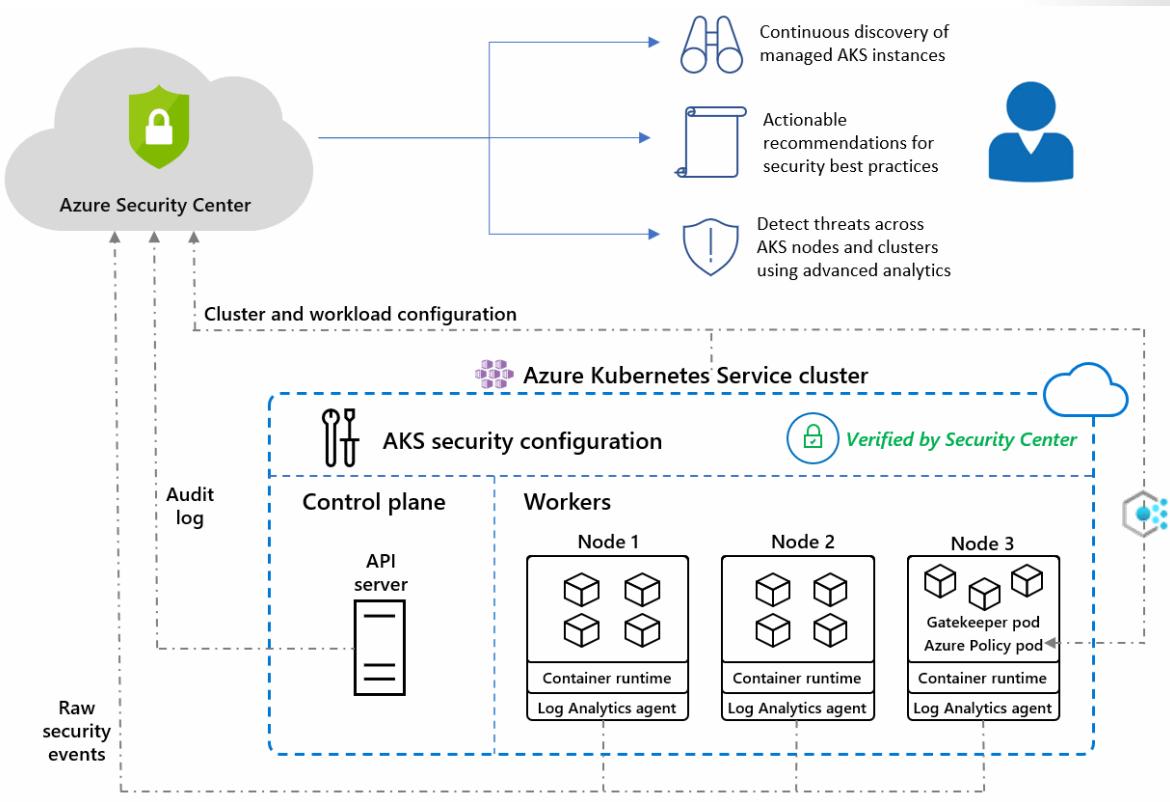
- **Host level (provided by Azure Defender for servers)** - Using the same Log Analytics agent that Security Center uses on other VMs, Azure Defender monitors your Linux AKS nodes for suspicious activities, such as web shell detection and connection with known suspicious IP addresses. The agent also monitors for container-specific analytics such as privileged container creation, suspicious access to API servers, and Secure Shell (SSH) servers running inside a Docker container.
- If you choose not to install the agents on your hosts, you will only receive a subset of the threat protection benefits and security alerts. You'll still receive alerts related to network analysis and communications with malicious servers.
- **AKS cluster level (provided by Azure Defender for Kubernetes)** - At the cluster level, the threat protection is based on analyzing Kubernetes' audit logs. To enable this agentless monitoring, enable Azure Defender. To generate alerts at this level, Security Center monitors your AKS-managed services using the logs retrieved by AKS. Examples of events at this level include exposed Kubernetes dashboards, creation of high privileged roles, and creation of sensitive mounts.

How does Security Center's Kubernetes protection work?

Below is a high-level diagram of the interaction between Azure Security Center, Azure Kubernetes Service, and Azure Policy.

You can see that the items received and analyzed by Security Center include:

- audit logs from the API server
- raw security events from the Log Analytics agent
- cluster configuration information from the AKS cluster
- workload configuration from Azure Policy (via the Azure Policy add-on for Kubernetes)



Azure Defender for container registries

Azure Container Registry (ACR) is a managed, private Docker registry service that stores and manages your container images for Azure deployments in a central registry. It's based on the open-source Docker Registry 2.0.

To protect all the Azure Resource Manager based registries in your subscription, enable Azure Defender for container registries at the subscription level. Security Center will then scan images that are pushed to the registry, imported into the registry, or any images pulled within the last 30 days. This feature is charged per image.

What are the benefits of Azure Defender for container registries?

Security Center identifies Azure Resource Manager based ACR registries in your subscription and seamlessly provides Azure-native vulnerability assessment and management for your registry's images.

Azure Defender for container registries includes a vulnerability scanner to scan the images in your Azure Resource Manager-based Azure Container Registry registries and provide deeper visibility into your images' vulnerabilities. The integrated scanner is powered by Qualys, the industry-leading vulnerability scanning vendor.

When issues are found by Qualys or Security Center, you'll get notified in the Security Center dashboard. Security Center provides actionable recommendations for every vulnerability, along with a severity classification and guidance for how to remediate the issue. For details of Security Center's recommendations for containers,

Security Center filters and classifies findings from the scanner. When an image is healthy, Security Center marks it as such. Security Center generates security recommendations only for images that have issues to be resolved. Security Center provides details of each reported vulnerability and a severity classification. Additionally, it gives guidance on how to remediate the specific vulnerabilities found in each image.

By only notifying when there are problems, Security Center reduces the potential for unwanted informational alerts.

When are images scanned?

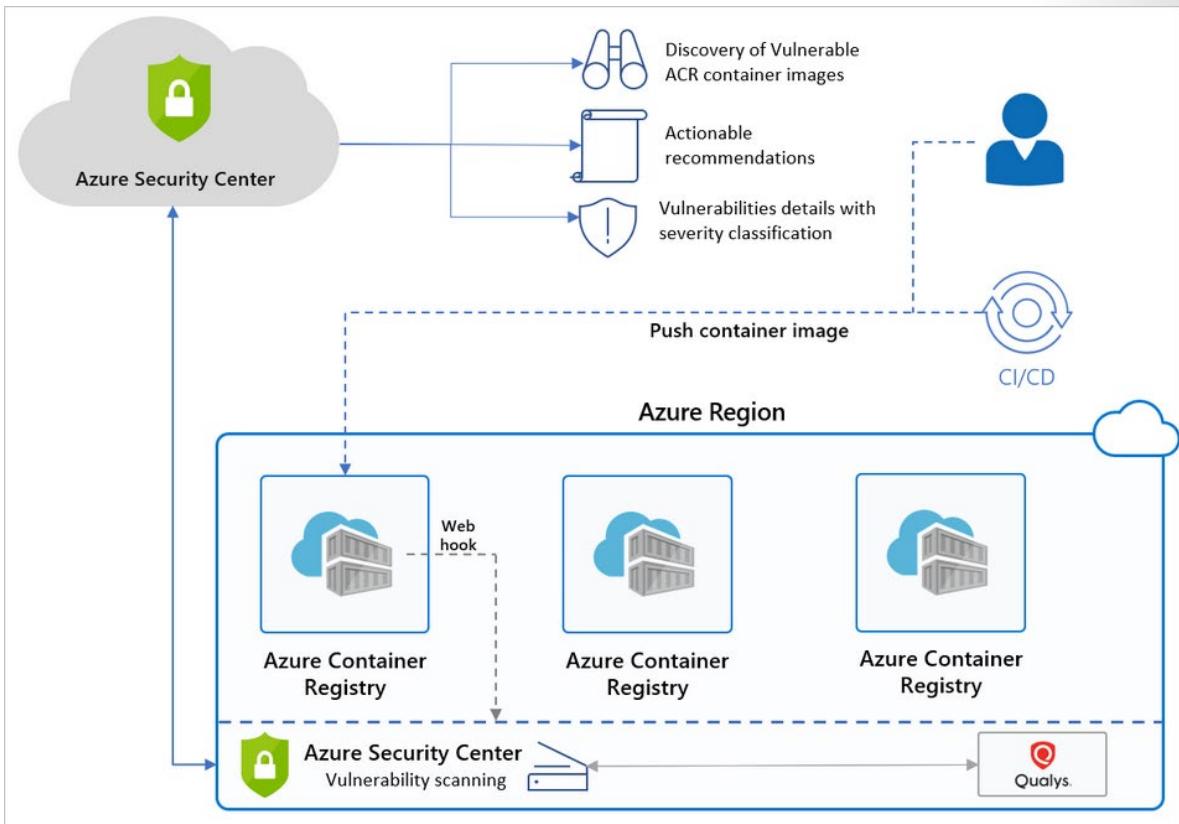
There are three triggers for an image scan:

- **On push** - Whenever an image is pushed to your registry, Security Center automatically scans that image. To trigger the scan of an image, push it to your repository.
- **Recently pulled** - Since new vulnerabilities are discovered every day, Azure Defender for container registries also scans any image that has been pulled within the last 30 days. There's no additional charge for a rescan; as mentioned above, you're billed once per image.
- **On import** - Azure Container Registry has import tools to bring images to your registry from Docker Hub, Microsoft Container Registry, or another Azure container registry. Azure Defender for container registries scans any supported images you import.

The scan typically completes within 2 minutes, but it might take up to 15 minutes. Findings are made available as Security Center recommendations.

How does Security Center work with Azure Container Registry

Below is a high-level diagram of the components and benefits of protecting your registries with Security Center.



Threat protection for Azure network layer

Security Center network-layer analytics are based on sample IPFIX data, which are packet headers collected by Azure core routers. Based on this data feed, Security Center uses machine learning models to identify and flag malicious traffic activities. Security Center also uses the Microsoft Threat Intelligence database to enrich IP addresses.

Some network configurations restrict Security Center from generating alerts on suspicious network activity. For Security Center to generate network alerts, ensure that:

- Your virtual machine has a public IP address (or is on a load balancer with a public IP address).
- Your virtual machine's network egress traffic isn't blocked by an external IDS solution.

Threat protection for Azure Cosmos DB

The Azure Cosmos DB alerts are generated by unusual and potentially harmful attempts to access or exploit Azure Cosmos DB accounts.

Threat protection for Azure WAF

Azure Application Gateway offers a web application firewall (WAF) that provides centralized protection of your web applications from common exploits and vulnerabilities. Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities. The Application Gateway WAF is based on Core Rule Set 3.0 or 2.2.9 from the Open Web Application Security Project. The WAF is updated automatically to protect against new vulnerabilities.

If you have a license for Azure WAF, your WAF alerts are streamed to Security Center with no extra configuration needed.

Threat protection for Azure DDoS Protection

Distributed denial of service (DDoS) attacks are known to be easy to execute. They've become a great security concern, particularly if you're moving your applications to the cloud. A DDoS attack attempts to exhaust an application's resources, making the application unavailable to legitimate users. DDoS attacks can target any endpoint that can be reached through the internet. To defend against DDoS attacks, purchase a license for Azure DDoS Protection and ensure you're following application design best practices. DDoS Protection provides different service tiers.

Connect Azure assets to Azure Defender

Lesson Introduction

Resource protection in Azure Defender can be automatically configured with autoprovisioning or may be manually deployed.

You are a Security Operations Analyst working at a company that is implementing cloud workload protection with Azure Defender. Your job is to ensure Azure Defender automatically protects the Azure resources.

Your organization has a few Azure virtual machines that are not part of the autoprovisioning scheme. you must manually configure protection for these Azure resources.

Learn how to connect your various Azure assets to Azure Defender to detect threats.

Learning objectives

After completing this lesson, you should be able to:

- Explore Azure assets
- Configure auto-provisioning in Azure Defender
- Describe manual provisioning in Azure Defender

Explore and manage your resources with asset inventory

The asset inventory page of Azure Security Center provides a single page for viewing the security posture of the resources you've connected to Security Center.

Security Center periodically analyzes the security state of your Azure resources to identify potential security vulnerabilities. It then provides you with recommendations on how to remediate those vulnerabilities.

When any resource has outstanding recommendations, they'll appear in the inventory.

Use this view and its filters to address such questions as:

- Which of my subscriptions with Azure Defender enabled have outstanding recommendations?
- Which of my machines with the tag 'Production' are missing the Log Analytics agent?
- How many of my machines tagged with a specific tag have outstanding recommendations?
- How many resources in a specific resource group have security findings from a vulnerability assessment service?

The asset management possibilities for this tool are substantial and continue to grow.

Key features of asset inventory

The inventory page provides the following tools:

- **Summaries** - Before you define any filters, a prominent strip of values at the top of the inventory view shows:
 - Total resources: The total number of resources connected to Security Center.

- Unhealthy resources: Resources with active security recommendations. Learn more about security recommendations.
- Unmonitored resources: Resources with agent monitoring issues - they have the Log Analytics agent deployed, but the agent isn't sending data or has other health issues.
- **Filters** - The multiple filters at the top of the page provide a way to quickly refine the list of resources according to the question you're trying to answer. For example, if you wanted to answer the question: Which of my machines with the tag 'Production' are missing the Log Analytics agent?
- As soon as you've applied filters, the summary values are updated to relate to the query results.
- Export options - Inventory provides the option to export the results of your selected filter options to a CSV file. You can also export the query itself to Azure Resource Graph Explorer to further refine, save, or modify the Kusto Query Language (KQL) query.
- Asset management options - Inventory lets you perform complex discovery queries. When you've found the resources that match your queries, inventory provides shortcuts for operations such as:
 - Assign tags to the filtered resources - select the checkboxes alongside the resources you want to tag.
 - Onboard new servers to Security Center - use the Add non-Azure servers toolbar button.
 - Automate workloads with Azure Logic Apps - use the Trigger Logic App button to run a logic app on one or more resources. Your logic apps have to be prepared in advance and accept the relevant trigger type (HTTP request).

How does asset inventory work?

Asset inventory utilizes Azure Resource Graph (ARG), an Azure service that provides the ability to query Security Center's security posture data across multiple subscriptions. ARG is designed to provide efficient resource exploration with the ability to query at scale. Using the Kusto Query Language (KQL), asset inventory can quickly produce deep insights by cross-referencing ASC data with other resource properties.

How to use asset inventory

- From Security Center's sidebar, select Inventory.
- Use the Filter by name box to display a specific resource, or use the filters as described below.
- Select the relevant options in the filters to create the specific query you want to perform.
- To use the Security findings contain filter, enter free text from the ID, security check, or CVE name of a vulnerability finding to filter to the affected resources:

The screenshot shows the Azure Security Center recommendations dashboard. At the top, it displays 'Unhealthy registries' (2/2), 'Severity' (High), and 'Total vulnerabilities' (131). A chart titled 'Vulnerabilities by severity' shows 33 High, 97 Medium, and 1 Low. Below this, there are sections for 'Description', 'Remediation steps', 'Affected resources', and 'Security Checks'. The 'Security Checks' section is expanded, showing a table of findings. The first two rows of the table are highlighted with a red border: 'ID' (176750) and 'Security Check' (Debian Security Update for apache2 (...)). The 'Affected resources' section on the right details the specific Debian update for systemd, including its ID (176875), category (Debian), and the fact that it applies to 5 of 12 scanned images.

ID	Security Check	Category	Applies To
176750	Debian Security Update for apache2 (...)	Debian	5 of 12 Scanned Images
176875	Debian Security Update for systemd	Debian	5 of 12 Scanned Images
176853	Debian Security Update for libssh2 (D...)	Debian	4 of 12 Scanned Images
177050	Debian Security Update for linux (DS...)	Debian	3 of 12 Scanned Images
177442	Debian Security Update for file (DSA ...)	Debian	3 of 12 Scanned Images
177260	Debian Security Update for linux (DS...)	Debian	3 of 12 Scanned Images

- To use the Azure Defender filter, select one or more options (Off, On, or Partial):
 - Off - Resources that aren't protected by an Azure Defender plan. You can right-click on any of these and upgrade them:
 - On - Resources that are protected by an Azure Defender plan
 - Partial - This applies to subscriptions that have some but not all of the Azure Defender plans disabled.

Configure auto provisioning

Security Center collects data from your Azure virtual machines (VMs), virtual machine scale sets, IaaS containers, and non-Azure (including on-premises) machines to monitor for security vulnerabilities and threats.

Data collection is required to provide visibility into missing updates, misconfigured OS security settings, endpoint protection status, and health and threat protection. Data collection is only needed for compute resources (VMs, virtual machine scale sets, IaaS containers, and non-Azure computers). You can benefit from Azure Security Center even if you don't provision agents; however, you will have limited security, and the capabilities listed above are not supported.

Data is collected using:

- The Log Analytics agent, which reads various security-related configurations and event logs from the machine and copies the data to your workspace for analysis. Examples of such data are operating system type and version, operating system logs (Windows event logs), running processes, machine name, IP addresses, and logged in user.
- Security extensions, such as the Azure Policy Add-on for Kubernetes, which can also provide data to Security Center regarding specialized resource types.

The screenshot shows the 'Auto provisioning - Extensions' section of the Azure Security Center settings. It includes a brief description of how Security Center collects security data and events from resources, and a button to 'Enable all extensions'. A table lists two extensions: 'Log Analytics agent for Azure VMs' and 'Policy Add-on for Kubernetes'. Both are currently set to 'On'. The Log Analytics agent extension is described as collecting security-related configurations and event logs from machines and storing them in a Log Analytics workspace for analysis. The Policy Add-on extension is described as extending Gatekeeper v3 to apply at-scale enforcements and safeguards on clusters. Configuration options for each extension are also visible.

Agent	Status	Resources missing agent	Description	Configuration
Log Analytics agent for Azure VMs	On	0 of 33 virtual machines	Collects security-related configurations and event logs from the machine and stores the data in your Log Analytics workspace for analysis. Learn more	Selected workspace: nsg Security events: Common Edit configurations
Policy Add-on for Kubernetes	On	1 of 1 managed cluster	Extends Gatekeeper v3, to apply at-scale enforcements and safeguards on your clusters in a centralized, consistent manner. Requires Kubernetes v1.14.0 or later. Learn more .	

Why use auto provisioning?

Any of the agents and extensions described on this page can be installed manually. However, auto provisioning reduces management overhead by installing all required agents and extensions on existing - and new - machines to ensure faster security coverage for all supported resources.

How does auto provisioning work?

Security Center's auto provisioning settings have a toggle for each type of supported extension. When you enable auto provisioning of an extension, you assign the appropriate Deploy if not exists policy to ensure that the extension is provisioned on all existing and future resources of that type.

Enable auto provisioning of the Log Analytics agent

When automatic provisioning is on for the Log Analytics agent, Security Center deploys the agent on all supported Azure VMs and any new ones created.

To enable auto provisioning of the Log Analytics agent:

1. From Security Center's menu, select **Pricing & settings**.
2. Select the relevant subscription.
3. In the Auto provisioning page, set the agent's status to **On**.
4. From the configuration options pane, define the workspace to use.

The screenshot shows the Azure Security Center Settings page with the 'Auto provisioning' extension selected. On the left, there's a sidebar with various settings like Azure Defender plans, Auto provisioning, Email notifications, Threat detection, Workflow automation, Continuous export, and Cloud connectors (Preview). The main area displays 'Auto provisioning - Extensions' with three listed: Log Analytics agent for Azure VMs (status: On), Microsoft Dependency agent (preview) (status: Off), and Policy Add-on for Kubernetes (status: Off). A blue button labeled 'Enable all extensions' is visible. To the right, a modal window titled 'Agent deployment configuration' is open, specifically for 'Log Analytics agent for virtual machines'. It has a section for 'Workspace configuration' where the user can choose to connect Azure VMs to the default workspace or a different workspace. The 'Connect Azure VMs to a different workspace' option is selected, and a dropdown menu shows 'NSGL' as the chosen workspace. Below this, there's a section for 'Store additional raw data - Windows security events' with options for 'All Events', 'Common' (selected), 'Minimal', and 'None'. The 'Common' option is described as a standard set of events for auditing purposes. At the bottom of the modal are 'Apply' and 'Cancel' buttons.

Connect Azure VMs to the default workspace(s) created by Security Center - Security Center creates a new resource group and default workspace in the same geolocation and connects the agent to that workspace. If a subscription contains VMs from multiple geolocations, Security Center creates multiple workspaces to ensure compliance with data privacy requirements.

The naming convention for the workspace and resource group is:

- Workspace: DefaultWorkspace-[subscription-ID]-[geo]
- Resource Group: DefaultResourceGroup-[geo]

Security Center automatically enables a Security Center solution on the workspace per the pricing tier set for the subscription.

Connect Azure VMs to a different workspace - From the dropdown list, select the workspace to store collected data. The dropdown list includes all workspaces across all of your subscriptions. You can use this option to collect data from virtual machines running in different subscriptions and store it all in your selected workspace.

If you already have an existing Log Analytics workspace, you might want to use the same workspace (requires read and write permissions on the workspace). This option is useful if you're using a centralized workspace in your organization and want to use it for security data collection. Learn more in Manage access to log data and workspaces in Azure Monitor.

If your selected workspace already has a Security or Security Center Free solution enabled, the pricing will be set automatically. If not, install a Security Center solution on the workspace:

1. From Security Center's menu, open Pricing & settings.
2. Select the workspace to which you'll be connecting the agents.
3. Select **Azure Defender on** or **Azure Defender off**.
4. From the Windows security events configuration, select the amount of raw event data to store:
 - None – Disable security event storage. This is the default setting.
 - Minimal – A small set of events for when you want to minimize the event volume.

- Common – A set of events that satisfies most customers and provides a full audit trail.
 - All events – For customers who want to make sure all events are stored.
5. Select **Apply** in the configuration pane.
6. Select **Save**. If a workspace needs to be provisioned, agent installation might take up to 25 minutes.

You'll be asked if you want to reconfigure monitored VMs that were previously connected to a default workspace:

- No - your new workspace settings will only be applied to newly discovered VMs that don't have the Log Analytics agent installed.
- Yes - your new workspace settings will apply to all VMs, and every VM currently connected to a Security Center created workspace will be reconnected to the new target workspace.

Enable auto provisioning of extensions

To enable automatic provisioning of an extension other than the Log Analytics agent:

1. From Security Center's menu in the Azure portal, select Pricing & settings.
2. Select the relevant subscription.
3. Select Auto provisioning.
4. If you're enabling auto provisioning for the Microsoft Dependency agent, ensure the Log Analytics agent is set to auto deploy too.
5. Toggle the status to On for the relevant extension.
6. Select **Save**. The Azure policy is assigned, and a remediation task is created.

Windows security event options for the Log Analytics agent

Selecting a data collection tier in Azure Security Center only affects the storage of security events in your Log Analytics workspace. The Log Analytics agent will still collect and analyze the security events required for Security Center's threat protection, regardless of the level of security events you choose to store in your workspace. Choosing to store security events enables investigation, search, and auditing of those events in your workspace.

Azure Defender is required for storing Windows security event data. Storing data in Log Analytics might incur more charges for data storage.

Information for Azure Sentinel users

The security events collection within the context of a single workspace can be configured from either Azure Security Center or Azure Sentinel, but not both. If you're planning to add Azure Sentinel to a workspace that is already getting alerts from Azure Security Center and is set to collect Security Events, you have two options:

- Leave the Security Events collection in Azure Security Center as is. You will be able to query and analyze these events in Azure Sentinel and Azure Defender. However, you will not be able to monitor the connector's connectivity status or change its configuration in Azure Sentinel. If this is important to you, consider the second option.

- Disable Security Events collection in Azure Security Center (by setting Windows security events to None in the configuration of your Log Analytics agent). Then add the Security Events connector in Azure Sentinel. As with the first option, you will be able to query and analyze events in both Azure Sentinel and Azure Defender/ASC, but you will now be able to monitor the connector's connectivity status or change its configuration in - and only in - Azure Sentinel.

What event types are stored for "Common" and "Minimal"?

These sets were designed to address typical scenarios. Make sure to evaluate which one fits your needs before implementing it.

To determine the events for the Common and Minimal options, we worked with customers and industry standards to learn about the unfiltered frequency of each event and their usage. We used the following guidelines in this process:

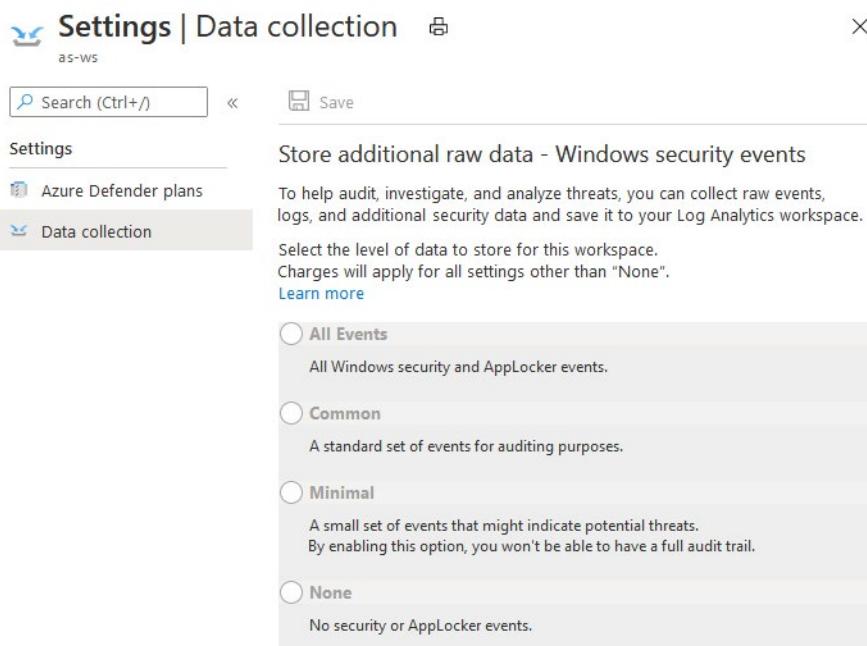
- Minimal - Make sure that this set covers only events that might indicate a successful breach and important events that have a low volume. For example, this set contains user successful and failed login (event IDs 4624, 4625), but it doesn't contain sign out, which is important for auditing but not meaningful for detection and has relatively high volume. Most of the data volume of this set is the login events and process creation event (event ID 4688).
- Common - Provide a full user audit trail in this set. For example, this set contains both user logins and user sign outs (event ID 4634). We include auditing actions like security group changes, key domain controller Kerberos operations, and other events that are recommended by industry organizations.

Events with very low volume were included in the Common set as the main motivation to choose it over all the events is to reduce the volume and not filter out specific events.

Setting the security event option at the workspace level

You can define the level of security event data to store at the workspace level.

- From Security Center's menu in the Azure portal, select Pricing & settings.
- Select the relevant workspace. The only data collection events for a workspace are the Windows security events described on this page.



- Select the amount of raw event data to store and select Save.

Manual log analytics agent provisioning

To manually install the Log Analytics agent:

1. Disable auto provisioning.
 2. Optionally, create a workspace.
 3. Enable Azure Defender on the workspace on which you're installing the Log Analytics agent:
 4. From Security Center's menu, select **Pricing & settings**.
 5. Set the workspace on which you're installing the agent. Make sure the workspace is in the same subscription you use in Security Center, and you have read/write permissions for the workspace.
 6. Select **Azure Defender on**, and **Save**.
- To deploy agents on new VMs using a Resource Manager template, install the Log Analytics agent:
 - **Install the Log Analytics agent for Windows²**
 - **Install the Log Analytics agent for Linux³**
 - To deploy agents on your existing VMs, follow the instructions in **Collect data about Azure Virtual Machines⁴**.
 - To use PowerShell to deploy the agents, use the instructions from the virtual machines documentation:
 - **For Windows machines⁵**

² <https://docs.microsoft.com/azure/virtual-machines/extensions/oms-windows?azure-portal=true>

³ <https://docs.microsoft.com/azure/virtual-machines/extensions/oms-linux?azure-portal=true>

⁴ <https://docs.microsoft.com/azure/azure-monitor/learn/quick-collect-azurerm?azure-portal=true>

⁵ <https://docs.microsoft.com/azure/virtual-machines/extensions/oms-windows?toc=/azure/azure-monitor/toc.json?azure-portal=true>

- **For Linux machines⁶**

⁶ <https://docs.microsoft.com/azure/virtual-machines/extensions/oms-linux?toc=/azure/azure-monitor/toc.json?azure-portal=true>

Connect non-Azure resources to Azure Defender

Lesson Introduction

Azure Defender can protect hybrid workloads, including on-premise, Amazon Web Services (AWS), and Google Cloud Platform (GCP).

You are a Security Operations Analyst working at a company that is in the process of implementing cloud workload protection with Azure Defender. You are responsible for protecting resources located on-premise, Amazon Web Services (AWS), and Google Cloud Platform (GCP). You decide to Azure Arc enable the servers to provide easier management of the non-Azure machines. Next, you protect the virtual machines with Azure Defender.

Learn how you can add Azure Defender capabilities to your hybrid environment.

Learning objectives

After completing this lesson, you should be able to:

- Connect non-Azure machines to Azure Defender
- Connect AWS accounts to Azure Defender
- Connect GCP accounts to Azure Defender

Protect non-Azure resources

In addition to defending your Azure environment, you can add Azure Defender capabilities to your hybrid environment to:

- Protect your non-Azure servers
- Protect your virtual machines in other clouds (such as AWS and GCP)
- Protect SQL databases

For machines, the Log Analytics agent is the only required technology. To provide more insights for security alerts, connecting other cloud providers (AWS, GCP) resources will provide cloud security posture management information.

Connect non-Azure machines

Security Center can monitor the security posture of your non-Azure computers, but first, you need to connect them to Azure.

You can connect your non-Azure computers in any of the following ways:

- Using Azure Arc enabled servers (recommended)
- From Security Center's pages in the Azure portal (Getting started and Inventory)

Add non-Azure machines with Azure Arc

Azure Arc enabled servers is the preferred way of adding your non-Azure machines to Azure Security Center. A machine with Azure Arc enabled servers becomes an Azure resource and appears in Security

Center with recommendations like your other Azure resources. In addition, Azure Arc enabled servers provides enhanced capabilities such as the option to enable guest configuration policies on the machine, deploy the Log Analytics agent as an extension, simplify deployment with other Azure services, and more.

What are Azure Arc enabled servers

Azure Arc enabled servers allows you to manage your Windows and Linux machines hosted outside of Azure, on your corporate network, or other cloud providers consistent with how you manage native Azure virtual machines. When a hybrid machine is connected to Azure, it becomes a connected machine and is treated as a resource in Azure. Each connected machine has a Resource ID, is included in a resource group, and benefits from standard Azure constructs such as Azure Policy and applying tags. Service providers who manage a customer's on-premises infrastructure can manage their hybrid machines, just like they do today with native Azure resources, across multiple customer environments, using Azure Lighthouse with Azure Arc.

To deliver this experience with your hybrid machines hosted outside of Azure, the Azure Connected Machine agent needs to be installed on each machine that you plan on connecting to Azure. **This agent does not deliver any other functionality, and it doesn't replace the Azure Log Analytics agent.** The Log Analytics agent for Windows and Linux is required when you want to proactively monitor the OS and workloads running on the machine, manage it using Automation runbooks or solutions like Update Management, or use other Azure services like Azure Security Center.

Add non-Azure machines from the Azure portal

You can start the process of adding a non-Azure server from two different locations in Security Center:

1. From Security Center's menu, open the Getting started page.
2. Select the **Get started** tab.
3. Below Add non-Azure servers, select **Configure**.
4. From Security Center's menu, open the Inventory page.
5. Select the **Add non-Azure servers** button.

A list of your Log Analytics workspaces is shown. The list includes, if applicable, the default workspace created for you by Security Center when automatic provisioning was enabled. Select this workspace or another workspace you want to use.

You can add computers to an existing workspace or create a new workspace. Optionally, to create a new workspace, select **Create new workspace**.

From the list of workspaces, select **Add Servers** for the relevant workspace. The Agents management page appears.

From here, choose the relevant procedure below depending on the type of machines you're onboarding:

- Onboard your Azure Stack VMs
- Onboard your Linux machines
- Onboard your Windows machines

Onboard your Azure Stack VMs

To add Azure Stack VMs, you need the information on the Agents management page and to configure the Azure Monitor, Update and Configuration Management virtual machine extension on the virtual machines running on your Azure Stack.

1. From the Agents management page, copy the Workspace ID and Primary Key into Notepad.
2. Log into your Azure Stack portal and open the Virtual machines page.
3. Select the virtual machine that you want to protect with Security Center.
4. Select Extensions. The list of virtual machine extensions installed on this virtual machine is shown.
5. Select the **Add** tab. The New Resource menu shows the list of available virtual machine extensions.
6. Select the Azure Monitor, Update and Configuration Management extension and select **Create**. The Install extension configuration page opens.
7. On the Install extension configuration page, paste the Workspace ID and Workspace Key (Primary Key) that you copied into Notepad in the previous step.
8. When you complete the configuration, select **OK**. The extension's status will show as *Provisioning Succeeded*. It might take up to one hour for the virtual machine to appear in Security Center.

Onboard your Linux machines

To add Linux machines, you need the WGET command from the Agents management page.

1. From the Agents management page, copy the WGET command into Notepad. Save this file to a location that is accessible from your Linux computer.
2. On your Linux computer, open the file with the WGET command. Select the entire content and copy and paste it into a terminal console.
3. When the installation completes, you can validate that the *omsagent* is installed by running the [pgrep] command. The command will return the omsagent PID. The logs for the Agent can be found at: /var/opt/microsoft/omsagent/workspace id/log/ It might take up to 30 minutes for the new Linux machine to appear in Security Center.

Onboard your Windows machines

To add Windows machines, you need to read the information on the Agents management page and to download the appropriate agent file (32/64-bit).

1. Select the Download Windows Agent link applicable to your computer processor type to download the setup file.
2. From the Agents management page, copy the Workspace ID and Primary Key into Notepad.
3. Copy the downloaded setup file to the target computer and run it.
4. Follow the installation wizard (Next, I Agree, Next, Next).
5. On the Azure Log Analytics page, paste the Workspace ID and Workspace Key (Primary Key) that you copied into Notepad.
6. If the computer should report to a Log Analytics workspace in Azure Government cloud, select **Azure US Government** from the Azure Cloud dropdown list.

7. If the computer needs to communicate through a proxy server to the Log Analytics service, select **Advanced** and provide the proxy server's URL and port number.
8. When you've entered all of the configuration settings, select **Next**.
9. From the Ready to Install page, review the settings to be applied and select **Install**.
10. On the Configuration completed successfully page, select **Finish**.

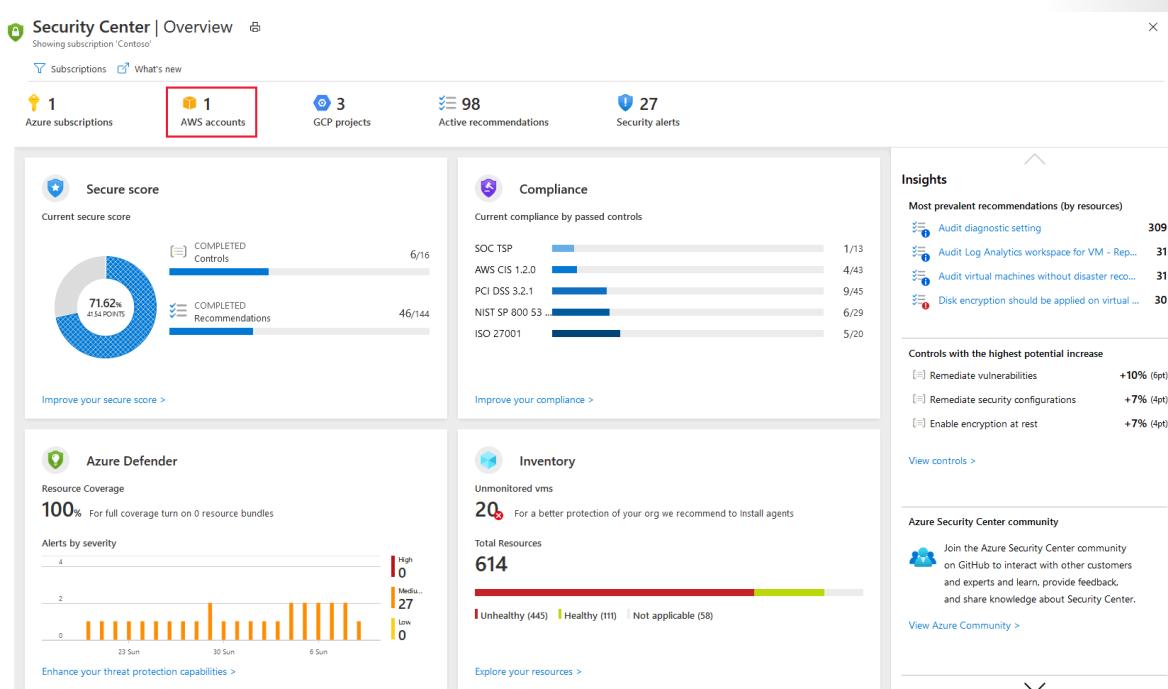
When complete, the Microsoft Monitoring agent appears in Control Panel. You can review your configuration there and verify that the agent is connected.

Connect AWS accounts

Onboarding your AWS account into Security Center, integrates AWS Security Hub and Azure Security Center. Security Center thus provides visibility and protection across both of these cloud environments to provide:

- Automatic agent provisioning (Security Center uses Azure Arc to deploy the Log Analytics agent to your AWS instances)
- Policy management
- Vulnerability management
- Embedded Endpoint Detection and Response (EDR)
- Detection of security misconfigurations
- A single view showing Security Center recommendations and AWS Security Hub findings
- Incorporation of your AWS resources into Security Center's secure score calculations
- Regulatory compliance assessments of your AWS resources

In the screenshot below, you can see AWS accounts displayed in Security Center's overview dashboard.



Follow the steps below to create your AWS cloud connector.

Set up AWS Security Hub:

To view security recommendations for multiple regions, repeat the following steps for each relevant region. If you're using an AWS master account, repeat the following three steps to configure the master account and all connected member accounts across all relevant regions

1. Enable AWS Config.
2. Enable AWS Security Hub.
3. Verify that there is data flowing to the Security Hub.

When you first enable Security Hub, it might take several hours for data to be available.

Set up authentication for Security Center in AWS

There are two ways to allow Security Center to authenticate to AWS:

- Create an IAM role for Security Center - This is the most secure method and is recommended
- AWS user for Security Center - A less secure option if you don't have IAM enabled

Create an IAM role for Security Center:

From your Amazon Web Services console, under Security, Identity & Compliance, select IAM.

1. Select **Roles** and Create role.
2. Select **Another AWS account**.
3. Enter the following details:
 - Account ID - enter the Microsoft Account ID (158177204117) as shown in the AWS connector page in Security Center.
 - Require External ID - should be selected
 - External ID - enter the subscription ID as shown in the AWS connector page in Security Center
4. Select **Next**.
5. In the Attach permission policies section, select the following policies:
 - SecurityAudit
 - AmazonSSMAutomationRole
 - AWSecurityHubReadOnlyAccess
6. Optionally add tags. Adding Tags to the user doesn't affect the connection.
7. Select **Next**.
8. In The Roles list, choose the role you created
9. Save the Amazon Resource Name (ARN) for later.

Configure the SSM Agent

AWS Systems Manager is required for automating tasks across your AWS resources. If your EC2 instances don't have the SSM Agent, follow the relevant instructions from Amazon:

Complete Azure Arc prerequisites

Make sure the appropriate Azure resources providers are registered:

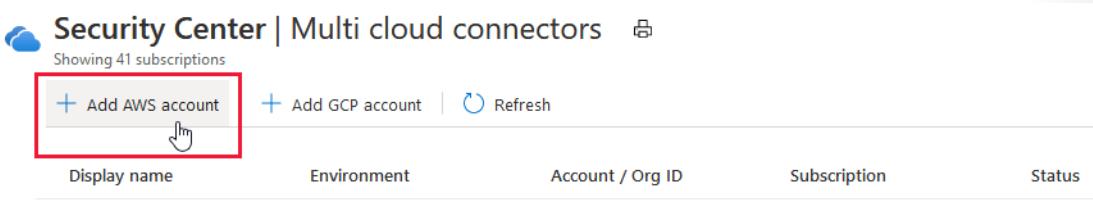
- Microsoft.HybridCompute
- Microsoft.GuestConfiguration

Create a Service Principal for onboarding at scale. As an Owner on the subscription you want to use for the onboarding, create a service principal for Azure Arc onboarding as described in Create a Service Principal for onboarding at scale.

Connect AWS to Security Center

From Security Center's menu, select Multi cloud connectors.

Select Add AWS account.



Configure the options in the AWS authentication tab:

1. Enter a Display name for the connector.
2. Confirm that the subscription is correct. It is the subscription that will include the connector and AWS Security Hub recommendations.
3. Depending on the authentication option, you chose in Step 2. Set up authentication for Security Center in AWS:
 - Select Assume Role and paste the ARN from Create an IAM role for Security Center. Pasting the ARN file in the relevant field of the AWS connection wizard in the Azure portal
or
 - Select Credentials and paste the access key and secret key from the .csv file you saved in Create an AWS user for Security Center.
4. Select **Next**.
5. Configure the options in the Azure Arc Configuration tab:
 - Security Center discovers the EC2 instances in the connected AWS account and uses SSM to onboard them to Azure Arc.
 - Select the Resource Group and Azure Region that the discovered AWS EC2s will be onboarded to in the selected subscription.

- Enter the Service Principal ID and Service Principal Client Secret for Azure Arc as described here [Create a Service Principal for onboarding at scale](#).
 - If the machine connects to the internet via a proxy server, specify the proxy server IP address or the name and port number that the machine uses to communicate with the proxy server.
6. Select **Review and create**.
 7. Review the summary information
 8. The Tags sections will list all Azure Tags that will be automatically created for each onboarded EC2 with its own relevant details to easily recognize it in Azure.

Confirmation

When the connector is successfully created and AWS Security Hub has been configured properly:

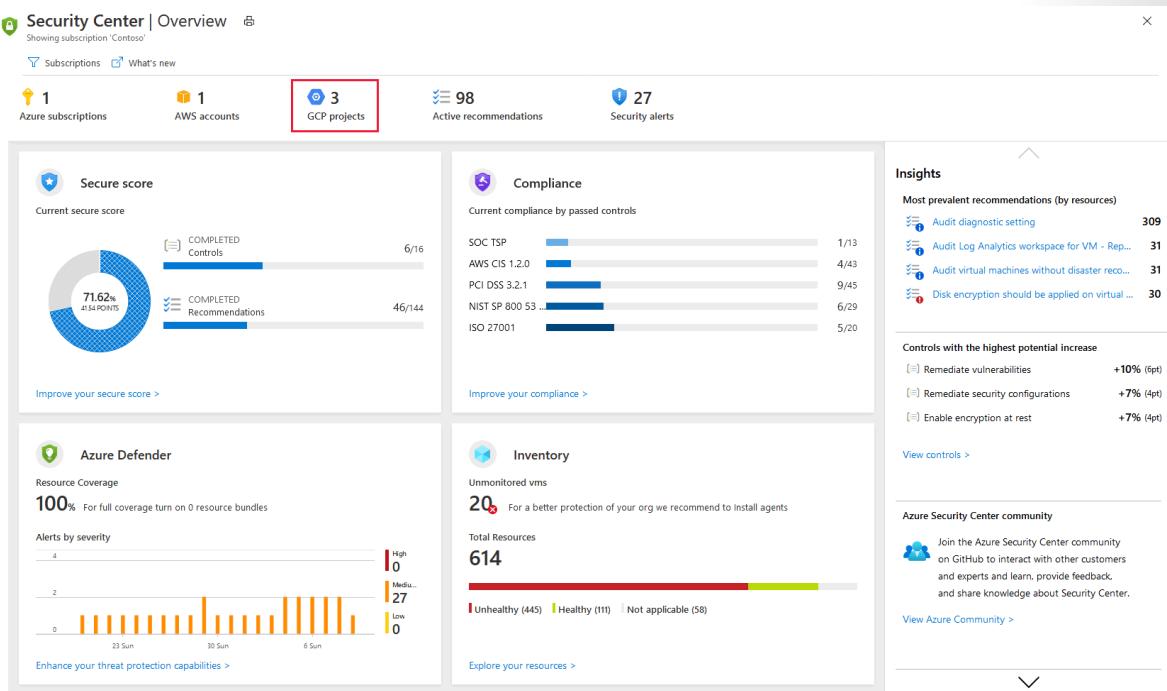
- Security Center scans the environment for AWS EC2 instances, onboarding them to Azure Arc, enabling it to install the Log Analytics agent and providing threat protection and security recommendations.
- The ASC service scans for new AWS EC2 instances every 6 hours and onboards them according to the configuration.
- The AWS CIS standard will be shown in the Security Center's regulatory compliance dashboard.
- If Security Hub policy is enabled, recommendations will appear in the Security Center portal and the regulatory compliance dashboard 5-10 minutes after onboard completes.

Connect your GCP accounts

Onboarding your GCP account into Security Center, integrates GCP Security Command and Azure Security Center. Security Center thus provides visibility and protection across both of these cloud environments to provide:

- Detection of security misconfigurations
- A single view showing Security Center recommendations and GCP Security Command Center findings
- Incorporation of your GCP resources into Security Center's secure score calculations
- Integration of GCP Security Command Center recommendations based on the CIS standard into the Security Center's regulatory compliance dashboard

In the screenshot below, you can see GCP projects displayed in Security Center's overview dashboard.



Follow the steps below to create your GCP cloud connector.

Set up GCP Security Command Center with Security Health Analytics

For all the GCP projects in your organization, you must also:

- Set up GCP Security Command Center using these instructions from the GCP documentation.
- Enable Security Health Analytics using these instructions from the GCP documentation.
- Verify that there is data flowing to the Security Command Center.

The instructions for connecting your GCP environment for security configuration follow Google's recommendations for consuming security configuration recommendations. The integration uses Google Security Command Center and will consume more resources that might impact your billing.

When you first enable Security Health Analytics, it might take several hours for data to be available.

Enable GCP Security Command Center API

1. From Google's Cloud Console API Library, select the project you want to connect to Azure Security Center.
2. In the API Library, find and select **Security Command Center API**.
3. On the API's page, select **ENABLE**.

Create a dedicated service account for the security configuration integration

1. In the GCP Console, select the project you want to connect to Security Center.
2. In the Navigation menu, Under IAM & admin options, select **Service accounts**.
3. Select **CREATE SERVICE ACCOUNT**.
4. Enter an account name, and select **Create**.
5. Specify the Role as Security Center Admin Viewer, and select **Continue**.
6. The Grant users access to this service account section is optional. Select **Done**.
7. Copy the Email value of the created service account, and save it for later use.
8. In the Navigation menu, Under IAM & admin options, select **IAM**
9. Switch to organization level.
10. Select **ADD**.
11. In the New members field, paste the Email value you copied earlier.
12. Specify the Role as **Security Center Admin Viewer** and then select **Save**.

Create a private key for the dedicated service account

Switch to project level.

1. In the Navigation menu, Under IAM & admin options, select **Service accounts**.
2. Open the dedicated service account and select **Edit**.
3. In the Keys section, select **ADD KEY** and then **Create new key**.
4. In the Create private key screen, select **JSON**, and then select **CREATE**.
5. Save this JSON file for later use.

