Building a Resilient SOC Workflow: Detection, Automation, and Visualization in Sentinel

Objective:

To enhance the organization's cybersecurity posture by leveraging advanced threat detection, automation, and data visualization tools within Microsoft Sentinel, ensuring proactive threat management and efficient incident response.

Executive Summary:

In a strategic initiative to bolster our cybersecurity defenses, I successfully implemented and configured various components of Microsoft Sentinel, focusing on automation, threat intelligence integration, and data visualization. This project involved setting up custom data connectors, creating advanced detection rules, and developing interactive workbooks to visualize security data. Additionally, I integrated threat intelligence on APT28—a known threat actor—to proactively detect and respond to sophisticated cyber threats. These efforts have significantly improved our ability to detect, investigate, and mitigate potential threats, thereby enhancing our overall security operations.

Microsoft Sentinel Content Hub and Data Connectors Documentation

Overview of Microsoft Sentinel Content Hub

The Microsoft Sentinel Content Hub is a unified interface designed to consolidate various security components, providing a comprehensive solution for organizations to manage their security operations. It offers essential Security Information and Event Management (SIEM) components that enable organizations to ingest data from diverse sources, monitor and detect threats, generate alerts, investigate security events, and automate responses.

Key Components of the Microsoft Sentinel Content Hub

1. **Data Connectors**
    - **Purpose**: Enable log ingestion from various sources, including Microsoft services, third-party security tools, and on-premises systems.
    - **Types**:
        - **Free Data Connectors**: Offer immediate value in Microsoft Sentinel while allowing time for planning and budgeting for additional connectors.
        - **Custom Data Connectors**: Allow organizations to build connectors for tools or applications not natively supported by Sentinel.
        - **Partner Data Connectors**: Facilitate integration with third-party tools that meet specific security requirements.
2. **Parsers**

    - **Purpose**: Convert raw log data into the Advanced Security Information Model (ASIM) format to ensure structured and consistent data across content types.
3. **Workbooks**
    - **Purpose**: Provide interactive dashboards for visualizing and monitoring log data, helping security teams derive actionable insights.
4. **Analytics Rules**
    - **Purpose**: Automatically detect anomalies and generate alerts by triggering automated actions based on defined logic.
5. **Hunting Queries**
    - **Purpose**: Enable security analysts to proactively search for threats and uncover hidden malicious activities.
6. **Notebooks**
    - **Purpose**: Facilitate advanced investigations using Jupyter and Azure notebooks, leveraging AI and machine learning for deeper threat analysis.
7. **Watchlists**
    - **Purpose**: Store custom datasets—such as VIP users, blocked IPs, or domains—to enhance detection precision and reduce alert fatigue.
8. **Playbooks and Logic Apps**
    - **Purpose**: Automate incident response and remediation workflows, integrating with external tools for streamlined security operations.

Connecting Data to Microsoft Sentinel

When selecting data connectors, adopt a prioritized approach:

1. **Free Data Connectors**: Use these first to gain quick value while planning for more complex integrations.
2. **Custom Data Connectors**: Evaluate the need for tailored integrations based on your environment.
3. **Partner Data Connectors**: Identify third-party tools that align with your organization's security stack.

Customizing Data Connector Settings

To optimize both visibility and cost-efficiency:

1. **Azure Portal Setup**:
    - Search for *Microsoft Sentinel* and select your workspace.
    - Navigate to **Content Management** > **Content Hub**.
    - Search for and install relevant connectors (e.g., Microsoft Defender for Cloud Apps).
    - Configure connector settings to ingest only essential data types.
2. **Cost Management**:
    - Use Sentinel's built-in cost analysis tools.

- Review and fine-tune data retention policies to reduce unnecessary storage.
- Leverage filters and automation rules to manage log ingestion efficiently.

Free Data Connectors and Their Data Types

As of now, the following connectors and associated data types are available **at no cost** in Microsoft Sentinel and Log Analytics:

- **Azure Activity Logs**
- **Health Monitoring for Microsoft Sentinel**
- **Microsoft Entra ID Protection (formerly Azure AD Protection)**
- **Office 365**
- **Microsoft Defender for Cloud**
- **IoT XDR**
- **Endpoint Identity and Cloud Apps**

Note: While security alerts from Microsoft services are often free, ingesting raw logs may incur charges. Prioritize only critical data streams to stay within budget.

Custom Data Connectors

If a required tool or platform isn't supported natively, consider building a custom data connector using the following options:

1. **Codeless Connector Platform (CCP)**:
   - Enables users to build connectors without writing code.
   - Utilizes configuration files for easy setup.
   - Fully SaaS-based, requiring no additional infrastructure.
2. **Azure Monitor Agent (AMA)**:
   - Collects and forwards custom logs from text-based sources.
   - More efficient and secure than legacy Log Analytics agents.
   - Centralizes data collection and supports advanced filtering to reduce ingestion overhead.
3. **Logstash**:
   - An open-source data pipeline for collecting, transforming, and forwarding logs.
   - Supports extensive input sources and complex filtering logic.
   - Uses Microsoft Sentinel's Logstash output plugin to forward data directly into Sentinel.
4. **Azure Logic Apps**:
   - A serverless automation tool that enables custom data ingestion workflows.
   - Ideal for low-volume log injection or data enrichment scenarios.

    - Supports real-time, event-driven processing without managing backend infrastructure.
5. **Log Injection API**:
    - Uses the Log Analytics Data Collector API to send logs directly into Sentinel.

Conclusion

The Microsoft Sentinel Content Hub provides a powerful suite of tools for enhancing security visibility, detection, and response. By strategically selecting and configuring data connectors, organizations can improve operational efficiency, optimize detection capabilities, and manage costs effectively.

Future chapters will explore each content type in detail, offering hands-on implementation strategies and best practices.

Microsoft Sentinel Custom Data Connectors and Entra ID Integration Documentation

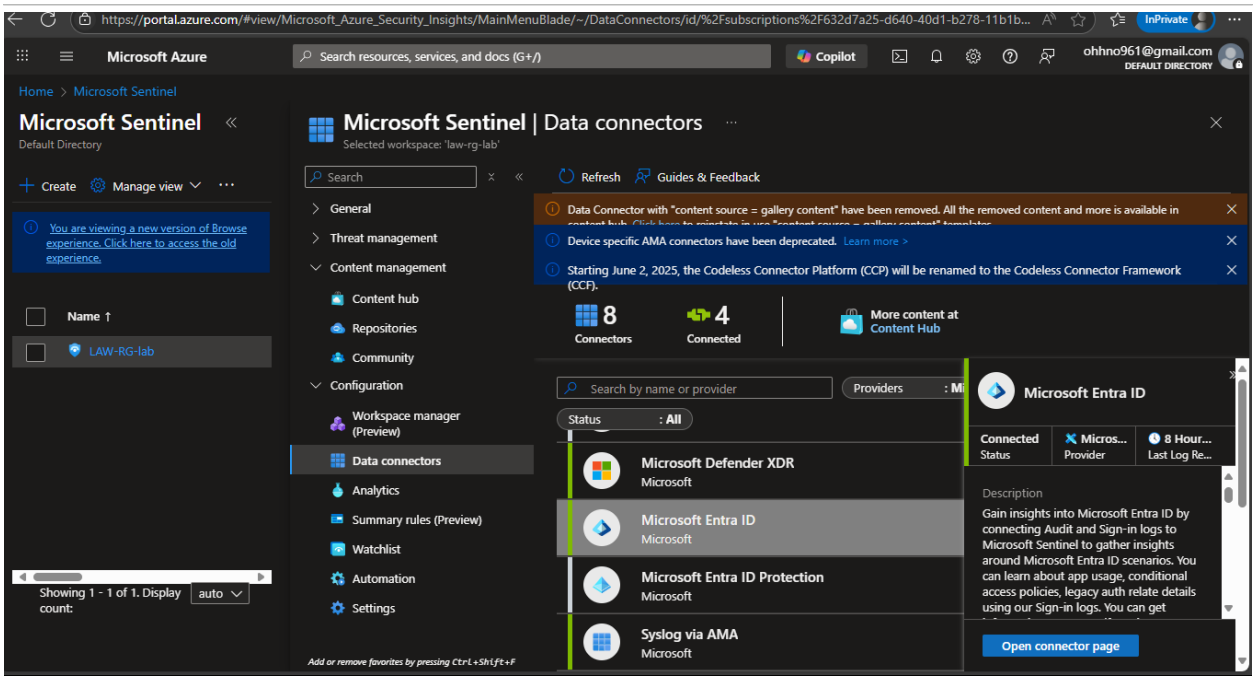
Custom Data Connectors

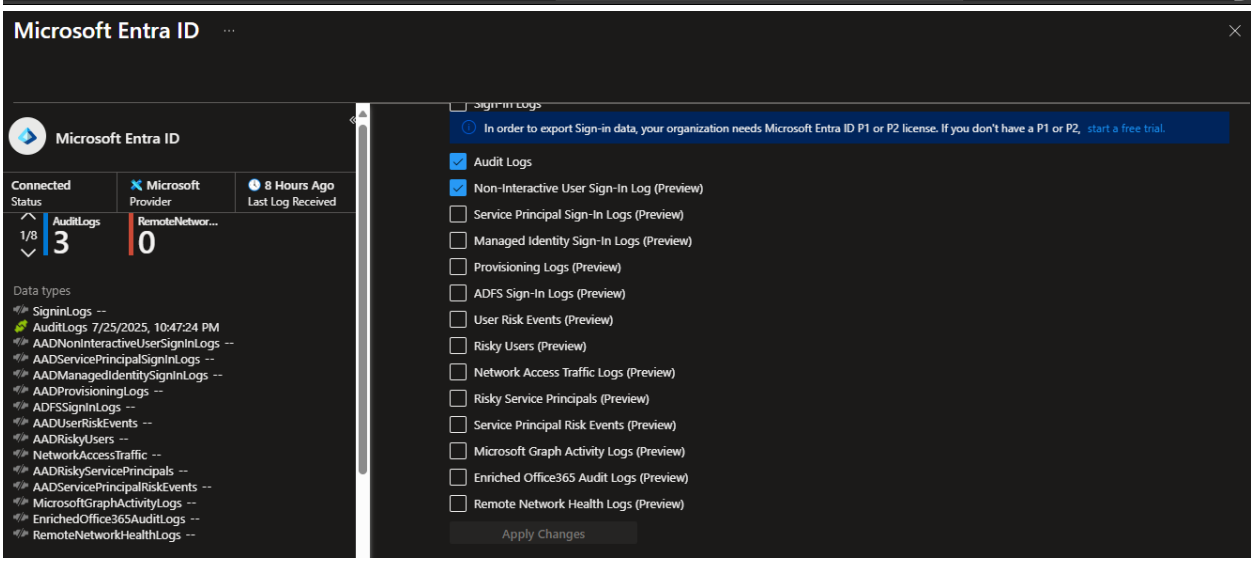
Creating custom data connectors for Microsoft Sentinel is essential when you need to integrate data sources that are not natively supported. Here are the available methods for creating custom connectors:

1. **Codeless Connector Platform (CCP)**
    - **Description**: Allows customers and partners to create custom data connectors without writing code.
    - **Features**:
        - Uses a configuration file for easy deployment.
        - Can be deployed to your own workspace or as a solution in the Microsoft Sentinel Hub.
        - Fully SaaS-based with no need for additional service installations.
        - Includes health monitoring and full Microsoft Sentinel support.
    - **Use Case**: A security team wants to ingest logs from a third-party SaaS application not natively supported by Sentinel. CCP can be used to configure and deploy a codeless connector, reducing development effort and maintenance costs.
2. **Azure Monitor Agent (AMA)**
    - **Description**: Collects and sends custom log data from text-based event sources to Microsoft Sentinel.
    - **Features**:
        - Best for text-based log sources like application logs or system logs.
        - More efficient and secure than legacy agents such as Log Analytics agents.

        - Provides centralized data collection and advanced filtering to optimize log ingestion costs.
    - **Use Case**: If your company has a legacy application that generates security logs as text files, you can configure Azure Monitor Agent to collect and forward logs to Microsoft Sentinel.
3. **Logstash**
    - **Description**: An open-source data processing pipeline that collects, transforms, and routes log data from various sources.
    - **Features**:
        - Supports a wide range of input sources, including files, databases, cloud services, and event hubs.
        - Allows for advanced filtering, such as parsing logs, removing unnecessary data, and masking sensitive information.
        - Uses the Microsoft Sentinel Logstash output plug-in to send transformed data directly to Sentinel.
    - **Use Case**: A company collects AWS CloudTrail logs for threat detection. Instead of sending raw logs, Logstash can be used to filter out unnecessary events and mask sensitive data before sending it to Sentinel.
4. **Azure Logic Apps**
    - **Description**: A serverless workflow automation service that enables custom connectors without managing infrastructure.
    - **Features**:
        - Best for low-volume data injection or enriching existing data in Sentinel.
        - Automates data retrieval from APIs, databases, and files.
        - Supports event-driven workflows for real-time data streaming.
        - Drag-and-drop interface for workflow creation.
    - **Use Case**: Suitable for recurring tasks like scheduling data retrieval from APIs, databases, or files (e.g., fetching logs from a SaaS platform every 15 minutes). It can also be used for on-demand triggering and real-time streaming when the source system can push data to Sentinel.
5. **Log Injection API**
    - **Description**: Allows sending log data directly to Microsoft Sentinel through a RESTful endpoint.
    - **Features**:
        - Maximum flexibility to customize log ingestion from any source.
        - Real-time data streaming, pushing logs as events occur.
        - No dependency on other tools—works independently of Logic Apps, AMA, or Logstash.
        - Supports structured data (JSON-formatted logs).
    - **Use Case**: An organization wants to stream real-time security logs from a custom application. A Python script can be developed to format logs as JSON and send them to Sentinel using the API.
6. **Azure Functions**
    - **Description**: A serverless computing service that allows executing code in response to events such as HTTP requests, timers, or messages from other services.

- **Features**:
  - Supports multiple programming languages (e.g., Python, PowerShell, JavaScript).
  - Execution time limits (default is 5 minutes for the consumption plan).
  - Not recommended for high-volume data ingestion.
- **Use Case**: Develop an Azure Function in PowerShell or Python to receive logs through REST API HTTP triggers or event sources, transform and format the logs into the required schema, and then send the logs to Sentinel using the Log Analytics API.





Connecting Entra ID to Microsoft Sentinel

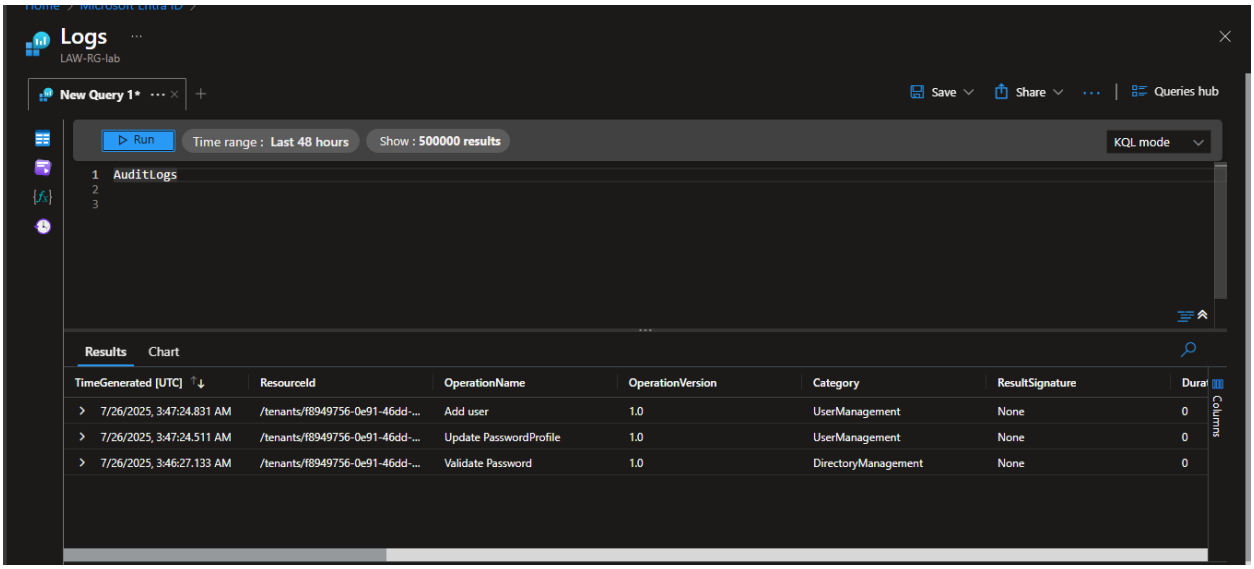
Entra ID (formerly known as Azure Active Directory) is Microsoft's cloud-based identity and access management service. Connecting Entra ID to Microsoft Sentinel allows you to ingest audit logs, sign-in logs, provisioning logs, risk events, and logs related to risky users or service principals.

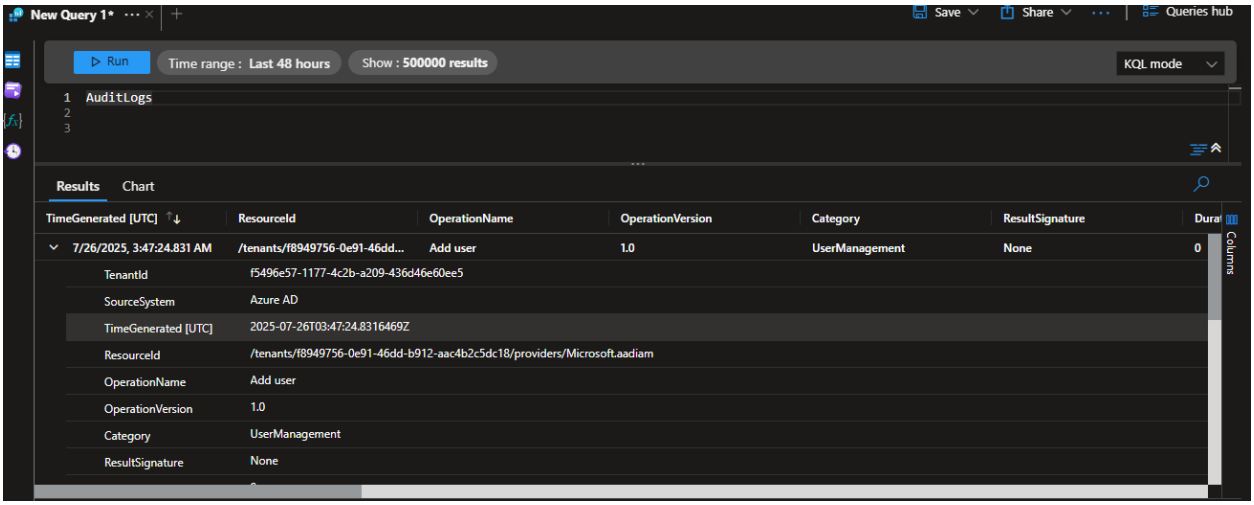
Steps to Connect Entra ID to Microsoft Sentinel:

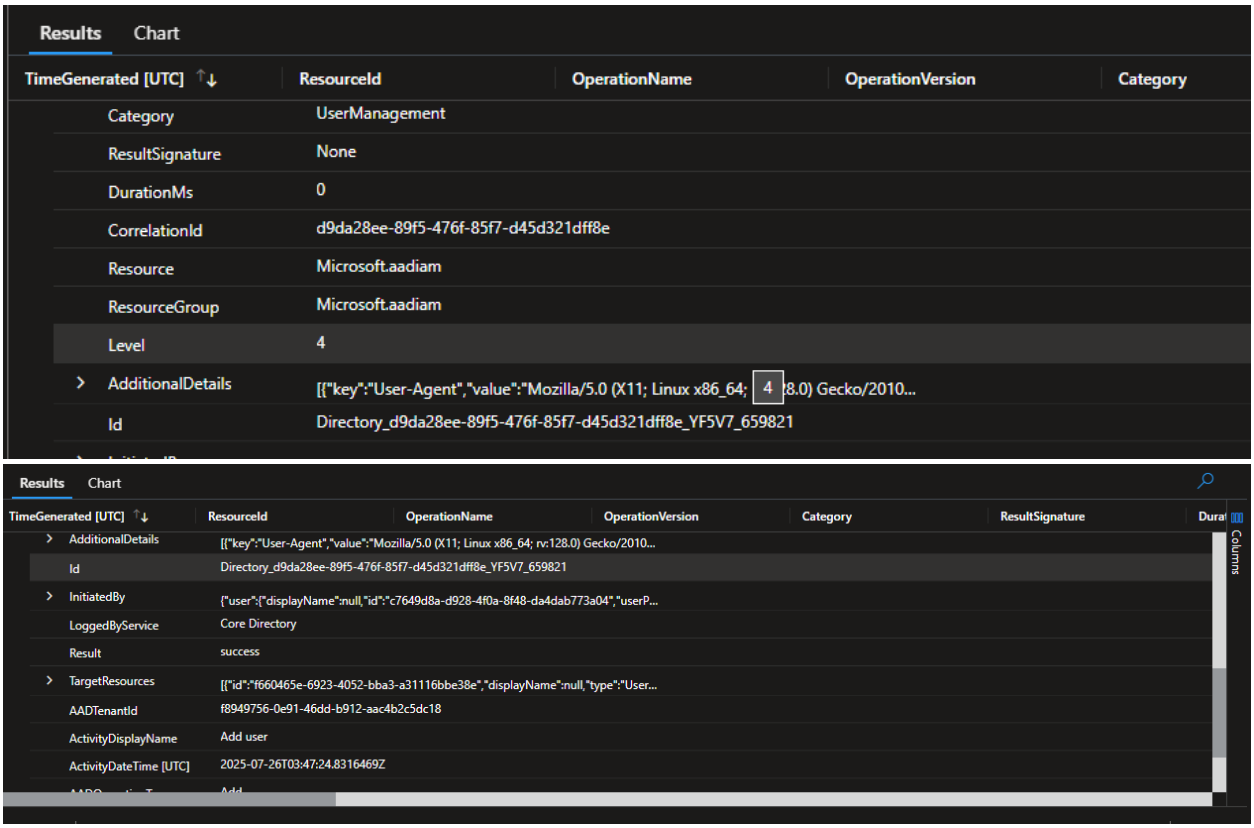
1. **Azure Portal Setup**:
    - Log in to the Azure portal.
    - Search for and select **Entra ID**.
    - Navigate to the **Monitoring** section to view sign-in logs, audit logs, and provisioning logs.
2. **Install Entra ID Solution in Sentinel**:
    - Search for **Microsoft Sentinel** in the Azure portal.
    - Select your Sentinel workspace.
    - Under **Content Management**, go to **Content Hub**.
    - Search for and install the **Microsoft Entra ID** solution.
3. **Configure Diagnostic Settings**:
    - Ensure your workspace has read and write permissions.
    - Ensure diagnostic settings have read and write permissions to Microsoft Entra ID.
    - Ensure tenant-level permissions (Global Administrator or Security Administrator).
    - In **Entra ID**, go to **Diagnostic Settings** and create a new setting to send audit logs, sign-in logs, and provisioning logs to your Sentinel workspace.
4. **Verify Log Ingestion**:
    - After configuring diagnostic settings, go to the **Microsoft Sentinel** workspace.
    - Navigate to the **Logs** section and run queries to verify that audit and sign-in logs are being ingested.
    - Example KQL queries:
      ```
      AuditLogs
      SigninLogs
      ```

Conclusion

This documentation provides an overview of creating custom data connectors using CCP, AMA, Logstash, Azure Logic Apps, the Log Injection API, and Azure Functions. It also outlines the steps to connect Entra ID to Microsoft Sentinel, ensuring that relevant logs are ingested for security monitoring and analysis. Future chapters will explore each component in depth, including implementation steps and best practices.


