

Threat Protection Solutions for Microsoft 365



Vlad Catrinescu

Microsoft MVP

@vladcatrinescu <https://VladTalksTech.com>



Overview



Introduction to SIEM, SOAR, & XDR

Microsoft 365 Defender

- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Defender for Endpoint

Microsoft Sentinel



Introduction to SIEM, SOAR, & XDR



Set of Security Tools

SIEM

Security Incident and Event Management

SOAR

Security Orchestration Automated Response

XDR

Extended Detection and Response



Security Incident and Event Management



Collect data from your digital estate

- Infrastructure
- Software
- Resources

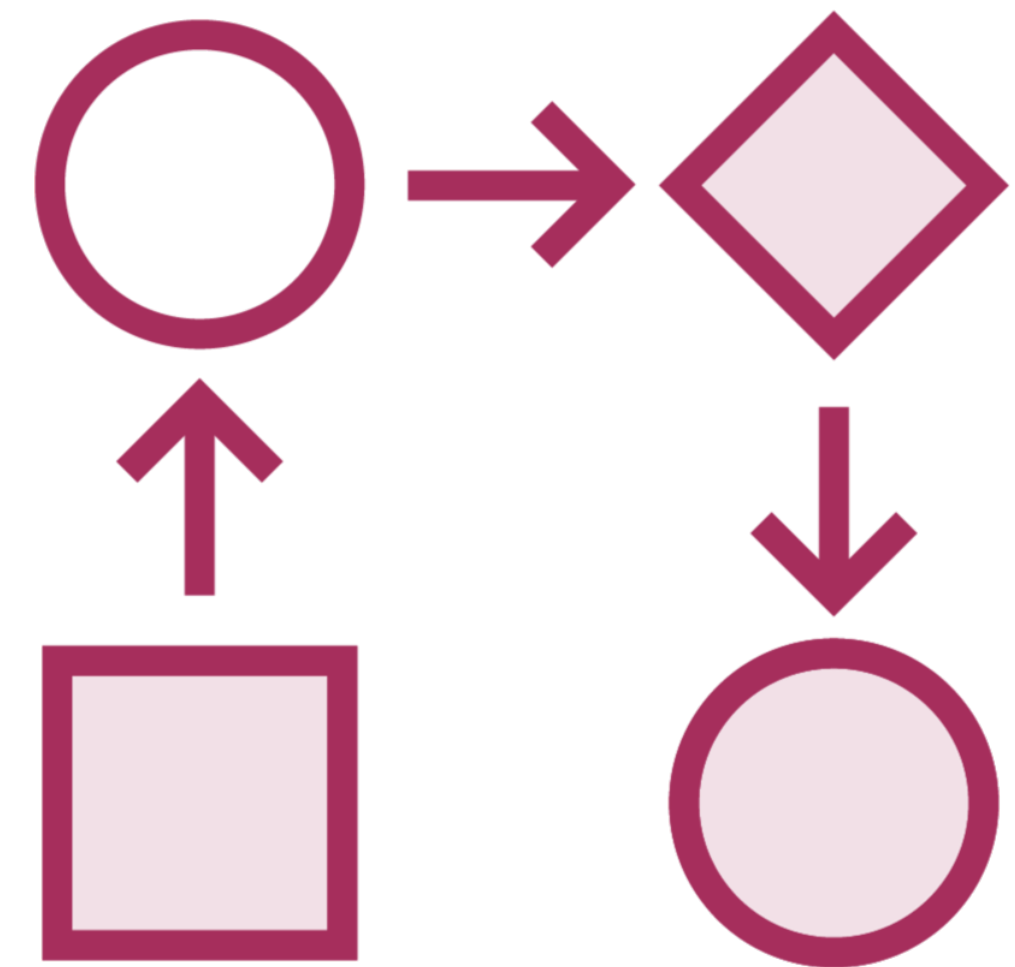
Analyzes data and looks for correlations or anomalies

Generates alerts and incidents

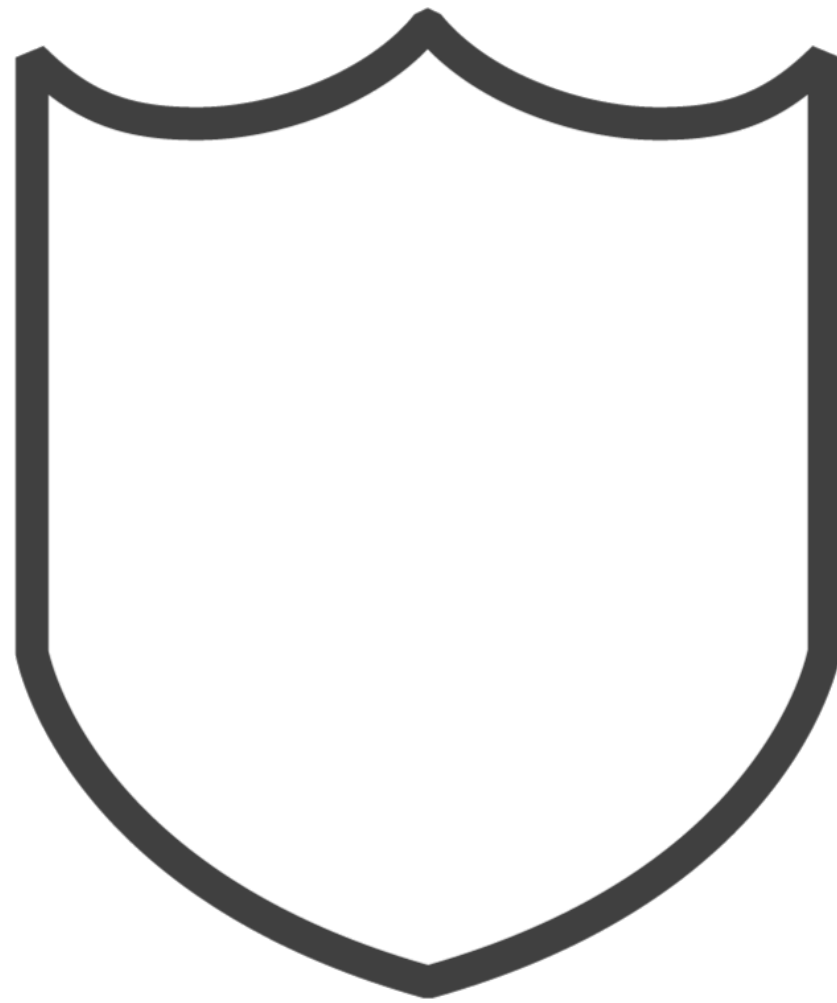
Security Orchestration Automated Response

Collects data from many sources
Similar to a SIEM system

Able to trigger automated workflows to mitigate the issue



Extended Detection and Response



Security threat detection and incident response tool

- Identities**
- Endpoints**
- Applications**
- E-mail**
- Infrastructure**



Microsoft Products

SIEM

Microsoft Sentinel

SOAR

Microsoft Sentinel

XDR

Microsoft 365 Defender



Microsoft 365 Defender



Microsoft 365 Defender

Microsoft 365 Defender is a unified pre- and post-breach enterprise defense suite that natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks.



