Microsoft Security

Azure Sentinel:
3 Use Cases for Threat Detection and Investigation

Contents

“Azure Sentinel uses machine learning to profile users, entities, and the environment, detecting attacks that might not be caught using predefined methodologies. This means you can empower Tier 1 analysts to focus their efforts less on sifting through mountains of data and more on highlighting relevant incidents.”

Your enterprise faces a growing array of increasingly sophisticated security threats

Detecting and defending against them requires intelligent analytics, effective teamwork, and advanced tools. Microsoft Azure Sentinel meets these needs with a scalable, cloud-native, security information event management (SIEM) solution that also makes it easier to orchestrate and automate threat responses.

As a single place for alert detection, threat visibility, proactive hunting, and incident response across the entire enterprise, Azure Sentinel empowers you to:

- **Collect data at cloud scale** across all users, devices, applications, and infrastructure, both on-premises and in multiple cloud environments.
- **Identify previously undetected threats,** and minimize false positives using Microsoft's analytics and unparalleled threat intelligence.
- **Investigate threats with artificial intelligence,** and hunt for suspicious activities at scale, tapping into years of cybersecurity work at Microsoft.
- **Respond to incidents rapidly** with built-in orchestration and automation of common tasks.

In this e-book, we'll take a look at three common scenarios to empower your security analysts in threat detection and investigation. From anomaly detection to automatic alert prioritization to the investigation of threats, we'll cover a range of foundational capabilities.

These use cases assume that you have already connected data sources to Azure Sentinel. For more information on basic setup and data ingestion, visit the **Azure Sentinel Quick Start Guide**.

Use case #1:

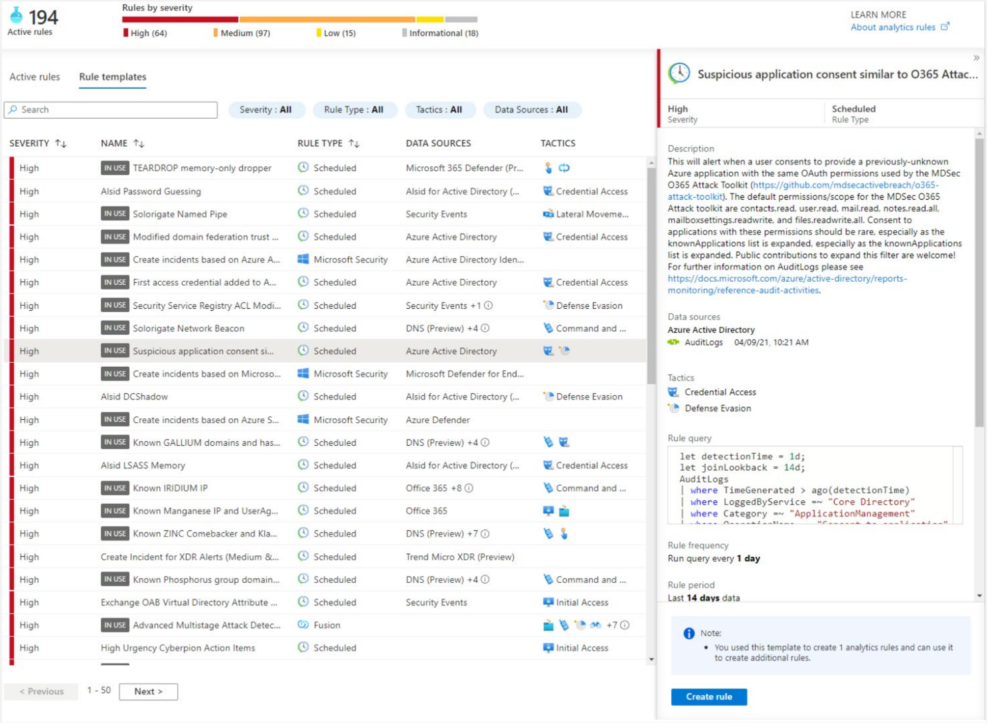
Anomaly detection

Azure Sentinel uses machine learning to profile users, entities, and the environment, detecting attacks that might not be caught using predefined methodologies

Traditional security software uses predefined rules to detect threats. While this can be an effective method when applied to known threats, it is not as effective when new types of risks emerge. Azure Sentinel uses machine learning to profile users, entities, and the environment, detecting attacks that might not be caught using predefined methodologies. This means you can empower Tier 1 analysts to focus their efforts less on sifting through mountains of data and more on highlighting relevant incidents.

To make it simple, Azure Sentinel provides built-in templates out of the box. These templates are designed by Microsoft security experts and analysts based on known threats, common attack vectors, and signature patterns of suspicious activity. They allow you to apply advanced analytics without the need to build your own machine learning models or become a data science expert.

By enabling these templates, you will automatically be alerted to anomalies that could indicate an attack. You can also customize them to search for or filter out types of activity that are specific to your enterprise.