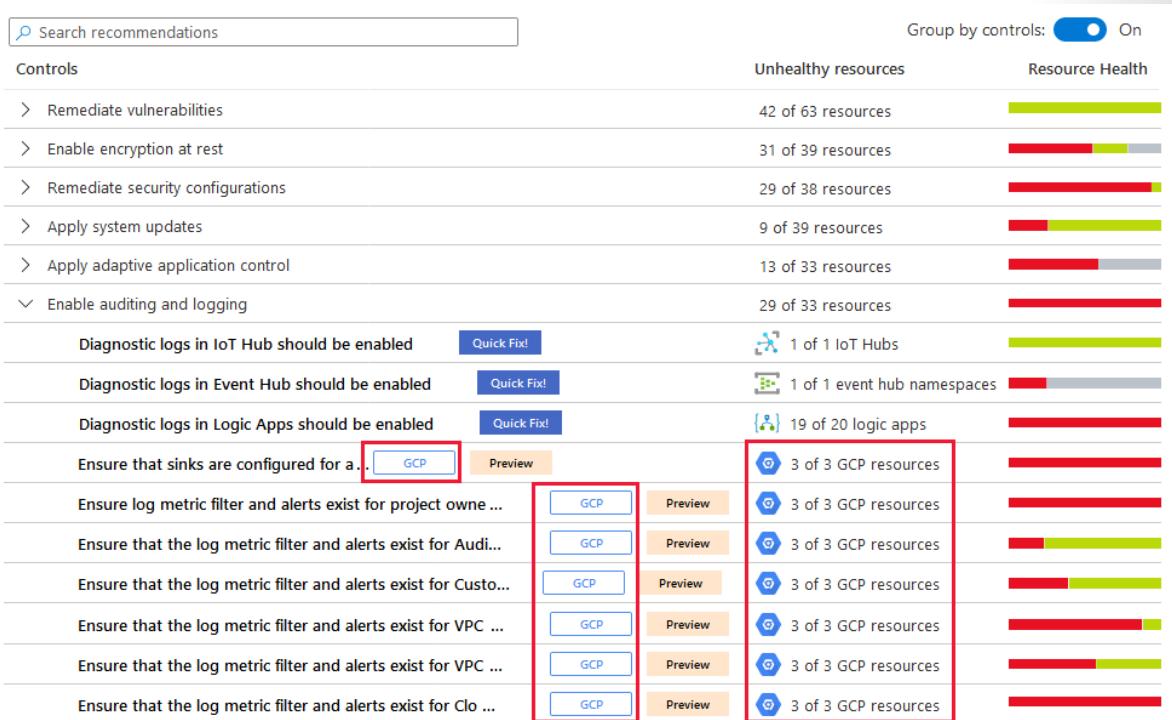
Connect GCP to security center

1. From Security Center's menu, select **Cloud connectors**.
2. Select **add GCP account**.
3. On the onboarding page, do the following and then select Next.
4. Validate the chosen subscription.
5. In the Display name field, enter a display name for the connector.
6. In the Organization ID field, enter your organization's ID.
7. In the Private key file box, browse to the JSON file you downloaded in the previous step. Create a private key for the dedicated service account.

Confirmation

When the connector is successfully created and GCP Security Command Center has been configured properly:

- The GCP CIS standard will be shown in the Security Center's regulatory compliance dashboard.
- Security recommendations for your GCP resources will appear in the Security Center portal and the regulatory compliance dashboard 5-10 minutes after onboard completes:



Remediate security alerts using Azure Defender

Lesson Introduction

Azure Defender provides a purpose-driven user interface to manage and investigate security incidents and alerts across protected resources. The alert includes actions to take to remediate the threat and steps to prevent future attacks.

You are a Security Operations Analyst working at a company that has deployed cloud workload protection with Azure Defender. You are responsible for remediating security alerts generated by Azure Defender detections.

You receive an alert regarding a container; the alert provides information to manually remediate the issue and what you can do in the future to prevent further attacks. You work with the infrastructure team to resolve the issue. The infrastructure team recommends creating automated remediation tasks for future alerts regarding the same problem. You create a Logic App to perform the actions for future alerts.

Learn how to remediate security alerts in Azure Defender.

Learning objectives

After completing this lesson, you should be able to:

- Describe alerts in Azure Defender
- Remediate alerts in Azure Defender
- Automate responses in Azure Defender

Explain security alerts

In Security Center, there are various alerts for many different resource types. Security Center generates alerts for resources deployed on Azure and for resources deployed on on-premises and hybrid cloud environments. Security alerts are triggered by advanced detections and are available only with Azure Defender.

Respond to today's threats

There have been significant changes in the threat landscape over the last 20 years. In the past, companies typically only had to worry about website defacement by individual attackers who were mostly interested in seeing "what they could do". Today's attackers are much more sophisticated and organized. They often have specific financial and strategic goals. They also have more resources available to them, as they might be funded by nation states or organized crime.

These changing realities have led to an unprecedented level of professionalism in the attacker ranks. No longer are they interested in web defacement. They are now interested in stealing information, financial accounts, and private data – all of which they can use to generate cash on the open market or use a particular business, political, or military position. Even more concerning than those attackers with a financial objective are the ones who breach networks to harm infrastructure and people.

In response, organizations often deploy various point solutions focused on defending either the enterprise perimeter or endpoints by looking for known attack signatures. These solutions tend to generate a

high volume of low fidelity alerts, which require a security analyst to triage and investigate. Most organizations lack the time and expertise required to respond to these alerts – so many go unaddressed.

In addition, attackers have evolved their methods to subvert many signature-based defenses and adapt to cloud environments. New approaches are required to more quickly identify emerging threats and expedite detection and response.

What are security alerts and security incidents?

Alerts are the notifications that Security Center generates when it detects threats on your resources. Security Center prioritizes and lists the alerts, along with the information needed for you to quickly investigate the problem. Security Center also provides recommendations for how you can remediate an attack.

A security incident is a collection of related alerts instead of listing each alert individually. Security Center uses Cloud Smart Alert Correlation to correlate different alerts and low fidelity signals into security incidents.

Using incidents, Security Center provides you with a single view of an attack campaign and all of the related alerts. This view enables you to quickly understand what actions the attacker took, and what resources were affected. For more information, see Cloud smart alert correlation.

How does Security Center detect threats?

Microsoft security researchers are constantly on the lookout for threats. Because of our global presence in the cloud and on-premises, we have access to an expansive set of telemetry. The wide-reaching and diverse collection of datasets enable us to discover new attack patterns and trends across our on-premises consumer and enterprise products, as well as our online services. As a result, Security Center can rapidly update its detection algorithms as attackers release new and increasingly sophisticated exploits. This approach helps you keep pace with a fast-moving threat environment.

To detect real threats and reduce false positives, Security Center collects, analyzes, and integrates log data from your Azure resources and the network. It also works with connected partner solutions, like firewall and endpoint protection solutions. Security Center analyzes this information, often correlating information from multiple sources, to identify threats.

Security Center employs advanced security analytics, which go far beyond signature-based approaches. Breakthroughs in big data and machine learning technologies are used to evaluate events across the entire cloud fabric – detecting threats that would be impossible to identify using manual approaches and predicting the evolution of attacks. These security analytics include:

- **Integrated threat intelligence:** Microsoft has an immense amount of global threat intelligence. Telemetry flows in from multiple sources, such as Azure, Microsoft 365, Microsoft CRM online, Microsoft Dynamics AX, outlook.com, MSN.com, the Microsoft Digital Crimes Unit (DCU), and Microsoft Security Response Center (MSRC). Researchers also receive threat intelligence information shared among major cloud service providers and feeds from other third parties. Azure Security Center can use this information to alert you to threats from known bad actors.
- **Behavioral analytics:** Behavioral analytics is a technique that analyzes and compares data to a collection of known patterns. However, these patterns are not simple signatures. They are determined through complex machine learning algorithms that are applied to massive datasets. They are also determined through careful analysis of malicious behaviors by expert analysts. Azure Security Center can use behavioral analytics to identify compromised resources based on analysis of virtual machine logs, virtual network device logs, fabric logs, and other sources.

- **Anomaly detection:** Azure Security Center also uses anomaly detection to identify threats. In contrast to behavioral analytics (which depends on known patterns derived from large data sets), anomaly detection is more “personalized” and focuses on baselines specific to your deployments. Machine learning is applied to determine normal activity for your deployments. Then, rules are generated to define outlier conditions that could represent a security event.

How are alerts classified?

Security Center assigns a severity to alerts to help you prioritize the order in which you attend to each alert, so when a resource is compromised, you can get to it right away. The severity is based on how confident Security Center is in the finding or the analytic used to issue the alert and the confidence level that there was malicious intent behind the activity that led to the alert.

- High: There is a high probability that your resource is compromised. You should look into it right away. Security Center has high confidence in both the malicious intent and in the findings used to issue the alert. For example, an alert detects the execution of a known malicious tool such as Mimikatz, a common tool used for credential theft.
- Medium: This is probably a suspicious activity that might indicate that a resource is compromised. Security Center's confidence in the analytic or finding is medium, and the confidence of malicious intent is medium to high. These would usually be machine learning or anomaly-based detections. For example, a sign-in attempt from an anomalous location.
- Low: This might be a benign positive or a blocked attack.
 - Security Center is not confident enough that the intent is malicious, and the activity might be innocent. For example, log clear is an action that might happen when an attacker tries to hide their tracks, but in many cases it is a routine operation performed by admins.
 - Security Center doesn't usually tell you when attacks were blocked unless it's an interesting case that we suggest you look into.
- Informational: You will only see informational alerts when you drill down into a security incident or if you use the REST API with a specific alert ID. An incident is typically made up of a number of alerts, some of which might appear on their own to be only informational, but in the context of the other alerts might be worthy of a closer look.

Continuous monitoring and assessments

Azure Security Center benefits from having security research and data science teams throughout Microsoft who continuously monitor for changes in the threat landscape. This includes the following initiatives:

- **Threat intelligence monitoring:** Threat intelligence includes mechanisms, indicators, implications, and actionable advice about existing or emerging threats. This information is shared in the security community, and Microsoft continuously monitors threat intelligence feeds from internal and external sources.
- **Signal sharing:** Insights from security teams across Microsoft's broad portfolio of cloud and on-premises services, servers, and client endpoint devices are shared and analyzed.
- **Microsoft security specialists:** Ongoing engagement with teams across Microsoft that work in specialized security fields, like forensics and web attack detection.
- **Detection tuning:** Algorithms are run against real customer data sets, and security researchers work with customers to validate the results. True and false positives are used to refine machine learning algorithms.

Understand alert types

The current alert reference list contains over 500 types of alerts. The reference list can be reviewed at: [Security alerts - a reference guide⁷](#)

Each alert type has a description, severity, and MITRE ATT&CK tactic

MITRE ATT&CK tactics

Understanding the intention of an attack can help you investigate and report the event more easily. To help with these efforts, Azure Security Center alerts include the MITRE tactics with many alerts. The series of steps that describe the progression of a cyberattack from reconnaissance to data exfiltration is often referred to as a "kill chain".

Security Center's supported kill chain intents are based on version 7 of the MITRE ATT&CK matrix and described in the table below.

Tactic	Description
PreAttack	PreAttack could be either an attempt to access a certain resource regardless of malicious intent or a failed attempt to gain access to a target system to gather information prior to exploitation. This step is usually detected as an attempt, originating from outside the network, to scan the target system and identify an entry point.
InitialAccess	InitialAccess is the stage where an attacker manages to get a foothold on the attacked resource. This stage is relevant for compute hosts and resources such as user accounts, certificates, etc. Threat actors will often be able to control the resource after this stage.
Persistence	Persistence is any access, action, or configuration change to a system that gives a threat actor a persistent presence on that system. Threat actors will often need to maintain access to systems through interruptions such as system restarts, loss of credentials, or other failures that would require a remote access tool to restart or provide an alternate backdoor for them to regain access.
PrivilegeEscalation	Privilege escalation is the result of actions that allow an adversary to obtain a higher level of permissions on a system or network. Certain tools or actions require a higher level of privilege to work and are likely necessary at many points throughout an operation. User accounts with permissions to access specific systems or perform specific functions necessary for adversaries to achieve their objective may also be considered an escalation of privilege.

⁷ <https://docs.microsoft.com/azure/security-center/alerts-reference?azure-portal=true>

Tactic	Description
DefenseEvasion	Defense evasion consists of techniques an adversary may use to evade detection or avoid other defenses. Sometimes these actions are the same as (or variations of) techniques in other categories that have the added benefit of subverting a particular defense or mitigation.
CredentialAccess	Credential access represents techniques resulting in access to or control over system, domain, or service credentials used within an enterprise environment. Adversaries will likely attempt to obtain legitimate credentials from users or administrator accounts (local system administrator or domain users with administrator access) to use within the network. With sufficient access within a network, an adversary can create accounts for later use within the environment.
Discovery	Discovery consists of techniques that allow the adversary to gain knowledge about the system and internal network. When adversaries gain access to a new system, they must align themselves to what they now have control of and what benefits operating from that system give to their current objective or overall goals during the intrusion. The operating system provides many native tools that aid in this post-compromise information-gathering phase.
LateralMovement	Lateral movement consists of techniques that enable an adversary to access and control remote systems on a network and could, but does not necessarily, include execution of tools on remote systems. The lateral movement techniques could allow an adversary to gather information from a system without needing more tools, such as a remote access tool. An adversary can use lateral movement for many purposes, including remote Execution of tools, pivoting to more systems, access to specific information or files, access to additional credentials, or to cause an effect.
Execution	The execution tactic represents techniques that result in execution of adversary-controlled code on a local or remote system. This tactic is often used in conjunction with lateral movement to expand access to remote systems on a network.
Collection	Collection consists of techniques used to identify and gather information, such as sensitive files, from a target network prior to exfiltration. This category also covers locations on a system or network where the adversary may look for information to exfiltrate.

Tactic	Description
Exfiltration	Exfiltration refers to techniques and attributes that result or aid in the adversary removing files and information from a target network. This category also covers locations on a system or network where the adversary may look for information to exfiltrate.
CommandAndControl	The command and control tactic represents how adversaries communicate with systems under their control within a target network.
Impact	Impact events primarily try to directly reduce the availability or integrity of a system, service, or network, including manipulation of data to impact a business or operational process. This would often refer to techniques such as ransomware, defacement, data manipulation, and others.

Remediate alerts

From Security Center's overview page, select the Security alerts tile at the top of the page or the link on the sidebar.

The screenshot shows the 'Security alerts (Preview)' page with the following details:

- Alert Count:** 644 Active alerts, 34 Affected resources.
- Severity Distribution:** Active alerts by severity: High (166), Medium (414), Low (64).
- Filtering:** Search by ID, title, or affected resource, Status = Active, Severity = Low, Medium, High, Time = Last month, Add filter, No grouping.
- Table Headers:** Severity, Alert title, Affected resource, Activity start time (UTC+2), MITRE ATT&CK® tactics, Status.
- Table Data:** A list of 10 alerts, each with a checkbox, severity (High), icon, alert title, affected resource, activity start time, tactic (e.g., Credential Access), and status (Active). Examples include "Suspicious process executed" on various hosts and "Azure Security Center test alert".
- Pagination:** < Previous, Page 1 of 17, Next >

From the Security alerts list, select an alert. A side pane opens and shows a description of the alert and all the affected resources.

Security alerts (Preview)

Refresh Change status Open query Suppression rules Security alerts map (Preview) Create sample alerts

3 Active alerts 1 Affected resources

Active alerts by severity
High (3)

Severity	Alert title	Affected resource	Activity start time
High	Exposed Kubernetes dashboard detect...	ASC-AKS-CLOUD-TALK	11/05/20, 1:58 PM
High	Azure Security Center test alert for AKS...	ASC-AKS-CLOUD-TALK	11/04/20, 11:50 AM
High	Exposed Kubernetes dashboard detect...	ASC-AKS-CLOUD-TALK	10/26/20, 10:44 PM

Search by ID, title, or affected resource Status == Active Severity == High Time == Last month Add filter No grouping

Alert description
Kubernetes audit log analysis detected exposure of the Kubernetes Dashboard by a LoadBalancer service. Exposed dashboard allows an unauthenticated access to the cluster management and poses a security threat.

Affected resource
ASC-AKS-CLOUD-TALK Kubernetes service ASC DEMO Subscription

MITRE ATT&CK® tactics
Initial Access

View full details Take action

For further information, select View full details.

The left pane of the security alert page shows high-level information regarding the security alert: title, severity, status, activity time, description of the suspicious activity, and the affected resource. Alongside the affected resource are the Azure tags relevant to the resource. Use these to infer the organizational context of the resource when investigating the alert.

The right pane includes the Alert details tab containing further details of the alert to help you investigate the issue: IP addresses, files, processes, and more.

The screenshot shows the 'Security alert' details page. On the left, there's a summary card for a 'Potential SQL Injection' alert. It includes fields for Severity (High), Status (Active), Activity time (06/11/20, 1...), and a description: 'Potential SQL Injection was detected on your database Demo on server R-DEV\SQLEXPRESS'. Below this are sections for Affected resource (R-DEV, Azure Arc machine, Env: Development) and Intent (Pre-attack). At the bottom is a feedback section 'Was this useful?' with 'Yes' and 'No' radio buttons. On the right, the 'Alert details' tab is selected, showing detailed information like Client IP Address (127.0.0.1), Oms Workspace ID (61d507e7), Vulnerable Statement (SELECT * FROM sql_users WHERE...), and a 'Take action' button.

Also in the right pane is the Take action tab. Use this tab to take further actions regarding the security alert. Actions such as:

- Mitigate the threat - provides manual remediation steps for this security alert
- Prevent future attacks - provides security recommendations to help reduce the attack surface, increase security posture, and thus prevent future attacks
- Trigger automated response - provides the option to trigger a logic app as a response to this security alert
- Suppress similar alerts - provides the option to suppress future alerts with similar characteristics if the alert isn't relevant for your organization

The screenshot shows the Microsoft Security Center interface. On the left, there's a sidebar with 'Dashboard >' and a 'Security alert' card for a 'Potential SQL Injection' on '25181-892ad5bb9a'. The main area is titled 'Take action' under 'Alert details'. It includes sections for 'Mitigate the threat' (with a link to 'Read more about SQL Injection threats and best practices for safe application code.'), 'Prevent future attacks' (listing 'Windows Defender Exploit Guard should be enabled on your machines' and 'Vulnerabilities on your SQL servers on machine should be remediated'), and options like 'Trigger automated response' and 'Suppress similar alerts (preview)'. At the bottom, there's a 'Next: Take Action >>' button.

Automate responses

Every security program includes multiple workflows for incident response. These processes might include notifying relevant stakeholders, launching a change management process, and applying specific remediation steps. Security experts recommend that you automate as many steps of those procedures as you can. Automation reduces overhead. It can also improve your security by ensuring the process steps are done quickly, consistently, and according to your predefined requirements.

This feature can trigger Logic Apps on security alerts and recommendations. For example, you might want Security Center to email a specific user when an alert occurs.

Create a logic app and define when it should automatically run

From Security Center's sidebar, select Workflow automation.

From this page, you can create new automation rules as well as enable, disable, or delete existing ones.

To define a new workflow, select Add workflow automation.

A pane appears with the options for your new automation. Here you can enter:

- A name and description for the automation.
- The triggers that will initiate this automatic workflow. For example, you might want your Logic App to run when a security alert that contains "SQL" is generated.
- The Logic App that will run when your trigger conditions are met.

The screenshot shows the Azure Security Center Workflow automation interface. On the left, there's a navigation menu with sections like General, Cloud Security, Management, and a highlighted 'Workflow automation'. A red box highlights the 'Add workflow automation' button at the top right of the main content area. To its right is a detailed view of 41 existing workflows, showing columns for Name, Status, Scope, and Trigger Type. On the far right, a large red-bordered dialog box titled 'Add workflow automation' is open. It has tabs for 'General', 'Trigger conditions', and 'Actions'. Under 'General', fields are provided for 'Name *', 'Description', 'Subscription' (set to 'ASC DEMO'), and 'Resource group *'. Under 'Trigger conditions', it lists 'Select Security Center data types *' (set to 'Threat detection alerts') and 'Alert name contains'. Under 'Actions', it shows 'Configure the Logic App that will be triggered' and a dropdown for 'Show Logic App instances from the following subscriptions *' (set to '41 selected'). A 'Logic App name' dropdown is also present. At the bottom of the dialog are 'Create' and 'Cancel' buttons.

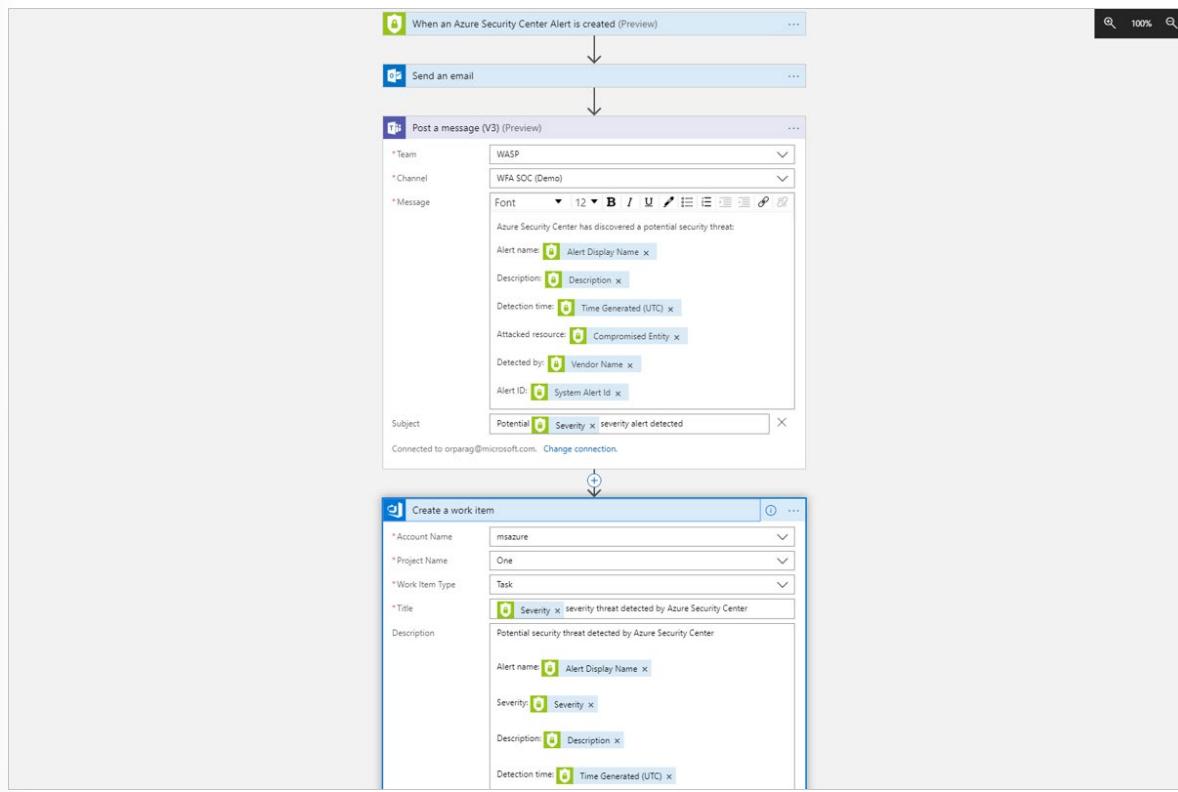
From the Actions section, select Create a new one to begin the Logic App creation process.

You'll be taken to Azure Logic Apps.

- Enter a name, resource group, and location, and select Create.
- In your new logic app, you can choose from built-in, predefined templates from the security category. Or you can define a custom flow of events to occur when this process is triggered.

The logic app designer supports the following Security Center triggers:

- When an Azure Security Center Recommendation is created or triggered - If your logic app relies on a recommendation that gets deprecated or replaced, your automation will stop working. You'll then need to update the trigger. To track changes to recommendations, see Azure Security Center release notes.
- When an Azure Security Center Alert is created or triggered - You can customize the trigger so that it relates only to alerts with the severity levels that interest you.



After you've defined your logic app, return to the workflow automation definition pane ("Add workflow automation"). Click Refresh to ensure your new Logic App is available for selection.

Select your logic app and save the automation. The Logic App dropdown only shows Logic Apps with supporting Security Center connectors mentioned above.

Manually trigger a logic app

You can also run Logic Apps manually when viewing any security alert or recommendation.

To manually run a Logic App, open an alert or a recommendation and select Trigger Logic App

Suppress alerts from Azure Defender

The various Azure Defender plans detect threats in any area of your environment and generate security alerts. When a single alert isn't interesting or relevant, you can manually dismiss it. Alternatively, use the suppression rules feature to automatically dismiss similar alerts in the future. Typically, you'd use a suppression rule to:

- Suppress alerts that you've identified as false positives
- Suppress alerts that are being triggered too often to be useful

Your suppression rules define the criteria for which alerts should be automatically dismissed. Suppression rules can only dismiss alerts that have already been triggered on the selected subscriptions.

Create a suppression rule

To create a rule directly in the Azure portal:

From Security Center's security alerts page:

- Locate the specific alert you don't want to see anymore, and from the ellipsis menu (...) for the alert, select Create suppression rule:

OR

- select the suppression rules link at the top of the page, and from the suppression rules page select Create new suppression rule:

In the new suppression rule pane, enter the details of your new rule.

- Your rule can dismiss the alert on all resources so you don't get any alerts like this one in the future.
- Your rule can dismiss the alert on specific criteria - when it relates to a specific IP address, process name, user account, Azure resource, or location.

New suppression rule (Preview)

Create auto-dismiss rules in order to automatically dismiss alerts by pre-defined conditions. [Learn more](#)

Rule Conditions

Subscription *

Alerts * Custom All

Entities

Rule details

Rule name *

State *

Reason *

Comment

Rule expiration
Set an end date and time for this rule

Test your rule

Azure Security Center may store your auto-dismiss rules in US and Europe regions.

Enter details of the rule:

- Name - A name for the rule. Rule names must begin with a letter or a number, be between 2 and 50 characters, and contain no symbols other than dashes (-) or underscores (_).
- State - Enabled or disabled.
- Reason - Select one of the built-in reasons or 'other' if they don't meet your needs.

- Expiration date - An end date and time for the rule. Rules can run for up to six months.

Optionally, test the rule using the Simulate button to see how many alerts would have been dismissed if this rule had been active.

Save the rule.

View suppressed alerts

Alerts that match your enabled suppression rules will still be generated, but their state will be set to dismissed. You can see the state in the Azure portal or however you access your Security Center security alerts.

Use Security Center's filter to view alerts that have been dismissed by your rules.

- From Security Center's security alerts page, open the filter options, and select **Dismissed**.

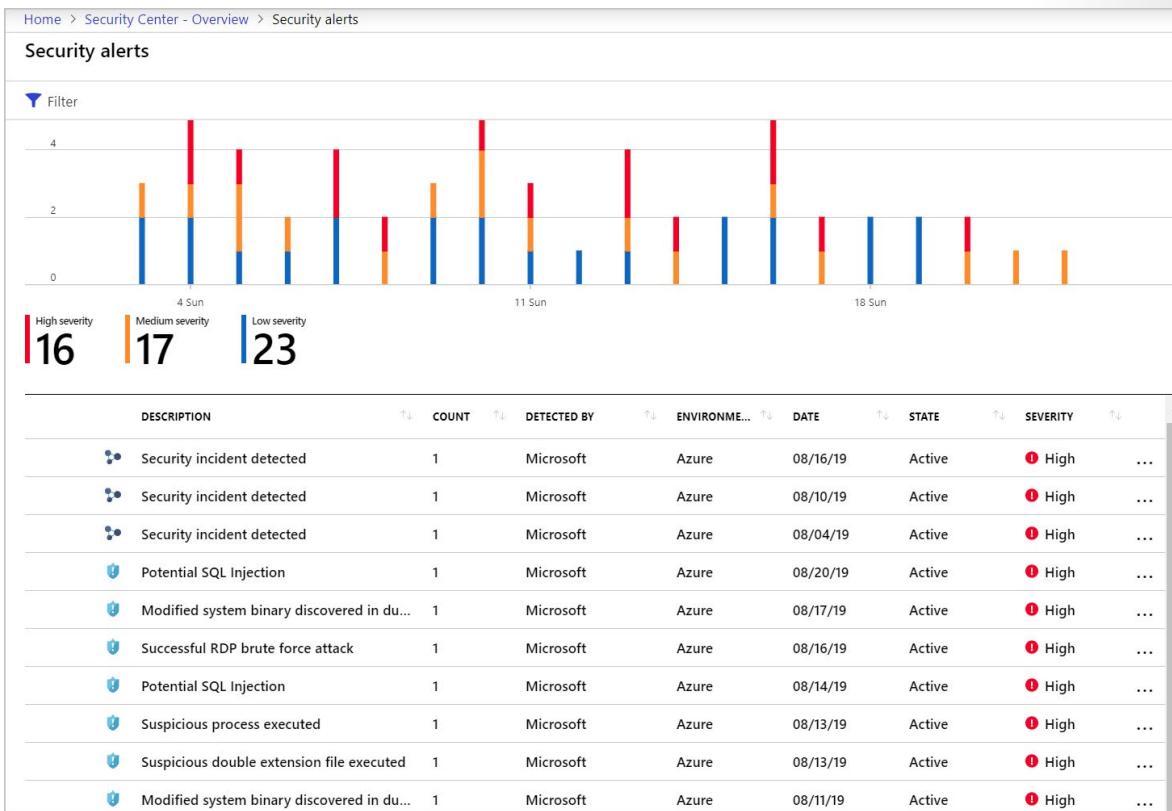
Manage security incidents and threat intelligence reports

Triage and investigating security alerts can be time consuming for even the most skilled security analysts. For many, it's hard to know where to begin.

Security Center uses analytics to connect the information between distinct security alerts. Using these connections, Security Center can provide a single view of an attack campaign and its related alerts to help you understand the attacker's actions and the affected resources.

Incidents appear on the Security alerts page. Select an incident to view the related alerts and get more information.

On the Security Center overview page, select the Security alerts tile. The incidents and alerts are listed. Notice that security incidents have a different icon to security alerts.



To view details, select an incident. The Security incident page shows more details.

The figure shows the Security incident page for a "Security incident detected" event. The left pane contains the following details:

- Title:** Security incident detected
- Severity:** High
- Status:** Active
- Activity time:** 06/11/20, 1...
- Description:** The incident which started on 2020-06-11 09:54:30 UTC and recently detected on 2020-06-11 19:58:55 UTC indicates that an attacker has abused resource in your resource R-DEV\SQLEXPRESS
- Affected resource:**
 - R-DEV (Azure Arc machine)
 - Env: Development
 - DS-ThreatDetection_Demo (Subscription)
- Feedback:** Was this useful? (radio buttons for Yes and No)
- Action:** Next: Take Action >>

The right pane shows a table of alerts:

Severity	Description	Count	Activity start time
High	Potential SQL Brute Force attempt	8	Thu Jun 11 2020 12:54:30
High	Potential SQL Injection	116	Thu Jun 11 2020 16:01:07

The left pane of the security incident page shows high-level information about the security incident: title, severity, status, activity time, description, and the affected resource. Next to the affected resource, you can see the relevant Azure tags. Use these tags to infer the organizational context of the resource when investigating the alert.

The right pane includes the Alerts tab with the security alerts that were correlated as part of this incident.

To switch to the Take action tab, select the tab or the button at the bottom of the right pane. Use this tab to take further actions such as:

- Mitigate the threat - provides manual remediation steps for this security incident
- Prevent future attacks - provides security recommendations to help reduce the attack surface, increase security posture, and prevent future attacks
- Trigger automated response - provides the option to trigger a Logic App as a response to this security incident
- Suppress similar alerts - provides the option to suppress future alerts with similar characteristics if the alert isn't relevant for your organization

To remediate the threats in the incident, follow the remediation steps provided with each alert.

Generate threat intelligence reports

Security Center threat protection works by monitoring security information from your Azure resources, the network, and connected partner solutions. It analyzes this information, often correlating information from multiple sources, to identify threats.

When Security Center identifies a threat, it triggers a security alert containing detailed information regarding the event, including suggestions for remediation. Security Center provides threat intelligence reports containing information about detected threats to help incident response teams investigate and remediate threats. The report includes information such as:

- Attacker's identity or associations (if this information is available)
- Attackers' objectives
- Current and historical attack campaigns (if this information is available)
- Attackers' tactics, tools, and procedures
- Associated indicators of compromise (IoC) such as URLs and file hashes
- Victimology, which is the industry and geographic prevalence to assist you in determining if your Azure resources are at risk
- Mitigation and remediation information

Security Center has three types of threat reports, which can vary according to the attack. The reports available are:

- Activity Group Report: provides deep dives into attackers, their objectives, and tactics.
- Campaign Report: focuses on details of specific attack campaigns.
- Threat Summary Report: covers all of the items in the previous two reports.

This type of information is useful during the incident response process, where there's an ongoing investigation to understand the source of the attack, the attacker's motivations, and what to do to mitigate this issue in the future.

To access the threat intelligence report

To generate the report:

From Security Center's sidebar, open the Security alerts page.

Select an alert. The alerts details page opens with more details about the alert. Below is the Ransomware indicators detected alert details page.

The screenshot shows the Azure Security Center alert details page for a 'Ransomware indicators detected' alert. The alert has a 'High Severity' and is 'Active'. It was detected on '06/16/2023' at 'Activity time'. The alert description states: 'Analysis of host data indicates suspicious activity traditionally associated with lock-screen and encryption ransomware. Lock screen ransomware displays a full-screen message preventing interactive use of the host and access to its files. Encryption ransomware prevents access by encrypting data files. In both cases a ransom message is typically displayed, requesting payment in order to restore file access.' Under 'Affected resource', there are two entries: 'AME' (Virtual machine) and 'Tests Prod' (Subscription). The 'Intent' section shows 'Execution' is the primary intent. The 'Alert details' tab is selected, showing the following data:

Compromised Host	Suspicious Command Line c:\users\invest~1\appdata\local\temp\rans...
User Name	Suspicious Process ID 0x6a4
Account Session ID	Enrichment_tas_threat_reports Report: Shadow Copy Delete
Suspicious Process	Detected by Microsoft

The 'Report: Shadow Copy Delete' link in the 'Enrichment_tas_threat_reports' section is highlighted with a red box and a cursor icon pointing to it. The 'Related entities' section lists: Account (1), File (1), Host (1), Host logon session (1), and Process (2). A 'Next: Take Action >>' button is at the bottom.

Select the link to the report, and a PDF will open in your default browser.

Respond to Azure Defender for Key Vault alerts

When you receive an alert from Azure Defender for Key Vault, we recommend you investigate and respond to the alert as described below. Azure Defender for Key Vault protects applications and credentials, so even if you're familiar with the application or user that triggered the alert, it's important to verify the situation surrounding every alert.

Every alert from Azure Defender for Key Vault includes the following elements:

- Object ID
- User Principal Name or IP Address of the suspicious resource

Contact

- Verify whether the traffic originated from within your Azure tenant. If the key vault firewall is enabled, it's likely that you've provided access to the user or application that triggered this alert.
- If you can't verify the source of the traffic, continue to Step 2. Immediate mitigation.
- If you can identify the source of the traffic in your tenant, contact the user or owner of the application.

Immediate mitigation

If you don't recognize the user or application, or if you think the access shouldn't have been authorized:

- If the traffic came from an unrecognized IP Address:
 - Enable the Azure Key Vault firewall as described in [Configure Azure Key Vault firewalls and virtual networks](#).
 - Configure the firewall with trusted resources and virtual networks.
- If the source of the alert was an unauthorized application or suspicious user:
 - Open the key vault's access policy settings.
 - Remove the corresponding security principal, or restrict the operations the security principal can perform.
- If the source of the alert has an Azure Active Directory role in your tenant:
 - Contact your administrator.
 - Determine whether there's a need to reduce or revoke Azure Active Directory permissions.

Identify impact

When the impact has been mitigated, investigate the secrets in your key vault that were affected:

1. Open the "Security" page on your Azure Key Vault and view the triggered alert.
2. Select the specific alert that was triggered. Review the list of the secrets that were accessed and the timestamp.
3. Optionally, if you have key vault diagnostic logs enabled, review the previous operations for the corresponding caller IP, user principal, or object ID.

Take action

When you've compiled your list of the secrets, keys, and certificates that the suspicious user or application accessed, you should immediately rotate those objects.

- Affected secrets should be disabled or deleted from your key vault.
- If the credentials were used for a specific application:
 - Contact the administrator of the application and ask them to audit their environment for any uses of the compromised credentials since they were compromised.
 - If the compromised credentials were used, the application owner should identify the information that was accessed and mitigate the impact.

Respond to Azure Defender for DNS alerts

When you receive an alert from Azure Defender for DNS, we recommend you investigate and respond to the alert as described below. Azure Defender for DNS protects all connected resources, so even if you're familiar with the application or user that triggered the alert, it's important to verify the situation surrounding every alert.

Contact

Contact the resource owner to determine whether the behavior was expected or intentional.

- If the activity is expected, dismiss the alert.
- If the activity is unexpected, treat the resource as potentially compromised and mitigate as described in the next step.

Immediate mitigation

Isolate the resource from the network to prevent lateral movement.

- Run a full antimalware scan on the resource, following any resulting remediation advice.
- Review installed and running software on the resource, removing any unknown or unwanted packages.
- Revert the machine to a known good state, reinstalling the operating system if required, and restore software from a verified malware-free source.
- Resolve any Azure Security Center recommendations for the machine, remediating highlighted security issues to prevent future breaches.

Respond to Azure Defender for Resource Manager alerts

When you receive an alert from Azure Defender for Resource Manager, we recommend you investigate and respond to the alert as described below. Azure Defender for Resource Manager protects all connected resources, so even if you're familiar with the application or user that triggered the alert, it's important to verify the situation surrounding every alert.

Contact

Contact the resource owner to determine whether the behavior was expected or intentional.

- If the activity is expected, dismiss the alert.
- If the activity is unexpected, treat the related user accounts, subscriptions, and virtual machines as compromised and mitigate as described in the following step.

Immediate mitigation

- Remediate compromised user accounts:
 - If they're unfamiliar, delete them as they may have been created by a threat actor
 - If they're familiar, change their authentication credentials
 - Use Azure Activity Logs to review all activities performed by the user and identify any that are suspicious
- Remediate compromised subscriptions:
 - Remove any unfamiliar Runbooks from the compromised automation account
 - Review IAM permissions for the subscription and remove permissions for any unfamiliar user account
 - Review all Azure resources in the subscription and delete any that are unfamiliar

- Review and investigate any security alerts for the subscription in Azure Security Center
- Use Azure Activity Logs to review all activities performed in the subscription and identify any that are suspicious
- Remediate the compromised virtual machines
 - Change the passwords for all users
 - Run a full antimalware scan on the machine
 - Reimage the machines from a malware-free source

Knowledge check

Check your Knowledge

Multiple choice

Item 1. Which of the following describe Azure Defender's primary role?

- Cloud security posture management
- Cloud workload protection
- Cloud configuration management

Multiple choice

Item 2. Which Security Center feature enables you to see the topology of your workloads?

- Inventory
- Secure Score
- Network map

Multiple choice

Item 3. To make sure Azure Defender covers all resources in a Subscription, which option do you enable?

- Automatic provisioning
- Continuous assessments
- Coverage type

Multiple choice

Item 4. What is a protection provided by Azure Defender for DNS?

- Malware communicating with C&C server
- Malware encrypting data on a Device
- Malware enumerating users on a Device

Multiple choice

Item 5. When does Azure Defender for Container Registries scan an image?

- Weekly
- Nightly
- Recently pulled

Multiple choice

Item 6. Which feature of Azure Defender for Servers examines files and registries of the operating system, application software, and others for changes that might indicate an attack?

- Adaptive application controls
- Adaptive network hardening
- File integrity monitoring

Multiple choice

Item 7. Which is a Windows security events configuration?

- Reasonable
- Maximum
- Minimal

Multiple choice

Item 8. What should you install on a new Azure Windows VM if you are not using auto provisioning?

- Log Analytics Agent
- Sysmon
- Windows Firewall

Multiple choice

Item 9. Which of the following is an auto provisioning extension?

- Policy Add-on for Kubernetes
- Windows Events
- Policy for Azure Policy

Multiple choice

Item 10. Which is an option to connect your non-Azure computers?

- Windows Store
- Using Azure Arc enabled servers
- From an Excel spreadsheet

Multiple choice

Item 11. Which resource can Azure Defender protect in a hybrid environment?

- Word Documents
- SQL Databases
- Cosmos DB

Multiple choice

Item 12. Which Cloud provider has a Cloud connector in Security Center?

- IBM Cloud
- GCP
- Oracle

Multiple choice

Item 13. Security Center employs which advanced security analytics?

- Biometric analytics
- Power BI
- Behavioral analytics

Multiple choice

Item 14. Which Azure technology is used to automate remediation?

- Azure Functions
- Azure Batch
- Azure Logic Apps

Multiple choice

Item 15. If available, which report provides Attackers tactics, tools, and procedures?

- Threat Intelligence
- Secure Score
- Incident

Lab - Mitigate threats using Azure Defender

Lab: Mitigate threats using Azure Defender

To download the most recent version of this lab, please visit the SC-200 [GitHub repository⁸](#).

Note: Depending on the lab hosting solution used for your class delivery, the lab instructions may display directly in the virtual lab environment, in addition to being available in the GitHub repository. In that case, follow guidance from your instructor as to where you will access the lab steps from. Even if the GitHub version is not used for your class, you may still find it useful to be able to reference the lab instructions on GitHub after class is over.

Lab scenario

You're a Security Operations Analyst working at a company that is implementing cloud workload protection with Azure Defender. In this lab you will enable Azure Defender.

Objectives

After you complete this lab, you will be able to:

- Mitigate security alerts.
- Create a Log Analytics Workspace.
- Enable Azure Defender.
- Install Azure Arc on an on-premises server.
- Protect an on-premises server.

Lab setup

- Estimated time: 30 minutes

⁸ <https://github.com/MicrosoftLearning/SC-200T00A-Microsoft-Security-Operations-Analyst>

Answers

Multiple choice

Item 1. Which of the following describe Azure Defender's primary role?

- Cloud security posture management
- Cloud workload protection
- Cloud configuration management

Explanation

Azure Defender is for Cloud workload protection.

Multiple choice

Item 2. Which Security Center feature enables you to see the topology of your workloads?

- Inventory
- Secure Score
- Network map

Explanation

Network map is a visualization of your workloads.

Multiple choice

Item 3. To make sure Azure Defender covers all resources in a Subscription, which option do you enable?

- Automatic provisioning
- Continuous assessments
- Coverage type

Explanation

Automatic provisioning will install the required agent for the resources.

Multiple choice

Item 4. What is a protection provided by Azure Defender for DNS?

- Malware communicating with C&C server
- Malware encrypting data on a Device
- Malware enumerating users on a Device

Explanation

Command and Control detection over DNS is detected.

Multiple choice

Item 5. When does Azure Defender for Container Registries scan an image?

- Weekly
- Nightly
- Recently pulled

Explanation

Azure Defender for container registries also scans any image that has been pulled within the last 30 days.

Multiple choice

Item 6. Which feature of Azure Defender for Servers examines files and registries of the operating system, application software, and others for changes that might indicate an attack?

- Adaptive application controls
- Adaptive network hardening
- File integrity monitoring

Explanation

File integrity monitoring examines files.

Multiple choice

Item 7. Which is a Windows security events configuration?

- Reasonable
- Maximum
- Minimal

Explanation

Minimal is a configuration option.

Multiple choice

Item 8. What should you install on a new Azure Windows VM if you are not using auto provisioning?

- Log Analytics Agent
- Sysmon
- Windows Firewall

Explanation

You need to install the Log Analytics Agent.

Multiple choice

Item 9. Which of the following is an auto provisioning extension?

- Policy Add-on for Kubernetes
- Windows Events
- Policy for Azure Policy

Explanation

Policy Add-on for Kubernetes is an extension.

Multiple choice

Item 10. Which is an option to connect your non-Azure computers?

- Windows Store
- Using Azure Arc enabled servers
- From an Excel spreadsheet

Explanation

Using Azure Arc enabled servers is an option to connect.

Multiple choice

Item 11. Which resource can Azure Defender protect in a hybrid environment?

- Word Documents
- SQL Databases
- Cosmos DB

Explanation

SQL Databases can be protected by Azure Defender.

Multiple choice

Item 12. Which Cloud provider has a Cloud connector in Security Center?

- IBM Cloud
- GCP
- Oracle

Explanation

GCP has a cloud connector.

Multiple choice

Item 13. Security Center employs which advanced security analytics?

- Biometric analytics
- Power BI
- Behavioral analytics

Explanation

Behavior analytics is used to detect threats.

Multiple choice

Item 14. Which Azure technology is used to automate remediation?

- Azure Functions
- Azure Batch
- Azure Logic Apps

Explanation

Correct. Logic Apps is the automation engine.

Multiple choice

Item 15. If available, which report provides Attackers tactics, tools, and procedures?

- Threat Intelligence
- Secure Score
- Incident

Explanation

The threat intelligence report contains attacker information if available.

Module 4 Create queries for Azure Sentinel using Kusto Query Language

Construct KQL statements for Azure Sentinel

Lesson Introduction

Kusto Query Language (KQL) is the query language used to perform analysis on data to create Analytics, Workbooks, and perform Hunting in Azure Sentinel. Understanding basic KQL statement structure provides the foundation to build more complex statements.

You are a Security Operations Analyst working at a company that is implementing Azure Sentinel. You are responsible for performing log data analysis to search for malicious activity, display visualizations, and perform threat hunting. To query log data, you use the Kusto Query Language (KQL).

To learn to write KQL, you start with the basic structure of a KQL statement. The basics include what table to query, how to apply a filter, and how to return specific columns.

Learning objectives

After completing this lesson, you should be able to:

- Construct KQL statements
- Search log files for security events using KQL
- Filter searches based on event time, severity, domain, and other relevant data using KQL

The Kusto Query Language statement structure

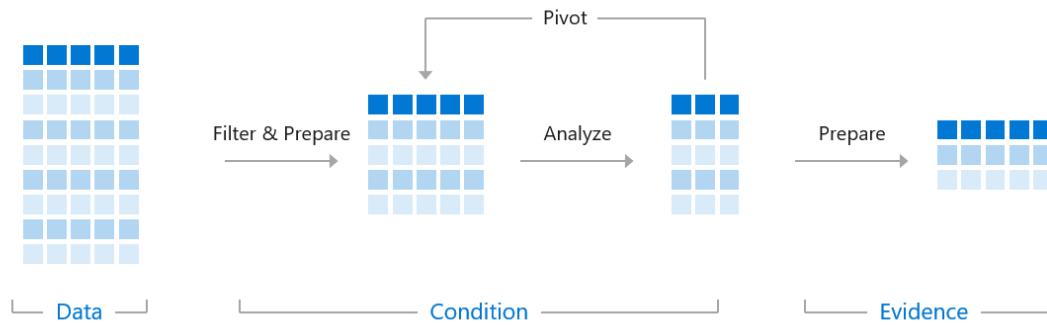
A KQL query is a read-only request to process data and return results. The request is stated in plain text, using a data-flow model designed to make the syntax easy to read, write, and automate. The query uses schema entities organized in a hierarchy similar to SQL's: databases, tables, and columns.

The query consists of a sequence of query statements. At least one statement is a tabular expression statement that produces data arranged in a table-like mesh of columns and rows. The query's tabular expression statements produce the results of the query.

The tabular expression statement's syntax has tabular data flow from one tabular query operator to another, starting with the data source and then flowing through a set of data transformation operators bound together through the use of the pipe (|) delimiter.

For example, the following Kusto query has a single statement, which is a tabular expression statement. The statement starts with a table called SecurityEvent. The EventID column's value then filters the data (rows) for that table and then summarizes the results by creating a new column for the count by Account. Next, in the Prepare phase, the results are then limited to 10 rows.

```
SecurityEvent | where EventID == "4626" | summarize count() by Account | limit 10
```



Important: It is essential to understand how the results flow through the pipe "|". Everything on the left of the pipe is processed then passed to the right of the pipe.

Access the Log Analytics demo environment

Microsoft provides access to an environment to practice writing KQL statements. The only requirement is to have an account to log into Azure. There are no charges to your Azure account to access this environment. You can execute the KQL statements in this module in the demo environment.