Microsoft 365 Defender



**Microsoft
Defender for
Endpoint**



**Microsoft
Defender for
Office 365**



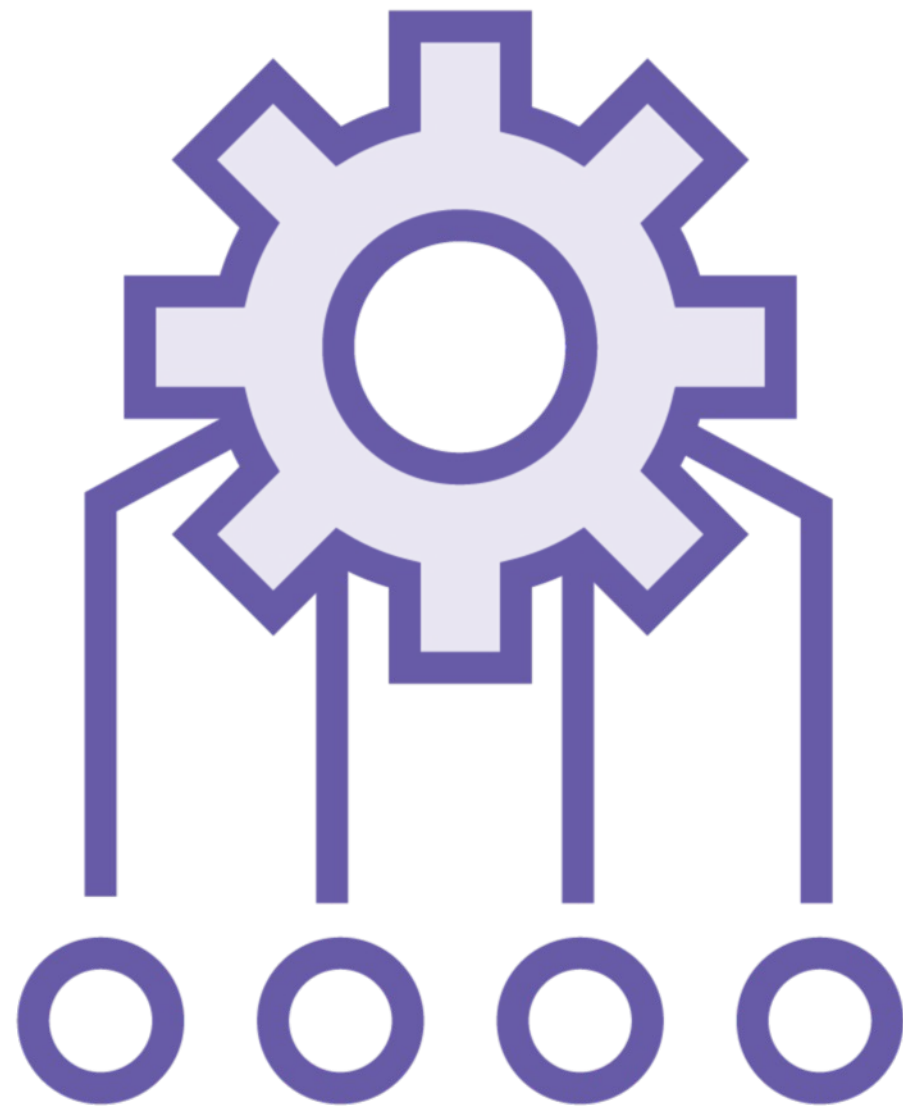
**Microsoft
Defender for
Identity**



**Microsoft
Defender for
Cloud Apps**



An Integrated Solution



Microsoft 365 Defender is an integrated – cross domain solution

- **Stiches together signals from**
 - **Endpoints**
 - **Identities**
 - **Data**
 - **Applications**
- **Groups signals from all domains in incidents**
 - **Allows security teams to see the full picture**



Microsoft 365 Defender Incident

Microsoft 365 Defender

Search

Settings Help Profile

Incidents > Multi-stage incident involving Initial access & Collection on multiple endpoints reported by multiple sources

Multi-stage incident involving Initial ...

Ask Defender Experts Comments and history

This incident is read-only because it contains alerts from service sources that you do not have permissions to view/manage. Contact a global admin for access

Summary Alerts (18) Devices (2) Users (5) Mailboxes (5) Apps (3) Investigations (4) Evidence and Response (22) Graph

Alerts and categories

18/18 active alerts
4 MITRE ATT&CK tactics
1 other alert categories

© 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

Scope

2 impacted devices
5 impacted users
5 impacted mailboxes
3 impacted apps

Top impacted entities

| Entity type | Risk level/investigation priority | Tags |
|---------------------|-----------------------------------|-----------|
| workstation14 | High | Exec Sec |
| workstation15 | High | HVA Sec |
| oking | 212 | All Users |
| kelsea | 79 | All Users |
| cjones@seccxp.ninja | No data available | |

Incident Information

This incident is read-only because it contains alerts from service sources that you do not have permissions to view/manage. Contact a global admin for access

Tags summary

Incident tags

Chain Event Detection BEC CAttack MDO Demo Exec HVA SecCxpNinja TEST

User groups

All Users SocTeam All Users SocTeam

Incident details

Status Active

Jul 26, 2022, 7:23:30 PM | New User accessed link in ZAP-...



Microsoft 365 Defender Portal

Central location for monitoring and managing security across your Microsoft

Identities

Data

Devices

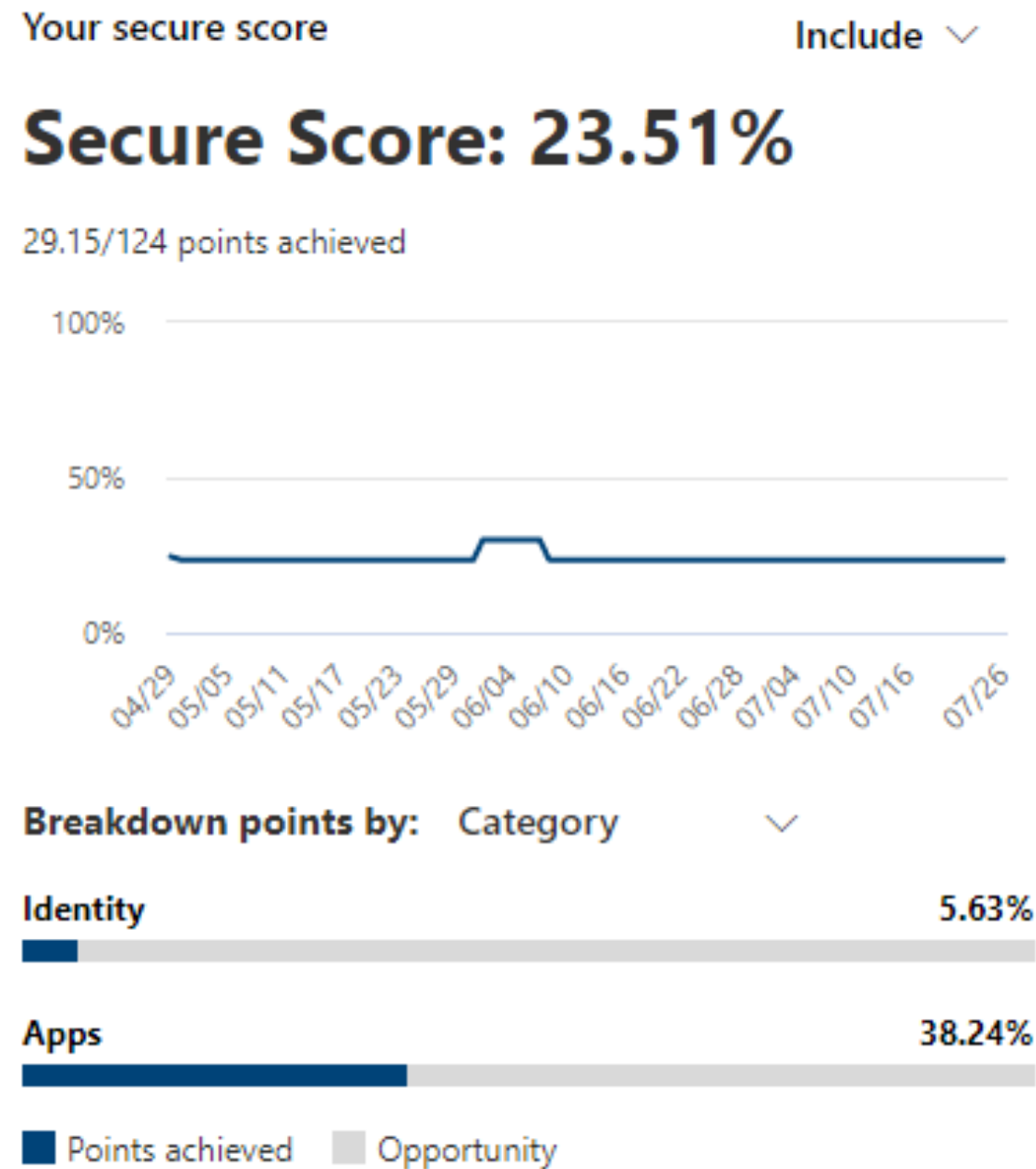
Apps

Infrastructure

Accessible at <https://security.microsoft.com>



Microsoft Secure Score



Quick way to understand your security posture

Helps prioritize actions based on potential to reduce risk

– Bigger the security impact – more points



Microsoft Secure Score Recommendations

Microsoft 365

**Azure Active
Directory**

**Microsoft Defender
for Endpoint**

**Microsoft Defender
for Identity**

**Microsoft Defender
for Cloud Apps**



Demo



Microsoft 365 Defender Portal

Microsoft Secure Score



Microsoft Defender for Identity



Microsoft Defender for Identity

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 Key Areas

Monitor and profile user behavior and activities

Protect user identities and reduce the attack surface

Identify suspicious activities and advanced attacks across the cyber-attack kill-chain

Investigate alerts and user activities



Monitor and Profile User Behavior and Activities



Monitors and analyzes

- User activities**
- Permissions**
- Group membership**

Creates a behavioral baseline for each user

Identify anomalies in user behavior

- Insights into suspicious activities and events**

Protect User Identities and Reduce the Attack Surface

Insights on identity configurations and security best practices

Reduce your organizational attack surface

Visual Lateral Movement Paths

Quickly understand how attackers can move laterally inside your network

Security reports to identify users & devices authenticating with clear-text passwords



Identify Suspicious Activities and Advanced Attacks

Reconnaissance

Identify rogue users and attackers' attempts to gain information

Compromised credentials

Identify attempts to compromise user credentials using brute force attacks, failed authentications, and other methods

Lateral movements

Detect attempts to move laterally inside the network to gain further control of sensitive users.

