Microsoft

Bezbedonosna analiza - Microsoft Sentinel

Uroš Babić
Security Architect at Crayon, Microsoft Security MVP, MCT
uros.babic@crayon.com





Agenda

1. **Podešavanje Microsoft Sentinel okruženja**
- Kreiranje Sentinel RBAC rola
- Kreiranje i podešavanje Log Analytics workspace
- Dodavanje Sentinela u workspace
- Konfiguracija API konekcije i autorizacija accounta

2. **Kreiranje Data Konektora na Content Hub i konfiguracija konektora u Data Connector na MS Sentinelu**
- Azure Activity,
- Microsoft Entra ID Protection
- Microsoft Defender for Cloud
- Microsoft Defender for XDR
- Microsoft Defender Threat Intelligence
- Microsoft 365
- Microsoft Defender for Office365
- Tenant-based Defender for Cloud

3. **Kreiranje analitičkih rulova**
- Enable an Azure Activity rule
- Kreiranje scheduled rulova
- Kireiranje Microsoft Sentinel custom analytics rule

4. **Kreiranje Workbooks**
- Sentinel Optimization Workbook
- LA Workbook

Agenda

5. Kreiranje Playbooks
- Prompt user Incident
- Block-AADUserOrAdmin-Incident
- Get-GeoFromIpAndTagIncident, etc.

6. Threat Hunting
- SharePointFileOperation via devices with previously unseen IPs
- Multiple users email forwarded to same destination
- Port opened for an Azure Resource

7. Incident Management Unified Security Operation XDR+Sentinel
- Reviewing Microsoft Sentinel incident tools and capabilities
- Handling the incident , Log Management
- Incident investigationsions Graph + Playbooks

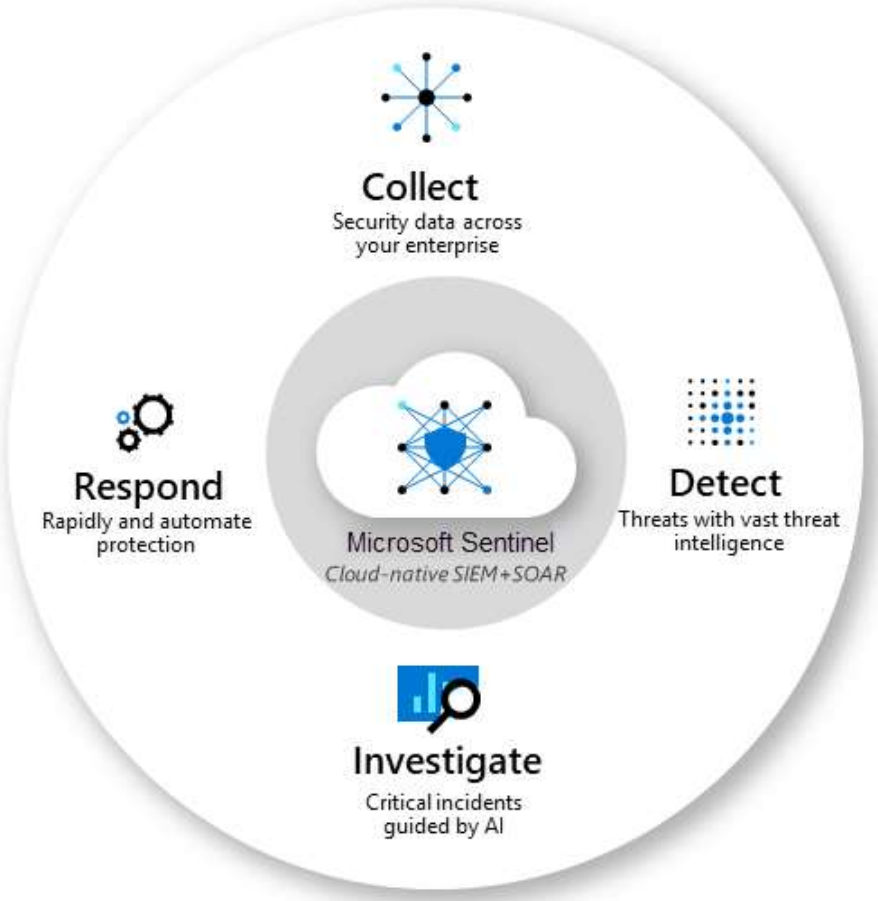
Microsoft Sentinel

Collect data at cloud scale across all users, devices, applications, and infrastructure

Detect threats, and minimize false positives

Investigate threats with artificial intelligence, and hunt for suspicious activities at scale

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

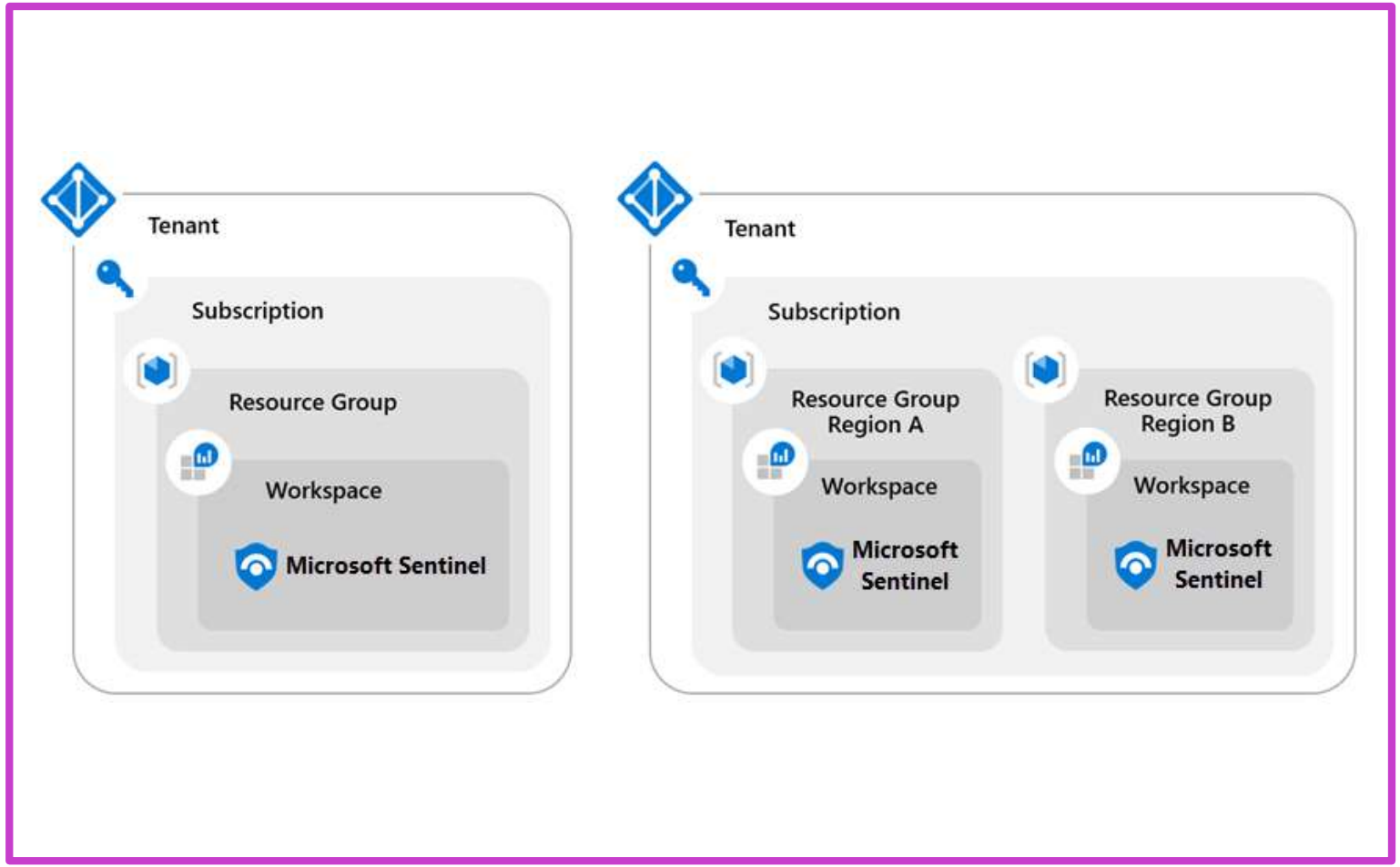


Create and manage Microsoft Sentinel workspaces



Plan for the Microsoft Sentinel workspace

- Single-Tenant with a single Microsoft Sentinel Workspace
- Single-Tenant with regional Microsoft Sentinel Workspaces
- Multi-Tenant



Create a Microsoft Sentinel workspace



Start the creation process

1. At the search bar, search for Sentinel, then select **Microsoft Sentinel**.
2. The Microsoft Sentinel Workspaces shows a list of the current workspaces. Select the **+ add** button.



Create and configure a Log Analytics Workspace

1. The next page, **Add Microsoft Sentinel to a workspace** will display a list of available Log Analytics workspaces to add Microsoft Sentinel. Select the **+ create a new workspace** button.
2. The Basics tab includes: Subscription, Resource Group, Name, Region.
3. Select the **Review + Create** button and then select the **Create** button.



Add Microsoft Sentinel to the workspace

The "Add Microsoft Sentinel to Workspace" screen will now appear after you've completed the previous steps.

1. Wait for the newly created "Log Analytics Workspace" to appear in the list.
2. Select the newly created Log Analytics workspace. And select the **Add** button.

Interactive Lab Simulation: Click the link to start the lab simulation.

© Copyright Microsoft Corporation. All rights reserved.