You can access the demo environment at <https://aka.ms/lademo>¹

¹ <https://aka.ms/lademo?azure-portal=true>

The screenshot shows the Microsoft Azure Log Analytics interface. On the left, there's a sidebar with 'Logs' and 'Demo' sections, and a 'Tables' list containing various security-related tables like 'UmcActivity', 'ProtectionStatus', 'SecurityAlert', etc., with 'SecurityEvent' currently selected. The main area has a 'Run' button and a 'Time range: Last 24 hours' dropdown. Below that, the results pane shows a table with columns: TimeGenerated [UTC], Account, AccountType, Computer, EventSourceName, and Channel. The results list several events from December 6, 2020, at 12:45:50.310 AM, involving accounts NT AUTHORITY\SYSTEM and WORKGROUP\RETAILVM01\$ on computers RETAILVM01 and RFTAIIVM01, with event sources like Microsoft-Windows-AppLocker and Microsoft-Windows-Security-Auditing.

The Query window has three primary sections:

- The left area is a reference list of the tables in the environment.
- The middle top area is the Query editor.
- The bottom area is the Query Results.

Before running a query, adjust the time range to scope the data. To change the result columns displayed, select the Columns box, and choose the required columns.

Use the let statement

Let statements bind names to expressions. For the rest of the scope, where the let statement appears, the name refers to its bound value. Let statements improve modularity and reuse since they allow you to break a potentially complex expression into multiple parts. Each part is bound to a name through the let statement, and together they compose the whole. The let statement allows for the creation of user-defined functions and views. The views are expressions whose results look like a new table.

Declare and reuse variables

The let statement allows for the creating variables to be used in later statements. In this example, timeOffset and discardEventId are created and used as part of the SecurityEvent "where" clause.

```
let timeOffset = 7d;
let discardEventId = 4688;

SecurityEvent
| where TimeGenerated > ago(timeOffset*2) and TimeGenerated < ago(timeOffset)
| where EventID != discardEventId
```

Tip: "ago()" is a function that will take the current Date and Time and subtract the value provided.

Declare dynamic tables or lists

The let statement allows for the creation of dynamics tables or lists.

```
let suspiciousAccounts = datatable(account: string) [
    @"\administrator",
    @"NT AUTHORITY\SYSTEM"
];

SecurityEvent | where Account in (suspiciousAccounts)

let LowActivityAccounts =
    SecurityEvent
    | summarize cnt = count() by Account
    | where cnt < 10;

LowActivityAccounts | where Account contains "Mal"
```

Use the search operator

The search operator provides a multi-table/multi-column search experience. Although this statement is easy to use, it is inefficient compared to the where operator. Even with this, use search to find data when unsure which table or column to filter.

The first statement will search for "err" across all tables. The second statement will search for "err" in tables SecurityEvent, SecurityAlert, and tables starting with A.

```
search "err"

search in (SecurityEvent,SecurityAlert,A*) "err"
```

Use the where operator

The where operator filters a table to the subset of rows that satisfy a predicate.

Try each of these queries separately to see the results.

```
SecurityEvent
| where TimeGenerated > ago(1d)

SecurityEvent
| where TimeGenerated > ago(1h) and EventID == "4624"

SecurityEvent
| where TimeGenerated > ago(1h)
| where EventID == 4624
| where AccountType =~ "user"

SecurityEvent | where EventID in (4624, 4625)
```

Use the extend operator

Create calculated columns and append the new columns to the result set.

In the example below, the result set will contain a new column named severityOrder.

```
SecurityAlert
| where TimeGenerated > ago(7d)
| extend severityOrder = case (
    AlertSeverity == "High", 3,
    AlertSeverity == "Medium", 2,
    AlertSeverity == "Low", 1,
    AlertSeverity == "Informational", 0,
    -1)
```

Let's take a look at a real-world example

The following is an Azure Sentinel detection rule. The essential concepts to review are;

First, the use of **let** to define the timeframe variable enables maintenance and readability.

Second, the **dynamic** list creation is stored in the let variable DomainList.

Third, the use of **extend** to create two new columns HTTP_Status_Code and Domain.

Fourth, the results sets' progression via the pipe statement allows us to use the newly created columns as filters.

```
let timeframe = 1d;

let DomainList = dynamic(["tor2web.org", "tor2web.com"]);

Syslog
| where TimeGenerated >= ago(timeframe)
| where ProcessName contains "squid"
| extend
    HTTP_Status_Code = extract("(TCP_(([A-Z]+)...-9]{3}))", 8, SyslogMessage),
    Domain = extract("(([A-Z]+ [a-z]{4...Z}+ )([^\:\\\/]*)", 3, SyslogMessage)
| where HTTP_Status_Code == "200"
| where Domain contains "."
| where Domain has_any (DomainList)
```

Use the order by operator

Sort the rows of the input table by one or more columns.

The order by operator can utilize any column or multiple columns by using a comma separator. Each column can be descending or ascending.

```
SecurityAlert
| where TimeGenerated > ago(7d)
| extend severityOrder = case (
    AlertSeverity == "High", 3,
    AlertSeverity == "Medium", 2,
    AlertSeverity == "Low", 1,
    AlertSeverity == "Informational", 0,
    -1)
| order by severityOrder desc
```

Use the project operators

The project operators control what columns to include, add, remove, or rename in the result set of a statement.

There are multiple types of project operators. The following table is a list of the variations.

Operator	Description
project	Select the columns to include, rename or drop, and insert new computed columns.
project-away	Select what columns from the input to exclude from the output.
project-keep	Select what columns from the input to keep in the output.
project-rename	Select the columns to rename in the resulting output.
project-reorder	Set the column order in the resulting output.

project operator

Select the columns to include, rename or drop, and insert new computed columns.

Tip: The project operator will limit the size of the result set, which will increase performance.

```
SecurityEvent
| project Computer, Account
```

project-away operator

Select what columns from the input to exclude from the output.

This example builds from our previous extend and order by operators. The goal of the statement was to set the AlertSeverity in a more meaningful order. If the order were only on the AlertSeverity column, the order would have been in alpha order. Creating the new column severityOrder and setting a numeric value would allow the sorting to provide a meaningful severity order. The severityOrder number is meaningless after the order by operator. The project-away will remove the unnecessary column from the result set.

```
SecurityAlert
| where TimeGenerated > ago(7d)
| extend severityOrder = case (
    AlertSeverity == "High", 3,
    AlertSeverity == "Medium", 2,
    AlertSeverity == "Low", 1,
    AlertSeverity == "Informational", 0,
    -1)
| order by severityOrder
| project-away severityOrder
```

Learn more

You can learn more by reviewing the following.

[KQL quick reference | Microsoft Docs²](#)

[Microsoft Tech Community Security Webinars³](#)

[Become an Azure Sentinel Ninja⁴](#)

² <https://docs.microsoft.com/azure/data-explorer/kql-quick-reference?azure-portal=true>

³ <https://techcommunity.microsoft.com/t5/microsoft-security-and-security-community-webinars/ba-p/927888?azure-portal=true>

⁴ <https://techcommunity.microsoft.com/t5/azure-sentinel/become-an-azure-sentinel-ninja-the-complete-level-400-training/ba-p/1246310?azure-portal=true>

Analyze query results using KQL

Lesson Introduction

Kusto Query Language (KQL) is the query language used to perform analysis on data to create Analytics, Workbooks, and perform Hunting in Azure Sentinel. Understanding how to summarize and visualize data with a KQL statement provides the foundation to build detections in Azure Sentinel.

You are a Security Operations Analyst working at a company that is implementing Azure Sentinel. You are responsible for performing log data analysis to search for malicious activity, display visualizations, and perform threat hunting. To query log data, you use the Kusto Query Language (KQL). You write KQL statements that aggregate and correlate data that allows for pattern detection. One such aggregation might be the number of failed logons. This information, combined with a predetermined threshold, can be used to generate an alert for "Account with over 10 failed logons in the past hour" as an example.

The KQL summarize operator performs the calculations. To quickly see a pattern, an analyst can visualize the results in a graph. The KQL render operator performs the visualization. Combining the summarize and render operators provides the foundation for advanced visualizations, including time bucketing and time slicing.

Learn how to summarize and visualize data with a KQL statement provides the foundation to build detections in Azure Sentinel.

Learning objectives

After completing this lesson, you should be able to:

- Summarize data using KQL statements
- Render visualizations using KQL statements

Use the summarize operator

The count operator with its variations will create a new column with the calculated result for the specified fields.

The first statement below will return one column that is a unique list of Activity column values.

The second statement will return a count of SecurityEvent rows where EventID equals 4688, and the count is grouped by Process and Computer. Because of the by clause, the result set will contain three columns: Process, Computer, Count.

Run each Query separately to see the results.

```
SecurityEvent | summarize by Activity

SecurityEvent
| where EventID == "4688"
| summarize count() by Process, Computer
```

count function example

An aggregate function column can be explicitly named by including the "fieldname=" before the aggregate function.

The KQL statement will return three columns: cnt, AccountType, and Computer. The cnt field name will replace the default "count_" name.

```
SecurityEvent
| where TimeGenerated > ago(1h)
| where EventID == 4624
| summarize cnt=count() by AccountType, Computer
```

dcount function example

The following example will return a count of unique IP Addresses.

```
SecurityEvent
| summarize dcount(IPAddress)
```

Let's take a look at a real-world example

The following statement is an Azure Sentinel Analytical rule to detect a password spray attempt.

The first three where operators will filter the result set to failed logins to disabled accounts. Next, the statement "summarize" a distinct count of application name and group by User and IP Address. Finally, there is a check against a variable created (threshold) to see if the number exceeds the allowed amount.

```
let timeframe = 1d;

let threshold = 3;

SigninLogs
| where TimeGenerated >= ago(timeframe)
| where ResultType == "50057"
| where ResultDescription =~ "User account is disabled. The account has
been disabled by an administrator."
| summarize applicationCount = dcount(AppDisplayName) by UserPrincipalName,
IPAddress
| where applicationCount >= threshold
```

Use the summarize operator to filter results

The arg_max() and arg_min() functions filter out top and bottom rows respectively.

arg_max function

The following statement will return the most current row from the SecurityEvent table for the computer SQL12.NA.contosohotels.com. The * in the arg_max function requests all columns for the row.

```
SecurityEvent
| where Computer == "SQL12.NA.contosohotels.com"
| summarize arg_max(TimeGenerated,*) by Computer
```

arg_min function

In this statement, the oldest SecurityEvent for the computer SQL12.NA.contosohotels.com will be returned as the result set.

```
SecurityEvent
| where Computer == "SQL12.NA.contosohotels.com"
| summarize arg_min(TimeGenerated,*) by Computer
```

Revisiting the result pipe

The order results pass through the pipe character matters. Review the following two KQL statements. What is the difference between the result sets?

Run each Query separately to see the results.

```
// Statement 1

SecurityEvent
| summarize arg_max(TimeGenerated, *) by Account
| where EventID == "4624"

// Statement 2

SecurityEvent
| where EventID == "4624"
| summarize arg_max(TimeGenerated, *) by Account
```

Statement 1 will have Accounts for which the last activity was a login.

The SecurityEvent table will first be summarized and return the most current row for each Account. Then only rows with EventID equals 4624 (login) will be returned.

Statement 2 will have the most recent login for Accounts that have logged in.

The SecurityEvent table will be filtered to only include EventID = 4624. Then these results will be summarized for the most current login row by Account.

Use the summarize operator to prepare data

The make_ functions return a dynamic (JSON) array based on the specific function's purpose.

make_list() function

The function returns a dynamic (JSON) array of all the values of Expression in the group.

This KQL query will first filter the EventID with the where operator. Next, for each Computer, the results are a JSON array of Accounts. The resulting JSON array will include duplicate accounts.

```
SecurityEvent
| where EventID == "4624"
| summarize make_list(Account) by Computer
```

The screenshot shows the Kusto Query Editor interface. At the top, there is a toolbar with various icons and a dropdown menu. Below the toolbar, the query editor window contains the following KQL code:

```
1 SecurityEvent
2 | where EventID == "4624"
3 | summarize make_list(Account) by Computer
4
```

Below the code, the results pane is visible. It has tabs for 'Results' (which is selected), 'Chart', and 'Columns'. The results table shows the output of the query. The columns are 'Computer' and 'list_Account'. The data rows are as follows:

Computer	list_Account
DC01.NA.contosohotels.com	[{"NA.CONTOSOHOTELS.COM\\SQL01\$"}, {"NA.CONTOSOHOTELS.COM\\DC01\$"}, {"NA.CONTOSOHOTELS.COM\\SQL12\$"}, {"NA.CONTOSOHOTELS.COM\\SQL01\$"}, {"NA.CONTOSOHOTELS.COM\\SQL00\$"}, {"NA.CONTOSOHOTELS.COM\\DC01\$"}, {"NA.CONTOSOHOTELS.COM\\SQL00\$"}, {"NA.CONTOSOHOTELS.COM\\DC01\$"}, {"NA.CONTOSOHOTELS.COM\\DC11\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}, {"NA.CONTOSOHOTELS.COM\\timadmin"}, {"NA.CONTOSOHOTELS.COM\\timadmin"}, {"NA.CONTOSOHOTELS.COM\\DC10\$"}, {"NA.CONTOSOHOTELS.COM\\DC10\$"}, {"NA.CONTOSOHOTELS.COM\\VICTIM00\$"}, {"NA.CONTOSOHOTELS.COM\\SQL12\$"}, {"NA.CONTOSOHOTELS.COM\\DC10\$"}, {"NA.CONTOSOHOTELS.COM\\DC20\$"}, {"NA.CONTOSOHOTELS.COM\\MABS20\$"}, {"NA.CONTOSOHOTELS.COM\\MABS20\$"}, {"NA.CONTOSOHOTELS.COM\\MABS20\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}]
DC21.NA.contosohotels.com	[{"NA.CONTOSOHOTELS.COM\\SQL00\$"}, {"NA.CONTOSOHOTELS.COM\\DC01\$"}, {"NA.CONTOSOHOTELS.COM\\SQL00\$"}, {"NA.CONTOSOHOTELS.COM\\DC01\$"}, {"NA.CONTOSOHOTELS.COM\\SQL00\$"}, {"NA.CONTOSOHOTELS.COM\\DC01\$"}, {"NA.CONTOSOHOTELS.COM\\SQL00\$"}, {"NA.CONTOSOHOTELS.COM\\DC01\$"}, {"NA.CONTOSOHOTELS.COM\\DC11\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}, {"NA.CONTOSOHOTELS.COM\\timadmin"}, {"NA.CONTOSOHOTELS.COM\\timadmin"}, {"NA.CONTOSOHOTELS.COM\\DC10\$"}, {"NA.CONTOSOHOTELS.COM\\DC10\$"}, {"NA.CONTOSOHOTELS.COM\\VICTIM00\$"}, {"NA.CONTOSOHOTELS.COM\\SQL12\$"}, {"NA.CONTOSOHOTELS.COM\\DC10\$"}, {"NA.CONTOSOHOTELS.COM\\DC20\$"}, {"NA.CONTOSOHOTELS.COM\\MABS20\$"}, {"NA.CONTOSOHOTELS.COM\\MABS20\$"}, {"NA.CONTOSOHOTELS.COM\\MABS20\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}]
DC11.NA.contosohotels.com	[{"NA.CONTOSOHOTELS.COM\\SQL00\$"}, {"NA.CONTOSOHOTELS.COM\\DC01\$"}, {"NA.CONTOSOHOTELS.COM\\SQL00\$"}, {"NA.CONTOSOHOTELS.COM\\DC01\$"}, {"NA.CONTOSOHOTELS.COM\\SQL00\$"}, {"NA.CONTOSOHOTELS.COM\\DC01\$"}, {"NA.CONTOSOHOTELS.COM\\SQL00\$"}, {"NA.CONTOSOHOTELS.COM\\DC01\$"}, {"NA.CONTOSOHOTELS.COM\\DC11\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}, {"NA.CONTOSOHOTELS.COM\\timadmin"}, {"NA.CONTOSOHOTELS.COM\\timadmin"}, {"NA.CONTOSOHOTELS.COM\\DC10\$"}, {"NA.CONTOSOHOTELS.COM\\DC10\$"}, {"NA.CONTOSOHOTELS.COM\\VICTIM00\$"}, {"NA.CONTOSOHOTELS.COM\\SQL12\$"}, {"NA.CONTOSOHOTELS.COM\\DC10\$"}, {"NA.CONTOSOHOTELS.COM\\DC20\$"}, {"NA.CONTOSOHOTELS.COM\\MABS20\$"}, {"NA.CONTOSOHOTELS.COM\\MABS20\$"}, {"NA.CONTOSOHOTELS.COM\\MABS20\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}]
MABS20.NA.contosohotels.com	[{"NT AUTHORITY\\SYSTEM"}, {"NT AUTHORITY\\NETWORK SERV"}, {"NA.CONTOSOHOTELS.COM\\DC10\$"}, {"NA.CONTOSOHOTELS.COM\\VICTIM00\$"}, {"NA.CONTOSOHOTELS.COM\\SQL12\$"}, {"NA.CONTOSOHOTELS.COM\\DC10\$"}, {"NA.CONTOSOHOTELS.COM\\DC20\$"}, {"NA.CONTOSOHOTELS.COM\\MABS20\$"}, {"NA.CONTOSOHOTELS.COM\\MABS20\$"}, {"NA.CONTOSOHOTELS.COM\\MABS20\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}]
DC10.NA.contosohotels.com	[{"NA.CONTOSOHOTELS.COM\\DC10\$"}, {"NA.CONTOSOHOTELS.COM\\VICTIM00\$"}, {"NA.CONTOSOHOTELS.COM\\SQL12\$"}, {"NA.CONTOSOHOTELS.COM\\DC10\$"}, {"NA.CONTOSOHOTELS.COM\\DC20\$"}, {"NA.CONTOSOHOTELS.COM\\MABS20\$"}, {"NA.CONTOSOHOTELS.COM\\MABS20\$"}, {"NA.CONTOSOHOTELS.COM\\MABS20\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}]
DC20.NA.contosohotels.com	[{"NA.CONTOSOHOTELS.COM\\DC20\$"}, {"NA.CONTOSOHOTELS.COM\\MABS20\$"}, {"NA.CONTOSOHOTELS.COM\\MABS20\$"}, {"NA.CONTOSOHOTELS.COM\\MABS20\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}]
DC00.NA.contosohotels.com	[{"NA.CONTOSOHOTELS.COM\\DC00\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}, {"NA.CONTOSOHOTELS.COM\\DC00\$"}]

make_set() function

Returns a dynamic (JSON) array containing distinct values that Expression takes in the group.

This KQL query will first filter the EventID with the where operator. Next, for each Computer, the results are a JSON array of unique Accounts.

```
SecurityEvent
| where EventID == "4624"
| summarize make_set(Account) by Computer
```

The screenshot shows the Kusto Query Editor interface. At the top, there are buttons for 'Run' (highlighted in blue), 'Feedback', 'Queries', 'Query explorer', and a gear icon. Below the toolbar, a query is displayed:

```

1 SecurityEvent
2 | where EventID == "4624"
3 | summarize make_set(Account) by Computer
4

```

The results section shows the following table:

Computer	set_Account
DC01.NA.contosohotels.com	["NA.CONTOSOHOTELS.COM\SQL01\$","NA.CONTOSOHOTELS.COM\DC01\$","NA.CONTOSOHOTELS.COM\SQL12\$","NA.CONTOSOHOTELS.COM\DC21\$","NA.CONTOSOHOTE
DC21.NA.contosohotels.com	["NA.CONTOSOHOTELS.COM\SQL00\$","NA.CONTOSOHOTELS.COM\DC01\$","NA.CONTOSOHOTELS.COM\DC20\$","NA.CONTOSOHOTELS.COM\DC21\$","NA.CONTOSOHOTE
DC11.NA.contosohotels.com	["NA.CONTOSOHOTELS.COM\DC11\$","NA.CONTOSOHOTELS.COM\DC00\$","NA.CONTOSOHOTELS.COM\timadmin","NT AUTHORITY\SYSTEM","NA.CONTOSOHOTELS.COM\
MABS20.NA.contosohotels.com	["NT AUTHORITY\SYSTEM","NT AUTHORITY\NETWORK SERVICE","NT AUTHORITY\LOCAL SERVICE","Window Manager\DWIM-1","NA.CONTOSOHOTELS.COM\MABS20\$"]
DC10.NA.contosohotels.com	["NA.CONTOSOHOTELS.COM\DC10\$","NA.CONTOSOHOTELS.COM\VICTIM00\$","NA.CONTOSOHOTELS.COM\SQL12\$","NA.CONTOSOHOTELS.COM\DC00\$","NA.CONTOSO
DC20.NA.contosohotels.com	["NA.CONTOSOHOTELS.COM\DC20\$","NA.CONTOSOHOTELS.COM\MABS20\$","NA.CONTOSOHOTELS.COM\timadmin","NA.CONTOSOHOTELS.COM\DC21\$","NA.CONTO
DC00.NA.contosohotels.com	["NA.CONTOSOHOTELS.COM\DC00\$","NA.CONTOSOHOTELS.COM\DC11\$","NA.CONTOSOHOTELS.COM\SQL12\$","NA.CONTOSOHOTELS.COM\DC10\$","NA.CONTOSOHOTE

Use the render operator to create visualizations

The render operator generates a visualization of the query results.

The supported visualizations are:

- areachart
- bacchanc
- columnchart
- piechart
- scatterchart
- timechart

```

SecurityEvent
| summarize count() by Account
| render barchart

```

Use the summarize operator to create time series

The bin() function rounds values down to an integer multiple of the given bin size. Used frequently in combination with summarize by If you have a scattered set of values, the values are grouped into a smaller set of specific values. Combining the generated time series and pipe to a render operator with a type of timechart provides a time-series visualization.

```

SecurityEvent
| summarize count() by bin(TimeGenerated, 1d)
| render timechart

```

Learn more

You can learn more by reviewing the following.

[KQL quick reference | Microsoft Docs⁵](#)

[Microsoft Tech Community Security Webinars⁶](#)

[Become an Azure Sentinel Ninja⁷](#)

⁵ <https://docs.microsoft.com/azure/data-explorer/kql-quick-reference?azure-portal=true>

⁶ <https://techcommunity.microsoft.com/t5/microsoft-security-and-security-community-webinars/ba-p/927888?azure-portal=true>

⁷ <https://techcommunity.microsoft.com/t5/azure-sentinel/become-an-azure-sentinel-ninja-the-complete-level-400-training/ba-p/1246310?azure-portal=true>

Build multi-table statements using KQL

Lesson Introduction

Kusto Query Language (KQL) is the query language used to perform analysis on data to create Analytics, Workbooks, and perform Hunting in Azure Sentinel. Understanding how to correlate data from different tables with a KQL statement provides the foundation to build detections in Azure Sentinel.

You are a Security Operations Analyst working at a company that is implementing Azure Sentinel. You are responsible for performing log data analysis to search for malicious activity, display visualizations, and perform threat hunting.

To query log data, you use the Kusto Query Language (KQL). Often a result set from a KQL statement needs to be combined or joined with another result set. You can use the union operator to combine two result sets. The join operator joins rows together based on a key value. You need to understand how the order of a KQL statement impacts your expected results.

Learn how to work with multiple tables using KQL.

Learning objectives

After completing this lesson, you should be able to:

- Create queries using unions to view results across multiple tables using KQL
- Merge two tables with the join operator using KQL

Use the union operator

The union operator takes two or more tables and returns the rows of all of them. Understanding how results are passed and impacted with the pipe character is essential.

Based on the time window set in the Query window:

- Query 1 will return all rows of SecurityEvent and all rows of SecurityAlert
- Query 2 will return one row and column, which is the count of all rows of SecurityEvent and all rows of SecurityAlert
- Query 3 will return all rows of SecurityEvent and one row for SecurityAlert. The row for SecurityAlert will have the count of the SecurityAlert rows.

Run each Query separately to see the results.

```
// Query 1

SecurityEvent
| union SecurityAlert

// Query 2

SecurityEvent
| union SecurityAlert
| summarize count()
| project count_


// Query 3
```

```
SecurityEvent
| union (SecurityAlert | summarize count())
| project count_
```

The union operator supports wildcards to union multiple tables. The following KQL will create a count for the rows in all tables with names that start with Security.

```
union Security*
| summarize count() by Type
```

Use the join operator

The join operator merges the rows of two tables to form a new table by matching the specified columns' values from each table.

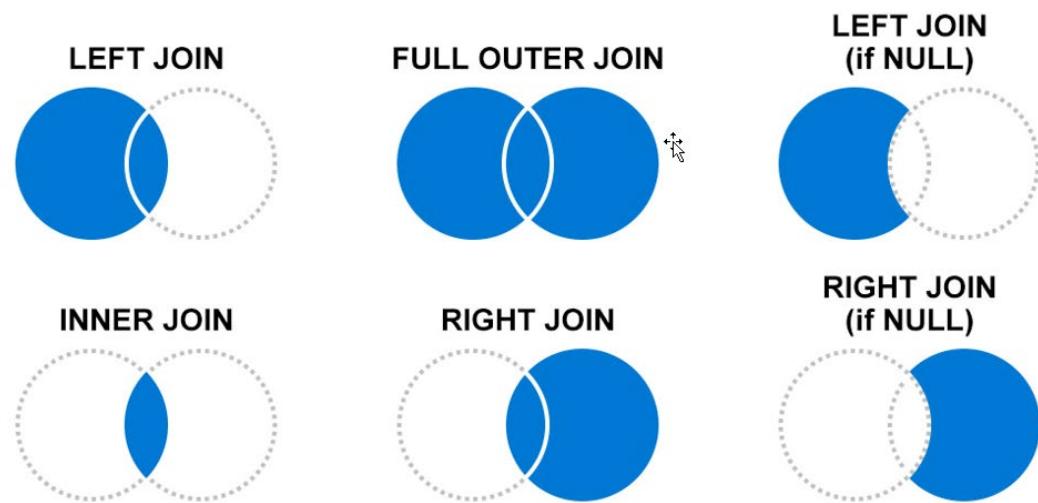
Syntax

LeftTable | join [JoinParameters] (RightTable) on Attributes

```
SecurityEvent
| where EventID == "4624"
| summarize LogOnCount=count() by EventID, Account
| project LogOnCount, Account
| join kind = inner (
    SecurityEvent
    | where EventID == "4634"
    | summarize LogOffCount=count() by EventID, Account
    | project LogOffCount, Account
) on Account
```

The first table specified in the join is considered the Left table. The table after the join keyword is the right table. When working with columns from the tables, the `$left.Column` name and `$right.Column` name is to distinguish which tables column are referencing.

When joining tables, you use Join flavors to determine the joining behavior. It is essential to understand the impact of records on the left and right side based on the join flavor. The graphic below shows which records will be kept if there is or isn't a matching record in the other dataset. The **inner join** will only show records from the left side if there is a matching record on the right side. The right side will also require a left side record.



Join Flavor	Output Records
kind=leftanti, kind=leftantisemi	Returns all the records from the left side that don't have matches from the right
kind=rightanti, kind=rightantisemi	Returns all the records from the right side that don't have matches from the left.
kind unspecified, kind=innerunique	Only one row from the left side is matched for each value of the on key. The output contains a row for each match of this row with rows from the right
kind=leftsemi	Returns all the records from the left side that have matches from the right.
kind=rightsemi	Returns all the records from the right side that have matches from the left.
kind=inner	Contains a row in the output for every combination of matching rows from left and right.
kind=leftouter (or kind=rightouter or kind=full-outer)	Contains a row for every row on the left and right, even if it has no match. The unmatched output cells contain nulls.

Learn more

You can learn more by reviewing the following.

[KQL quick reference | Microsoft Docs⁸](#)

[Microsoft Tech Community Security Webinars⁹](#)

[Become an Azure Sentinel Ninja¹⁰](#)

⁸ <https://docs.microsoft.com/azure/data-explorer/kql-quick-reference?azure-portal=true>

⁹ <https://techcommunity.microsoft.com/t5/microsoft-security-and-security-community-webinars/ba-p/927888?azure-portal=true>

¹⁰ <https://techcommunity.microsoft.com/t5/azure-sentinel/become-an-azure-sentinel-ninja-the-complete-level-400-training/ba-p/1246310?azure-portal=true>

Work with string data using KQL statements

Lesson Introduction

Kusto Query Language (KQL) is the query language used to perform analysis on data to create Analytics, Workbooks, and perform Hunting in Azure Sentinel. Understanding how to work with fields containing structured and unstructured string data with a KQL statement provides the foundation for extracting data used in building detections in Azure Sentinel.

You are a Security Operations Analyst working at a company that is implementing Azure Sentinel. You are responsible for performing log data analysis to search for malicious activity, display visualizations, and perform threat hunting.

To query log data, you use the Kusto Query Language (KQL). Often fields in a table store structured and unstructured string data. You write KQL statements to extract and manipulate data stored in these fields. A typical scenario is a key-value pair stored in a field, and you need to query the specific value of a key.

Learn how to use the Kusto Query Language (KQL) to manipulate string data ingested from log sources.

Learning objectives

After completing this lesson, you should be able to:

- Extract data from unstructured string fields using KQL
- Extract data from structured string data using KQL
- Create Functions using KQL

Extract data from unstructured string fields

Security log data is often contained in unstructured string fields and requires parsing to extract data. There are multiple ways of pulling information from string fields in KQL. The two primary operators used are extract and parse.

extract

Extract gets a match for a regular expression from a text string. You have the option to convert the extracted substring to the indicated type.

```
print extract("x=([0-9.]+)", 1, "hello x=45.6|wo") == "45.6"
```

Arguments

- regex: A regular expression.
- captureGroup: A positive int constant indicating the capture group to extract. 0 stands for the entire match, 1 for the value matched by the first '(' parenthesis' in the regular expression, 2 or more for subsequent parentheses.
- text: A string to search.
- typeLiteral: An optional type literal (e.g., typeof(long)). If provided, the extracted substring is converted to this type.

Returns

If regex finds a match in text: the substring matched against the indicated capture group captureGroup, optionally converted to typeLiteral.

If there's no match, or the type conversion fails: null.

The following example uses the extract function to pull out the Account Name from the Account field of the SecurityEvent table.

```
// Shows fail user logons divided in to account names in attempts. Shows 5
top account names and others are named 'Other'.

// Tags: #Initial Access #LateralMovement #Persistence

let top5 = SecurityEvent
| where EventID == 4625 and AccountType == 'User'
| extend Account_Name = extract(@"^(.*\\)?([^\0]*)(@.*)?$", 2, tolower(Account))
| summarize Attempts = count() by Account_Name
| where Account_Name != ""
| top 5 by Attempts
| summarize make_list(Account_Name);

SecurityEvent
| where EventID == 4625 and AccountType == 'User'
| extend Name = extract(@"^(.*\\)?([^\0]*)(@.*)?$", 2, tolower(Account))
| extend Account_Name = iff(Name in (top5), Name, "Other")
| where Account_Name != ""
| summarize Attempts = count() by Account_Name
```

parse

Evaluates a string expression and parses its value into one or more calculated columns. The computed columns will have nulls for unsuccessfully parsed strings.

Syntax

T | parse [kind=regex [flags=regex_flags] |simple|relaxed] Expression with * (StringConstant ColumnName [: ColumnType]) *...

Arguments

- T: The input table.
- kind:
 - simple (the default): StringConstant is a regular string value and the match is strict. All string delimiters should appear in the parsed string, and all extended columns must match the required types.
 - regex: StringConstant may be a regular expression and the match is strict. All string delimiters, which can be a regex for this mode, should appear in the parsed string, and all extended columns must match the required types.
 - flags: Flags to be used in regex mode like U (Ungreedy), m (multi-line mode), s (match new line \n), i (case-insensitive) in RE2 flags.

- relaxed: StringConstant is a regular string value and the match is relaxed. All string delimiters should appear in the parsed string, but extended columns may partially match the required types. Extended columns that didn't match the required types will get the value null.
- Expression: An expression that evaluates to a string.
- ColumnName: The name of a column to assign a value to, extracted from the string expression.
- ColumnType: Optional. The scalar value that indicates the type to convert the value to. The default is the string type.

Returns

The input table extended according to the list of columns that are provided to the operator.

The following example uses a parse to SQL Audit events in the Application log of Windows Events.

Note: This example is not available in the demo environment.

```
// KQL SQL Audit Event Parser

let SQLData = Event
| where Source has "MSSQL"
;

let Sqlactivity = SQLData
| where RenderedDescription !has "LGIS" and RenderedDescription !has "LGIF"
| parse RenderedDescription with * "action_id:" Action:string
    " " *
| parse RenderedDescription with * "client_ip:" ClientIP:string
" permission" *
| parse RenderedDescription with * "session_server_principal_name:" CurrentUser:string
" " *
| parse RenderedDescription with * "database_name:" DatabaseName:string
"schema_name:" Temp:string
"object_name:" ObjectName:string
"statement:" Statement:string
". " *
;
;

let FailedLogon = SQLData
| where EventLevelName has "error"
| where RenderedDescription startswith "Login"
| parse kind=regex RenderedDescription with "Login" LogonResult:string
    "for user '" CurrentUser:string
    "'. Reason:" Reason:string
    "provided" *
| parse kind=regex RenderedDescription with * "CLIENT" * ":" ClientIP:string
    "] " *
;
;

let dbfailedLogon = SQLData
| where RenderedDescription has " Failed to open the explicitly specified
database"
```

```
| parse kind=regex RenderedDescription with "Login" LogonResult:string  
    "for user '" CurrentUser:string  
    "'." Reason:" Reason:string  
    " '" DatabaseName:string  
    "''' *  
  
| parse kind=regex RenderedDescription with * "CLIENT" * ":" ClientIP:string  
    "]" *  
;  
  
let successLogon = SQLData  
| where RenderedDescription has "LGIS"  
| parse RenderedDescription with * "action_id:" Action:string  
    " " LogonResult:string  
    ":" Temp2:string  
    "session_server_principal_name:" CurrentUser:string  
    " " *  
| parse RenderedDescription with * "client_ip:" ClientIP:string  
    " " *  
;  
(union isfuzzy=true  
Sqlactivity, FailedLogon, dbfailedLogon, successLogon )  
| project TimeGenerated, Computer, EventID, Action, ClientIP, LogonResult,  
CurrentUser, Reason, DatabaseName, ObjectName, Statement
```

Extract data from structured string data

Strings fields may also contain structured data like JSON or Key-Value pairs. KQL provides easy access to these values for further analysis.

Dynamic Fields

Within a Log Analytics table, there are field types defined as Dynamic. Dynamic fields contain a key-value pair such as:

```
{"eventCategory":"Autoscale","eventName":"GetOperationStatusResult","operationId":"xxxxxxxx-6a53-4aed-bab4-575642a10226","eventProperties": "{\"OldInstancesCount\":6,\"NewInstancesCount\":5}","eventDataId":"xxxxxxxx -efe3-43c2-8c86-cd84f70039d3","eventSubmissionTimestamp":"2020-11-30T04:06:17.0503722Z","resource":"ch-appfevmss-pri","resourceGroup":"CH-RE-TAILRG-PRI","resourceProviderValue":"MICROSOFT.COMPUTE","subscriptionId":"xxxxxxxx -7fde-4caf-8629-41dc15e3b352","activityStatusValue":"Succeeded"}
```

To access the strings within a Dynamic field, use the dot notation. The Properties_d field from the AzureActivity table is of type dynamic. In this example, you could access the eventCategory with the Properties_d.eventCategory field name.

```
AzureActivity  
| project Properties_d.eventCategory
```

The following example shows the use of Dynamic fields with the SigninLogs table.

Note: This example is not available in the demo environment.

```
// Example query for SigninLogs showing how to break out packed fields.

SigninLogs
| where TimeGenerated >= ago(1d)
| extend OS = DeviceDetail.operatingSystem, Browser = DeviceDetail.browser
| extend ConditionalAccessPol0Name = tostring(ConditionalAccessPolicies[0].displayName), ConditionalAccessPol0Result = tostring(ConditionalAccessPolicies[0].result)
| extend ConditionalAccessPol1Name = tostring(ConditionalAccessPolicies[1].displayName), ConditionalAccessPol1Result = tostring(ConditionalAccessPolicies[1].result)
| extend ConditionalAccessPol2Name = tostring(ConditionalAccessPolicies[2].displayName), ConditionalAccessPol2Result = tostring(ConditionalAccessPolicies[2].result)
| extend StatusCode = tostring(Status.errorCode), StatusDetails = tostring(Status.additionalDetails)
| extend State = tostring(LocationDetails.state), City = tostring(LocationDetails.city)
| extend Date = startofday(TimeGenerated), Hour = datetime_part("Hour", TimeGenerated)
| summarize count() by Date, Identity, UserDisplayName, UserPrincipalName, IPAddress, ResultType, ResultDescription, StatusCode, StatusDetails, ConditionalAccessPol0Name, ConditionalAccessPol0Result, ConditionalAccessPol1Name, ConditionalAccessPol1Result, ConditionalAccessPol2Name, ConditionalAccessPol2Result, Location, State, City
| sort by Date
```

JSON

KQL provides functions to manipulate JSON stored in string fields. Many logs submit data in JSON format, which requires you to know how to transform JSON data to queryable fields.

The following is a list of JSON related functions.

Function	Description
parse_json() or todynamic()	Interprets a string as a JSON value and returns the value as dynamic. Use either of these to refer to a field: JsonField.Key or JsonField["Key"]
mv_expand()	is applied on a dynamic-typed array or property bag column so that each value in the collection gets a separate row. All the other columns in an expanded row are duplicated. mv_expand is the easiest way to process JSON arrays.

Function	Description
mv_apply()	Applies a subquery to each record and returns the union of the results of all subqueries. Apply a query to each value in an array.

Run each query separately to see the results.

```
SecurityAlert
| extend ExtendedProperties = todynamic(ExtendedProperties)
| extend ActionTaken = ExtendedProperties.ActionTaken
| extend AttackerIP = ExtendedProperties["Attacker IP"]

SecurityAlert
| mv-expand entity = todynamic(Entities)

SecurityAlert
| mv-apply entity = todynamic(Entities) on
( where entity.Type == "account" | extend account = strcat (entity.NTDomain, "\\\", entity.Name))
```

Integrate external data

The externaldata operator returns a table whose schema is defined in the query itself and whose data is read from an external storage artifact, such as a blob in Azure Blob Storage or an Azure Data Lake Storage file.

Syntax

```
externaldata ( ColumnName : ColumnType [, ...] )
[ StorageConnectionString [, ...] ]
[with (PropertyName = PropertyValue [, ...] )]
```

Arguments

- ColumnName, ColumnType: The arguments define the schema of the table. The syntax is the same as the syntax used when defining a table in .create table.
- StorageConnectionString: Storage connection strings that describe the storage artifacts holding the data to return.
- PropertyName, PropertyValue, ...: Additional properties that describe how to interpret the data retrieved from storage, as listed under ingestion properties.

Currently, supported properties are:

ARGUMENTS

Property	Type	Description
format	string	Data format. If not specified, an attempt is made to detect the data format from file extension (defaults to CSV). Any of the ingestion data formats are supported.
ignoreFirstRecord	bool	If set to true, indicates that the first record in every file is ignored. This property is useful when querying CSV files with headers.
ingestionMapping	string	A string value that indicates how to map data from the source file to the actual columns in the operator result set. See data mappings.

Returns

The externaldata operator returns a data table of the given schema with data parsed from the specified storage artifact, indicated by the storage connection string.

Note: This example is not available in the demo environment.

```
Users
| where UserID in ((externaldata (UserID:string) [
    @"https://storageaccount.blob.core.windows.net/storagecontainer/users.
    txt"
        h@"?...SAS..." // Secret token needed to access the blob
    ]))
| ...
```

Create parsers using functions

Parsers are functions that define a virtual table with already parsed unstructured strings fields such as Syslog data.

The following is a KQL query created by the community for Mailbox forwarding monitoring.

In the Logs window, you create a query, click the Save button, enter the Name, and select Save As Function from the drop-down. In this case, if we name the function "MailboxForward." I can then access the table using the name MailboxForward.

```
OfficeActivity
| where TimeGenerated >= ago(30d)
| where Operation == 'New-InboxRule'
| extend details = parse_json(Parameters)
| where details contains 'ForwardTo' or details contains 'RedirectTo'
| extend ForwardTo = iif(details[0].Name contains 'ForwardTo', de-
tails[0].Value,
    iif(details[1].Name contains 'ForwardTo', details[1].Value,
```

```
iif(details[2].Name contains 'ForwardTo', details[2].Value,
    iif(details[3].Name contains 'ForwardTo', details[3].Value,
        iif(details[4].Name contains 'ForwardTo', details[4].
Value,
            'Check Parameters'))))
| extend RedirectTo = iif(details[0].Name contains 'RedirectTo', de-
tails[0].Value,
    iif(details[1].Name contains 'RedirectTo', details[1].Value,
        iif(details[2].Name contains 'RedirectTo', details[2].Value,
            iif(details[3].Name contains 'RedirectTo', details[3].
Value,
                iif(details[4].Name contains 'RedirectTo', details[4].
Value,
                    'Check Parameters'))))
| extend RuleName = iif(details[3].Name contains 'Name', details[3].
Value,
    iif(details[4].Name contains 'Name', details[4].Value,
        iif(details[5].Name contains 'Name', details[5].Value,
            'Check Parameters')))
| extend RuleParameters = iif(details[2].Name != 'ForwardTo' and de-
tails[2].Name != 'RedirectTo',
    strcat(tostring(details[2].Name), '-', tostring(details[2].Value)),
    iif(details[3].Name != 'ForwardTo' and details[3].Name != 'Redi-
rectTo' and details[3].Name != 'Name',
        strcat(tostring(details[3].Name), '-', tostring(details[3].
Value)),
        iff(details[4].Name != 'ForwardTo' and details[4].Name != 'RedirectTo' and details[4].Name != 'Name' and details[4].Name != 'StopPro-
cessingRules',
            strcat(tostring(details[4].Name), '-', tostring(details[4].
Value)),
            'All Mail')))
| project TimeGenerated, Operation, RuleName, RuleParameters, iif(de-
tails contains 'ForwardTo', ForwardTo, RedirectTo), ClientIP, UserId
| project-rename Email_Forwarded_To = Column1, Creating_User = UserId
```

MailboxForward

Learn more

You can learn more by reviewing the following.

[KQL quick reference | Microsoft Docs¹¹](#)

[Microsoft Tech Community Security Webinars¹²](#)

¹¹ <https://docs.microsoft.com/azure/data-explorer/kql-quick-reference?azure-portal=true>

¹² <https://techcommunity.microsoft.com/t5/microsoft-security-and-security-community-webinars/ba-p/927888?azure-portal=true>

Become an Azure Sentinel Ninja¹³

¹³ <https://techcommunity.microsoft.com/t5/azure-sentinel/become-an-azure-sentinel-ninja-the-complete-level-400-training/ba-p/1246310?azure-portal=true>

Knowledge check

Check your Knowledge

Multiple choice

Item 1. What does the search operator do?

- Searches across tables and is not column-specific.
- Searches only data in the last hour.
- Searches in columns specified.

Multiple choice

Item 2. What are project operators?

- Project operators filter a table to the subset of rows that satisfy a predicate.
- Project operators create summarized columns and append them to the result set.
- Project operators add, remove, or rename columns in a result set.

Multiple choice

Item 3. The dcount() function will do which of the following?

- Return a day count on the expression difference provided to the function.
- Return a difference count on the expression provided to the function.
- Return a distinct count on the expression provided to the function.

Multiple choice

Item 4. The arg_max() function will do which of the following?

- Return the maximum value across a group.
- Return a JSON Array of the max values.
- Return the most current row.

Multiple choice

Item 5. The bin() function provides the most value to which type of chart?

- scatterchart
- timechart
- barchart

Multiple choice

Item 6. Which join flavor contains a row in the output for every combination of matching rows from left and right?

- kind=leftouter
- kind=inner
- kind=fullouter

Multiple choice

Item 7. When using the join operator, how do you specify fields from each table?

- \$1.columnname and \$2.columnname
- \$left.columnname and \$right.columnname
- \$inner.columnname and \$outer.columnname

Multiple choice

Item 8. When you union two tables, the two tables need matching columns?

- No.
- Yes.
- Only when the project operator is used.

Multiple choice

Item 9. Which KQL statement should you use to parse external data into a virtual table?

- parse_json
- extract
- externaldata

Multiple choice

Item 10. A Dynamic field contains which of the following items?

- Calculated data.
- Key-value pair data.
- External data.

Multiple choice

Item 11. To create a virtual table, save your KQL as a which type?

- Module.
- Function.
- Definition.

Lab - Create queries for Azure Sentinel using KQL

Lab: Create queries for Azure Sentinel using Kusto Query Language

To download the most recent version of this lab, please visit the SC-200 [GitHub repository¹⁴](#).

Note: Depending on the lab hosting solution used for your class delivery, the lab instructions may display directly in the virtual lab environment, in addition to being available in the GitHub repository. In that case, follow guidance from your instructor as to where you will access the lab steps from. Even if the GitHub version is not used for your class, you may still find it useful to be able to reference the lab instructions on GitHub after class is over.

Lab scenario

You are a Security Operations Analyst working at a company that is implementing Azure Sentinel. You are responsible for performing log data analysis to search for malicious activity, display visualizations, and perform threat hunting. To query log data, you use the Kusto Query Language (KQL).

Objectives

After you complete this lab, you will be able to:

- Run Basic KQL Statements.
- Analyze Results in KQL with the Summarize Operator.
- Create visualizations in KQL with the Render Operator.
- Build multi-table statements in KQL.
- Work with string data in KQL.

Lab setup

- Estimated time: 60 minutes

¹⁴ <https://github.com/MicrosoftLearning/SC-200T00A-Microsoft-Security-Operations-Analyst>

Answers

Multiple choice

Item 1. What does the search operator do?

- Searches across tables and is not column-specific.
- Searches only data in the last hour.
- Searches in columns specified.

Explanation

The search will search across all columns in tables specified.

Multiple choice

Item 2. What are project operators?

- Project operators filter a table to the subset of rows that satisfy a predicate.
- Project operators create summarized columns and append them to the result set.
- Project operators add, remove, or rename columns in a result set.

Explanation

project operators control what columns to include, add, remove or rename in the result set of a statement.

Multiple choice

Item 3. The `dcount()` function will do which of the following?

- Return a day count on the expression difference provided to the function.
- Return a difference count on the expression provided to the function.
- Return a distinct count on the expression provided to the function.

Explanation

dcount provides a distinct count.

Multiple choice

Item 4. The `arg_max()` function will do which of the following?

- Return the maximum value across a group.
- Return a JSON Array of the max values.
- Return the most current row.

Explanation

The arg_max function returns the most current row in the result set based on the by clause.

Multiple choice

Item 5. The `bin()` function provides the most value to which type of chart?

- scatterchart
- timechart
- barchart

Explanation

Bin() will round down values to an integer multiple of the given bin size. The timechart displays a time series based on the bin size.

Multiple choice

Item 6. Which join flavor contains a row in the output for every combination of matching rows from left and right?

- kind=leftouter
- kind=inner
- kind=fullouter

Explanation

Inner contains a row in the output for every combination of matching rows from left and right.

Multiple choice

Item 7. When using the join operator, how do you specify fields from each table?

- \$1.columnname and \$2.columnname
- \$left.columnname and \$right.columnname
- \$inner.columnname and \$outer.columnname

Explanation

The \$left and \$right preceding the field name specifies the table.

Multiple choice

Item 8. When you union two tables, the two tables need matching columns?

- No.
- Yes.
- Only when the project operator is used.

Explanation

The results contain all columns from both tables.

Multiple choice

Item 9. Which KQL statement should you use to parse external data into a virtual table?

- parse_json
- extract
- externaldata

Explanation

Use the externaldata operator to create a virtual table from an external source.

Multiple choice

Item 10. A Dynamic field contains which of the following items?

- Calculated data.
- Key-value pair data.
- External data.

Explanation

The properties in the field are accessed with the dot notation.

Multiple choice

Item 11. To create a virtual table, save your KQL as a which type?

- Module.
- Function.
- Definition.

Explanation

Functions then can be referenced in other KQL statements.

Module 5 Configure your Azure Sentinel environment

Introduction to Azure Sentinel

Lesson Introduction

Imagine that you work as a security operations center (SOC) analyst. Your organization wants to advance its security-management capabilities. The business has already started moving some workloads to the public cloud.

You've been asked to evaluate security information and event management (SIEM) solutions that can help in both an on-premises and a multiple-cloud environment. You've heard about Azure Sentinel and want to find out whether it could be the right SIEM solution for your business.