Domain dominance

Highlighting attacker behavior if domain dominance is achieved, through remote code execution on the domain controller and other methods



Investigate Alerts and User Activities



Provide only relevant security alerts

Real-time organizational attack timeline



Microsoft Defender for Office 365



Microsoft Defender for Office 365 Key Areas

Threat protection policies

Reports

**Threat investigation and
response capabilities**

**Automated investigation and
response capabilities**



Threat Protection Policies

Safe Attachments

Provides zero-day protection to safeguard your messaging system, by checking email attachments for malicious content

Safe Links

Provides time-of-click verification of URLs, for example, in emails messages and Office files

Anti-phishing protection

Detects attempts to impersonate your users and internal or custom domains

Safe Attachments for SharePoint, OneDrive, & Teams

Protects your organization when users collaborate and share files, by identifying and blocking malicious files in document libraries



Microsoft Defender for Office 365 Reports

Real-time reports to monitor performance

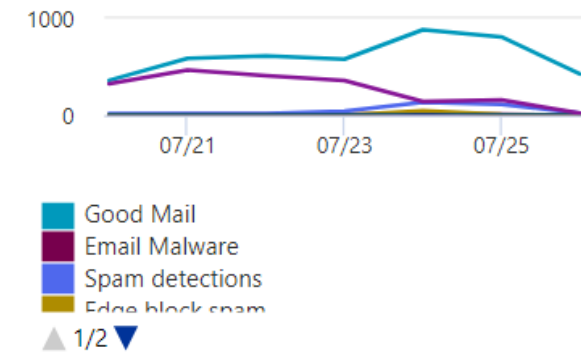
URL protection report

Threat protection status

User reported messages

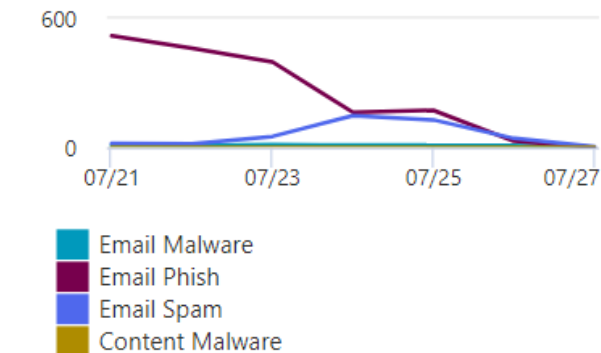
Email & collaboration reports

Mailflow status summary



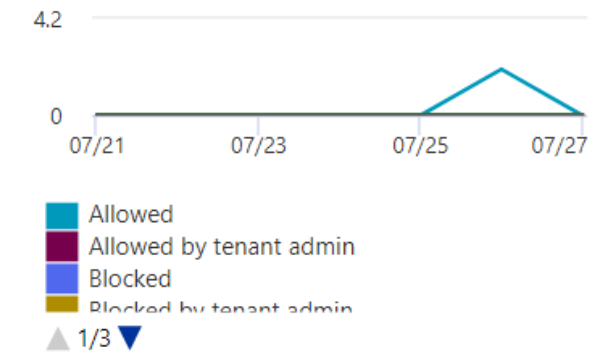
[View details](#)

Threat protection status



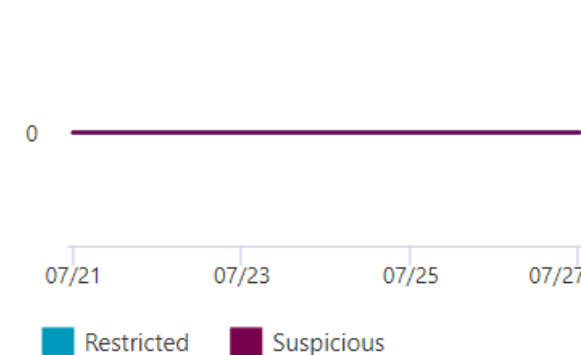
[View details](#)

URL protection report



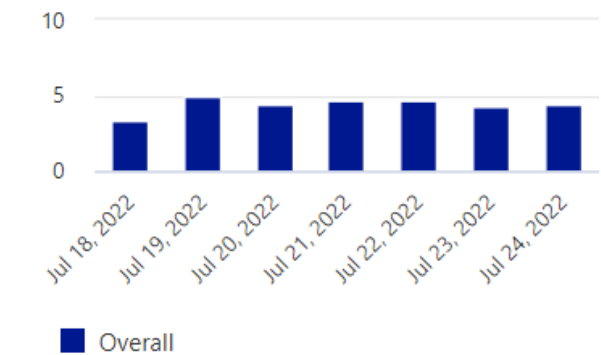
[View details](#)

Compromised users



[View details](#)

Mail latency report



[View details](#)

User reported messages



[View details](#)

[Go to Submissions](#)



Threat Investigation and Response Capabilities



Threat trackers

Threat explorer / real-time detections

- Identify and analyze recent threats

Attack simulator

- Run realistic attack scenarios in your organization
 - Spear phishing
 - Attachment attack
 - Password spray

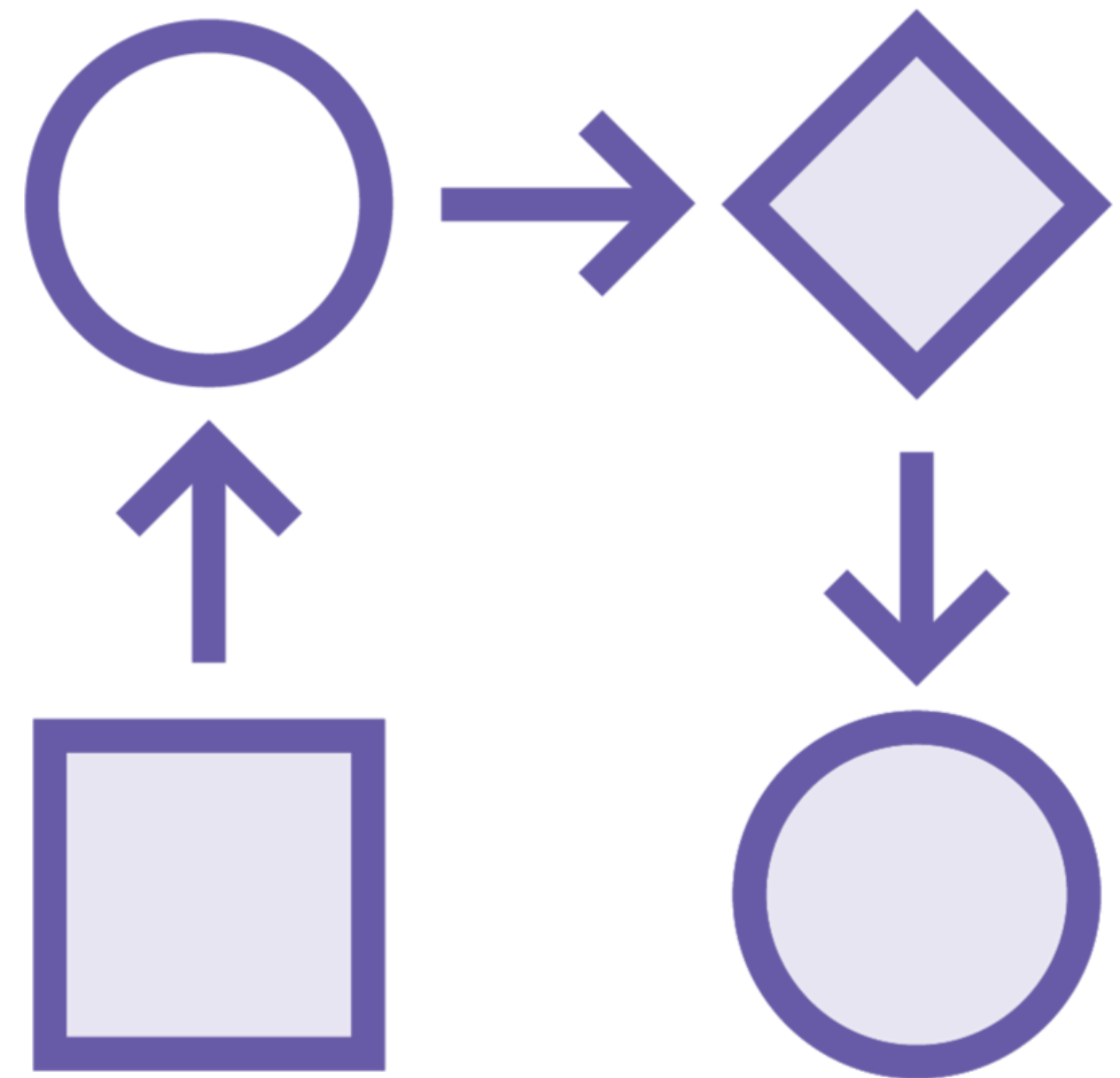
Automated Investigation and Response (AIR)