Logs
LAW-RG-lab
New Query 1*
Save
Share
Queries hub
Run
Time range : Last 48 hours
Show : 500000 results
KQL mode
1 AuditLogs
2
3
Results
Chart
TimeGenerated [UTC]
ResourceId
OperationName
OperationVersion
Category
ResultSignature
Dura
7/26/2025, 3:47:24.831 AM
/tenants/f8949756-0e91-46dd-...
Add user
1.0
UserManagement
None
0
7/26/2025, 3:47:24.511 AM
/tenants/f8949756-0e91-46dd-...
Update PasswordProfile
1.0
UserManagement
None
0
7/26/2025, 3:46:27.133 AM
/tenants/f8949756-0e91-46dd-...
Validate Password
1.0
DirectoryManagement
None
0
Columns


New Query 1*
Save
Share
Queries hub
Run
Time range : Last 48 hours
Show : 500000 results
KQL mode
1 AuditLogs
2
3
Results
Chart
TimeGenerated [UTC]
ResourceId
OperationName
OperationVersion
Category
ResultSignature
Dura
7/26/2025, 3:47:24.831 AM
/tenants/f8949756-0e91-46dd...
Add user
1.0
UserManagement
None
0
TenantId
f5496e57-1177-4c2b-a209-436d46e60ee5
SourceSystem
Azure AD
TimeGenerated [UTC]
2025-07-26T03:47:24.8316469Z
ResourceId
/tenants/f8949756-0e91-46dd-b912-aac4b2c5dc18/providers/Microsoft.aadiam
OperationName
Add user
OperationVersion
1.0
Category
UserManagement
ResultSignature
None
Columns



Microsoft Sentinel Threat Intelligence and Analytics Rules Documentation

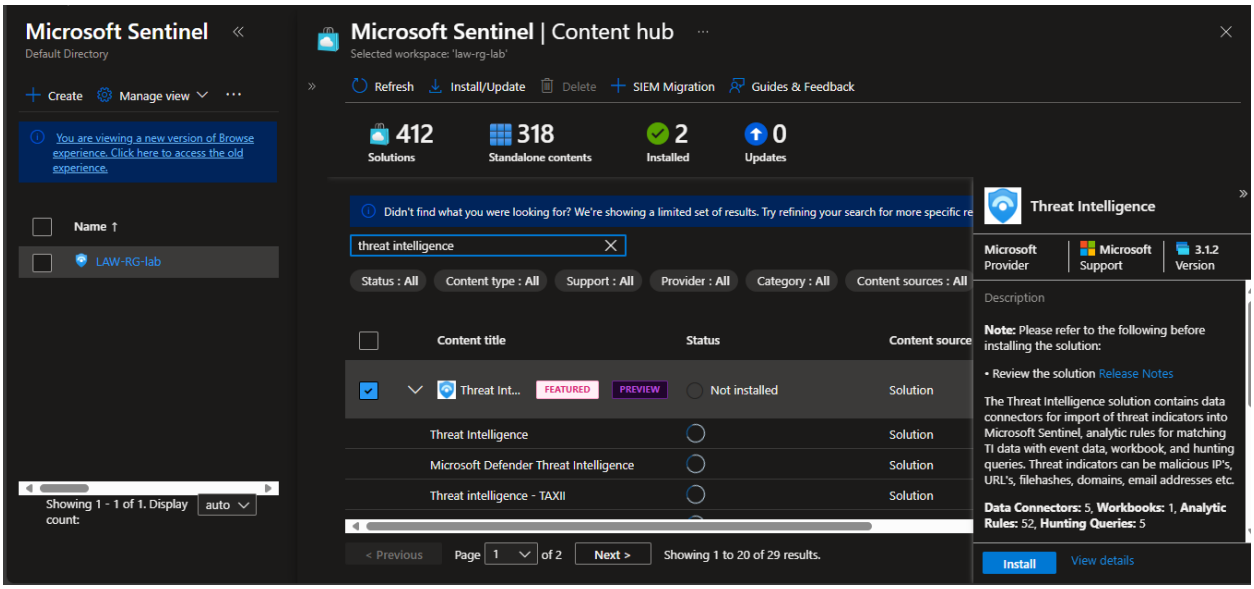
Threat Intelligence in Microsoft Sentinel

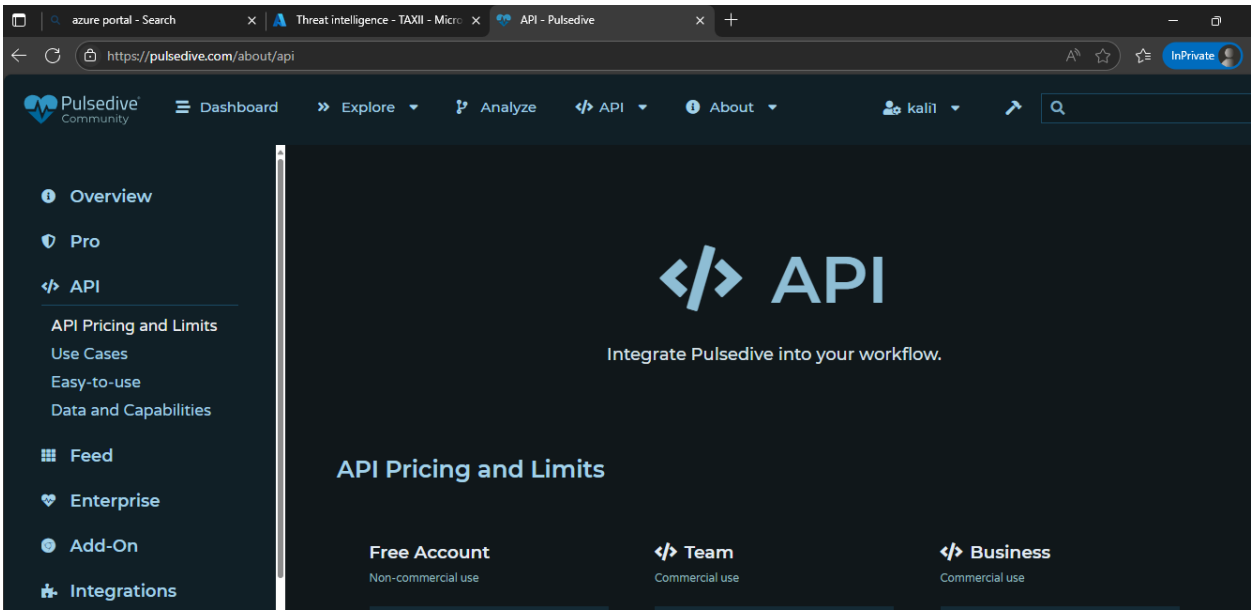
Threat intelligence is a crucial component of Microsoft Sentinel, providing organizations with actionable insights to identify and mitigate potential threats. Here's an overview of threat intelligence and its integration with Sentinel:

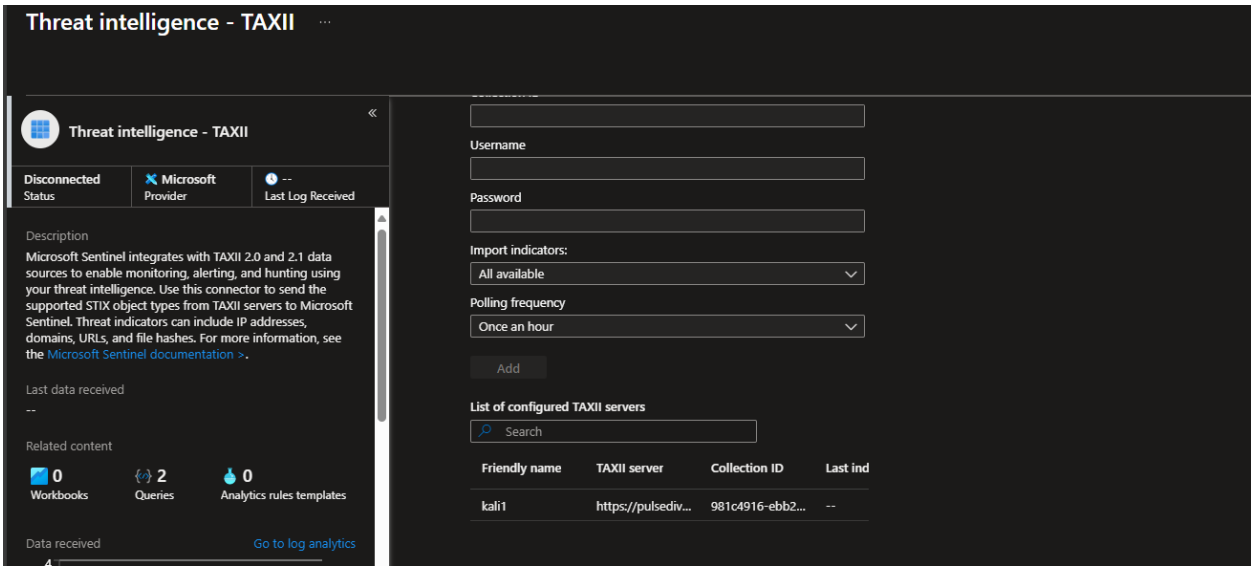
1. **Components of Threat Intelligence**:
    - **Data Collection**: Gathering raw data from multiple sources such as open-source intelligence, commercial feeds, internal logs, and information-sharing communities.
    - **Analysis**: Processing and analyzing the collected data to uncover patterns and TTPs (Tactics, Techniques, and Procedures) used by threat actors.
    - **Dissemination**: Sharing actionable intelligence with security teams, decision-makers, and automated systems to enable proactive defense and rapid response.
2. **Why Threat Intelligence Matters**:
    - **Proactive Defense**: Anticipate and prepare for potential attacks.
    - **Enhanced Detection**: Improve the ability to detect and block threats early.
    - **Informed Decision-Making**: Shape security policies and investments.
    - **Improved Incident Response**: Quickly identify, contain, and remediate incidents.
3. **Importing Threat Intelligence into Sentinel**:

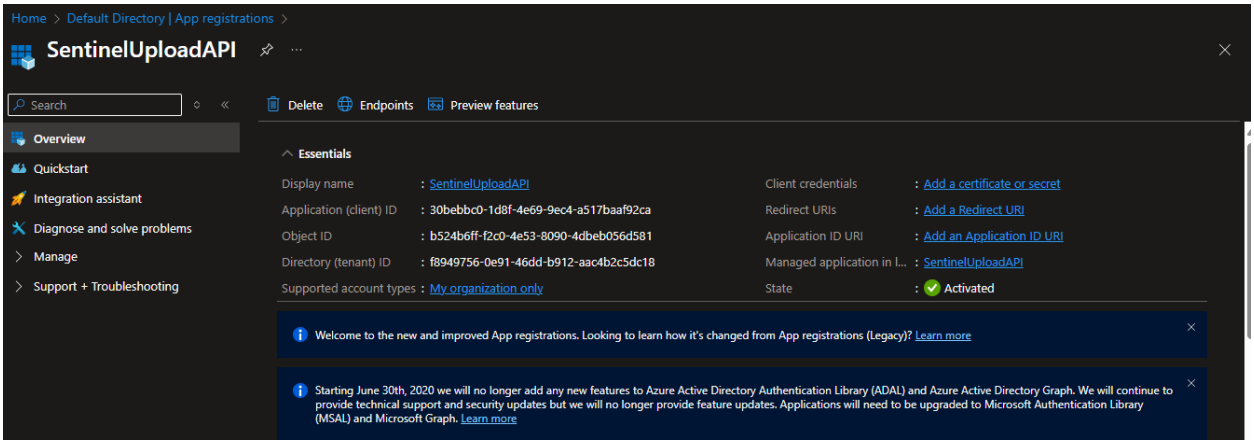
- **Microsoft Defender Threat Intelligence Connector**:
  - **Standard Connector**: Free; ingests public and open-source threat intelligence.
  - **Premium Connector**: Paid; provides enriched and curated IoCs (Indicators of Compromise) for deeper analytics.
- **Threat Intelligence TAXII**:
  - **TAXII (Trusted Automated Exchange of Indicator Information)**: A standardized protocol for sharing cybersecurity threat intelligence.
  - **STIX (Structured Threat Information eXpression)**: Defines the format for threat data.
  - **Sentinel TAXII Data Connector**: Enables importing threat intelligence in STIX format from TAXII servers.
- **Threat Intelligence Upload API**:
  - **Description**: Allows organizations to import STIX objects directly into Microsoft Sentinel.
  - **Requirements**: Microsoft Sentinel Contributor role, Microsoft Entra application, and API permissions.
- **Threat Intelligence Platform (TIP)**:
  - **Deprecation Notice**: This data connector is being deprecated. Microsoft recommends switching to the Threat Intelligence Upload API.

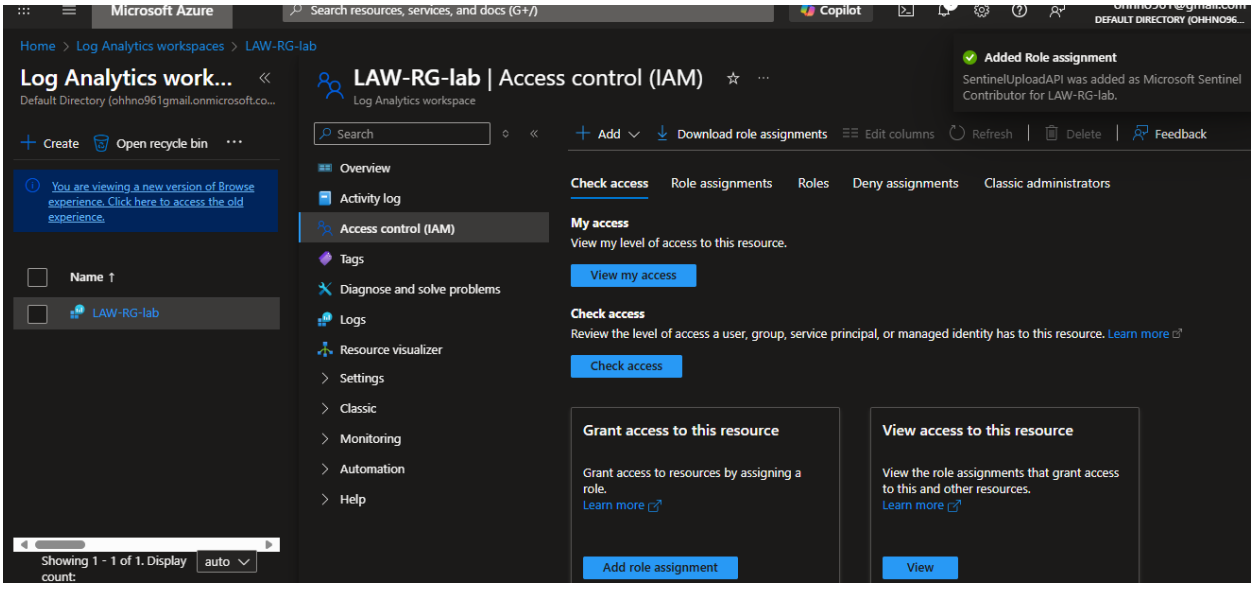
4. **Using Threat Intelligence in Sentinel**:
   - **Upload Threat Intelligence Files**: Import data using CSV or JSON files.
   - **Threat Indicators in Analytics Rules**: Use matching analytics to detect threats.
   - **Threat Indicators in Incidents**: Add indicators to incidents for detailed analysis.


Microsoft Sentinel
Default Directory
Create
Manage view
You are viewing a new version of Browse experience. Click here to access the old experience.
Name ↑
LAW-RG-lab
Showing 1 - 1 of 1. Display count:
auto
Microsoft Sentinel | Content hub
Selected workspace: 'law-rg-lab'
Refresh
Install/Update
Delete
SIEM Migration
Guides & Feedback
412
Solutions
318
Standalone contents
2
Installed
0
Updates
Didn't find what you were looking for? We're showing a limited set of results. Try refining your search for more specific re
threat intelligence
Status : All
Content type : All
Support : All
Provider : All
Category : All
Content sources : All
Content title
Status
Content source
Threat Int...
FEATURED
PREVIEW
Not installed
Solution
Threat Intelligence
Solution
Microsoft Defender Threat Intelligence
Solution
Threat intelligence - TAXII
Solution
< Previous
Page 1 of 2
Next >
Showing 1 to 20 of 29 results.
Threat Intelligence
Microsoft Provider
Microsoft Support
3.1.2 Version
Description
Note: Please refer to the following before installing the solution:
• Review the solution Release Notes
The Threat Intelligence solution contains data connectors for import of threat indicators into Microsoft Sentinel, analytic rules for matching TI data with event data, workbook, and hunting queries. Threat indicators can be malicious IP's, URL's, filehashes, domains, email addresses etc.
Data Connectors: 5, Workbooks: 1, Analytic Rules: 52, Hunting Queries: 5
Install
View details


azure portal - Search
Threat intelligence - TAXII - Micro
API - Pulsedive
https://pulsedive.com/about/api
InPrivate
Pulsedive Community
Dashboard
Explore
Analyze
API
About
kali
Overview
Pro
API
API Pricing and Limits
Use Cases
Easy-to-use
Data and Capabilities
Feed
Enterprise
Add-On
Integrations
API
Integrate Pulsedive into your workflow.
API Pricing and Limits
Free Account
Non-commercial use
Team
Commercial use
Business
Commercial use



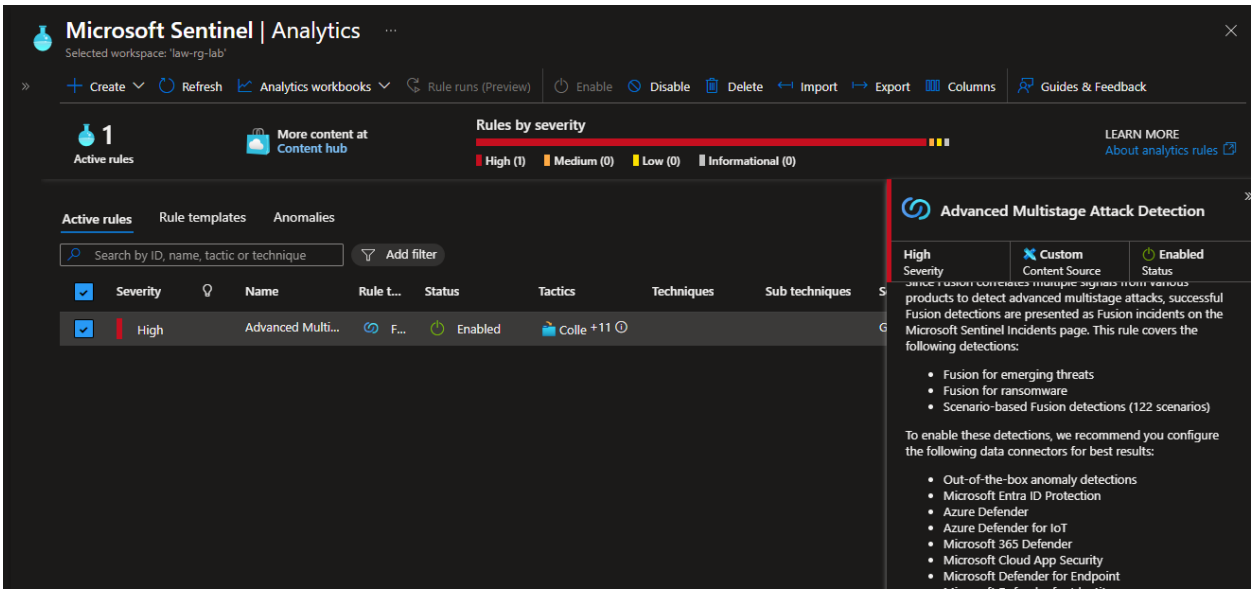


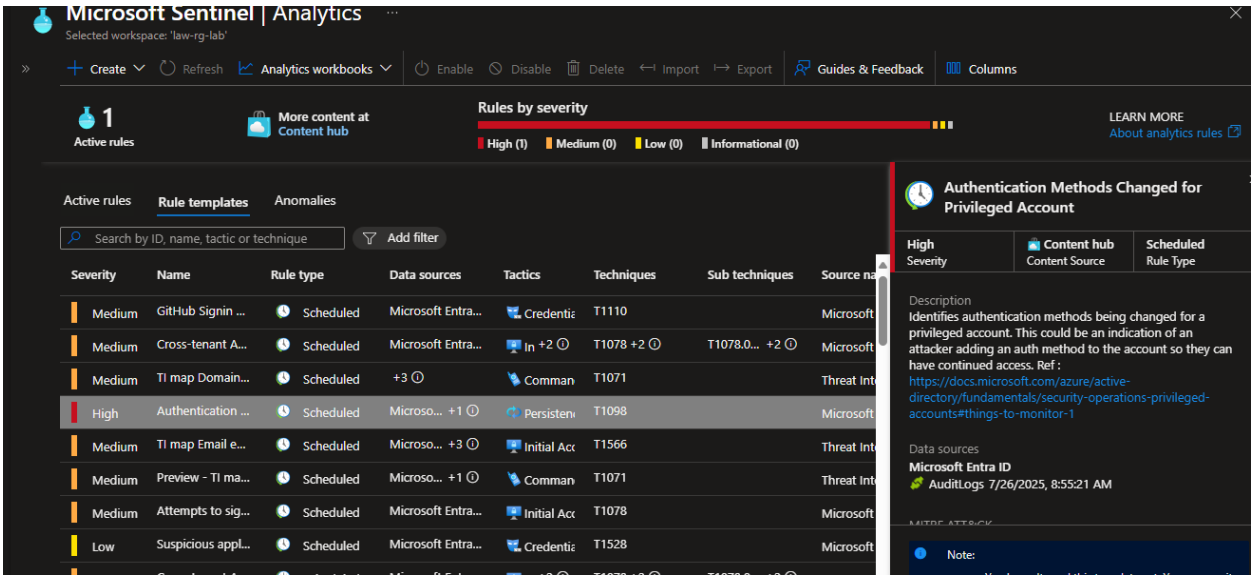


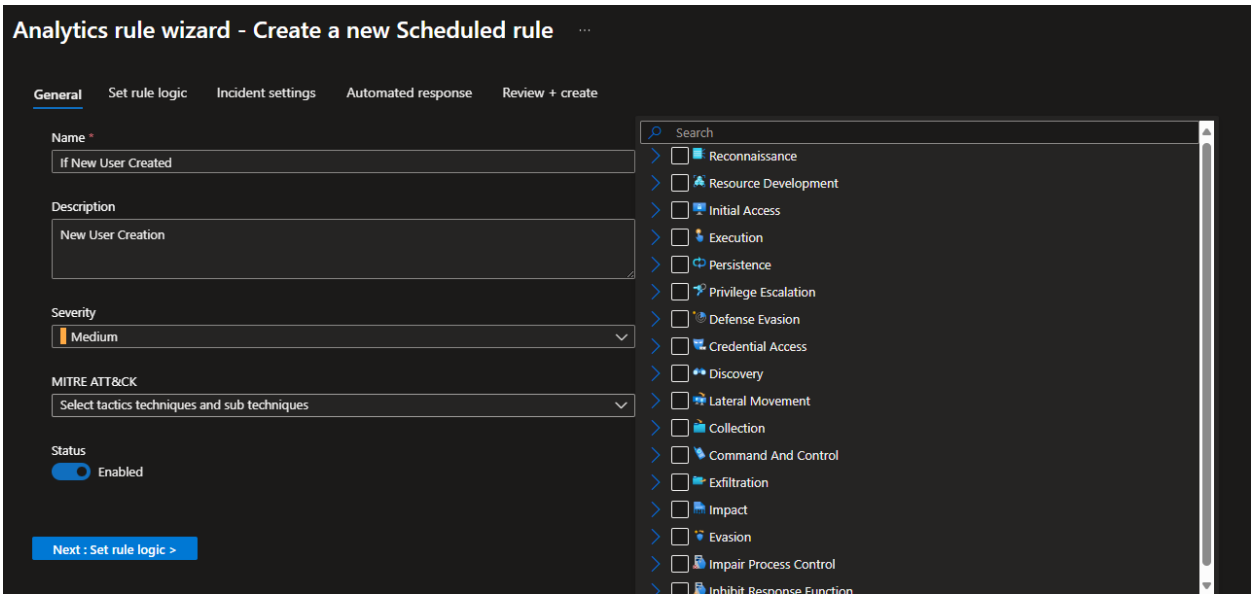
Analytics Rules in Microsoft Sentinel

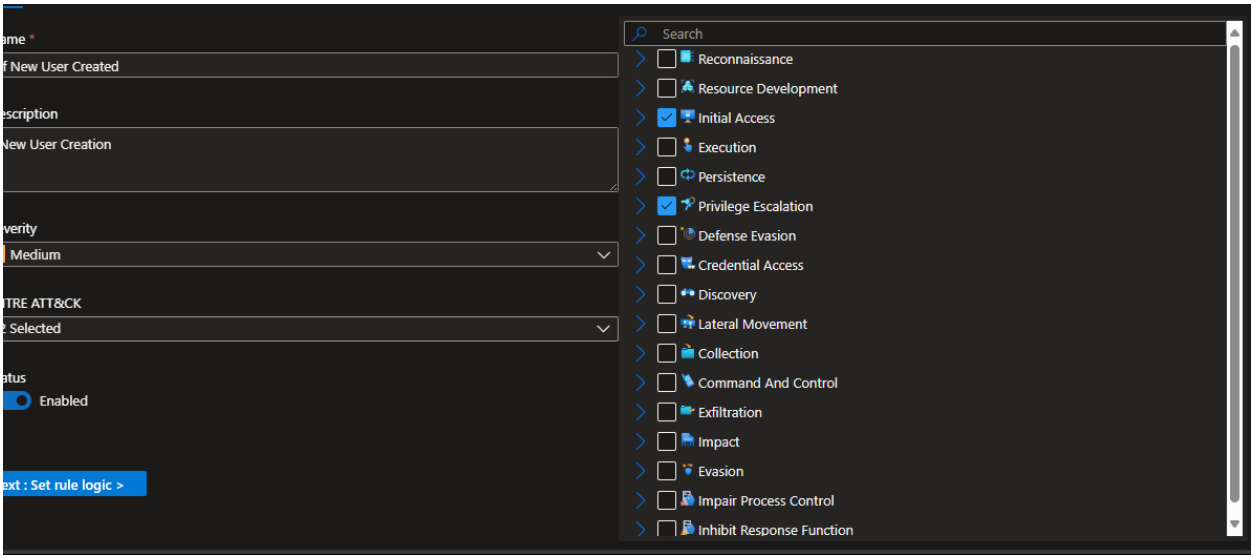
Analytics rules are automated detection mechanisms that continuously analyze security data to identify potential threats. Here's an overview of the main types of analytics rules and how to create them:

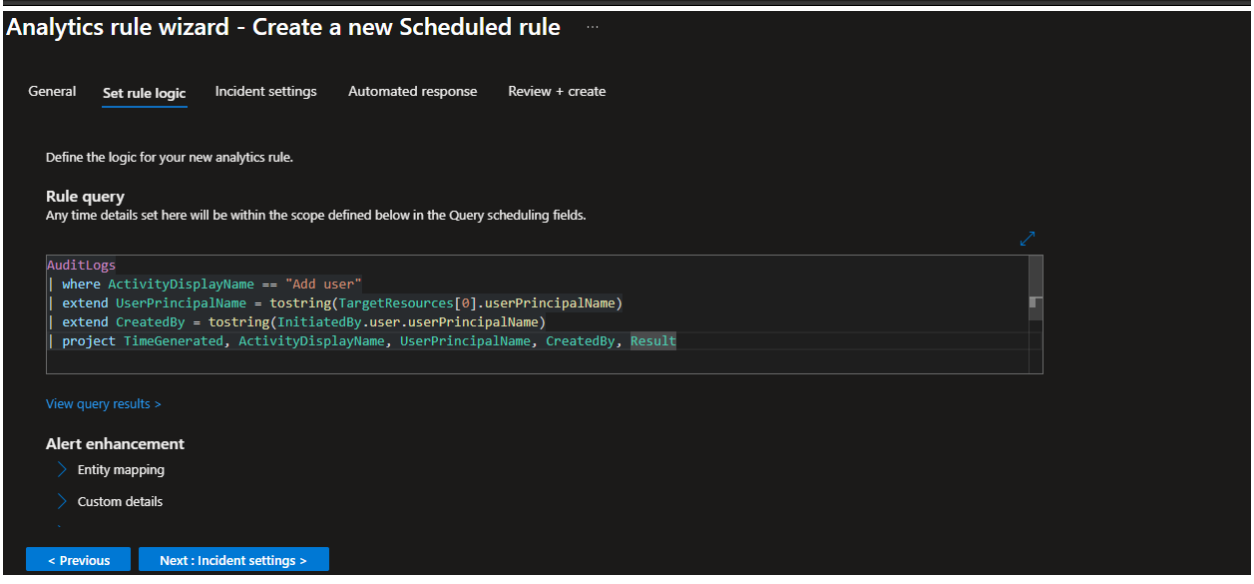
1. **Types of Analytics Rules**:
    - **Scheduled Rules**: Run at predefined intervals to scan collected logs for specific patterns.
    - **Near Real-Time (NRT) Rules**: Execute queries at high frequency for rapid threat detection.
    - **Anomaly Rules**: Use machine learning to detect unusual behaviors.
    - **Microsoft Security Rules**: Integrate with Microsoft security products to generate alerts in Sentinel.
    - **Specialized Rules**:
        - **Threat Intelligence Rules**: Compare ingested logs against known threat indicators.
        - **Fusion Rules**: Correlate multiple low-confidence signals to detect complex attacks.
        - **Machine Learning Behavior Analytics**: Use AI-driven behavioral analytics to spot evolving threats.
2. **Creating Analytics Rules**:
    - **Scheduled Rule Example**:
        - **Rule Name**: New User Creation
        - **Description**: Detects new user creation events.
        - **Severity**: Medium
        - **MITRE ATT&CK**: Initial Access, Privilege Escalation
        - **Rule Query**: KQL query to fetch and filter Azure AD audit logs for user creation events.
        - **Entity Mapping**: Map entities like user principal names to enhance alert details.
        - **Alert Enhancement**: Add custom details to alerts for faster triage.
        - **Query Scheduling**: Run the query every 5 hours; look back at the last 5 hours.
        - **Alert Threshold**: Generate an alert when the number of query results is greater than zero.
        - **Incident Settings**: Group related alerts into a single incident.
        - **Automated Response**: Create automation rules for automated responses.
    - **Near Real-Time Rule Example**:
        - **Rule Name**: New User Creation (NRT)
        - **Description**: Detects new user creation events in near real-time.
        - **Severity**: Medium
        - **MITRE ATT&CK**: Initial Access
        - **Rule Query**: Same KQL query as the scheduled rule.
        - **Incident Settings**: Group related alerts into a single incident.
        - **Automated Response**: Create automation rules for automated responses.