Ideally, you'd select a service that provides the features and functionality that you need, with minimal administration and a flexible pricing model.

Azure Sentinel offers exactly those benefits.

In this lesson, you'll explore Azure Sentinel and discover why and when to use it. You'll investigate the key features and capabilities of Azure Sentinel, including how and when to deploy it.

Learning objectives

After completing this lesson, you should be able to:

- Identify the various components and functionality of Azure Sentinel.
- Identify use cases where Azure Sentinel would be a good solution.

Azure Sentinel explained

Let's start with a few definitions and a look at *security information and event management* (SIEM) systems and Azure Sentinel.

What is security incident and event management (SIEM)?

A SIEM system is a tool that an organization uses to collect, analyze, and perform security operations on its computer systems. Those systems can be hardware appliances, applications, or both.

In its simplest form, a SIEM system enables you to:

- Collect and query logs.
- Do some form of correlation or anomaly detection.
- Create alerts and incidents based on your findings.

A SIEM system might offer functionality such as:

- **Log management:** The ability to collect, store, and query the log data from resources within your environment.
- **Alerting:** A proactive look inside the log data for potential security incidents and anomalies.
- **Visualization:** Graphs and dashboards that provide visual insights into your log data.
- **Incident management:** The ability to create, update, assign, and investigate incidents that have been identified.
- **Querying data:** A rich query language, similar to that for log management, that you can use to query and understand your data.

What is Azure Sentinel?

Azure Sentinel is a cloud-native SIEM system that a security operations team can use to:

- Get security insights across the enterprise by collecting data from virtually any source.
- Detect and investigate threats quickly by using built-in machine learning and Microsoft threat intelligence.
- Automate threat responses by using playbooks and by integrating Azure Logic Apps.

Unlike with traditional SIEM solutions, to run Azure Sentinel, you don't need to install any servers either on-premises or in the cloud. Azure Sentinel is a service that you deploy in Azure. You can get up and running with Sentinel in just a few minutes in the Azure portal.

Azure Sentinel is tightly integrated with other cloud services. Not only can you quickly ingest logs, but you can also use other cloud services natively (for example, authorization and automation).

Azure Sentinel helps you enable end-to-end security operations including collection, detection, investigation, and response:



Let's take a look at the key components in Azure Sentinel.

How Azure Sentinel works

As you've already learned, Azure Sentinel helps you enable end-to-end security operations. It starts with log ingestion and continues through to automated response to security alerts.

Here are the key features and components of Azure Sentinel.

Data connectors

The first thing to do is to have your data ingested into Azure Sentinel. Data connectors enable you to do just that. You can add some services, such as Azure activity logs, just by selecting a button. Others, such as syslog, require a little configuration. There are data connectors that cover all scenarios and sources, including but not limited to:

- syslog
- Common Event Format (CEF)
- Trusted Automated eXchange of Indicator Information (TAXII) (for threat intelligence)
- Azure
- AWS services

The screenshot shows the Azure Sentinel Data connectors page. At the top, it displays '56 Connectors' (3 Connected, 0 Coming soon). Below this is a search bar and filters for 'Providers: All', 'Data Types: All', and 'Status: All'. The main area lists various connectors with their names and providers: AI Vectra Detect (Preview) - Vectra AI, Alcide kAudit (Preview) - Alcide, Amazon Web Services - Amazon, Azure Active Directory - Microsoft, Azure Active Directory Identity Protection - Microsoft, Azure Activity - Microsoft, and Azure Advanced Threat Protection (Preview) - Microsoft. To the right, there's a sidebar for 'Azure Activity' showing connected status, provider (Microsoft), and last log received (5 hours ago). Below that is a section for related content (1 Workbooks, 2 Queries, 7 Analytic rules template), data received (140, 120), and a link to 'Open connector page'.

Log retention

After it's been ingested into Azure Sentinel, your data is stored by using Log Analytics. The benefits of using Log Analytics include the ability to use the Kusto Query Language (KQL) to query your data. KQL is a rich query language that gives you the power to dive into and gain insights from our data.

The screenshot shows the Azure Sentinel Logs interface. On the left, there's a navigation sidebar with sections like General, Overview, Logs (which is selected), News & guides, Threat management, Configuration, and Settings. The main area has a search bar at the top, followed by a 'New Query' button and a warning message about resource consumption. Below that is a table with a single row: '1 AzureActivity | where Level != "Informational"'. The table includes columns for TimeGenerated [UTC], CallerIpAddress, CategoryValue, and CorrelationId. The results show several log entries from August 25, 2020, at various times between 2:54:29 and 4:34:48 PM, all categorized as 'Policy'.

Workbooks

You use workbooks to visualize your data within Azure Sentinel. Think of workbooks as dashboards. Each component in the dashboard is built by using an underlying KQL query of your data. You can use the built-in workbooks within Azure Sentinel, edit them to meet your own needs, or create your own workbooks from scratch. If you've used Azure Monitor workbooks, this feature will be familiar to you because it's Sentinel's implementation of Monitor workbooks.

The screenshot shows a SharePoint & OneDrive workbook. At the top, there are filters for TimeRange (Last 30 days), Operations (All), Users (All), and Workspaces (All). The 'General overview' section displays three metrics: All (5.01k), OneDrive (3.26k), and SharePoint (1.76k). The 'Operation summary' section lists operations with their counts: FileAccessed (3327), FileModified (1042), SearchQueryPerformed (335), FilePreviewed (149), and PageViewed (62). The 'Activities over time' section is a line chart showing the count of various operations over time, with specific values labeled at the bottom: FileAccessed (Sum) 3.33k, FileModified (Sum) 1.04k, SearchQueryPerformed (Sum) 335, FilePreviewed (Sum) 149, PageViewed (Sum) 62, DipClassification (Sum) 33, FileAccessedExtended (Sum) 17, ListColumnCreated (Sum) 10, ListColumnUpdated (Sum) 8, ListItemCreated (Sum) 7, ListItemUpdated (Sum) 22, Other (Sum) 22.

Analytics alerts

So far, you have your logs and some data visualization. Now it would be great to have some proactive analytics across your data, so you're notified when something suspicious occurs. You can enable built-in analytics alerts within your Sentinel workspace. There are various types of alerts, some of which you can edit to your own needs. Other alerts are built on machine-learning models that are proprietary to Microsoft. You can also create custom, scheduled alerts from scratch.

The screenshot shows the Azure Sentinel Analytics interface. On the left, there's a navigation sidebar with sections like General, Threat management, Configuration, and Analytics (which is selected). The main area displays a list of 'Active rules' with the following columns: Severity, Name, Rule Type, and Data Sources. There are 2 active rules listed:

Severity	Name	Rule Type	Data Sources
High	Create incidents based on Azure Security Center...	Microsoft Security (Preview)	Azure Security Center for IoT (Pr...
High	Suspicious application consent similar to O365 ...	Scheduled	Azure Active Directory
High	Known Phosphorus group domains/IP	Scheduled	DNS (Preview) +4
High	Known IRIDIUM IP	Scheduled	Office 365 +10
High	Create incidents based on Azure Active Director...	Microsoft Security (Preview)	Azure Active Directory Identity P...
High	THALLIUM domains included in DCU takedown	Scheduled	DNS (Preview) +3
High	Create incidents based on Microsoft Defender ...	Microsoft Security (Preview)	Microsoft Defender Advanced T...
IN USE	Advanced Multistage Attack Detection	Fusion	
High	Create incidents based on Azure Security Cente...	Microsoft Security (Preview)	Azure Security Center
High	Known Manganese IP and UserAgent activity	Scheduled	Office 365

On the right side, there's a detailed view of the last rule: 'Known Manganese IP and UserAgent ac...'. It shows the rule type as 'High Severity Scheduled Rule Type', its description, data sources used (Office 365, OfficeActivity (SharePoint)), and a note indicating it hasn't been used yet. A 'Create rule' button is also present.

Threat hunting

We won't dive deeply into threat hunting in this module. However, if SOC analysts need to hunt for suspicious activity, there are some built-in hunting queries that they can use. Analysts can also create their own queries. Sentinel also integrates with Azure Notebooks. It provides example notebooks for advanced hunters who want to use the full power of a programming language to hunt through their data.

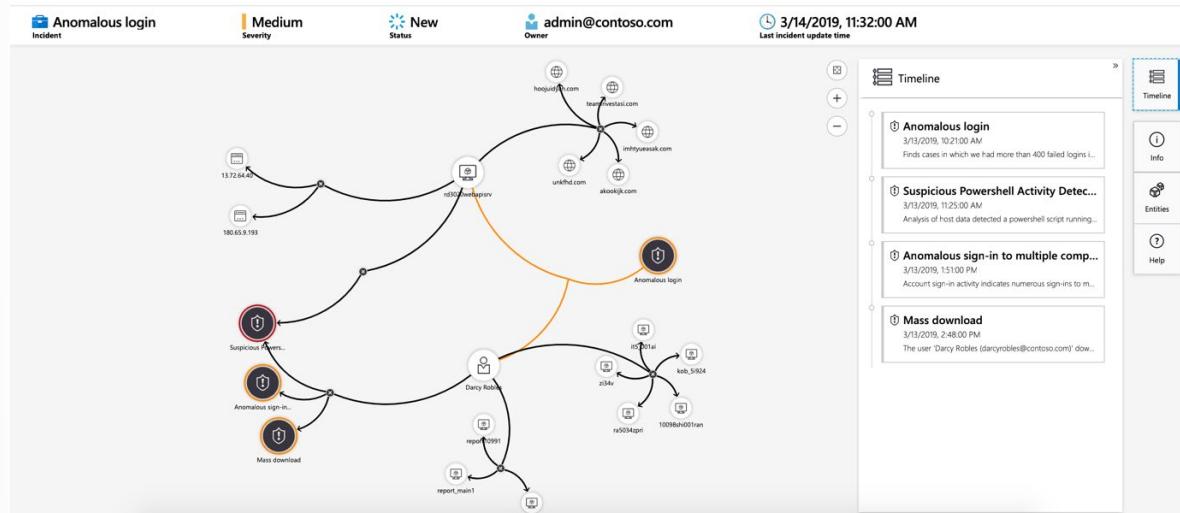
The screenshot shows the Azure Sentinel Hunting interface. The left sidebar includes sections for General, Threat management, Configuration, and Hunting (selected). The main area displays a list of 'Queries' with columns: Provider, Data Source, Results, and Tactics. There are 92 total queries listed:

Provider	Data Source	Results	Tactics
Microsoft	AWSCloudTrail	--	Persistence
Microsoft	AuditLogs +1	--	Discovery
Microsoft	AuditLogs	--	Discovery
Microsoft	AuditLogs +1	--	Discovery
Microsoft	AzureActivity	--	Discovery
Microsoft	DnsEvents	--	Discovery
Microsoft	DnsEvents	--	Discovery
Microsoft	DnsEvents	--	Discovery
Microsoft	DnsEvents	--	Discovery
Microsoft	DnsEvents	--	Discovery

On the right, there's a detailed view of a specific query: 'Changes made to AWS IAM policy'. It shows the provider (AWSCloudTrail), data source (AuditLogs), and a description of the query: 'Identity and Access Management (IAM) securely manages access to AWS services and resources. This query looks for when an API call is made to change an IAM, particularly those related to new policies being attached to users and roles, as well as changes to access methods and changes to account level policies. If these turn out to be noisy filter out the most common for your environment'. Below this, there's a 'Run Query' button and a 'View Results' button.

Incidents and investigations

An incident is created when an alert that you've enabled is triggered. In Azure Sentinel, you can do standard incident management tasks like changing status or assigning incidents to individuals for investigation. Azure Sentinel also has investigation functionality, so you can visually investigate incidents by mapping entities across log data along a timeline.



Automation playbooks

With the ability to respond to incidents automatically, you can automate some of your security operations and make your SOC more productive. Azure Sentinel integrates with Azure Logic Apps, enabling you to create automated workflows, or *playbooks*, in response to events. This functionality could be used for incident management, enrichment, investigation, or remediation. These capabilities are often referred to as *security orchestration, automation, and response (SOAR)*.

The screenshot shows the Azure Logic App Designer interface for a template named 'yoafrTestAlertsTemplate'. The left sidebar lists various tools and settings, with 'Logic app designer' selected. The main workspace shows a workflow starting with a trigger 'When an Azure Security Center Alert is created or triggered' (with a preview showing an alert from 'Alert name: Alert Display Name'). This triggers a 'Send an email (V2)' action. The 'Send an email' step has a configuration panel with a rich text editor and fields for 'Body' containing a template message about a discovered security threat, and 'Subject' and 'To' fields. The URL for the logic app is <https://logicapps.yoafrengel.com/api/sendEmail>.

As the SOC Analyst, you now start to see how Azure Sentinel might help you achieve your goals. For example, you could:

- Ingest data from your cloud and on-premises environments.

- Perform analytics on that data.
- Manage and investigate any incidents that occur.
- Perhaps even respond automatically by using playbooks.

In other words, Azure Sentinel gives you an end-to-end solution for your security operations.

When to use Azure Sentinel

Azure Sentinel is a solution for performing security operations on your cloud and on-premises environments.

Use Azure Sentinel if you want to:

- Collect event data from various sources.
- Perform security operations on that data to identify suspicious activity.

Security operations could include:

- Visualization of log data.
- Anomaly detection.
- Threat hunting.
- Security incident investigation
- Automated response to alerts and incidents.

Azure Sentinel offers other capabilities that could help you decide whether it's the right fit for you:

- Cloud-native SIEM. There are no servers to provision, so scaling is effortless.
- Integration with the Azure Logic Apps service and its hundreds of connectors.
- Benefits of Microsoft research and machine learning.
- Key log sources provided for free.
- Support for hybrid cloud and on-premises environments.
- SIEM and a data lake all in one.

When you began investigating Azure Sentinel, your organization had some clear requirements:

- Support for data from multiple cloud environments
- Features and functionality required for a security operations center (SOC), without too much administrative overhead

You've found that Azure Sentinel could be a good fit. It offers data connectors for syslog, Amazon Web Services (AWS), and other sources, and the ability to scale effortlessly without provisioning servers. During your analysis, you also realized that your organization should make automation a key part of its SOC strategy. Automation wasn't something the organization had considered before, but now you'll look into using automation playbooks.

If you're collecting infrastructure or application logs for performance monitoring, consider also using Azure Monitor and Log Analytics for that purpose.

And perhaps you want to understand the security posture of your environment, make sure that you're compliant with policy, and check for security misconfigurations. If so, consider also using Azure Security Center. You can ingest Security Center alerts as a data connector for Azure Sentinel.

Create and manage Azure Sentinel workspaces

Lesson Introduction

Deploying the Azure Sentinel environment involves designing a workspace configuration to meet your security and compliance requirements. The provisioning process includes creating a Log Analytics workspace and configuring the Azure Sentinel options.

You're a Security Operations Analyst working at a company that is implementing Azure Sentinel. You're responsible for setting up the Azure Sentinel environment to meet the company requirement to minimize cost, meet compliance regulations, and provide the most manageable environment for your security team to perform their daily job responsibilities.

You start by understanding the Azure Sentinel workspace's architecture. After you have decided on your workspace implementation options, you create your first Azure Sentinel workspace.

Learn about the architecture of Azure Sentinel workspaces to ensure you configure your system to meet your organization's security operations requirements.

Learning objectives

After completing this lesson, you should be able to:

- Describe Azure Sentinel workspace architecture
- Install Azure Sentinel workspace
- Manage an Azure Sentinel workspace

Plan for the Azure Sentinel workspace

Before deploying Azure Sentinel, it is crucial to understand the workspace options. The Azure Sentinel solution is installed in a Log Analytics Workspace, and most implementation considerations are focused on the Log Analytics Workspace creation. The single most important option when creating a new Log Analytics Workspace is the region. The region specifies the location where the log data will reside.

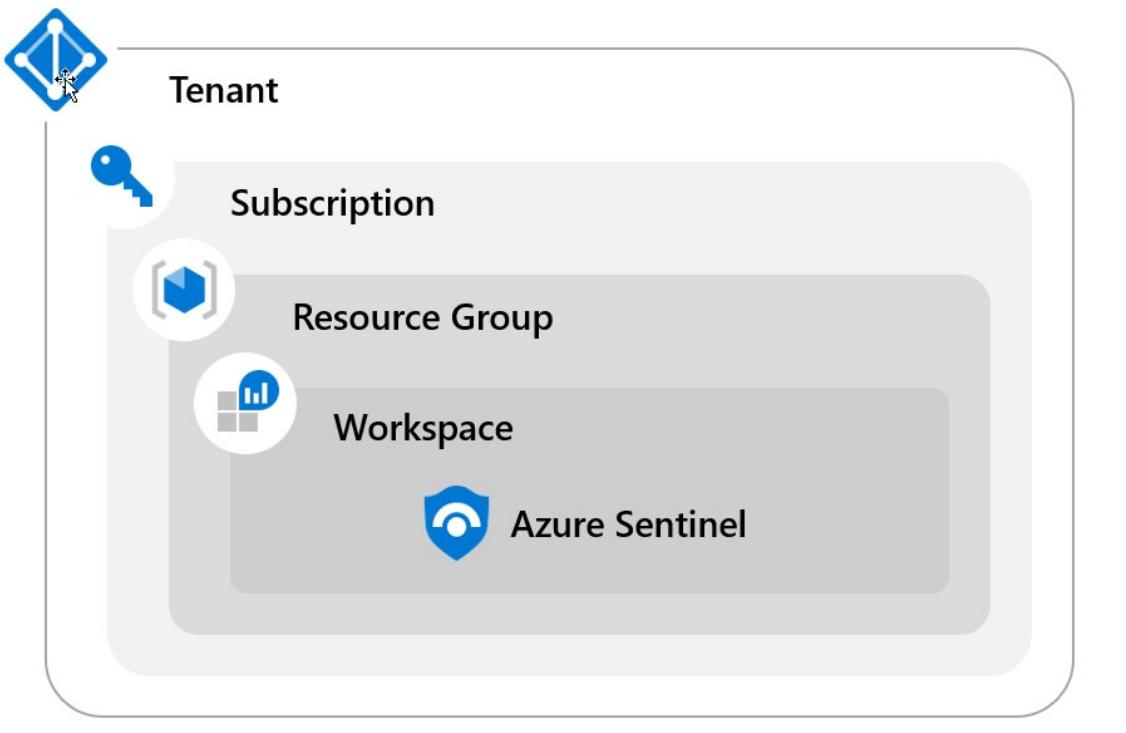
The three implementation options:

- Single-Tenant with a single Azure Sentinel Workspace
- Single-Tenant with regional Azure Sentinel Workspaces
- Multi-Tenant

Single-tenant single workspace

The single-tenant with a single Azure Sentinel workspace will be the central repository for logs across all resources within the same tenant.

This workspace receives logs from resources in other regions within the same tenant. Because the log data (when collected) will travel across regions and stored in another region, this creates two possible concerns. First, it can incur a bandwidth cost. Second, if there is a data governance requirement to keep data in a specific region, the single workspace option would not be an implementation option.

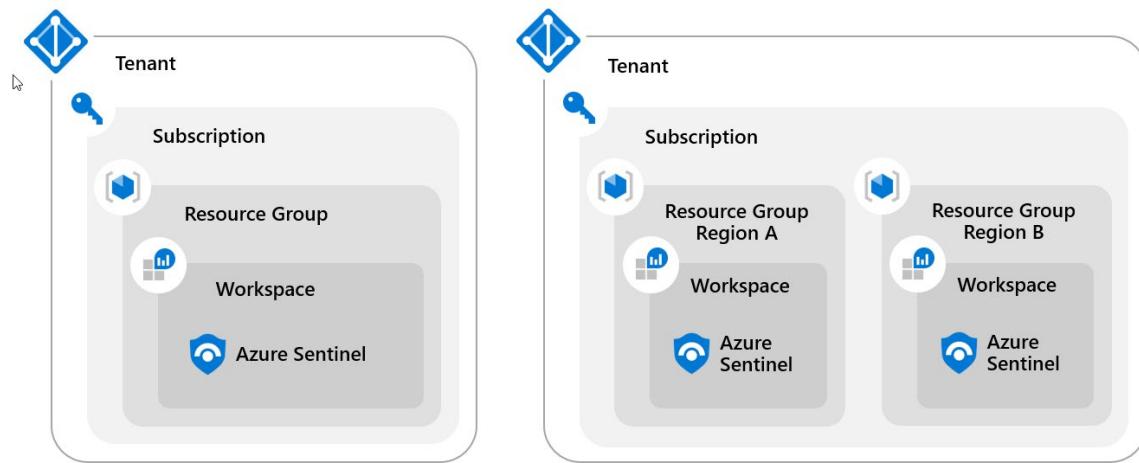


Single-Tenant with a single workspace pros and cons include:

Pros	Cons
Central Pane of Glass	May not meet Data Governance Requirements
Consolidates all security logs and information	Can incur bandwidth cost for cross region
Easier to query all information	
Azure Log Analytics RBAC to control data access	
Azure Sentinel RBAC for service RBAC	

Single-tenant with regional Azure Sentinel workspaces

The single-tenant with regional Azure Sentinel workspaces will have multiple Sentinel workspaces requiring the creation and configuration of multiple Azure Sentinel and Log Analytics workspaces.



Pros	Cons
No cross-region bandwidth costs	No central pane of glass. You are not looking in one place to see all the data.
May be required to meet Data Governance requirements	Analytics, Workbooks, etc. must be deployed multiple times.
Granular data access control	
Granular retention settings	
Split billing	

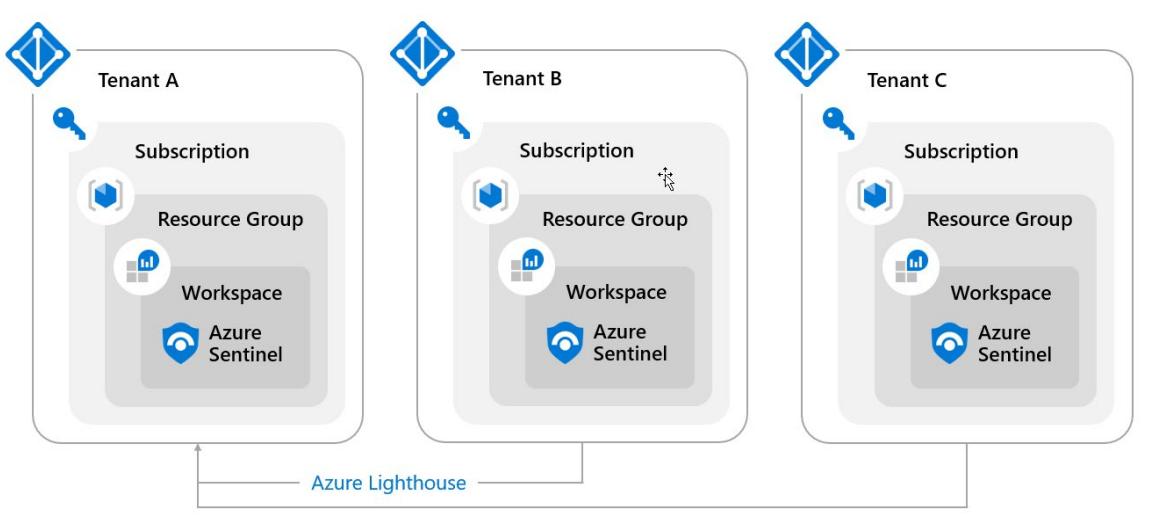
To query data across workspaces, use the workspace() function before the table name.

```
TableName
```

```
| union workspace("WorkspaceName") .TableName
```

Multi-tenant workspaces

If you are required to manage an Azure Sentinel workspace, not in your tenant, you implement Multi-Tenant workspaces using Azure Lighthouse. This security configuration grants you access to the tenants. The tenant configuration within the tenant (regional or multi-regional) is the same consideration as before.



Create an Azure Sentinel workspace

After designing the workspace architecture, log into the Azure portal. At the search bar, search for **Sentinel**, then select **Azure Sentinel**. The Azure Sentinel Workspaces shows a list of the current workspaces. Select the **+ add** button to start the creation process.

Azure Sentinel installation prerequisites

To enable Azure Sentinel, you need contributor permissions to the subscription in which the Azure Sentinel workspace resides. To use Azure Sentinel, you need either contributor or reader permissions on the resource group that the workspace belongs.

Create and configure a Log Analytics Workspace

1. The next page, **Add Azure Sentinel to a workspace** will display a list of available Log Analytics workspaces to add Azure Sentinel. Select the **+ create a new workspace** button to start the “Create Log Analytics workspace” process.
2. The Basics tab includes the following options:

Option	Description
Subscription	Select the Subscription
Resource Group	Select or create a Resource Group
Name	Name is the name of the Log Analytics workspace and will also be the name of your Azure Sentinel Workspace
Region	The region is the location the log data will be stored.

Important: The Name will be the name of the Azure Sentinel workspace. The Azure Sentinel name will default to the Log Analytics Workspace Name. The Region is the location where ingested data is stored. The data location impacts data governance requirements. Workspaces can't move from region to region; you will need to recreate the workspace if the region option needs to be changed.

3. Select the **Review + Create** button and then select the **Create** button.

Add Azure Sentinel to the workspace

The "Add Azure Sentinel to Workspace" screen will now appear after you've completed the previous steps.

1. Wait for the newly created "Log Analytics Workspace" to appear in the list. This could take a few minutes.
2. Select the newly created Log Analytics workspace. And select the **Add** button.

The new Azure Sentinel workspace will now be the active screen. The Azure Sentinel left navigation has three areas:

- General
- Threat Management
- Configuration

The Overview tab displays a standard dashboard of information about the ingested data, alerts, and incidents.

Azure Sentinel permissions and roles

Azure role-based access control (Azure RBAC) is the authorization system that manages access to Azure resources. It's built on Azure Resource Manager, which provides fine-grained access management of Azure resources.

Use Azure RBAC to create and assign roles in your SecOps team. Azure RBAC lets you grant appropriate access to Azure Sentinel. The different roles give you specific control over what users of Azure Sentinel can access and do.

Azure Sentinel-specific roles

The following are the three dedicated, built-in Azure Sentinel roles:

- **Reader:** This role can review data, incidents, workbooks, and other Azure Sentinel resources.
- **Responder:** This role has all the permissions of the Reader role. Plus, it can manage incidents by assigning or dismissing them.
- **Contributor:** This role has all the permissions of the Reader and Responder roles. Also, it can create and edit workbooks, analytics rules, and other Azure Sentinel resources. To deploy Azure Sentinel on your tenant, you need Contributor permissions for the subscription where the Azure Sentinel workspace is deployed.

All built-in Azure Sentinel roles grant read access to the data in your Azure Sentinel workspace. For best results, these roles should be assigned to the resource group that contains the Azure Sentinel workspace. The roles then apply to all the resources that deploy to support Azure Sentinel, if those resources are in the same resource group.

Azure roles and Azure Monitor Log Analytics roles

In addition to Azure Sentinel-dedicated Azure RBAC roles, other Azure and Log Analytics Azure RBAC roles can grant a wider set of permissions. These roles include access to your Azure Sentinel workspace and other resources.

- Azure roles grant access across all your Azure resources. They include Log Analytics workspaces and Azure Sentinel resources:
 - Owner
 - Contributor
 - Reader
- Log Analytics roles grant access across all your Log Analytics workspaces:
 - Log Analytics Contributor
 - Log Analytics Reader

For example, a user who is assigned with the Azure Sentinel Reader and Azure Contributor (not Azure Sentinel Contributor) roles can edit data in Azure Sentinel. If you want to only grant permissions to Azure Sentinel, you should carefully remove the user's prior permissions. Make sure you don't break any needed permission role for another resource.

Azure Sentinel roles and allowed actions

The following table summarizes the roles and allowed actions in Azure Sentinel.

Roles	Create and run playbooks	Create and edit workbooks, analytic rules, and other Azure Sentinel resources	Manage incidents such as dismissing and assigning	View data incidents, workbooks, and other Azure Sentinel resources
Azure Sentinel Reader	No	No	No	Yes
Azure Sentinel Responder	No	No	Yes	Yes
Azure Sentinel Contributor	No	Yes	Yes	Yes
Azure Sentinel Contributor and Logic App Contributor	Yes	Yes	Yes	Yes

Custom roles and advanced Azure RBAC

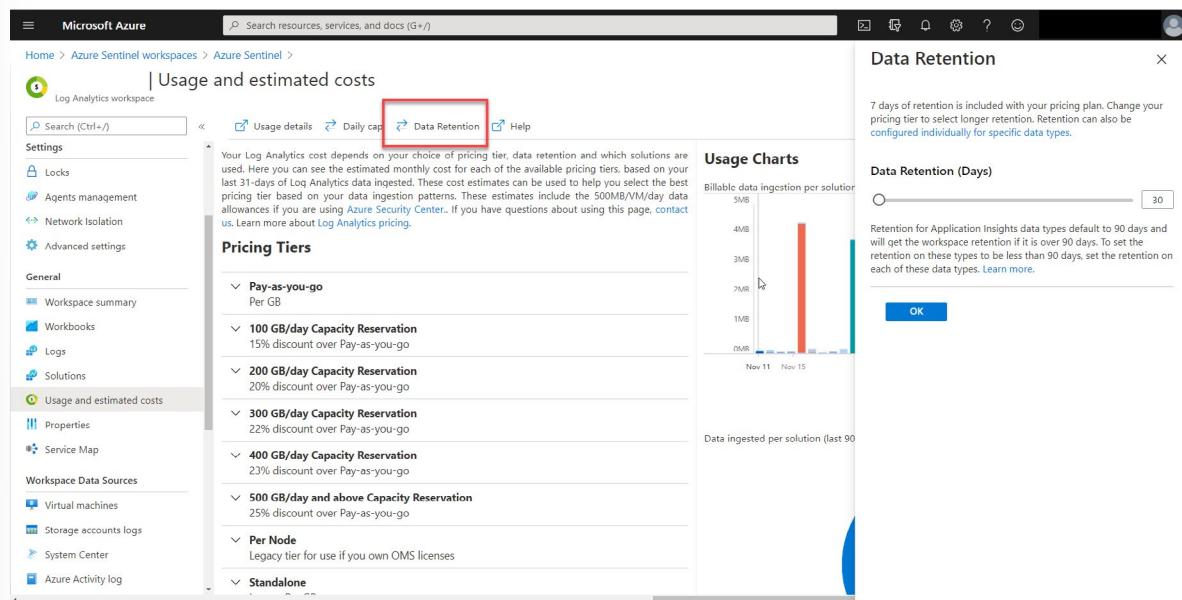
If the built-in Azure roles don't meet the specific needs of your organization, you can create your own custom roles. Just like built-in roles, you can assign custom roles to users, groups, and service principals for management-group, subscription, and resource-group scopes.

Manage Azure Sentinel settings

Azure Sentinel Environment Settings are managed in two areas. In Azure Sentinel and in the Log Analytics workspace where Azure Sentinel resides. In Azure Sentinel, the left navigation has an option for Settings. The Settings includes tabs for Pricing, Settings, and Workspace Settings—the Settings changes over time based on the current and in-preview feature set. Most Azure Sentinel Environment settings are managed in the Log Analytics workspace. Other areas within the Azure Sentinel portal will transfer you to the Log Analytics portal. One example of this is specific data connector configurations will be performed in the log analytics workspace.

Configure log retention

By default, log retention is set for 30 days. To adjust the retention days, select the workplace settings in the Azure Sentinel Settings area. The next screen is in the Log Analytics portal. Select the "Usage and estimated costs" tab. At the top of the page, select the "Retention" button. A blade will open, allowing for the adjustment of the retention days.



Manage workspaces across tenants using Azure Lighthouse

If you are required to manage an Azure Sentinel workspace not in your tenant, implementing Azure Lighthouse will provide the option to enable your access to the tenant. Once Azure Lighthouse is onboarded, use the directory + subscription selector on the Azure portal to select all the subscriptions containing workspaces you manage.

Query logs in Azure Sentinel

Lesson Introduction

Azure Sentinel collects log data that is stored in tables. The Logs page in Azure Sentinel provides a user interface to build and view query results using the Kusto Query Language (KQL). KQL is the query language used to perform data analysis to create analytics, workbooks, and perform hunting in Azure Sentinel.

You are a Security Operations Analyst working at a company that is implementing Azure Sentinel. You must explore the tables available in your workspace. The Logs page in Azure Sentinel allows you to write Kusto Query Language (KQL) statements to view data stored in the tables. When you connect log data to the Azure Sentinel workspace, the connectors will write data to specific tables.

You need to have a basic understanding of the provided tables and their intended purpose. For example, the “SecurityEvents” table is designed for Windows Security Event log data. With this knowledge, you will be able to query the required tables to use in your search for malicious activity.

As a Security Operations Analyst, you must understand the tables, fields, and data ingested in your workspace. Learn how to query the most used data tables in Azure Sentinel.

Learning objectives

After completing this lesson, you should be able to:

- Use the Logs page to view data tables in Azure Sentinel
- Query the most used tables using Azure Sentinel

Query logs in the logs page

KQL is the language used to query the log data in the Log Analytics workspace. In Azure Sentinel, the Logs page provides access to the query window. The query window allows you to run queries, save queries, run saved queries, create a new alert rule, and export. The left side provides a list of tables and related table fields. To run a query, enter the query text and press the run button. Query results appear in the bottom section of the form.

Understand Azure Sentinel tables

Azure Sentinel has Analytic Rules that will generate Alerts and Incidents based on querying the tables within Log Analytics. The primary tables to manage alerts and incidents are SecurityAlert and SecurityIncident. Azure Sentinel provides tables to be a repository of indicators and watchlists.

Note: Some of the Sentinel Data Connectors will ingest alerts directly.

The table below is the Azure Sentinel feature related tables.

Table	Description
SecurityAlert	Contains Alerts Generated from Sentinel Analytical Rules. Also, it could include Alerts created directly from a Sentinel Data Connector
SecurityIncident	Alerts can generate Incidents. Incidents are related to Alert(s).

Table	Description
ThreatIntelligenceIndicator	Contains user-created or data connector ingested Indicators such as File Hashes, IP Addresses, Domains
Watchlist	An Azure Sentinel watchlist contains imported data.

Understand common tables

When Sentinel ingests data from the Data Connectors, the following table lists the most commonly used tables.

Table	Description
AzureActivity	Entries from the Azure Activity log that provides insight into any subscription-level or management group level events that have occurred in Azure.
AzureDiagnostics	Stores resource logs for Azure services that use Azure Diagnostics mode. Resource logs describe the internal operation of Azure resources.
AuditLogs	Audit log for Azure Active Directory. Includes system activity information about user and group management managed applications and directory activities.
CommonSecurityLog	Syslog messages using the Common Event Format (CEF).
McasShadowItReporting	Microsoft Cloud App Security logs
OfficeActivity	Audit logs for Office 365 tenants collected by Azure Sentinel. Including Exchange, SharePoint and Teams logs.
SecurityEvent	Security events collected from windows machines by Azure Security Center or Azure Sentinel
SigninLogs	Azure Activity Directory Sign in logs
Syslog	Syslog events on Linux computers using the Log Analytics agent.
Event	Sysmon Events collected from a Windows host.
WindowsFirewall	Windows Firewall Events

Understand Microsoft 365 Defender tables

The Microsoft 365 Defender Sentinel Data Connector can populate tables with raw data collected from the Microsoft 365 Defender solutions.

Microsoft Defender for Endpoint tables.

Table	Description
DeviceEvents	The miscellaneous device events table contains information about various event types, including events triggered by security controls, such as Microsoft Defender Antivirus and exploit protection.
DeviceFileEvents	This table contains information about file creation, modification, and other file system events.
DeviceImageLoadEvents	This table contains information about DLL loading events.
DeviceInfo	This table contains information about devices in the organization, including their OS version, active users, and computer name.
DeviceLogonEvents	This table contains information about user logons and other authentication events.
DeviceNetworkEvents	This table contains information about network connections and related events.
DeviceNetworkInfo	This table contains information about networking configuration of devices, including network adapters, IP and MAC addresses, and connected networks or domains.
DeviceProcessEvents	This table contains information about process creation and related events.
DeviceRegistryEvents	This table contains information about the creation and modification of registry entries.

Use watchlists in Azure Sentinel

Lesson Introduction

Azure Sentinel provides a table to store list data accessible to Kusto Query Language (KQL) queries. The Watchlists page in Azure Sentinel provides the management options to maintain the lists.

You are a Security Operations Analyst working at a company that has implemented Azure Sentinel. The Security Operations team members need to prioritize alerts that are impacting high-value target servers.

You must import a list of server names into Azure Sentinel, which can then be used by detection queries to set a priority field. You import a list of servers into the Watchlist page of Azure Sentinel. Once created, you instruct the Security Operations team to use the watch list in their KQL queries.

Learn how to create Azure Sentinel watchlists that are a named list of imported data. Once created, you can easily use the named watchlist in KQL queries.

Learning objectives

After completing this lesson, you should be able to:

- Create a watchlist in Azure Sentinel
- Use KQL to access the watchlist in Azure Sentinel

Plan for Azure Sentinel watchlists

Azure Sentinel watchlists enable collecting data from external data sources for correlation with the events in your Azure Sentinel environment. Once created, you can use watchlists in your search, detection rules, threat hunting, and response playbooks. Watchlists are stored in your Azure Sentinel workspace as name-value pairs and are cached for optimal query performance and low latency.

Common scenarios for using watchlists include:

- Investigating threats and responding to incidents quickly with the rapid import of IP addresses, file hashes, and other data from CSV files. Once imported, you can use watchlist name-value pairs for joins and filters in alert rules, threat hunting, workbooks, notebooks, and general queries.
- Importing business data as a watchlist. For example, import user lists with privileged system access, or terminated employees, and then use the watchlist to create allow and deny lists used to detect or prevent those users from logging in to the network.
- Reducing alert fatigue. Create allow lists to suppress alerts from a group of users, such as users from authorized IP addresses that perform tasks that would normally trigger the alert, and prevent benign events from becoming alerts.
- Enriching event data. Use watchlists to enrich your event data with name-value combinations derived from external data sources.

Tip: You can create and delete Watchlists, but you can't update Watchlists. If you are working with more dynamic lists, use KQL external data operators to create temporary virtual tables.

Create a watchlist

To create a watchlist from the Azure portal do the following:

1. Go to **Azure Sentinel > Configuration > Watchlist** and select **Add new**.

The screenshot shows the Azure Sentinel Watchlist (Preview) interface. The left sidebar has sections for General (Overview, Logs, News & guides), Threat management (Incidents, Workbooks, Hunting, Notebooks (Preview), Entity behavior analytics (Preview), Threat intelligence (Preview)), Configuration (Data connectors, Analytics, Watchlist (Preview) - highlighted with a red box), Playbooks, Community, and Settings. The main area shows a 'Watchlists' section with a count of 0. A message says 'There was an error retrieving the data.'

2. On the General page, provide the name, description, and alias for the watchlist, then select **Next**.
3. On the Source page, select the dataset type, upload a file, then select **Next**.
Note: File uploads are currently limited to files of up to 3.8 MB in size.
4. Next, review the information, verify that it is correct, then select **Create**. A notification appears once the watchlist is ready.

To use the watchlist data in KQL, use the KQL function `_GetWatchlist('watchlist name')`.

```
_GetWatchlist('HighValueMachines')
```

Utilize threat intelligence in Azure Sentinel

Lesson Introduction

Azure Sentinel provides a table to store indicator data accessible to Kusto Query Language (KQL) queries. The Threat intelligence page in Azure Sentinel provides the management options to maintain the indicators.

You are a Security Operations Analyst working at a company that implemented Azure Sentinel. You receive threat indicators from threat intelligence providers and your threat hunting team. The Indicators include IP addresses, domains, and file hashes that can be utilized by many components within Azure Sentinel.

The indicators from the threat intelligence providers are automatically imported into the workspace using connectors. You are tasked with adding the indicators from the threat hunting team. You use the Threat Intelligence page to add the indicators for use by the detection KQL queries.

Learn how the Azure Sentinel Threat Intelligence page enables you to manage threat indicators.

Learning objectives

After completing this lesson, you should be able to:

- Manage threat indicators in Azure Sentinel
- Use KQL to access threat indicators in Azure Sentinel

Define threat intelligence

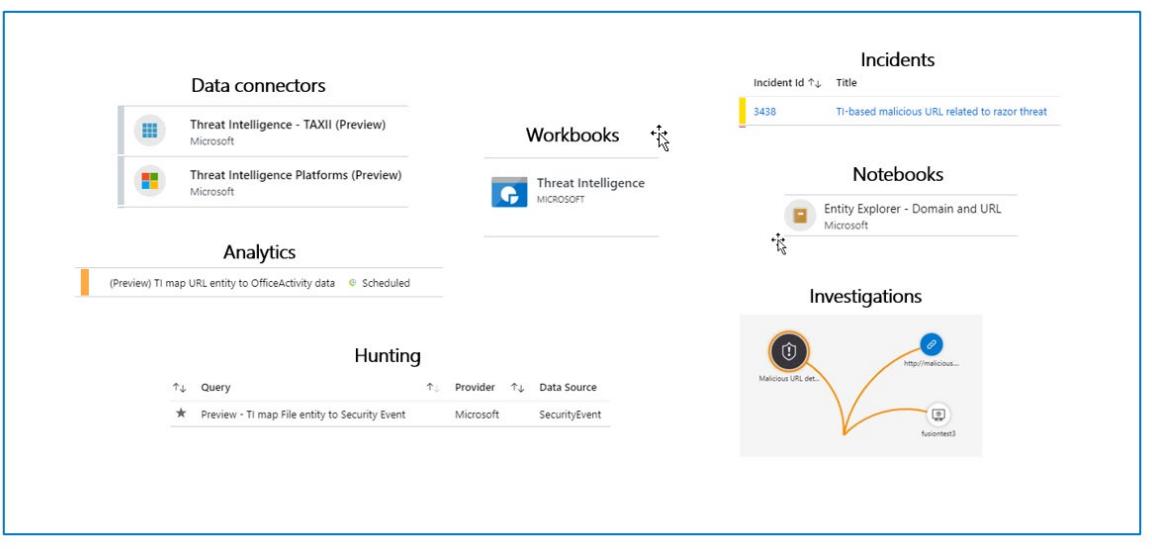
Cyber threat intelligence (CTI) is information describing known existing or potential threats to systems and users. This type of knowledge takes many forms, from written reports detailing a particular threat actor's motivations, infrastructure, and techniques, to specific observations of IP addresses, domains, and file hashes associated with cyber threats. Organizations use CTI to provide essential context to unusual activity so that security personnel can quickly take action to protect their people and assets. CTI can be sourced from many places, such as open-source data feeds, threat intelligence-sharing communities, commercial intelligence feeds, and local intelligence gathered in security investigations within an organization.

Within a Security Information and Event Management (SIEM) solution like Azure Sentinel, the most utilized form of CTI is threat indicators, often referred to as Indicators of Compromise or IoCs. Threat indicators are data that associate observations such as URLs, file hashes, or IP addresses with known threat activity such as phishing, botnets, or malware. This form of threat intelligence is often referred to as tactical threat intelligence because it can be applied to security products and automation on a large scale to protect and detect potential threats to an organization. In Azure Sentinel, you can use threat indicators to help detect malicious activity observed in your environment and provide context to security investigators to help inform response decisions.

You can integrate threat intelligence (TI) into Azure Sentinel through the following activities:

- Use Data connectors to various TI platforms to import threat intelligence into Azure Sentinel.
- View and manage the imported threat intelligence in Logs and the new Threat Intelligence area of Azure Sentinel.
- Use the built-in Analytics rule templates to generate security alerts and incidents using your imported threat intelligence.

- Visualize critical information about your threat intelligence in Azure Sentinel with the Threat Intelligence workbook.
- Perform threat hunting with your imported threat intelligence.



Manage your threat indicators

With the Threat Intelligence area, accessible from the Azure Sentinel menu, you can also view, sort, filter, and search your imported threat indicators without even writing a Logs query. This area also allows you to create threat indicators directly within the Azure Sentinel interface and perform everyday threat intelligence administrative tasks like indicator tagging and creating new indicators related to security investigations. Let's look at two of the most common tasks, creating new threat indicators and tagging indicators for easy grouping and reference.

1. Open the **Azure portal**¹ and navigate to the Azure Sentinel service.
2. Choose the workspace to which you've imported threat indicators using either threat intelligence data connector.
3. Select **Threat intelligence** from the **Threat management** section of the Azure Sentinel menu.
4. Select the **Add new** button from the top menu of the page.
5. Choose the indicator type, then complete the required fields marked with a red asterisk (*) on the New indicator panel. Select **Apply**.

Tagging threat indicators is an easy way to group them to make them easier to find. Typically, you might apply a tag to indicators related to a particular incident or indicators representing threats from a known actor or a well-known attack campaign. You can tag threat indicators individually or multi-select indicators and tag them all at once. Since tagging is free-form, a recommended practice is to create standard naming conventions for threat indicator tags. You can apply multiple tags to each indicator.

¹ <https://portal.azure.com/?azure-portal=true>

View your threat indicators with KQL

The indicators reside in the *ThreatIntelligenceIndicator* table. This table is the basis for queries performed by other Azure Sentinel features such as Analytics and Workbooks. Here's how to find and view your threat indicators in the *ThreatIntelligenceIndicator* table.

To view your threat indicators with KQL. Select **Logs** from the General section of the Azure Sentinel menu. Then run a query on the *ThreatIntelligenceIndicator* table.

`ThreatIntelligenceIndicator`

Knowledge check

Check your Knowledge

Multiple choice

Item 1. Where is your log data stored?

- Azure Sentinel Workspace
- Azure Lighthouse
- Log Analytics workspace

Multiple choice

Item 2. Which Azure Sentinel security role can create workbooks?

- Azure Sentinel Responder
- Azure Sentinel Reader
- Azure Sentinel Contributor

Multiple choice

Item 3. Why is it important to set the region when creating the Log Analytics workspace?

- Specifies where the log data will be stored.
- Specifies the timezone the data will be displayed in.
- Specifies the log retention period

Multiple choice

Item 4. Which table stores Defender for Endpoint logon events?

- DeviceLogonEvents
- OfficeActivity
- SigninLogs

Multiple choice

Item 5. What table contains logs from Windows hosts collected directly to Azure Sentinel?

- SecurityEvent
- AuditLogs
- SecurityAlert

Multiple choice

Item 6. Which table stores Alerts from Microsoft Defender for Endpoint?

- SecurityIncident
- DeviceEvents
- SecurityAlert

Multiple choice

Item 7. Which of the following is a typical scenario for using an Azure Sentinel watchlist?

- Creating more alerts to help identify issues.
- Export business data as a watchlist.
- Responding to incidents quickly with the rapid import of IP addresses.

Multiple choice

Item 8. How do you access a new watchlist named MyList in KQL?

- _Watchlist('MyList')
- _GetWatchlist('MyList')
- _Getlist('MyList')

Multiple choice

Item 9. In Threat Intelligence, indicators are considered as which of the following?

- Strategic
- Operational
- Tactical

Multiple choice

Item 10. Which of these items is an example of a Threat indicator?

- Threat Actor Name
- Domain Name
- Threat Campaign

Multiple choice

Item 11. What table do you query in KQL to view your indicators?

- Indicator
- TI Indicator
- ThreatIntelligenceIndicator

Lab - Configure your Azure Sentinel environment

Lab: Configure your Azure Sentinel environment

To download the most recent version of this lab, please visit the SC-200 [GitHub repository²](#).

Note: Depending on the lab hosting solution used for your class delivery, the lab instructions may display directly in the virtual lab environment, in addition to being available in the GitHub repository. In that case, follow guidance from your instructor as to where you will access the lab steps from. Even if the GitHub version is not used for your class, you may still find it useful to be able to reference the lab instructions on GitHub after class is over.

Lab scenario

You're a Security Operations Analyst working at a company that is implementing Azure Sentinel. You're responsible for setting up the Azure Sentinel environment to meet the company requirement to minimize cost, meet compliance regulations, and provide the most manageable environment for your security team to perform their daily job responsibilities.

Objectives

After you complete this lab, you will be able to:

- Initialize the Azure Sentinel Workspace.
- Create a Watchlist.
- Create a Threat Indicator.