Understand Microsoft Sentinel permissions and roles

Microsoft Sentinel uses Azure role-based access control (Azure RBAC) to provide built-in roles that can be assigned to users, groups, and services in Azure.

Microsoft Sentinel-specific roles

All Microsoft Sentinel built-in roles grant read access to the data in your Microsoft Sentinel workspace:

- **Microsoft Sentinel Reader**
- **Microsoft Sentinel Responder**
- **Microsoft Sentinel Contributor**
- **Microsoft Sentinel Automation Contributor**

Additional roles and permissions

- Working with playbooks to automate responses to threats
- Giving Microsoft Sentinel permissions to run playbooks
- Connecting data sources to Microsoft Sentinel
- Guest users assigning incidents
- Creating and deleting workbooks

Azure roles and Azure Monitor Log Analytics roles

- Azure roles grant access across all your Azure resources. They include Log Analytics workspaces and Microsoft Sentinel resources:
  - Owner
  - Contributor
  - Reader
- Log Analytics roles grant access across all your Log Analytics workspaces:
  - Log Analytics Contributor
  - Log Analytics Reader

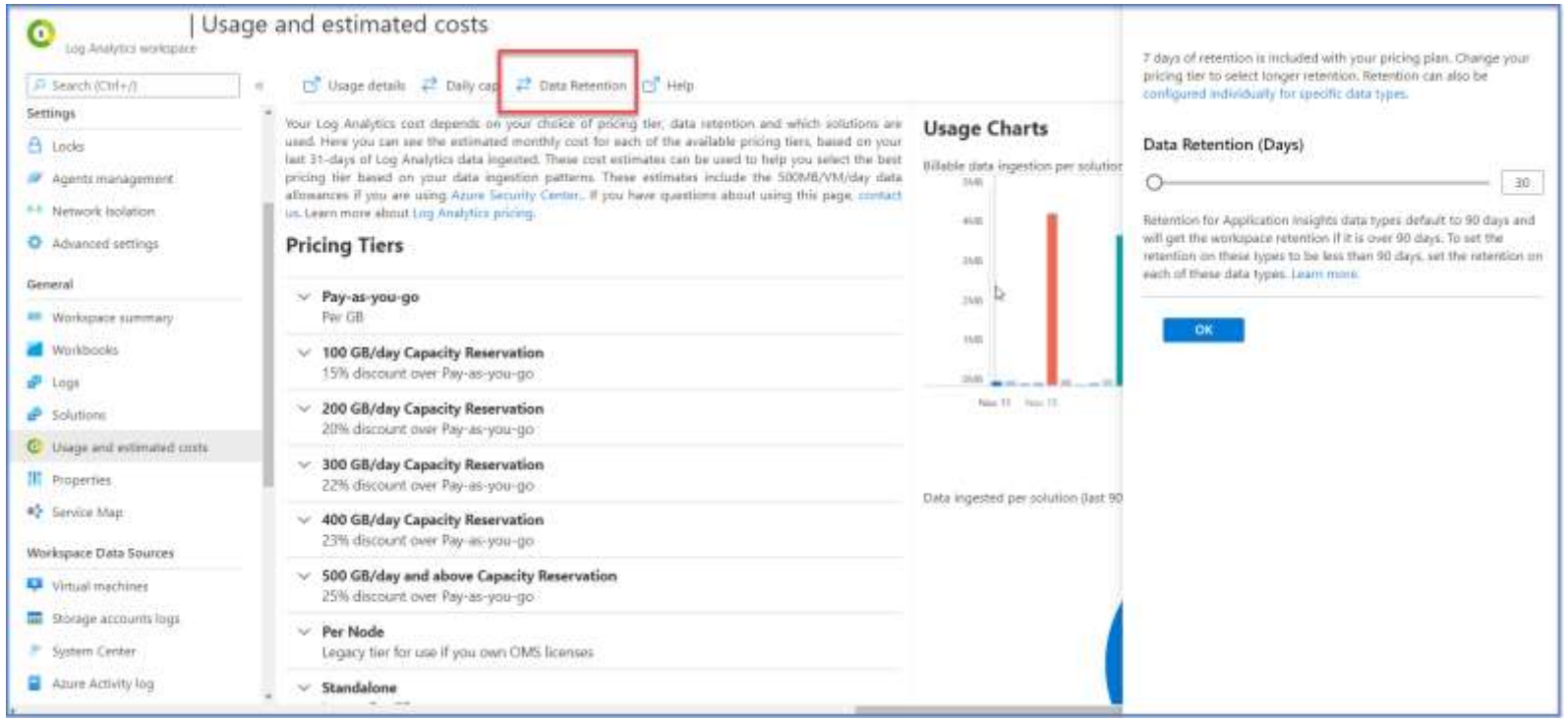
© Copyright Microsoft Corporation. All rights reserved.

Manage Microsoft Sentinel settings

Microsoft Sentinel environment settings are managed in two areas:

- In Microsoft Sentinel
- In the Log Analytics workspace where Microsoft Sentinel resides

To configure Log Retention:

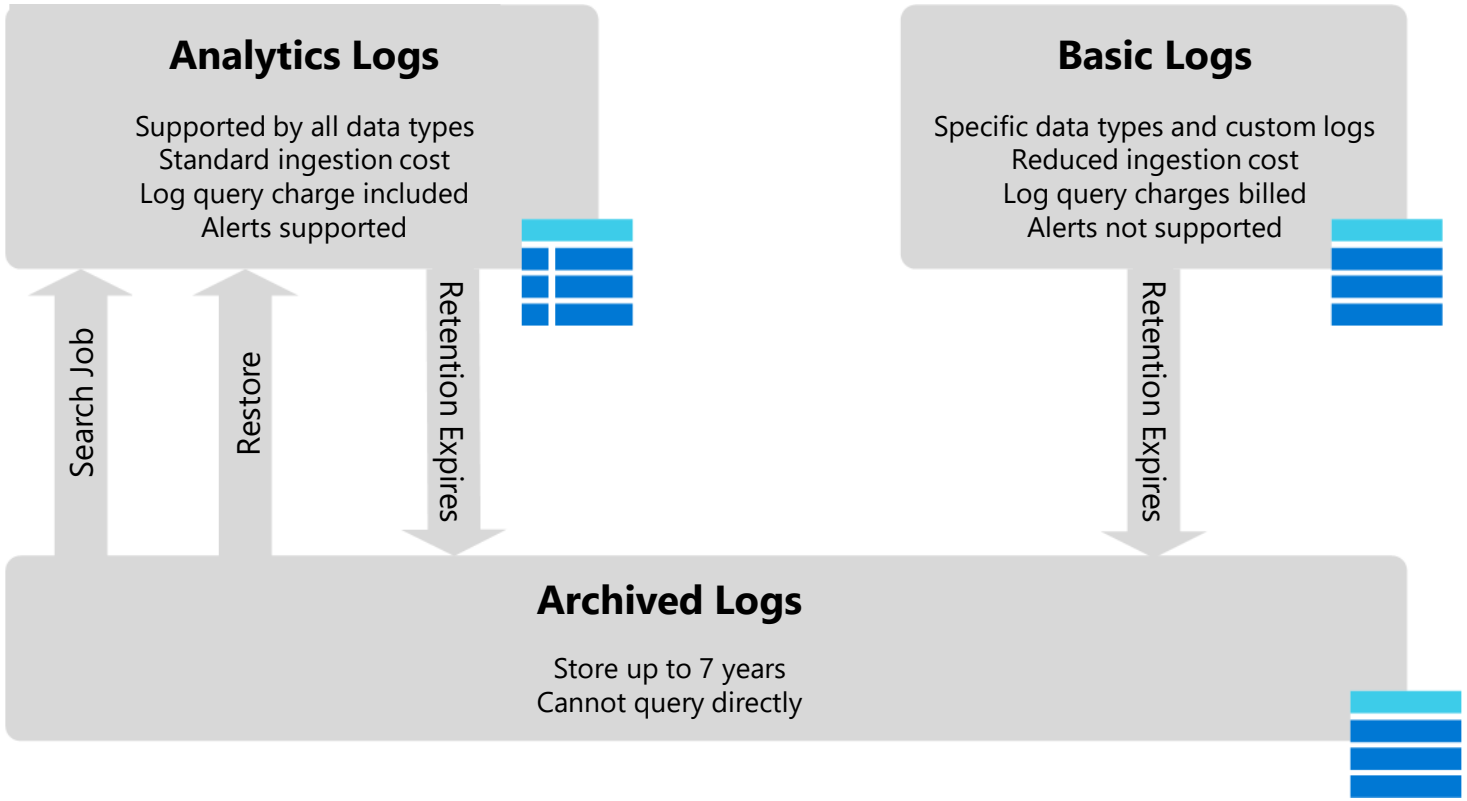


© Copyright Microsoft Corporation. All rights reserved.

Configure logs

There are three primary log types in Microsoft Sentinel:

- Analytics Logs
- Basic Logs
- Archive Logs



To access archived data, you must first retrieve data from it in an Analytics Logs table using one of the following methods:

- Search Jobs
- Restore

© Copyright Microsoft Corporation. All rights reserved.

Knowledge check



1 **Where is your log data stored?**

- ☐ Microsoft Sentinel Workspace
- ☐ Azure Lighthouse
- ☐ Log Analytics workspace

2 **Which Microsoft Sentinel security role can create workbooks?**

- ☐ Microsoft Sentinel Responder
- ☐ Microsoft Sentinel Reader
- ☐ Microsoft Sentinel Contributor

3 **Why is it important to set the region when creating the Log Analytics workspace?**

- ☐ Specifies where the log data will be stored.
- ☐ Specifies the timezone the data will be displayed in.
- ☐ Specifies the log retention period

Connect Microsoft services to Microsoft Sentinel

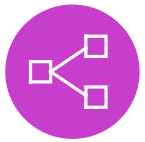


© Copyright Microsoft Corporation. All rights reserved.