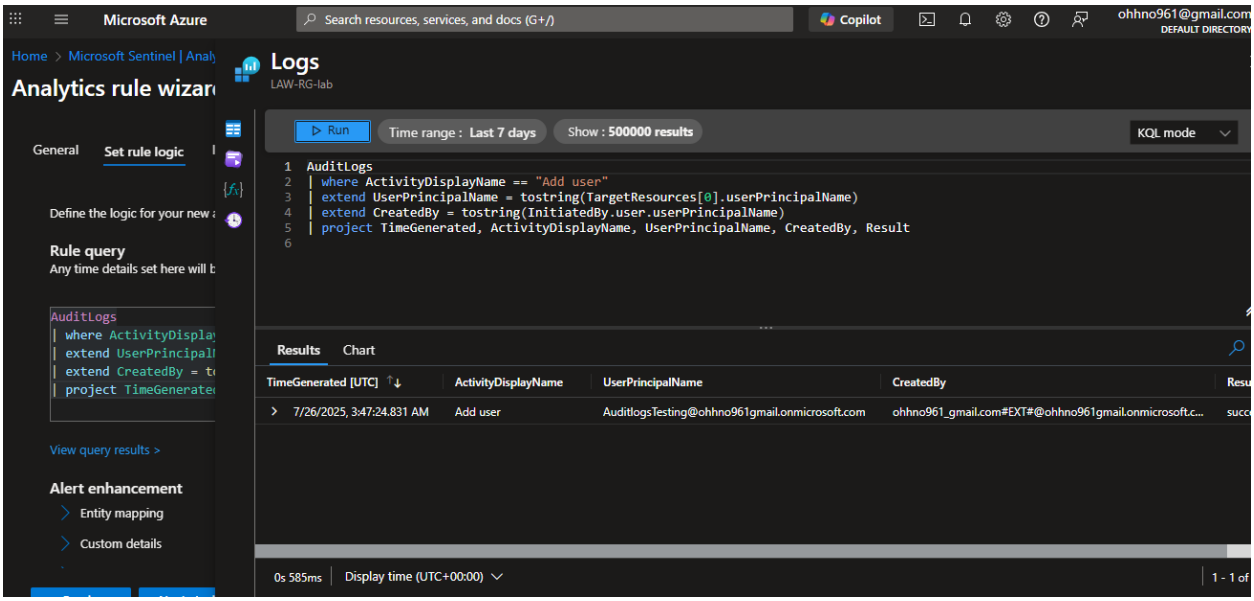

Microsoft Sentinel | Analytics
Selected workspace: 'law-rg-lab'
Create
Refresh
Analytics workbooks
Rule runs (Preview)
Enable
Disable
Delete
Import
Export
Columns
Guides & Feedback
1
Active rules
More content at
Content hub
Rules by severity
High (1)
Medium (0)
Low (0)
Informational (0)
LEARN MORE
About analytics rules
Active rules
Rule templates
Anomalies
Search by ID, name, tactic or technique
Add filter
Severity
Name
Rule t...
Status
Tactics
Techniques
Sub techniques
High
Advanced Multi...
F...
Enabled
Colle +11
Advanced Multistage Attack Detection
High
Severity
Custom
Content Source
Enabled
Status
products to detect advanced multistage attacks, successful Fusion detections are presented as Fusion incidents on the Microsoft Sentinel Incidents page. This rule covers the following detections:
Fusion for emerging threats
Fusion for ransomware
Scenario-based Fusion detections (122 scenarios)
To enable these detections, we recommend you configure the following data connectors for best results:
Out-of-the-box anomaly detections
Microsoft Entra ID Protection
Azure Defender
Azure Defender for IoT
Microsoft 365 Defender
Microsoft Cloud App Security
Microsoft Defender for Endpoint

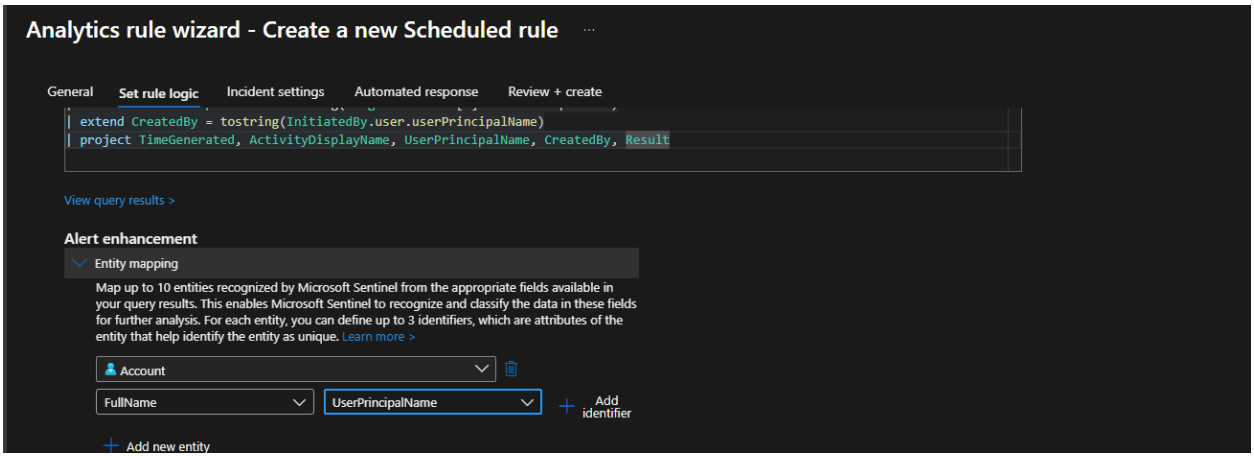

Microsoft Sentinel | Analytics
Selected workspace: 'law-rg-lab'
Create
Refresh
Analytics workbooks
Enable
Disable
Delete
Import
Export
Guides & Feedback
Columns
1
Active rules
More content at
Content hub
Rules by severity
High (1)
Medium (0)
Low (0)
Informational (0)
LEARN MORE
About analytics rules
Active rules
Rule templates
Anomalies
Search by ID, name, tactic or technique
Add filter
Severity
Name
Rule type
Data sources
Tactics
Techniques
Sub techniques
Source na
Medium
GitHub Signin ...
Scheduled
Microsoft Entra...
Credentia
T1110
Microsoft
Medium
Cross-tenant A...
Scheduled
Microsoft Entra...
In +2
T1078 +2
T1078.0... +2
Microsoft
Medium
TI map Domain...
Scheduled
+3
Comman
T1071
Threat Int
High
Authentication ...
Scheduled
Microso... +1
Persisten
T1098
Microsoft
Medium
TI map Email e...
Scheduled
Microso... +3
Initial Acc
T1566
Threat Int
Medium
Preview - TI ma...
Scheduled
Microso... +1
Comman
T1071
Threat Int
Medium
Attempts to sig...
Scheduled
Microsoft Entra...
Initial Acc
T1078
Microsoft
Low
Suspicious appl...
Scheduled
Microsoft Entra...
Credentia
T1528
Microsoft
Authentication Methods Changed for Privileged Account
High
Severity
Content hub
Content Source
Scheduled
Rule Type
Description
Identifies authentication methods being changed for a privileged account. This could be an indication of an attacker adding an auth method to the account so they can have continued access. Ref : https://docs.microsoft.com/azure/active-directory/fundamentals/security-operations-privileged-accounts#things-to-monitor-1
Data sources
Microsoft Entra ID
AuditLogs 7/26/2025, 8:55:21 AM
Note:

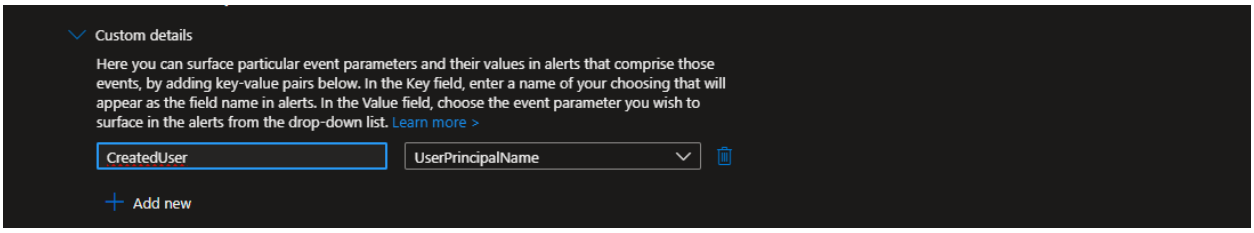

Analytics rule wizard - Create a new Scheduled rule
General
Set rule logic
Incident settings
Automated response
Review + create
Name *
If New User Created
Description
New User Creation
Severity
Medium
MITRE ATT&CK
Select tactics techniques and sub techniques
Status
Enabled
Next : Set rule logic >
Search
Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command And Control
Exfiltration
Impact
Evasion
Impair Process Control
Inhibit Response Function


Search
Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command And Control
Exfiltration
Impact
Evasion
Impair Process Control
Inhibit Response Function

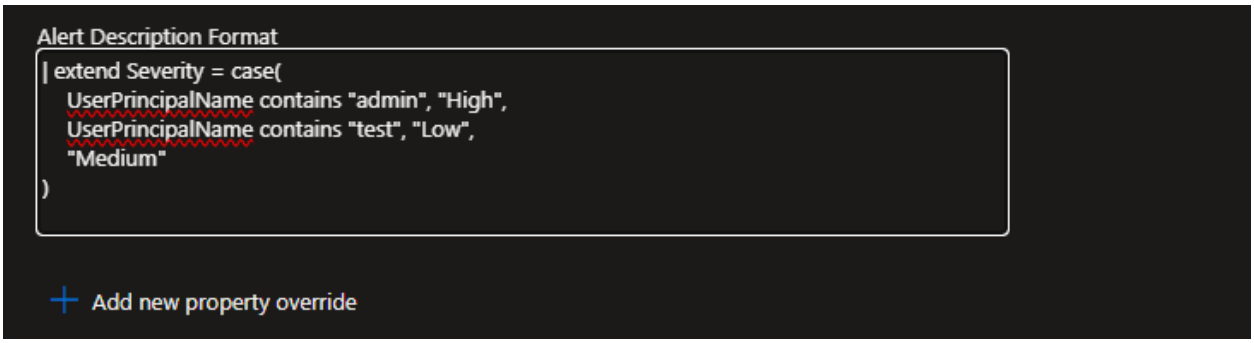

Analytics rule wizard - Create a new Scheduled rule
General
Set rule logic
Incident settings
Automated response
Review + create
Define the logic for your new analytics rule.
Rule query
Any time details set here will be within the scope defined below in the Query scheduling fields.
AuditLogs
| where ActivityDisplayName == "Add user"
| extend UserPrincipalName = tostring(TargetResources[0].userPrincipalName)
| extend CreatedBy = tostring(InitiatedBy.user.userPrincipalName)
| project TimeGenerated, ActivityDisplayName, UserPrincipalName, CreatedBy, Result
View query results >
Alert enhancement
Entity mapping
Custom details
< Previous
Next : Incident settings >

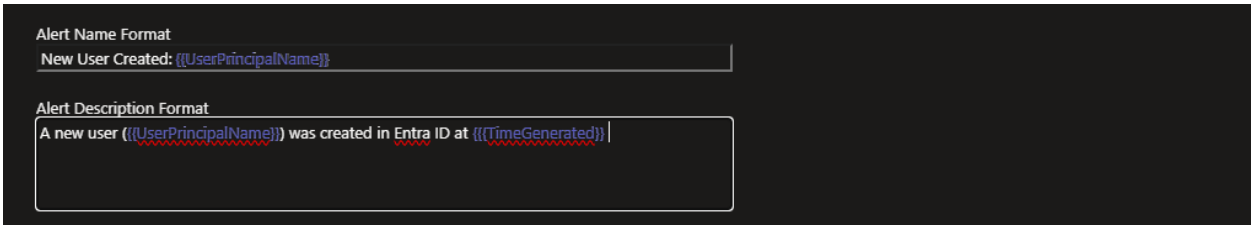

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home > Microsoft Sentinel | Analy
Analytics rule wizar
Logs
LAW-RG-lab
General
Set rule logic
Define the logic for your new
Rule query
Any time details set here will b
AuditLogs
| where ActivityDisplay
| extend UserPrincipalN
| extend CreatedBy = t
| project TimeGenerate
View query results >
Alert enhancement
Entity mapping
Custom details
Run
Time range : Last 7 days
Show : 500000 results
KQL mode
1 AuditLogs
2 | where ActivityDisplayName == "Add user"
3 | extend UserPrincipalName = tostring(TargetResources[0].userPrincipalName)
4 | extend CreatedBy = tostring(InitiatedBy.user.userPrincipalName)
5 | project TimeGenerated, ActivityDisplayName, UserPrincipalName, CreatedBy, Result
6
Results
Chart
TimeGenerated [UTC]
ActivityDisplayName
UserPrincipalName
CreatedBy
7/26/2025, 3:47:24.831 AM
Add user
AuditlogsTesting@ohhno961gmail.onmicrosoft.com
ohhno961_gmail.com#EXT#@ohhno961gmail.onmicrosoft.c...
0s 585ms
Display time (UTC+00:00)
1 - 1 of

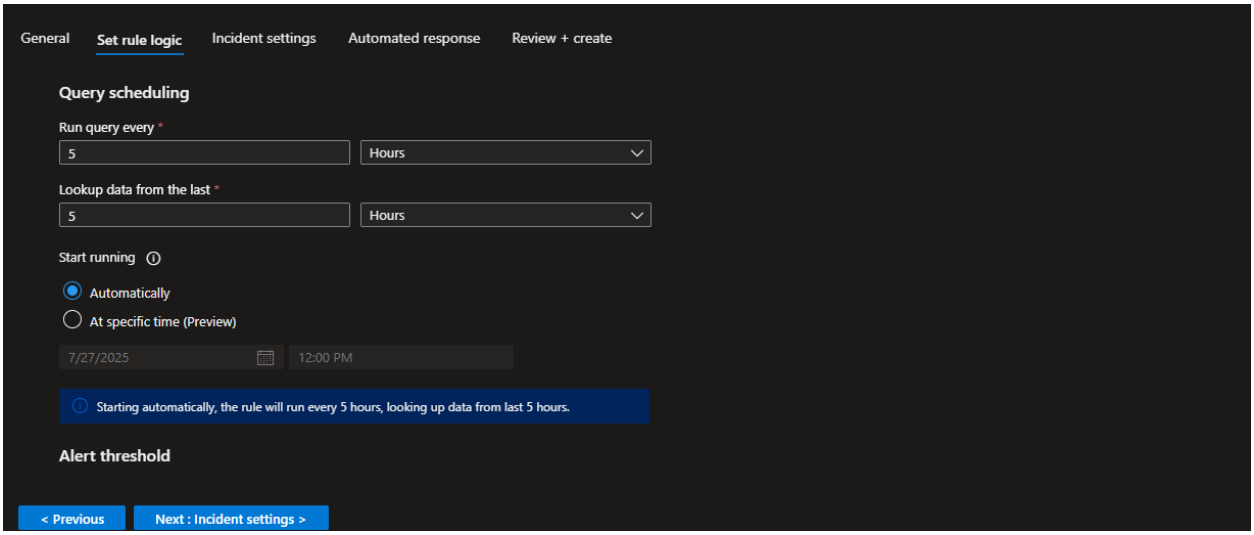

Analytics rule wizard - Create a new Scheduled rule
General
Set rule logic
Incident settings
Automated response
Review + create
| extend CreatedBy = tostring(InitiatedBy.user.userPrincipalName)
| project TimeGenerated, ActivityDisplayName, UserPrincipalName, CreatedBy, Result
View query results >
Alert enhancement
Entity mapping
Map up to 10 entities recognized by Microsoft Sentinel from the appropriate fields available in your query results. This enables Microsoft Sentinel to recognize and classify the data in these fields for further analysis. For each entity, you can define up to 3 identifiers, which are attributes of the entity that help identify the entity as unique. Learn more >
Account
FullName
UserPrincipalName
Add identifier
Add new entity

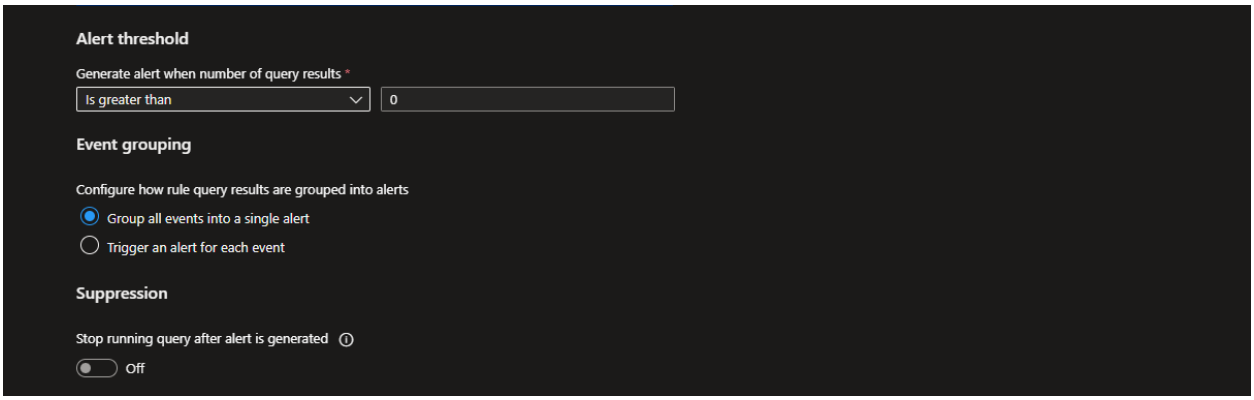

Custom details
Here you can surface particular event parameters and their values in alerts that comprise those events, by adding key-value pairs below. In the Key field, enter a name of your choosing that will appear as the field name in alerts. In the Value field, choose the event parameter you wish to surface in the alerts from the drop-down list. Learn more >
CreatedUser
UserPrincipalName
Add new


Alert Name Format
Example: Alert from {{ProviderName}}
Alert Description Format
New user created in Entra ID
New user created: {{UserPrincipalName}}
Created by: {{CreatedBy}}
Add new property override
Query scheduling


Alert Description Format
| extend Severity = case(
UserPrincipalName contains "admin", "High",
UserPrincipalName contains "test", "Low",
"Medium"
)
Add new property override


Alert Name Format
New User Created: {{UserPrincipalName}}
Alert Description Format
A new user ({{UserPrincipalName}}) was created in Entra ID at {{TimeGenerated}}


General
Set rule logic
Incident settings
Automated response
Review + create
Query scheduling
Run query every *
5
Hours
Lookup data from the last *
5
Hours
Start running
Automatically
At specific time (Preview)
7/27/2025
12:00 PM
Starting automatically, the rule will run every 5 hours, looking up data from last 5 hours.
Alert threshold
< Previous
Next : Incident settings >


Alert threshold
Generate alert when number of query results *
Is greater than
0
Event grouping
Configure how rule query results are grouped into alerts
Group all events into a single alert
Trigger an alert for each event
Suppression
Stop running query after alert is generated
Off

Suppression

Stop running query after alert is generated

On

Stop running query for *

5 Hours

Results simulation

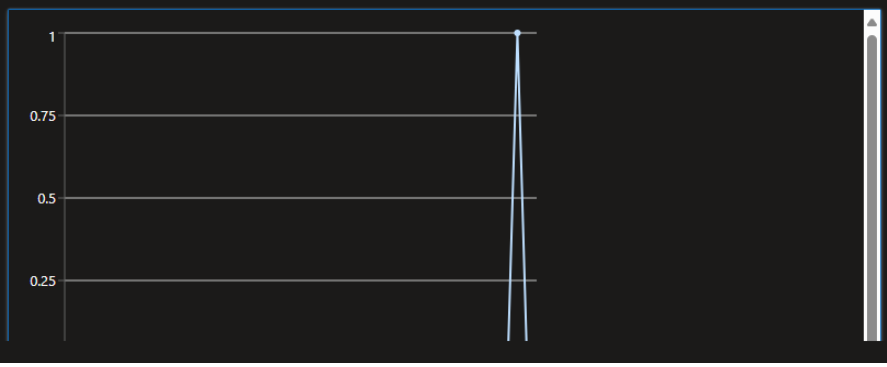
This chart shows the results of the last 50 evaluations of the defined analytics rule. Click a point on the chart to display the raw events for that point in time.

Test with current data

Results simulation

This chart shows the results of the last 50 evaluations of the defined analytics rule. Click a point on the chart to display the raw events for that point in time.

Test with current data



Analytics rule wizard - Create a new Scheduled rule

General | Set rule logic | Incident settings | Automated response | Review + create

Incident settings

Microsoft Sentinel alerts can be grouped together into an Incident that should be looked into.
You can set whether the alerts that are triggered by this analytics rule should generate incidents.

Create incidents from alerts triggered by this analytics rule

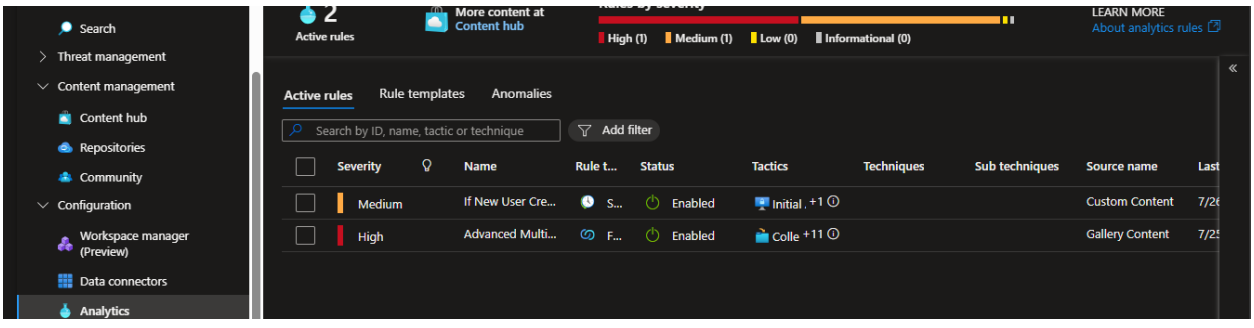
Enabled

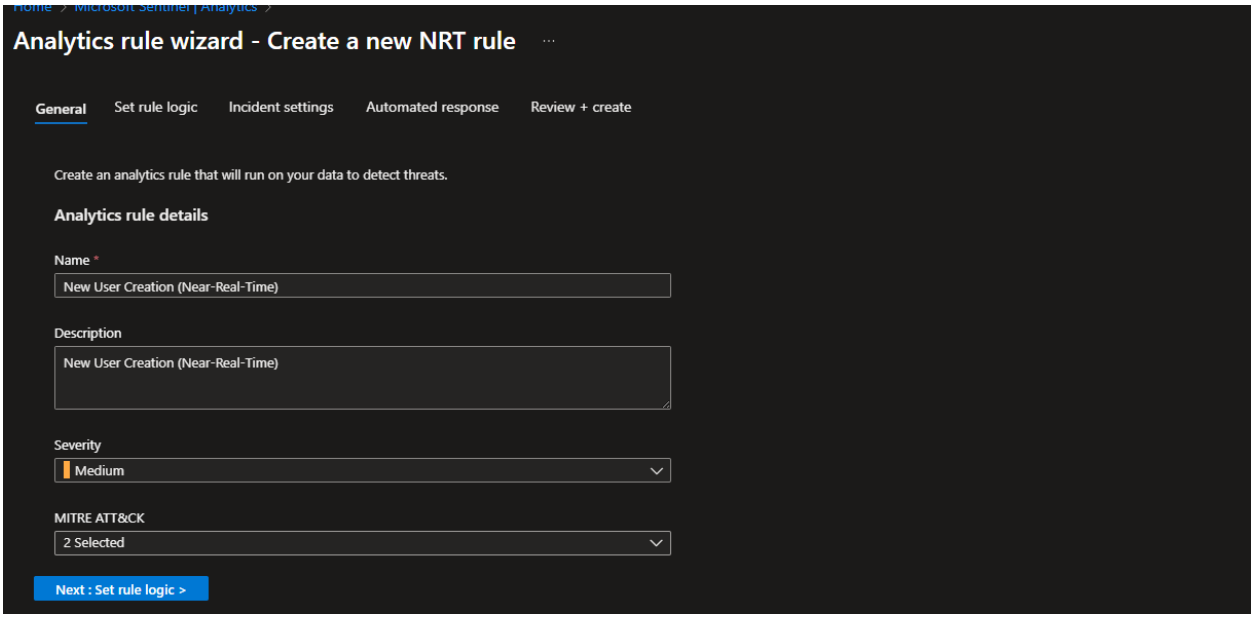
Alert grouping

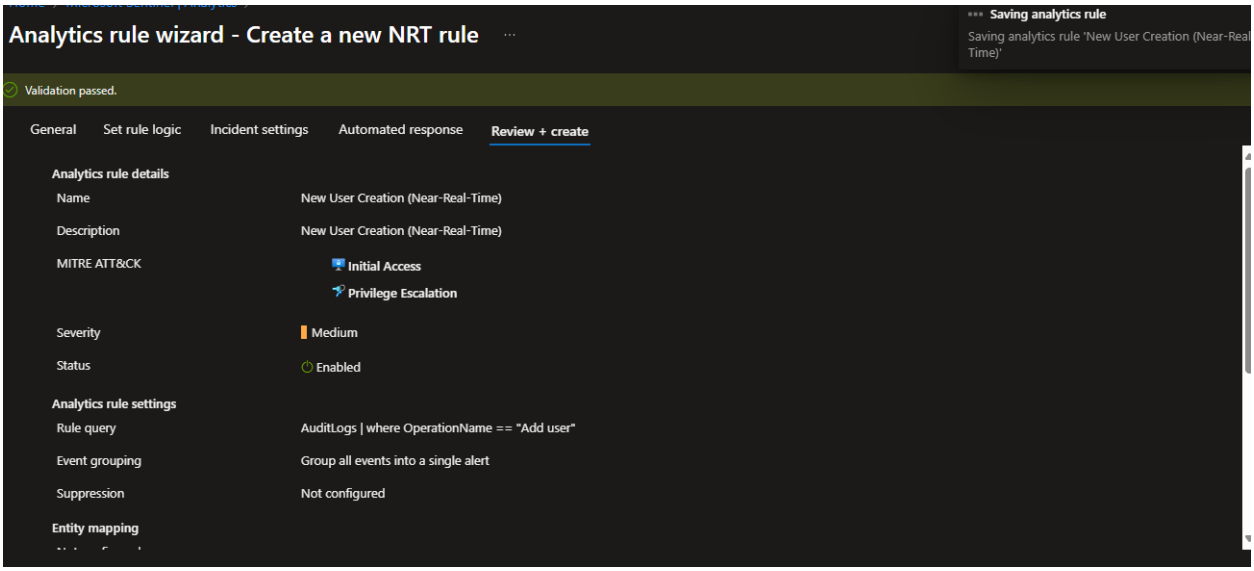
Set how the alerts that are triggered by this analytics rule, are grouped into incidents.
Grouping alerts into incidents provides the context you need to respond and reduces the noise from single alerts.