SEVERITY ↑↓	NAME ↑↓	RULE TYPE ↑↓	DATA SOURCES	TACTICS
High	IN USE TEARDROP memory-only dropper	Scheduled	Microsoft 365 Defender (Pr...	
High	Alsid Password Guessing	Scheduled	Alsid for Active Directory (...	Credential Access
High	IN USE Solorigate Named Pipe	Scheduled	Security Events	Lateral Moveme...
High	IN USE Modified domain federation trust ...	Scheduled	Azure Active Directory	Credential Access
High	IN USE Create incidents based on Azure A...	Microsoft Security	Azure Active Directory Iden...	
High	IN USE First access credential added to A...	Scheduled	Azure Active Directory	Credential Access
High	IN USE Security Service Registry ACL Modi...	Scheduled	Security Events +1 ⓘ	Defense Evasion
High	IN USE Solorigate Network Beacon	Scheduled	DNS (Preview) +4 ⓘ	Command and ...
High	IN USE Suspicious application consent si...	Scheduled	Azure Active Directory	
High	IN USE Create incidents based on Microso...	Microsoft Security	Microsoft Defender for End...	
High	Alsid DCShadow	Scheduled	Alsid for Active Directory (...	Defense Evasion
High	IN USE Create incidents based on Azure S...	Microsoft Security	Azure Defender	
High	IN USE Known GALLIUM domains and has...	Scheduled	DNS (Preview) +4 ⓘ	
High	Alsid LSASS Memory	Scheduled	Alsid for Active Directory (...	Credential Access
High	IN USE Known IRIDIUM IP	Scheduled	Office 365 +8 ⓘ	Command and ...
High	IN USE Known Manganese IP and UserAg...	Scheduled	Office 365	
High	IN USE Known ZINC Comebacker and Kla...	Scheduled	DNS (Preview) +7 ⓘ	
High	Create Incident for XDR Alerts (Medium &...	Scheduled	Trend Micro XDR (Preview)	
High	IN USE Known Phosphorus group domain...	Scheduled	DNS (Preview) +4 ⓘ	Command and ...
High	Exchange OAB Virtual Directory Attribute ...	Scheduled	Security Events	Initial Access
High	IN USE Advanced Multistage Attack Detec...	Fusion		+7 ⓘ
High	High Urgency Cyberpion Action Items	Scheduled		Initial Access

Suspicious application consent similar to O365 Attac...

High
Severity

Scheduled
Rule Type

Description

This will alert when a user consents to provide a previously-unknown Azure application with the same OAuth permissions used by the MDSec O365 Attack Toolkit (https://github.com/mdsecactivebreach/o365-attack-toolkit). The default permissions/scope for the MDSec O365 Attack toolkit are contacts.read, user.read, mail.read, notes.read.all, mailboxsettings.readwrite, and files.readwrite.all. Consent to applications with these permissions should be rare, especially as the knownApplications list is expanded, especially as the knownApplications list is expanded. Public contributions to expand this filter are welcome! For further information on AuditLogs please see https://docs.microsoft.com/azure/active-directory/reports-monitoring/reference-audit-activities.

Data sources

Azure Active Directory
AuditLogs 04/09/21, 10:21 AM

Tactics

Credential Access
Defense Evasion

Rule query

```
let detectionTime = 1d;
let joinLookback = 14d;
AuditLogs
| where TimeGenerated > ago(detectionTime)
| where LoggedByService =~ "Core Directory"
| where Category =~ "ApplicationManagement"
```

Rule frequency

Run query every **1 day**

Rule period

Last **14 days** data

Note:

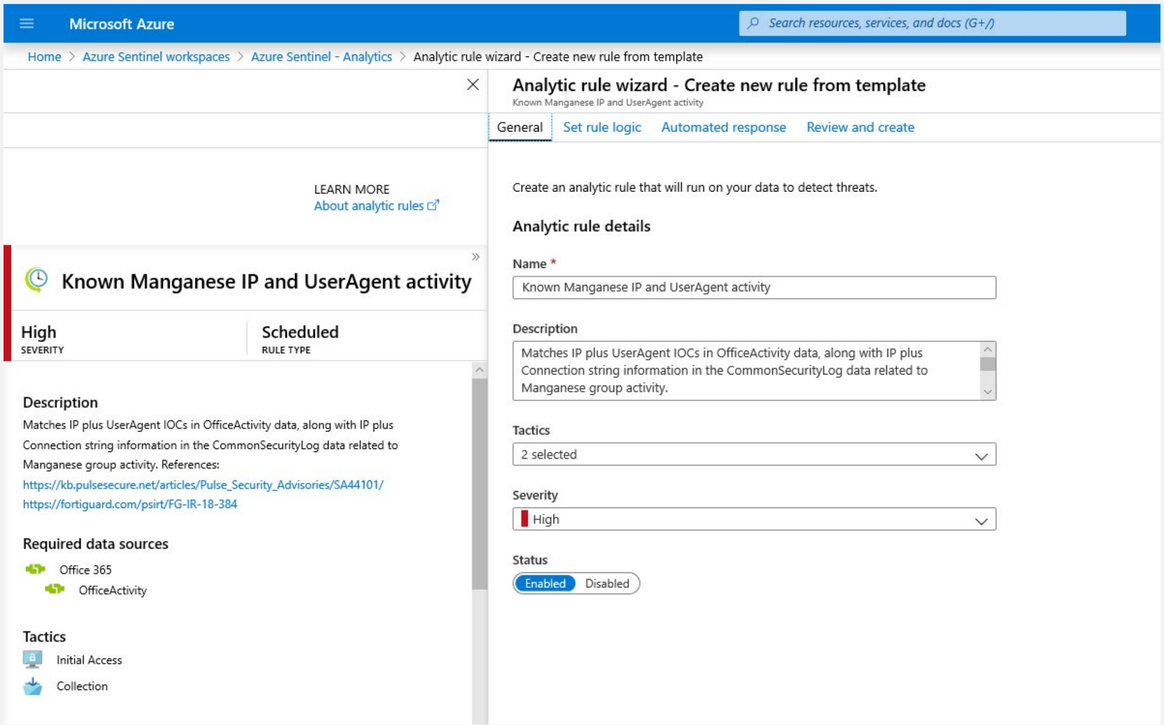
- You used this template to create 1 analytics rules and can use it to create additional rules.

Azure Sentinel analytics options.

To view all the out-of-the-box detection templates available in Azure Sentinel, go to **Analytics** and then **Rule templates**. This tab contains all the Azure Sentinel built-in rules.

Azure Sentinel comes with four types of rules built in.