Set of security playbooks

Can be launched manually or automatically

Remediation actions are proposed

Security team approves or rejects them



Microsoft Defender for Endpoint



Microsoft Defender for Endpoint

Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.



Microsoft Defender for Endpoint Key Areas

**Threat &
Vulnerability
Management**

**Attack surface
reduction**

**Next-generation
protection**

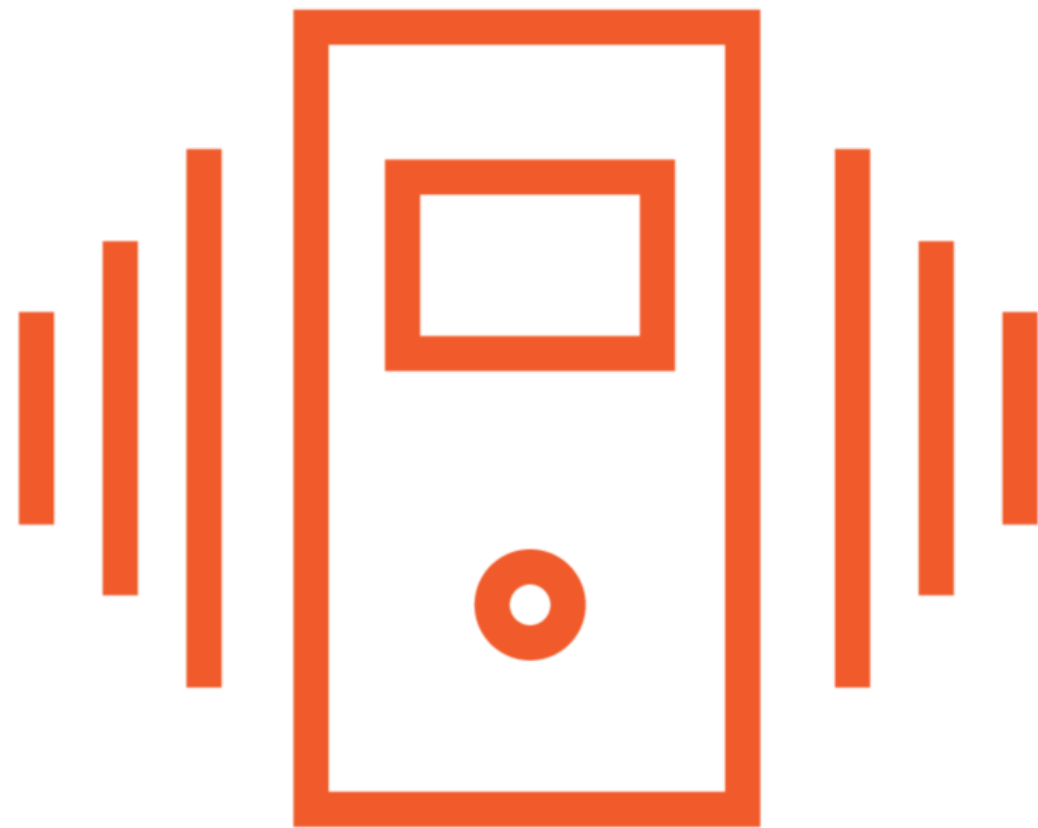
**Endpoint detection
and response**

**Automated
investigation and
remediation**

**Microsoft Threat
Experts**



Threat & Vulnerability Management



Risk-based approach to

- Discovery**
- Prioritization**
- And remediation of endpoint vulnerabilities**

Uses sensors for real-time discovery

- No agents / scans needed**

Attack Surface Reduction

Reduce the places where your organization is vulnerable

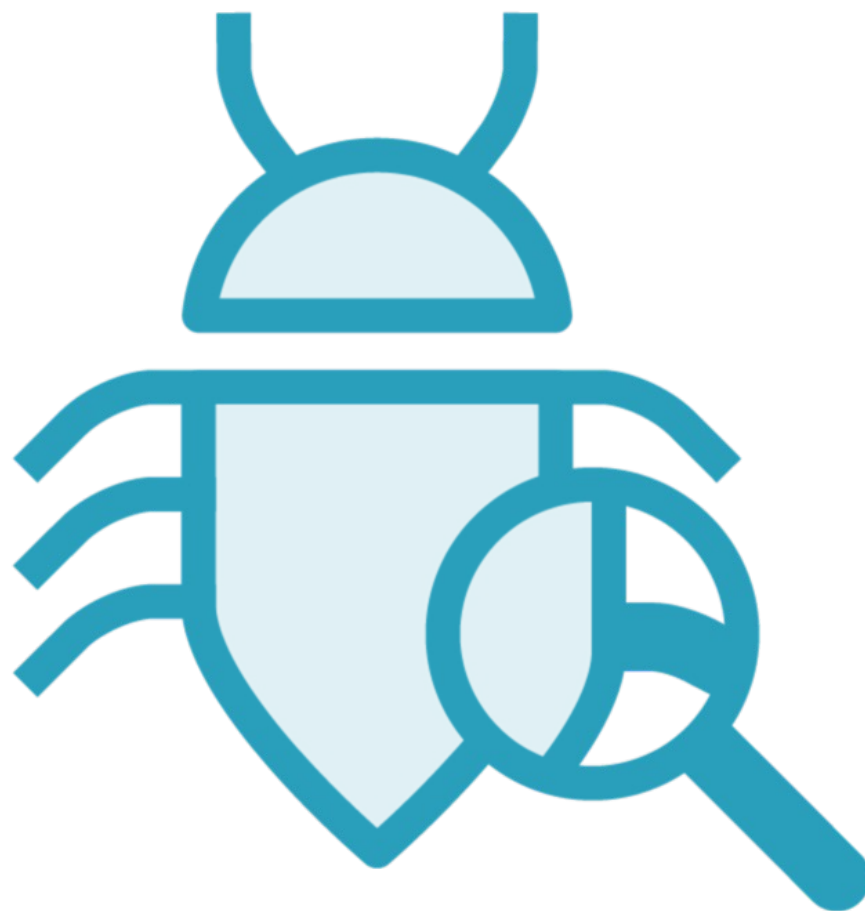
Provides a first line of defense

Ensures configurations are properly set

Network & web protection



Next-generation Protection



Microsoft Defender Antivirus

- Behavior-based & real-time antivirus protection
- Cloud-delivered protection
- Protection & product updates