Plan for Microsoft services connectors



Office 365 connector: The Configuration option allows for the sending of Exchange, SharePoint, and Teams data.



Microsoft Entra ID: Has two configuration options for Sign-On logs and Audit logs.



Microsoft Entra ID Protection: Integrates Microsoft Entra ID Protection alerts with Microsoft Sentinel when connected.



Azure Activity: The Azure Activity Log is a subscription log that provides insight into subscription-level events that occur in Azure.

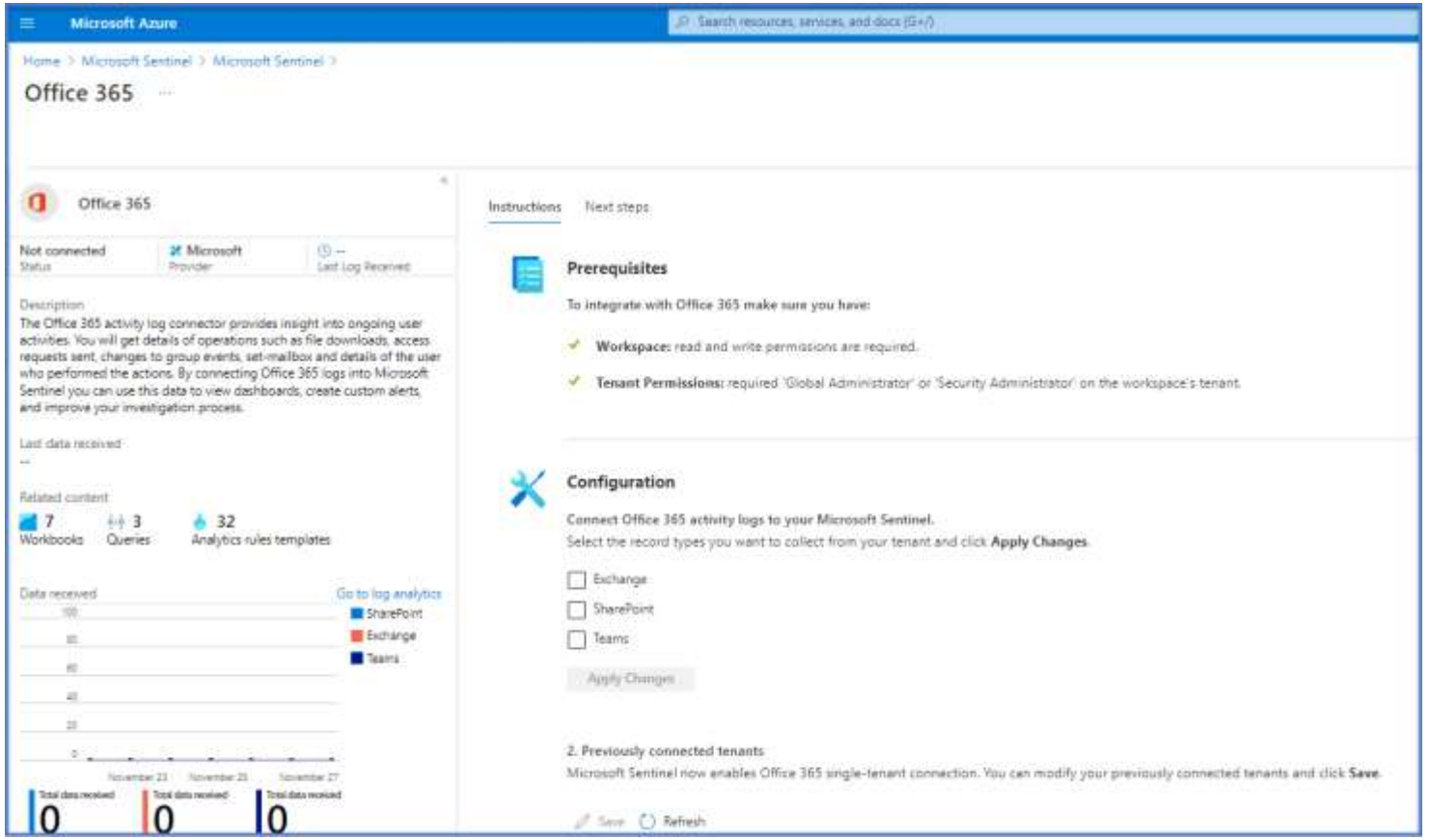
© Copyright Microsoft Corporation. All rights reserved.

Connect the Microsoft 365 connector

The Microsoft 365 activity log connector provides insight into ongoing user activities.

To view the connector page, do these steps:

1. Select Data connectors page in Sentinel.
2. Select **Office 365**.
3. Then select the **Open connector** page on the preview pane.
4. Under the section labeled Configuration, mark the Office 365 activity logs' checkboxes to connect to Microsoft Sentinel.
5. Select **Apply Changes**.



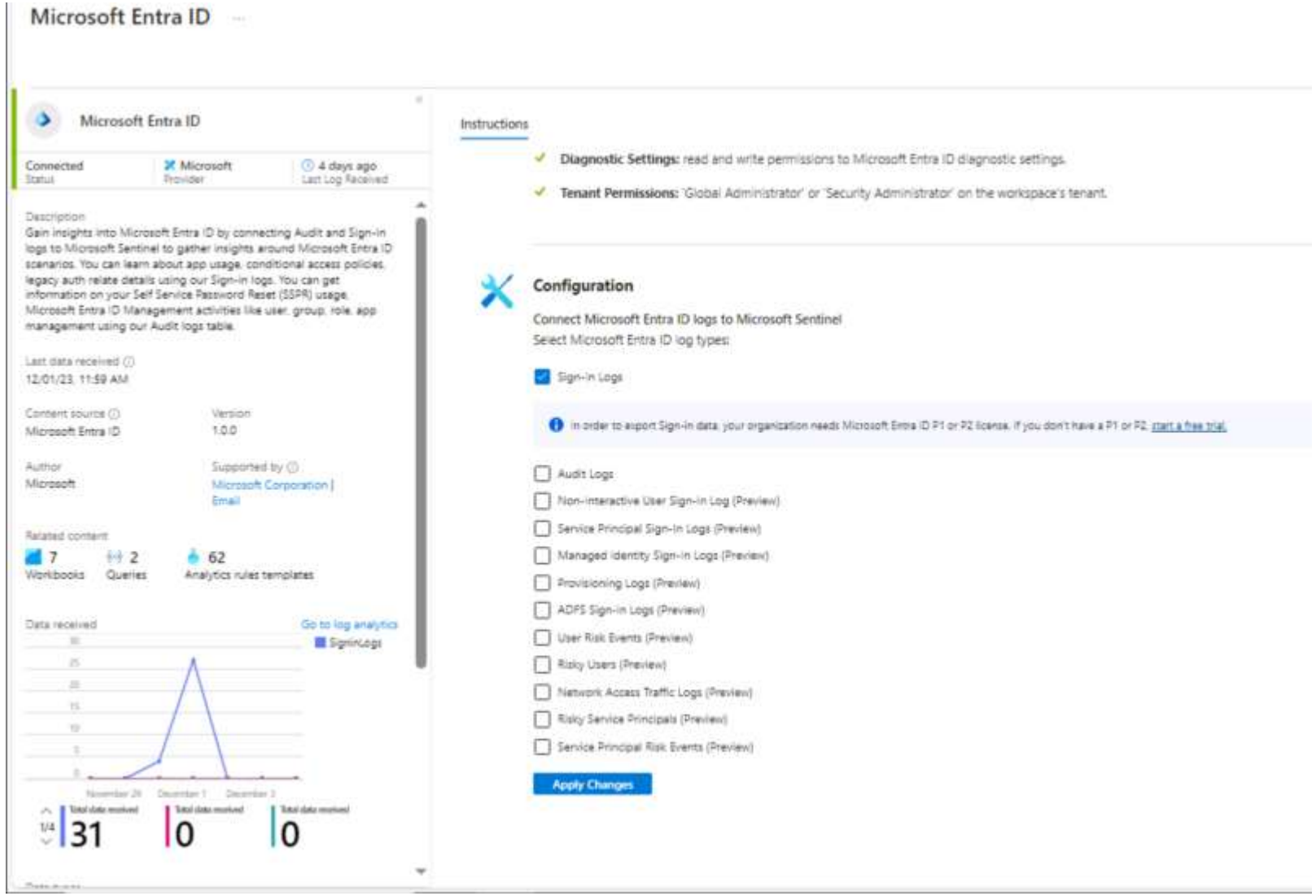
© Copyright Microsoft Corporation. All rights reserved.

Connect the Microsoft Entra ID connector

Gain insights into Microsoft Entra ID by connecting Audit and Sign in logs to Microsoft Sentinel to gather insights around Microsoft Entra ID scenarios.

To view the connector page, do these steps:

1. Select Data connectors page in Microsoft Sentinel.
2. Select **Microsoft Entra ID**
3. Then select the **Open connector** page on the preview pane.
4. Mark the checkboxes next to the logs you want to stream into Microsoft Sentinel, and select **Connect**.