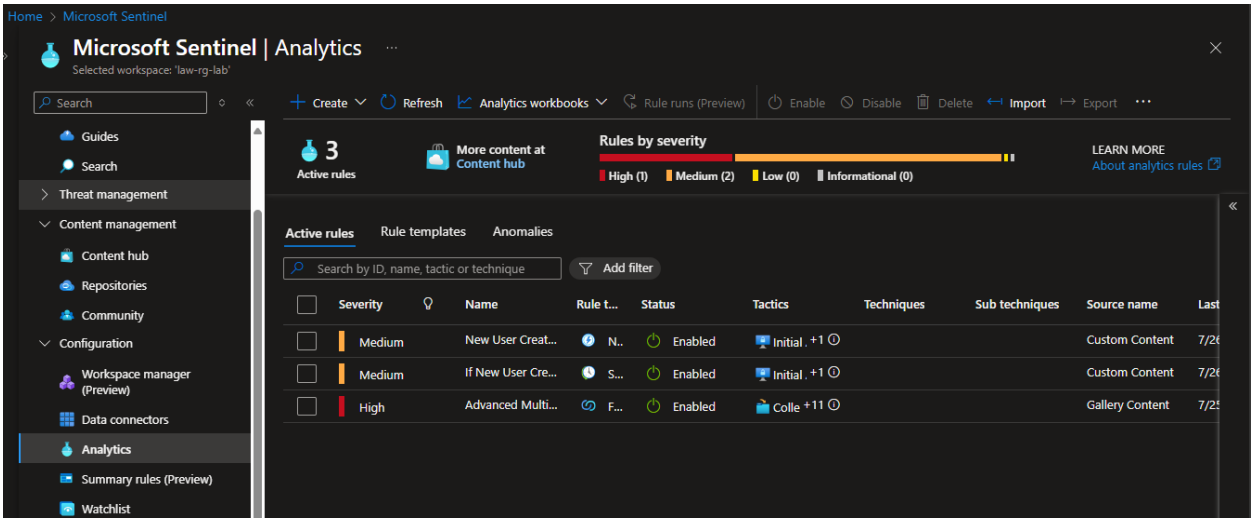
Group related alerts, triggered by this analytics rule, into incidents

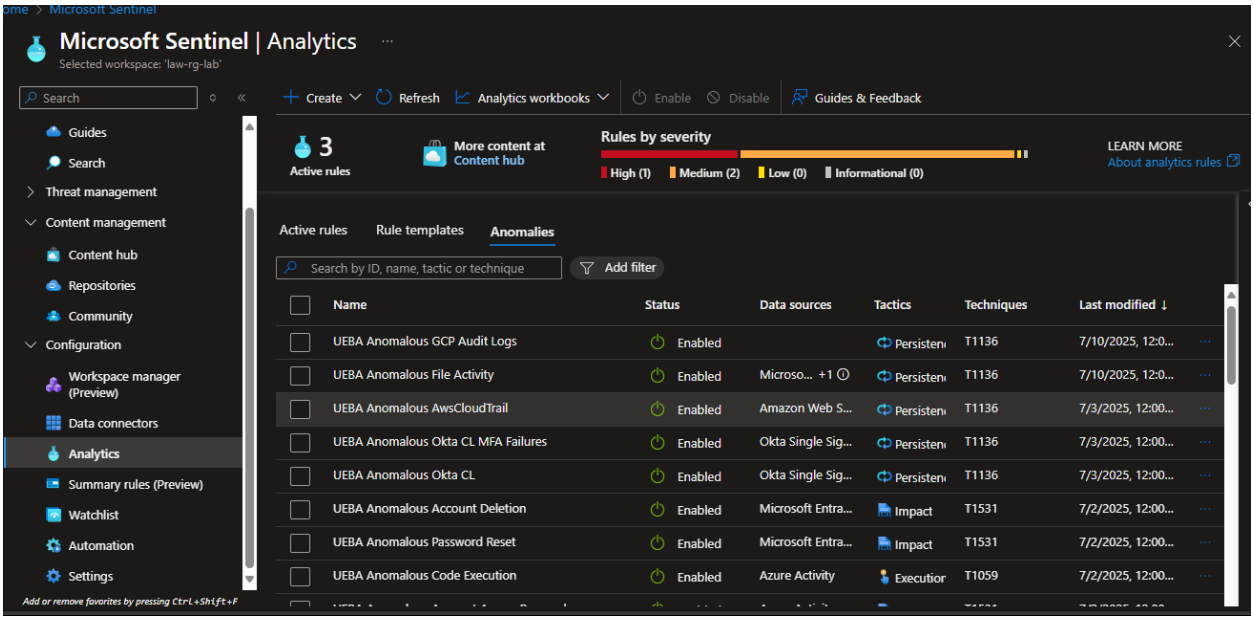
Disabled

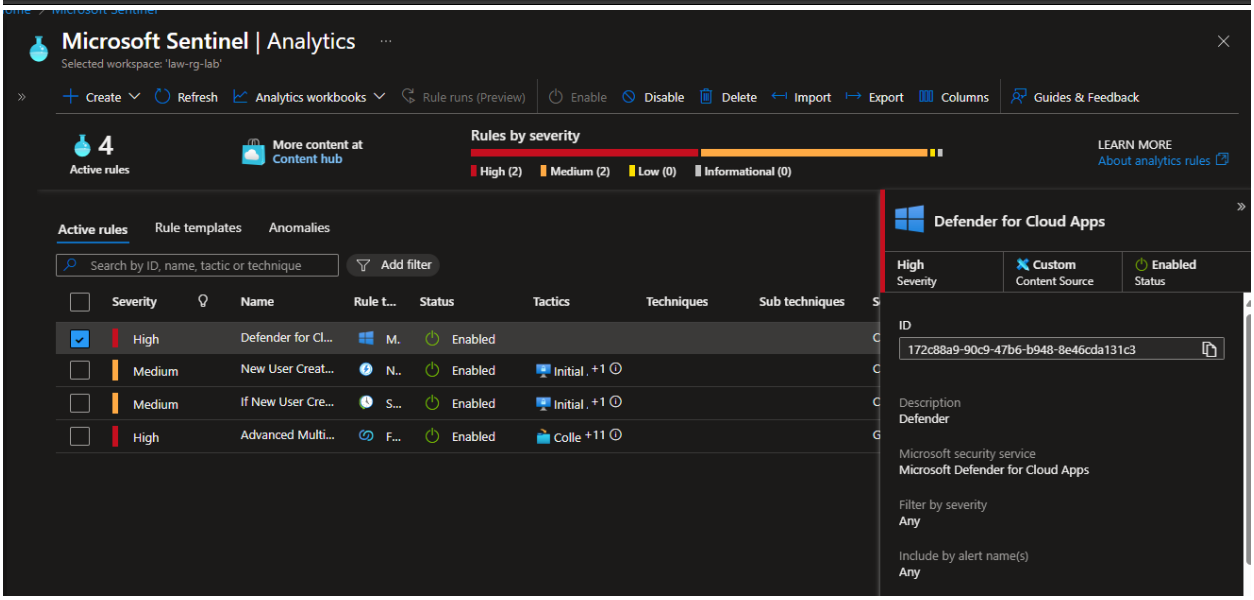


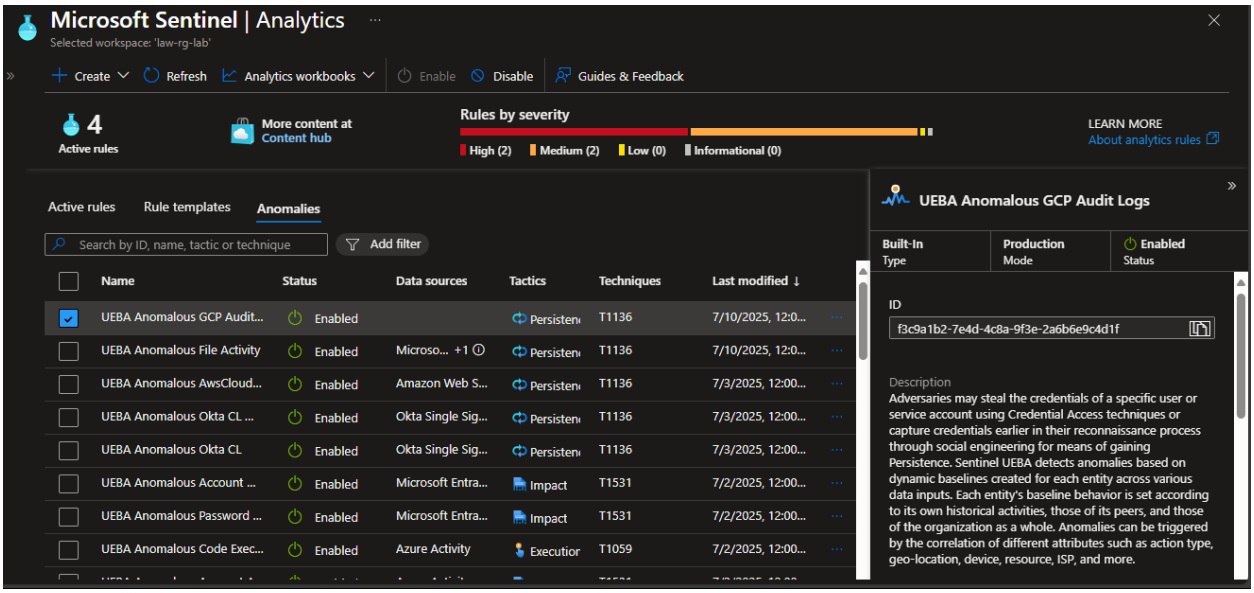

Analytics rule wizard - Create a new NRT rule
General
Set rule logic
Incident settings
Automated response
Review + create
Create an analytics rule that will run on your data to detect threats.
Analytics rule details
Name *
New User Creation (Near-Real-Time)
Description
New User Creation (Near-Real-Time)
Severity
Medium
MITRE ATT&CK
2 Selected
Next : Set rule logic >

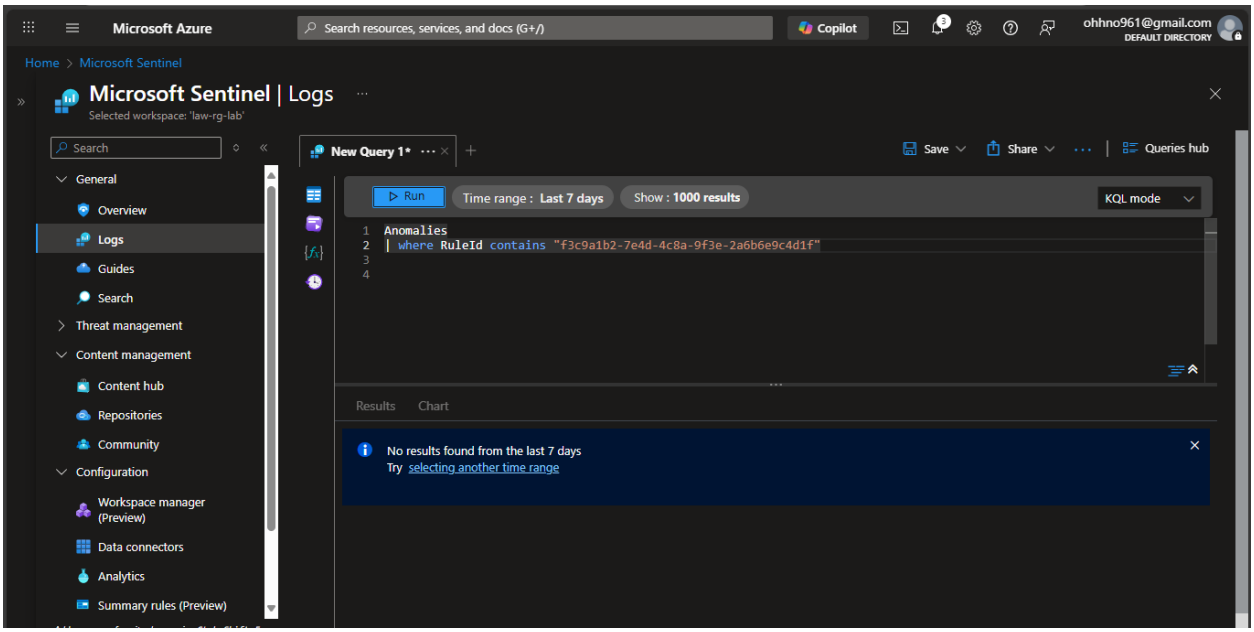

Analytics rule wizard - Create a new NRT rule
Saving analytics rule
Saving analytics rule 'New User Creation (Near-Real-Time)'
Validation passed.
General
Set rule logic
Incident settings
Automated response
Review + create
Analytics rule details
Name
New User Creation (Near-Real-Time)
Description
New User Creation (Near-Real-Time)
MITRE ATT&CK
Initial Access
Privilege Escalation
Severity
Medium
Status
Enabled
Analytics rule settings
Rule query
AuditLogs | where OperationName == "Add user"
Event grouping
Group all events into a single alert
Suppression
Not configured
Entity mapping

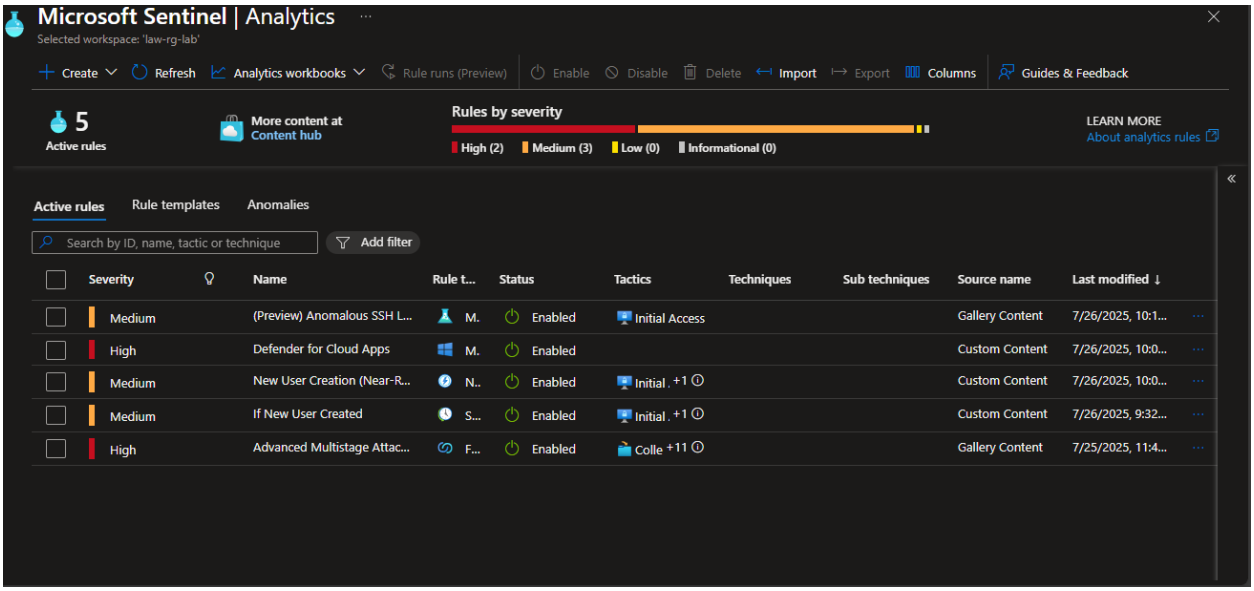

Home > Microsoft Sentinel
Microsoft Sentinel | Analytics
Selected workspace: 'law-rg-lab'
Search
Guides
Search
Threat management
Content management
Content hub
Repositories
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Summary rules (Preview)
Watchlist
Create
Refresh
Analytics workbooks
Rule runs (Preview)
Enable
Disable
Delete
Import
Export
3
Active rules
More content at Content hub
Rules by severity
High (1)
Medium (2)
Low (0)
Informational (0)
LEARN MORE
About analytics rules
Active rules
Rule templates
Anomalies
Search by ID, name, tactic or technique
Add filter
Severity
Name
Rule t...
Status
Tactics
Techniques
Sub techniques
Source name
Last
Medium
New User Creat...
N..
Enabled
Initial +1
Custom Content
7/2
Medium
If New User Cre...
S...
Enabled
Initial +1
Custom Content
7/2
High
Advanced Multi...
F...
Enabled
Colle +11
Gallery Content
7/2


Microsoft Sentinel | Analytics
Selected workspace: 'law-rg-lab'
Search
Create
Refresh
Analytics workbooks
Enable
Disable
Guides & Feedback
Guides
Search
Threat management
Content management
Content hub
Repositories
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Summary rules (Preview)
Watchlist
Automation
Settings
Add or remove favorites by pressing Ctrl+Shift+F
3
Active rules
More content at Content hub
Rules by severity
High (1)
Medium (2)
Low (0)
Informational (0)
LEARN MORE
About analytics rules
Active rules
Rule templates
Anomalies
Search by ID, name, tactic or technique
Add filter
Name
Status
Data sources
Tactics
Techniques
Last modified
UEBA Anomalous GCP Audit Logs
UEBA Anomalous File Activity
UEBA Anomalous AwsCloudTrail
UEBA Anomalous Okta CL MFA Failures
UEBA Anomalous Okta CL
UEBA Anomalous Account Deletion
UEBA Anomalous Password Reset
UEBA Anomalous Code Execution
Enabled
T1136
T1531
T1059
7/10/2025, 12:0...
7/3/2025, 12:00...
7/2/2025, 12:00...


Microsoft Sentinel | Analytics
Selected workspace: 'law-rg-lab'
Create
Refresh
Analytics workbooks
Rule runs (Preview)
Enable
Disable
Delete
Import
Export
Columns
Guides & Feedback
4
Active rules
More content at Content hub
Rules by severity
High (2)
Medium (2)
Low (0)
Informational (0)
LEARN MORE
About analytics rules
Active rules
Rule templates
Anomalies
Search by ID, name, tactic or technique
Add filter
Severity
Name
Rule t...
Status
Tactics
Techniques
Sub techniques
High
Defender for Cl...
Medium
New User Creat...
Medium
If New User Cre...
High
Advanced Multi...
Enabled
Defender for Cloud Apps
High
Severity
Custom
Content Source
Enabled
Status
ID
172c88a9-90c9-47b6-b948-8e46cda131c3
Description
Defender
Microsoft security service
Microsoft Defender for Cloud Apps
Filter by severity
Any
Include by alert name(s)
Any


Microsoft Sentinel | Analytics
Selected workspace: 'law-rg-lab'
Create
Refresh
Analytics workbooks
Enable
Disable
Guides & Feedback
4
Active rules
More content at
Content hub
Rules by severity
High (2)
Medium (2)
Low (0)
Informational (0)
LEARN MORE
About analytics rules
Active rules
Rule templates
Anomalies
Search by ID, name, tactic or technique
Add filter
Name
Status
Data sources
Tactics
Techniques
Last modified
UEBA Anomalous GCP Audit...
Enabled
Persisten
T1136
7/10/2025, 12:0...
UEBA Anomalous File Activity
Enabled
Microso... +1
Persisten
T1136
7/10/2025, 12:0...
UEBA Anomalous AwsCloud...
Enabled
Amazon Web S...
Persisten
T1136
7/3/2025, 12:00...
UEBA Anomalous Okta CL ...
Enabled
Okta Single Sig...
Persisten
T1136
7/3/2025, 12:00...
UEBA Anomalous Okta CL
Enabled
Okta Single Sig...
Persisten
T1136
7/3/2025, 12:00...
UEBA Anomalous Account ...
Enabled
Microsoft Entra...
Impact
T1531
7/2/2025, 12:00...
UEBA Anomalous Password ...
Enabled
Microsoft Entra...
Impact
T1531
7/2/2025, 12:00...
UEBA Anomalous Code Exec...
Enabled
Azure Activity
Executior
T1059
7/2/2025, 12:00...
UEBA Anomalous GCP Audit Logs
Built-In
Type
Production
Mode
Enabled
Status
ID
f3c9a1b2-7e4d-4c8a-9f3e-2a6b6e9c4d1f
Description
Adversaries may steal the credentials of a specific user or service account using Credential Access techniques or capture credentials earlier in their reconnaissance process through social engineering for means of gaining Persistence. Sentinel UEBA detects anomalies based on dynamic baselines created for each entity across various data inputs. Each entity's baseline behavior is set according to its own historical activities, those of its peers, and those of the organization as a whole. Anomalies can be triggered by the correlation of different attributes such as action type, geo-location, device, resource, ISP, and more.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Home > Microsoft Sentinel
Microsoft Sentinel | Logs
Selected workspace: 'law-rg-lab'
Search
General
Overview
Logs
Guides
Search
Threat management
Content management
Content hub
Repositories
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Summary rules (Preview)
New Query 1*
Save
Share
Queries hub
Run
Time range : Last 7 days
Show : 1000 results
KQL mode
1 Anomalies
2 | where RuleId contains "f3c9a1b2-7e4d-4c8a-9f3e-2a6b6e9c4d1f"
3
4
Results
Chart
No results found from the last 7 days
Try selecting another time range



Conclusion

This documentation provides an in-depth look at threat intelligence and analytics rules in Microsoft Sentinel. Threat intelligence helps organizations stay ahead of potential threats, while analytics rules enable automated detection and response mechanisms. By integrating threat intelligence and creating effective analytics rules, security teams can enhance their threat detection and mitigation capabilities. Future chapters will delve deeper into each component and provide detailed guidance on implementation and best practices.

Microsoft Sentinel UEBA and Windows Event Logs Ingestion Documentation

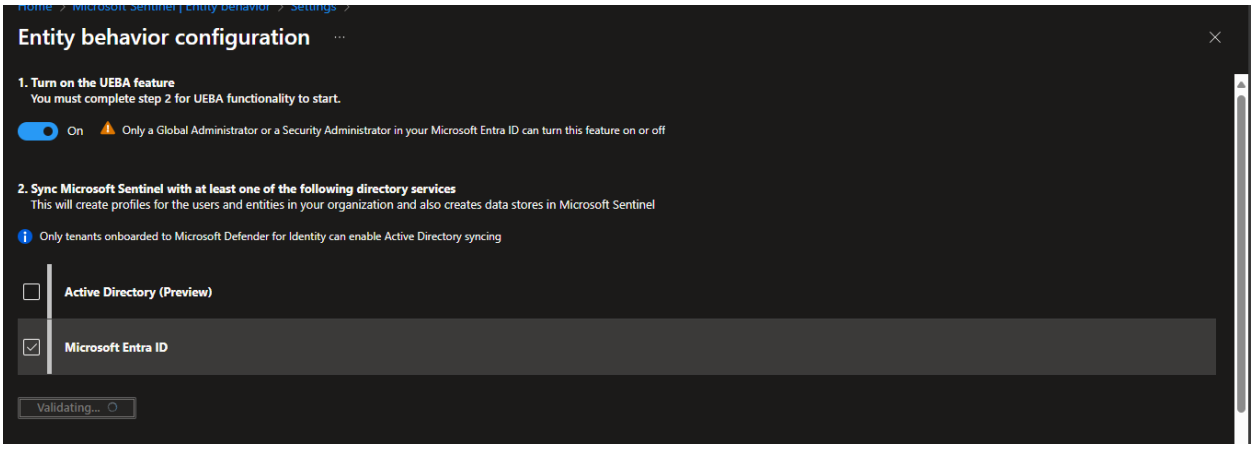
User and Entity Behavior Analytics (UEBA) in Microsoft Sentinel

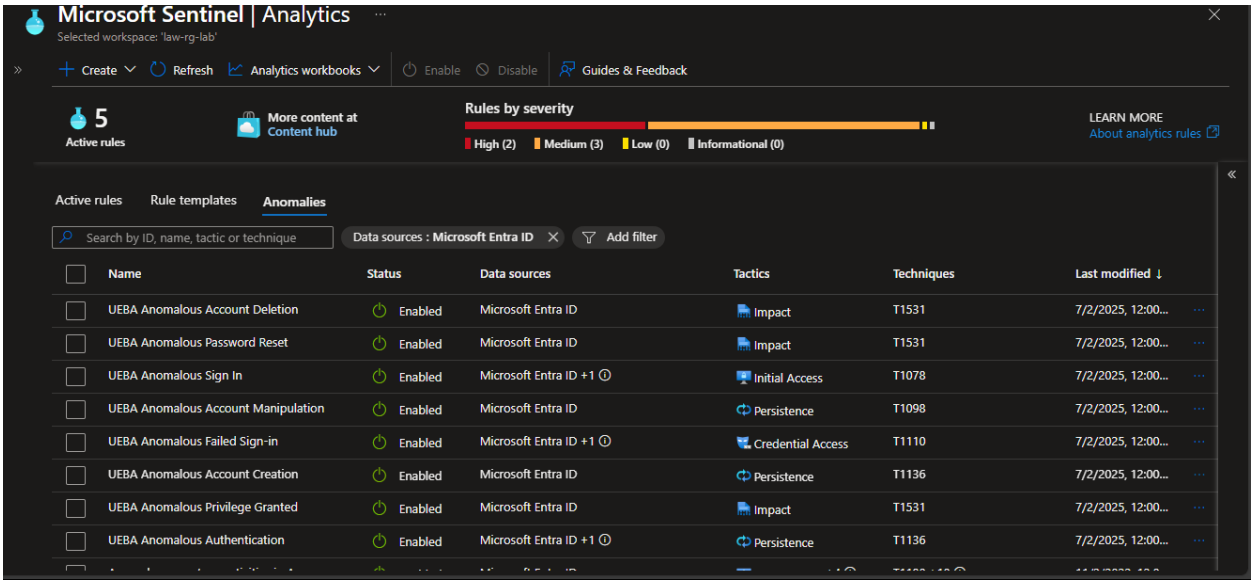
UEBA is a powerful feature in Microsoft Sentinel that detects suspicious activities by analyzing user and entity behaviors over time. It uses machine learning and anomaly detection to identify potential threats.

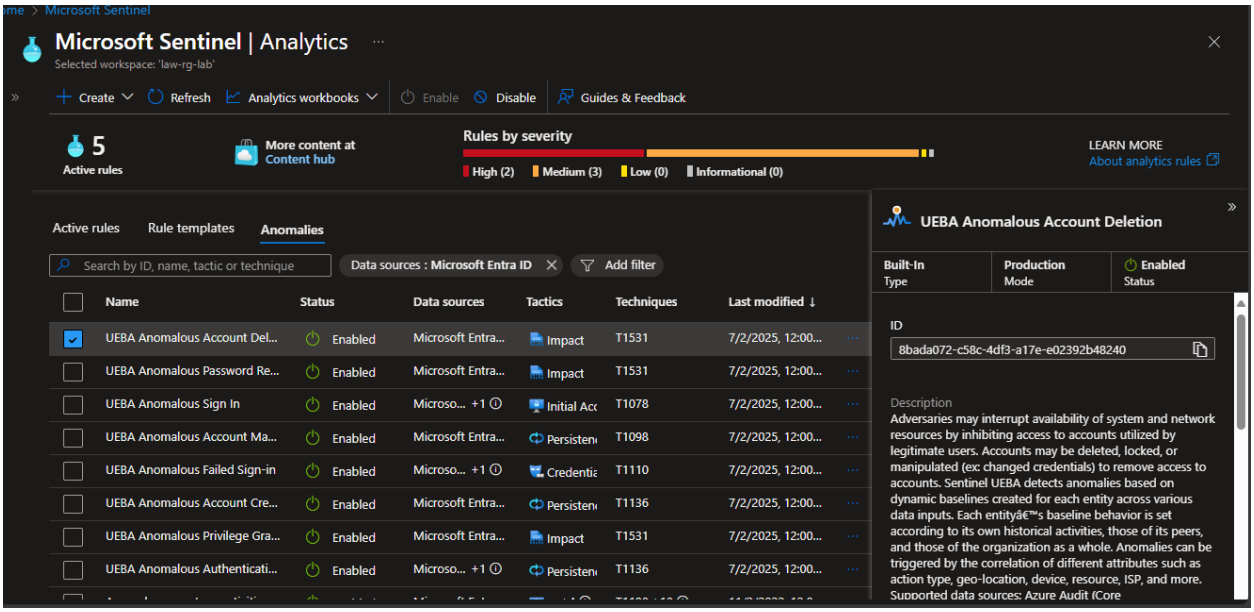
1. **How UEBA Works**:
    - **Builds Baselines**: Learns the normal behavior of users, hosts, IP addresses, and applications over time.
    - **Detects Anomalies**: Identifies deviations from normal behavior using machine learning techniques.
    - **Correlates Events**: Connects unusual activities across multiple data sources for better threat detection.
    - **Assesses Sensitivity and Impact**: Evaluates the importance of an asset, its peer group, and its blast radius.
2. **Key Aspects of UEBA**:
    - **Asset Sensitivity**: Determines the criticality of an asset based on its function, access level, and importance.