- **Microsoft security:** Automatically create Azure Sentinel incidents from the alerts generated in other Microsoft security solutions in real time.
- **Fusion:** Correlate many low-fidelity alerts and events across multiple products into high-fidelity and actionable incidents. We will discuss Fusion in more detail in the next section.
- **Machine learning behavioral analytics:** Detect threats based on anomalies in user behavior.
- **Scheduled:** Deploy scheduled queries written by Microsoft security experts.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Azure Sentinel workspaces > Azure Sentinel - Analytics > Analytic rule wizard - Create new rule from template
LEARN MORE
About analytic rules
General
Set rule logic
Automated response
Review and create

Known Manganese IP and UserAgent activity

High SEVERITY | Scheduled RULE TYPE

Description
Matches IP plus UserAgent IOCs in OfficeActivity data, along with IP plus Connection string information in the CommonSecurityLog data related to Manganese group activity. References:
https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101/
https://fortiguard.com/psirt/FG-IR-18-384

Required data sources
Office 365
OfficeActivity

Tactics
Initial Access
Collection

Analytic rule wizard - Create new rule from template
Known Manganese IP and UserAgent activity

Create an analytic rule that will run on your data to detect threats.

Analytic rule details

Name *: Known Manganese IP and UserAgent activity

Description: Matches IP plus UserAgent IOCs in OfficeActivity data, along with IP plus Connection string information in the CommonSecurityLog data related to Manganese group activity.

Tactics: 2 selected

Severity: High

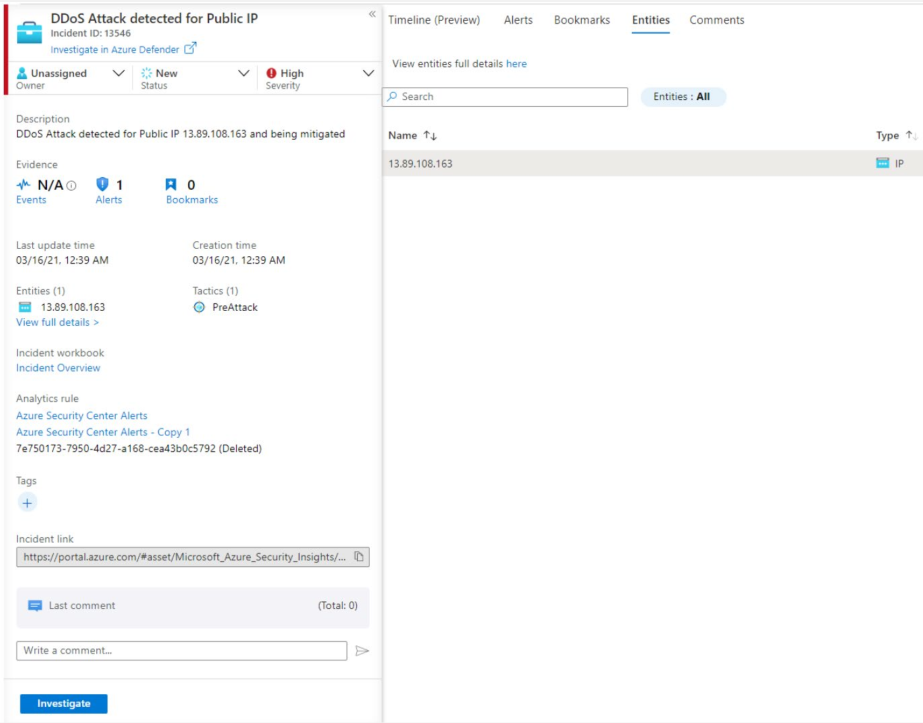
Status: ● Enabled ○ Disabled

The rule creation wizard.

To use a built-in template, click on **Create rule**. (Note that your rule options will be determined by your data sources.)

This opens the rule creation wizard, based on the selected template. All the details are automatically filled in. For **Scheduled rules** or **Microsoft security rules**, you can customize the logic to better suit your organization, or create additional rules based on the built-in template. The new rule appears in the **Active rules** tab.

In the following example, a pattern of anomalous sign-in activity. Azure Sentinel has applied behavioral analytics based on machine learning to identify the anomaly.



DDoS Attack detected for Public IP
Incident ID: 13546
Investigate in Azure Defender

Owner: Unassigned
Status: New
Severity: High

Description
DDoS Attack detected for Public IP 13.89.108.163 and being mitigated

Evidence
N/A Events
1 Alerts
0 Bookmarks

Last update time
03/16/21, 12:39 AM

Creation time
03/16/21, 12:39 AM

Entities (1)
13.89.108.163
View full details >

Tactics (1)
PreAttack

Incident workbook
Incident Overview

Analytics rule
Azure Security Center Alerts
Azure Security Center Alerts - Copy 1
7e750173-7950-4d27-a168-cea43b0c5792 (Deleted)

Tags

Incident link
https://portal.azure.com/#asset/Microsoft_Azure_Security_Insights/...

Last comment (Total: 0)

Write a comment...