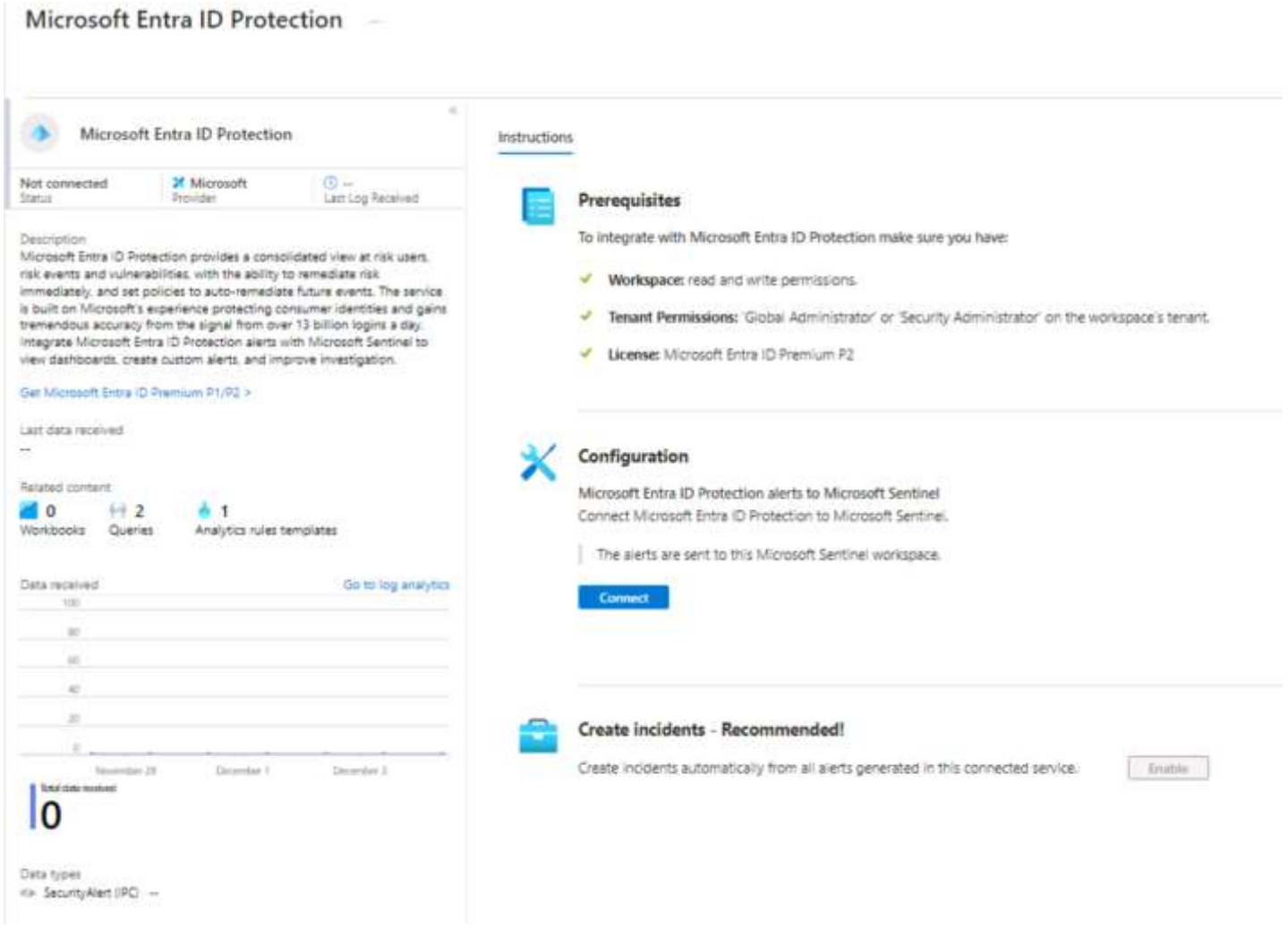
© Copyright Microsoft Corporation. All rights reserved.

Connect the Microsoft Entra ID Protection connector

Microsoft Entra ID Protection provides a consolidated view of at-risk users, risk events, and vulnerabilities, with the ability to remediate risk immediately and set policies to autoremediate future events.

To view the connector page, do these steps:

1. Select Data connectors page.
2. Select **Microsoft Entra ID Protection**.
3. Then select the **Open connector** page on the preview pane.
4. Select **Connect** to start streaming the Microsoft Entra ID Protection alerts.
5. Select whether alerts from Microsoft Entra ID Protection automatically generate incidents by selecting **Enable**.



© Copyright Microsoft Corporation. All rights reserved.

Connect the Azure Activity connector



The Azure Activity Log is a subscription log that provides insight into subscription-level events that occur in Azure.

The events included are from Azure Resource Manager operational data, service health events, write operations taken on the resources in your subscription, and the status of activities performed in Azure.

The Azure Activity Data connector uses Azure Policy to apply an Azure Subscription log-streaming pipeline that sends the event data to Log Analytics.

Important:
Prerequisites require your user to be assigned the owner role on the relevant subscription

© Copyright Microsoft Corporation. All rights reserved.

Knowledge check



1 **Which table (data type) would you query for the Microsoft Entra ID data?**

- ☐ OfficeActivity
- ☐ SigninLogs
- ☐ SecurityAlert

2 **Which table (data type) would you query for the Microsoft 365 data?**

- ☐ OfficeActivity
- ☐ SecurityAlert
- ☐ SigninLogs

3 **Which table (data type) would you query for the Microsoft Entra ID Protection data?**

- ☐ OfficeActivity
- ☐ SigninLogs
- ☐ SecurityAlert

Connect Windows hosts to Microsoft Sentinel



Plan for Windows hosts security events connector

Based on your organization requirements, you have the option of installing an agent on each windows device to forward events to Microsoft Sentinel. There are two agents available:

- Windows Security Events via AMA Connector
- Security Events via Legacy Agent Connector

Windows Security Events via AMA Connector vs. Security Events via Legacy Agent Connector

The Windows Security Events via AMA Connector:

Benefits:

- Manage collection settings at scale
- Azure Monitoring Agent shared with other solutions
- Performance improvements
- Security improvements

Limitations:

- The Azure Monitor Agent is released in preview and is supported with the CSPM plan and Microsoft Defender for Servers Plan 2.

© Copyright Microsoft Corporation. All rights reserved.

Connect using the Windows Security Events via AMA Connector

Prerequisites.

Required read and write permissions on Microsoft Sentinel workspace.

Azure Arc must be installed and enabled on non-Azure VMs.

Including as shown on the right.

Connection Steps

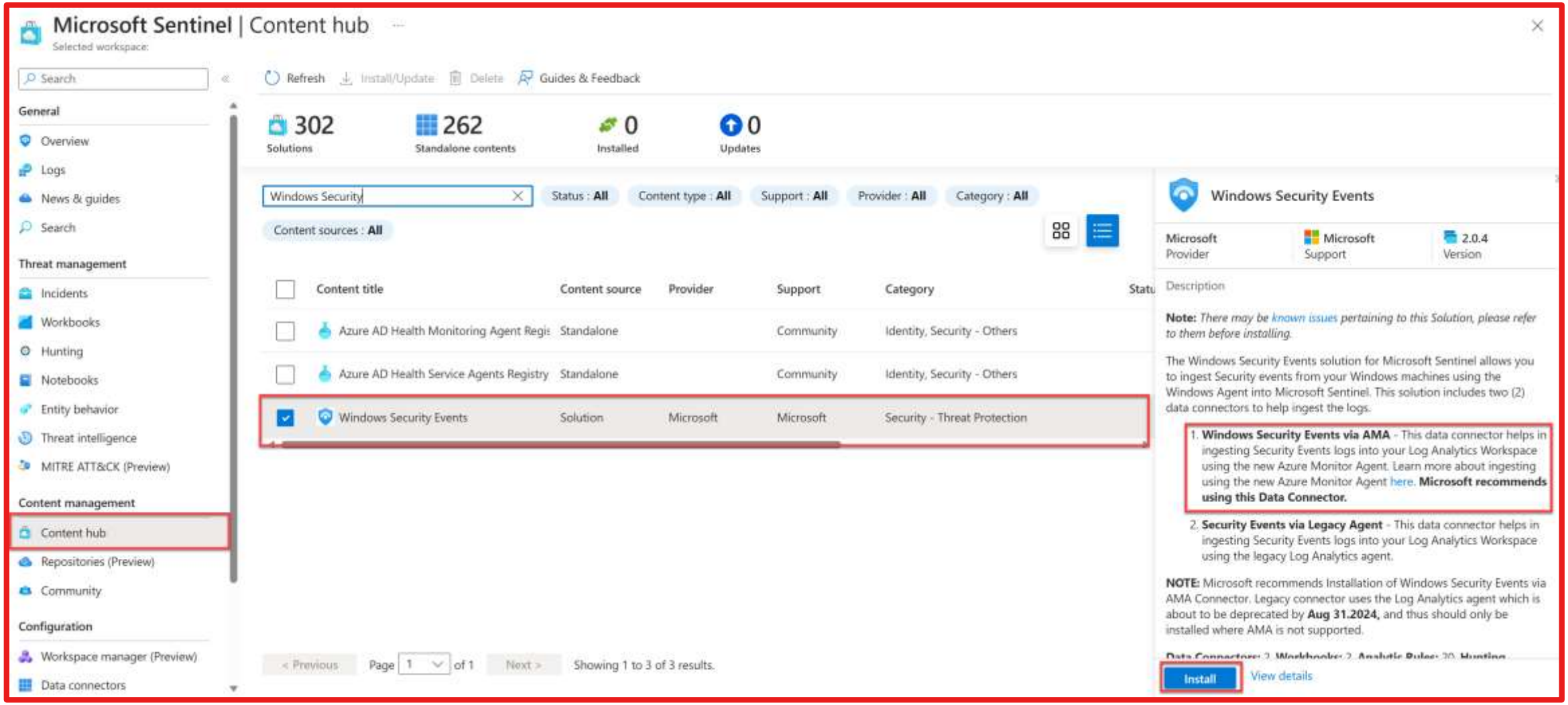
1. Navigate to Data connectors in Microsoft Sentinel.
2. Select the Windows Security Events via AMA connector.
3. Select Open connector page.
4. Verify necessary permissions.
5. Under Configuration, select +Add data collection rule.
6. Enter rule name, subscription, and resource group.
7. Add resources and machines for the rule.
8. Choose events to collect (All, Common, Minimal, Custom).
9. When you've added all the filter expressions you want, select Next: Review + create.
10. When you see the "Validation passed" message, select Create.

```
- Windows servers installed on physical machines
- Windows servers installed on on-premises virtual machines
- Windows servers installed on virtual machines in non-Azure clouds;
```

```
PowerShell
$XPath = '*[System[EventID=1035]]’
Get-WinEvent -LogName 'Application' -FilterXPath $XPath
```

© Copyright Microsoft Corporation. All rights reserved.