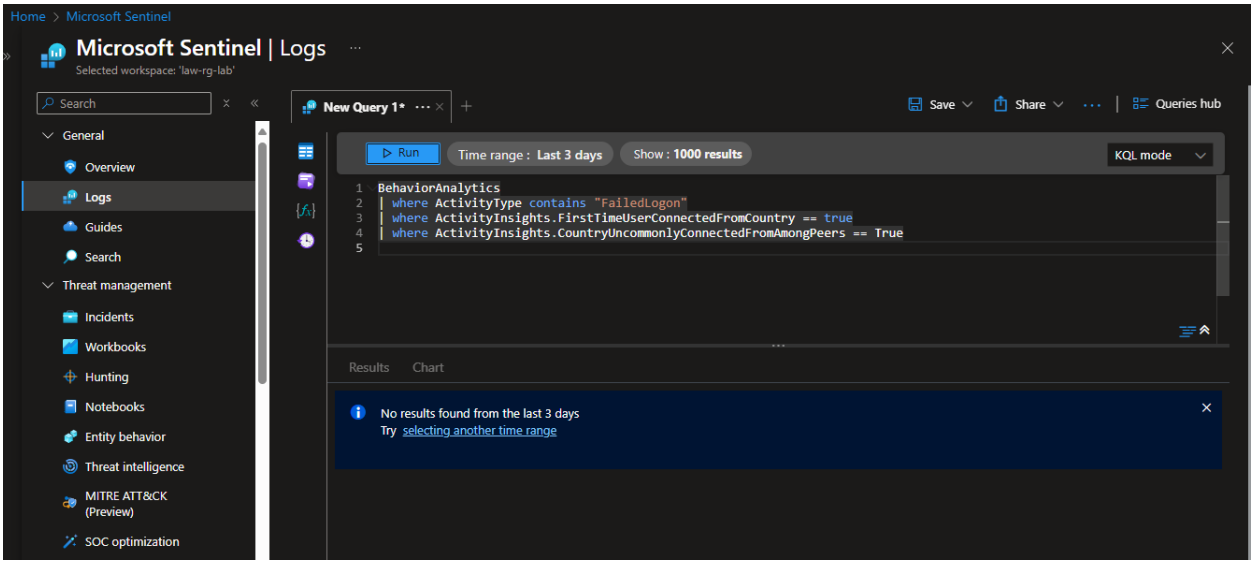
- **Peer Grouping**: Identifies similar assets to assess abnormal behavior or common attack targets.
- **Lateral Movement Analysis**: Evaluates how an attacker could move from one asset to another.
- **Potential Impact Assessment**: Helps prioritize response actions based on the potential damage a compromise could cause.

3. **Why UEBA Matters**:
   - **Reduces False Positives**: Understands context and identifies true anomalies.
   - **Detects Advanced Threats**: Identifies insider threats, compromised accounts, and lateral movement by attackers.
   - **Enhances Response Prioritization**: Helps security teams focus on critical threats first, reducing alert fatigue.
4. **Configuring UEBA in Microsoft Sentinel**:
   - **Enable UEBA**:
     - Go to Microsoft Sentinel.
     - Navigate to *Threat Management > Entity Behavior*.
     - Click on "Set UEBA" or go to *Entity Behavior Settings*.
     - Ensure you have the necessary permissions (Global Administrator or Security Administrator).
     - Sync Microsoft Sentinel with at least one directory (e.g., Microsoft Entra ID).
     - Select existing data sources (e.g., audit logs, sign-in logs) to enable for entity behavior analytics.
   - **Anomalies Table**: Stores detected anomalies for use in detection rules, hunting queries, and investigations.
   - **Behavior Analytics Table**: Contains insights into login attempts, access patterns, and anomalies based on historical data.


Entity behavior configuration
1. Turn on the UEBA feature
You must complete step 2 for UEBA functionality to start.
On
Only a Global Administrator or a Security Administrator in your Microsoft Entra ID can turn this feature on or off
2. Sync Microsoft Sentinel with at least one of the following directory services
This will create profiles for the users and entities in your organization and also creates data stores in Microsoft Sentinel
Only tenants onboarded to Microsoft Defender for Identity can enable Active Directory syncing
Active Directory (Preview)
Microsoft Entra ID
Validating...


Microsoft Sentinel | Analytics
Selected workspace: 'law-rg-lab'
Create
Refresh
Analytics workbooks
Enable
Disable
Guides & Feedback
5
Active rules
More content at
Content hub
Rules by severity
High (2)
Medium (3)
Low (0)
Informational (0)
LEARN MORE
About analytics rules
Active rules
Rule templates
Anomalies
Search by ID, name, tactic or technique
Data sources : Microsoft Entra ID
Add filter
Name
Status
Data sources
Tactics
Techniques
Last modified
UEBA Anomalous Account Deletion
Enabled
Microsoft Entra ID
Impact
T1531
7/2/2025, 12:00...
UEBA Anomalous Password Reset
Enabled
Microsoft Entra ID
Impact
T1531
7/2/2025, 12:00...
UEBA Anomalous Sign In
Enabled
Microsoft Entra ID +1
Initial Access
T1078
7/2/2025, 12:00...
UEBA Anomalous Account Manipulation
Enabled
Microsoft Entra ID
Persistence
T1098
7/2/2025, 12:00...
UEBA Anomalous Failed Sign-in
Enabled
Microsoft Entra ID +1
Credential Access
T1110
7/2/2025, 12:00...
UEBA Anomalous Account Creation
Enabled
Microsoft Entra ID
Persistence
T1136
7/2/2025, 12:00...
UEBA Anomalous Privilege Granted
Enabled
Microsoft Entra ID
Impact
T1531
7/2/2025, 12:00...
UEBA Anomalous Authentication
Enabled
Microsoft Entra ID +1
Persistence
T1136
7/2/2025, 12:00...





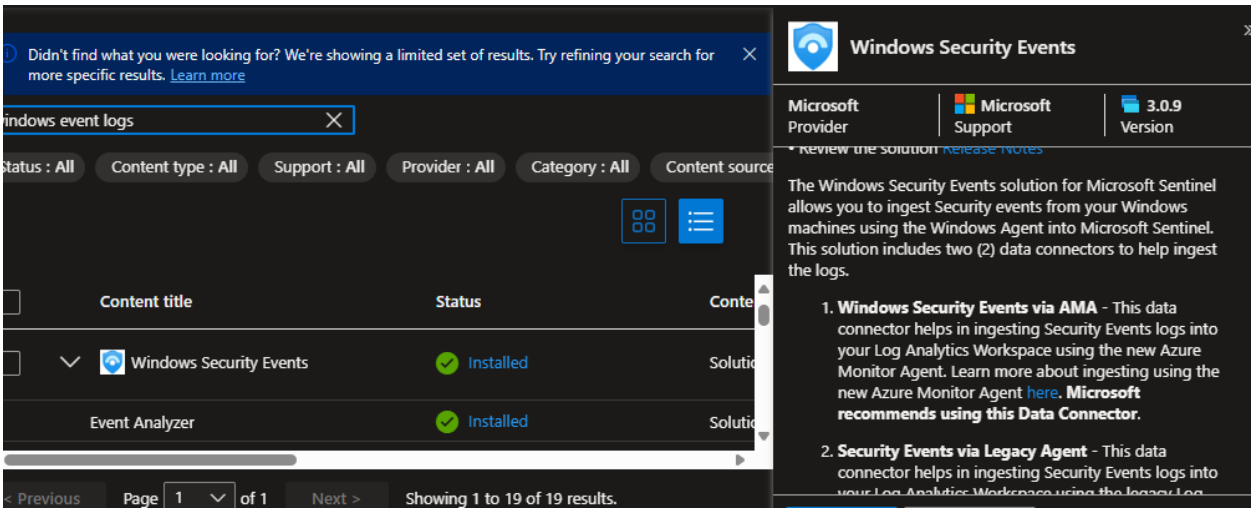
Ingesting Windows Event Logs Using Azure Monitor Agent (AMA)

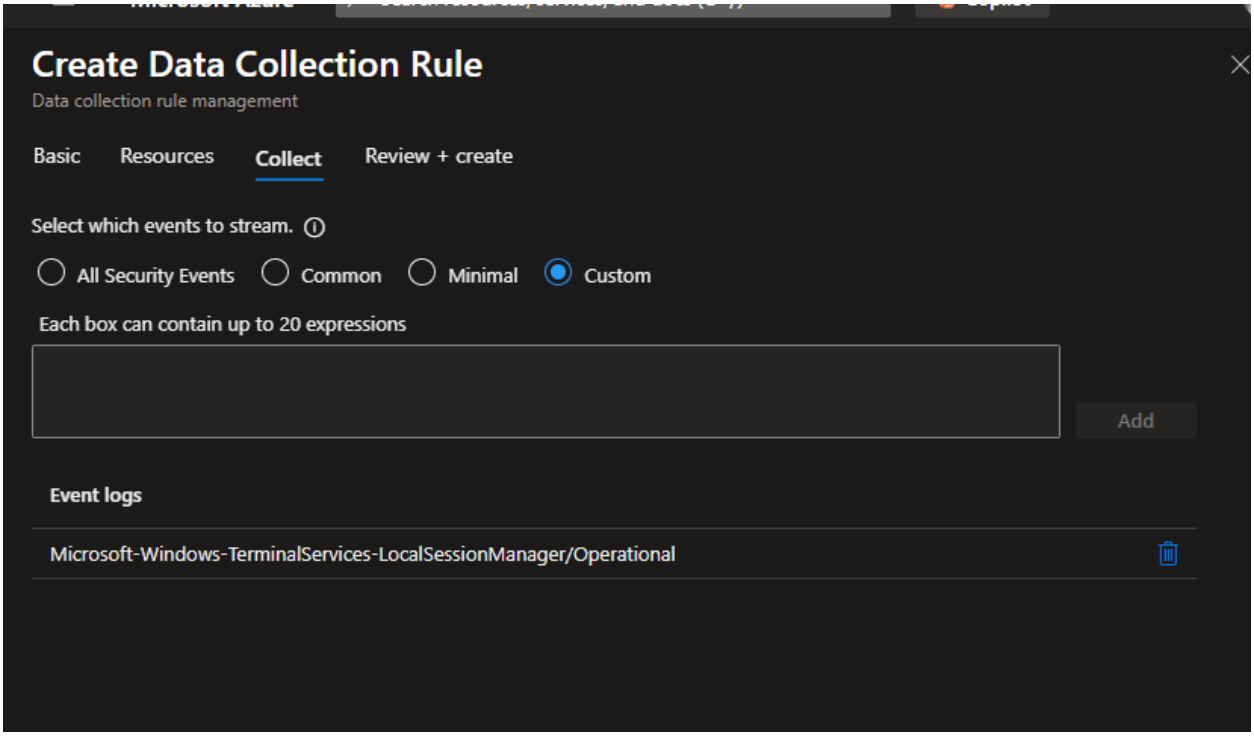
Azure Monitor Agent (AMA) is a telemetry collection agent designed to collect and send logs and metrics from various resources to Azure Monitor, Log Analytics, Event Hubs, or Azure Storage.

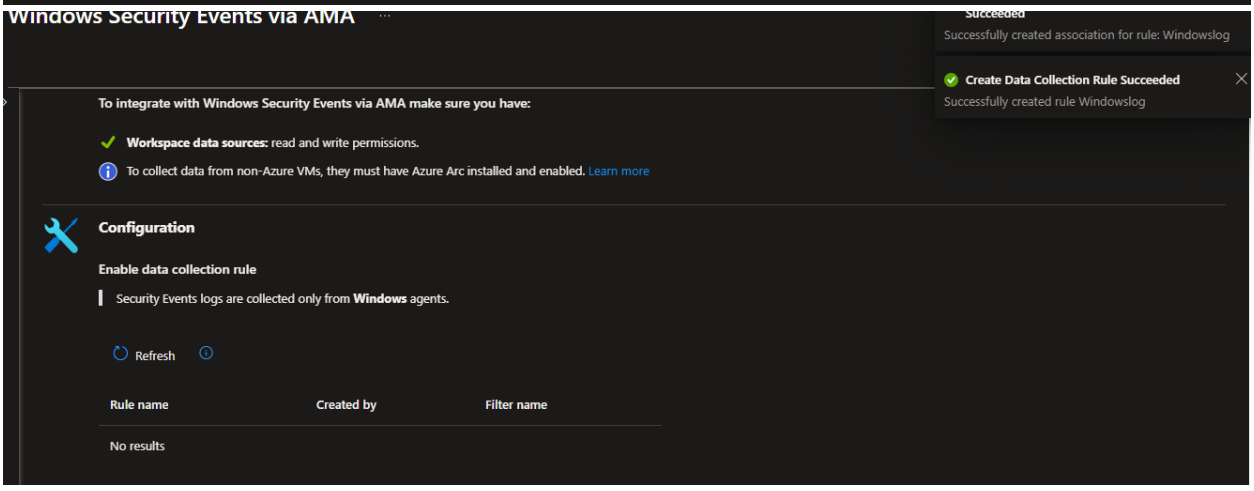
1. **Resources AMA Can Collect Data From**:
    - Azure Virtual Machines (VMs)
    - Azure VM Scale Sets
    - On-premises or multicloud VMs (with Azure Arc enabled)
    - Azure Kubernetes Service (AKS)
    - Azure Functions and App Services
2. **Data AMA Can Collect**:
    - Windows Event Logs

- Linux Logs (Syslog)
- Performance Metrics
- Azure Monitor Logs
- Container Logs (AKS)

3. **Data Collection Rules (DCRs)**:
   - Define what data to collect (e.g., log types, performance counters).
   - Target specific resources (e.g., VMs, resource groups, subscriptions).
   - Transform data before sending (e.g., filter, aggregate, modify).
   - Send data to multiple destinations (e.g., Log Analytics, Event Hubs, Azure Storage).
4. **Ingesting Windows Event Logs from a VM Using AMA**:
   - **Create a Virtual Machine**:
     - Go to the Azure portal.
     - Search for and select *Virtual Machines*.
     - Click *Create > Azure Virtual Machine*.
     - Provide details (e.g., VM name, region, image, size, admin user credentials).
     - Review and create the VM.
   - **Install AMA and Configure Data Collection**:
     - Go to Microsoft Sentinel.
     - Navigate to *Content Management > Content Hub*.
     - Search for and install the **Windows Security Events** solution.
     - Open the **Windows Security Events** data connector.
     - Ensure you have read and write permissions.
     - Enable data collection for the VM (AMA will be installed automatically).
     - Create a Data Collection Rule (DCR) to specify what data to collect (e.g., all security events).
     - Select the VM and apply the DCR.


Didn't find what you were looking for? We're showing a limited set of results. Try refining your search for more specific results. Learn more
indows event logs
tatus : All
Content type : All
Support : All
Provider : All
Category : All
Content source
Content title
Status
Conte
Windows Security Events
Installed
Solutio
Event Analyzer
Installed
Solutio
< Previous
Page 1 of 1
Next >
Showing 1 to 19 of 19 results.
Windows Security Events
Microsoft
Provider
Microsoft
Support
3.0.9
Version
The Windows Security Events solution for Microsoft Sentinel allows you to ingest Security events from your Windows machines using the Windows Agent into Microsoft Sentinel. This solution includes two (2) data connectors to help ingest the logs.
1. Windows Security Events via AMA - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the new Azure Monitor Agent. Learn more about ingesting using the new Azure Monitor Agent here. Microsoft recommends using this Data Connector.
2. Security Events via Legacy Agent - This data connector helps in ingesting Security Events logs into


Create Data Collection Rule
Data collection rule management
Basic
Resources
Collect
Review + create
Select which events to stream.
All Security Events
Common
Minimal
Custom
Each box can contain up to 20 expressions
Add
Event logs
Microsoft-Windows-TerminalServices-LocalSessionManager/Operational


Windows Security Events via AMA
Succeeded
Successfully created association for rule: Windowslog
Create Data Collection Rule Succeeded
Successfully created rule Windowslog
To integrate with Windows Security Events via AMA make sure you have:
Workspace data sources: read and write permissions.
To collect data from non-Azure VMs, they must have Azure Arc installed and enabled. Learn more
Configuration
Enable data collection rule
Security Events logs are collected only from Windows agents.
Refresh
Rule name
Created by
Filter name
No results

Conclusion

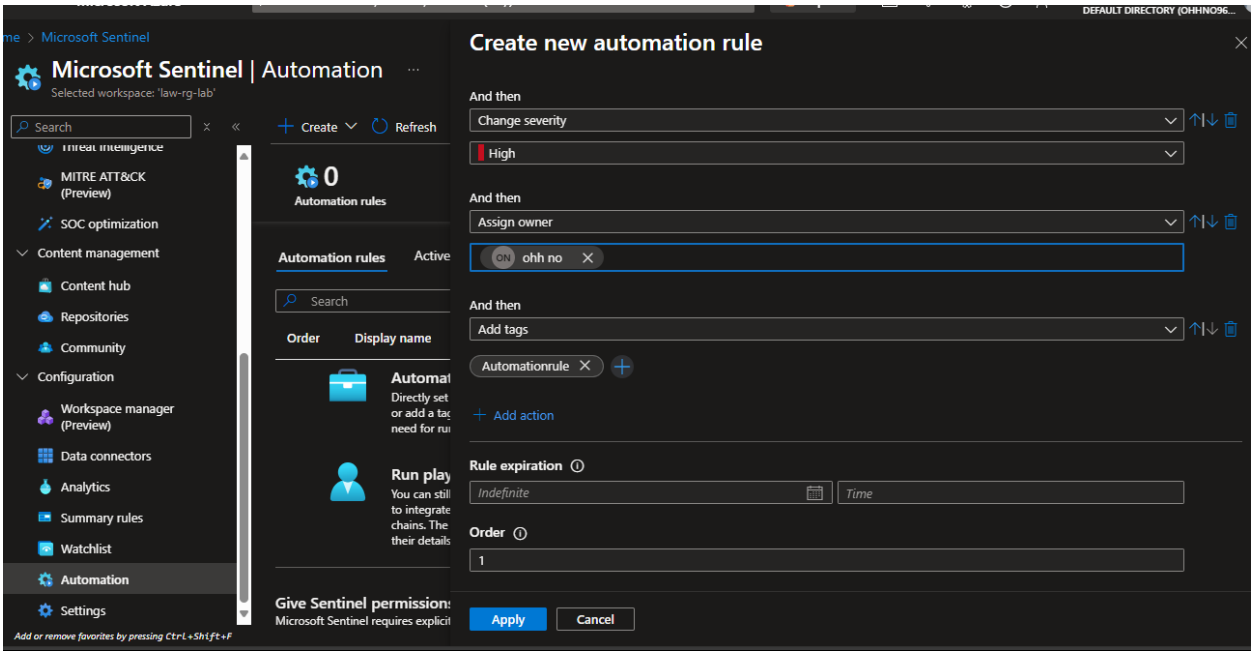
This documentation provides an in-depth look at UEBA and the ingestion of Windows event logs using Azure Monitor Agent in Microsoft Sentinel. UEBA helps detect suspicious activities by analyzing user and entity behaviors, while AMA enables efficient collection and forwarding of logs and metrics. By configuring UEBA and AMA, organizations can enhance their threat detection and response capabilities. Future chapters will delve deeper into each component and provide detailed guidance on their implementation and best practices.

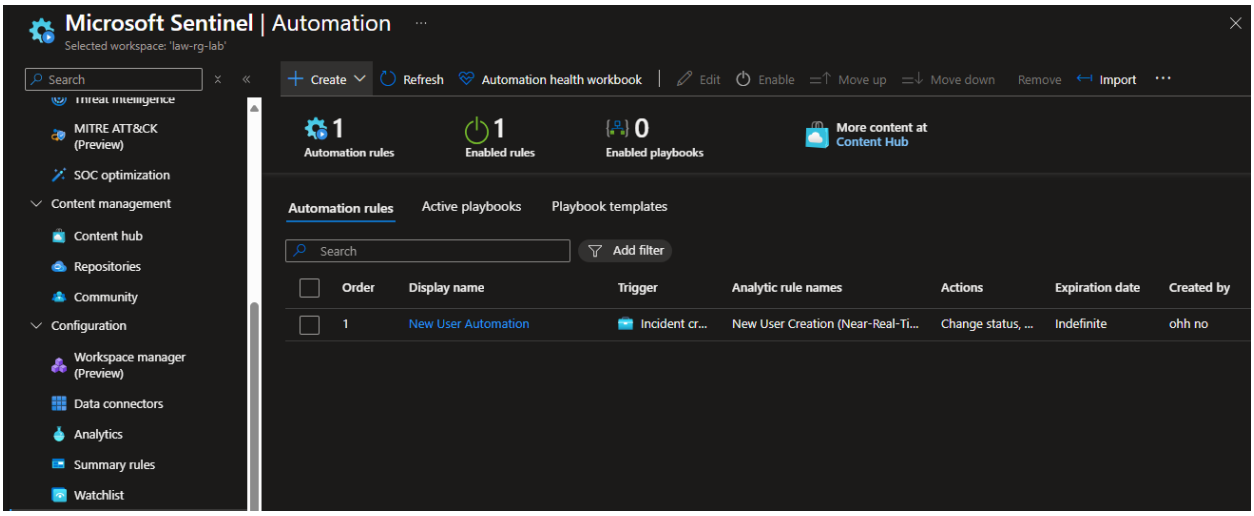
Microsoft Sentinel Automation, Workbooks, and Watch Lists Documentation

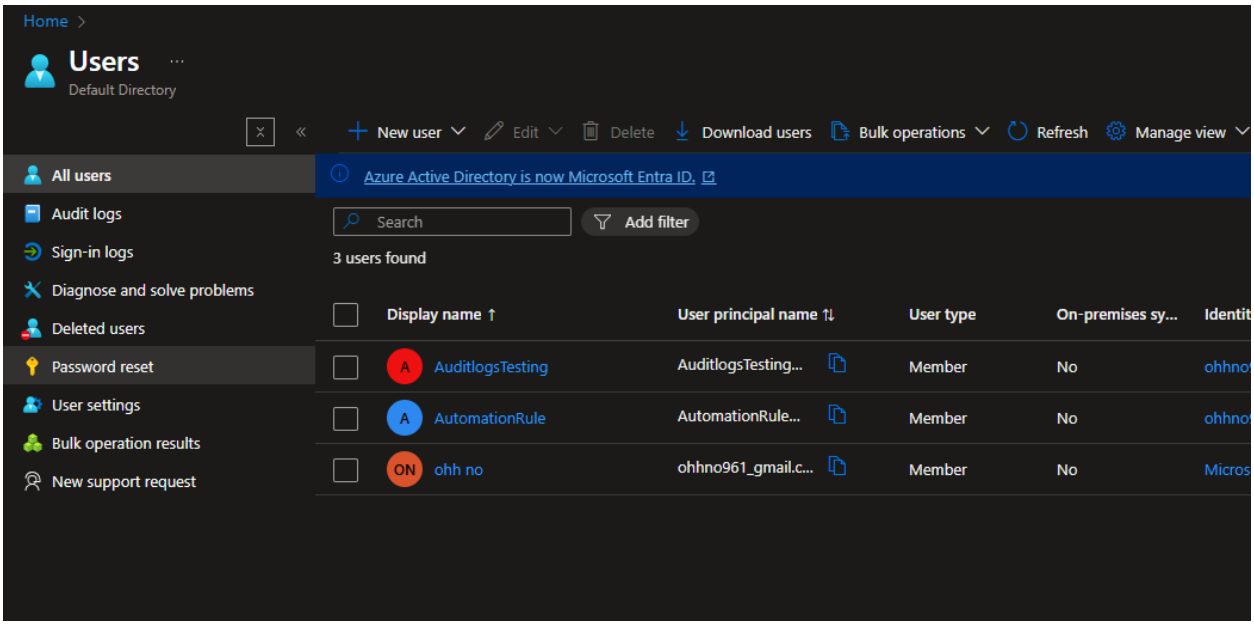
Automating Threat Responses in Microsoft Sentinel

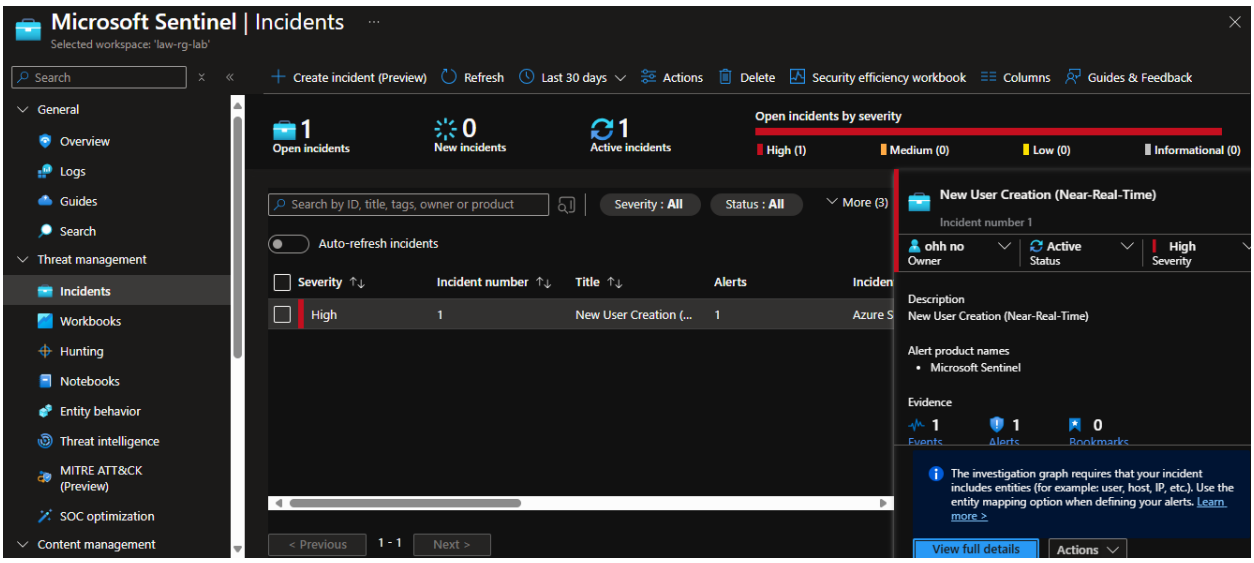
Microsoft Sentinel is not only a SIEM system but also a platform for SOAR (Security Orchestration, Automation, and Response). Automating threat responses helps streamline and scale security operations.