Endpoint Detection and Response

Advanced attack detection

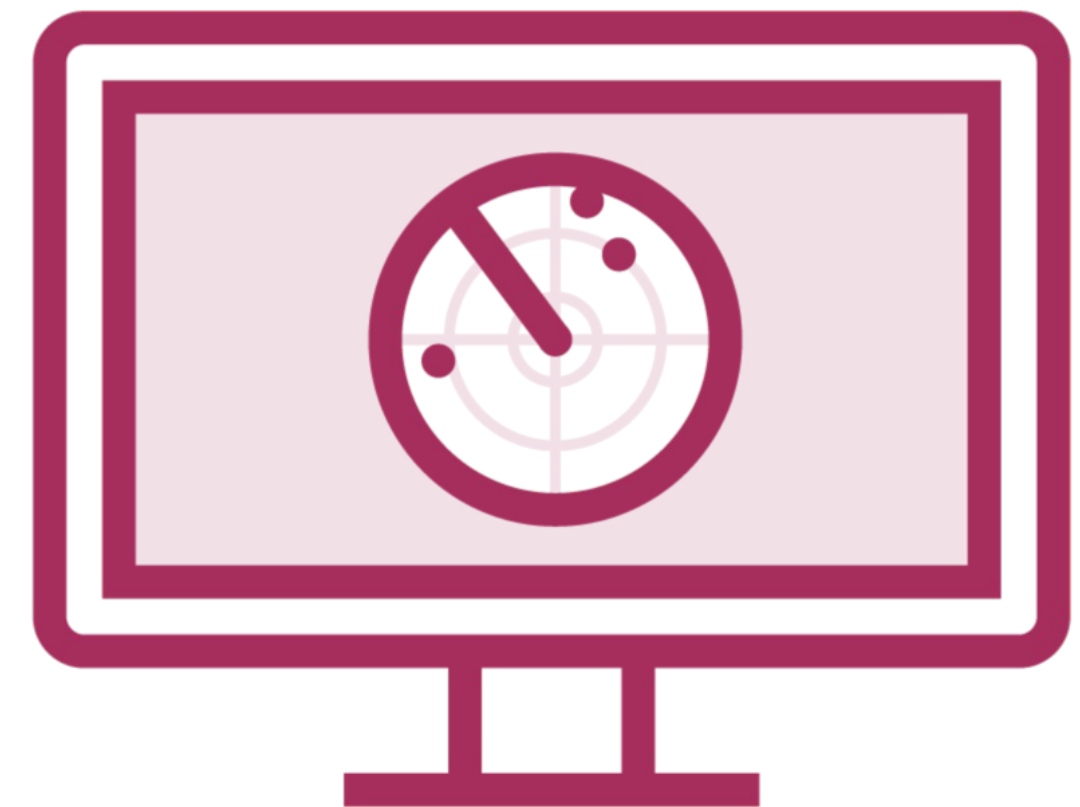
Near real-time

Actionable

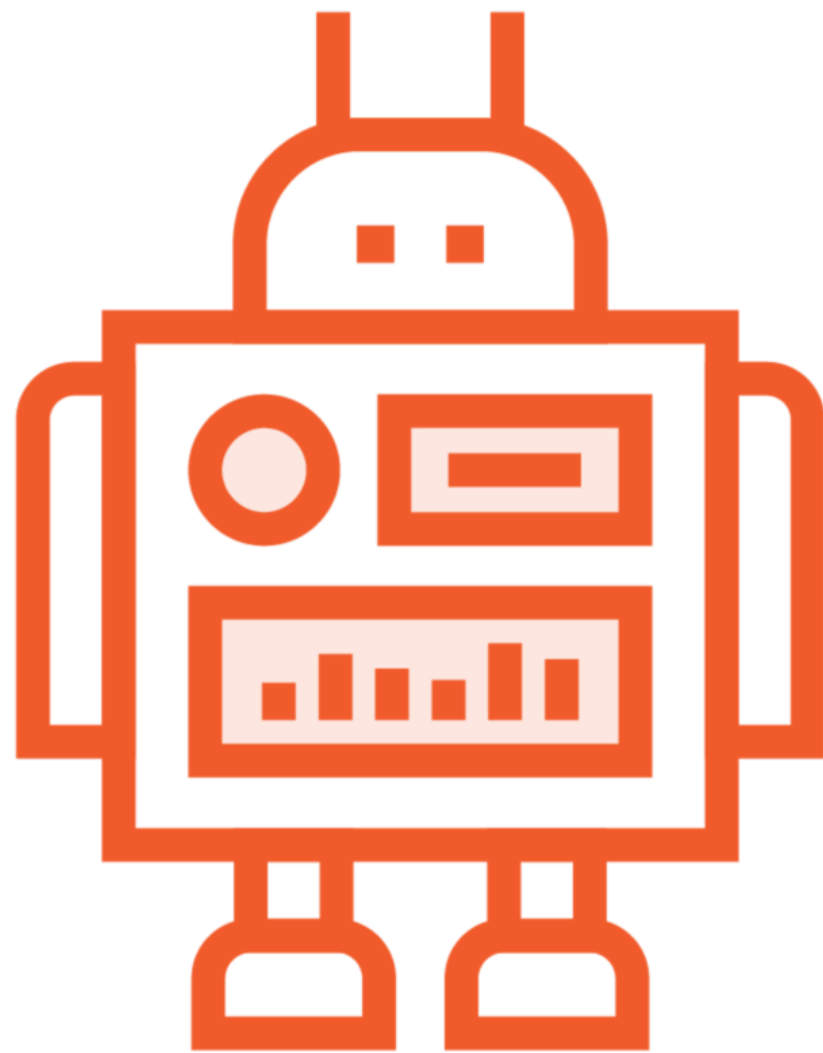
Prioritize alerts & gain visibility into the full scope of a breach

Alerts with same technique / attacker are aggregated into an incident

Easier to investigate and respond to a threat



Automated Investigation and Remediation (AIR)



Inspection algorithm and processes to examine alerts and take quick remediation

Remediation can occur automatically or only upon approval

- Depending on your organization configuration**



Microsoft Threat Experts

Managed threat hunting service

Expert level monitoring and analysis

Targeted attack notification

Access to experts on demand

Customers need to apply for the Microsoft Threat Experts program

Extra cost



Demo



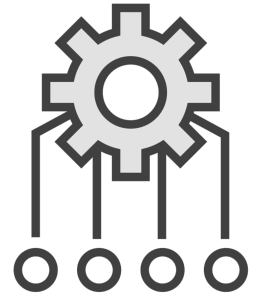
**Navigate an incident in the Microsoft 365
Defender dashboard**



Microsoft Sentinel



Microsoft Sentinel Functionality



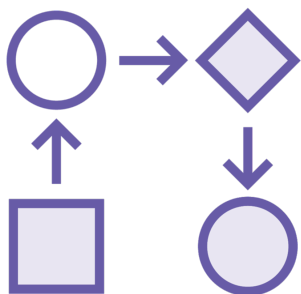
Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds



Detect previously uncovered threats and minimize false positives using analytics and unparalleled threat intelligence



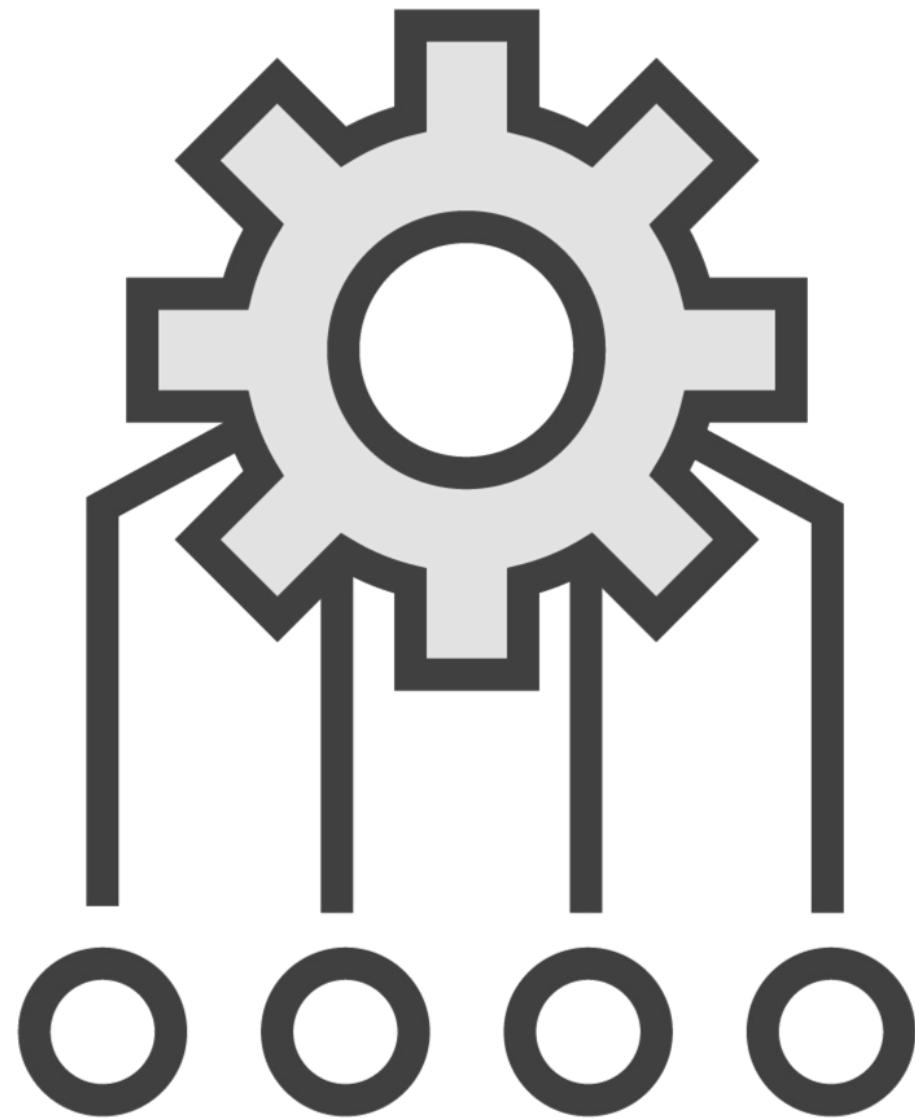
Investigate threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft



Respond to incidents rapidly with built-in orchestration and automation of common security tasks



Connect to All Your Data



Great number of built-in connectors

- **Microsoft Services**
 - Azure Active Directory
 - Microsoft 365 Defender
 - Office 365
- **External Solutions**
 - F5 BIG-IP
 - Okta SSO
 - Google Workspace



100+ Connectors Built-In

Microsoft Sentinel | Data connectors

Selected workspace: 'test'

Search (Ctrl+/)

Refresh

Guides & Feedback

General

Overview

Logs

News & guides

Search (Preview)

Threat management

Incidents

Workbooks

Hunting

Notebooks

Entity behavior

Threat intelligence

MITRE ATT&CK (Preview)

Content management

Content hub (Preview)

Repositories (Preview)

Community

Configuration

Data connectors

Analytics

Watchlist

Automation

Settings

123 Connectors

0 Connected












More content at Content hub


Search by name or provider

Providers : All


Data Types : All


Status : All

| Status | Connector name ↑ |
|--------|---|
| |  Agari Phishing Defense and Brand Protection (Preview) Agari |
| |  AI Analyst Darktrace (Preview) Darktrace |
| |  AI Vectra Detect (Preview) Vectra AI |
| |  Akamai Security Events (Preview) Akamai |
| |  Alcide kAudit (Preview) Alcide |
| |  Alsid for Active Directory (Preview) Alsid |
| |  Amazon Web Services Amazon |
| |  Amazon Web Services S3 (Preview) Amazon |
| |  Apache HTTP Server (Preview) Apache |
| |  Apache Tomcat (Preview) Apache |
| |  Aruba ClearPass (Preview) Aruba Networks |

 **Amazon Web Services**

Disconnected Status

 Amazon Provider

 -- Last Log Received


Description


Follow these instructions to connect to AWS and stream your CloudTrail logs into Microsoft Sentinel.


Last data received

--

Related content

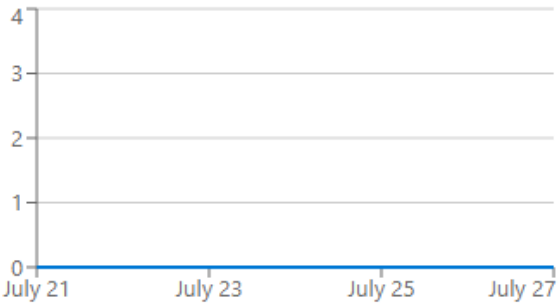
 2 Workbooks

 2 Queries

 21 Analytics rule template

Data received


Go to log analytics



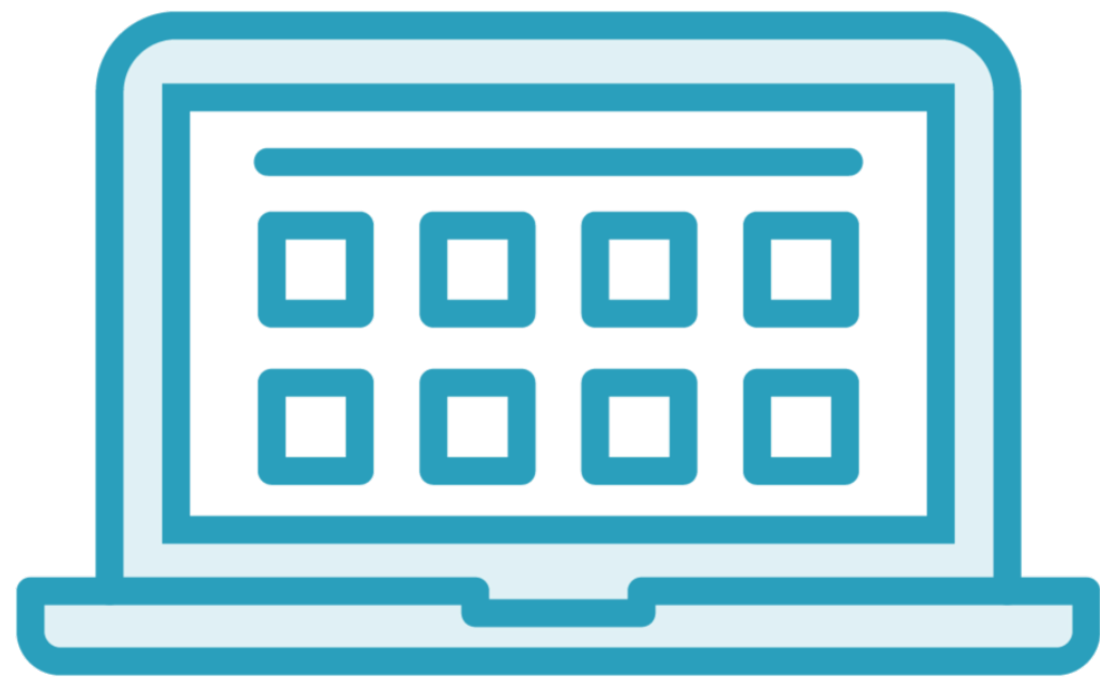
awsCloudTrail

0

Data types

 AWSCloudTrail --

Workbooks



Sentinel integrates with Azure Monitor Workbooks

- **Flexible canvas for data analysis and rich visual reports in the Azure portal**