View entities full details here

Entities : All

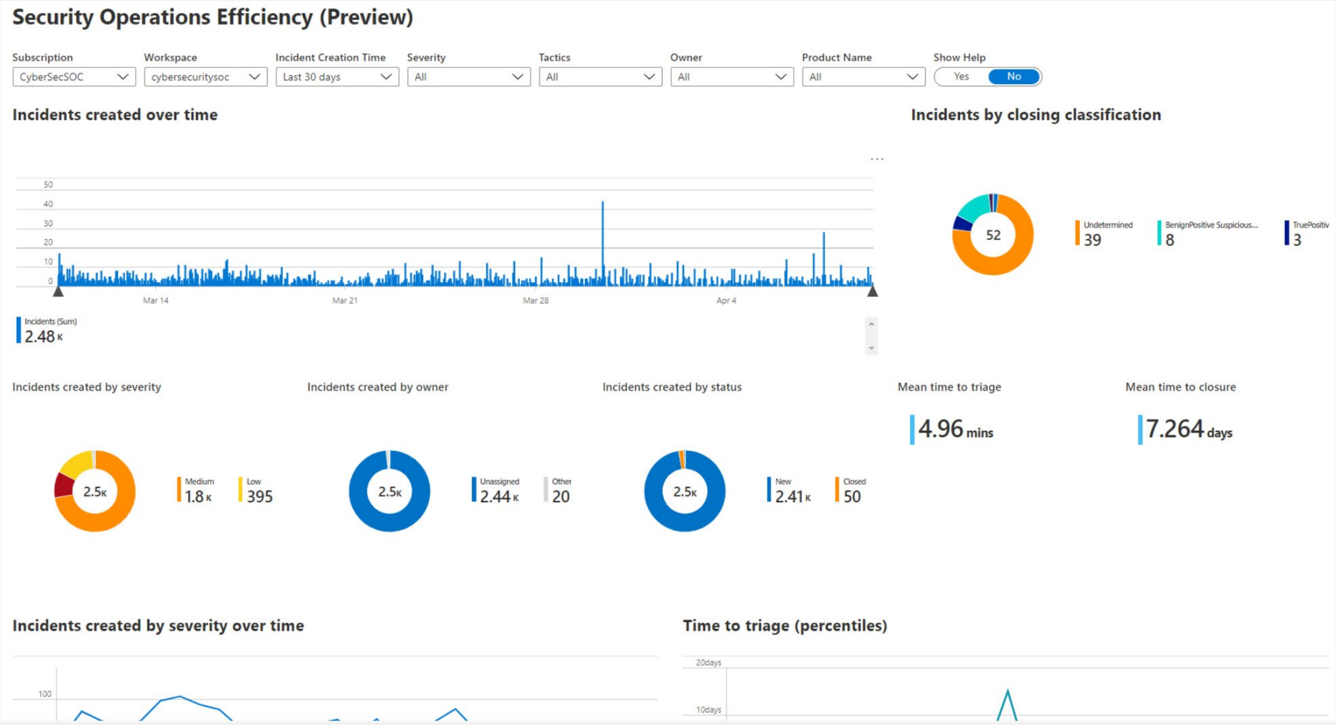
Name	Type
13.89.108.163	IP

An incident in Azure Sentinel.

You can use Azure Sentinel in a number of ways to investigate and respond. For example, you can explore your security data and detected issues using built-in workbooks, which are collections of visualizations that make it easy to get a bird’s eye view of your enterprise security posture.

You can also create playbooks to automatically respond to threats.

Finally, you can use investigation tools to explore incidents and better understand the most effective response. We will look at some of these tools in section three of this guide.

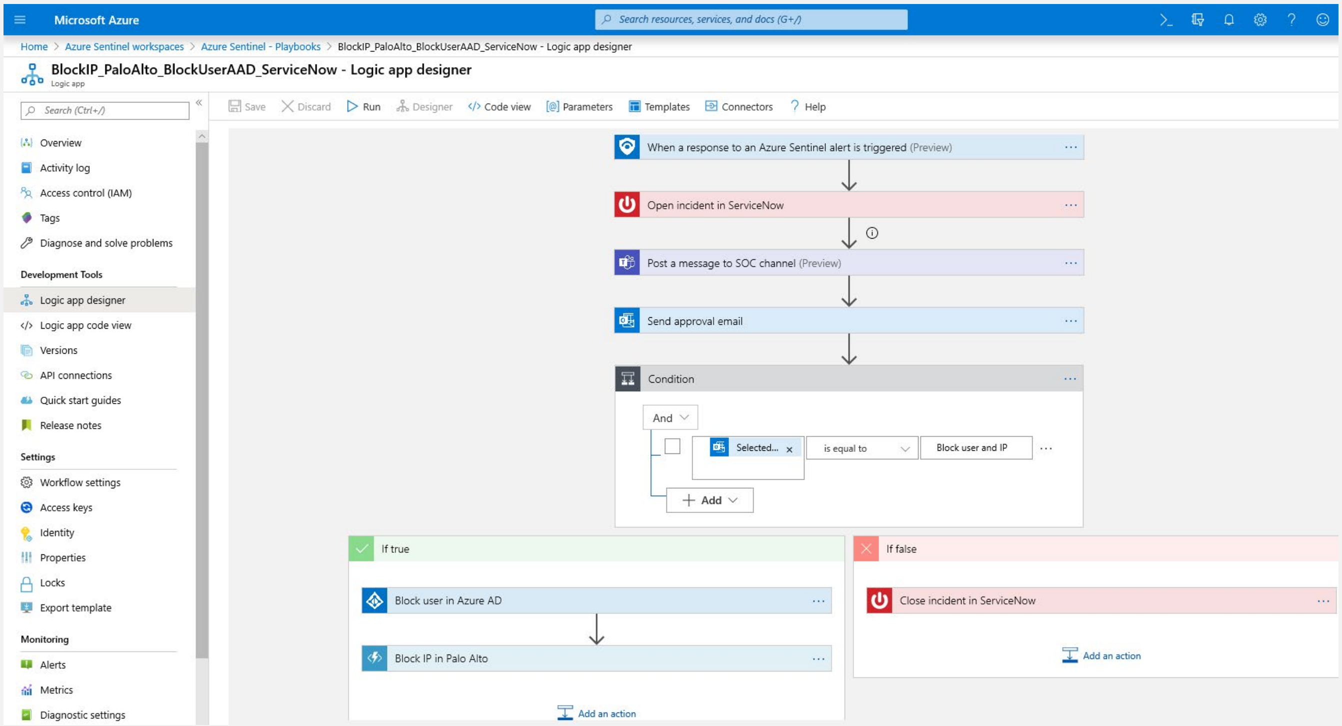


Security Operations Efficiency (Preview)