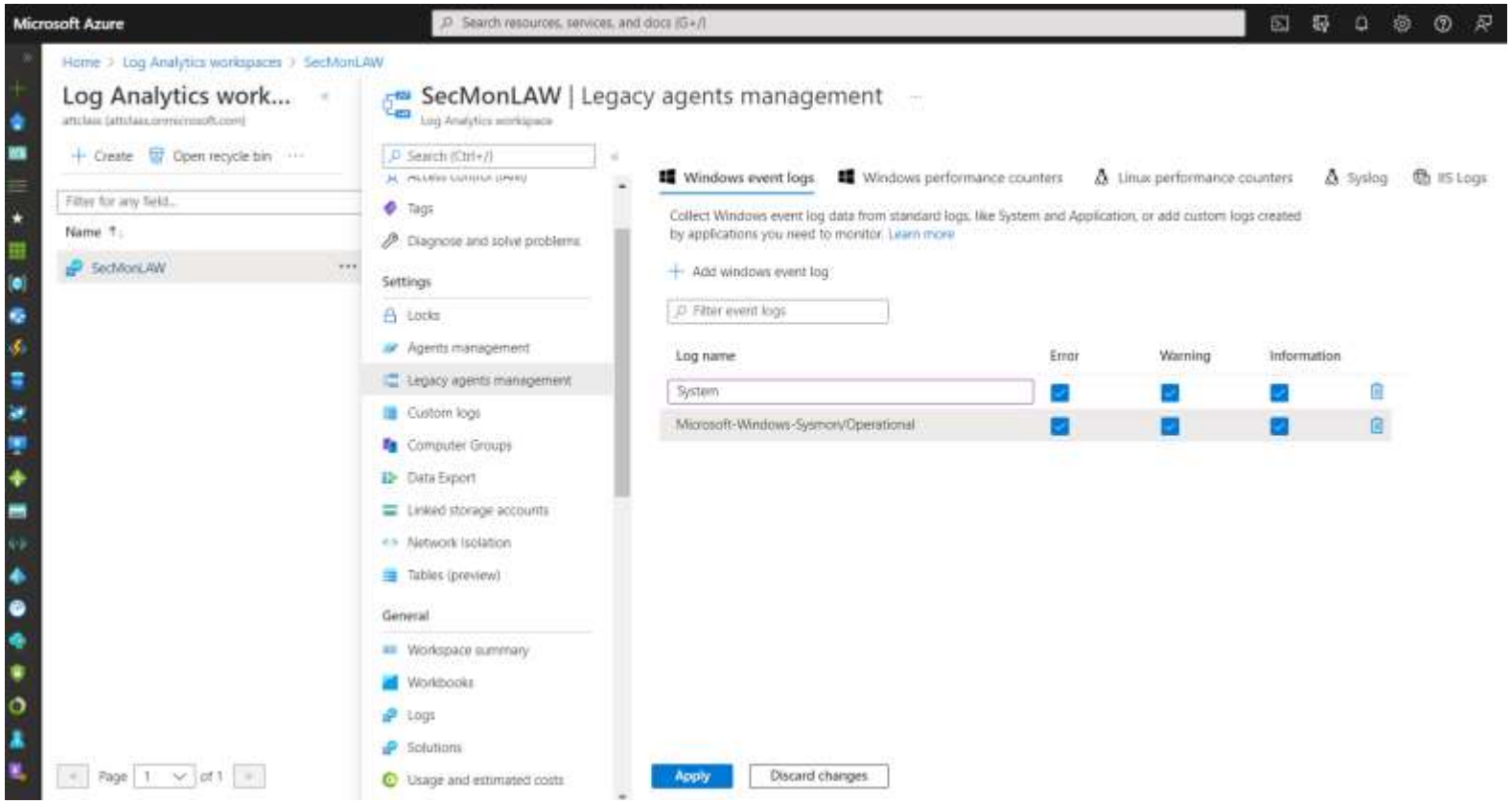
Windows Security Events via AMA Connector



Collect Sysmon event logs

System Monitor (Sysmon) is a Windows system service, and device driver that remains resident across system reboots to monitor and log system activity to the Windows event log once installed on a system.

It provides detailed information about process creations, network connections, and changes to file creation time.



© Copyright Microsoft Corporation. All rights reserved.

Knowledge check



1 **Which connector do you use to collect Windows security events?**

- ☐ Windows Security Events via AMA
- ☐ Common Event Format
- ☐ Syslog

2 **To collect Sysmon events with the Security Events connector, what is the log name used to collect it in advanced settings?**

- ☐ Microsoft-Windows-Sysmon/Operational
- ☐ Microsoft-Windows-Sysmon/Events
- ☐ Microsoft-Windows-Sysmon/Logs

3 **Which table contains the ingested Sysmon events?**

- ☐ Event
- ☐ CommonSecurityLog
- ☐ SecurityEvents

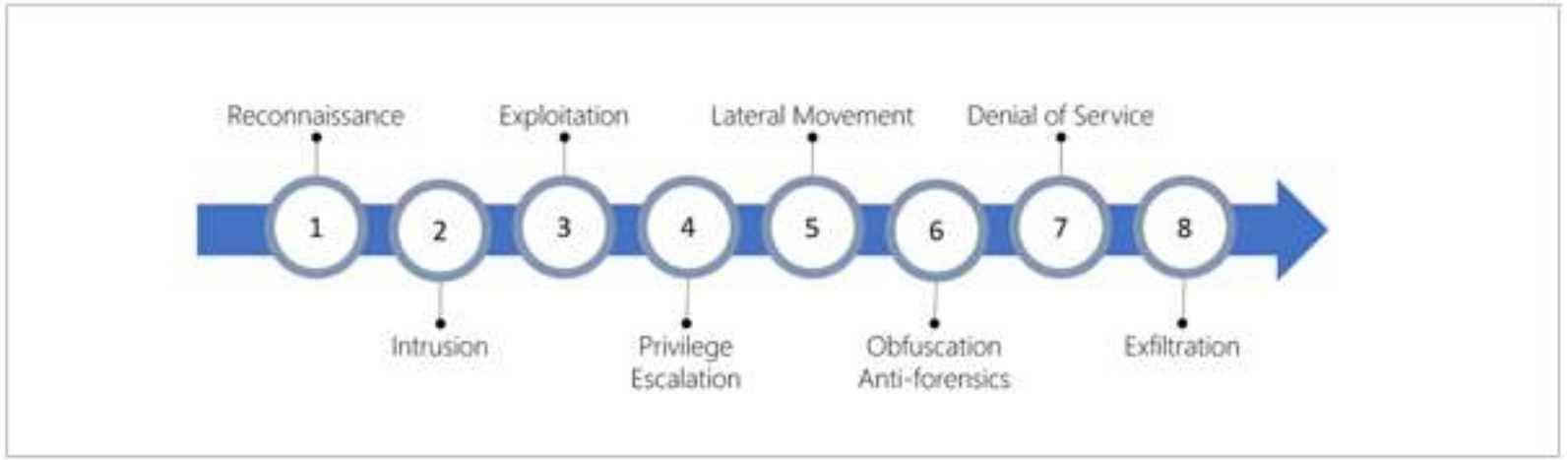
Threat detection with Microsoft Sentinel analytics



© Copyright Microsoft Corporation. All rights reserved.