Lab setup

- Estimated time: 20 minutes

² <https://github.com/MicrosoftLearning/SC-200T00A-Microsoft-Security-Operations-Analyst>

Answers

Multiple choice

Item 1. Where is your log data stored?

- Azure Sentinel Workspace
- Azure Lighthouse
- Log Analytics workspace

Explanation

Log Analytics workspace is where the data resides

Multiple choice

Item 2. Which Azure Sentinel security role can create workbooks?

- Azure Sentinel Responder
- Azure Sentinel Reader
- Azure Sentinel Contributor

Explanation

The Contributor role can create workbooks.

Multiple choice

Item 3. Why is it important to set the region when creating the Log Analytics workspace?

- Specifies where the log data will be stored.
- Specifies the timezone the data will be displayed in.
- Specifies the log retention period

Explanation

Region is the data center where your log data is stored

Multiple choice

Item 4. Which table stores Defender for Endpoint logon events?

- DeviceLogonEvents
- OfficeActivity
- SigninLogs

Explanation

The Defender for Endpoint data is stored in tables starting with Device

Multiple choice

Item 5. What table contains logs from Windows hosts collected directly to Azure Sentinel?

- SecurityEvent
- AuditLogs
- SecurityAlert

Explanation

Logs from Windows events are stored in this table.

Multiple choice

Item 6. Which table stores Alerts from Microsoft Defender for Endpoint?

- SecurityIncident
- DeviceEvents
- SecurityAlert

Explanation

The Alerts will reside in the SecurityAlert table.

Multiple choice

Item 7. Which of the following is a typical scenario for using an Azure Sentinel watchlist?

- Creating more alerts to help identify issues.
- Export business data as a watchlist.
- Responding to incidents quickly with the rapid import of IP addresses.

Explanation

This is a typical scenario for using Azure Sentinel watchlist.

Multiple choice

Item 8. How do you access a new watchlist named MyList in KQL?

- _Watchlist('MyList')
- _GetWatchlist('MyList')
- _Getlist('MyList')

Explanation

This is the proper function.

Multiple choice

Item 9. In Threat Intelligence, indicators are considered as which of the following?

- Strategic
- Operational
- Tactical

Explanation

Indicators are considered Tactical Threat Intelligence.

Multiple choice

Item 10. Which of these items is an example of a Threat indicator?

- Threat Actor Name
- Domain Name
- Threat Campaign

Explanation

This indicator can be used to query against your log data.

Multiple choice

Item 11. What table do you query in KQL to view your indicators?

- Indicator
- TI Indicator
- ThreatIntelligenceIndicator

Explanation

The proper table is ThreatIntelligenceIndicator

Module 6 Connect logs to Azure Sentinel

Connect data to Azure Sentinel using data connectors

Lesson Introduction

Data is sent to the Azure Sentinel workspace by configuring the provided data connectors. The included data connectors are for Microsoft 365 services, Azure, and third-party specific.

You're a Security Operations Analyst working at a company that implemented Azure Sentinel. You must learn how to connect log data from the many different data sources in your organization. The organization has data from Microsoft 365, Microsoft 365 Defender, Azure resources, non-azure virtual machines, and network appliances.

You plan on using the Azure Sentinel data connectors to integrate the log data from the various sources. You need to write a connector plan for management that maps each of the organization's data sources to the proper Azure Sentinel data connector.

The primary approach to connect log data is using the Azure Sentinel provided data connectors. This module provides an overview of the available data connectors.

Learning objectives

After completing this lesson, you should be able to:

- Explain the use of data connectors in Azure Sentinel
- Describe the Azure Sentinel data connector providers
- Explain the Common Event Format and Syslog connector differences in Azure Sentinel

Ingest log data with data connectors

To collect log data, you need to connect your data sources with Azure Sentinel Connectors. The Data Connectors page displays a growing list of connectors provided by Azure Sentinel.

The screenshot shows the Microsoft Azure Azure Sentinel Data connectors page. The left blade lists various connectors, while the right blade provides detailed information about a specific connector.

After selecting the Open connector page, the detailed connector page has a left blade and a right blade.

The screenshot shows the Microsoft Azure Azure Active Directory Identity Protection connector page. The left blade displays basic connector status and data reception information. The right blade provides instructions and configuration options for connecting the connector to Azure Sentinel.

The left blade provides information about the connector, the connector's status, and the last time a log was received if connected. On the bottom section of the left blade is the Data Types. The Data Types will list the table(s) that the connector will write to.

The right blade has two tabs: Instructions and Next steps. The Instructions tab can be different based on the connector. In general, there will be Prerequisites and Configuration. Follow the Configuration to connect to the data source. The Next steps tab provides a quick reference to workbooks, query samples, and analytical templates. Data Connectors can only be disconnected/deactivated, not deleted.

Note: The connector does not install Workbooks and Analytics Templates. Workbooks and Analytic Templates for out of the box connectors are already available in the Sentinel environment.

Understand data connector providers

Microsoft 365 Defender

The Microsoft 365 Defender and related data connectors provide alerts and data that has already been normalized and used in the Microsoft 365 Defender portal.

The Microsoft 365 Defender products include:

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Cloud App Security

Microsoft/Azure Services

The connectors for Microsoft and Azure-related services include (but are not limited to):

- Azure Active Directory - audit logs and sign-in logs
- Azure Activity
- Azure AD Identity Protection
- Azure DDoS Protection
- Azure Defender for IoT (formerly Azure Security Center for IoT)
- Azure Information Protection
- Azure Firewall
- Azure Security Center - alerts from Azure Defender solutions
- Azure Web Application Firewall (WAF) (formerly Microsoft WAF)
- Cloud App Security
- Domain name server
- Office 365
- Windows firewall
- Security Events

Vendor connectors

Azure Sentinel provides an ever-growing list of vendor-specific data connectors. These connectors primarily use the CEF and Syslog connector.

Tip: Remember to check the connector page to see the Data Type (table) that the connector writes to

Custom connectors using the Log Analytics API

You can use the Log Analytics Data Collector API to send log data to the Azure Sentinel Log Analytics workspace.

Logstash plugin

Using Azure Sentinel's output plugin for the Logstash data collection engine, you can send any log you want through Logstash directly to your Log Analytics workspace in Azure Sentinel. The logs are written to a custom table that you define using the output plugin.

CEF and Syslog connector

If there is no vendor-provided connector, you can use the generic Common Event Format(CEF) or Syslog Connector.

Syslog is an event logging protocol that is common to Linux. Applications will send messages that may be stored on the local machine or delivered to a Syslog collector.

Common Event Format (CEF) is an industry-standard format on top of Syslog messages, used by many security vendors to allow event interoperability among different platforms.

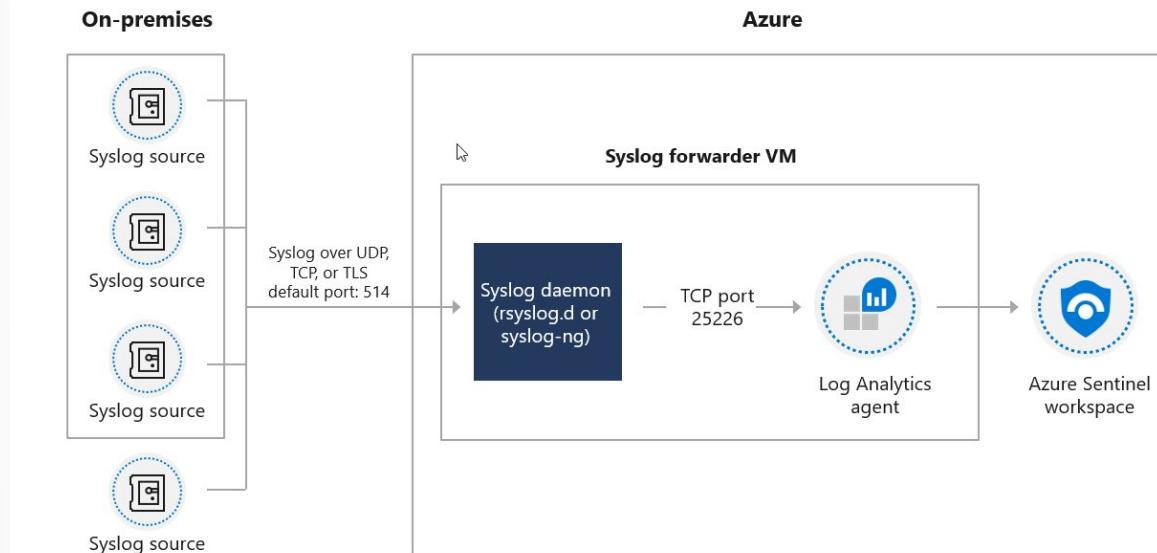
Syslog vs. Common Event Format

CEF is always a superior choice because the log data is parsed into predefined fields in the CommonSecurityLog table. Syslog provides header fields, but the raw log message is stored in a field named Syslog-Message in the Syslog table. For the Syslog data to be queried, you will need to write a parser to extract the specific fields. The process to create a Parser for a Syslog message will be demonstrated in a later module.

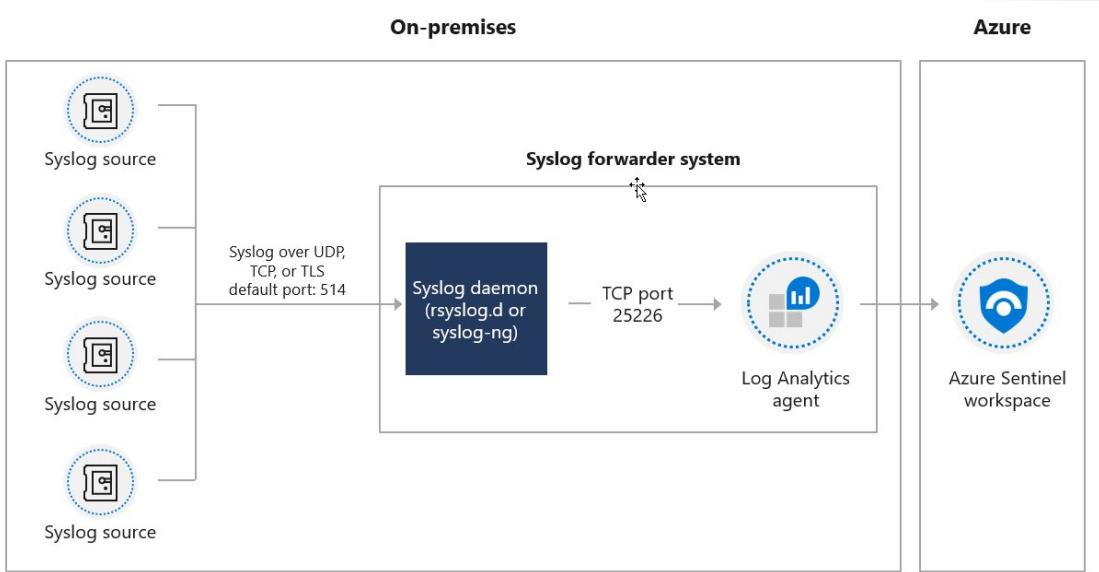
Connector architecture options

To connect the CEF or Syslog Collector to Azure Sentinel, the agent must deploy on a dedicated Azure virtual machine (VM) or an on-premises system to support the appliance's communication with Azure Sentinel. You can deploy the agent automatically or manually. Automatic deployment is only available if your dedicated machine is a Virtual Machine in Azure.

The following diagram illustrates on-premises systems sending Syslog data to a dedicated Azure VM running the Azure Sentinel agent.



Alternatively, you can manually deploy the agent on an existing Azure VM, on a VM in another cloud, or an on-premises machine. The following diagram illustrates on-premises systems sending Syslog data to a dedicated on-premises system running the Azure Sentinel agent.



View connected hosts

The Data Connector page shows the connectors that are connected. The amount of Windows and Linux hosts connected with the Log Analytics agent is available in the Log Analytics workspace. To see your connected hosts do the following steps:

1. Select **Settings**
2. Workspace Settings (this will transfer you to Log Analytics)
3. In Log Analytics Settings area select **Agents Management**
4. There are two tabs to view - one for Windows another for Linux.

Connect Microsoft services to Azure Sentinel

Lesson Introduction

You connect Microsoft 365 and Azure services to the Azure Sentinel workspace using the provided data connectors.

You are a Security Operations Analyst working at a company that implemented Azure Sentinel. You need to connect Microsoft 365 and Azure services to Azure Sentinel.

Based on your previously documented connector plan, you use the data connector page to enable the specific connectors. As you activate the connectors, you notice the option to have incidents created from the Azure Active Directory Identity Protection service. You don't follow the recommended option to create incidents as you plan to activate the incident creation rule with custom options later in your implementation process.

Learn how to connect Microsoft 365 and Azure service logs to Azure Sentinel.

Learning objectives

After completing this lesson, you should be able to:

- Connect Microsoft service connectors
- Explain how connectors auto-create incidents in Azure Sentinel

Plan for Microsoft services connectors

You can connect Microsoft and Azure-related services in the Data Connector page configuration section in just a few clicks. It is easy to overlook specific considerations for each connector. This module will demonstrate the connecting of three services. Each service sends data to different Data Types (tables).

First is the Office 365 connector. The Configuration option allows for the sending of Exchange, SharePoint, and Teams data. Based on your organization's specific needs, you can decide which data to ingest. The Data types show that all the data will reside in the OfficeActivity table.

The second is Azure Active Directory, which has two options for Sign-on logs and Audit logs.

Third is Azure Active Directory Identity Protection. This connector will send data to the SecurityAlert table. The SecurityAlert table will hold the alert data only without the underlying data that caused the alert. A second option is to Create Incidents - Recommended! Which will automatically create an Incident based on and connected to the alert ingested to the SecurityAlert table from Azure Active Directory Identity Protection. You can also activate the incident creation rule on the Analytics page.

Connect the Microsoft Office 365 connector

The Office 365 activity log connector provides insight into ongoing user activities. You will get details of operations such as file downloads, access requests sent, changes to group events, set-mailbox, and details of the user who performed the actions.

To view the connector page do these steps:

1. Select Data connectors page.
2. Select **Office 365**.
3. Then select the Open connector page on the preview pane.

4. Under the section labeled Configuration, mark the Office 365 activity logs' checkboxes to connect to Azure Sentinel.
5. Select **Apply Changes**.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with 'Microsoft Azure' and a search bar. Below it, the URL 'Home > Azure Sentinel workspaces > Azure Sentinel > Office 365' is visible. The main content area has a title 'Office 365'. On the left, there's a summary card with 'Connected Status' (4 Workbooks, 3 Queries, 22 Analytic rules templates), a chart titled 'Data received' (with a Y-axis from 0K to 1.2K and an X-axis from December 6 to December 7), and three summary numbers: 'Total data received' (3.68k), 'Total data received' (989), and 'Total data received' (0). Below this is a 'Data types' section with entries for 'OfficeActivity (SharePoint)' and 'OfficeActivity (Exchange)'. On the right, there are two sections: 'Prerequisites' (with a note about workspace permissions and tenant permissions) and 'Configuration' (with checkboxes for 'Exchange', 'SharePoint', and 'Teams (Preview)'). An 'Apply Changes' button is located at the bottom of the configuration section.

Connect the Azure Active Directory connector

Gain insights into Azure Active Directory by connecting Audit and Sign in logs to Azure Sentinel to gather insights around Azure Active Directory scenarios. You can learn about app usage, conditional access policies, and legacy auth relate details using our Sign-in logs. You can get information on your Self-Service Password Reset (SSPR) usage, Azure Active Directory Management activities like user, group, role, and app management in the Audit logs table.

To view the connector page do the following steps:

1. Select Data connectors page.
2. Select **Azure Active Directory**
3. Then select the Open connector page on the preview pane.
4. Mark the checkboxes next to the logs you want to stream into Azure Sentinel, and select **Connect**.

The screenshot shows the Azure Active Directory connector configuration page. On the left, there's a preview pane showing a line chart of data received over time, with a total of 767 data points. Below the chart, it says "Total data received" and lists "SigninLogs" and "AuditLogs" with their respective last log received times. The main pane has tabs for "Instructions" and "Next steps". Under "Prerequisites", it lists requirements for Workspace, Diagnostic Settings, Tenant Permissions, and License. Under "Configuration", it shows options to connect Azure Active Directory logs to Azure Sentinel, with checkboxes for "Azure Active Directory Sign-In logs" and "Azure Active Directory Audit logs", and a "Apply Changes" button.

Connect the Azure Active Directory Identity Protection connector

Azure Active Directory Identity Protection provides a consolidated view of at-risk users, risk events, and vulnerabilities, with the ability to remediate risk immediately and set policies to autoremediate future events.

To view the connector page do the following steps:

1. Select Data connectors page.
2. Select **Azure Active Directory Identity Protection**.
3. Then select the Open connector page on the preview pane.
4. Select **Connect** to start streaming the Azure AD Identity Protection alerts.
5. Select whether alerts from Azure AD Identity Protection automatically generate incidents by selecting **Enable**.

Azure Active Directory Identity Protection

Connected Status Microsoft Provider Last Log Received

Last data received

Related content

- Workbooks 0
- Queries 2
- Analytic rules templates 2

Data received

Go to log analytics

Total data received 0

December 6

Prerequisites

To integrate with Azure Active Directory Identity Protection make sure you have:

- ✓ **Workspace:** read and write permissions are required.
- ✓ **Tenant Permissions:** required 'Global Administrator' or 'Security Administrator' on the workspace's tenant.
- ✓ **License:** required AAD P1/P2.

Configuration

Azure Active Directory Identity Protection alerts to Azure Sentinel
Connect Azure Active Directory Identity Protection to Azure Sentinel.

The alerts are sent to this Azure Sentinel workspace.

Azure Active Directory Identity Protection Disconnect

If you enable creating incidents, the default analytics rule "Create incidents based on Azure Active Directory Identity Protection alerts" is enabled with default values. You can edit this analytical rule on the Analytics page.

Connect Microsoft 365 Defender to Azure Sentinel

Lesson Introduction

You connect Microsoft 365 Defender security solutions to the Azure Sentinel workspace using the provided data connectors.

You are a Security Operations Analyst working at a company that implemented Azure Sentinel. As you continue your process to activate data connectors in Azure Sentinel, you now need to focus on the Microsoft 365 Defender solutions, including Microsoft Defender for Endpoint and Microsoft Defender for Office 365.

You realize more consideration is required because the alerts and incidents could already be investigated in the Microsoft 365 security portal. You take time to understand how you would use the Defender data in Azure Sentinel. You write a document on how alerts, incidents, and raw data will be used for event correlation in detection rules. After documenting your decisions, you activate each Microsoft 365 Defender-related data connector.

Learn about the configuration options and data provided by Azure Sentinel connectors for Microsoft 365 Defender.

Learning objectives

After completing this lesson, you should be able to:

- Activate the Microsoft 365 Defender connector in Azure Sentinel
- Activate the Microsoft Defender for Endpoint connector in Azure Sentinel
- Activate the Microsoft Defender for Office 365 connector in Azure Sentinel

Plan for Microsoft 365 Defender connectors

The Microsoft 365 security portal provides a purpose-driven user interface to mitigate threats detected by Microsoft 365 Defender. The Microsoft 365 Defender family of products include:

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Cloud App Security

The products each have a connector that will send alerts to the SecurityAlerts table in Sentinel. Which then can generate an Incident. Another connector - Microsoft 365 Defender - allows for the raw normalized data to be ingested by Azure Sentinel. Currently, only Microsoft Defender for Endpoint data is configurable in the Microsoft 365 Defender connector. You must decide if you want Microsoft 365 Defender products alerts in Azure Sentinel.

- Should those alerts generate incidents when the incidents are already being investigated in the Microsoft 365 security portal?
- Should Azure Sentinel ingest the Microsoft Defender for Endpoints data?

A security team needs to understand what raw log data is required, how alerts should be handled, and where incidents should be investigated.

This lesson will demonstrate the connecting of three services:

- Microsoft Defender for Office 365
- Microsoft Defender for Endpoint
- Microsoft 365 Defender

Connect alerts from Microsoft Defender for Office 365

Microsoft Defender for Office 365 (formerly named Office 365 Advanced Threat Protection) safeguards your organization against malicious threats posed by email messages, links (URLs), and collaboration tools. By ingesting Microsoft Defender for Office 365 alerts into Azure Sentinel, you can incorporate information about email-based and URL-based threats into your broader risk analysis and build response scenarios accordingly.

The following types of alerts are ingested:

- A potentially malicious URL click was detected
- Email messages containing malware removed after delivery
- Email messages containing phish URLs removed after delivery
- Email reported by the user as malware or phish
- Suspicious email sending patterns detected
- User restricted from sending email

To view the connector page do the following steps:

1. Select Data connectors page.
2. Select **Microsoft Defender for Office 365** (may still be called Office 365 Advanced Threat Protection).
3. Select the Open connector page on the preview pane.

4. Select **Connect** to start streaming the alerts.
5. Select whether alerts from Microsoft Defender for Office 365 automatically generate incidents by selecting **Enable**.

Connect alerts from Microsoft Defender for End-point

Microsoft Defender for Endpoint (formerly named Microsoft Defender Advanced Threat Protection) is a security platform designed to prevent, detect, investigate, and respond to advanced threats. The platform creates alerts when suspicious security events are seen in an organization. Fetch alerts generated in Microsoft Defender ATP so that you can effectively analyze security events.

The screenshot shows the Microsoft Azure portal with the URL [https://portal.azure.com/#blade/Microsoft_Azure_Sentinel/ConnectorBladeBlade/connectorId/Microsoft_Defender_Advanced_Threat_Protection](#). The page title is "Microsoft Defender Advanced Threat Protection". The left sidebar shows "Not connected" status with "Last data received" as December 6. It has sections for "Related content" (Workbooks: 0, Queries: 1, Analytic rules templates: 2), "Data received" (chart from 0 to 100, December 6 to December 13), and "Data types" (SecurityAlert (MDATP)). The main content area is divided into "Instructions" and "Next steps". Under "Prerequisites", it lists: "Workspace: read and write permissions are required.", "Tenant Permissions: required 'Global Administrator' or 'Security Administrator' on the workspace's tenant.", and "License: requires Microsoft Defender Advanced Threat Protection.". Under "Configuration", it says "Connect Microsoft Defender Advanced Threat Protection alerts to Azure Sentinel" and "Connecting Microsoft Defender Advanced Threat Protection will cause your data that is collected by Microsoft Defender Advanced Threat Protection service to be stored and processed in the location that you have configured your Azure Sentinel workspace." A "Connect" button is present. A note at the bottom states: "Microsoft Defender Advanced Threat Protection Advanced Hunting raw logs are available as part of the Microsoft 365 Defender (Preview) connector".

To view the connector page do the following steps:

1. Select Data connectors page.
2. Select **Microsoft Defender for Endpoint** (may still be called Microsoft Defender Advanced Threat Protection).
3. Select the Open connector page on the preview pane.
4. Select **Connect** to start streaming the alerts.
5. Select whether alerts from Microsoft Defender for Endpoint automatically generate incidents by selecting **Enable**.

Connect the Microsoft 365 Defender connector

The Microsoft 365 Defender connector lets you stream advanced hunting logs - a type of raw event data - from Microsoft 365 Defender into Azure Sentinel.

With the integration of Microsoft Defender for Endpoint into the Microsoft 365 Defender security umbrella, you can collect your Microsoft Defender for Endpoint advanced hunting events using the Microsoft 365 Defender connector and stream them straight into new purpose-built tables in your Azure Sentinel workspace. These tables are built on the same schema that is used in the Microsoft 365 Defender

portal, giving you complete access to the full set of advanced hunting logs and allowing you to do the following:

- Easily copy your existing Microsoft Defender ATP advanced hunting queries into Azure Sentinel.
- Use the raw event logs to provide more insights for your alerts, hunting, and investigation, and correlate events with data from other data sources in Azure Sentinel.
- Store the logs with increased retention, beyond Microsoft Defender for Endpoint or Microsoft 365 Defender's default retention of 30 days. You can do so by configuring the retention of your workspace or by configuring per-table retention in Log Analytics.

To deploy the connector, do the following steps:

1. Select **Data connectors** page.
2. Select Microsoft Defender for Endpoint (may still be called Microsoft Defender Advanced Threat Protection).
3. Then select the Open connector page on the preview pane.
4. Mark the checkboxes of the event types you wish to collect.
5. Select **Apply Changes**

The Microsoft Defender for Endpoint collection options are as follows:

Events type	Table name
Machine information (including OS information)	DeviceInfo
Network properties of machines	DeviceNetworkInfo
Process creation and related events	DeviceProcessEvents
Network connection and related events	DeviceNetworkEvents
File creation, modification, and other file system events	DeviceFileEvents
Creation and modification of registry entries	DeviceRegistryEvents
Sign-ins and other authentication events	DeviceLogonEvents
DLL loading events	DeviceImageLoadEvents

Events type	Table name
More events types	DeviceEvents

Connect Windows hosts to Azure Sentinel

Lesson Introduction

You connect Windows devices to the Azure Sentinel workspace using the provided data connector. The connector offers options to control which events to collect.

You're a Security Operations Analyst working at a company that implemented Azure Sentinel. You must collect event log data from Windows Hosts. The hosts could be located on-premise or as a virtual machine in Azure.

Your Security Operations team relies on event data created by the Sysmon tool installed on some of the Windows Hosts. You will configure the Windows hosts to send event data to Azure Sentinel. You also need to ensure that the Sysmon events are available to be used in detection rules.

One of the most common logs to collect is Windows security events. Learn how Azure Sentinel makes this easy with the Security Events connector.

Learning objectives

After completing this lesson, you should be able to:

- Connect Azure Windows Virtual Machines to Azure Sentinel
- Connect non-Azure Windows hosts to Azure Sentinel
- Configure Log Analytics agent to collect Sysmon events

Plan for Windows hosts security events connector

The Security Events connector lets you stream all security events from your Windows systems (servers and workstations, physical and virtual) to your Azure Sentinel workspace. This enables you to view Windows security events in your dashboards, use them to create custom alerts, and rely on them to improve your investigations, giving you more insight into your organization's network and expanding your security operations capabilities. You can select which events to stream from among the following sets:

- All events - All Windows security and AppLocker events.
- Common - A standard set of events for auditing purposes. A full user audit trail is included in this set. For example, it contains both user sign-in and user sign-out events (event IDs 4624, 4634). There are also auditing actions such as security group changes, key domain controller Kerberos operations, and other types of events in line with accepted best practices.
- The Common event set may contain some types of events that aren't so common. This is because the main point of the Common set is to reduce the volume of events to a more manageable level while still maintaining full audit trail capability.
- Minimal - A small set of events that might indicate potential threats. This set does not contain a full audit trail. It covers only events that might indicate a successful breach and other significant events with low rates of occurrence. For example, it contains successful and failed user logons (event IDs 4624, 4625). Still, it doesn't contain sign-out information (4634), which, while important for auditing, is not meaningful for breach detection and has a relatively high volume. Most of this set's data volume comprises sign-in events and process creation events (event ID 4688).

- None - No security or AppLocker events. (This setting is used to disable the connector.)

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with 'Connected Status' (status: Connected), 'Microsoft Provider' (provider: Security Events), and a note about 'Last Log Received'. Below that are sections for 'Related content' (Workbooks: 5, Queries: 1, Analytic rules templates: 31), 'Data received' (a chart from December 6 to December 13 with a total of 10 items), and 'Data types' (SecurityEvents). On the right, under 'Instructions', there's a 'Configuration' section. It includes steps for 'Download and install the agent' (mentioning logs are collected only from Windows agents) and 'Choose where to install the agent' (with options for 'Install agent on Azure Windows Virtual Machine' and 'Install agent on non-Azure Windows Machine'). Below that is a section for 'Select which events to stream' with options for 'All events', 'Common', 'Minimal', and 'None'. A radio button for 'All Events' is selected. At the bottom right of the configuration pane is an 'Apply Changes' button.

Connect Azure Windows Virtual Machines

To view the connector page:

1. Select **Data connectors** page.
2. Select **Security Events**.
3. Then select the **Open connector** page on the preview pane.
4. Verify that you have the appropriate permissions as described under Prerequisites.
5. Select **Install agent on Azure Windows Virtual Machine**, and then on the link that appears below.
6. For each virtual machine that you want to connect, select its name in the list that appears on the right, and then select **Connect**.
7. Select which event set (**All, Common, or Minimal**¹) you want to stream.
8. Select **Update**.

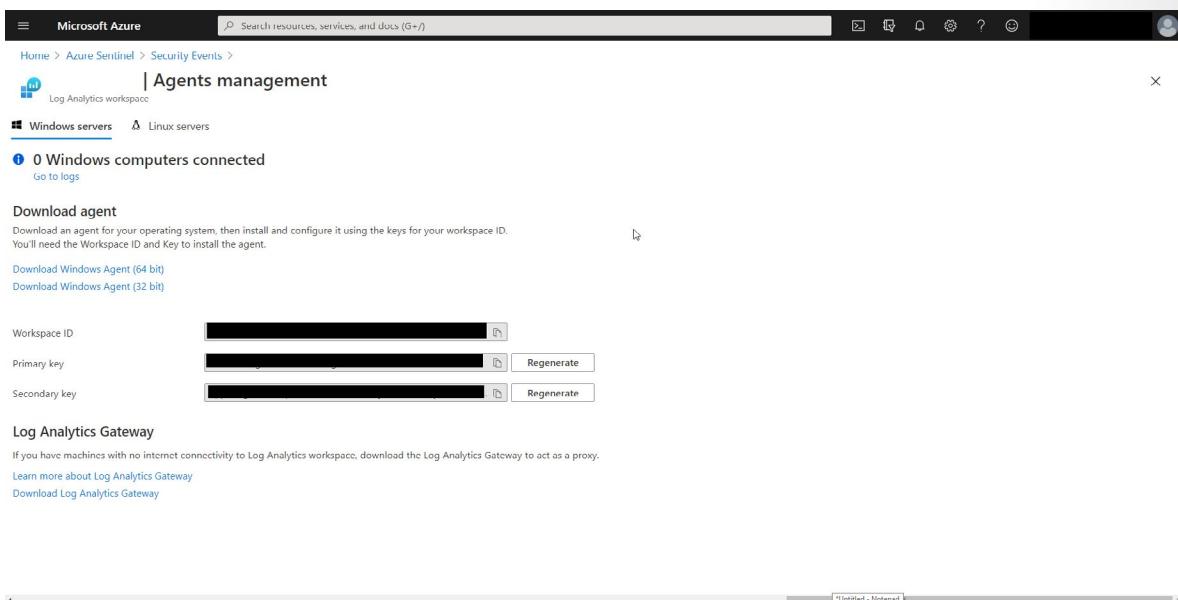
Connect non-Azure Windows Machines

To view the connector page:

1. Select **Data connectors** page.
2. Select **Security Events**.
3. Then select the **Open connector** page on the preview pane.
4. Verify that you have the appropriate permissions as described under Prerequisites.
5. Select **Install agent on non-Azure Windows Machine**, and then on the link that appears below.
6. Select the appropriate download links that appear on the right, under Windows Computers.

¹ <https://docs.microsoft.com/azure/sentinel/connect-windows-security-events?azure-portal=true>

7. Using the downloaded executable file, install the agent on the Windows systems of your choice, and configure it using the Workspace ID and Keys that appear below the download links mentioned above.
8. Select which event set (All, Common, or Minimal) you want to stream.
9. Select **Update**.



Collect Sysmon event logs

System Monitor (Sysmon) is a Windows system service, and device driver that remains resident across system reboots to monitor and log system activity to the Windows event log once installed on a system. It provides detailed information about process creations, network connections, and changes to file creation time. By collecting the events it generates using Windows Event Collection or SIEM agents and then analyzing them, you can identify malicious or anomalous activity and understand how intruders and malware operate on your network.

Installing and configuring Sysmon is out of the scope of this module. Because Sysmon is a telemetry tool that many organizations use, it is essential to know how to configure the Log Analytics Agent and Workspace to collect the Sysmon events.

After connecting the agent to the windows machine:

1. Select the **Settings** page.
2. Select **Workspace Settings**.
3. In the Log Analytics Workspace Settings area, select **Advanced Settings**.
4. Select **Data**.
5. Make sure Windows Event Logs is selected
6. In the "Collect events from the following log events" textbox, enter: *Microsoft-Windows-Sysmon/Operational*
7. Then select the **+**
8. Select **save** in the command bar.

Once configured, the Sysmon events will be available in the Event table.

The screenshot shows the Microsoft Azure Advanced settings interface for collecting event logs. On the left, there's a sidebar with 'Connected Sources', 'Data' (which is selected), and 'Computer Groups'. The main area is titled 'Collect events from the following event logs' and contains a search bar and a table. The table has columns for 'LOG NAME', 'ERROR' (with a checked checkbox), 'WARNING' (with a checked checkbox), and 'INFORMATION' (with a checked checkbox). One row is visible, showing 'Microsoft-Windows-Sysmon/Oper...' under 'LOG NAME'. A '+' button is at the top right of the table, and a 'Remove' button is at the bottom right.

Connect Common Event Format logs to Azure Sentinel

Lesson Introduction

You want to send Common Event Format (CEF) log data to the Azure Sentinel workspace using the provided data connector.

You are a Security Operations Analyst working at a company that implemented Azure Sentinel. You need to collect log data from on-premises network appliances. You can use the Common Event Format connector as the network appliances' data is provided in a structured format.

You install an on-premises Linux host used as a forwarder to send the log data. Next, follow the Common Event Format connector page's instructions to run the deployment script on the Linux host. The final step is to configure the network appliances to forward their logs to your Linux host. Now the network appliances send logs to the new Linux host; the Linux host is then forwarding the logs to the Azure Sentinel workspace.

Learn about the Common Event Format (CEF) connector's configuration options.

Learning objectives

After completing this lesson, you should be able to:

- Explain the Common Event Format connector deployment options in Azure Sentinel
- Run the deployment script for the Common Event Format connector

Plan for Common Event Format connector

You can stream events from Linux-based, Syslog-supporting machines or appliances into Azure Sentinel using the Log Analytics agent for Linux (formerly known as the OMS agent). You can do this streaming for any device that allows you to install the Log Analytics agent directly on the host. The host's native Syslog daemon will collect local events of the specified types and forward them locally to the agent, which will stream them to your Log Analytics workspace.

Log Analytics supports collecting messages sent by the **rsyslog** or **syslog-**ng**** daemons, where rsyslog is the default. The default syslog daemon on version 5 of Red Hat Enterprise Linux (RHEL), CentOS, and Oracle Linux version sysklog is not supported for Syslog event collection. The rsyslog daemon should be installed and configured to replace sysklog for these versions of Linux.

How it works

Syslog is an event logging protocol that is common to Linux. When the **Log Analytics agent for Linux** is installed on your VM or appliance, the installation routine configures the local Syslog daemon to forward messages to the agent on TCP port 25224. The agent then sends the message to your Log Analytics workspace over HTTPS, where it is parsed into an event log entry in the Syslog table in **Azure Sentinel Logs**.

Connect your external solution using the CEF connector

You need to designate and configure a Linux machine to forward the logs from your security solution to your Azure Sentinel workspace. This machine can be physical or virtual in your on-premises environment, an Azure VM, or a VM in another cloud. Using the link provided, you will run a script on the designated machine that performs the following tasks:

Installs the Log Analytics agent for Linux (also known as the OMS agent) and configures it for the following purposes:

- listening for CEF messages from the built-in Linux Syslog daemon on TCP port 25226
- sending the messages securely over TLS to your Azure Sentinel workspace, where they are parsed and enriched

Configures the built-in Linux Syslog daemon (rsyslog.d/syslog-ng) for the following purposes:

- listening for Syslog messages from your security solutions on TCP port 514
- forwarding only the messages it identifies as CEF to the Log Analytics agent on localhost using TCP port 25226

Run the deployment script

To view the connector page:

1. Select Data connectors page.
2. Select Common Event Format (CEF).
3. select the Open connector page on the preview pane.
4. Verify that you have the appropriate permissions as described under Prerequisites.
5. Copy the “sudo wget ...” command and run with elevated permissions on the dedicated Linux VM.

The screenshot shows the Microsoft Azure portal interface with the title 'Common Event Format (CEF)'. The left sidebar displays 'Not connected' status, 'Any Provider', and 'Last Log Received'. Below this, there are sections for 'Related content' (Workbooks: 0, Queries: 1), 'Data received' (100, 80, 60, 40, 20, 0), and a 'Total data received' bar (value 0). A 'Go to log analytics' button is present. On the right, the 'Configuration' section is expanded, showing steps for 'Linux Syslog agent configuration' and 'Install the CEF collector on the Linux machine'. It includes a command line for running a script: `sudo wget -O cef_installer.py https://raw.githubusercontent.com/Azure/Azure-.../`.

Using the same machine to forward both plain Syslog and common even format messages

If you plan to use this log forwarder machine to forward Syslog messages as CEF, then to avoid the duplication of events to the Syslog and CommonSecurityLog tables:

On each source machine that sends logs to the forwarder in CEF format, you must edit the Syslog configuration file to remove the facilities used to send CEF messages.

Connect syslog data sources to Azure Sentinel

Lesson Introduction

You send Syslog log data to the Azure Sentinel workspace using the provided data connector.

You are a Security Operations Analyst working at a company that implemented Azure Sentinel. You need to collect log data from on-premise network appliances. You need to use the Syslog connector as the network appliances' data is provided in an unstructured format.

You install an on-premise Linux host used as a forwarder to send the log data. Next, you follow the Syslog connector page's instructions to run the Linux host deployment script. The final step is to configure the network appliances to forward their logs to your Linux host.

Now the network appliances send logs to the new Linux host; the Linux host is then forwarding the logs to the Azure Sentinel workspace. You create a parser using a KQL function to make it easier for the Security Operations team to query the log records containing the unstructured string data.

Learn about the Syslog connector's configuration options which will enable you to parse Syslog data.

Learning objectives

After completing this lesson, you should be able to:

- Describe the Syslog connector deployment options in Azure Sentinel
- Run the connector deployment script to send data to Azure Sentinel
- Configure the Log Analytics agent integration for Azure Sentinel
- Create a parse using KQL in Azure Sentinel

Plan for the syslog connector

You can stream events from Linux-based, Syslog-supporting machines or appliances into Azure Sentinel using the Log Analytics agent for Linux (formerly known as the OMS agent). You can do this streaming for any device that allows you to install the Log Analytics agent directly on the host. The host's native Syslog daemon will collect local events of the specified types and forward them locally to the agent, which will stream them to your Log Analytics workspace.

Log Analytics supports collecting messages sent by the **rsyslog** or **syslog-ng** daemons, where rsyslog is the default. The default syslog daemon on version 5 of Red Hat Enterprise Linux (RHEL), CentOS, and Oracle Linux version sysklog is not supported for Syslog event collection. The rsyslog daemon should be installed and configured to replace sysklog for these versions of Linux.

How it works

Syslog is an event logging protocol that is common to Linux. When the **Log Analytics agent for Linux** is installed on your VM or appliance, the installation routine configures the local Syslog daemon to forward messages to the agent on TCP port 25224. The agent then sends the message to your Log Analytics workspace over HTTPS, where it is parsed into an event log entry in the Syslog table in **Azure Sentinel Logs**.

Collect data from Linux-based sources using syslog

To view the connector page:

1. Select **Data** connectors page.
2. Select **Syslog**.
3. Then select the Open connector page on the preview pane.
4. Verify that you have the appropriate permissions as described under Prerequisites.
5. Select the Choose where to install the agent option to expand the instructions.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with 'Microsoft Azure' and a search bar. Below it, the breadcrumb navigation shows 'Home > Azure Sentinel > Syslog'. The main content area has a title 'Syslog' with a 'Not connected' status, a Microsoft Provider icon, and a 'Last Log Received' section. On the left, there's a sidebar with 'Related content' (Workbooks, Queries, Analytic rules templates) and a chart titled 'Data received' showing values from 0 to 100 over a period from December 6 to December 13. The total data received is currently at 0. On the right, there are two tabs: 'Instructions' (selected) and 'Next steps'. Under 'Instructions', there's a section titled 'Configuration' with the following steps:

1. Install and onboard the agent for Linux

Typically, you should install the agent on a different computer from the one on which the logs are generated.

Syslog logs are collected only from **Linux** agents.

Choose where to install the agent:

- ✓ Install agent on Azure Linux Virtual Machine
- ✓ Install agent on a non-Azure Linux Machine

2. Configure the logs to be collected

Configure the facilities you want to collect and their severities.

Under workspace advanced settings **Configuration**, select **Data** and then **Syslog**.

Select **Apply below configuration to my machines** and select the facilities and severities.

Click **Save**.

[Open your workspace advanced settings configuration >](#)

For an Azure Linux VM:

To install the agent on an Azure Linux virtual machine:

1. Install agent on Azure Linux Virtual Machine.
2. Select the link Download & install agent for Azure Linux Virtual machines.
3. Select **Connect** on the row of the Linux VM.

For any other Linux machine:

To install the agent on non-Azure Linux virtual hosts:

1. Install agent on a non-Azure Linux Machine.
2. Select the link Download & install agent for non-Azure Linux machines.
3. In the Agents management blade, select the Linux servers tab.
4. Copy the command for Download and onboard agent for Linux and run it on your Linux machine.
5. The page also displays your Workspace ID, primary key, and secondary key.

The screenshot shows the Microsoft Azure Log Analytics workspace Agents management page. The URL is [https://logAnalyticsworkspaceName.azureedge.net/_logAnalytics/_api/v1.0/agents](#). The page title is "Agents management". It shows "0 Linux computers connected". There is a "Download agent" section with a link to "Download Linux Agent". Below it, there is a "Download and onboard agent for Linux" section with a command-line wget command: "wget https://raw.githubusercontent.com/Microsoft/OMS-Agent-for-Linux/master/installer/scripts/onboa...". There are fields for "Workspace ID", "Primary key", and "Secondary key", each with a "Regenerate" button.

Configure the log analytics agent

The Log Analytics agent for Linux will only collect events with the facilities and severities that are specified in its configuration. You can add a new facility in the Log Analytics workspace advanced settings.

To configure the Log Analytics agent for syslog facilities:

1. Access the Log Analytics Workspace Advanced Settings page:
 - From the Syslog Data connector page, select Open your workspace advanced settings configuration.
 - From the Azure Sentinel portal, select **Settings** in the Configuration area. Select **Workspace Settings** Tab. Select **Advanced settings** in the Settings area.
2. Select **Data**.
3. Select **Syslog**.
4. Select the option **Apply below configuration to my machines**.
5. Enter the facility name and select + for each facility.

FACILITY NAME	EMERGENCY	ALERT	CRITICAL	ERROR	WARNING	NOTICE	INFO	DEBUG	
auth	<input checked="" type="checkbox"/>	Remove							
authpriv	<input checked="" type="checkbox"/>	Remove							
cron	<input checked="" type="checkbox"/>	Remove							
daemon	<input checked="" type="checkbox"/>	Remove							
kern	<input checked="" type="checkbox"/>	Remove							
local0	<input checked="" type="checkbox"/>	Remove							
local1	<input checked="" type="checkbox"/>	Remove							
mail	<input type="checkbox"/>	Remove							
syslog	<input checked="" type="checkbox"/>	Remove							
user	<input checked="" type="checkbox"/>	Remove							

By default, all configuration changes are automatically pushed to all agents. If you want to configure Syslog manually on each Linux agent, then uncheck the box *Apply below configuration to my machines*.

The following facilities are supported with the Syslog collector:

- kern
- user
- mail
- daemon
- auth
- syslog
- lpr
- news
- uucp
- cron
- authpriv
- ftp
- local0-local7

Parse syslog data with KQL

The Syslog collector writes log data to the Syslog table. One difference from the CEF Collector is that the message's data is stored in a string field named SyslogMessage. The Common Event Format (CEF) Connector writes to the CommonSecurityLog with the fields already parsed. For Syslog, you will need to parse fields on every query that uses the Sysmon table or write a Parser. A Parser is a KQL Function that is a query saved as a function and then referenced with the function name. The reference to the function name is like accessing any other table. By creating parses, you only need to write the SyslogMessage parsing once.

In the Logs window, create a query, select the Save button, and select Function from the drop-down. Then specify function name and alias. In this case, if we create the Function named MyParser, I then can access the table using the name MyParser.

```
Syslog
| where ProcessName contains "squid"
| extend URL = extract("(([A-Z]+ [a-z]{4,5}:\\""/\\/) | [A-Z]+ )([^\n:]*)",3,SyslogMessage),
    SourceIP = extract("[0-9]+ ([0-9]{1,3})\\.([0-9]{1,3})\\.([0-9]{1,3})\\\\.([0-9]{1,3})",2,SyslogMessage),
    Status = extract("(TCP_(([A-Z]+) (_[A-Z]+)* )|UDP_(([A-Z]+) (_[A-Z]+)*))",1,SyslogMessage),
    HTTP_Status_Code = extract("(TCP_(([A-Z]+) (_[A-Z]+)* )|UDP_(([A-Z]+) (_[A-Z]+)*))/([0-9]{3})",8,SyslogMessage),
    User = extract("(CONNECT |GET )([^\n]* )([^\n]+)",3,SyslogMessage),
    RemotePort = extract("(CONNECT |GET )([^\n]* )(:)([0-9]*)",4,SyslogMessage),
    Domain = extract("(([A-Z]+ [a-z]{4,5}:\\""/\\/) | [A-Z]+ )([^\n:\\/]*)",3,SyslogMessage)
| extend TLD = extract("\\.[a-z]*$",0,Domain)
```

MyParser

Connect threat indicators to Azure Sentinel

Lesson Introduction

You connect Threat Intelligence Indicators to the Azure Sentinel workspace using the provided data connectors.

You are a Security Operations Analyst working at a company that implemented Azure Sentinel. Your company has subscriptions to threat intelligence platform services that provide known malicious indicators for use in your detection rules.

You need to configure Azure Sentinel to import the indicators from these services automatically. The first service uses a TAXII server to allow indicators to be pulled. You configure the TAXII data connector to pull indicators from the service.

The next service provider does not use a TAXII server, but has created push integration capabilities to Azure Sentinel. You follow the instructions to configure the Threat Intelligence Platform connector. Now that the connectors are flowing into Azure Sentinel, the SecOps teams can use the indicators as part of their detection queries.

Learn how to connect Threat Intelligence Indicators to the Azure Sentinel workspace using the provided data connectors.

Learning objectives

After completing this lesson, you should be able to:

- Configure the TAXII connector in Azure Sentinel
- Configure the Threat Intelligence Platform connector in Azure Sentinel
- View threat indicators in Azure Sentinel

Plan for threat intelligence connectors

Azure Sentinel lets you import the threat indicators your organization uses, which can enhance your security analysts' ability to detect and prioritize known threats. Several features from Azure Sentinel then become available or are enhanced:

- Analytics includes a set of scheduled rule templates you can enable to generate alerts and incidents based on matches of log events from your threat indicators.
- Workbooks provide summarized information about the threat indicators imported into Azure Sentinel and any alerts generated from analytics rules that match your threat indicators.
- Hunting queries allow security investigators to use threat indicators within the context of common hunting scenarios.
- Notebooks can use threat indicators when you investigate anomalies and hunt for malicious behaviors.

You can stream threat indicators to Azure Sentinel by using one of the integrated threat intelligence platform (TIP) products, connecting to TAXII servers, or direct integration with the Microsoft Graph Security `threatIndicators` API.

There are two Threat Intelligence Connectors. The TAXII Connector and the Threat Intelligence Platforms Connector. Both connectors write to the `ThreatIntelligenceIndicator` table. The two connectors have different configuration procedures.

Connect the threat intelligence TAXII connector

Azure Sentinel integrates with TAXII 2.0 and 2.1 data sources to enable monitoring, alerting, and hunting using your threat intelligence. Use this connector to send threat indicators from TAXII servers to Azure Sentinel. Threat indicators can include IP addresses, domains, URLs, and file hashes.

In the Azure portal, navigate to Azure Sentinel > Data connectors and then select the Threat Intelligence - TAXII (Preview) connector.

To view the connector page:

1. Select Data connectors page.
2. Select **Threat intelligence - TAXII**.
3. select the Open connector page on the preview pane.
4. Specify the required and optional information in the text boxes.
 - Friendly name (for server)
 - API root URL
 - Collection ID
 - Username
 - Password
5. Select **Add** to enable the connection.