Subscription: CyberSecSOC
Workspace: cybersecuritysoc
Incident Creation Time: Last 30 days
Severity: All
Tactics: All
Owner: All
Product Name: All
Show Help: Yes [✓ No]

Incidents created over time
50
40
30
20
10
0
Mar 14
Mar 21
Mar 28
Apr 4
Incidents (Sum)
2.48K
Incidents by closing classification
52
Undetermined 39
BenignPositive Suspicious... 8
TruePositiv 3
Incidents created by severity
2.5K
Medium 1.8K
Low 395
Incidents created by owner
2.5K
Unassigned 2.44K
Other 20
Incidents created by status
2.5K
New 2.41K
Closed 50
Mean time to triage
4.96 mins
Mean time to closure
7.264 days
Incidents created by severity over time
100
Time to triage (percentiles)
20days
10days

An Azure Sentinel workbook.



When a response to an Azure Sentinel alert is triggered (Preview)

Open incident in ServiceNow

Post a message to SOC channel (Preview)

Send approval email

Condition

And
Selected... | is equal to | Block user and IP
+ Add

If true
Block user in Azure AD
Block IP in Palo Alto

If false
Close incident in ServiceNow

Playbook logic used to automate threat response.

Use case #2:
Prioritizing alerts into incidents

Using alerts to identify significant issues requires intelligent correlation—a capability built into Azure Sentinel

As the amount of data flowing in and out of your enterprise grows, and as IT becomes more complex and interrelated, the volume of alerts your security team must deal with can become hard to manage. Unfortunately, a substantial proportion of the alerts generated by security solutions are of little value individually. Using them to identify significant issues requires intelligent correlation—a capability built into Azure Sentinel.

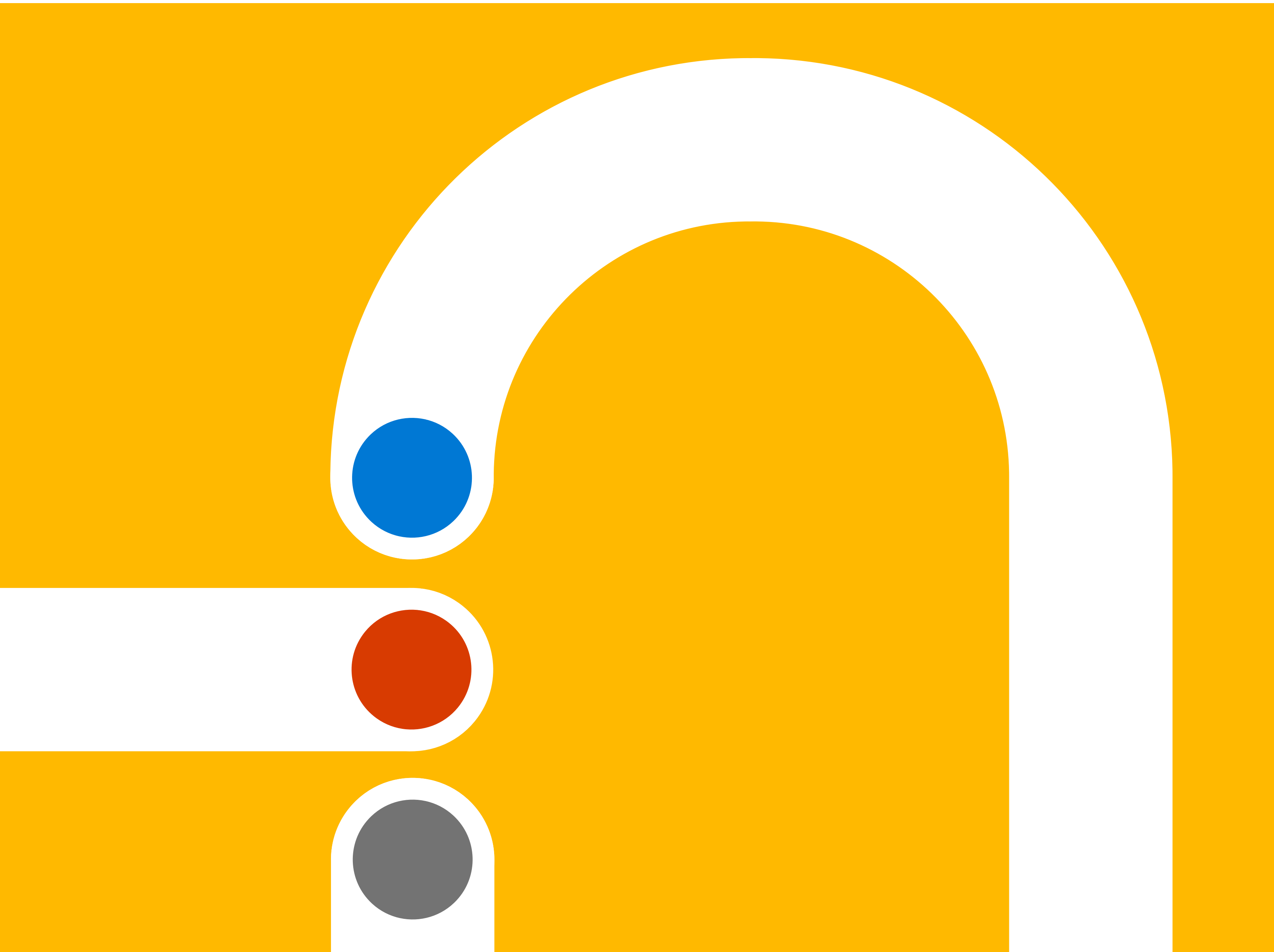
Known as advanced multistage attack detection, this capability minimizes the expertise needed to triage alerts and employs advanced machine learning to accurately identify real threats and minimize false positives by up to 90 percent. Each incident is prioritized to focus security professionals on the most relevant information.