Cloud Forensics investigations in Azure

Cyber Kill Chain



Series of steps that trace the stages of a cyberattack

Different types of attacks are associated with each stage, and they target various subsystems

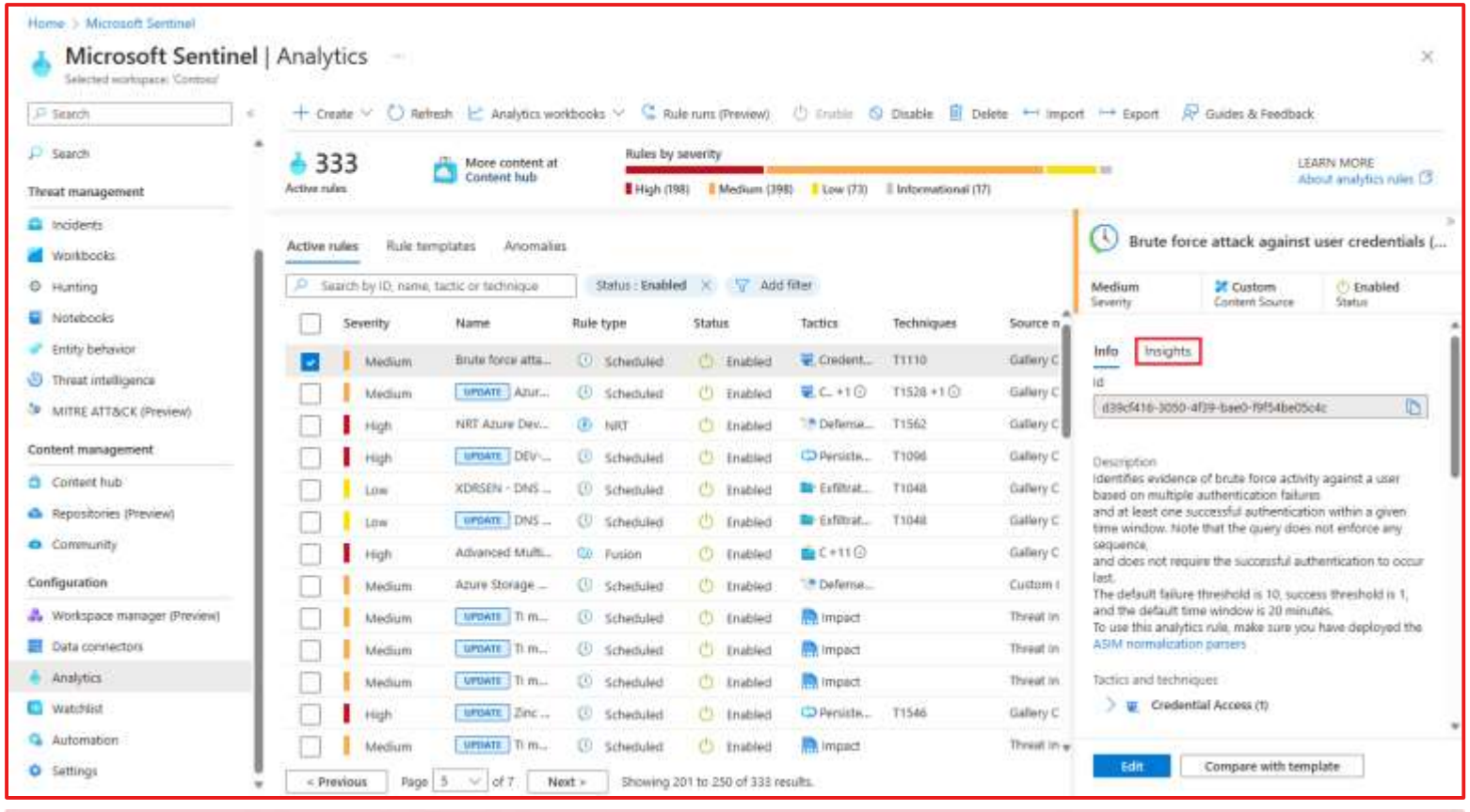
Security Center is designed around the kill chain

What is Microsoft Sentinel Analytics?

Microsoft Sentinel Analytics provides several functionalities that you can use to implement security for the data and resources at Contoso.

With the proper analytics rule, you can get insights into where an attack originated from, what resources were compromised, potential data lost, along with the timeline for the incident.

You can create analytics rules from the **Analytics** home page. You can access the **Analytics** page in Microsoft Sentinel from the navigation pane.



© Copyright Microsoft Corporation. All rights reserved.

Types of analytics rules



Anomaly: Anomaly alerts are informational and identify anomalous behaviors.



Fusion: Fusion alerts identify suspicious activities at various stages of the cyber kill chain. Fusion correlates multiple security alerts from various products and uses machine learning to detect advanced multistage attacks.



Microsoft security: You can configure Microsoft security solutions that are connected to Microsoft Sentinel to automatically create incidents from all alerts generated in the connected service.



Machine learning (ML) behavior analytics: Microsoft Sentinel Analytics includes built-in machine learning behavior analytics rules.



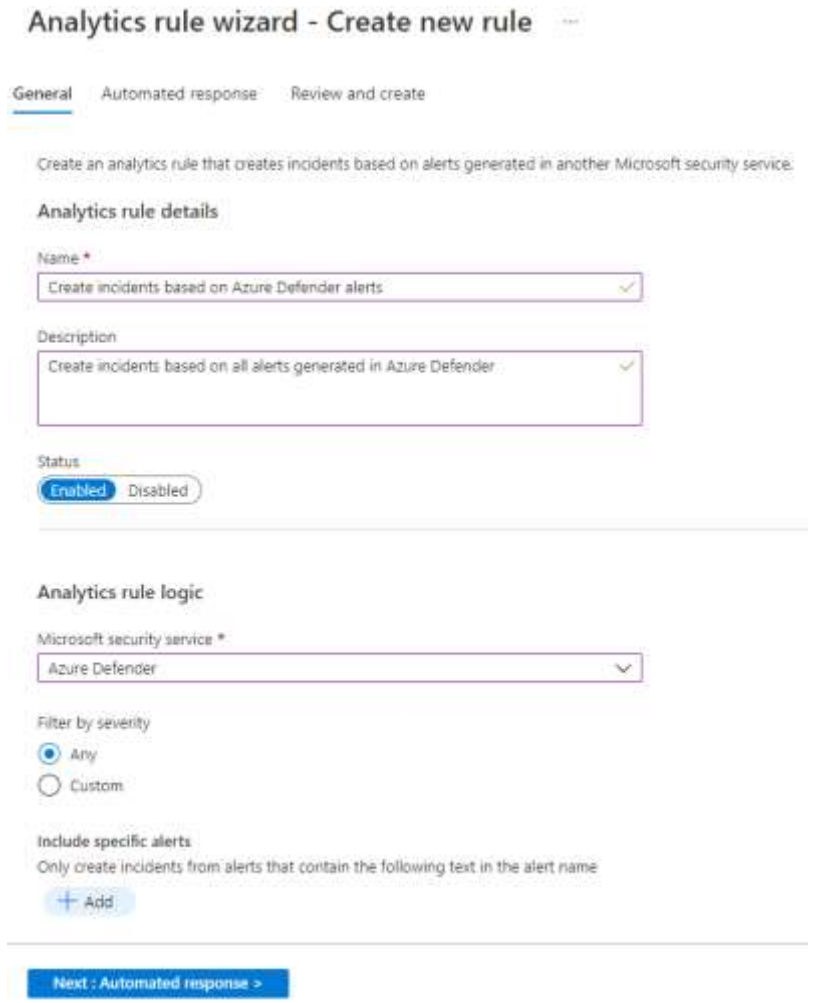
Scheduled alerts: Scheduled alerts analytics rules provide you the highest level of customization.

© Copyright Microsoft Corporation. All rights reserved.

Create an analytics rule from templates

By selecting one of the rules on the Rule Templates tab, you can observe the properties of the rule. For each rule, you can review:

- **Severity level.** This indicates the importance of the alert. There are four severity levels: High, Medium, Low and Informational
- **Name of the rule.** This provides a meaningful name for the alert rule.
- **Rule type.** This defines the type of the rule, which can be one of the following types: Anomaly, Fusion, Microsoft Security, ML Behavior Analytics and Scheduled.
- **Data Source.** This specifies the data source connector that generated the alert.
- **Tactics.** This specifies methodologies in MITRE ATT&CK model used by different kinds of malware.

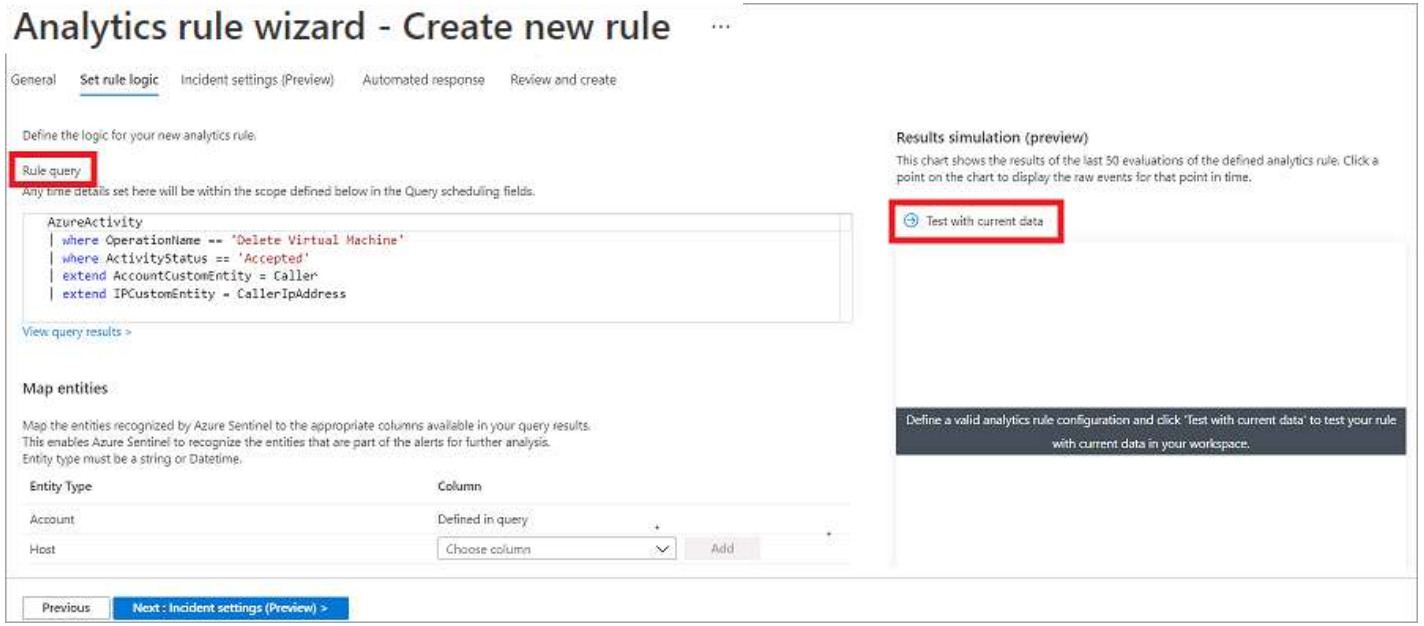


© Copyright Microsoft Corporation. All rights reserved.