Built-in workbooks with most connectors

- **You can also create your own!**

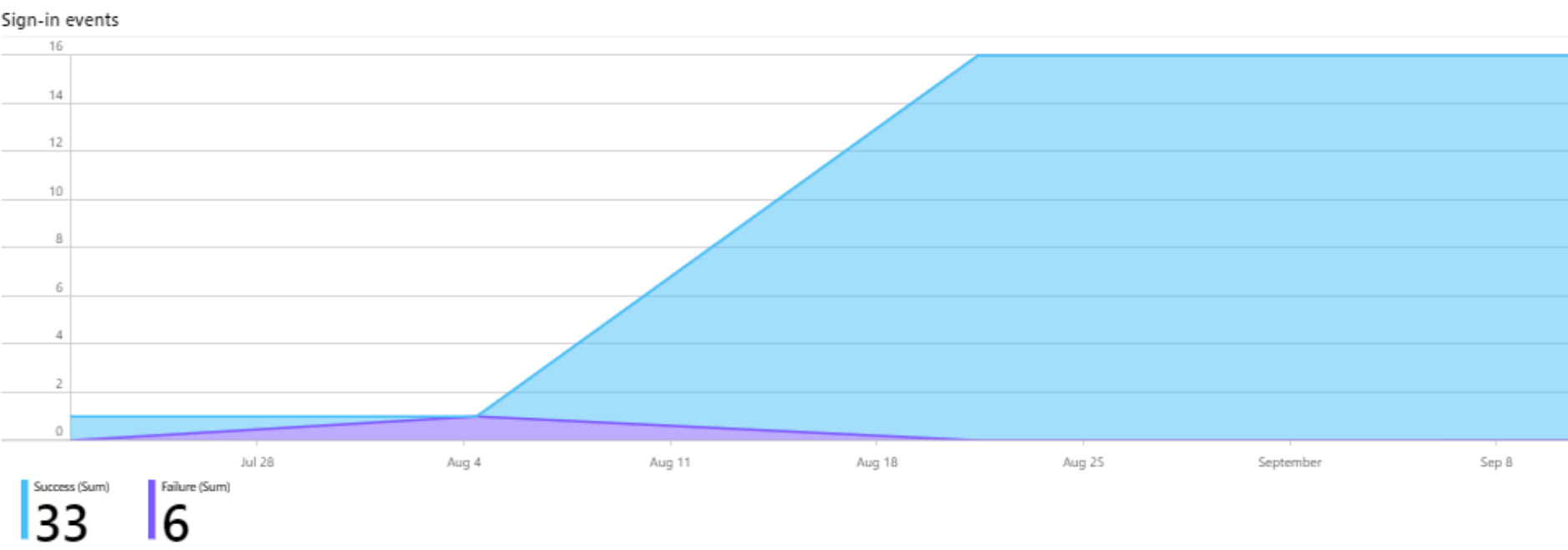


Workbook Example – AWS User Activities

AWS user activities

TimeRange: Last 60 days

Signin and login events

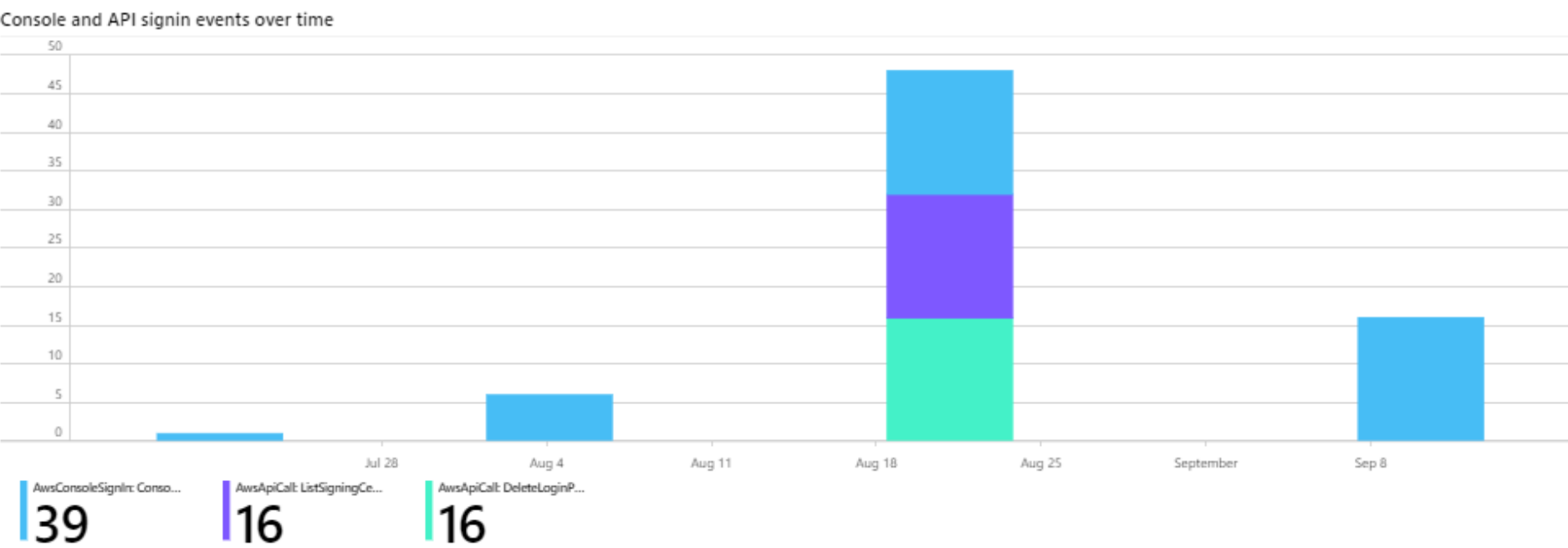


Sign-in events results

| Name | Type | LoginResults Count | Trend |
|---------|-------------|--------------------|-------|
| Success | LoginResult | 33 | |
| Failure | LoginResult | 6 | |

User sign-ins, by failure rate, and IP addresses

| UserIdentityUserName | UserIdentityAccountid | SourceIpAddress | EventName | Success | Failure |
|----------------------|-----------------------|-----------------|-----------|---------|---------|
| moshabi | 1 | 1 | 1 | 0 | 6 |
| None | 1 | 2 | 1 | 32 | 0 |
| mahasan | 1 | 1 | 1 | 1 | 0 |



Workbook Example – SharePoint & OneDrive

TimeRange: Last 30 days Operations: All Users: All Workspaces: All

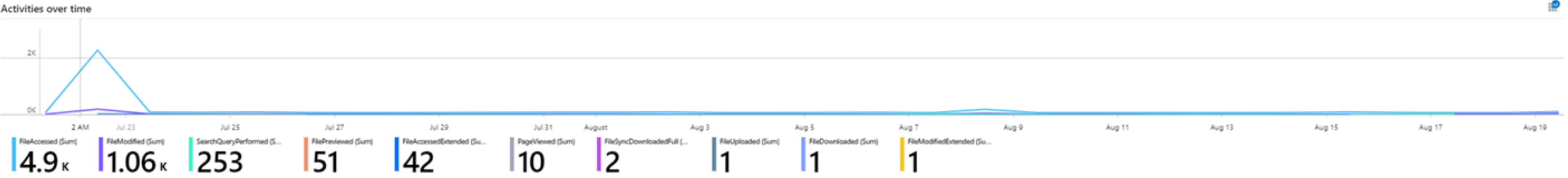
General overview



Operation summary

Search

| Name | Type | Operations Count | Trend |
|----------------------|-----------|------------------|-------|
| FileAccessed | Operation | 4897 | |
| FileModified | Operation | 1060 | |
| SearchQueryPerformed | Operation | 253 | |
| FilePreviewed | Operation | 51 | |
| FileAccessedExtended | Operation | 42 | |



Analytics & Incidents



Built-in analytics templates for most connectors

- **Get notified when anything suspicious occurs**

Sentinel can correlate alerts into incidents

- **Built-in correlation rules / create your own**

Microsoft Sentinel Incidents

Home > Microsoft Sentinel

Microsoft Sentinel | Incidents

Selected workspace: 'Contoso'

Search (Ctrl+/) Refresh Last 24 hours Actions Security efficiency workbook Columns Guides & Feedback

General

- Overview
- Logs
- News & guides
- Search (Preview)

Threat management

- Incidents**
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence
- MITRE ATT&CK (Preview)

Content management

- Content hub (Preview)
- Repositories (Preview)
- Community

Configuration

- Data connectors
- Analytics
- Watchlist
- Automation

403 Open incidents **400** New incidents **3** Active incidents

Open incidents by severity

High (82) Medium (95) Low (207) Informational (19)

Search by ID, title, tags, owner or product

Severity: All Status: 2 selected Product name: All Owner: All

Auto-refresh incidents

| Severity | Status | Incident ID | Title | Alerts | Product names | Created time |
|----------|--------|-------------|---------------------------------------|--------|---------------------------|--------------------|
| High | New | 203444 | Authentication Methods Change... | 1 | Microsoft Sentinel | 05/11/22, 12:52 PM |
| High | New | 203443 | Authentication Methods Change... | 1 | Microsoft Sentinel | 05/11/22, 12:49 PM |
| High | New | 203440 | User login from different countri... | 1 | Microsoft Sentinel | 05/11/22, 12:41 PM |
| High | New | 203437 | Preview: User and IP address rec... | 2 | Microsoft Defender fo... | 05/11/22, 12:25 PM |
| High | New | 203436 | Preview: Suspicious PowerShell c... | 2 | Microsoft Defender fo... | 05/11/22, 12:23 PM |
| High | New | 203435 | Preview: Network intrusion dete... | 2 | Microsoft Defender fo... | 05/11/22, 12:23 PM |
| High | New | 203426 | Preview: Multiple alerts possibly ... | 5 | Microsoft Defender fo... | 05/11/22, 11:52 AM |
| High | New | 203425 | Preview: Multiple alerts possibly ... | 11 | Microsoft Cloud App ... | 05/11/22, 11:52 AM |
| High | New | 203424 | Preview: Crypto-mining activity f... | 2 | Azure Defender, Azur... | 05/11/22, 11:52 AM |
| High | New | 203423 | Impossible travel to atypical loca... | 2 | Azure Active Directory... | 05/11/22, 11:52 AM |
| High | New | 203421 | Preview: Suspicious PowerShell c... | 2 | Azure Active Directory... | 05/11/22, 11:51 AM |
| High | New | 203422 | Preview: Multiple alerts possibly ... | 16 | Microsoft Defender fo... | 05/11/22, 11:51 AM |
| High | New | 203420 | Preview: Connection to web pag... | 2 | Azure Defender, Micr... | 05/11/22, 11:48 AM |
| High | New | 203419 | Authentication Methods Change... | 1 | Microsoft Sentinel | 05/11/22, 11:39 AM |

< Previous 1 - 50 Next >

Authentication Methods Changed for Privileged Acc...