Depending on the data sources you have connected, you can identify a wide variety of anomalous scenarios. For example, if you are using Azure Active Directory Identity Protection and Microsoft Cloud App Security, Azure Sentinel could identify that a user attempted to sign in from a location that would be impossible to reach since their last attempt. It could also identify that the location is not typical for that user. Then, it would correlate that information with anomalous Office 365 activity, such as downloading a large amount of information from the account.

This could indicate unauthorized sign-in activity using stolen credentials, followed by data theft. Individually, alerts generated by these activities might be lost in a large volume of trivial alerts. With Azure Sentinel, they are correlated into a high-impact incident that can generate an automatic response and trigger subsequent investigation. Best of all, advanced multistage attack detection is enabled by default inside of Azure Sentinel. You don’t need to do anything special to benefit from this feature.

Use case #3:

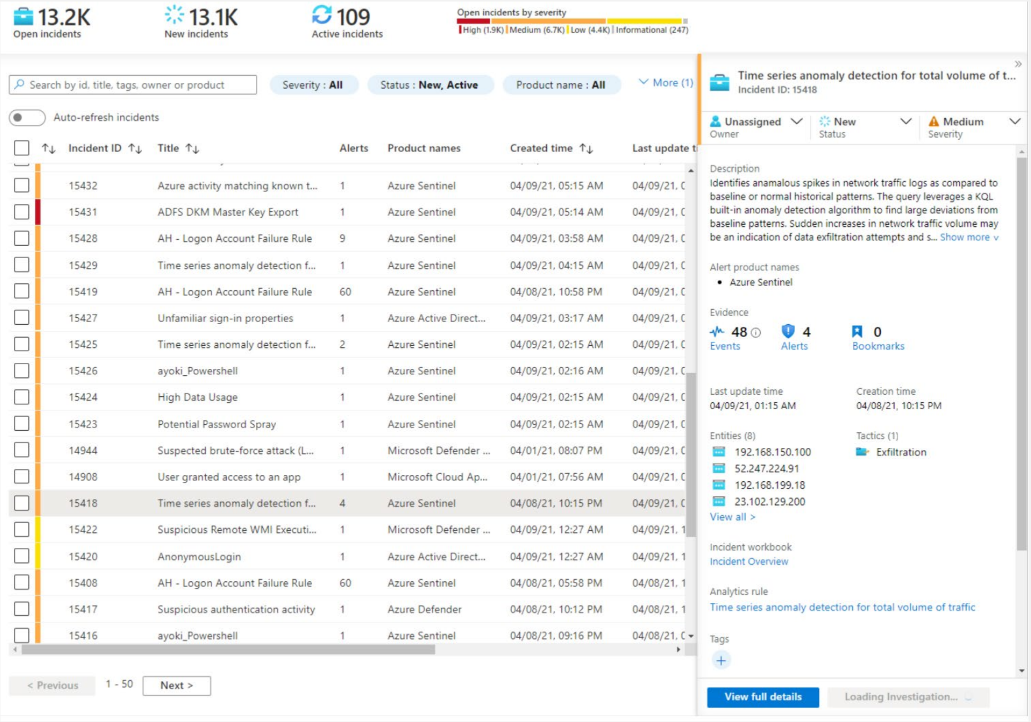
Investigating threats



Azure Sentinel provides your security team with powerful, intuitive tools for investigating threats rapidly and accurately identifying the most effective response

By understanding the root cause of complex threats, you can take steps to minimize future risk.

These tools are highly intuitive and easy to use, meaning you can engage more of your team on analysis that once would have been the sole province of highly trained experts. The tools are visual and graph-based, empowering individuals to investigate without having to write complex queries (although rich query-based hunting is also an option for true Tier 3 analysts). Second, they provide a guided experience that helps quickly zero in on the most important aspects of a threat. Azure Sentinel investigation tools were built by Microsoft researchers based on analyst best practices and can also be used to hunt for undetected threats.



13.2K Open incidents | 13.1K New incidents | 109 Active incidents

Open incidents by severity: High (1.9K) | Medium (6.7K) | Low (4.4K) | Informational (247)

Search by id, title, tags, owner or product | Severity : **All** | Status : **New, Active** | Product name : **All** | More (1)

Auto-refresh incidents

□		Incident ID	Title	Alerts	Product names	Created time	Last update t
□	🟧	15432	Azure activity matching known t...	1	Azure Sentinel	04/09/21, 05:15 AM	04/09/21, C
□	🟥	15431	ADFS DKM Master Key Export	1	Azure Sentinel	04/09/21, 05:14 AM	04/09/21, C
□	🟧	15428	AH - Logon Account Failure Rule	9	Azure Sentinel	04/09/21, 03:58 AM	04/09/21, C
□	🟧	15429	Time series anomaly detection f...	1	Azure Sentinel	04/09/21, 04:15 AM	04/09/21, C
□	🟧	15419	AH - Logon Account Failure Rule	60	Azure Sentinel	04/08/21, 10:58 PM	04/09/21, C
□	🟧	15427	Unfamiliar sign-in properties	1	Azure Active Direct...	04/09/21, 03:17 AM	04/09/21, C
□	🟧	15425	Time series anomaly detection f...	2	Azure Sentinel	04/09/21, 02:15 AM	04/09/21, C
□	🟧	15426	ayoki_Powershell	1	Azure Sentinel	04/09/21, 02:16 AM	04/09/21, C
□	🟧	15424	High Data Usage	1	Azure Sentinel	04/09/21, 02:15 AM	04/09/21, C
□	🟧	15423	Potential Password Spray	1	Azure Sentinel	04/09/21, 02:15 AM	04/09/21, C
□	🟧	14944	Suspected brute-force attack (L...	1	Microsoft Defender ...	04/01/21, 08:07 PM	04/09/21, C
□	🟧	14908	User granted access to an app	1	Microsoft Cloud Ap...	04/01/21, 07:56 AM	04/09/21, C
□	🟧	15418	Time series anomaly detection f...	4	Azure Sentinel	04/08/21, 10:15 PM	04/09/21, C
□	🟨	15422	Suspicious Remote WMI Executi...	1	Microsoft Defender ...	04/09/21, 12:27 AM	04/09/21, 1
□	🟨	15420	AnonymousLogin	1	Azure Active Direct...	04/09/21, 12:27 AM	04/09/21, 1
□	🟧	15408	AH - Logon Account Failure Rule	60	Azure Sentinel	04/08/21, 05:58 PM	04/08/21, 1
□	🟧	15417	Suspicious authentication activity	1	Azure Defender	04/08/21, 10:12 PM	04/08/21, 1
□	🟧	15416	ayoki_Powershell	1	Azure Sentinel	04/08/21, 09:16 PM	04/08/21, C