Create an analytics rule from a wizard

Creating a custom rule from a scheduled query rule type provides you with the highest level of customization. You can define your own KQL code, set a schedule to run an alert, and provide an automated action by associating the rule with a Microsoft Sentinel Playbook.

To create a scheduled query rule, in the Azure portal, under **Microsoft Sentinel**, select **Analytics**. In the header bar, select **+Create**, and then select **Scheduled query rule**.



© Copyright Microsoft Corporation. All rights reserved.

Manage analytics rules

You can perform the following four actions on existing active rules:

Edit rules:

- You can modify existing rules by selecting **Edit** in the details pane.
- To edit a rule, you navigate the same pages that you did in creating the rule.

Disable rules:

- You can disable a rule when you're performing an activity that can trigger the rule alert.
- Disabled rules retain their configuration, and you can enable them again at a later time.

Duplicate rules:

- When you duplicate a rule, the rule contains all the configuration provided from the original rule.
- You can further modify the configuration based on your requirements.

Delete rules:

- Deleting the rule prompts you for confirmation before Microsoft Sentinel Analytics removes it from the set of active rules.
- Be aware that deleting a rule is permanent, and there isn't an undo feature.

© Copyright Microsoft Corporation. All rights reserved.

Automation in Microsoft Sentinel



© Copyright Microsoft Corporation. All rights reserved.

Understand automation options

Automation rules

- Automation rules centralize incident handling automation.
- They automate responses for multiple analytics rules simultaneously.
- Users can automatically tag, assign, or close incidents without playbooks.
- Users can control the execution order of actions.
- Automation rules streamline automation in Microsoft Sentinel and simplify incident orchestration workflows.

Playbooks

- Playbooks automate response and remediation actions in Microsoft Sentinel.
- They integrate with internal and external systems.
- Playbooks can be triggered automatically by alerts, incidents, analytics rules, or automation rules.
- Playbooks benefit from Logic Apps' design tools, scalability, and reliability as a Tier 1 Azure service.

© Copyright Microsoft Corporation. All rights reserved.

Create automation rules (1)



Automation blade

- The new Automation blade replaces the Playbooks blade for central management of automation rules.
- In the Automation blade, you can create, edit, enable, disable, and reorder automation rules.
- Automation rules can be applied to multiple analytics rules, offering flexibility in configuration.
- The Automation blade displays all defined rules, their status, and the analytics rules to which they apply.



Analytics rule wizard

- The Automated response tab in the analytics rule wizard manages and creates automation rules specific to the edited or created analytics rule.
- When using the Analytics blade, you can select rule types and open the rule wizard to access the Automated response tab.
- The creation of automation rules within this tab is tailored to the analytics rule you're editing, with the condition preset, while other configuration options remain accessible.



Incidents blade

- Automation rules can be created in the Incidents blade for responding to single or recurring incidents, especially for suppression purposes.
- When creating an automation rule from an incident, the rule's name, analytics rule, conditions, actions, and expiration date are pre-populated, with a default suppression action.
- Users have the flexibility to modify conditions, actions, and the expiration date according to their needs.

© Copyright Microsoft Corporation. All rights reserved.

Create automation rules (2)



Trigger: Automation rules are triggered by the creation of an incident.



Conditions: Complex sets of conditions can be defined to govern when actions should run.



Actions: Actions can be defined to run when the conditions are met.



Expiration date: You can define an expiration date on an automation rule.



Order: You can define the order in which automation rules will run.

© Copyright Microsoft Corporation. All rights reserved.

Knowledge check



1 **Automation rules are triggered by?**

- ☐ Incidents
- ☐ Connectors
- ☐ Watchlists

2 **You use a Logic Apps to create a_?**

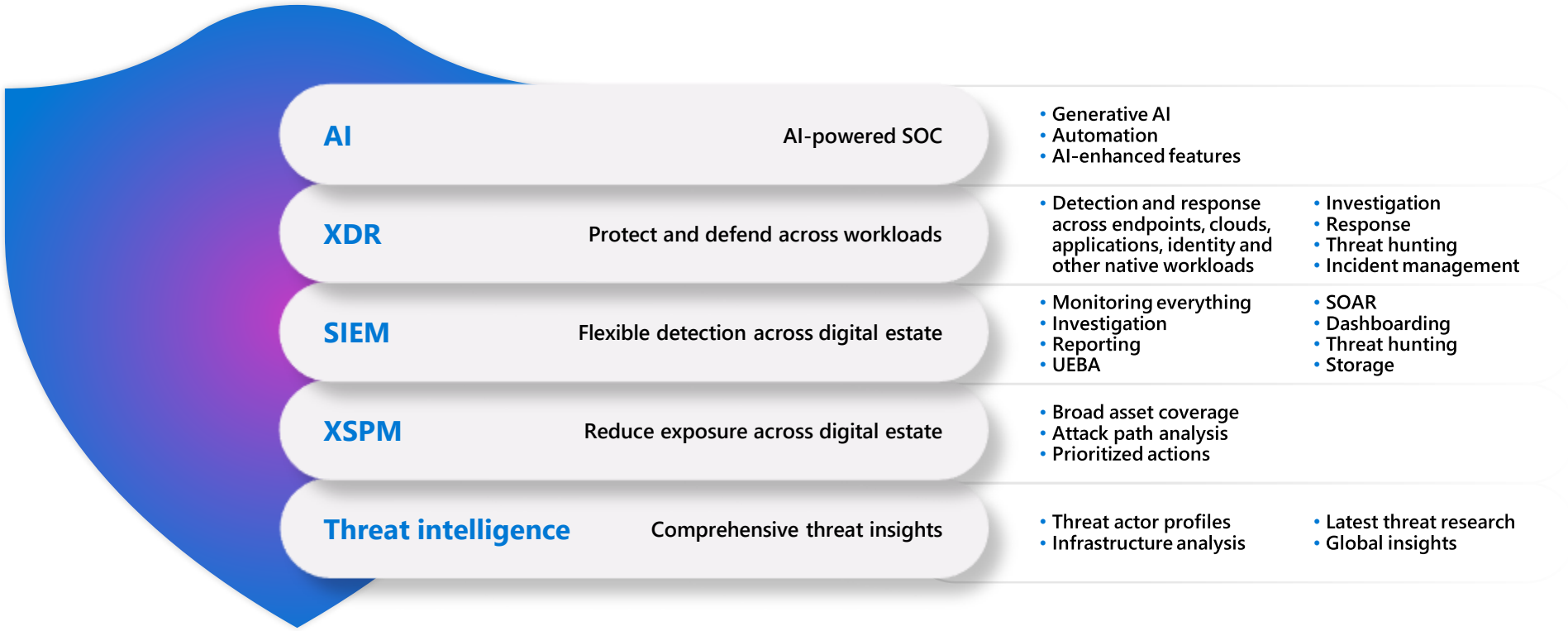
- ☐ Automation rule
- ☐ Playbook
- ☐ Workbook

3 **An Automation rule action can?**

- ☐ Update the incident title
- ☐ Delete the incident
- ☐ Change the incident status

It's time for a unified security operations platform

Optimized analyst experience | Targeted assistance | Automated protection and remediation