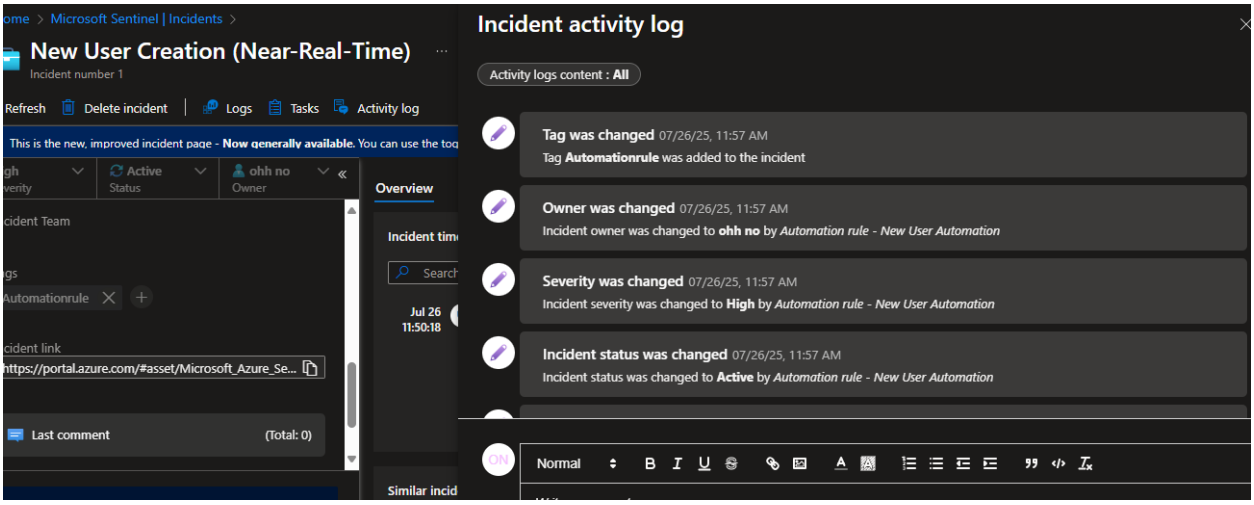
1. **Why Automate Responses**:
    - **Reduces Alert Fatigue**: Automates triage, reducing noise and false positives.
    - **Improves Incident Response Time**: Speeds up containment and remediation.
    - **Frees Up Analysts**: Allows them to focus on strategic activities like threat hunting and investigations.
2. **Options to Automate Responses**:
    - **Automation Rules**: Centrally manage incident handling workflows.
    - **Playbooks**: Use Azure Logic Apps to orchestrate complex automated responses.
3. **Creating Automation Rules**:
    - **Identify Incidents/Alerts**: Determine which incidents or alerts the rule should apply to.
    - **Define Actions**: Assign tasks, change statuses, add tags, or trigger playbooks.
    - **Set Conditions**: Specify conditions for rule execution.
    - **Order and Expiration**: Define the execution order and set expiration dates if needed.
4. **Creating Playbooks**:
    - **Use Templates**: Start with predefined templates for common use cases.
    - **Customize Playbooks**: Add your own logic, triggers, and actions.
    - **Integrate Systems**: Connect to internal and external systems for end-to-end response automation.

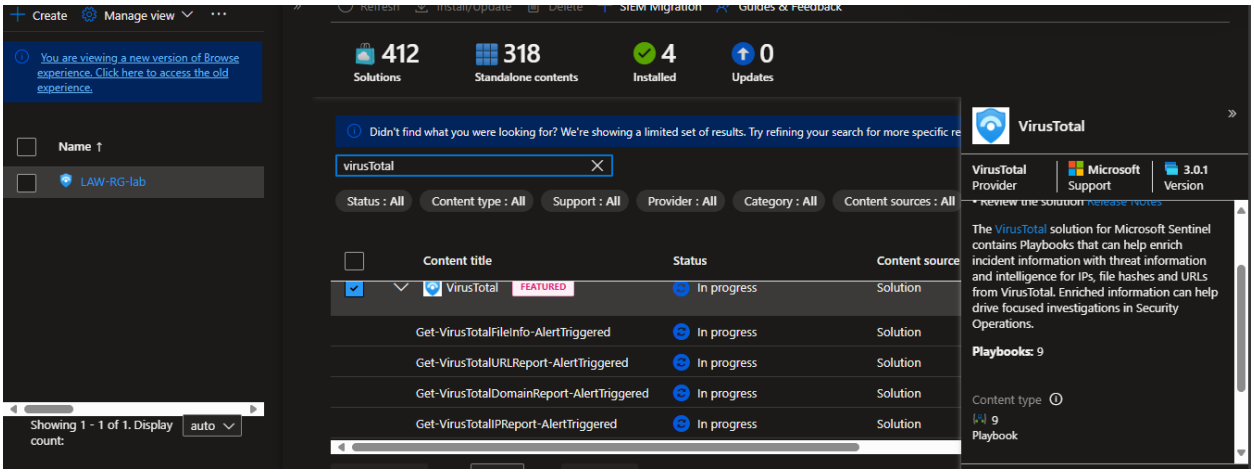

Microsoft Sentinel
Microsoft Sentinel | Automation
Selected workspace: 'law-rg-lab'
Search
Create
Refresh
0
Automation rules
Automation rules
Active
Search
Order
Display name
Give Sentinel permissions
Microsoft Sentinel requires explicit
MITRE ATT&CK (Preview)
SOC optimization
Content management
Content hub
Repositories
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Summary rules
Watchlist
Automation
Settings
Add or remove favorites by pressing Ctrl+Shift+F
Create new automation rule
And then
Change severity
High
And then
Assign owner
ohh no
And then
Add tags
Automationrule
Add action
Rule expiration
Indefinite
Time
Order
1
Apply
Cancel

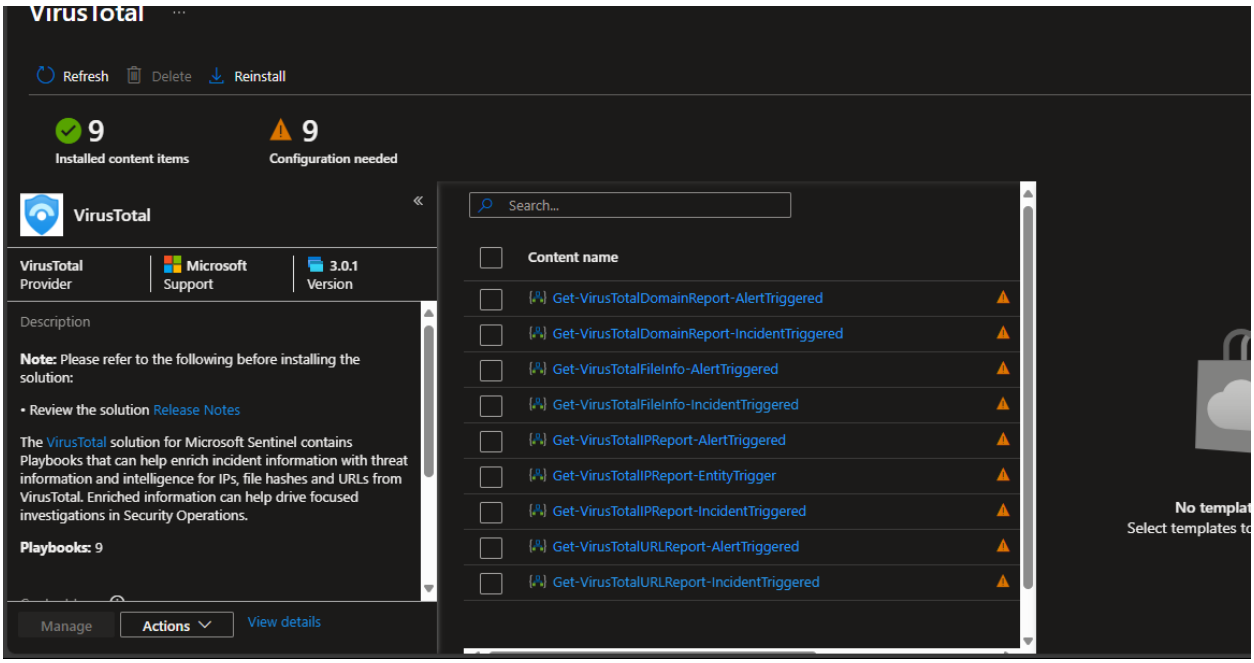

Microsoft Sentinel | Automation
Selected workspace: 'law-rg-lab'
Search
Create
Refresh
Automation health workbook
Edit
Enable
Move up
Move down
Remove
Import
1
Automation rules
1
Enabled rules
0
Enabled playbooks
More content at
Content Hub
Automation rules
Active playbooks
Playbook templates
Search
Add filter
Order
Display name
Trigger
Analytic rule names
Actions
Expiration date
Created by
1
New User Automation
Incident cr...
New User Creation (Near-Real-Ti...
Change status, ...
Indefinite
ohh no
MITRE ATT&CK (Preview)
SOC optimization
Content management
Content hub
Repositories
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Summary rules
Watchlist

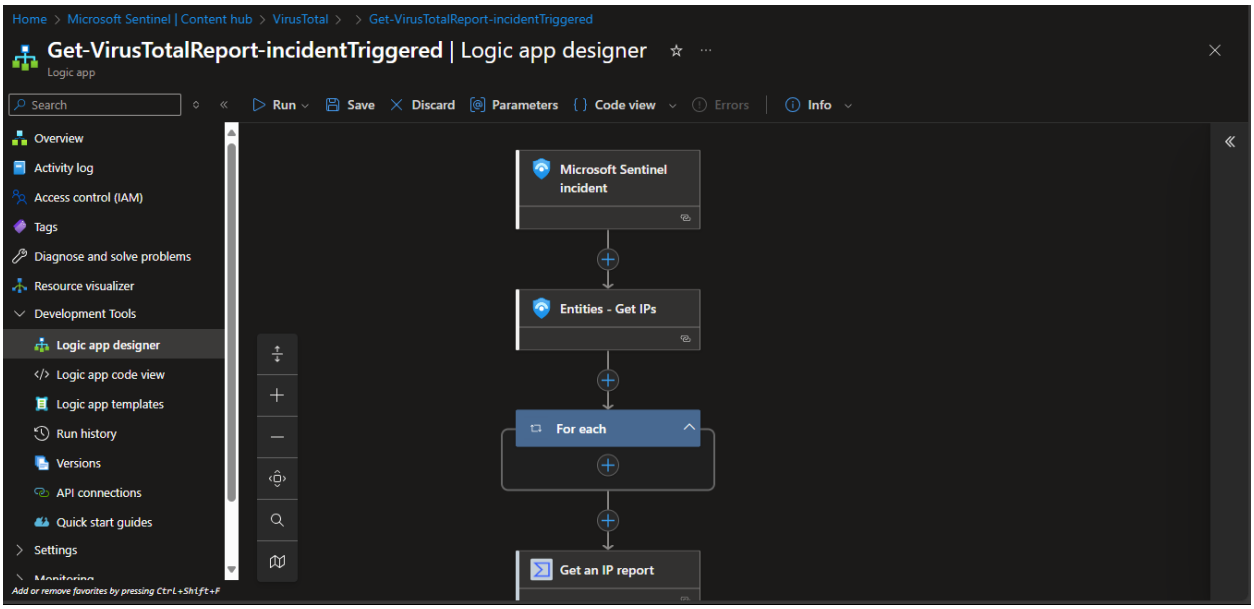

Home
Users
Default Directory
New user
Edit
Delete
Download users
Bulk operations
Refresh
Manage view
All users
Audit logs
Sign-in logs
Diagnose and solve problems
Deleted users
Password reset
User settings
Bulk operation results
New support request
Azure Active Directory is now Microsoft Entra ID.
Search
Add filter
3 users found
Display name
User principal name
User type
On-premises sy...
AuditlogsTesting
AuditlogsTesting...
Member
No
AutomationRule
AutomationRule...
Member
No
ohh no
ohhno961_gmail.c...
Member
No

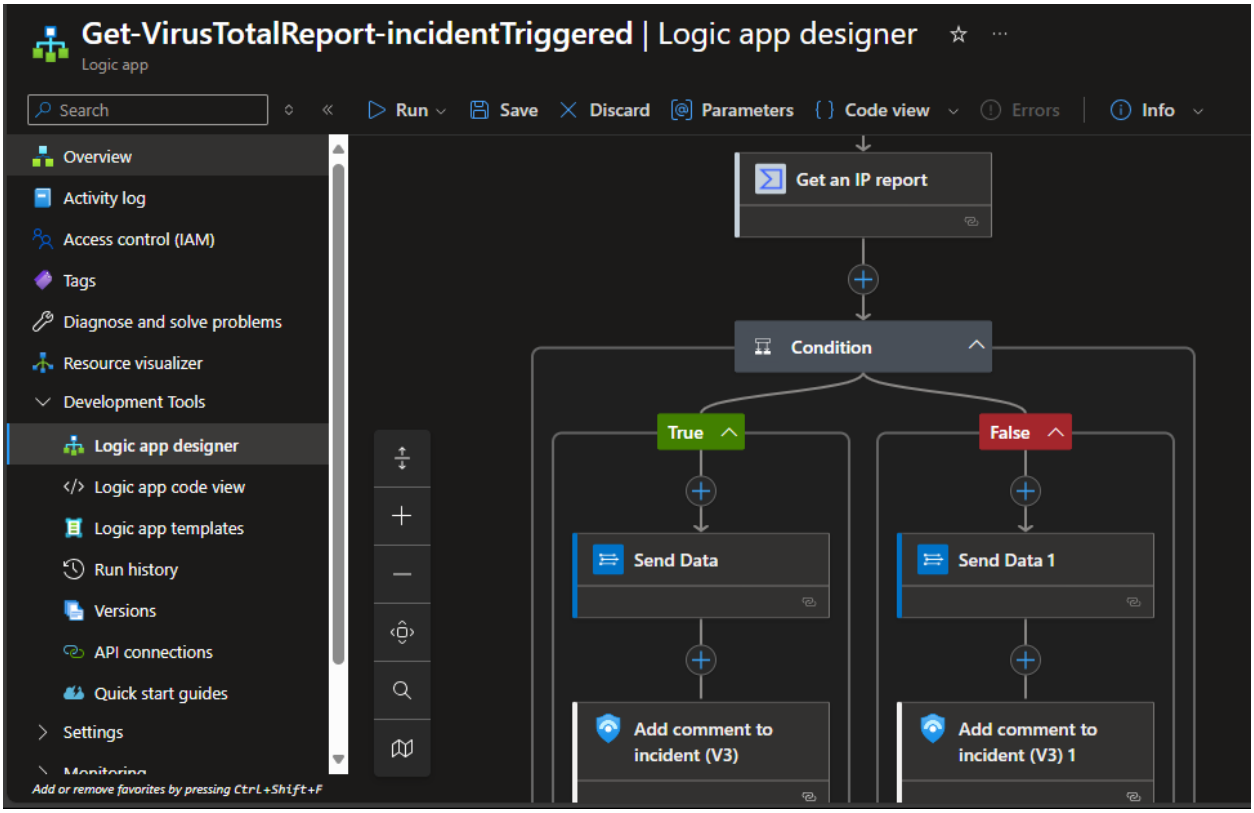

Microsoft Sentinel | Incidents
Selected workspace: 'law-rg-lab'
Create incident (Preview)
Refresh
Last 30 days
Actions
Delete
Security efficiency workbook
Columns
Guides & Feedback
General
Overview
Logs
Guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
SOC optimization
Content management
1 Open incidents
0 New incidents
1 Active incidents
Open incidents by severity
High (1)
Medium (0)
Low (0)
Informational (0)
Search by ID, title, tags, owner or product
Severity : All
Status : All
More (3)
Auto-refresh incidents
Severity
Incident number
Title
Alerts
High
1
New User Creation (...
1
New User Creation (Near-Real-Time)
Incident number 1
ohh no
Owner
Active
Status
High
Severity
Description
New User Creation (Near-Real-Time)
Alert product names
Microsoft Sentinel
Evidence
1
1
0
The investigation graph requires that your incident includes entities (for example: user, host, IP, etc.). Use the entity mapping option when defining your alerts. Learn more >
View full details
Actions
< Previous
1 - 1
Next >

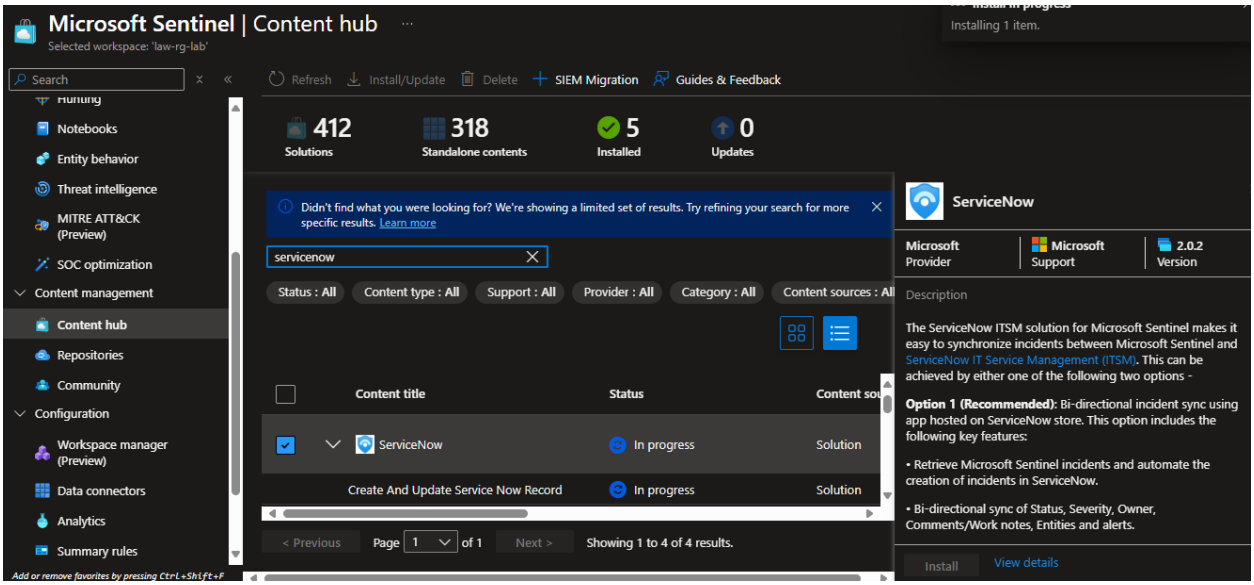

Microsoft Sentinel | Incidents
New User Creation (Near-Real-Time)
Incident number 1
Refresh
Delete incident
Logs
Tasks
Activity log
Overview
Automationrule
Last comment
(Total: 0)
Incident activity log
Activity logs content : All
Tag was changed 07/26/25, 11:57 AM
Tag Automationrule was added to the incident
Owner was changed 07/26/25, 11:57 AM
Incident owner was changed to ohh no by Automation rule - New User Automation
Severity was changed 07/26/25, 11:57 AM
Incident severity was changed to High by Automation rule - New User Automation
Incident status was changed 07/26/25, 11:57 AM
Incident status was changed to Active by Automation rule - New User Automation
Normal

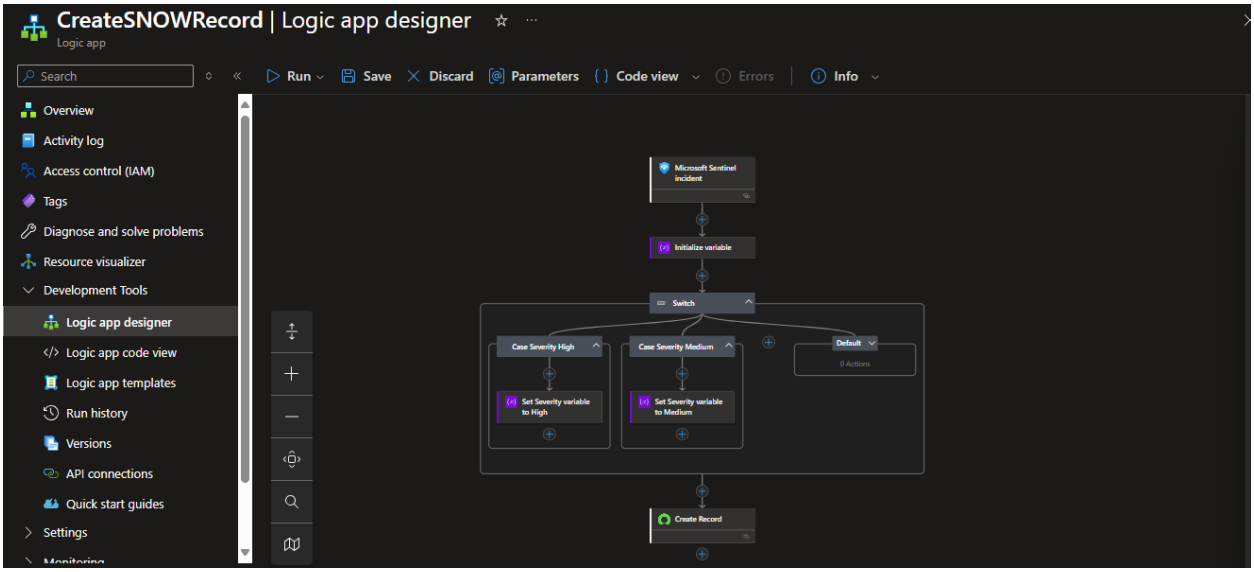

Create
Manage view
You are viewing a new version of Browse experience. Click here to access the old experience.
Name ↑
LAW-RG-lab
Showing 1 - 1 of 1. Display count: auto
412 Solutions
318 Standalone contents
4 Installed
0 Updates
Didn't find what you were looking for? We're showing a limited set of results. Try refining your search for more specific re
virusTotal
Status : All
Content type : All
Support : All
Provider : All
Category : All
Content sources : All
Content title
Status
Content source
VirusTotal FEATURED
In progress
Solution
Get-VirusTotalFileInfo-AlertTriggered
Get-VirusTotalURLReport-AlertTriggered
Get-VirusTotalDomainReport-AlertTriggered
Get-VirusTotalIPReport-AlertTriggered
VirusTotal
VirusTotal Provider
Microsoft Support
3.0.1 Version
The VirusTotal solution for Microsoft Sentinel contains Playbooks that can help enrich incident information with threat information and intelligence for IPs, file hashes and URLs from VirusTotal. Enriched information can help drive focused investigations in Security Operations.
Playbooks: 9
Content type
9
Playbook

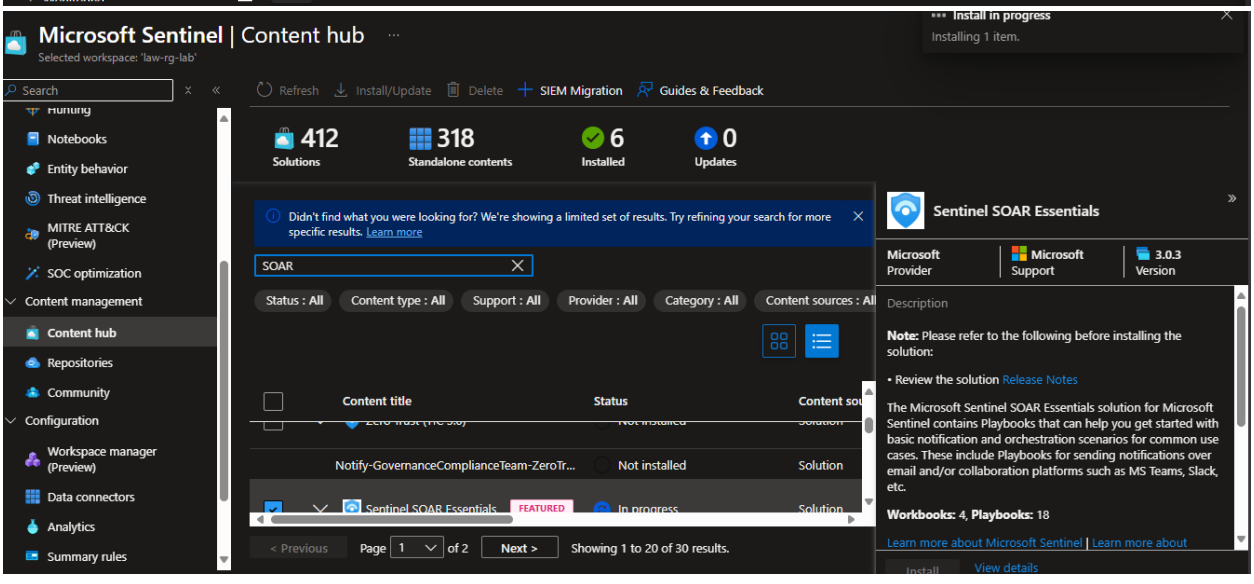

VirusTotal
Refresh
Delete
Reinstall
9
Installed content items
9
Configuration needed
VirusTotal
VirusTotal Provider
Microsoft Support
3.0.1 Version
Description
Note: Please refer to the following before installing the solution:
• Review the solution Release Notes
The VirusTotal solution for Microsoft Sentinel contains Playbooks that can help enrich incident information with threat information and intelligence for IPs, file hashes and URLs from VirusTotal. Enriched information can help drive focused investigations in Security Operations.
Playbooks: 9
Manage
Actions
View details
Search...
Content name
Get-VirusTotalDomainReport-AlertTriggered
Get-VirusTotalDomainReport-IncidentTriggered
Get-VirusTotalFileInfo-AlertTriggered
Get-VirusTotalFileInfo-IncidentTriggered
Get-VirusTotalIPReport-AlertTriggered
Get-VirusTotalIPReport-EntityTrigger
Get-VirusTotalIPReport-IncidentTriggered
Get-VirusTotalURLReport-AlertTriggered
Get-VirusTotalURLReport-IncidentTriggered
No templat
Select templates to