The list of configure TAXII servers shows the currently connected TAXII servers and the last indicator received time. The ellipse at the end of the configured server provides the option to remove the server configuration.

The screenshot shows the Azure Sentinel Threat intelligence - TAXII (Preview) configuration page. On the left, there's a sidebar with a 'Connected' status (2 days ago), a Microsoft Provider icon, and a 'Last Log Received' timestamp (12/13/20, 12:51 PM). Below this are sections for 'Related content' (Workbooks: 2, Queries: 2, Analytic rules templates: 28), 'Data received' (10.05k total, with a chart showing a sharp peak around December 13), and 'Data types' (ThreatIntelligenceIndicator, 12/13/20, 12:51 PM). The main right-hand panel has tabs for 'Instructions' (selected) and 'Next steps documentation'. It contains fields for 'Friendly name (for server)*', 'API root URL*', 'Collection ID*', 'Username', and 'Password', each with a placeholder and a red asterisk indicating it's required. A large blue 'Add' button is centered below these fields. At the bottom, there's a table titled 'List of configured TAXII servers' with columns for 'Friendly name', 'TAXII server', 'Collection ID', and 'Last indicator receiv..'. One entry is listed: 'LimoPhishURLS' with 'https://limo.anomali.com/' as the TAXII server, '107' as the Collection ID, and '12/13/20, 10:28 AM' as the last indicator received time. A search bar is also present above the table.

Connect the threat intelligence platforms connector

Azure Sentinel integrates with Microsoft Graph Security API data sources to enable monitoring, alerting, and hunting using your threat intelligence. Use this connector to send threat indicators to Azure Sentinel from your Threat Intelligence Platform (TIP), such as Threat Connect, Palo Alto Networks MindMeld, MISP, or other integrated applications. Threat indicators can include IP addresses, domains, URLs, and file hashes.

Connect Azure Sentinel to your threat intelligence platform

The screenshot shows the Azure portal interface with the title 'Threat Intelligence Platforms (Preview)'. On the left, there's a sidebar with 'Connected Status' (Status: Microsoft Provider, Last log received: 100), 'Related content' (Workbooks: 2, Queries: 2, Analytic rules templates: 28), and a chart titled 'Data received' showing a count of 100 from December 6 to December 13. On the right, under 'Instructions', it says 'You can connect your threat intelligence data sources to Azure Sentinel by either:' followed by two bullet points: 'Using an integrated Threat Intelligence Platform (TIP), such as Threat Connect, Palo Alto Networks MindMeld, MISP, and others.' and 'Calling the Microsoft Graph Security API directly from another application.' Below this, a section titled 'Follow These Steps to Connect your Threat Intelligence:' lists four steps: 1) Register an application in Azure Active Directory, 2) Configure permissions and add the ThreatIndicators.ReadWrite.OwnedBy permission, 3) Ask your Azure AD tenant administrator to grant consent, and 4) Configure your TIP or application to push indicators to Azure Sentinel by specifying the application ID, secret, and target (Azure Sentinel). A note at the bottom says 'For the latest list of integrated Threat Intelligence Platforms and detailed configuration instructions, see the full documentation.'

1. Register an application in Azure Active Directory to get an application ID, application secret, and Azure Active Directory tenant ID. You need these values for when you configure your integrated TIP product or app that uses direct integration with Microsoft Graph Security `tilndicators` API.
2. Configure API permissions for the registered application: Add the Microsoft Graph Application permission **ThreatIndicators.ReadWrite.OwnedBy** to your registered application.
3. Ask your Azure Active Directory tenant administrator to grant admin consent to the registered application for your organization. From the Azure portal: Azure Active Directory - App registrations - *app name* - View API Permissions - Grant admin consent for *tenant name*.
4. Configure your TIP product or app that uses direct integration with Microsoft Graph Security `tilndicators` API to send indicators to Azure Sentinel by specifying the following:
 - The values for the registered application's ID, secret, and tenant ID.
 - For the target product, specify Azure Sentinel.
 - For the action, specify alert.
5. In the Azure portal, navigate to **Azure Sentinel** then **Data connectors** and then select the **Threat Intelligence Platforms (Preview)** connector.
6. Select **Open connector page**, and then **Connect**.

7. To view the threat indicators imported into Azure Sentinel, navigate to **Azure Sentinel Logs** then **SecurityInsights**, and lastly expand **ThreatIntelligenceIndicator**.

View your threat indicators

The indicators reside in the ThreatIntelligenceIndicator table. This table is the basis for queries performed by other Azure Sentinel features such as Analytics and Workbooks. Here's how to find and view your threat indicators in the ThreatIntelligenceIndicator table.

To view your threat indicators with KQL. Select Logs from the General section of the Azure Sentinel menu. Then run a query on the ThreatIntelligenceIndicator.

ThreatIntelligenceIndicator

Knowledge check

Check your Knowledge

Multiple choice

Item 1. Where can you see the number of connected Windows hosts?

- On the CEF Connector page
- On the Agent Management page in Log Analytics
- On the Data connectors page

Multiple choice

Item 2. Which connector provides the log data in an unparsed field?

- Azure Active Directory
- Syslog
- CEF

Multiple choice

Item 3. The vendor-provided connectors primarily use which of the following?

- Azure Activity Connector
- Security Events Connector
- CEF Connector

Multiple choice

Item 4. Which table (data type) would you query for the Azure Active Directory data?

- OfficeActivity
- SigninLogs
- SecurityAlert

Multiple choice

Item 5. Which table (data type) would you query for the Office 365 data?

- OfficeActivity
- SecurityAlert
- SigninLogs

Multiple choice

Item 6. Which table (data type) would you query for the Azure Active Directory Information Protection data?

- OfficeActivity
- SigninLogs
- SecurityAlert

Multiple choice

Item 7. Which connector would you use to connect the raw data from Microsoft Defender for Endpoint?

- Microsoft Defender for Office 365
- Microsoft Defender for Endpoint
- Microsoft 365 Defender

Multiple choice

Item 8. Which Microsoft security product is part of the Microsoft 365 Defender suite of products?

- Microsoft Cloud App Security
- Azure Active Directory Identity Protection
- Azure Active Directory

Multiple choice

Item 9. Which table (Data type) does the Microsoft Defender for Office 365 connector write to?

- SecurityAlert
- CommonSecurityLog
- SecurityEvent

Multiple choice

Item 10. Which connector do you use to collect Windows security events?

- Security Events
- Common Event Format
- Syslog

Multiple choice

Item 11. To collect Sysmon events with the Security Events connector, what is the log name used to collect it in advanced settings?

- Microsoft-Windows-Sysmon/Operational
- Microsoft-Windows-Sysmon/Events
- Microsoft-Windows-Sysmon/Logs

Multiple choice

Item 12. Which table contains the ingested Sysmon events?

- Event
- CommonSecurityLog
- SecurityEvents

Multiple choice

Item 13. The CEF connector writes to which table?

- CommonSecurityLog
- SecurityEvent
- Syslog

Multiple choice

Item 14. The CEF connector deploys what type of forwarder?

- Syslog
- Event
- Sysmon

Multiple choice

Item 15. The CEF connector can be deployed on which platform?

- Azure Windows Virtual Machine
- On-premises Windows Host
- Azure Linux Virtual Machine

Multiple choice

Item 16. What field contains the unstructured event data?

- SyslogData
- SyslogEvent
- SyslogMessage

Multiple choice

Item 17. To create a parser in the Log query window, save the query as which of the following?

- Module
- Function
- Table

Multiple choice

Item 18. The Syslog connector can be deployed on which platform?

- Azure Windows Virtual Machine
- On-premise Windows Host
- Azure Linux Virtual Machine

Lab - Connect logs to Azure Sentinel

Lab: Connect logs to Azure Sentinel

To download the most recent version of this lab, please visit the SC-200 [GitHub repository²](#).

Note: Depending on the lab hosting solution used for your class delivery, the lab instructions may display directly in the virtual lab environment, in addition to being available in the GitHub repository. In that case, follow guidance from your instructor as to where you will access the lab steps from. Even if the GitHub version is not used for your class, you may still find it useful to be able to reference the lab instructions on GitHub after class is over.

Lab scenario

You're a Security Operations Analyst working at a company that implemented Azure Sentinel. You must learn how to connect log data from the many different data sources in your organization. The organization has data from Microsoft 365, Microsoft 365 Defender, Azure resources, non-azure virtual machines, and network appliances.

You plan on using the Azure Sentinel data connectors to integrate the log data from the various sources. You need to write a connector plan for management that maps each of the organization's data sources to the proper Azure Sentinel data connector.

Objectives

After you complete this lab, you will be able to:

- Connect data to Azure Sentinel using data connectors.
- Connect Windows devices to Azure Sentinel using data connectors.
- Connect Linux hosts to Azure Sentinel using data connectors.
- Connect Threat intelligence to Azure Sentinel using data connectors.

Lab setup

- Estimated time: 60 minutes

² <https://github.com/MicrosoftLearning/SC-200T00A-Microsoft-Security-Operations-Analyst>

Answers

Multiple choice

Item 1. Where can you see the number of connected Windows hosts?

- On the CEF Connector page
- On the Agent Management page in Log Analytics
- On the Data connectors page

Explanation

On the Agent Management page in Log Analytics, this page will display the hosts connected.

Multiple choice

Item 2. Which connector provides the log data in an unparsed field?

- Azure Active Directory
- Syslog
- CEF

Explanation

The data is stored in the SyslogMessage

Multiple choice

Item 3. The vendor-provided connectors primarily use which of the following?

- Azure Activity Connector
- Security Events Connector
- CEF Connector

Explanation

Most Vendor-provided connectors use the CEF connector.

Multiple choice

Item 4. Which table (data type) would you query for the Azure Active Directory data?

- OfficeActivity
- SigninLogs
- SecurityAlert

Explanation

The connector writes to SigninLogs.

Multiple choice

Item 5. Which table (data type) would you query for the Office 365 data?

- OfficeActivity
- SecurityAlert
- SigninLogs

Explanation

This connector writes to the OfficeActivity table.

Multiple choice

Item 6. Which table (data type) would you query for the Azure Active Directory Information Protection data?

- OfficeActivity
- SigninLogs
- SecurityAlert

Explanation

This connector writes to the SecurityAlert table.

Multiple choice

Item 7. Which connector would you use to connect the raw data from Microsoft Defender for Endpoint?

- Microsoft Defender for Office 365
- Microsoft Defender for Endpoint
- Microsoft 365 Defender

Explanation

The connector can be configured to send the raw data from Defender for Endpoint.

Multiple choice

Item 8. Which Microsoft security product is part of the Microsoft 365 Defender suite of products?

- Microsoft Cloud App Security
- Azure Active Directory Identity Protection
- Azure Active Directory

Explanation

Microsoft Cloud App Security is part of the Microsoft 365 Defender suite of products.

Multiple choice

Item 9. Which table (Data type) does the Microsoft Defender for Office 365 connector write to?

- SecurityAlert
- CommonSecurityLog
- SecurityEvent

Explanation

The connect ingests alerts.

Multiple choice

Item 10. Which connector do you use to collect Windows security events?

- Security Events
- Common Event Format
- Syslog

Explanation

THe Security Events connector will collect Windows security events.

Multiple choice

Item 11. To collect Sysmon events with the Security Events connector, what is the log name used to collect it in advanced settings?

- Microsoft-Windows-Sysmon/Operational
- Microsoft-Windows-Sysmon/Events
- Microsoft-Windows-Sysmon/Logs

Explanation

This is the name to enter.

Multiple choice

Item 12. Which table contains the ingested Sysmon events?

- Event
- CommonSecurityLog
- SecurityEvents

Explanation

The Event table contains the ingested logs.

Multiple choice

Item 13. The CEF connector writes to which table?

- CommonSecurityLog
- SecurityEvent
- Syslog

Explanation

The connector writes to the CommonSecurityLog

Multiple choice

Item 14. The CEF connector deploys what type of forwarder?

- Syslog
- Event
- Sysmon

Explanation

The CEF connector deploys a Syslog forwarder

Multiple choice

Item 15. The CEF connector can be deployed on which platform?

- Azure Windows Virtual Machine
- On-premises Windows Host
- Azure Linux Virtual Machine

Explanation

Linux is required.

Multiple choice

Item 16. What field contains the unstructured event data?

- SyslogData
- SyslogEvent
- SyslogMessage

Explanation

This field contains unstructured data.

Multiple choice

Item 17. To create a parser in the Log query window, save the query as which of the following?

- Module
- Function
- Table

Explanation

A Function is a named KQL query that is access like a regular table.

Multiple choice

Item 18. The Syslog connector can be deployed on which platform?

- Azure Windows Virtual Machine
- On-premise Windows Host
- Azure Linux Virtual Machine

Explanation

Linux is required.

Module 7 Create detections and perform investigations using Azure Sentinel

Threat detection with Azure Sentinel analytics

Lesson Introduction

Microsoft Azure Sentinel Analytics provides an intelligent solution that you can use to detect potential threats and vulnerabilities in your organizations.

Imagine that you work as Security Operations Center (SOC) analyst in Contoso, Ltd. Contoso is a midsize financial services company in London with a New York branch office. Contoso uses several Microsoft products and services to implement data security and threat protection for its resources. These products are:

- Microsoft 365
- Azure Active Directory (Azure AD)
- Azure AD Identity Protection
- Microsoft Cloud App Security
- Microsoft Defender for Identity
- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- System Center Endpoint Protection
- Microsoft Azure Information Protection

Contoso provides threat protection for its Azure-based and on-premises resources by using the paid version of Azure Security Center. The company also monitors and protects other non-Microsoft assets. Security analysts at Contoso face a huge triage burden. They deal with a high volume of alerts from multiple products. They correlate alerts in the following ways:

- Manually from different project dashboards
- By using a traditional correlation engine

Additionally, the time spent to set up and maintain IT infrastructure takes the SOC team away from its security tasks.

The IT director believes that Azure Sentinel Analytics will help the security analysts perform complex investigations faster and improve their Security Operations Center (SOC). As Contoso's lead system engineer and Azure administrator, you've been asked to set up analytics rules in Azure Sentinel so that the SecOps team can identify and analyze attacks to Contoso's resources.

In this module, you'll understand the importance of using Azure Sentinel Analytics, create, and implement analytics rules from existing templates, create new rules and queries using the wizard, and manage rules with modifications.

In this module, you learned how Azure Sentinel Analytics can help the SecOps team identify and stop cyber attacks.

Learning objectives

After completing this lesson, you should be able to:

- Explain the importance of Azure Sentinel Analytics.
- Explain different types of analytics rules.
- Create rules from templates.
- Create new analytics rules and queries using the analytics rule wizard.
- Manage rules with modifications.

Azure Sentinel Analytics explained

Azure Sentinel Analytics helps you detect, investigate, and remediate cybersecurity threats. The Contoso SOC team can use Azure Sentinel Analytics to set up analytics rules and queries to detect issues in your environment.

What is Azure Sentinel Analytics?

Azure Sentinel Analytics provides several functionalities that you can use to implement security for the data and resources at Contoso.

You can analyze historical data collected from your workstations, servers, networking devices, firewalls, intrusion prevention, sensors, and so on. Azure Sentinel Analytics analyzes data from various sources to identify correlations and anomalies.

By using analytics rules, you can trigger alerts based on the attack techniques that are used by known malicious actors. You can set up these rules to help ensure your SOC is alerted to potential security incidents in your environment in a timely fashion.

Why use analytics rules for security operations?

Although some of the other products that Contoso has implemented can help you identify threats, Azure Sentinel Analytics plays an important part in the overall detection of the security threat by correlating and matching the signals that impact the presence of a cybersecurity threat. With the proper analytics rule, you can get insights into where an attack originated from, what resources were compromised, potential data lost, along with the timeline for the incident.

Common security analytics use cases include:

- Identification of compromised accounts
- User behavior analysis to detect potentially suspicious patterns
- Network traffic analysis to locate trends indicating potential attacks
- Detection of data exfiltration by attackers
- Detection of insider threats
- Investigation of incidents
- Threat hunting

You might not be able to detect some of the threats by using conventional protection tools, such as firewalls or antimalware solutions. Certain threats can go undetected for months. Combining data, gathered by multiple tools and products, with the power of threat intelligence can help you to detect, analyze, and mitigate insider threats.

You can also use analytics rules to create custom alerts that use indicators of attack. These indicators can identify potential attacks that are in progress in real time.

Analytics will help the Contoso SOC team to improve the efficiency of their complex investigation and detect threats faster.

Exploring the Analytics home page

You can create analytics rules from the **Analytics** home page. You can access the **Analytics** page in Azure Sentinel from the navigation pane.

The screenshot shows the Azure Sentinel Analytics interface. The Header bar at the top displays the title "Azure Sentinel | Analytics" and the workspace name "Contoso-Demo78". Below the header is a toolbar with buttons for Create, Refresh, Enable, Disable, and Delete. A red box highlights the "Header bar" area. The main content area is titled "Rules and Templates". It contains a search bar and filters for Severity (All), Rule Type (All), Status (All), and Tactics (All). A red box highlights the "Rules and Templates" section. A table lists three rule templates: "Advanced Multistage Attack Detection" (High severity, Fusion rule type, Enabled status, Tactics: BuiltInFusion), "Create incidents based on Azure Active Directory Identity Changes" (High severity, Microsoft Security rule type, Enabled status, Tactics: None), and "Create incidents based on Azure Security Center alerts" (High severity, Microsoft Security rule type, Enabled status, Tactics: None). A red box highlights this table. To the right is a "Detailed Pane" for the first rule template, titled "Advanced Multistage Attack Detection". It shows the rule's status as "Enabled" and its ID as "BuiltInFusion". The "Description" section explains that the rule uses Fusion technology to detect multistage attacks by identifying anomalous behaviors and suspicious activities. A blue "Edit" button is at the bottom of the pane.

The **Analytics** home page has three main parts:

- The header bar contains information on the number of the rules that are currently in use.
- The list of rules and templates contains all the rule templates that Microsoft has preloaded from the Azure Sentinel GitHub repository.
- The details pane contains additional information that explains each template and rule that you can use in detection.

Filter the rule templates

Currently Microsoft has preloaded over 150 template rules from the Azure Sentinel GitHub repository. To search these templates and to access the appropriate rule, you need to apply filters. For example, you might want to review only template rules that detect threats with a high severity level or rules from specific data sources.

To use filters, in the header bar, select the filters you want to use.



The **Analytics** home page provides the following filters:

- **Severity**. Use to filter the rules by levels of severity.
- **Rule Type**. There are currently four types of rules: Scheduled, Fusion, Microsoft Security, Machine Learning Behavior Analytics.
- **Tactics**. Use to filter the rules based on 14 specific techniques and methodologies in ATT&CK model.
- **Data Sources**. Use to filter the rules by the data source connector that generates the alert.

Note: MITRE ATT&CK is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

Types of analytics rules

By using Azure Sentinel Analytics rules, you can configure notification and alerts based on data coming from the sources that are connected to Azure Sentinel. These alerts will help ensure that the Contoso SOC team knows when a threat occurs, and the team can then appropriately react to prevent the threat from reaching your corporate assets.

You can search for potential threats by using the built-in analytics rules that Azure Sentinel Analytics provides. There are currently four types of analytics rules:

- Fusion
- Microsoft security
- Machine learning (ML) behavior analytics
- Scheduled alerts

SEVERITY ↑↓	NAME ↑↓	RULE TYPE ↑↓	DATA SOURCES	TACTICS
High	Create incidents based on ...	Microsoft Security (Preview)	Azure Security Cent...	
High	Create incidents based on ...	Microsoft Security (Preview)	Office 365 Advance...	
High	Suspicious application con...	Scheduled	Azure Active Direct...	🎭🌐
High	Known Phosphorus group ...	Scheduled	DNS (Preview) +4 ⓘ	📱Command and ...
High	Known IRIDIUM IP	Scheduled	Office 365 +10 ⓘ	📱Command and ...
High	Create incidents based on ...	Microsoft Security (Preview)	Azure Active Direct...	

Fusion alerts

Fusion alerts identify anomalous behaviors and suspicious activities at various stages of the cyber kill chain. Fusion correlates multiple security alerts from various products and uses machine Learning to detect advanced multistage attacks.

Note: The cyber kill chain describes the typical workflow, including techniques, tactics, and procedures (TTPs), used by attackers to infiltrate an organization's networks and systems.

By default, Fusion detection is enabled in Azure Sentinel. Microsoft is constantly updating Fusion detection scenarios for threat detection. At the time of writing this article, for Fusion detection, you must configure the following data connectors:

- Azure Active Directory Identity Protection
- Microsoft Cloud App Security
- Microsoft Defender Advanced Threat Protection
- Palo Alto Networks

Some of the common attack detection scenarios that Fusion alerts identify include:

- **Data exfiltration.** Suspicious activity detected, such as suspicious forwarding rule in Microsoft 365 mailbox, after a suspicious sign-in to Azure AD account can indicate compromised user account.
- **Data destruction.** Anomalous number of unique files that were deleted after a suspicious sign-in to Azure AD account can signal that a compromised user account was used to destroy data.
- **Denial of service.** Significant number of Azure virtual machines (VMs) deleted after a suspicious sign-in to Azure AD account can signal a compromised user account that can be used to destroy the organization's assets.
- **Lateral movement.** Significant number of impersonation actions that occur after a suspicious sign-in to Azure AD account can indicate a compromised user account that was used for malicious purposes.
- **Ransomware.** After a suspicious sign-in to an Azure AD account, unusual user behavior used to encrypt data can trigger a ransomware execution alert.

Note: For more information on the Fusion technology in Azure Sentinel, see [Advanced multistage attack detection in Azure Sentinel¹](#)

¹ <https://docs.microsoft.com/azure/sentinel/fusion>

Microsoft security

You can configure Microsoft security solutions that are connected to Azure Sentinel to automatically create incidents from all alerts generated in the connected service.

For example, you can configure for Contoso to be alerted when a user who has been categorized as a high-risk threat attempts to sign in and access corporate resources.

You can configure the following security solutions to pass their alerts to Azure Sentinel:

- Microsoft Cloud App Security
- Azure Defender for Server
- Azure Defender for IoT
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Azure Active Directory Identity Protection
- Microsoft Defender for Endpoint

Note: Microsoft unifies security information and event management (SIEM) and extended detection and response (XDR) terminology across their security products.

You can filter these alerts by severity and by specific text that is contained in the alert name.

Machine learning behavioral analytics

Azure Sentinel Analytics includes built-in machine learning behavioral analytics rules. You can't edit these built-in rules or review the rule settings. These rules use Microsoft machine learning algorithms to detect suspicious activity. Machine Learning algorithms correlate several low-fidelity incidents into a high-fidelity security incident. This saves hours that you might otherwise spend manually analyzing numerous alerts from different products and correlating them. Machine learning algorithms that analytics rules use also help reduce the noise around alerts by quickly ingesting and connecting important data.

For example, by using a machine learning behavioral analytics rule, you can detect an anomalous secure shell protocol (SSH) Login or remote desktop protocol (RDP) login activity.

Scheduled alerts

Scheduled alerts analytics rules provide you the highest level of customization. You can define your own expression using Kusto Query Language (KQL) to filter the security events, and you can set up a schedule for the rule to run.

Create an analytics rule from a template

The Analytics section in Azure Sentinel contains rule templates that are preloaded from the Azure Sentinel GitHub repository. You can use these templates to create a rule to detect security threats.

Exploring the existing rule templates

You can use some of the existing rule templates to create a single rule and others to create multiple rules with different customization options. Templates that are in use display the **IN USE** label on the template page as displayed in the following screenshot.

High	Create incidents based on Microsoft Defender Advanced Threat Protect...	Microsoft Security (Preview)	Microsoft Defender Advanced Threat Protectio...
High	IN USE Advanced Multistage Attack Detection	Fusion	
High	IN USE Create incidents based on Azure Security Center alerts	Microsoft Security (Preview)	Azure Security Center

By selecting one of the rules on the **Rule Template** tab, you can observe the properties of the rule. For each rule, you can review:

- Severity level. This indicates the importance of the alert. There are four severity levels:
 - High
 - Medium
 - Low
 - Informational
- Name of the rule. This provides a meaningful name for the alert rule.
- Rule type. This defines the type of the rule that can be one of the following four types:
 - Fusion
 - Microsoft Security
 - ML Behavior Analytics
 - Scheduled
- Data Source. This specifies the data source connector that generated the alert.
- Tactics. This specifies techniques and methodologies in MITRE ATT&CK model used by different kinds of malware.

Note: MITRE ATT&CK is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base provides a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

When you select a rule name on the template page, the details pane of the selected rule provides more information for the rule. Depending on the type of the rule that you select, the details pane can contain different fields of information. For Fusion and ML behavior analytics rules, Microsoft doesn't provide any additional information. However, for scheduled rules, you can review the query rule used in the threat detection.

Creating an analytic rule from a rule template

When you select a predefined rule template, the details pane provides the **Create rule** button. By selecting this button, you can create an analytics rule from that template. The composition of the analytics rule built from the template depends on the rule type that you select.

By default, Azure Sentinel Analytics creates an alert rule using the Fusion rule template. For ML behavior analytics, you can only create a rule as enabled or disabled, and you don't have the option to further customize the rule.

A rule you create from the Microsoft security templates consists of the following elements:

- **Name.** This is prepopulated from the name of the rule template.

- **Description.** This provides more details on the creation of the alerts.
- **Status.** This indicates whether the analytics rule is enabled or disabled.
- **Analytic rule logic.** This indicates the source of the alert from one of the Microsoft security services.
- **Filter by severity.** Use to tune alerts from a source based on the severity level, which can be High, Medium, Low, or Informational.
- **Include specific alerts.** Use to filter alerts that contain a specific text in their name.
- **Exclude specific alerts.** Use to filter alerts that don't contain a specific text in their name.

NOTE: When you implement filters to include or exclude specific alerts based on a text string, these alerts will not appear in Azure Sentinel.

The following screenshot presents an example of creating an incident from alerts generated by the Azure Security Center.

Analytics rule wizard - Create new rule from template

Create incidents based on Azure Security Center alerts

General Review and create

Create an analytics rule that creates incidents based on alerts generated in another Microsoft security service.

Analytics rule details

Name *****
Create incidents based on Azure Security Center alerts

Description
Create incidents based on all alerts generated in Azure Security Center

Status
Enabled Disabled

Analytics rule logic

Microsoft security service *****
Azure Security Center

Filter by severity
 Any
 Custom

Include specific alerts
Only create incidents from alerts that contain the following text in the alert name
[redacted]

Next : Review >

The “Creating an Analytics” rule from the wizard describes how to create an analytics rule from a scheduled template rule type.

Note: For certain rule templates, the **Create rule** button might be disabled, which indicates that you can't create a rule from selected template because of a missing data source.

Create an analytics rule from a wizard

You can create a custom analytics rule to search for suspicious activities and threats at Contoso.

Creating a custom rule from the scheduled query rule type provides you with the highest level of customization. You can define your own KQL code, set a schedule to run the alerts, or provide an automated action by associating an Azure Sentinel Playbook.

To create an analytics rule, in the Azure portal, under **Azure Sentinel**, select **Analytics**. In the top menu bar, select **Create**, and then select **Scheduled query rule**.

Set rule logic

On the **Set rule logic** page, you can define the detection method by specifying KQL code that will run against the Azure Sentinel workspace. The KQL query will filter the security data that is used to trigger and create an incident.

When you enter the KQL query string in the **Rule query** field, you can use the **Results simulation (preview)** section to review the results of the query. The **Results simulation (preview)** section will help you determine whether your query returned the expected results.

The screenshot shows the 'Analytics rule wizard - Edit existing rule' interface. The 'General' tab is selected. The 'Set rule logic' tab is active, showing a KQL query for 'Azure VM Deletion'. The 'Results simulation (preview)' section displays a chart of the last 50 evaluations. A red box highlights the 'Test with current data' button.

The following sample query alerts you when an anomalous number of resources is created in Azure Activity.

```
AzureActivity
| where OperationName == "Create or Update Virtual Machine" or OperationName
== "Create Deployment"
| where ActivityStatus == "Succeeded"
| make-seriesdcnt(ResourceId) default=0 on EventSubmissionTimestamp
inrange(ago(7d), now(), 1d) by Caller
```

Tip: For assistance with the query language, refer to the Query Language Reference at <https://docs.microsoft.com/en-us/azure/kusto/query/>²

² <https://docs.microsoft.com/azure/kusto/query/>

Map entities

In the **Map entities** section, you can define the entities that are returned as part of the query rule, and then use these entities to perform in-depth analysis by selecting **Add** to add these entities in the query rule. These entities can help you perform a visual investigation because they will appear as a group on the **Incident** tab. Some of the entities contain information that represents a user, a host, or an IP address.

Query Scheduling

In the **Query Scheduling** section, you can configure how often the query should run, and how far back in history the query should search the data. It's important that you don't search for data that is older than the query's run frequency because that can create duplicate alerts.

Alert threshold

In the **Alert threshold** section, you can specify the number of a positive result that can be returned for the rule before it generates an alert. You can use the following logical operators to define an appropriate logical expression:

- Is greater than
- Is fewer than
- Is equal to
- Is not equal to

Event grouping

In the **Event grouping** section, you can select one of the following two options:

- **Group all events into a single alert.** This is the default option, and it creates a single alert if the query returns more results than that the specified alert threshold.
- **Trigger an alert for each event.** This option creates unique alerts for each event returned by the query.

Suppression

In the **Suppression** section, you can set the **Stop running the Query after the alert is generated** option to **On** or **Off**. When you select **On**, Azure Sentinel pauses the creation of additional incidents if the rule is triggered again for the duration you want the rule to be suppressed.

Incident settings

Use the **Incident settings** page to create an Incident from the alerts that are triggered by the analytics rule.

In the **Alert grouping** section, you can reduce the noise from multiple alerts by grouping them into one incident. When you enable grouping of related alerts, you can choose from the following options:

- **Grouping alerts into a single incident if all the entities match (recommended)**
- **Grouping all alerts triggered by this rule into a single incident**

- **Grouping alerts into a single incident if the selected entities match** - for example source or target IP addresses.

In the **Reopen closed matching incidents** section, you can configure Azure Sentinel Analytics to open a previously closed incident again if another alert is generated that also belongs to the previously closed incident.

Automated response

You can use the **Automated Response** section to select a playbook to run automatically when the alert is generated. Only the playbooks that contain Logic App Azure Sentinel connector are displayed.

For more information on how to create a playbook and run the automated activity on an incident creation, see the "Threat response with Azure Sentinel Playbooks" module.

Review and create

You can use the **Review and create** section to review the settings you have configured in the wizard before creating new rules.

Manage analytics rules

You can connect several data sources to Azure Sentinel, which can rapidly generate many security alerts.

To adjust the noise and filter the more important threats detected, you should manage the analytics rules on an ongoing basis. This will help ensure that your rules remain useful and efficient in detecting potential security threats.

You can perform the following four actions on existing active rules:

- Edit
- Disable
- Duplicate
- Delete

Edit rules

You can modify existing rules by selecting **Edit** in the details pane. To edit a rule, you navigate the same pages that you did in creating the rule. The previous inputs that you used to create the rule are preserved. You can change any properties of the rule to further tune the result of the threat detection.

A typical modification that you might want to implement is to attach an automated response to an already detected threat. To do this, on the **Automated Response** page, you can select one of the existing playbooks that defines the automated activity that will run if the threat is detected.

For example, your analytics rule might be detecting an incident that has already been resolved, and you want to reduce further alerts if similar activity occurs. By attaching a playbook that contains automated activity, you can change the incident status or add comments when a similar incident is detected.

Analytics rule wizard - Edit existing rule

Azure VM Deletion

General Set rule logic Incident settings (Preview) **Automated response** Review and create

Select a playbook to be run automatically when your analytics rule generates an alert.

You only see playbooks in your selected subscriptions and for which you have permissions.

Selected playbook: Dismiss-AADRiskyUser

Name ↑	Trigger kind ↑↓	Status ↑↓
<input checked="" type="checkbox"/> A Dismiss-AADRiskyUser	Azure Sentinel Alert	Enabled
<input type="checkbox"/> A Get-GeoFromIpAndTagIncident	Azure Sentinel Alert	Enabled
<input type="checkbox"/> A Prompt-User	Azure Sentinel Alert	Enabled

Disable rules

You can disable a rule when you are performing an activity that can trigger the rule alert. Disabled rules retain their configuration, and you can enable them again at a later time.

Duplicate rules

When you duplicate a rule, the rule contains all the configuration provided from the original rule. You can further modify the configuration based on your requirements. Don't forget to change the name of the duplicated rule because by default, the duplicate rule has the same name as the original rule with the string **Copy** appended to it.

Delete rules

Deleting the rule prompts you for confirmation before Azure Sentinel Analytics removes it from the set of active rules. For example, you can delete a rule about a service or a resource that isn't in use, which eliminates the need for the rule. Be aware that deleting a rule is permanent, and there isn't an undo feature. Therefore, we recommend you first disable the rule for a period of time until you're sure you don't need it.

Learn more

You can learn more by reviewing the following documents.

Getting started

- [Azure Sentinel documentation³](#)
- [Quickstart: On-board Azure Sentinel⁴](#)
- [Azure Sentinel pricing⁵](#)
- [Permissions in Azure Sentinel⁶](#)
- [Tutorial: Visualize and monitor your data⁷](#)

³ <https://docs.microsoft.com/azure/sentinel?azure-portal=true>

⁴ <https://docs.microsoft.com/azure/sentinel/quickstart-onboard?azure-portal=true>

⁵ <https://azure.microsoft.com/pricing/details/azure-sentinel?azure-portal=true>

⁶ <https://docs.microsoft.com/azure/sentinel/roles?azure-portal=true>

⁷ <https://docs.microsoft.com/azure/sentinel/tutorial-monitor-your-data?azure-portal=true>

- **Quickstart: Get started with Azure Sentinel⁸**
- **What is Azure Lighthouse?⁹**
- **Extend Azure Sentinel across workspaces and tenants¹⁰**
- **What is Azure Resource Manager?¹¹**
- **Azure Foundation 4-Week Implementation¹²**

Azure Sentinel agent

- **Tutorial: Detect threats out-of-the-box¹³**
- **Connect data sources¹⁴**

⁸ <https://docs.microsoft.com/azure/sentinel/quickstart-get-visibility?azure-portal=true>

⁹ <https://docs.microsoft.com/azure/lighthouse/overview?azure-portal=true>

¹⁰ <https://docs.microsoft.com/azure/sentinel/extend-sentinel-across-workspaces-tenants#cross-workspace-monitoring?azure-portal=true>

¹¹ <https://docs.microsoft.com/azure/azure-resource-manager/management/overview?azure-portal=true>

¹² <https://azuremarketplace.microsoft.com/marketplace/consulting-services/servent.servent-azure-foundation?azure-portal=true>

¹³ <https://docs.microsoft.com/azure/sentinel/tutorial-detect-threats-built-in?azure-portal=true>

¹⁴ <https://docs.microsoft.com/azure/sentinel/connect-data-sources?azure-portal=true>

Threat response with Azure Sentinel playbooks

Lesson Introduction

A Microsoft Azure Sentinel playbook is a collection of security procedures that you can run in response to alerts.

Contoso, Ltd. is a midsize financial services company in London with a New York branch office. Contoso uses several Microsoft products and services to implement data security and threat protection for its resources. These products are:

- Microsoft Office 365
- Azure Active Directory (Azure AD)
- Azure AD Identity Protection
- Cloud App Security
- Microsoft Defender for Identity
- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- System Center Endpoint Protection
- Microsoft Azure Information Protection

Contoso provides threat protection for its Azure-based and on-premises resources by using the paid version of Azure Security Center. The company also monitors and protects other non-Microsoft assets.

The Contoso Security Operations (SecOps) team didn't respond quickly enough to the organization's latest security incident. Contoso's IT director wants to implement Azure Sentinel playbooks to help the SecOps team identify and stop potential security threats. As Contoso's lead security engineer and Azure administrator, you've been tasked with setting up an Azure Sentinel playbook to respond to security incidents.

This module describes how to create Azure Sentinel playbooks to respond to security threats.

Learning objectives

After completing this lesson, you should be able to:

- Explain Azure Sentinel SOAR capabilities.
- Explore the Azure Sentinel Logic Apps connector.
- Create a playbook to automate an incident response.
- Run a playbook on demand in response to an incident.

Azure Sentinel playbooks explained

In addition to assessing and addressing problems with their security configuration, Contoso must also monitor for new problems and threats, and then respond appropriately.

Azure Sentinel as a SIEM and SOAR solution

Azure Sentinel is both a Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) solution that's designed for hybrid environments.

Note: SIEM solutions provide storage and analysis of logs, events, and alerts that other systems generate. You can configure these solutions to raise their own alerts. SOAR solutions support the remediation of vulnerabilities and the overall automation of security processes.

Azure Sentinel uses built-in and custom detections to alert you to potential security threats such as attempts to access Contoso's resources from outside its infrastructure or when data from Contoso appears to be sent to a known malicious IP address. You can also create incidents based on these alerts.

Azure Sentinel playbooks

You can create security playbooks in Azure Sentinel to respond to alerts. *Security playbooks* are collections of procedures based on Azure Logic Apps that run in response to an alert. You can run these security playbooks manually in response to your investigation of an incident or you can configure an alert to run a playbook automatically.

With the ability to respond to incidents automatically, you can automate some of your security operations and make your Service Organization Controls (SOC) more productive.

For example, to address Contoso's concerns, you can develop a workflow with defined steps that can block a suspicious username from accessing resources from a non-secure IP address. Alternatively, you can configure the playbook to perform a simple operation such as notifying the SecOps team about a high-level security alert.

Azure Logic Apps

Azure Logic Apps is a cloud service that automates the operation of your business processes. You use a graphical design tool called the *Logic Apps Designer* to arrange prebuilt components into the sequence you need. You can also use the code view and write your automated process in the JSON file.

Logic Apps Connector

Logic apps use connectors to connect to hundreds of services. A *connector* is a component that provides an interface to an external service.

Note: An Azure Sentinel data connector and a Logic Apps connector are not the same thing. An Azure Sentinel data connector connects Azure Sentinel with Microsoft security products and security ecosystems for non-Microsoft solutions. A Logic Apps connector is a component that provides an API connection for an external service and allows integration of events, data, and actions across other apps, services, systems, protocols, and platforms.

What are triggers and actions

Azure Logic Apps use triggers and actions, which are defined as follows:

- A *trigger* is an event that occurs when a specific set of conditions is satisfied. Triggers activate automatically when conditions are met. For example, a security incident occurs in Azure Sentinel, which is a trigger for an automated action.
- An *action* is an operation that performs a task in the Logic Apps workflow. Actions run when a trigger activates, another action completes, or a condition is met.

Azure Sentinel Logic Apps connector

An Azure Sentinel playbook uses an Azure Sentinel Logic Apps connector. It provides the triggers and actions that can start the playbook and perform defined actions.

Currently, there are two triggers from Azure Sentinel Logic Apps connector:

- When a response to an Azure Sentinel alert is triggered
- When Azure Sentinel incident creation rule is triggered

Note: Because Azure Sentinel Logic App connector is in preview, the features described in this module might change in the future.

The following table lists all the current actions for the Azure Sentinel connector.

Name	Description
Add comment to incident	Adds comments to the selected incident.
Add labels to incident	Adds labels to the selected incident.
Alert - Get incident	Returns the incident associated with the selected alert.
Change incident description	Changes the description for the selected incident.
Change incident severity	Changes the severity for the selected incident.
Change incident status	Changes the status for the selected incident.
Change incident title (V2)	Changes the title for the selected incident.
Entities - Get Accounts	Returns a list of accounts associated with the alert.
Entities - Get FileHashes	Returns a list of File Hashes associated with the alert.
Entities - Get Hosts	Returns a list of hosts associated with the alert.
Entities - Get IPs	Returns a list of IPs associated with the alert.
Entities - Get URLs	Returns a list of URLs associated with the alert.
Remove labels from incident	Removes the labels for the selected incident.

Note: Actions that have **(V2)** or a higher number provide a new version of the action and might differ from the old functionality of the action.

Some actions require integration with actions from another connectors. For example, if Contoso wants to identify all suspicious accounts returned in the alert from the defined entities, you must combine the **Entities - Get Accounts** action with the **For Each** action. Similarly, to get all individual hosts in an incident that detect suspicious hosts, you must combine the **Entities - Get Hosts** action with the **For Each** action.

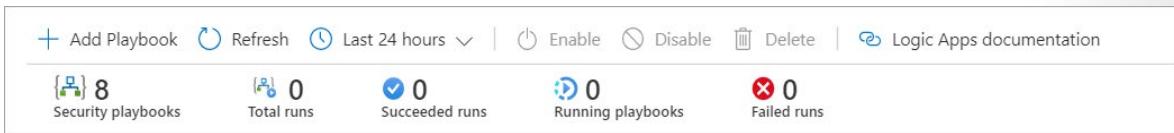
Create a Logic App

You can configure Azure Sentinel playbooks at Contoso to respond to security threats.

Explore the Playbooks page

You can automate responses to threats on the **Playbooks** page. On this page, you can observe all the playbooks that are created from Azure Logic Apps. The column **Trigger kind** presents what type of connectors are used in the logic app.

You can use the header bar, as displayed in the following diagram, to create new playbooks or to enable or disable existing playbooks.



The header bar provides the following options:

- Use the **Add Playbook** option to create a new playbook.
- Use the **Refresh** option to refresh the display, for example, after you create a new playbook.
- Use the drop-down time field to filter the status of the running of the playbooks.
- The **Enable**, **Disable**, and **Delete** option are only available if you select one or more logic apps.
- Use the **Logic Apps documentation** option to review links to official Microsoft documentation for more information on logic apps.

Contoso wants to use automated actions to prevent suspicious users from accessing their network. As their security administrator, you can create a playbook to implement this action. To create a new playbook, select **Add Playbook**. You will be directed to the page where you should create a new logic app by providing inputs for the following settings:

- **Subscription**. Select the subscription that contains Azure Sentinel.
- **Resource Group**. You can use an existing resource group or create a new one.
- **Logic App name**. Provide a descriptive name for the logic app.
- **Location**. Select the same location as where your Log Analytics workspace is located.
- **Log Analytics**. If you enable Log Analytics, you can get information about playbook's runtime events.

After providing these inputs, select the **Review + Create** option, and then select **Create**.

Logic Apps Designer

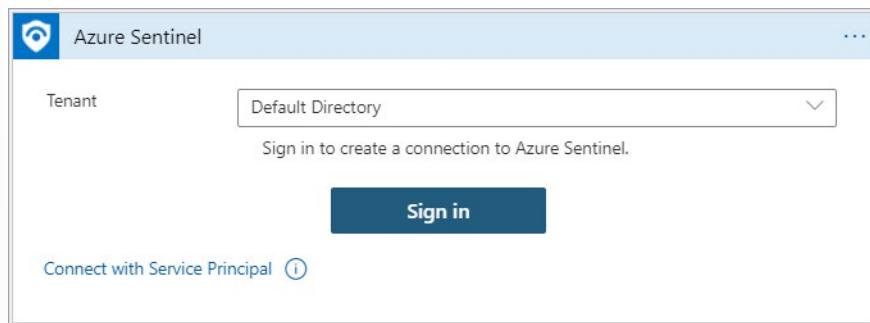
Azure Sentinel creates the logic app, and then you are directed to the **Logic App Designer** page.

The Logic App Designer provides a design canvas that you use to add a trigger and actions to your workflow. For example, you can configure the trigger to originate from the Azure Sentinel Connector when a new security incident is created. The Logic App Designer page provides many predefined templates that you can use. However, to create a playbook, you should start with the **Blank Logic App** template to design the logic app from scratch.

The automated activity in the playbook is initiated by the Azure Sentinel trigger. You can search for the Azure Sentinel trigger in the search box of the design canvas, and then select one of the following two available triggers:

- When a response to an Azure Sentinel alert is triggered
- When Azure Sentinel incident creation rule was triggered

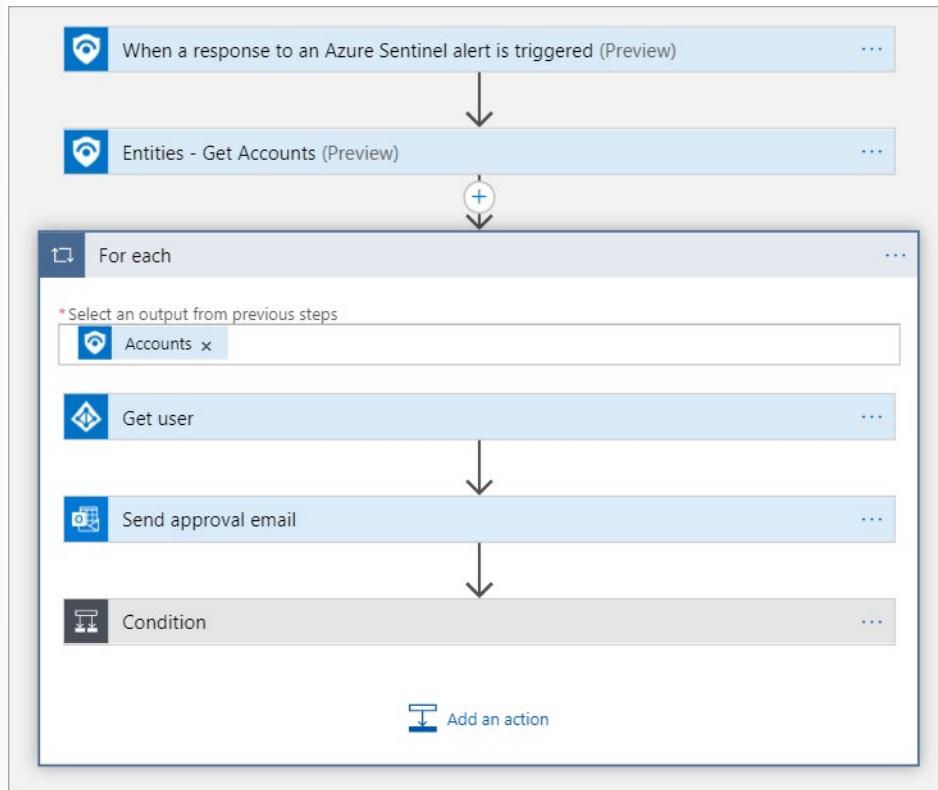
Opening Azure Sentinel Connector for the first time prompts you to **Sign in** to your tenant either with a user account from Azure Active Directory (Azure AD) or with Service Principal. This establishes an API connection to your Azure AD. The API connections store variables and tokens that are required to access the API for the connection, such as Azure AD, Office 365, or similar.



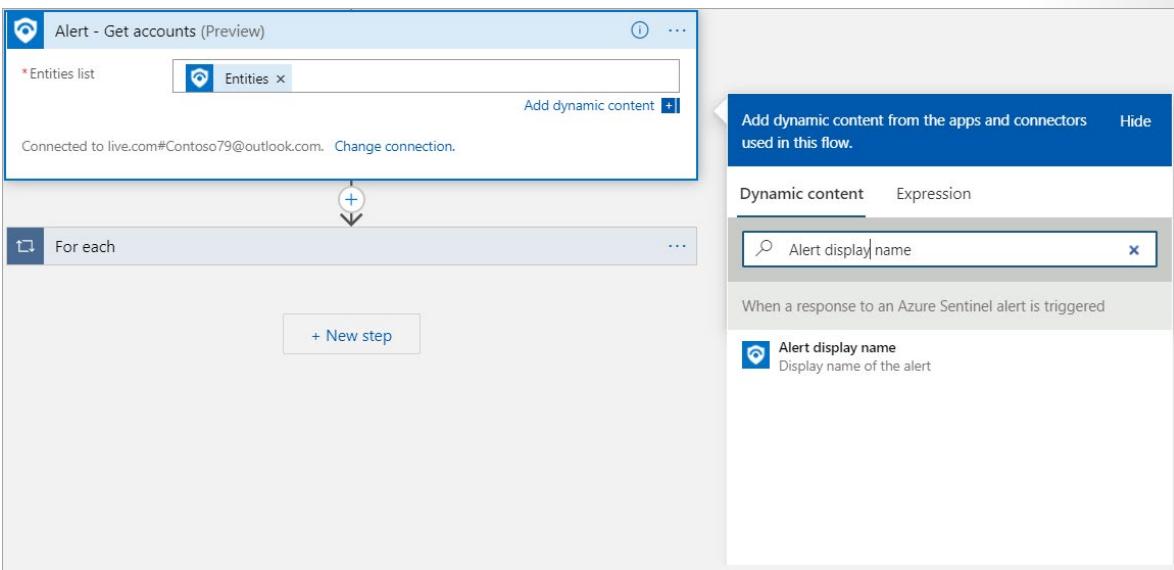
Each playbook starts with a trigger followed by actions that define the automated response on a security incident. You can combine actions from an Azure Sentinel connector with other actions from other Logic Apps connectors.