Empowering defenders to secure more & move quicker



Proactive Protection

Prevent

Block

Detect

Disrupt

Remediate

Securing organizations at machine speed



SOC Productivity

Delightful analyst experience

Guided with AI

Unified tools

Recommendations

Customizable automation

Quick time to value

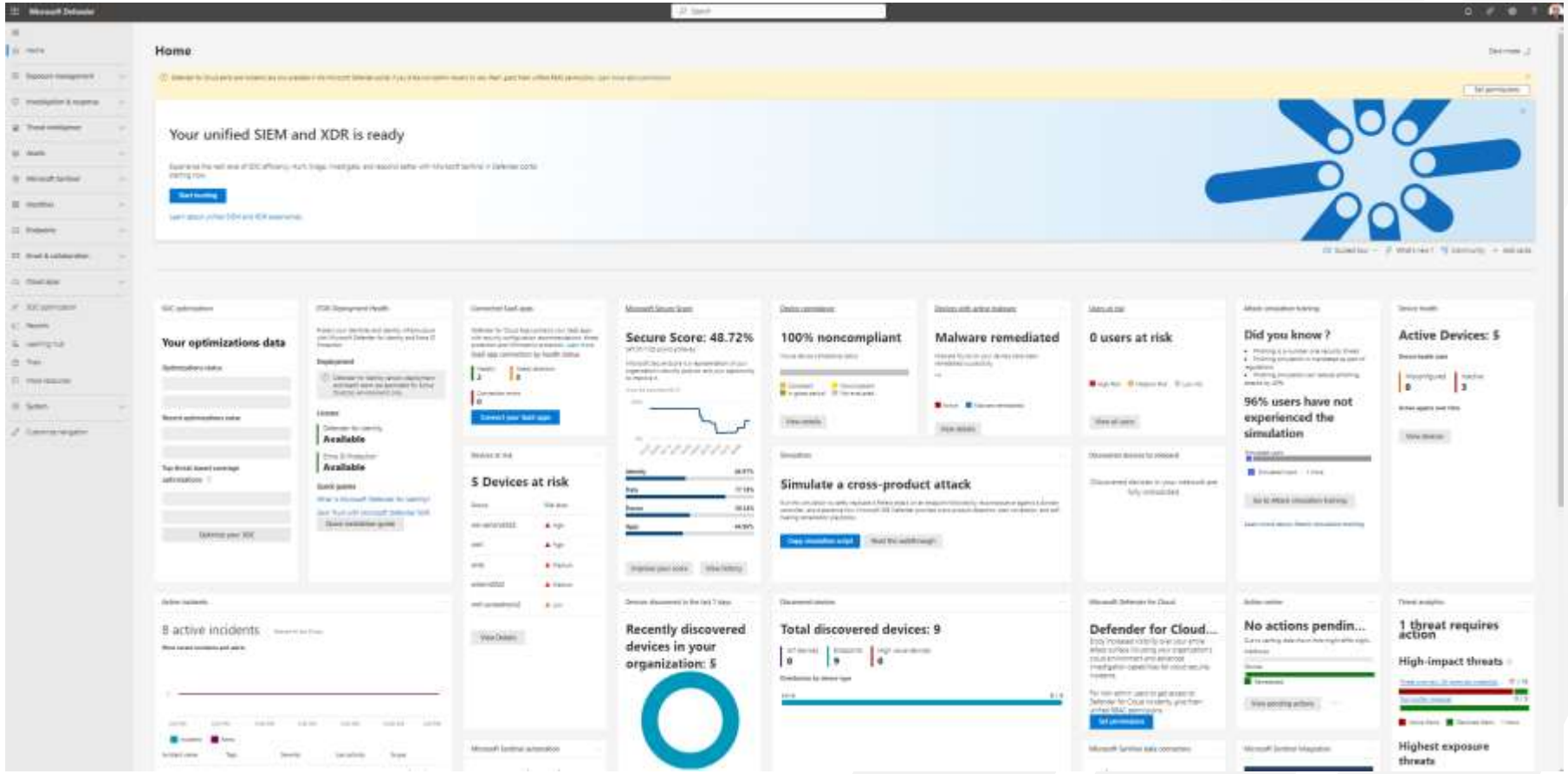
Uplevel the SOC to achieve more

Generative AI

Tailored optimizations

Threat research

Introducing the new unified security operations experience from Microsoft

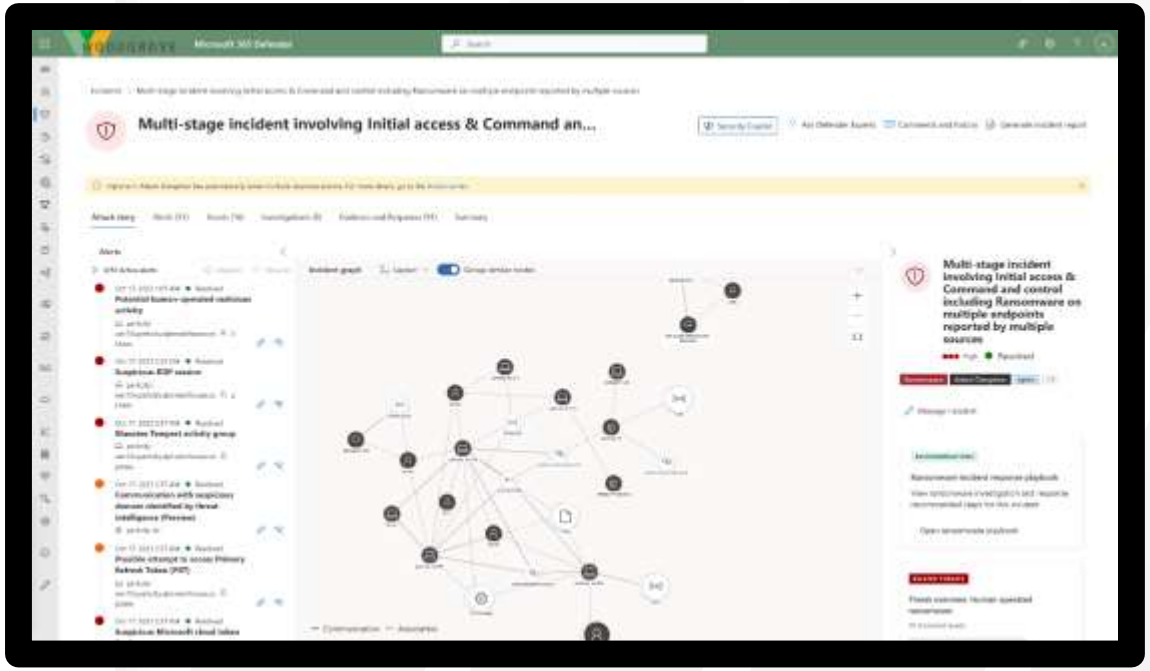


Automatic attack disruption for all MDE customers in Defender XDR

Automatically disrupt human-operated ransomware attacks
early in the kill chain

Prevent lateral movement
by automatically containing compromised users across all devices

On by default
for all MDE customers

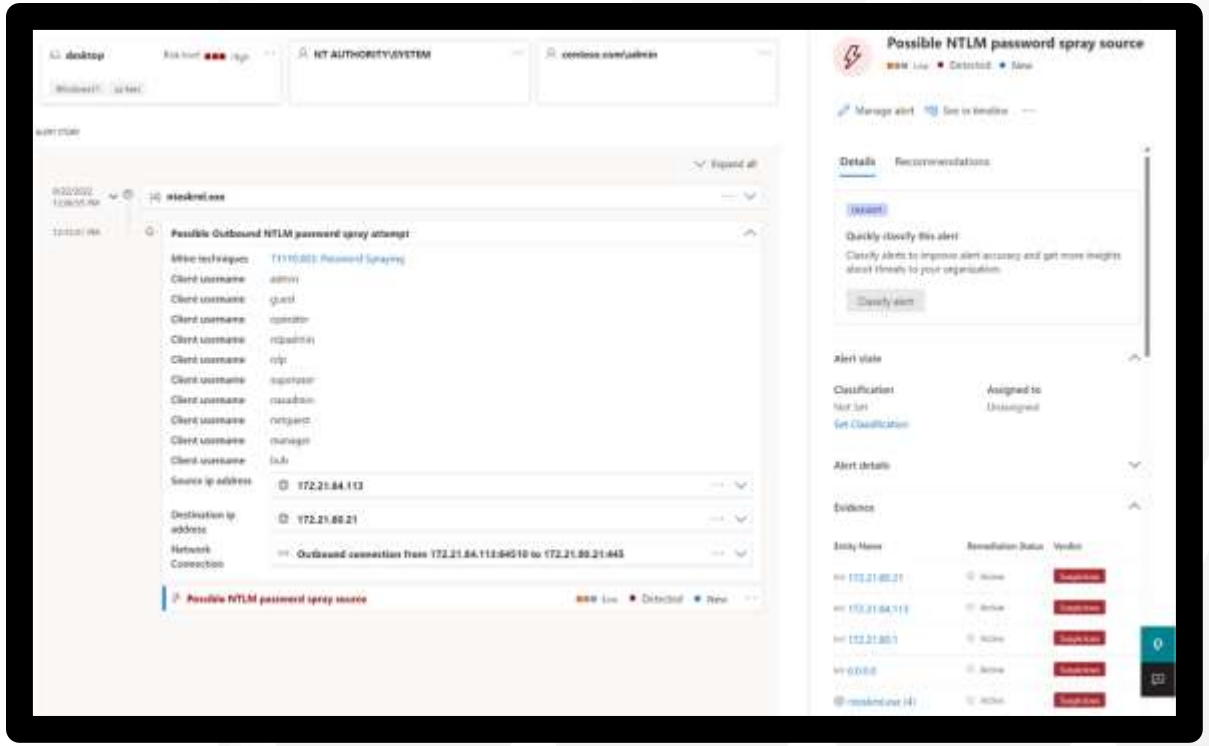


Get early-stage, high-confidence signal with deception techniques

Automatically generate decoys and lures resembling authentic endpoint profiles

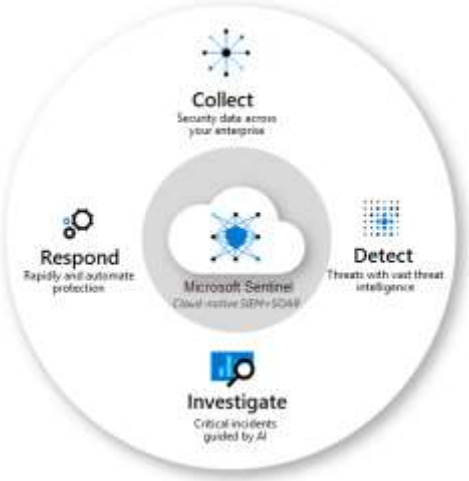
Detect threats more effectively and automatically disrupt with high fidelity signals from targeted decoys

Built into Microsoft's XDR reducing deployment and management friction



Introducing the new unified security operations experience from Microsoft

Microsoft Sentinel





Security Copilot



Microsoft

Thank you.