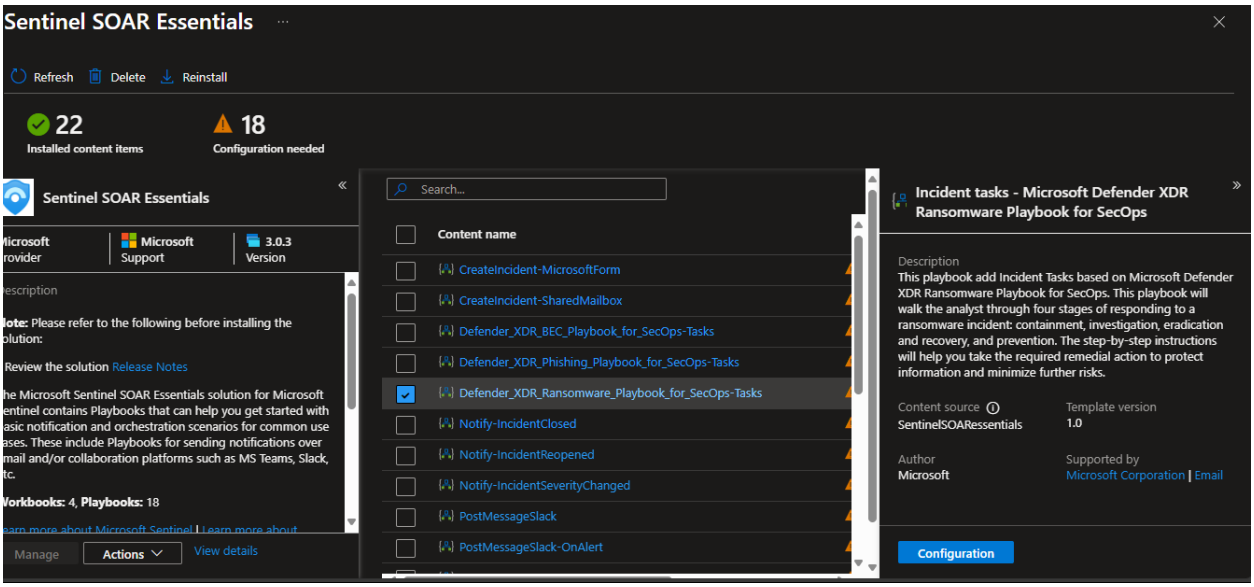

Home > Microsoft Sentinel | Content hub > VirusTotal > Get-VirusTotalReport-incidentTriggered
Get-VirusTotalReport-incidentTriggered | Logic app designer
Logic app
Search
Run
Save
Discard
Parameters
Code view
Errors
Info
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Development Tools
Logic app designer
Logic app code view
Logic app templates
Run history
Versions
API connections
Quick start guides
Settings
Add or remove favorites by pressing Ctrl+Shift+F
Microsoft Sentinel incident
Entities - Get IPs
For each
Get an IP report

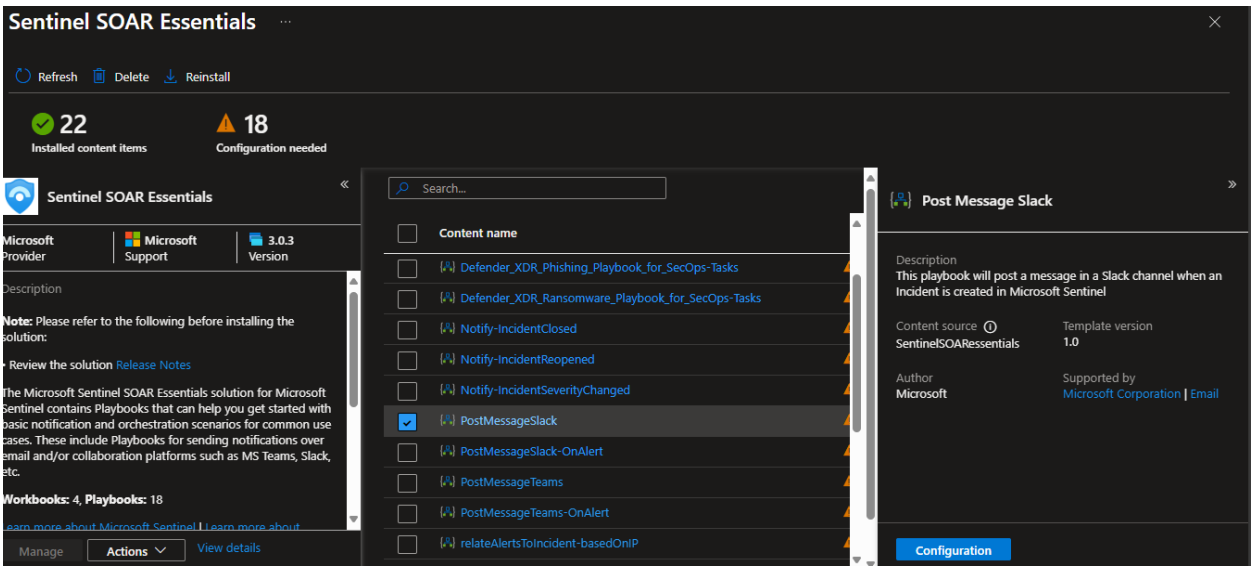

Get-VirusTotalReport-incidentTriggered | Logic app designer
Logic app
Search
Run
Save
Discard
Parameters
Code view
Errors
Info
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Development Tools
Logic app designer
Logic app code view
Logic app templates
Run history
Versions
API connections
Quick start guides
Settings
Add or remove favorites by pressing Ctrl+Shift+F
Get an IP report
Condition
True
False
Send Data
Send Data 1
Add comment to incident (V3)
Add comment to incident (V3) 1

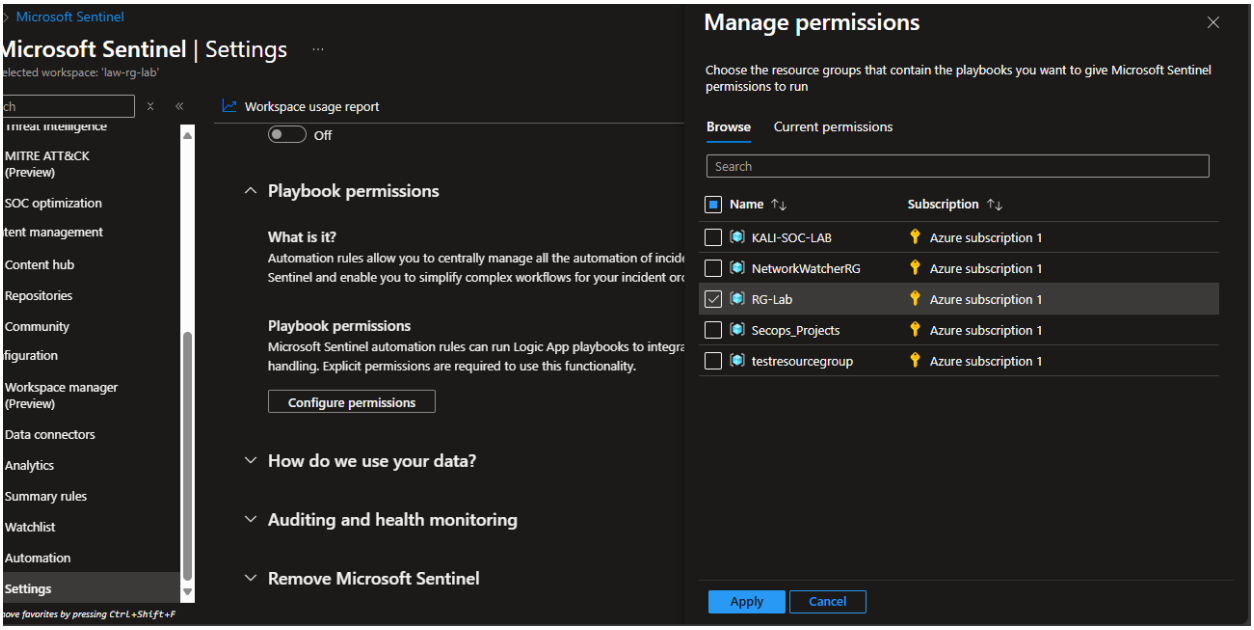

Microsoft Sentinel | Content hub
Selected workspace: 'law-rg-lab'
Installing 1 item.
Search
Refresh
Install/Update
Delete
SIEM Migration
Guides & Feedback
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
SOC optimization
Content management
Content hub
Repositories
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Summary rules
412
Solutions
318
Standalone contents
5
Installed
0
Updates
Didn't find what you were looking for? We're showing a limited set of results. Try refining your search for more specific results. Learn more
servicenow
Status : All
Content type : All
Support : All
Provider : All
Category : All
Content sources : All
Content title
Status
ServiceNow
In progress
Solution
Create And Update Service Now Record
In progress
Solution
< Previous
Page 1 of 1
Next >
Showing 1 to 4 of 4 results.
ServiceNow
Microsoft Provider
Microsoft Support
2.0.2 Version
Description
The ServiceNow ITSM solution for Microsoft Sentinel makes it easy to synchronize incidents between Microsoft Sentinel and ServiceNow IT Service Management (ITSM). This can be achieved by either one of the following two options -
Option 1 (Recommended): Bi-directional incident sync using app hosted on ServiceNow store. This option includes the following key features:
• Retrieve Microsoft Sentinel incidents and automate the creation of incidents in ServiceNow.
• Bi-directional sync of Status, Severity, Owner, Comments/Work notes, Entities and alerts.
Install
View details


CreateSNOWRecord | Logic app designer
Logic app
Search
Run
Save
Discard
Parameters
Code view
Errors
Info
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Development Tools
Logic app designer
Logic app code view
Logic app templates
Run history
Versions
API connections
Quick start guides
Settings
Microsoft Sentinel incident
Initialize variable
Switch
Case Severity High
Case Severity Medium
Default
0 Actions
Set Severity variable to High
Set Severity variable to Medium
Create Record


Microsoft Sentinel | Content hub
Selected workspace: 'law-rg-lab'
Install in progress
Installing 1 item.
Search
Refresh
Install/Update
Delete
SIEM Migration
Guides & Feedback
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
SOC optimization
Content management
Content hub
Repositories
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Summary rules
412
Solutions
318
Standalone contents
6
Installed
0
Updates
Didn't find what you were looking for? We're showing a limited set of results. Try refining your search for more specific results. Learn more
SOAR
Status : All
Content type : All
Support : All
Provider : All
Category : All
Content sources : All
Content title
Status
Notify-GovernanceComplianceTeam-ZeroTr...
Not installed
Solution
Sentinel SOAR Essentials
FEATURED
In progress
Solution
< Previous
Page 1 of 2
Next >
Showing 1 to 20 of 30 results.
Sentinel SOAR Essentials
Microsoft Provider
Microsoft Support
3.0.3 Version
Description
Note: Please refer to the following before installing the solution:
• Review the solution Release Notes
The Microsoft Sentinel SOAR Essentials solution for Microsoft Sentinel contains Playbooks that can help you get started with basic notification and orchestration scenarios for common use cases. These include Playbooks for sending notifications over email and/or collaboration platforms such as MS Teams, Slack, etc.
Workbooks: 4, Playbooks: 18
Learn more about Microsoft Sentinel | Learn more about
Install
View details


Sentinel SOAR Essentials
Refresh
Delete
Reinstall
22
Installed content items
18
Configuration needed
Sentinel SOAR Essentials
Microsoft Support
3.0.3 Version
Description
Note: Please refer to the following before installing the solution:
Review the solution Release Notes
The Microsoft Sentinel SOAR Essentials solution for Microsoft Sentinel contains Playbooks that can help you get started with basic notification and orchestration scenarios for common use cases. These include Playbooks for sending notifications over email and/or collaboration platforms such as MS Teams, Slack, etc.
Workbooks: 4, Playbooks: 18
Manage
Actions
View details
Search...
Content name
CreateIncident-MicrosoftForm
CreateIncident-SharedMailbox
Defender_XDR_BEC_Playbook_for_SecOps-Tasks
Defender_XDR_Phishing_Playbook_for_SecOps-Tasks
Defender_XDR_Ransomware_Playbook_for_SecOps-Tasks
Notify-IncidentClosed
Notify-IncidentReopened
Notify-IncidentSeverityChanged
PostMessageSlack
PostMessageSlack-OnAlert
Incident tasks - Microsoft Defender XDR Ransomware Playbook for SecOps
Description
This playbook add Incident Tasks based on Microsoft Defender XDR Ransomware Playbook for SecOps. This playbook will walk the analyst through four stages of responding to a ransomware incident: containment, investigation, eradication and recovery, and prevention. The step-by-step instructions will help you take the required remedial action to protect information and minimize further risks.
Content source
SentinelSOAREssentials
Template version
1.0
Author
Microsoft
Supported by
Microsoft Corporation | Email
Configuration

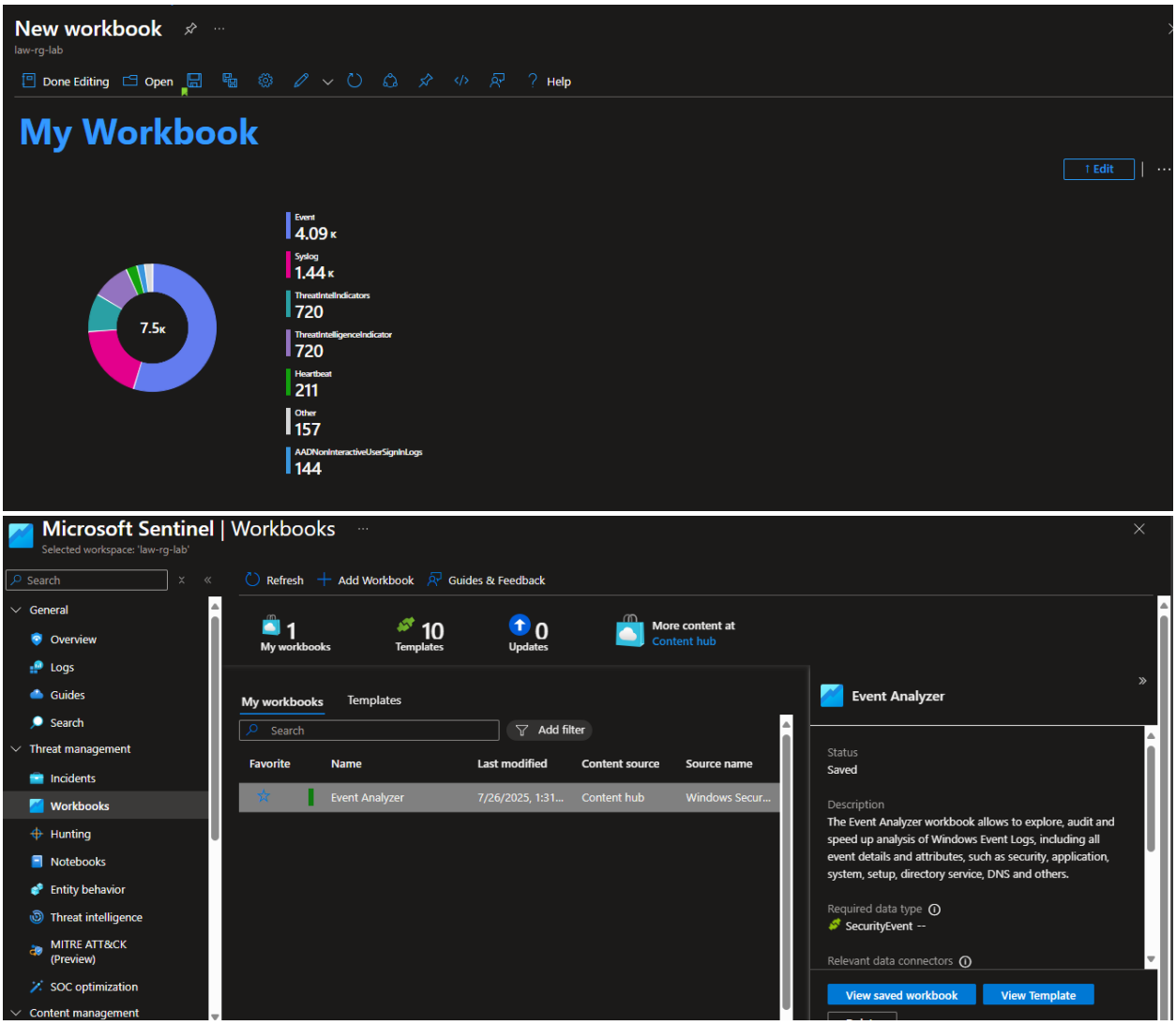

Sentinel SOAR Essentials
Refresh
Delete
Reinstall
22
Installed content items
18
Configuration needed
Sentinel SOAR Essentials
Microsoft Support
3.0.3 Version
Description
Note: Please refer to the following before installing the solution:
Review the solution Release Notes
The Microsoft Sentinel SOAR Essentials solution for Microsoft Sentinel contains Playbooks that can help you get started with basic notification and orchestration scenarios for common use cases. These include Playbooks for sending notifications over email and/or collaboration platforms such as MS Teams, Slack, etc.
Workbooks: 4, Playbooks: 18
Manage
Actions
View details
Search...
Content name
Defender_XDR_Phishing_Playbook_for_SecOps-Tasks
Defender_XDR_Ransomware_Playbook_for_SecOps-Tasks
Notify-IncidentClosed
Notify-IncidentReopened
Notify-IncidentSeverityChanged
PostMessageSlack
PostMessageSlack-OnAlert
PostMessageTeams
PostMessageTeams-OnAlert
relateAlertsToIncident-basedOnIP
Post Message Slack
Description
This playbook will post a message in a Slack channel when an Incident is created in Microsoft Sentinel
Content source
SentinelSOAREssentials
Template version
1.0
Author
Microsoft
Supported by
Microsoft Corporation | Email
Configuration



Microsoft Sentinel Workbooks

Workbooks in Microsoft Sentinel are interactive, customizable dashboards that help visualize and analyze security data.

1. **Key Use Cases**:
    - **SOC Monitoring**: Track security events in real time.
    - **Compliance and Audit Reporting**: Generate compliance-related visualizations.
    - **Threat Hunting**: Visualize anomalies, patterns, and indicators of compromise (IoCs).
2. **Creating Workbooks**:
    - **Use Templates**: Browse and customize from available templates.
    - **Create from Scratch**: Build dashboards with custom queries and visualizations.
    - **Customize**: Edit titles, descriptions, and content using Markdown and KQL.
    - **Publish**: Save and share workbooks in structured formats (e.g., JSON).

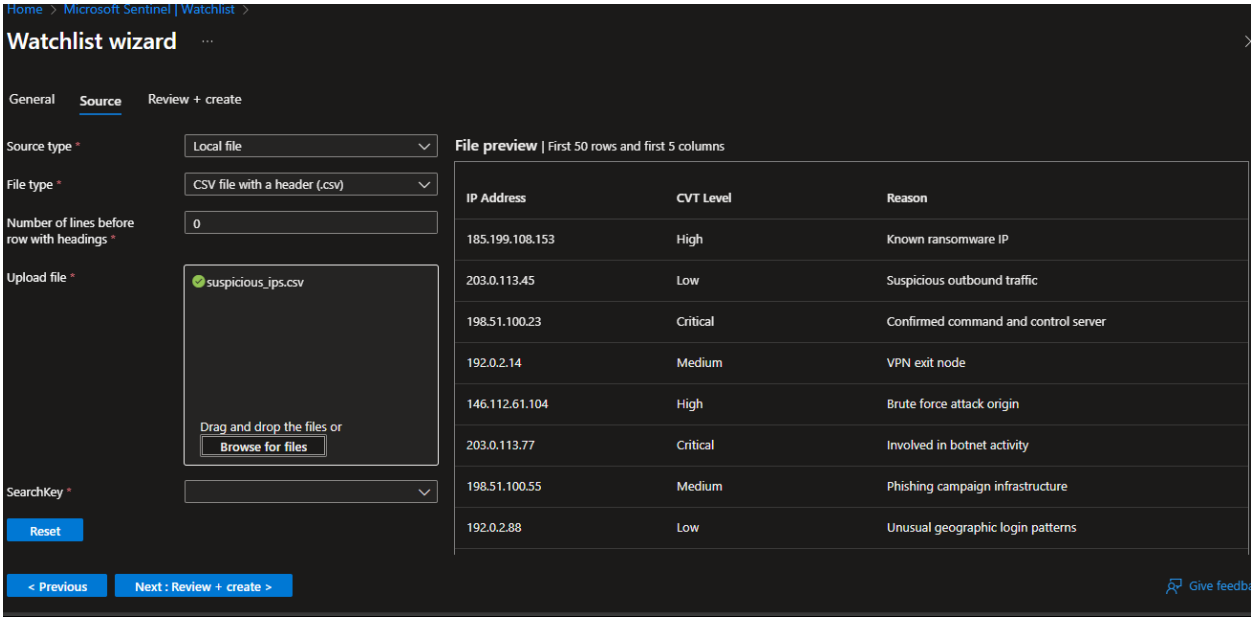


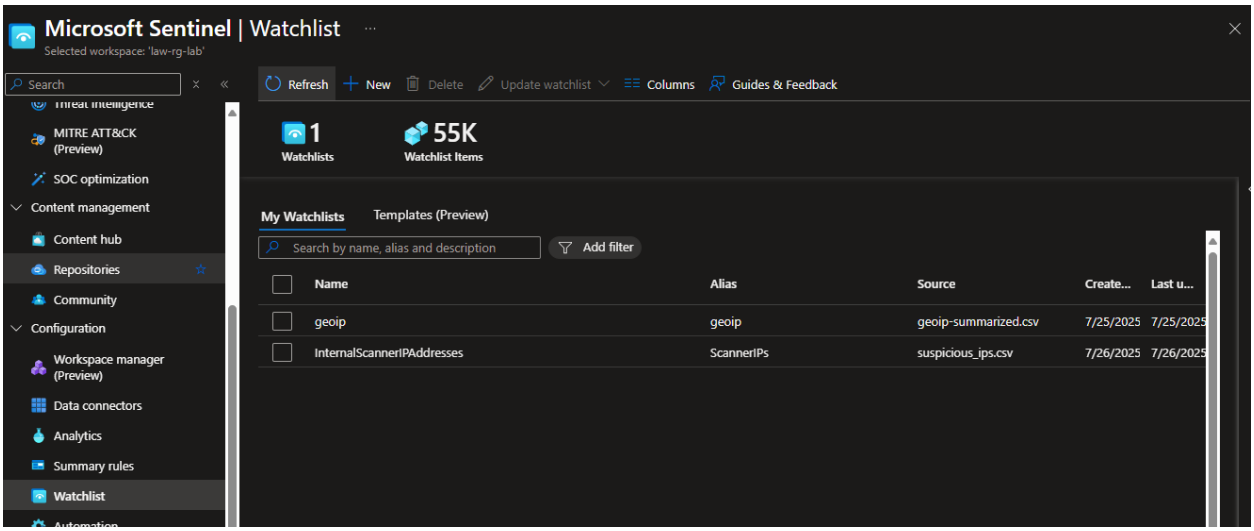
Microsoft Sentinel Watch Lists

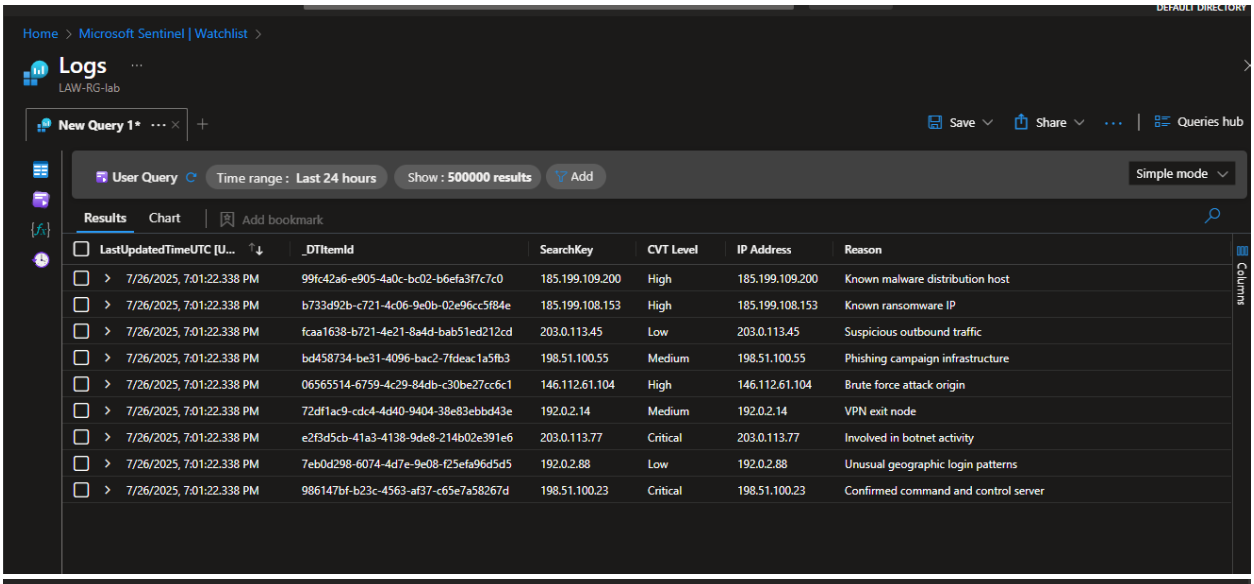
Watch Lists help organize and manage critical data such as IP addresses, domains, user accounts, and device names.

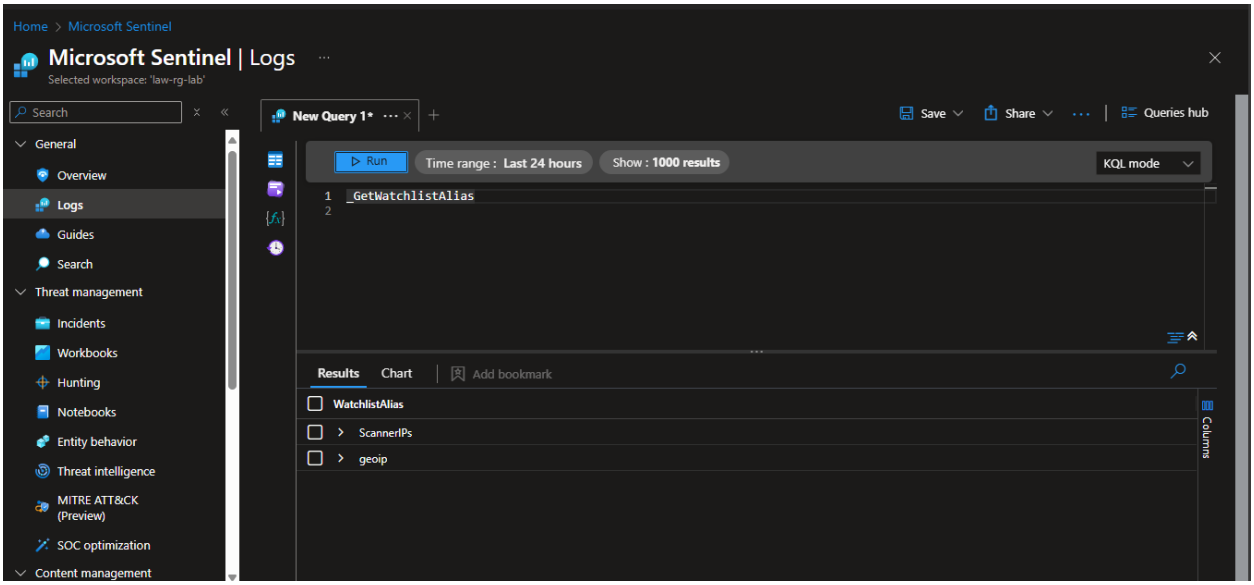
1. **Key Use Cases**:
    - **Rapid Threat Investigation**: Quickly correlate security data with known entities.
    - **Manage Business Data**: Track allowlists, blocklists, or sensitive user/device groups.
    - **Reduce Alert Fatigue**: Suppress alerts triggered by trusted or known-good sources.
    - **Enhance Event Data**: Enrich security logs using external or contextual business data.
2. **Creating Watch Lists**:
    - **Add New Watch List**: Define the name, description, and alias.
    - **Upload Data**: Use CSV files or connect to Azure Storage.

- **Define Search Key**: Specify a primary key field for referencing the list in analytics.
- **Update and Manage**: Edit items manually or bulk-update as needed.