For example, you can add the trigger from an Azure Sentinel connector when an incident is triggered, follow it with an action that identifies the entities from the Azure Sentinel alert, and then another action that sends an email to an Office 365 email account. Azure Sentinel creates every action as a **New Step** and defines the activity that you are adding in the logic app.

The following screenshot displays the incident triggered by Azure Sentinel connector, which detects a suspicious account and sends an email to the administrator.

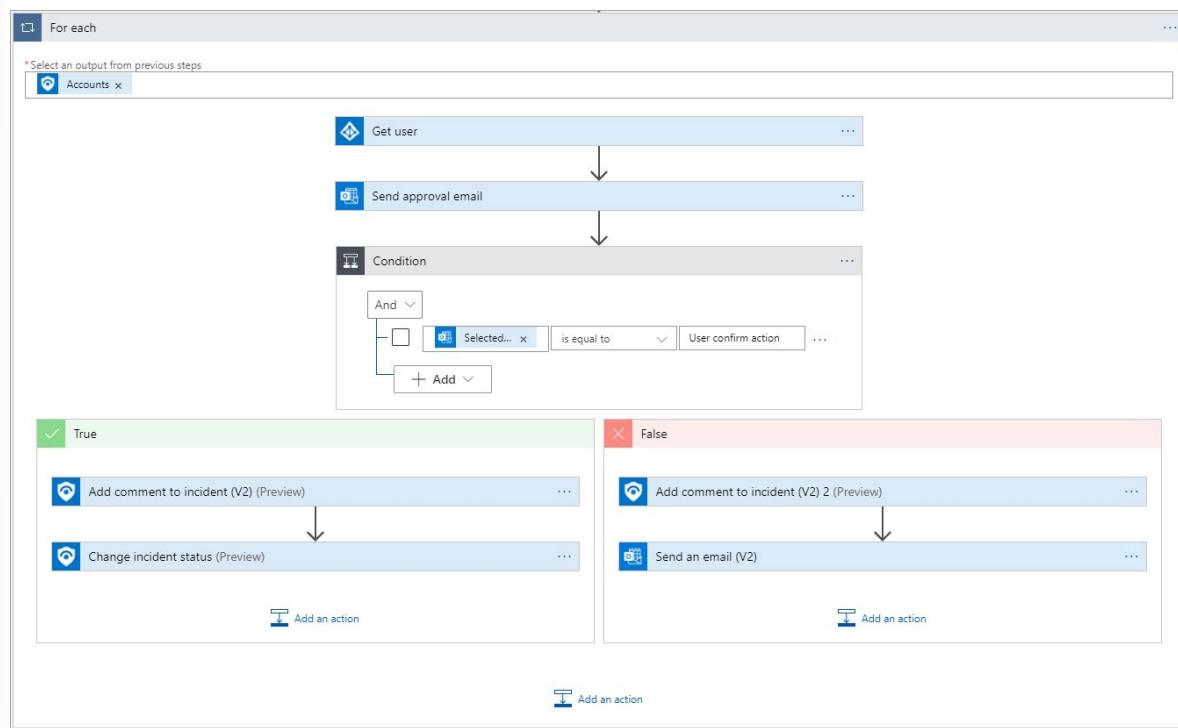


Each step in the workflow design has different fields that you must fill. For example, the **Entities - Get Accounts** action requires you to provide the list of entities from an Azure Sentinel alert. An advantage of using Azure Logic Apps is that you can provide this input from the **Dynamic content** list, which is populated with the outputs of the previous step. For example, the Azure Sentinel connector trigger **When a response to Azure Sentinel Alert is triggered** provides dynamic properties such as **Entities**, **Alert Display name**, which you can use to fill the inputs.



You can also add a control actions group that lets your logic app make decisions. The control actions group can include logical conditions, switch case conditions, or loops.

A **condition** action is an **if** statement that lets your app perform different actions based on the data you're processing. It consists of a Boolean expression and two actions. At runtime, the execution engine evaluates the expression and chooses an action based on whether the expression is true or false. For example, Contoso receives a large volume of alerts, many of them with recurring patterns, which cannot be processed or investigated. Using real-time automation, the Contoso SecOps teams can significantly reduce their workload by fully automating the routine responses to recurring types of alerts. The following screenshot presents a similar situation, where based on the user input, the playbook can change the status of the alert. The control action intercepts the user input, and if the expression evaluates to be a true statement, the playbook changes the status of the alert. In case the control action evaluates the expression to be false, the playbook can run other activities, such as sending an email as depicted in the following screenshot.



After you provide all the steps in the Logic Apps Designer, save the logic app to create a playbook in Azure Sentinel.

The Logic Apps page in Azure Sentinel

The playbooks you create appear on the **Playbooks** page, and you can further edit them. From the **Playbooks** page, you can select an existing playbook and that will open the Logic Apps page for that playbook in Azure Sentinel.

You can run several actions on the playbook from the Logic Apps header bar:

- **Run Trigger.** Use to run the logic app to test the playbook.
- **Refresh.** Use to refresh the status of the logic app to retrieve the status of the activity.
- **Edit.** Use to further edit the playbook in the **Logic Apps Designer** page.
- **Delete.** Use to delete the logic app if you do not need it.
- **Disable.** Use to temporarily disable the logic app to prevent the action from being performed even if the trigger is activated.
- **Update Schema.** Use to update the schema of the logic app after a significant change in the logic.
- **Clone.** Use to make a copy of the existing logic app, and then use that as a basis for further modification.
- **Export.** Use to export the logic app to Microsoft Power Automate and Microsoft Power Apps.

The **Essentials** section displays descriptive information about the logic app. For example, the logic app definition displays the number of triggers and actions that the logic app provides.

You can use the **Summary** section, to review summarized information about the logic app. From this section, you can select the logic app link to open it in the Logic Apps Designer or review the trigger history.

The **Runs history** section displays the previous runs of the logic app and whether they succeeded or failed.

Automate response to an incident in Azure Sentinel

As a final step, you need to attach this playbook to an analytics rule to automate responses to an incident. You can use the **Automated Response** section in the analytics rule to select a playbook to run automatically when the alert is generated. For more information on how to create analytics rule, see the "Threat detection with Azure Sentinel analytics" module.

Run a playbook on demand

Some incidents at Contoso might require further investigation before you run a playbook. Azure Sentinel allows you to run playbooks on demand to facilitate in-depth investigations.

You can configure playbooks to run on demand based on incident details, to trigger specific steps as part of the investigation, or to conduct some remediation action.

Consider the scenario where suspicious users are prevented from accessing corporate resources. As the security administrator at Contoso, you find one false positive incident. Some users at Contoso were accessing resources over a virtual private network connection from remote computers while being connected to the office computers at the same time. Microsoft Cloud Security received signals and based on the vulnerability that detects potential threat from atypical travel locations, it tagged the users as medium risk.

You can use a playbook that can automatically dismiss this risky user property in Azure AD.

Azure Sentinel repository on GitHub

Azure Sentinel repository on GitHub¹⁵ contains ready-to-use playbooks to help you automate responses on incidents. These playbooks are defined with Azure Resource Manager (ARM template) that use Logic App Azure Sentinel triggers.

For the scenario described earlier, you can use the **Dismiss-AADRiskyUser** playbook, which is located in the Azure Sentinel repository on GitHub, and deploy it directly in your Azure subscription.

For each deployment from GitHub, you first must authorize each connection in the playbook before you edit them in Logic Apps Designer. Authorization will create an API connection to the appropriate connector and store the token and variables. You can locate the API connection in the resource group where you created the logic app.

The name of each API connection is appended with the **azuresentinel** prefix. You can also edit the connection in the Logic Apps Designer when you edit the logic app.

¹⁵ <https://github.com/Azure/Azure-Sentinel>

The screenshot shows the 'Edit API connection' page for 'azuresentinel-Dismiss-AADRiskyUser'. The left sidebar lists various settings like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Locks, General, Properties, Edit API connection selected), Monitoring (Alerts, Tasks, Export template), and Support + troubleshooting (New support request). The main panel has a heading 'Edit API connection' with a sub-instruction 'Edit API connection lets you update the display name and refresh the authorization for this SaaS provider.' It shows the 'API' section set to 'Azure Sentinel'. Under 'Display Name', there is a placeholder '<username>@<domain>'. Below it is an 'Authorize' button. At the bottom are 'Save' and 'Discard' buttons.

Attach a playbook to an existing incident

After your playbook is ready, you can open the **Incident** page in Azure Sentinel, and then select the existing incident. In the details pane, you can select **View full details** to explore the properties of the incident. From the **Alerts panel**, you can select **View playbooks**, and then you can run one of the existing playbooks.

The following screenshot depicts the suspicious user activity example for which you can attach the **Dismiss-AADRiskyUser** playbook.

The screenshot shows the Azure Security Center Incident view for Incident ID 5. The main pane displays a summary of a "Suspicious authentication activity" incident. Key details include:

- Owner:** Unassigned
- Status:** New
- Severity:** Medium

The "Description" section states: "Although none of them succeeded, some of them used accounts were recognized by the host. This resembles a dictionary attack, in which an attacker performs numerous authentication attempts using a dictionary of predefined account names and passwords in order to find valid credentials to access the host. This indicates that some of your host account names might exist in a well-known account name dictionary."

The "Evidence" section shows:

- Events: N/A (1)
- Alerts: 1
- Bookmarks: 0

Timestamps: Last update time is 11/05/20, 02:12 PM; Creation time is 11/05/20, 02:12 PM.

Associated entities: vm1 (1). Associated tactics: PreAttack (1).

Links: "View full details >" and "Incident workbook".

Analytic rule links: "Create incidents based on Azure Security Center alerts" (2).

Tags: None.

A prominent blue "Investigate" button is at the bottom left.

The right sidebar contains a navigation bar with "Alerts" selected, followed by "Bookmarks", "Entities", and "Comments". A search bar and a table titled "Suspicious authentication activity" are also present.

Severity ↑↓	ALERT NAME ↑↓	Alert status ↑↓
Medium	Suspicious authenticatio...	New

After you have investigated the incident, you can choose to run the playbook manually to respond to a security threat.

Security incident management in Azure Sentinel

Lesson Introduction

Learn how Azure Sentinel gives you the ability to identify anomalies in your Azure environment and helps you manage incidents.

You're a security engineer for Contoso, Ltd. It's a midsize financial services company in London with a New York branch office. Contoso uses Microsoft 365, Azure Active Directory (Azure AD), Azure AD Identity Protection, Microsoft Cloud App Security, Microsoft Defender for Identity, Microsoft Defender for Endpoint, Microsoft Defender for Office 365, Intune Endpoint Protection, and Microsoft Azure Information Protection.

Contoso uses Azure Security Center with Azure Defender as threat protection for resources that run on Azure and on-premises. The company also monitors and protects other non-Microsoft assets.

Recently, you've been asked to investigate and identify anomalies in the company's Azure Activity log. You learn that Azure Sentinel is a cloud application that can assist you.

In this module, you'll investigate Azure Sentinel incident management, learn about Azure Sentinel events and entities, and discover ways to resolve incidents.

Learning objectives

After completing this lesson, you should be able to:

- Understand Azure Sentinel incident management
- Explore Azure Sentinel evidence and entity management
- Investigate and manage incident resolution

Describe incident management

Like any business, Contoso faces technology-related threats to its organization. Azure Sentinel can help Contoso's IT team organize, investigate, and track these threats from creation to resolution. The threats are called *incidents*.

Key concepts

Before you begin managing incidents, it's important to understand the following key incident management concepts in Azure Sentinel:

- **Data connectors.** You use data connectors in Azure Sentinel to ingest and collect data from security-related services. These events are forwarded to a Log Analytics workspace associated with Azure Sentinel. Events can be collected from Linux or Windows computers running the Log Analytics agent, from a Linux syslog server (for devices like firewalls or proxies), or directly from Microsoft Azure services.
- **Events.** Azure Sentinel stores events in a Log Analytics workspace. These events contain the details of security-related activity that you want to monitor with Azure Sentinel.

- **Analytic rules.** You create analytics rules to detect important security events and generate alerts. You can create analytics rules by using built-in templates or by using custom Kusto Query Language (KQL) queries against Log Analytics workspaces in Sentinel.
- **Alerts.** Analytics rules generate alerts when they detect important security events. You can also configure alerts to generate incidents.
- **Incidents.** Azure Sentinel creates incidents from analytics rule alerts. Incidents can contain multiple related alerts. You use each incident as a starting point and tracking mechanism for investigation into security concerns in your environment.

Incident management in Azure Sentinel

Incident management is the complete process of incident investigation, from creation, to in-depth investigation, and finally to resolution. Azure Sentinel provides a complete incident management environment in which you can perform these steps. You can use Sentinel to review detailed incident information, assign an incident owner, set and maintain incident severity, and manage incident status.

Overview page

Incident management in Azure Sentinel begins on the overview page, where you can review the current Azure Sentinel environment.



The overview page contains a list of the most recent incidents, along with other important Azure Sentinel information. Use this page to understand the general security situation before investigating incidents.

Choose the best response for each of the following questions. Then select **Check your answers**.

Explain evidence and entities

Azure Sentinel uses various sources of security information to create incidents. As lead system engineer at Contoso, you'll need to understand these sources to best utilize incident management in Azure Sentinel.

Incident evidence

Incident evidence consists of the security event information and related Azure Sentinel assets that identify threats in the Azure Sentinel environment. Evidence displays how a threat has been identified in

Azure Sentinel. It links you back to the specific resources that you can use to increase your awareness of incident details.

Events

Events link you back to one or more events from the Log Analytics workspaces associated with Azure Sentinel. On their own, these workspaces typically contain thousands of events that are too numerous to manually parse. If a query attached to an Azure Sentinel analytics rule returns events, these events are attached to the generated incident for potential further review. You can use events to understand the scope and frequency of the incident before investigating further.

Alerts

Most incidents are generated because of an analytics rule alert. Examples of alerts include:

- Detection of suspicious files.
- Detection of suspicious user activities.
- Attempted elevation of privilege.

Analytics rules generate alerts, based on either KQL queries or direct connection to Microsoft Security solutions such as Azure Security Center or Microsoft Defender 365. If you enable alert grouping, Azure Sentinel includes any related alert evidence for the incident.

Bookmarks

While investigating an incident, you might identify events that you want to track or mark for later investigation. You can preserve the queries run in Log Analytics by choosing one or more events and designating them as bookmarks. You can also record notes and tags to better inform later threat-hunting processes. Bookmarks are available to you and your teammates.

Incident entities

An *entity* refers to a network or user resource involved with an event. You can use entities as entry points to explore all alerts and correlations associated with that entity.

Entity relationships are useful when you're investigating incidents. Instead of analyzing the identity alerts, network alerts, and data access alerts individually, you can use entities to observe any alerts associated with a particular user, host, or address in your environment.

Some of the entity types include:

- Account
- Host
- IP
- URL
- FileHash

For instance, entities would help you identify all of the alerts associated with a specific user at Contoso, the user's host machine, and other hosts that the user has connected to. You can determine which IP addresses are associated with the user in question, exposing which events and alerts could be part of the same attack.

Choose the best response for each of the following questions. Then select **Check your answers**.

Investigate incidents

After you start using Azure Sentinel to generate incidents, you and the IT team at Contoso will want to investigate those incidents. You can use the advanced investigation and analysis tools to gather information and determine remediation steps.

To identify and resolve security issues at Contoso, you'll first want to investigate any incidents. The **Overview** page in Azure Sentinel provides a list of the most recent incidents for quick reference. For more details and a complete overview of the incidents at Contoso, you'll use the **Incidents** page, which displays all incidents in the current workspace and details about those incidents.

The screenshot shows the Azure Sentinel Incidents page. At the top, there are three summary counts: Open Incidents (1), New Incidents (1), and Active Incidents (0). Below these are filters for Severity (All), Status (New, Active), Product name (All), and Owner (All). A checkbox for 'Auto-refresh incidents' is checked. The main area is a table with columns: Incident ID, Title, Alerts, Product names, Created time, Last update time, and Owner. One incident is listed:

Incident ID	Title	Alerts	Product names	Created time	Last update time	Owner
1	Deleted VMs	2	Azure Sentinel	11/11/20, 12:21 AM	11/11/20, 12:26 AM	Unassigned

On the right side, there's a circular icon with a plus sign and a brief message: "No incidents selected. Select an incident to view more details". At the bottom, there are navigation links: < Previous, 1 - 1, and Next >.

From this page, you can take various steps to investigate incidents.

Important: Azure Active Directory users who investigate incidents must be members of the Directory Reader role.

Review incidents

The **Incidents** page provides a complete list of incidents in Azure Sentinel. It also provides basic incident information, including severity, ID, title, alerts, product names, created time, last update time, owner, and status. You can sort by any incident column and filter the incident list by name, severity, status, product name, or owner.

Selecting any incident will display more information about the incident in the **Details** column. This information can help you clarify the nature, context, and course of action for an incident.

Examine incident details

The **Incident details** page provides a description of the incident and lists the evidence, entities, and tactics related to the incident. It also contains links to associated workbooks and the analytic rule that generated the incident.

The screenshot shows the Azure Sentinel interface for an incident titled "Deleted VMs" with Incident Id: 1. At the top, there are dropdown menus for "Owner" (Unassigned), "Status" (New), and "Severity" (Medium). Below this, the "Description" field contains the query "Query for VMs deleted in Microsoft Azure". The "Provider" is listed as "Azure Sentinel". Under "Evidence", there are three counts: 2 Events, 2 Alerts, and 0 Bookmarks. The "Last update time" is 11/11/20, 12:26 AM, and the "Creation time" is 11/11/20, 12:21 AM. The "Entities" section lists two users: admin@contoso.com and the IP address 204.83.34.106, along with a link to "View full details >". The "Tactics" section shows one entry: "Initial Access". Under "Incident workbook", there is a link to "Incident Auditing and Metrics". At the bottom, there are two buttons: "Investigate" (blue) and "View full details" (white).

You can reference all these details to better understand the context of the incident. For example, in a brute force attack incident, you might go to the Log Analytics query for the alert to determine the number of attacks made.

Manage incident ownership, status, and severity

Each incident created in Azure Sentinel has manageable metadata attached to it. This information can help you:

- Set and track the status of an incident from creation to resolution.
- Set and review severity.
- Assign and track ownership for the incident.

This screenshot is identical to the one above, showing the "Deleted VMs" incident details. It highlights the "Owner" dropdown menu, which is currently set to "Unassigned".

Ownership

In a typical environment, each incident should be assigned an owner from your security team. The incident owner is responsible for overall management of the incident, including investigation and status

updates. You can change ownership at any time to assign the incident to another security team member for further investigation or escalation.

Status

Every new incident that's created in Azure Sentinel is assigned a status of **New**. As you review and respond to incidents at Contoso, you'll manually change the status to reflect the current state of the incident. For incidents under investigation, set the status to **Active**. When an incident is fully resolved, set the status to **Closed**.

When you set the status to **Closed**, you'll be prompted to choose one of the following from a drop-down list:

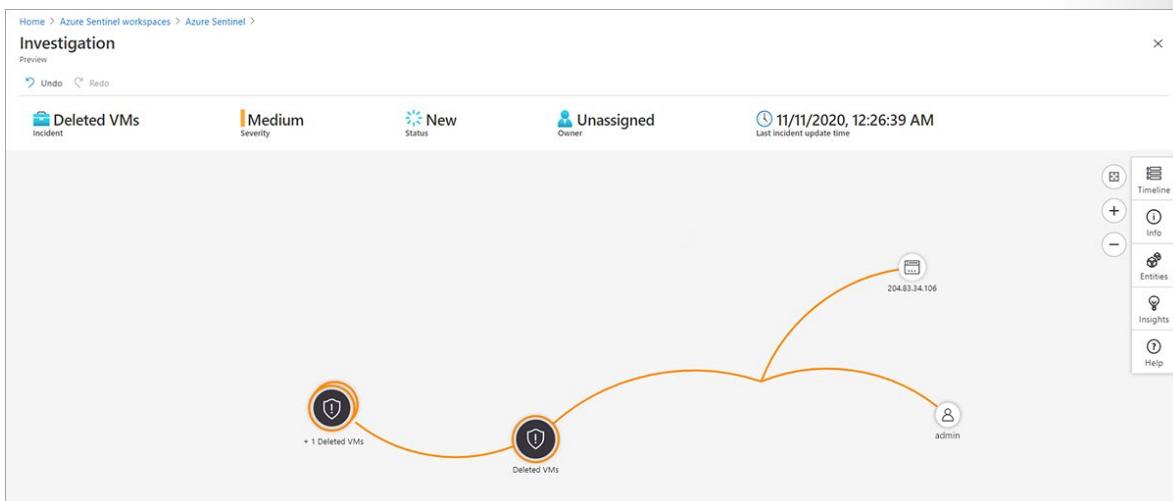
- **True Positive**: suspicious activity
- **Benign Positive**: suspicious but expected
- **False Positive**: incorrect alert logic
- **False Negative**: incorrect data
- **Undetermined**

Severity

Incident severity is set by the rule or Microsoft security source from which the incident is generated. In most cases, incident severity remains unchanged. But you might manually set the severity if you decide that the incident is more or less severe than initially classified. Severity options include **Informational**, **Low**, **Medium**, and **High**.

Perform deep analysis with an investigation graph

You can further investigate an incident by selecting **Investigate** on the **Incident details** page. This action opens the investigation graph, a visual tool that helps to identify entities involved in the attack and the relationships between those entities. If the incident involves multiple alerts over time, you can also review the alert timeline and correlations between alerts.



Review entity details

You can select each entity on the graph to observe more information about the entity. This information includes relationships to other entities, account usage, and data flow information. For each information area, you can go to the related events in Log Analytics and add the related alert data into the graph.

Review incident details

You can select the incident item on the graph to observe important incident metadata related to the incident's security and environment context.

Choose the best response for each of the following questions. Then select **Check your answers**.

Use entity behavior analytics in Azure Sentinel

Lesson Introduction

As Azure Sentinel collects logs and alerts from all of its connected data sources, it builds baseline behavioral profiles of your organization's entities, including users, hosts, IP addresses, and domains.

You are a Security Operations Analyst working at a company that implemented Azure Sentinel. The threat hunting team has raised concerns about a specific user account based on discovered threat indicators and needs to see a profile containing historical and related entity data quickly.

As Azure Sentinel collects logs and alerts from all of its connected data sources, it analyzes them. It builds baseline behavioral profiles of your organization's entities (users, hosts, IP addresses, applications, etc.). You have the threat hunting team member navigate to the Entity behavior page to perform further analysis on the account.

Learn how to use entity behavior analytics in Azure Sentinel to identify threats inside your organization.

Learning objectives

After completing this lesson, you should be able to:

- Explain User and Entity Behavior Analytics in Azure Sentinel
- Explore entities in Azure Sentinel

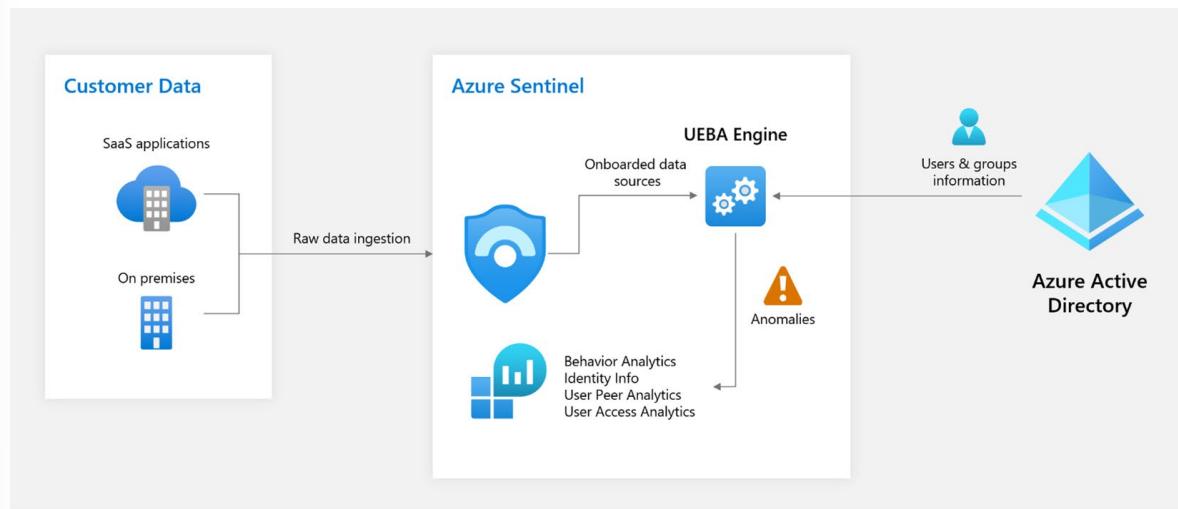
User and entity behavior analytics explained

Identifying threats inside your organization and their potential impact - whether a compromised entity or a malicious insider - has always been a time-consuming and labor-intensive process. Sifting through alerts, connecting the dots, and active hunting all add up to massive amounts of time and effort expended with minimal returns and the possibility of sophisticated threats evading discovery. Elusive threats like zero-day, targeted, and advanced persistent threats can be the most dangerous to your organization, making their detection all the more critical.

The UEBA capability in Azure Sentinel eliminates the drudgery from your analysts' workloads and the uncertainty from their efforts, and delivers high-fidelity, actionable intelligence, so they can focus on investigation and remediation.

As Azure Sentinel collects logs and alerts from all of its connected data sources, it analyzes them and builds baseline behavioral profiles of your organization's entities (users, hosts, IP addresses, applications etc.) across time and peer group horizon. Using various techniques and machine learning capabilities, Sentinel can then identify anomalous activity and help you determine if an asset has been compromised. Not only that, but it can also figure out the relative sensitivity of particular assets, identify peer groups of assets, and evaluate the potential impact of any given compromised asset (its "blast radius"). Armed with this information, you can effectively prioritize your investigation and incident handling.

Architecture overview



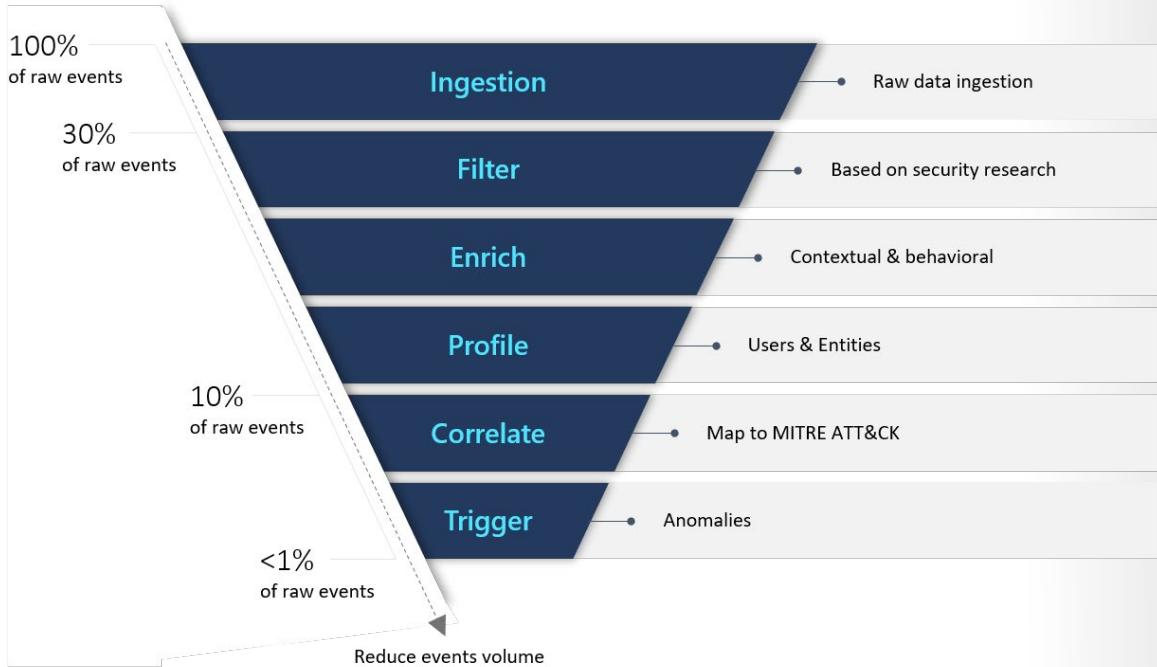
Security-driven analytics

Inspired by Gartner's paradigm for UEBA solutions, Azure Sentinel provides an "outside-in" approach, based on three frames of reference:

Use cases: By prioritizing relevant attack vectors and scenarios based on security research aligned with the MITRE ATT&CK framework of tactics, techniques, and subtechniques that put various entities as victims, perpetrators, or pivot points in the kill chain; Azure Sentinel focuses specifically on the most valuable logs each data source can provide.

Data Sources: While first and foremost supporting Azure data sources, Azure Sentinel thoughtfully selects third-party data sources to provide data that matches our threat scenarios.

Analytics: Using various machine learning (ML) algorithms, Azure Sentinel identifies anomalous activities and presents evidence clearly and concisely in the form of contextual enrichments, some examples of which appear below.



Azure Sentinel presents artifacts that help your security analysts get a clear understanding of anomalous activities in context, and in comparison with the user's baseline profile. Actions performed by a user (or a host, or an address) are evaluated contextually, where a "true" outcome indicates an identified anomaly:

- across geographical locations, devices, and environments.
- across time and frequency horizons (compared to user's own history).
- as compared to peers' behavior.
- as compared to organization's behavior.

Context



Scoring

Each activity is scored with "Investigation Priority Score", which determines the probability of a specific user performing a specific activity based on behavioral learning of the user and their peers. Activities identified as the most abnormal receive the highest scores (on a scale of 0-10).

Explore entities

When alerts are sent to Azure Sentinel, they include data elements that Azure Sentinel identifies and classifies as entities, such as user accounts, hosts, IP addresses and others. On occasion, this identification can be a challenge, if the alert does not contain sufficient information about the entity.

For example, user accounts can be identified in more than one way: using an Azure AD account's numeric identifier (GUID), or its User Principal Name (UPN) value, or alternatively, using a combination of its username and its NT domain name. Different data sources can identify the same user in different ways. Therefore, whenever possible, Azure Sentinel merges those identifiers into a single entity, so that it can be properly identified.

It can happen, though, that one of your resource providers creates an alert in which an entity is not sufficiently identified - for example, a user name without the domain name context. In such a case, the user entity cannot be merged with other instances of the same user account, which would be identified as a separate entity, and those two entities would remain separate instead of unified.

In order to minimize the risk of this happening, you should verify that all of your alert providers properly identify the entities in the alerts they produce. Additionally, synchronizing user account entities with Azure Active Directory may create a unifying directory, which will be able to merge user account entities.

The following types of entities are currently identified in Azure Sentinel:

- User account (Account)
- Host
- IP address (IP)
- Malware
- File
- Process
- Cloud application (CloudApplication)
- Domain name (DNS)
- Azure resource
- File (FileHash)
- Registry key
- Registry value
- Security group
- URL
- IoT device
- Mailbox
- Mail cluster
- Mail message
- Submission mail

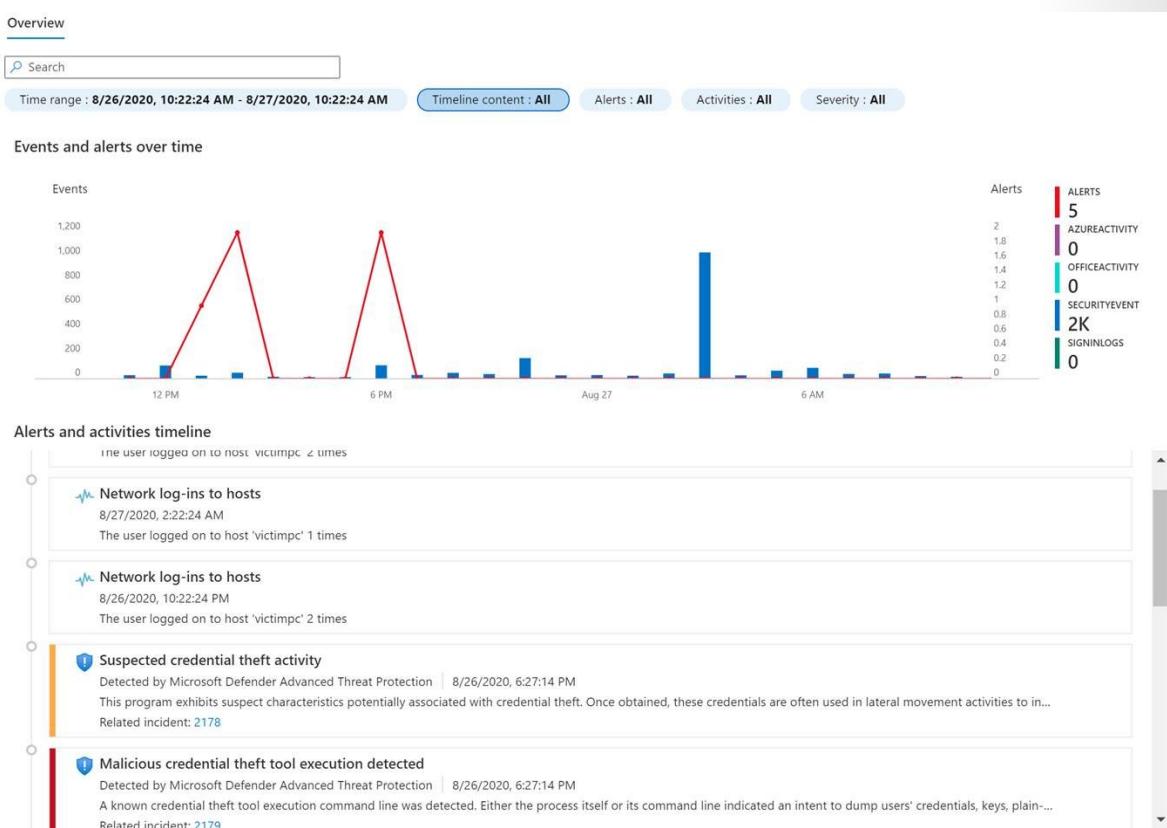
Entity pages

When you encounter any entity (currently limited to users and hosts) in a search, an alert, or an investigation, you can select the entity and be taken to an **entity page**, a datasheet full of useful information about that entity. The types of information you will find on this page include basic facts about the entity, a timeline of notable events related to this entity and insights about the entity's behavior.

Entity pages consist of three parts:

- The left-side panel contains the entity's identifying information, collected from data sources like Azure Active Directory, Azure Monitor, Azure Security Center, and Microsoft Defender.
- The center panel shows a graphical and textual timeline of notable events related to the entity, such as alerts, bookmarks, and activities. Activities are aggregations of notable events from Log Analytics. The queries that detect those activities are developed by Microsoft security research teams.
- The right-side panel presents behavioral insights on the entity. These insights help to quickly identify anomalies and security threats. The insights are developed by Microsoft security research teams, and are based on anomaly detection models.

The timeline



The timeline is a major part of the entity page's contribution to behavior analytics in Azure Sentinel. It presents a story about entity-related events, helping you understand the entity's activity within a specific time frame.

You can choose the **time range** from among several preset options (such as *last 24 hours*), or set it to any custom-defined time frame. Additionally, you can set filters that limit the information in the timeline to specific types of events or alerts.

The following types of items are included in the timeline:

Alerts - any alerts in which the entity is defined as a **mapped entity**. Note that if your organization has created **custom alerts using analytics rules¹⁶**, you should make sure that the rules' entity mapping is done properly.

Bookmarks - any bookmarks that include the specific entity shown on the page.

Activities - aggregation of notable events relating to the entity.

Entity Insights

Entity insights are queries defined by Microsoft security researchers to help your analysts investigate more efficiently and effectively. The insights are presented as part of the entity page, and provide valuable security information on hosts and users, in the form of tabular data and charts. Having the information here means you don't have to detour to Log Analytics. The insights include data regarding sign-ins, Group Additions, Anomalous Events and more, and include advanced ML algorithms to detect anomalous behavior. The insights are based on the following data types:

- Syslog
- SecurityEvent
- Audit Logs
- Sign-in Logs
- Office Activity
- BehaviorAnalytics (UEBA)

How to use entity pages

Entity pages are designed to be part of multiple usage scenarios, and can be accessed from incident management, the investigation graph, bookmarks, or directly from the entity search page under **Entity behavior analytics** in the Azure Sentinel main menu.



¹⁶ <https://docs.microsoft.com/azure/sentinel/tutorial-detect-threats-custom?azure-portal=true>

Display entity behavior information

The Entity behavior page allows you to search for entities or select from the list of already displayed entities. Once selected the Entity page is displayed with information and timeline of alerts and activities

The screenshot shows the Azure Sentinel Entity behavior page. On the left, there's a navigation sidebar with sections like General, Threat management, Configuration, and Entity behavior (which is currently selected). The main area features a central illustration of a brain with various icons (flask, key, shield) representing data sources and analysis. Below the illustration are two tables: 'Accounts by # of alerts' and 'Hosts by # of alerts'.
Accounts by # of alerts:

Account	# of alerts
Weidah	3
uuid	2
WIN2016ATP\Administrator	1
cgreen	1
damdemo	1

Hosts by # of alerts:

Host	# of alerts
linusserverapp1	2
win2016atp	1
attackerwin	1
test2019	1
/subscriptions/7cd395f1-4264...	1

The Incident Investigation Graph includes an option for **Insights**. Insights display information from the Entity behavior data.

Query, visualize, and monitor data in Azure Sentinel

Lesson Introduction

Microsoft Azure Sentinel Workbooks provide interactive reports that help you visualize important signals by combining text, table, charts, and tiles.

Contoso, Ltd. is a midsize financial services company in London with a New York branch office. Contoso uses several Microsoft products and services to implement data security and threat protection for its resources. These products are:

- Microsoft 365
- Azure Active Directory (Azure AD)
- Azure AD Identity Protection
- Cloud App Security
- Microsoft Defender for Identity
- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- System Center Endpoint Protection
- Microsoft Azure Information Protection

Contoso provides threat protection for its Azure-based and on-premises resources by using the paid version of Azure Defender. The company also monitors and protects other non-Microsoft assets. A recent incident with compromised identities led to exposed customer data. The Contoso Security Operations (SecOps) team wants to ensure that proper monitoring and reporting methods are in place. As Contoso's security administrator, you need to demonstrate the Azure Sentinel reporting and monitoring capabilities, and how they can alert your organization to potential security incidents.

This module describes how to query, visualize, and monitor data in Azure Sentinel.

Learning objectives

After completing this lesson, you should be able to:

- Visualize security data using Azure Sentinel Workbooks.
- Explain workbook queries.
- Explore workbook capabilities.
- Create an Azure Sentinel Workbook.

Azure Sentinel Workbooks

Azure Sentinel provides several templates that are ready for use. You can use these templates to create your own workbook and then modify them as needed for Contoso.

Most of the data connectors Azure Sentinel uses to ingest data come with their own workbooks. You can get better insight into the data that is being ingested by using tables and visualizations, including bar and

pie charts. You can also make your own workbooks from the beginning instead of using the predefined templates.

Workbook page

You can access the **Workbook** page from the Azure Sentinel from the navigation pane.

The **Workbook** page consists of the:

- Workbook header. You can add a new workbook and review the saved workbooks and templates that are available on the **Workbook** page.
- Templates section. You can access existing workbook templates on the **Templates** tab. You can save some of the workbooks for quick access and they will appear on the **My workbooks** tab.

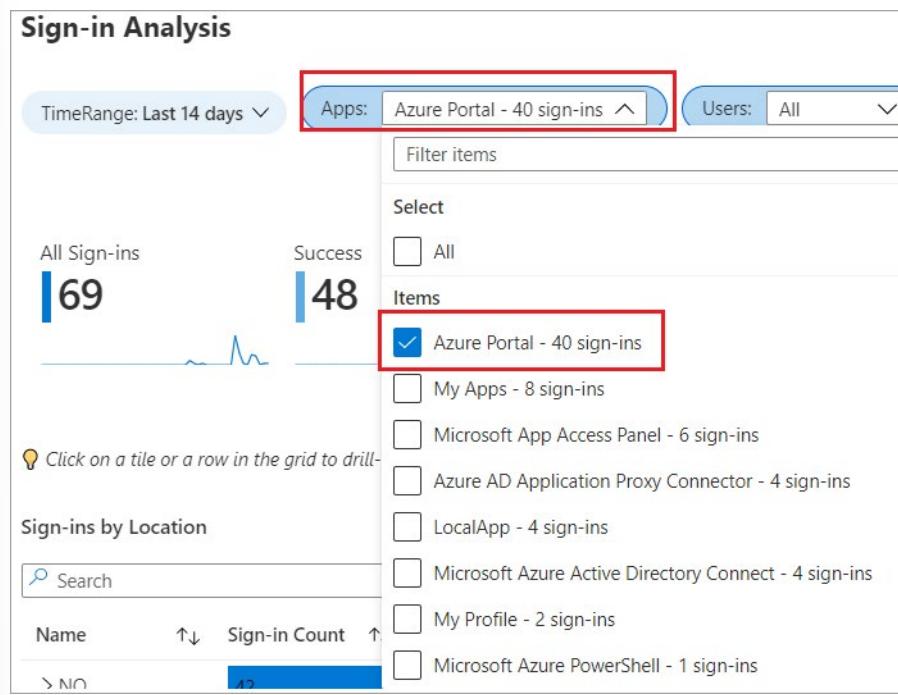
From the **Templates** page, you can select an existing workbook to display a details pane for it, which contains additional information for the templates. The details pane also contains information about the required data types and data connectors that must be connected to Azure Sentinel. You can also review how the report will display.

Review an existing workbook template

As mentioned earlier, Contoso is concerned about compromised identities. As the security administrator, you can examine the existing **Audit AD Sign-in logs** workbook by selecting the template in the template section, and then selecting **View template** in the details pane.

The **Azure AD Sign-in logs** workbook contains predefined charts, graphs, and tables that can provide important insight about the sign-in activity in Azure AD. You can find information about user sign-ins and locations, email addresses, and IP addresses of your users. In addition, you can also review information about failed activities and the errors that triggered the failures.

On the **Azure AD Sign-in logs** page, you can expand the time range or filter the apps and users that have sign-in privileges in the Azure AD. For example, Contoso wants to identify users that can sign-in to the Azure portal, so they can filter the data as displayed below.



Contoso is interested in identifying the failed sign-in attempts, so that they can display these accounts by selecting the information tiles, and then selecting a tile or a row to display more information such as:

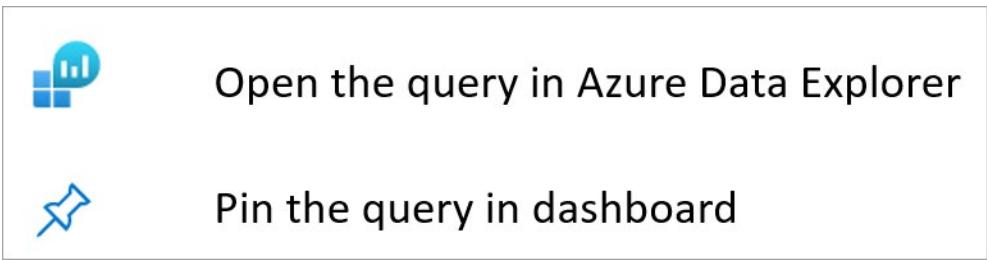
- **Sign-in Location.** This section indicates the location from which the user signed in to Azure AD.
- **Location Sign-in details.** This section displays the users, their sign-in status, and the time of the sign-in attempt.
- **Sign-ins by Device.** This section lists devices used by the users to sign-in Azure AD.
- **Device Sign-in details.** This section displays the users that signed in on a particular device and the time they signed in.

This information tile in the background is configured to run the query and filter the data collected from the Azure AD connector. Azure Sentinel then visualizes and presents the data collected with tables that are more meaningful and provide useful insight on user sign-in attempts.

The workbook contains additional tiles that indicate the users who signed in using conditional access. From the **Conditional access status** table, you can review users who required multifactor authentication (MFA) to validate their identity.

Conditional access status			
Name	Count	↑↓	Trend
Disabled	63		
Other	38		
Require MFA	25		

The rest of the page also contains tables and charts that are interactive, and by selecting some of the rows or tiles, you can filter the data that is presented. Some tables are created with links to corresponding logs as displayed in the following screenshot.



Note: You can also pin the query step in the private or shared dashboard for quick retrieval.

Edit the query from the workbook

For example, Contoso wants to search the logs for more information that presents the failed user sign-in and they are redirected to the Azure Data Explorer, where Azure Sentinel performs the log query to filter the information.

```

Logs
New Query 1*
Select scope
Run Time range: Custom Save Copy link + New alert rule Export Pin to dashboard Format query
Tables Queries Filter <>
Search Filter Group by: Solution
Filter
Favorites
CommonSecurityLog
Azure Monitor for VMs
Azure Sentinel
LogManagement
SecurityCenterFree
Custom Logs
Functions
1 SigninLogs
2 |where AppDisplayName in ('*') or '*' in ('*')
3 |where UserDisplayName in ('*') or '*' in ('*')
4 | extend ErrorCode = tostring(Status.errorCode)
5 | extend FailureReason = tostring(Status.failureReason)
6 | where ErrorCode in ("0","50053","50140","51006","50050","50091","50094","50055","50144","50072","50074","16000","16001","16003","50127","50125","50120","50143","81010","81014")
7 | summarize errCount = count() by ErrorCode, tostring(FailureReason)
8 | sort by errCount
9 |project [* Error Code] = ErrorCode, [*Reason]=FailureReason, [*Error Count] = toint(errCount)

```

Results Chart Columns Display time (UTC+00:00) Group columns

Completed. Showing results from the custom time range.

Error Code	Reason	Error Count
50126	Invalid username or password or Invalid on-premise username or password.	2

00:04:1 1 records

Explore saved workbooks

From the **Templates** page, you can save a workbook from existing templates by selecting one of the templates, and then selecting **Save**. You must provide a location to indicate where you want to save the workbook. This creates an Azure resource based on the template with template's JSON file.

Saved workbooks are available on the **My Workbooks** tab, and you can further customize them. You can open saved workbooks by selecting **View saved workbook**. This opens the same page as the template workbook page, but you can customize this one based on Contoso's requirements.

You can select **Edit** to open the workbook in the edit mode, where you can add or remove items and provide additional customization. The editing mode displays all content in the workbook, including steps and parameters that would be hidden in the reading mode.

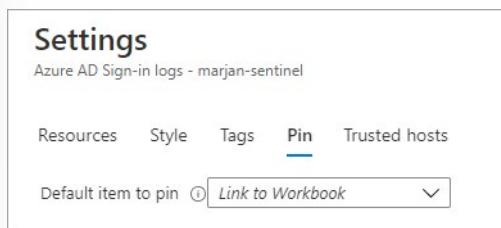
The header bar in the editing mode contains several options, which the following screenshot depicts.

 Done Editing	Done Editing	Change from edit mode to view mode
 Open	Open	Open existing Sentinel report
 Save	Save	Save changes to this workbook
 Save As	Save As	Save this workbook with another name
 Settings	Settings	Open the settings page for advanced settings, including, styles, tags, trusted hosts.
 More editing options	More editing options	Revert changes, or actions on the sentinel report, including, rename, move and delete.
 Refresh	Refresh	Refreshing the page will rerun any queries on the workbook
 Share	Share	Share a link to this report
 Show Pin Options	Show Pin Options	Pin the entire workbook or individual steps to a dashboard
 Advanced editor	Advanced editor	Open a JSON editor of the existing workbook
 Feedback	Feedback	Provides feedback to Microsoft
 Help	Help	Opens a Microsoft workbook documentation

When you switch to the editing mode, you'll notice several **Edit** options, which correspond to each individual aspect of your workbook.