< Previous | 1 - 50 | Next >

Time series anomaly detection for total volume of t...
Incident ID: 15418

Owner: Unassigned | Status: New | Severity: Medium

Description
Identifies anamalous spikes in network traffic logs as compared to baseline or normal historical patterns. The query leverages a KQL built-in anomaly detection algorithm to find large deviations from baseline patterns. Sudden increases in network traffic volume may be an indication of data exfiltration attempts and s... Show more

Alert product names
- Azure Sentinel

Evidence
48 Events | 4 Alerts | 0 Bookmarks

Last update time
04/09/21, 01:15 AM

Creation time
04/08/21, 10:15 PM

Entities (8)
192.168.150.100
52.247.224.91
192.168.199.18
23.102.129.200
View all >

Tactics (1)
Exfiltration

Incident workbook
Incident Overview

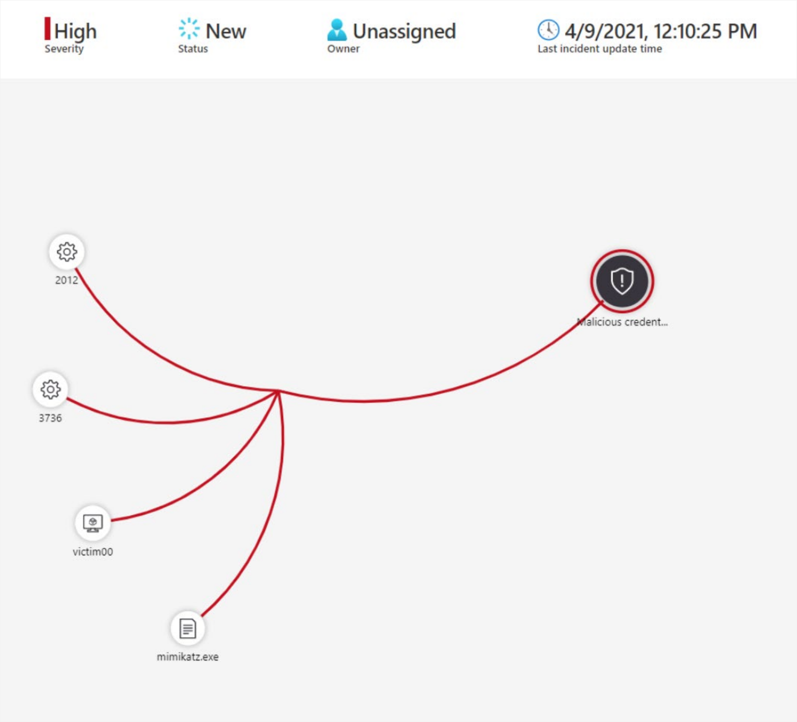
Analytics rule
Time series anomaly detection for total volume of traffic

Tags

The Azure Sentinel incidents page.

The Incidents page is your starting point. It shows the basic details of each incident, including severity, to help you decide which to investigate first.

Simply select an incident to begin your investigation. You can view more details, the alerts that were generated, and drill down into underlying events. You can also assign an incident to an individual and add comments as the investigation proceeds.



High
Severity

New
Status

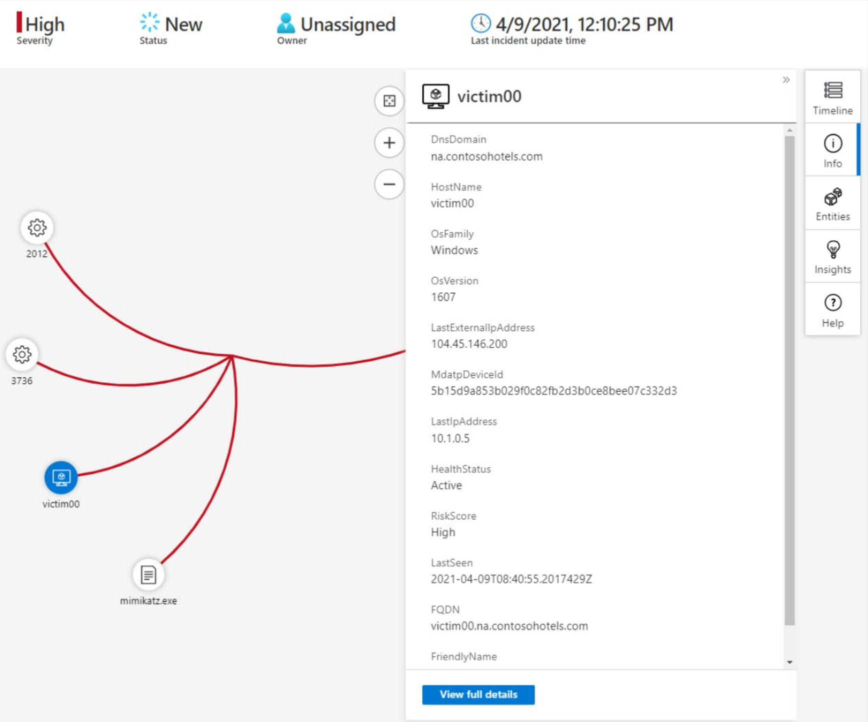
Unassigned
Owner

4/9/2021, 12:10:25 PM
Last incident update time

The Azure Sentinel investigation graph.