Incident ID: 203443

Unassigned Owner New Status High Severity

Description

Identifies authentication methods being changed for a privileged account. This could be an indicated of an attacker adding an auth method to the account so they can have continued access. Ref : <https://docs.microsoft.com/azure/active-directory/fundamentals/security-operations-privileged-accounts#things-to-monitor-1>

Alert product names

- Microsoft Sentinel

Evidence

1 Events 1 Alerts 0 Bookmarks

Last update time 05/11/22, 12:50 PM Creation time 05/11/22, 12:49 PM

Entities (2)

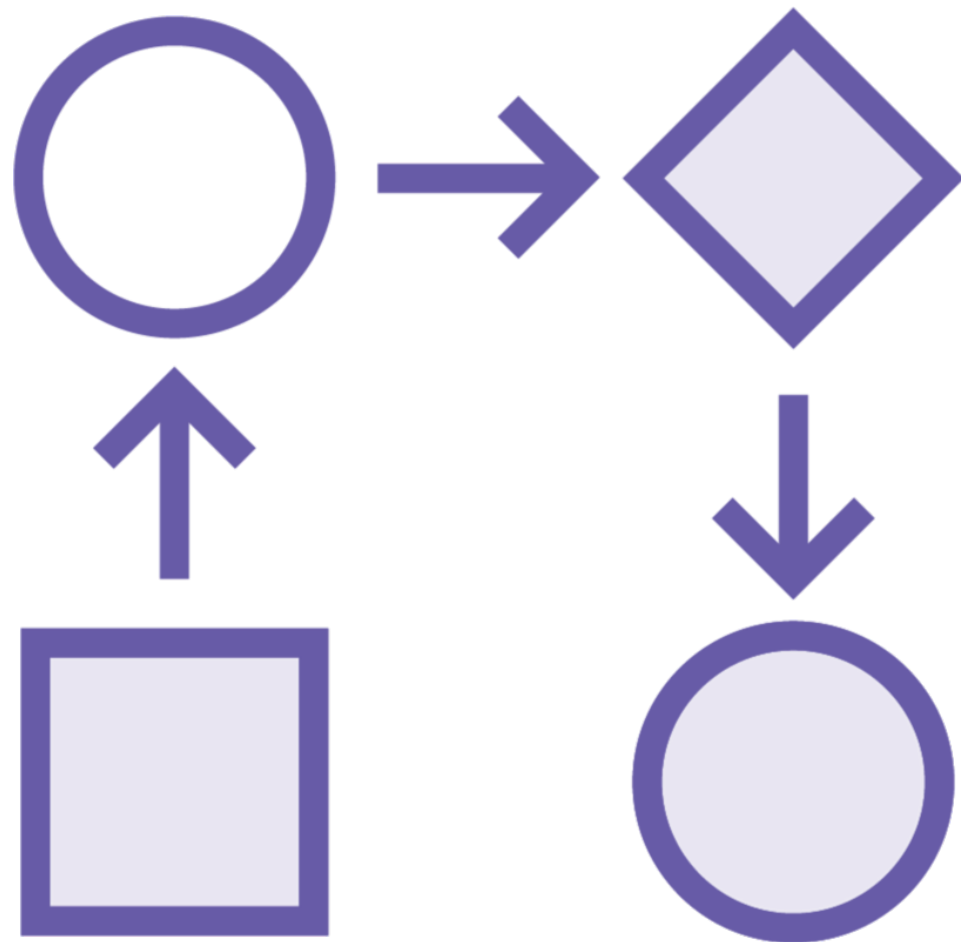
- gbarnes@contoso...
- 192.168.65.82

[View full details >](#)

Tactics and techniques

[View full details](#) Actions

Security Automation & Orchestration



Automation rules can help you be more productive in Microsoft Sentinel

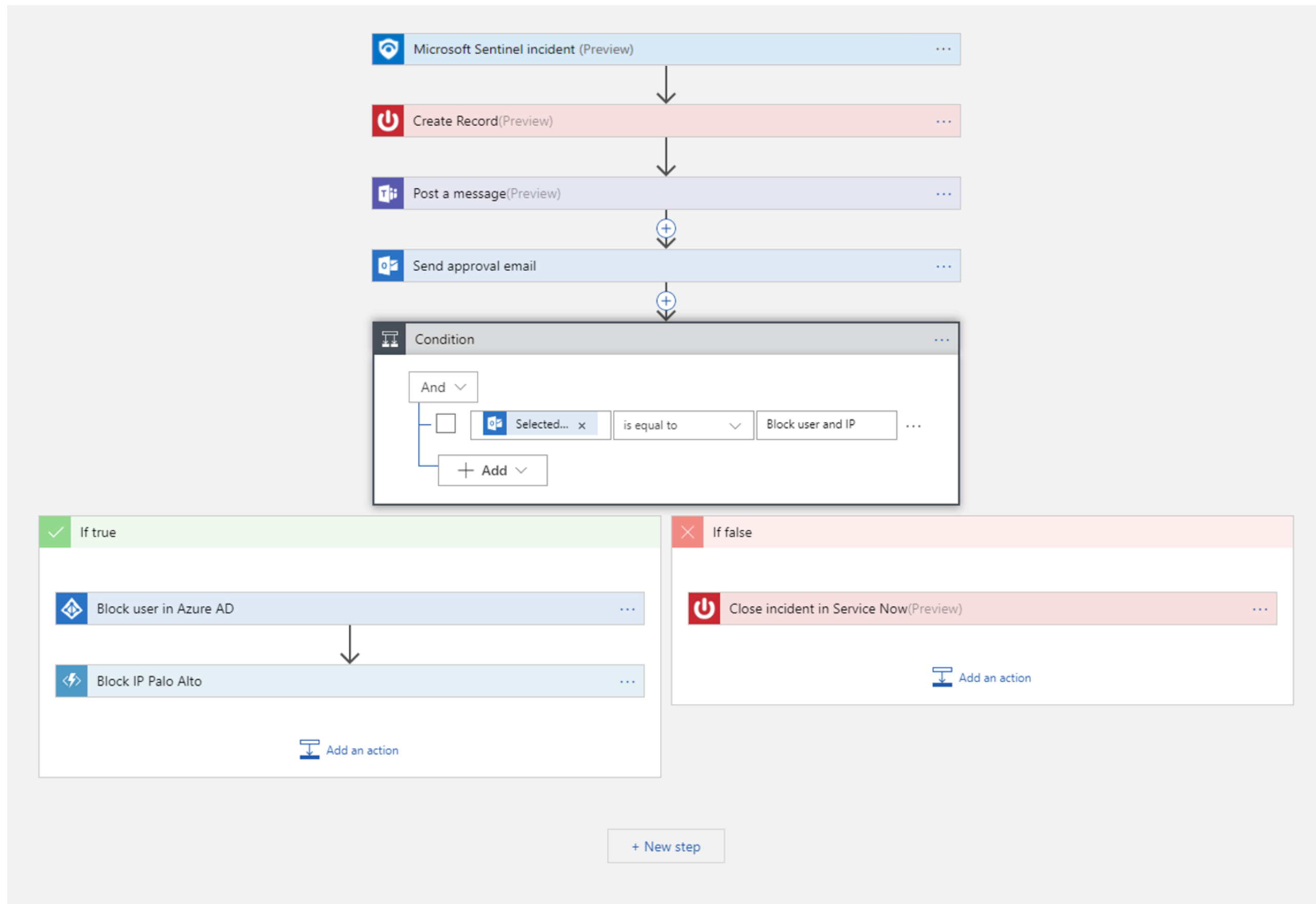
- Tag Incidents
- Assign them to the right personnel
- Change Severity
- Run Playbooks

Playbooks are collections of procedures that can be run

- Based on workflows built with Azure Logic Apps
- Over 200 connectors built in for your own custom logic



Microsoft Sentinel Playbook Example



Conclusion



Introduction to SIEM, SOAR, and XDR

Microsoft 365 Defender

- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Defender for Endpoint

Microsoft Sentinel



Up Next:

Compliance Solutions for Microsoft 365