If you select one of these edit options, you can examine the query that Azure Sentinel uses to filter the data from the corresponding log.

When you select the settings icon, the **Settings** page opens, where you can provide additional resources that you want to use in the workbook. You can also change the style of the workbook, provide tagging, or pin an item in the workbook.



You can rearrange the placement of different tables in the workbook by selecting **Show Pin Options**.

For advanced customization, you can select **Advanced Editor** to open the JSON representation of the current workbook, and then further customize it in the text editor.

You can save your changes in the existing workbook or save as another workbook. When you are done with all the customization, you can exit the edit mode by selecting **Done Editing**.

Explore the Azure Sentinel repository on GitHub

The Azure Sentinel repository contains out-of-the-box detections, exploration queries, hunting queries, workbooks, playbooks and much more to help you secure your environment and detect threats. Microsoft and the Azure Sentinel community contribute to this repository.

The repository contains folders with contributed content for several areas of Azure Sentinel functionality, including detection queries. You can use the code from these queries to create custom queries in your Azure Sentinel workspace.

Create a new Azure Sentinel Workbook

In addition to using built-in templates to create a customized workbook, you can also create custom workbooks from the beginning to produce highly interactive reports that contains, texts, analytic queries, metrics, and parameters.

Create a custom workbook

You can create a custom workbook by selecting **+Add workbook** on the header bar from the **Workbooks** page in Azure Sentinel. The **New workbook** page opens, which contains a basic analytics query to get you started.

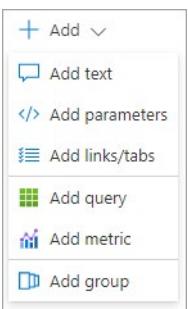
Tip: Each workbook that you create is saved as a workbook resource in the Azure Sentinel resource group.

You can start building your workbook by selecting **Edit** on the **New Workbook** page, and then again select the **Edit** option to change the text that appears in the new workbook template.

Each workbook provides a rich set of capabilities for visualizing the security data collected from the connectors. You can design your workbook with the following visualization types and elements:

- Text
- Query
- Parameters
- Links/tabs
- Metric

You can add a new element to your workbook by selecting **+Add** as the following screenshot depicts.



Text visualizations

You can use text blocks to interpret your security data, section headings, telemetry data, and other information. You can edit the text using the Markdown markup language, which provides different formatting options for headings, font styles, hyperlinks, and tables.

Note: Markdown is a markup language that you can use to format text in plain-text documents. For more information on how to format text by using Markdown controls, see the markdown guides available online.

After you add the text, you can select the **Preview** tab to preview how your content will appear. Finally, when you complete editing the text, select the **Done Editing** option.

Query item

You can create a different query from the logs and visualize the data as text, charts, or grids. You can write the query using KQL, and then format the data using various visualizations including:

- Grids (or tables)
- Area charts
- Bar charts
- Line charts
- Pie charts
- Scatter charts
- Time charts
- Tiles

When you create a query, Azure Sentinel adds a new Run Query step to the workbook as the following screenshot depicts:

```
let data = SigninLogs
|where AppDisplayName in ({Apps}) or '*' in ({Apps})
|where UserDisplayName in ({Users}) or '*' in ({Users})
|extend CAStatus = case(ConditionalAccessStatus == "success", "Successful",
    ConditionalAccessStatus == "failure", "Failed",
    ConditionalAccessStatus == "notApplied", "Not applied",
    isempty(ConditionalAccessStatus), "Not applied",
    "Disabled")
|mvexpand ConditionalAccessPolicies
|extend CAGrantControlName = tostring(ConditionalAccessPolicies.enforcedGrantControls[0])
|extend CAGrantControl = case(CAGrantControlName contains "MFA", "Enforcing MFA", "Not Enforcing MFA")
```

On the header bar, there are several fields that provide you options to tune the output of the query.

Name	Description
Run Query	Use this option to test the result of the query.

Name	Description
Samples	Microsoft provides sample code that contains sample queries that you can add to the workbook.
Data Source	Use this option to specify the data source for the query.
Resource type	Use this option select the type of resource.
Log Analytics workspace	Use this option if you want to query data against more than one resource.
Time Range	Use this option to specify a time range parameter to use in the query.
Visualization	Use this option to choose a specific visualization or choose Set by query to present the data in a different format.
Size	Use this option to choose the size of the visualization element.
Color palette	Use this option to choose specific series colors in chart settings.

On the **Advanced Settings** tab, you can provide additional customization for the settings and the styles of your query step. On the **Advanced Settings** tab, you can modify properties in the following two tabs:

- **Settings** tab. Use this tab to provide values that affect how the step will appear.
- **Style** tab. Use this tab to set the values that affect how this step will appear.

For example, on the **Settings** tab, you can enter the **Chart title**, as the following screenshot depicts.



You can use the **Style** tab to adjust the margin and padding element in the step. After you are done customizing the settings and styles, remember to save the step by selecting **Done Editing**.

Chart visualizations

When you create a query to present the security data as charts, you can customize:

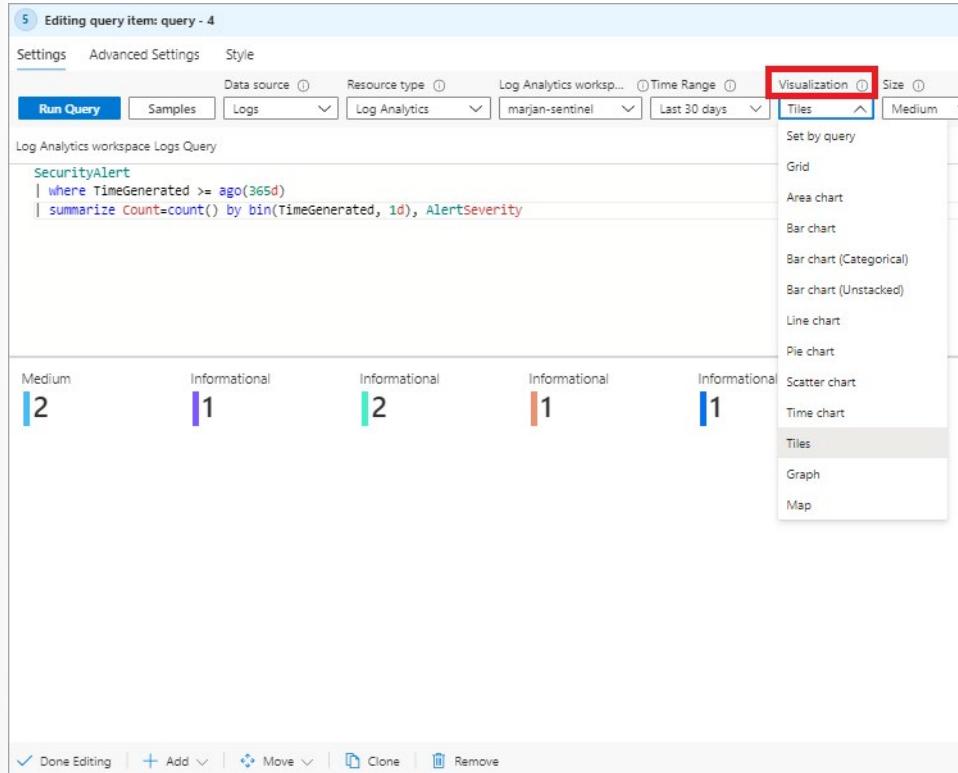
- Height

- Width
- Color palette
- Legend
- Titles
- Axis types and series

The following example counts all the security alerts and visualizes them in a pie chart.

```
SecurityAlert  
| where TimeGenerated >= ago(180d)  
| summarize Count=count() by AlertSeverity  
| render piechart
```

In the previous example, the query indicated the visualization type for the data. You can also use the query without including the *render* parameter, and then use the **Visualization** drop-down menu to select one of the offered types of visualizations, as indicated in the following screenshot.



Grid visualizations

You can use the grid visualization option from the **Visualization** drop-down menu to present data in tables, which provides an enriched UI for the reports. You can then select the **Column Settings** option to specify which column will be displayed in the table and to provide column labels, if necessary.

On the **Edit Column settings** tab, you can select a different column renderer such as, heatmap, bar, and spark area. If you select **Custom formatting**, you can set units, style, and formatting options for number values.

Parameters

You can use parameters in your interactive workbook to manipulate the results of the query in different ways. When you create a new parameter step in the workbook, a **New Parameter** page opens, where you can provide the name and other inputs required for the parameter.

You can create the following parameter types:

- Text. You can enter arbitrary text.
- Drop-down. You can modify the appearance of a query step to include a drop-down menu, in which you can select a value from a set of values. In this parameter type, you can enter a KQL query or a JSON string to provide the choices for the drop-down list.
- Options group. You can group multiple properties into group.
- Time range picker. You can select from prepopulated time ranges or select a custom range.
- Resource picker. You can select one or more Azure resources.
- You can select one or more Azure subscription resources.
- Resource type. You can select one or more Azure resource type values.
- You can select one or more Azure location values.

You can reference parameter values in other parts of the workbooks either by using bindings or by using value expansions.

On the **New Parameters** page, in the **Previews** section, you can review the variables that will be displayed and used in the query code.

Links/tabs

You can add a links/tabs step to customize the navigation in the workbook with tabs, lists, paragraphs, or bullet lists. You can provide the following inputs while adding a new links/tabs step:

- **Text before link.** Use this option to display the text before the link is selected.
- **Link text.** Use this option to specify the actual text that is displayed in the link.
- **Text after link.** Use this option to indicate the text that is displayed after the link is selected.
- **Action.** Use this option to specify the action that will be performed when you select the link, such as **Url**, **Set a parameter value** and **Scroll to a step**.
- **Value.** Use this option to indicate a value for the link.
- **Settings.** Use this option to configure specific settings based on the link type, and support parameters syntax.
- **Context.** Use this option to open a new context panel to the side instead of a full view.
- **Style.** Use this option to select between Link, Button (primary), Button (secondary) style.

You can add a new tab by selecting **TABS** from the **Style** drop-down menu on the header bar.

Metric steps

You can use metric steps to combine the results of the workbook with metrics from different Azure resources. After you are done making all your custom modifications to your workbook, remember to save the workbook by selecting **Done Editing**.

Knowledge check

Check your Knowledge

Multiple choice

Item 1. What are Entities?

- Data elements
- Tables
- Alerts

Multiple choice

Item 2. In the timeline of the Entity page, what type of items are an aggregation of notable events relating to the entity?

- Alerts
- Activities
- Bookmarks

Multiple choice

Item 3. While viewing the investigation graph, what option will show UEBA information?

- Entities
- Timeline
- Insights

Lab - Create detections and perform investigations

Lab: Create detections and perform investigations using Azure Sentinel

To download the most recent version of this lab, please visit the SC-200 [GitHub repository¹⁷](#).

Note: Depending on the lab hosting solution used for your class delivery, the lab instructions may display directly in the virtual lab environment, in addition to being available in the GitHub repository. In that case, follow guidance from your instructor as to where you will access the lab steps from. Even if the GitHub version is not used for your class, you may still find it useful to be able to reference the lab instructions on GitHub after class is over.

Lab scenario

You're a Security Operations Analyst working at a company that implemented Azure Sentinel. You must learn how to detect and mitigate threats using Azure Sentinel. You need to enable alerts from other Microsoft 365 and Azure services.

Objectives

After you complete this lab, you will be able to:

- Activate a Microsoft Security Rule.
- Create a Security Operations Center Team in Microsoft Teams.
- Create a scheduled query.
- Describe detection modeling.
- Attack Windows configured with Defender for Endpoint.
- Create detections.
- Create workbooks.

Lab setup

- Estimated time: 150 minutes

¹⁷ <https://github.com/MicrosoftLearning/SC-200T00A-Microsoft-Security-Operations-Analyst>

Answers

Multiple choice

Item 1. What are Entities?

- Data elements
- Tables
- Alerts

Explanation

The data elements include such things as Accounts, IP Addresses, Hosts

Multiple choice

Item 2. In the timeline of the Entity page, what type of items are an aggregation of notable events relating to the entity?

- Alerts
- Activities
- Bookmarks

Explanation

Activities are the aggregation of events.

Multiple choice

Item 3. While viewing the investigation graph, what option will show UEBA information?

- Entities
- Timeline
- Insights

Explanation

Insights will display UEBA information.

Module 8 Perform threat hunting in Azure Sentinel

Threat hunting concepts in Azure Sentinel

Lesson Introduction

Use Azure Sentinel to hunt for security threats across on-premises and cloud environments by using interactive queries and other tools.

In this lesson you will learn the fundamental concepts of hunting for threats using Azure Sentinel.

Learning objectives

After completing this lesson, you should be able to:

- Describe threat hunting concepts for use with Azure Sentinel
- Define a threat hunting hypothesis for use in Azure Sentinel

Cybersecurity threat hunting

The term "threat hunting" is defined differently by different people. The most commonly used definition is the idea that you are proactively hunting through your environment for a threat or a set of activities that you have not previously detected. The "not previously detected" part is what differentiates threat hunting from incident response or alert triage.

Other uses of the term hunting include searching for threats with newly obtained indicators. If a Threat Intelligence Feed provides a new IP Address considered harmful, an analyst can then take the IP Address and search the logs to find if the new indicator was seen in the past. Technically this is not threat hunting because you are using a known bad such as an IP Address. Azure Sentinel already provides hunting queries to facilitate this process. Next, hunt for more evidence-based threats from a current Incident or Alert as part of an Incident Analysis process. It is vital to explore data based on evidence found in a current incident. Both Azure Sentinel and Microsoft 365 Defender provide this type of hunting capability.

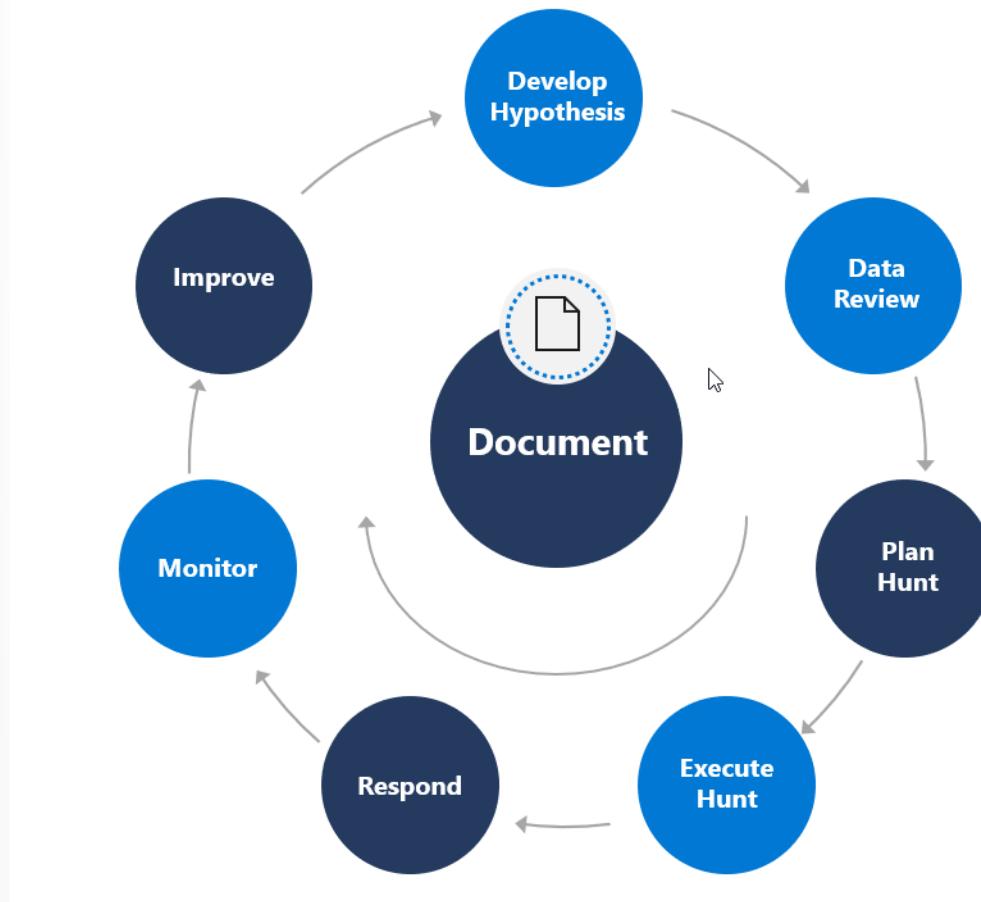
All of these approaches have one thing in common: using KQL queries to find threats.

Microsoft Defender and Microsoft Defender Endpoint are more focused on indicator and analysis types of hunting. Azure Sentinel provides more features to manage the threat hunting process.

Proactive hunts

Why do proactive hunting? As you hunt for "not previously detected" threats, the concern is that if you wait for the threat to be detected, the compromise impact could be more significant. If we don't have a known indicator, then what are we hunting? We hunt based on a Hypothesis. The Hypothesis might start with "Operational Threat Intelligence," and then list the attackers' tactics and techniques. A Hypothesis can search for a specific technique, not an indicator like an IP address. If malicious activity is identified, we might have discovered the attacker earlier in the attack process before they have an opportunity to exfiltrate data.

Process to hunt threats



Threat hunting should be a continual process. We start at the top of our cycle with our Hypothesis. Our Hypothesis helps us plan out what we are going to hunt for, which requires us to understand where we are going to hunt and how we will do it. This means we need to understand the data we have, the tools we have, the expertise we have, and how to work with them. The hunting cycle doesn't stop when we execute the hunt. There are still several phases we need to conduct throughout the life cycle, including responding to anomalies. Even if we don't find an active threat, there will be activities to perform.

Routine tasks should include:

- Setting up new monitoring.
- Improving our detection capabilities.

Everything done in Threat Hunting should be documented. Documentation for the hunt should include:

- What, How, and Why
- Input and Output
- How to replicate the hunt
- Next Steps

Develop a threat hunting hypothesis

Hunting starts with a Hypothesis. The idea of what we are going to hunt. Getting this right is critical because it drives our focus on what we are going to do. What makes a good Hypothesis?

There are many factors, but here are the key ones:

Keep it achievable. Don't perform a hunt where you know you have no hope of finding results because you do not have the data available or have insufficient knowledge about the threat to understand how to find it.

Keep the scope narrow. Avoid broad a hypothesis such as "I am going to hunt for strange log-ons." Such a hypothesis fails to define what the results could mean.

Keep it time-bound. Are you looking for any login since the beginning of your logs? Are you looking for last week? The last day? The time-bounded also is used in documentation. You will want Threat Hunting to be a continual process. If you don't time-bound your hunts, there is a chance that you will end up just repeating the same hunt on the same dataset. You will be able to say, "I did this hunt, at this time, covering this period." With this documented, your team members will know what period was hunted for with this Hypothesis.

Keep it useful and efficient. You want to target threats that maybe you don't have adequate coverage for in your detections. These might be things that you know that you've previously missed or that you haven't detected. A good SOC team typically has a good idea about where their coverage is good and where it may be weaker and needs improvement. You also want to make sure it relates to realistic threats. There is no point in hunting for an advanced threat that targets an industry you're not in or a platform you are not using.

Keep it related to the threat model that you are defending against. Otherwise, you may spend much time threat hunting for things that you will never find and which are not a threat.

Don't start your Threat Hunting journey going after the most advanced threats. Start with the basics and incrementally mature your organization's Threat Hunting capabilities. Start with a simple Hunt Hypothesis. An example hypothesis could be that we have Threat Intel that a Threat Actor, has automated attacks that use the cmd.exe process.

Another Hypothesis could be; We want to check for the last day in which accounts have run cmd.exe, but that have not run cmd.exe during the past week.

Threat hunting with Azure Sentinel

Lesson introduction

Contoso, Ltd., is a midsize financial services company in London with a New York branch office. Contoso uses Microsoft 365, Azure Active Directory (Azure AD), Azure AD Identity Protection, Microsoft Cloud App Security, Microsoft Defender for Identity, Microsoft Defender for Endpoint, Microsoft Defender for Office 365, Endpoint Protection, and Azure Information Protection.

As part of the Security Operations Center team, you've been tasked with using Azure Sentinel to identify security threats within Contoso's Azure environment.

By the end of this lesson, you'll be able to hunt for threats by using the tools available in Azure Sentinel. Specifically, you'll be able to proactively identify threat behaviors by using Azure Sentinel queries. You'll also be able to use bookmarks and livestream to identify specific account usage patterns for Contoso's Azure environment.

Learning objectives

After completing this lesson, you should be able to:

- Use queries to hunt for threats.
- Save key findings with bookmarks.
- Observe threats over time with livestream.

Manage Azure Sentinel threat-hunting queries

Azure Sentinel contains powerful query tools that can help you, as part of the Security Operations Center team, find and isolate security threats and unwanted activity in Contoso's environment.

Hunt by using built-in queries

You can use the search and query tools in Azure Sentinel to hunt for security threats and tactics throughout your environment. Hunting queries enable you to filter through large amounts of events and security data sources to identify potential threats or track down known or expected threats.

The **Hunting** page in Azure Sentinel has built-in queries. These queries can guide your hunting process and help you pursue the appropriate hunting paths to uncover issues in your environment. Hunting queries can expose issues that aren't significant enough on their own to generate an alert but have happened often enough over time to warrant investigation.

The screenshot shows the Azure Sentinel Hunting page. At the top, there are navigation links for 'Total queries' (173), 'My bookmarks' (0), and 'Livestream Results' (0). Below these are filters for 'Favorites : All', 'Provider : All', 'Data sources : All', and 'Tactics : All'. The main area is a table listing hunting queries. Each query row includes a star icon for favoriting, the provider (e.g., Microsoft), data source (e.g., DnsEvents, SecurityEvent, SecurityAlert, AuditLogs), results count, and a tactics column showing related MITRE ATT&CK tactics. A sidebar on the right titled 'MITRE ATT&CK™' shows a timeline of tactics with counts: Initial Access (27), Impact (24), Persistence (52), Collection (26), Credential Access (13), Execution (10), T1059 (12), T1078 (15), T1079 (14), T1083 (17), T1087 (26), and T1093 (0). Below the sidebar, a message says 'No query selected' and 'Select a query to view more details'.

The **Hunting** page provides a list all hunting queries. You can filter and sort queries by name, provider, data source, results, and tactics. You can save queries by selecting the **Favorites** star icon for the query in the list.

Tip: When a query is selected as a favorite, it runs automatically each time you open the **Hunting** page.

Manage hunting queries

When you select a query from the list, the query details appear on a new pane. The query details pane contains a description, code, and other information about the query. That information includes related entities and identified tactics. You can run a query interactively by selecting **Run Query** on the details pane.

Hunt for threats by using the MITRE ATT&CK framework

Azure Sentinel uses the MITRE ATT&CK framework to categorize and order queries by tactics. ATT&CK is a knowledge base of tactics and techniques that are used and observed in the global threat landscape. You can use MITRE ATT&CK to develop and inform your threat-hunting models and methods in Azure Sentinel. When you're threat hunting in Azure Sentinel, you can use the ATT&CK framework to categorize and run queries by using the MITRE ATT&CK tactics timeline.

Note: You can select individual MITRE ATT&CK tactics from the timeline on the **Hunting** page.

The screenshot shows the MITRE ATT&CK timeline. It features a horizontal bar with various tactic icons and their counts: Initial Access (27), Impact (24), Persistence (52), Collection (26), Credential Access (13), Execution (10), T1059 (12), T1078 (15), T1079 (14), T1083 (17), T1087 (26), and T1093 (0).

Selecting any tactic will filter the available queries by the selected tactic. Tactics include:

- **Initial access.** Tactics that the adversary uses to gain entry to a network, by exploiting vulnerabilities or configuration weaknesses in public-facing systems. An example is targeted spear-phishing.
- **Execution.** Tactics that result in an adversary running their code on a target system. For example, a malicious hacker might run a PowerShell script to download more attacker tools and/or scan other systems.

- **Persistence.** Tactics that allow an adversary to maintain access to a target system, even after restarts and credential changes. An example of a persistence technique is an attacker who creates a scheduled task that runs their code at a specific time or on restart.
- **Privilege escalation.** Tactics that an adversary uses to gain higher-level privileges on a system, such as local administrator or root.
- **Defense evasion.** Tactics that attackers use to avoid detection. Evasion tactics include hiding malicious code within trusted processes and folders, encrypting or obfuscating adversary code, or disabling security software.
- **Credential access.** Tactics deployed on systems and networks to steal usernames and credentials for reuse.
- **Discovery.** Tactics that adversaries use to obtain information about systems and networks that they want to exploit or use for their tactical advantage.
- **Lateral movement.** Tactics that allow an attacker to move from one system to another within a network. Common techniques include pass-the-hash methods of authenticating users and abuse of the Remote Desktop Protocol.
- **Collection.** Tactics that an adversary uses to gather and consolidate the information they were targeting as part of their objectives.
- **Command and control.** Tactics that an attacker uses to communicate with a system under their control. One example is an attacker communicating with a system over an uncommon or high-numbered port to evade detection by security appliances or proxies.
- **Exfiltration.** Tactics used to move data from the compromised network to a system or network that's fully under control of the attacker.
- **Impact.** Tactics that an attacker uses to affect the availability of systems, networks, and data. Methods in this category include denial-of-service attacks and disk-wiping or data-wiping software.

Create custom queries to refine threat hunting

All Azure Sentinel hunting queries use Kusto Query Language (KQL) syntax used in Log Analytics. You can modify a query in the details pane and run the new query. Or you can save it as a new query that can be reused in your Azure Sentinel workspace.

You can also create your own custom queries by using KQL code to hunt for threats.

Create custom query

Delete Query

Name *

Description

Custom query

[View query results >](#)

Custom queries enable you to define the following:

Query parameter	Description
Name	Provide a name for the custom query.
Description	Provide a description of your query's functionality.
Entity mapping	Map entity types to columns from your query result to populate your query results with more actionable information. You can also map entities by using code in your KQL query.
Tactics	Specify the tactics that your query is designed to expose.

Custom queries are listed alongside built-in queries for management.

Explore the Azure Sentinel repository on GitHub

The Azure Sentinel repository contains out-of-the-box detections, exploration queries, hunting queries, workbooks, playbooks, and much more to help you secure your environment and hunt for threats. Microsoft and the Azure Sentinel community contribute to this repo.

The repo contains folders with contributed content for several areas of Azure Sentinel functionality, including hunting queries. You can use the code from these queries to create custom queries in your Azure Sentinel workspace.

Choose the best response for the following question. Then select **Check your answers**.

Save key findings with bookmarks

To hunt for threats to Contoso's environment, you have to review large amounts of log data for evidence of malicious behavior. During this process, you might find events that you want to remember, revisit, and analyze as part of validating potential hypotheses and understanding the full story of a compromise.

Hunt by using bookmarks

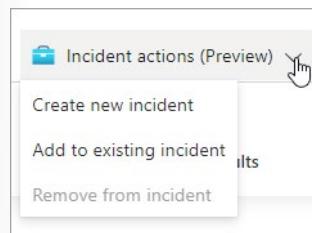
Bookmarks in Azure Sentinel can help you hunt for threats by preserving the queries you ran in Azure Sentinel, along with the query results that you deem relevant. You can also record your contextual observations and reference your findings by adding notes and tags. Bookmarked data is visible to you and your teammates for easy collaboration.

You can revisit your bookmarked data at any time on the **Bookmarks** tab of the **Hunting** page. You can use filtering and search options to quickly find specific data for your current investigation. Alternatively, you can review your bookmarked data directly in the **HuntingBookmark** table in your Log Analytics workspace.

Note: Bookmarked events contain standard event information but can be used in different ways throughout the Azure Sentinel interface.

Create or add to incidents by using bookmarks

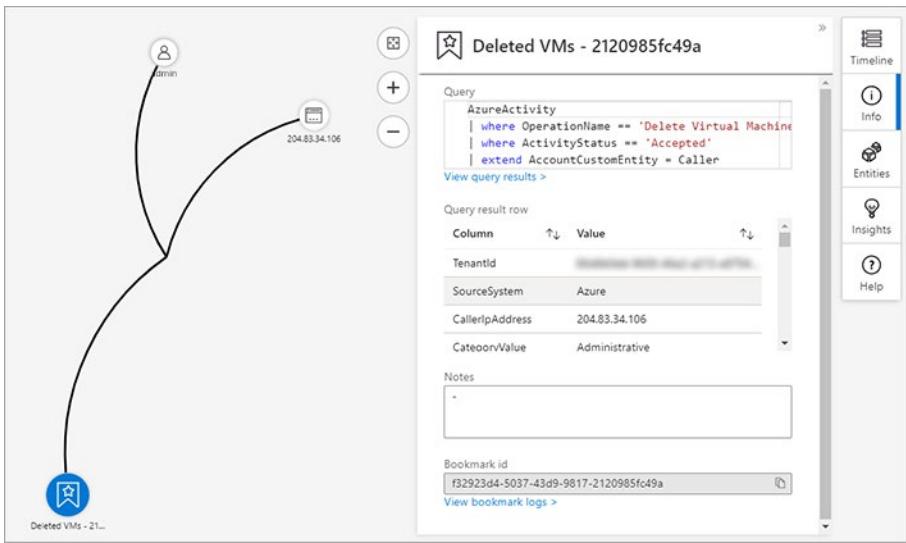
You can use bookmarks to create a new incident or add bookmarked query results to existing incidents. The **Incident actions** button on the toolbar enables you to perform either of these tasks when a bookmark is selected.



Incidents that you create from bookmarks can be managed from the **Incidents** page alongside other incidents created in Azure Sentinel.

Use the investigation graph to explore bookmarks

You can investigate bookmarks in the same way that you'd investigate incidents in Azure Sentinel. From the **Hunting** page, select **Investigate** to open the investigation graph for the incident. The investigation graph is a visual tool that helps to identify entities involved in the attack and the relationships between those entities. If the incident involves multiple alerts over time, you can also review the alert timeline and correlations between alerts.



Review entity details

You can select each entity on the graph to observe complete contextual information about it. This information includes relationships to other entities, account usage, and data flow information. For each information area, you can go to the related events in Log Analytics and add the related alert data into the graph.

Review bookmark details

You can select the bookmark item on the graph to observe important bookmark metadata related to the bookmark's security and environment context.

Observe threats over time with livestream

You can use the hunting livestream to test queries against live events as they occur. Livestream provides interactive sessions that can notify you when Azure Sentinel finds matching events for your query.

A livestream is always based on a query. Typically, you use the query to narrow down streaming log events, so only the events that are related to your threat-hunting efforts appear. You can use a livestream to:

- Test new queries against live events.
- Generate notifications for threats.
- Launch investigations.

Livestream queries refresh every 30 seconds and generate Azure notifications of any new results from the query.

Create a livestream

To create a livestream from the **Hunting** page in Azure Sentinel, select the **Livestream** tab and then select **New livestream** from the toolbar.

Note: Livestream queries run continuously against your live environment, so you can't use time parameters in a livestream query.

The screenshot shows the 'Livestream' page. At the top, there's a toolbar with icons for Play, Save, Delete, Create analytics rule, Add bookmark, and Columns. A message says 'Livestream session is paused, click 'Play' to start'. Below that is a 'Name' input field containing a redacted name. Under 'Query', there's a list with item '1' and a text input field. At the bottom, there's a link 'View query results >'.

View a livestream

On the new **Livestream** page, specify a name for the livestream session and the query that will provide results for the session. Notifications for livestream events will appear in your Azure portal notifications.

Manage a livestream

You can play the livestream to review results or save the livestream for later reference. Saved livestream sessions can be viewed from the **Livestream** tab on the **Hunting** page. You can also elevate events from a livestream session to an alert by selecting the events and then selecting **Elevate to alert** from the command bar.

You might use a livestream to track baseline activities for Azure resource deletion at Contoso and identify other Azure resources that should be tracked. For example, the following query will return any Azure Activity events that recorded a deleted resource:

```
AzureActivity  
| where OperationName has 'delete'  
| where ActivityStatus == 'Accepted'  
| extend AccountCustomEntity = Caller  
| extend IPCustomEntity = CallerIpAddress
```

Use a livestream query to create an analytics rule

If the query returns significant results, you can select **Create analytics rule** from the command bar to create an analytics rule based on the query. After the rule refines the query to identify the specific resources, it can generate alerts or incidents when the resources are deleted.

Choose the best response for the following question. Then select **Check your answers**.

Hunt for threats using notebooks in Azure Sentinel

Lesson Introduction

You can use notebooks in Azure Sentinel for advanced hunting.

You are a Security Operations Analyst working at a company that implemented Azure Sentinel. You want to mature your Security Operations team to proactively hunt for malicious activity in your environment with advanced machine learning capabilities.

After developing your hunting hypothesis, you utilize a Jupyter notebook to integrate machine learning libraries, advanced visualizations, and external data to detect malicious activity patterns.

Learn how to use notebooks in Azure Sentinel for advanced hunting.

Learning objectives

After completing this lesson, you should be able to:

- Explore API libraries for advanced threat hunting in Azure Sentinel
- Describe notebooks in Azure Sentinel
- Create and use notebooks in Azure Sentinel

Access Azure Sentinel data with external tools

Before hunting with notebooks, it is essential to understand the foundation of Azure Sentinel is the Log Analytics data store, which combines high-performance querying, dynamic schema, and scales to massive data volumes. The Azure portal and all Azure Sentinel tools use a standard API to access this data store. The same API is also available for external tools such as Python and PowerShell. There are two libraries that you can use to simplify API access:

- Kqlmagic
- msticpy

Kqlmagic

The Kqlmagic library provides an easy to implement API wrapper to run KQL queries.

msticpy

Microsoft Threat Intelligence Python Security Tools is a set of Python tools intended to be used for security investigations and hunting. Many of the tools originated as code Jupyter notebooks written to solve a problem as part of a security investigation. Some of the tools are only useful in notebooks (for example, much of the nbtools subpackage), but many others can be used from the Python command line or imported into your code.

The package addresses three central needs for security investigators and hunters:

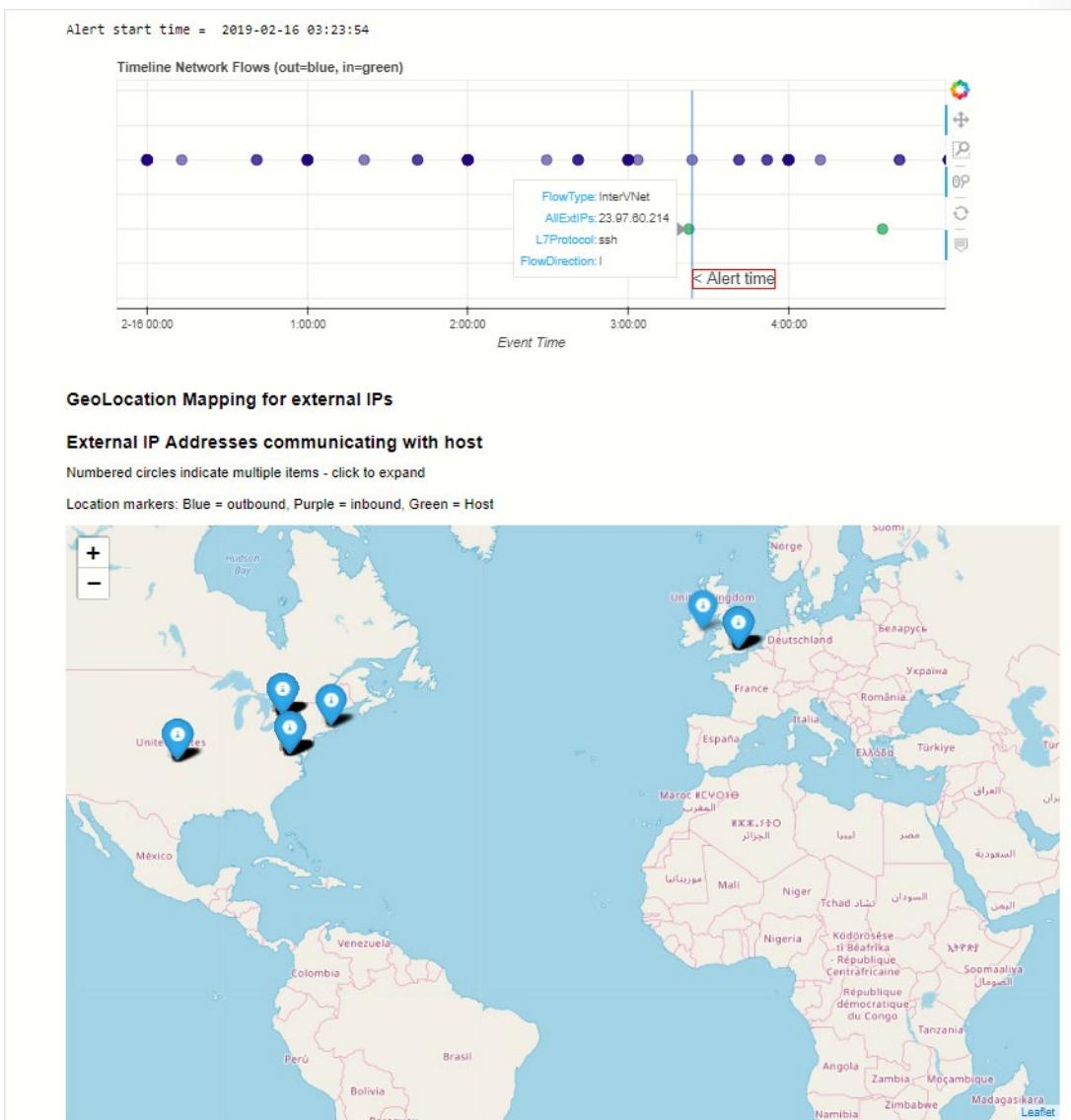
- Acquiring and enriching data
- Analyzing data

- Visualizing data

msticpy can query using KQL; the library also provides predefined queries for Azure Sentinel, Microsoft 365 Defender for Endpoint, and the Microsoft Security Graph. An example of a function is the `list_logons_by_account`, which retrieves the logon events for an account. For details about `msticpy` visit: <https://msticpy.readthedocs.io/>¹

Hunt with notebooks

A Jupyter Notebook allows you to create and share documents that contain live code, equations, visualizations, and explanatory text. Uses include data cleaning and transformation, numerical simulation, statistical modeling, machine learning, and much more. Jupyter extends the scope of what you can do with Azure Sentinel data. It combines full programmability with a vast library collection for machine learning, visualization, and data analysis. These attributes make Jupyter a useful tool for security investigation and hunting.



¹ <https://msticpy.readthedocs.io/?azure-portal=true>

Several notebooks, developed by some of Microsoft's security analysts, are packaged with Azure Sentinel. Some of these notebooks are built for a specific scenario and can be used as-is. Others are samples intended to illustrate techniques and features that you can copy or adapt for use in your own notebooks. Other notebooks may also be imported from the Azure Sentinel Community GitHub.

Notebooks have two components:

- The browser-based interface where you enter and run queries and code and where the execution results are displayed.
- The kernel is responsible for parsing and executing the code itself.

The Azure Sentinel notebook's kernel runs on an Azure virtual machine (VM). Several licensing options exist to use more powerful virtual machines if your notebooks include complex machine learning models.

The Azure Sentinel notebooks use many popular Python libraries such as pandas, matplotlib, bokeh, etc. There are a great many other Python packages for you to choose from, covering areas such as:

- Visualizations and graphics
- Data processing and analysis
- Statistics and numerical computing
- Machine learning and deep learning

The msticpy package is used in many of the included notebooks. Msticpy tools are explicitly designed to help with creating notebooks for hunting and investigation.

Create a notebook

To start with Notebooks, use the "Getting Started Guide For Azure Sentinel ML Notebooks" notebook.

1. In the Azure Sentinel Workspace, select **Notebooks** (Preview)
2. Select *A Getting Started Guide For Azure Sentinel ML Notebooks*. Then select **Launch notebook** in the bottom right.
3. Next, you need to select an AzureML Workspace. Select **Create new**.
4. In the Subscription box, select your subscription.
5. Select **Create a new Resource group** and choose a name for your new resource group.
6. In the Workspace details section:
 - Give your workspace a unique name.
 - Choose your Region
 - Save your Storage account, Key vault, and Application insights information.
 - The Container registry option can remain as None.
7. At the bottom of the page, select **Review + create**. Then on the next page, select **create**. It will take a moment to deploy the workspace.
8. After the deployment is finished, select the **Go to resource** button.
9. Select the **Launch studio** button that appears in the center of the screen.
10. On the Welcome to the studio page, select your directory and subscription and the workspace you just created. Then select **Get started**.
11. Select the **Notebooks** button on the toolbar on the left side of your screen.

12. A new area showing your files will appear. In Users/yourusername/ select the *A Getting Started Guide For Azure Sentinel ML Notebooks* file.
13. Next to the Compute instance selector at the top of the screen, select the ..., and select **New Compute**.
14. Choose your compute settings.
15. Name your Compute instance and select the **Create** button at the bottom of the screen.
16. In the top right of the notebook, select a Kernel to use.

If you cannot complete the steps above to access the notebook, you can view the steps on its GitHub page instead. See the notebook file here: [Azure-Sentinel-Notebooks²](#)

Explore notebook code

The following code blocks of the "Getting Started Guide For Azure Sentinel ML Notebooks" notebook provide a representative example of working with Azure Sentinel data.

Code Block

In this snippet of code:

- Create a new variable [test_query] that contains the KQL query.
- Next, you run the query [qry_prov.exec_query()]. This utilizes the msticpy library to execute the KQL query in the Azure Sentinel Log Analytics related workspace. The results are stored in the [test_df] variable.
- Next, display the first five rows with the .head() function.

```
In [ ]: # Define our query
test_query = """
SigninLogs
| where TimeGenerated > ago(7d)
| take 10
"""

# Pass that query to our QueryProvider
test_df = qry_prov.exec_query(test_query)

# Check that we have some data
if isinstance(test_df, pd.DataFrame) and not test_df.empty:
    # .head() returns the first 5 rows of our results DataFrame
    display(test_df.head())
# If there is no data Load some sample data to use instead
else:
    md("You don't appear to have any SigninLogs - we will load sample data for you to use.")
    if not Path("nbdemo/data/aad_logons.pkl").exists():
        Path("nbdemo/data/").mkdir(parents=True, exist_ok=True)
        urlretrieve('https://github.com/Azure/Azure-Sentinel-Notebooks/blob/master/nbdemo/data/aad_logons.pkl?raw=true', 'nbdemo/data/aad_logons.pkl')
        urlretrieve('https://raw.githubusercontent.com/Azure/Azure-Sentinel-Notebooks/master/nbdemo/data/queries.yaml', 'nbdemo/data/queries.yaml')
    qry_prov = QueryProvider("LocalData", data_paths=["nbdemo/data/"], query_paths=["nbdemo/data/"])
    logons_df = qry_prov.Azure.list_all_signins_geo()
    display(logons_df.head())
```

Code Block

In this snippet of code:

- You create a new function called lookup_res that takes a variable row.
- Next, you save the IP address stored in row to the variable [ip].
- The next line of code uses the msticpy function [ti.lookup_ioc()] to query the ThreatIntelligenceIndicator table for a row that is sourced from VirusTotal with a matching ip address.

² <https://github.com/Azure/Azure-Sentinel-Notebooks/blob/8122bca32387d60a8ee9c058ead9d3ab8f4d61e6/A%20Getting%20Started%20Guide%20For%20Azure%20Sentinel%20ML%20Notebooks.ipynb?azure-portal=true>

- Next, the msticpy function [ti.result_to_df()] will return a DataFrame representation of response.
- The new function returns the Severity of the IP address.

```
In [ ]: vis_q = """
SigninLogs
| where TimeGenerated > ago(7d)
| sample 5"""

# Try and query for data but if using sample data Load that instead
try:
    vis_data = qry_prov.exec_query(vis_q)
except FileNotFoundError:
    vis_data = logons_df

# Check we have some data in our results and if not use previously used dataset
if not isinstance(vis_data, pd.DataFrame) or vis_data.empty:
    vis_data = logons_df

# Plot up to the first 5 IP addresses
vis_data.head()["IPAddress"].value_counts().plot.bar(
    title="IP prevalence", legend=False
)
```



Code Block

In this snippet of code:

- Create a new variable [vis_q] that contains the KQL query.
- Next, you run the query [qry_prov.exec_query()]. This utilizes the msticpy library to execute the KQL query in the Azure Sentinel Log Analytics related workspace. The results are stored in the [vis_data] variable.
- Then, [qry_prov.exec_query()] returns a pandas DataFrame that provides visualization features. You then plot a bar graph with the unique IP addresses and how many times they were used in the first five entries of the Dataframe.

```
In [ ]: # Take the IP address in each row, Look it up against TI and return the severity score
def lookup_res(row):
    ip = row['IPAddress']
    resp = ti.lookup_ioc(ip, providers=["VirusTotal"])
    resp = ti.result_to_df(resp)
    return resp["Severity"].iloc[0]
```

Knowledge check

Check your Knowledge

Multiple choice

Item 1. The msticpy package provides which of the following functionality?

- Data wrangling
- Analyzing data
- Creating data

Multiple choice

Item 2. Which is a component of notebooks in Azure Sentinel?

- Telemetry analyzer
- Kernel
- Workbook

Multiple choice

Item 3. What coding language is most commonly used in the sample Notebooks?

- Python
- C#
- Java

Multiple choice

Item 4. Which of the following best describes a good Hypothesis?

- is Time-bound
- focuses on known Indicators
- focuses on all current threats

Multiple choice

Item 5. Threat Hunting is considered which of the following?

- Retroactive.
- Reactive.
- Proactive.

Multiple choice

Item 6. "We want to check which accounts have run cmd.exe." Why is this hypothesis poor?

- Cmd.exe is not a program.
- Accounts are not associated with the running of cmd.exe
- The scope is too broad.

Lab - Threat hunting in Azure Sentinel

Lab: Threat hunting in Azure Sentinel

To download the most recent version of this lab, please visit the SC-200 [GitHub repository³](#).

Note: Depending on the lab hosting solution used for your class delivery, the lab instructions may display directly in the virtual lab environment, in addition to being available in the GitHub repository. In that case, follow guidance from your instructor as to where you will access the lab steps from. Even if the GitHub version is not used for your class, you may still find it useful to be able to reference the lab instructions on GitHub after class is over.

Lab scenario

You're a Security Operations Analyst working at a company that implemented Azure Sentinel. You have received threat intelligence about a Command and Control (C2) technique. You need to perform a hunt and watch for the threat.

Objectives

After you complete this lab, you will be able to:

- Create a hunting query, bookmark a result, and create a Livestream.
- Use a Notebook to hunt for threats using Azure Sentinel.

Lab setup

- Estimated time: 25 minutes

³ <https://github.com/MicrosoftLearning/SC-200T00A-Microsoft-Security-Operations-Analyst>

Answers

Multiple choice

Item 1. The msticpy package provides which of the following functionality?

- Data wrangling
- Analyzing data
- Creating data

Explanation

The msticpy package has several functions that help security investigators and hunters analyze data.

Multiple choice

Item 2. Which is a component of notebooks in Azure Sentinel?

- Telemetry analyzer
- Kernel
- Workbook

Explanation

Notebooks use the Kernel to parse and execute the code within the notebook

Multiple choice

Item 3. What coding language is most commonly used in the sample Notebooks?

- Python
- C#
- Java

Explanation

Python is the most commonly used coding language in the sample notebooks.

Multiple choice

Item 4. Which of the following best describes a good Hypothesis?

- is Time-bound
- focuses on known Indicators
- focuses on all current threats

Explanation

The Hypothesis should be time-bound.

Multiple choice

Item 5. Threat Hunting is considered which of the following?

- Retroactive.
- Reactive.
- Proactive.

Explanation

You are not waiting for detections to flag an anomaly.

Multiple choice

Item 6. "We want to check which accounts have run cmd.exe." Why is this hypothesis poor?

- Cmd.exe is not a program.
- Accounts are not associated with the running of cmd.exe
- The scope is too broad.

Explanation

Knowing which accounts have run cmd.exe doesn't prove a possible anomaly.