To dive deeper into an incident, you can use the investigation graph to:

- **Easily see connections across different data sources** using a visual graph generated automatically from the raw data.
- **Expand your investigation scope** using built-in exploration queries to surface the full scope of a breach.
- **Use predefined exploration options** to make sure you are asking the right questions in the face of a threat.



High
Severity

New
Status

Unassigned
Owner

4/9/2021, 12:10:25 PM
Last incident update time

victim00

DnsDomain
na.contosohotels.com

HostName
victim00

OsFamily
Windows

OsVersion
1607

LastExternalIpAddress
104.45.146.200

MdatpDeviceId
5b15d9a853b029f0c82fb2d3b0ce8bee07c332d3

LastIpAddress
10.1.0.5

HealthStatus
Active

RiskScore
High

LastSeen
2021-04-09T08:40:55.2017429Z

FQDN
victim00.na.contosohotels.com

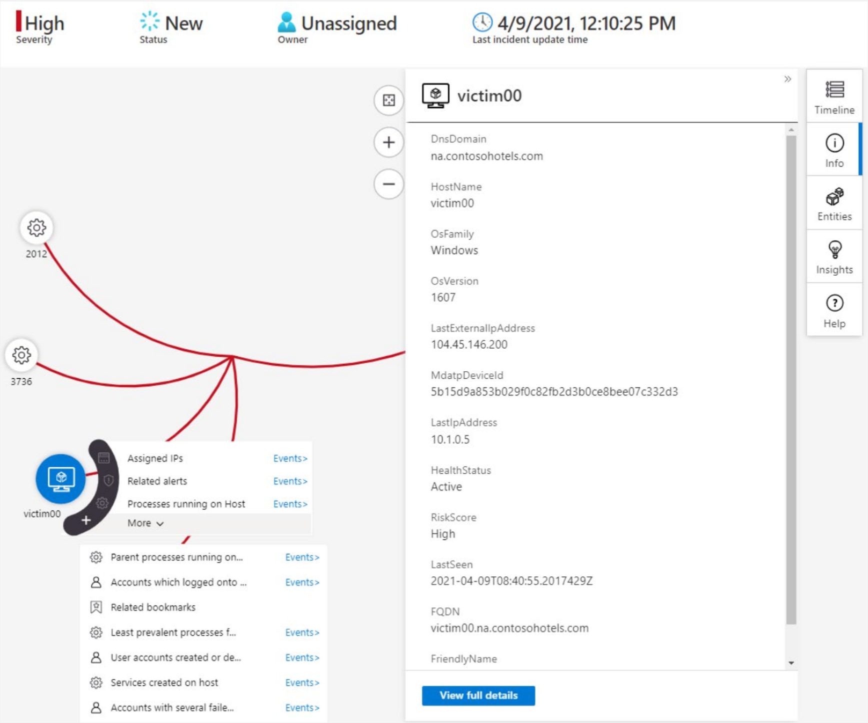
FriendlyName

Exploring an entity with the Entities pane.

To use the investigation graph, select an incident, then select **Investigate**. This takes you to the investigation graph.

Select an entity to open the **Entities** pane so you can review information on that entity.

Hovering over each entity reveals a list of **exploration queries** designed by our security experts to deepen your investigation.


2012
3736
victim00
Assigned IPs Events>
Related alerts Events>
Processes running on Host Events>
More
Parent processes running on... Events>
Accounts which logged onto ... Events>
Related bookmarks
Least prevalent processes f... Events>
User accounts created or de... Events>
Services created on host Events>
Accounts with several faile... Events>
Timeline
Info
Entities
Insights
Help
View full details

High
Severity

New
Status

Unassigned
Owner

4/9/2021, 12:10:25 PM
Last incident update time

victim00

DnsDomain
na.contosohotels.com

HostName
victim00

OsFamily
Windows

OsVersion
1607

LastExternalIpAddress
104.45.146.200

MdatpDeviceId
5b15d9a853b029f0c82fb2d3b0ce8bee07c332d3

LastIpAddress
10.1.0.5

HealthStatus
Active

RiskScore
High

LastSeen
2021-04-09T08:40:55.2017429Z

FQDN
victim00.na.contosohotels.com

FriendlyName

Suggested exploration queries.

You can also view related alerts, look in detail at the associated events and queries, and explore a timeline of events. All of these capabilities are point-and-click simple yet offer powerful insights into the nature of the threats you face. After an investigation is complete, you can respond to threats quickly using playbooks.

A security playbook is a collection of procedures that can be run from Azure Sentinel in response to an alert. It helps automate and orchestrate your response and can be run manually or set to run automatically when specific alerts are triggered. **Learn more about playbooks**.

These tools are highly intuitive and easy to use, meaning you can engage more of your team on analysis that once would have been the sole province of highly trained experts. The tools are visual and graph-based, empowering individuals to investigate without having to write complex queries.”

Try Azure Sentinel today

No infrastructure investment. Powerful AI built in. Tools for every role. Virtually unlimited scalability. All backed by Microsoft security research. If you're looking to improve the security posture of your enterprise while simplifying security operations, consider Azure Sentinel.

See how fast, easy, and inexpensive it is to get started.

Talk to an Azure Specialist about Azure Sentinel now >

Microsoft