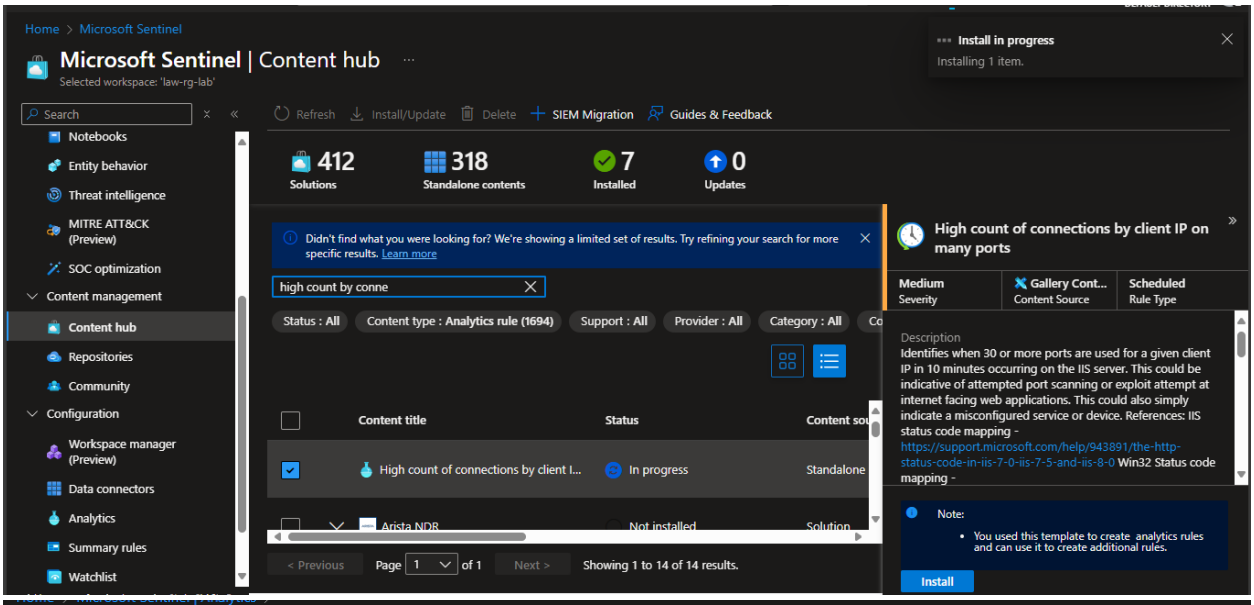


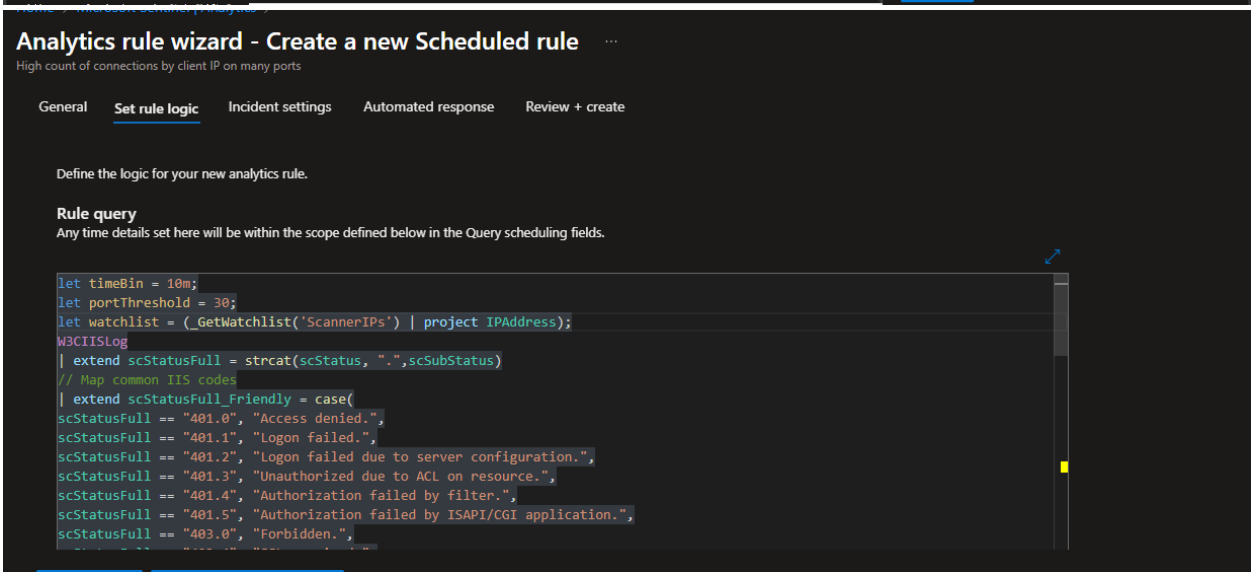


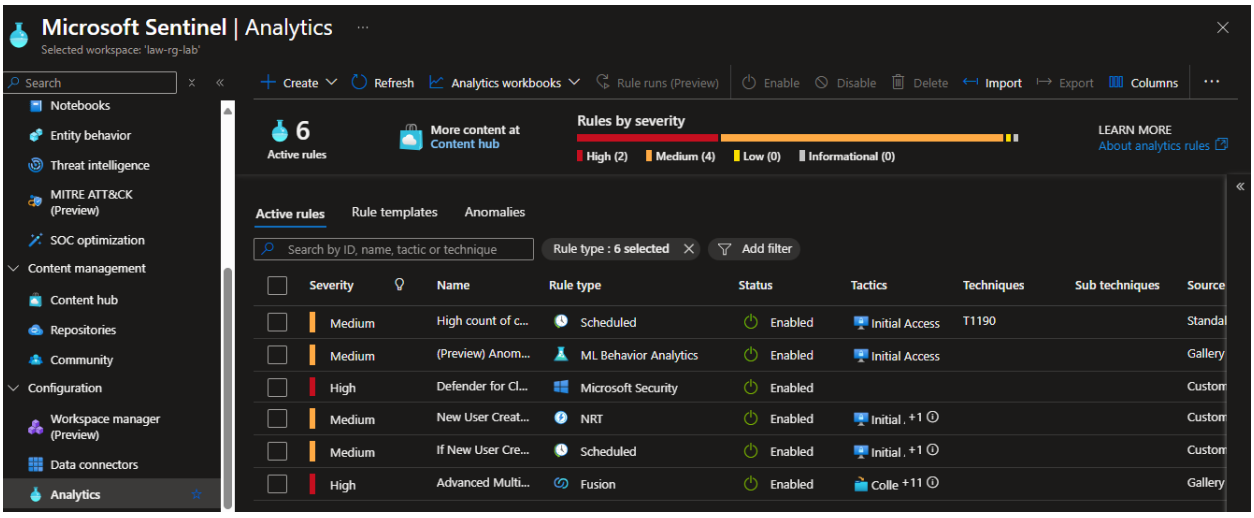


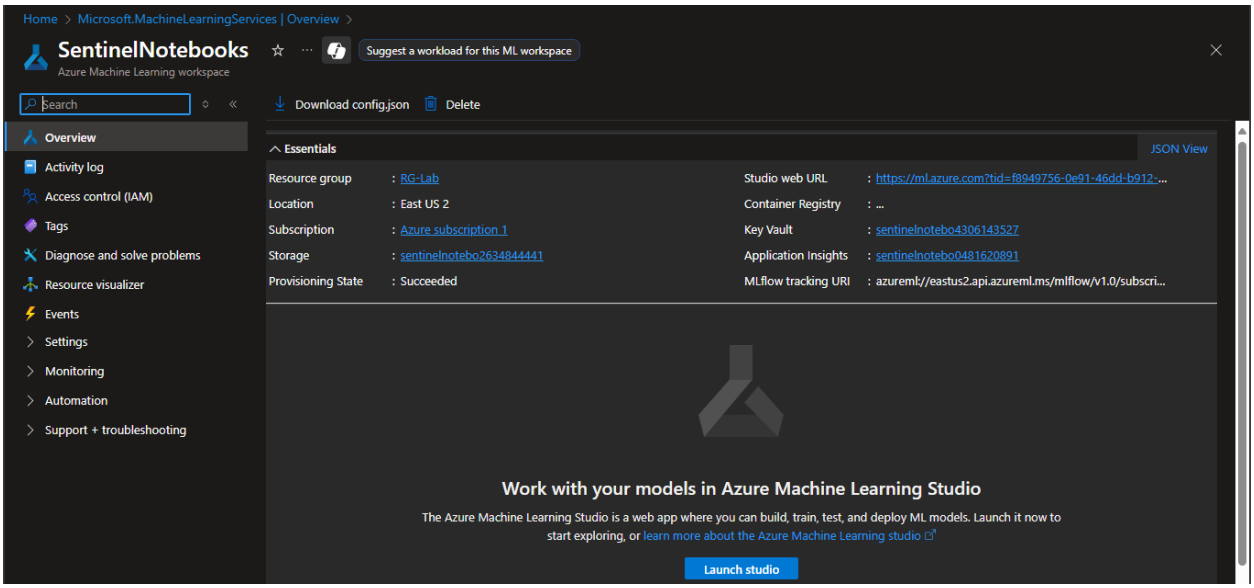
Conclusion

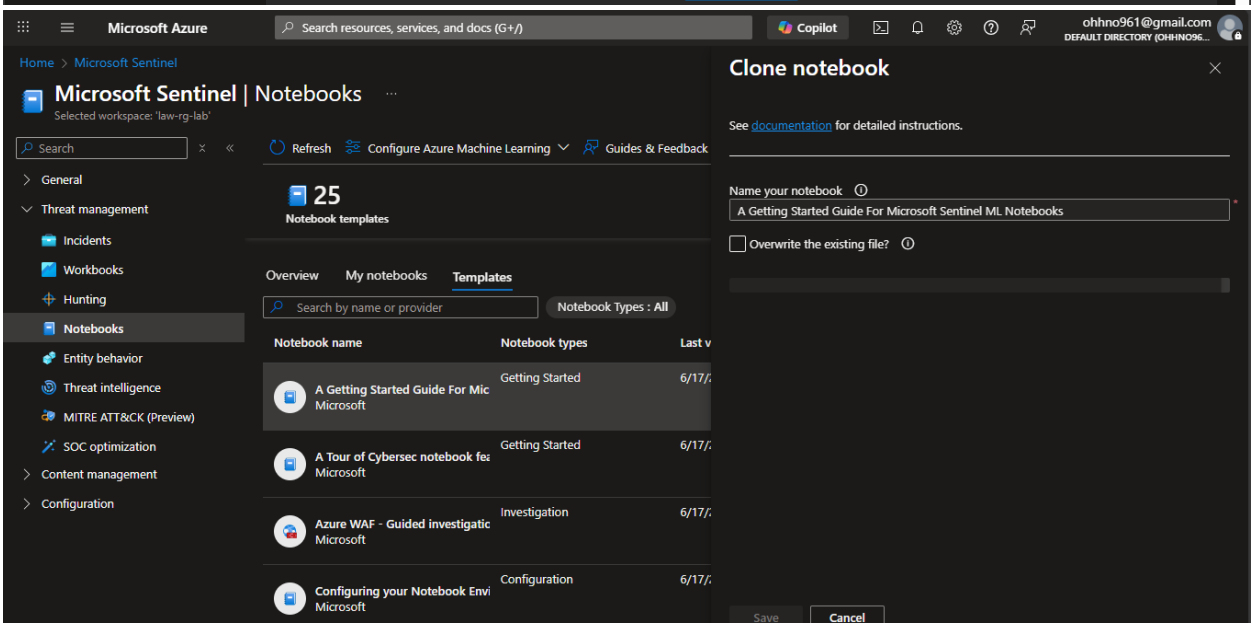
This documentation provides an in-depth look at automating threat responses, building workbooks, and managing watch lists in Microsoft Sentinel. By automating responses, organizations can reduce alert fatigue and accelerate incident handling. Workbooks offer powerful, real-time visualizations for SOC monitoring and threat hunting. Watch lists help correlate data and manage critical security context. Future chapters will explore these components in more depth, offering implementation details and best practices.

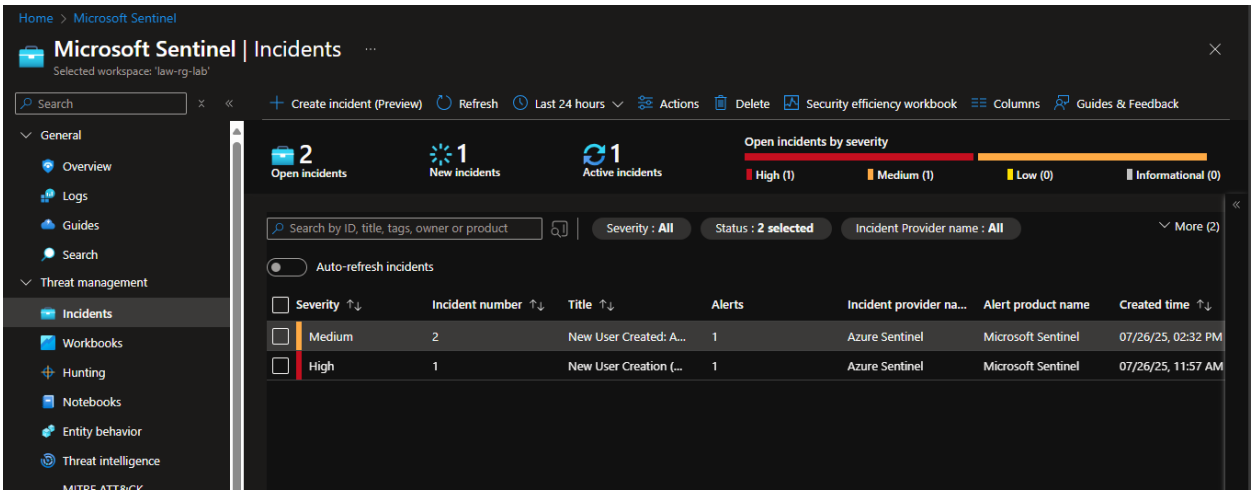

Home > Microsoft Sentinel
Microsoft Sentinel | Content hub
Selected workspace: 'law-rg-lab'
Install in progress
Installing 1 item.
Search
Refresh
Install/Update
Delete
SIEM Migration
Guides & Feedback
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
SOC optimization
Content management
Content hub
Repositories
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Summary rules
Watchlist
412
Solutions
318
Standalone contents
7
Installed
0
Updates
Didn't find what you were looking for? We're showing a limited set of results. Try refining your search for more specific results. Learn more
high count by conne
Status : All
Content type : Analytics rule (1694)
Support : All
Provider : All
Category : All
Content title
Status
High count of connections by client I...
In progress
Standalone
Arista NDR
Not installed
Solution
< Previous
Page 1 of 1
Next >
Showing 1 to 14 of 14 results.
High count of connections by client IP on many ports
Medium
Severity
Gallery Cont...
Content Source
Scheduled
Rule Type
Description
Identifies when 30 or more ports are used for a given client IP in 10 minutes occurring on the IIS server. This could be indicative of attempted port scanning or exploit attempt at internet facing web applications. This could also simply indicate a misconfigured service or device. References: IIS status code mapping - https://support.microsoft.com/help/943891/the-http-status-code-in-iis-7-0-iis-7-5-and-iis-8-0 Win32 Status code mapping -
Note:
You used this template to create analytics rules and can use it to create additional rules.
Install

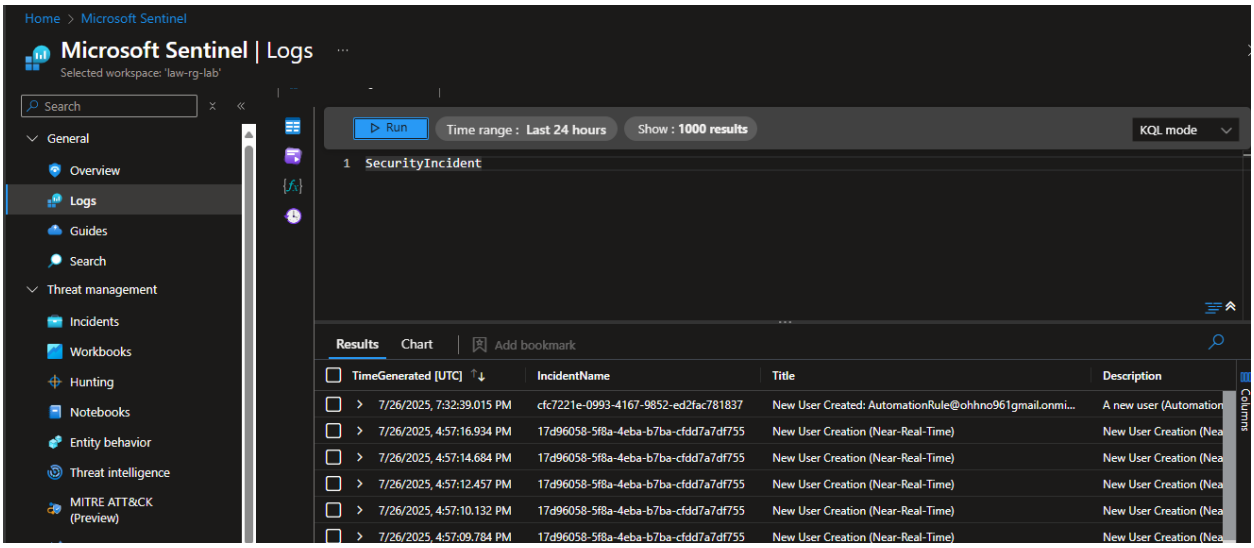

Analytics rule wizard - Create a new Scheduled rule
High count of connections by client IP on many ports
General
Set rule logic
Incident settings
Automated response
Review + create
Define the logic for your new analytics rule.
Rule query
Any time details set here will be within the scope defined below in the Query scheduling fields.
let timeBin = 10m;
let portThreshold = 30;
let watchlist = (_GetWatchlist('ScannerIPs') | project IPAddress);
W3CIISLog
| extend scStatusFull = strcat(scStatus, ".",scSubStatus)
// Map common IIS codes
| extend scStatusFull_Friendly = case(
scStatusFull == "401.0", "Access denied.",
scStatusFull == "401.1", "Logon failed.",
scStatusFull == "401.2", "Logon failed due to server configuration.",
scStatusFull == "401.3", "Unauthorized due to ACL on resource.",
scStatusFull == "401.4", "Authorization failed by filter.",
scStatusFull == "401.5", "Authorization failed by ISAPI/CGI application.",
scStatusFull == "403.0", "Forbidden.",

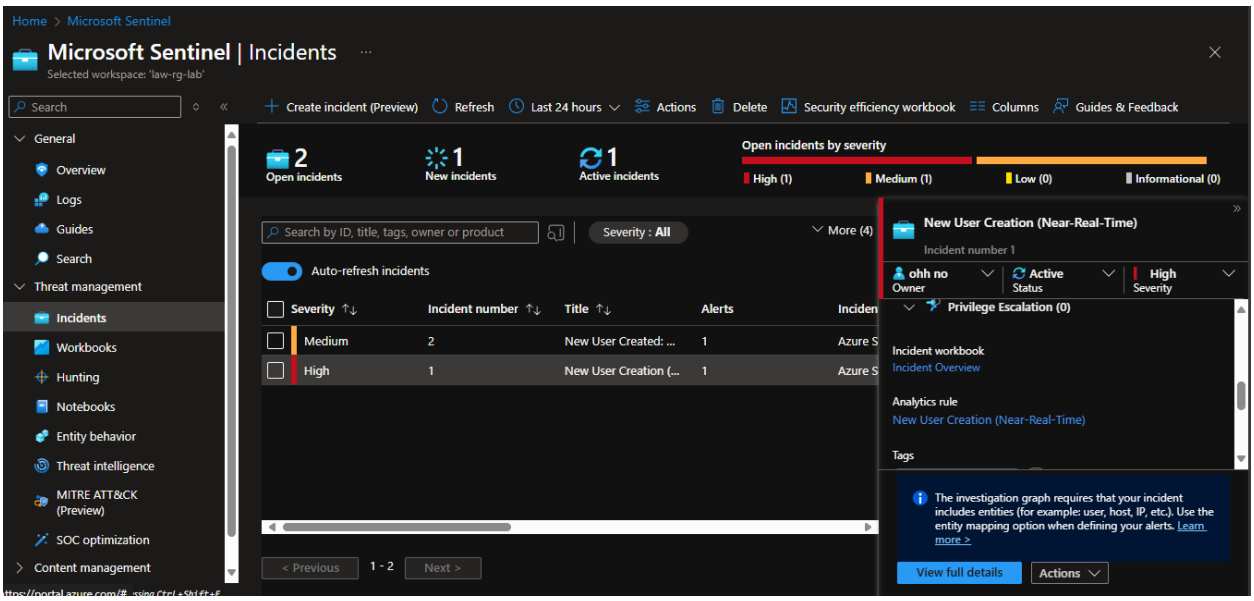

Microsoft Sentinel | Analytics
Selected workspace: 'law-rg-lab'
Search
Create
Refresh
Analytics workbooks
Rule runs (Preview)
Enable
Disable
Delete
Import
Export
Columns
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
SOC optimization
Content management
Content hub
Repositories
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
6
Active rules
More content at Content hub
Rules by severity
High (2)
Medium (4)
Low (0)
Informational (0)
LEARN MORE
About analytics rules
Active rules
Rule templates
Anomalies
Search by ID, name, tactic or technique
Rule type : 6 selected
Add filter
Severity
Name
Rule type
Status
Tactics
Techniques
Sub techniques
Source
Medium
High count of c...
Scheduled
Enabled
Initial Access
T1190
Standal
Medium
(Preview) Anom...
ML Behavior Analytics
Enabled
Initial Access
Gallery
High
Defender for Cl...
Microsoft Security
Enabled
Custom
Medium
New User Creat...
NRT
Enabled
Initial , +1
Custom
Medium
If New User Cre...
Scheduled
Enabled
Initial , +1
Custom
High
Advanced Multi...
Fusion
Enabled
Colle +11
Gallery

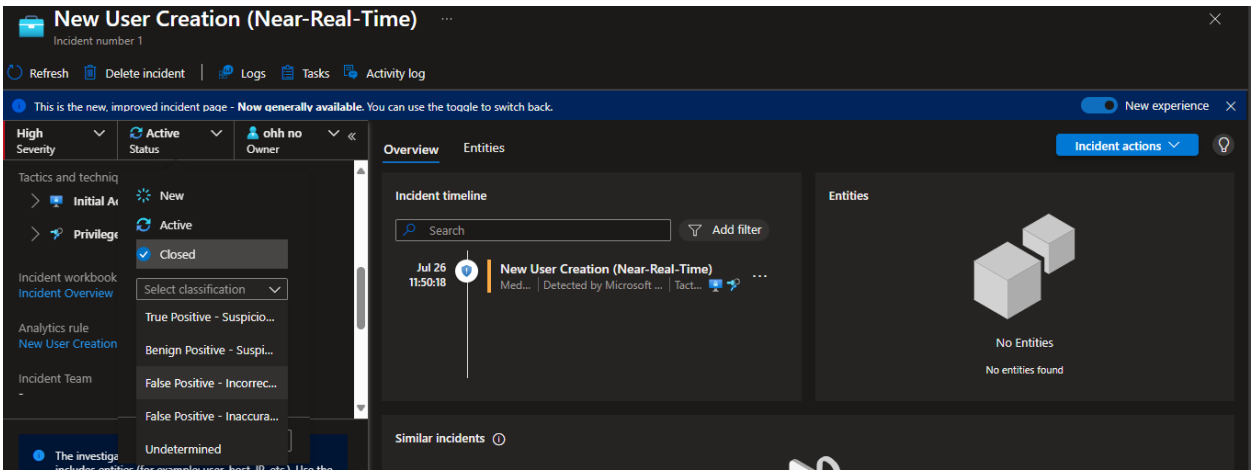

Home > Microsoft.MachineLearningServices | Overview >
SentinelNotebooks
Azure Machine Learning workspace
Suggest a workload for this ML workspace
Search
Download config.json
Delete
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Events
Settings
Monitoring
Automation
Support + troubleshooting
Essentials
JSON View
Resource group : RG-Lab
Location : East US 2
Subscription : Azure subscription 1
Storage : sentinelnotebo2634844441
Provisioning State : Succeeded
Studio web URL : https://ml.azure.com?tid=f8949756-0e91-46dd-b912-...
Container Registry : ...
Key Vault : sentinelnotebo4306143527
Application Insights : sentinelnotebo0481620891
MLflow tracking URI : azureml://eastus2.api.azureml.ms/mlflow/v1.0/subscri...
Work with your models in Azure Machine Learning Studio
The Azure Machine Learning Studio is a web app where you can build, train, test, and deploy ML models. Launch it now to start exploring, or learn more about the Azure Machine Learning studio
Launch studio

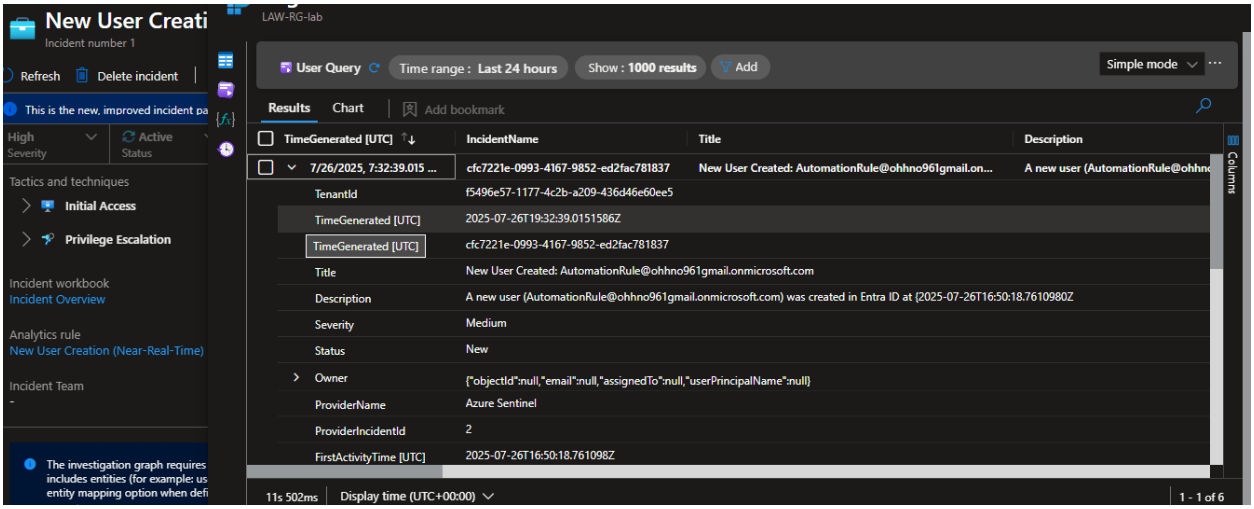

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
Home > Microsoft Sentinel
Microsoft Sentinel | Notebooks
Selected workspace: 'law-rg-lab'
Search
Refresh
Configure Azure Machine Learning
Guides & Feedback
General
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
SOC optimization
Content management
Configuration
25
Notebook templates
Overview
My notebooks
Templates
Search by name or provider
Notebook Types : All
Notebook name
Notebook types
Last v
A Getting Started Guide For Mic
Microsoft
Getting Started
6/17/
A Tour of Cybersec notebook fea
Microsoft
Getting Started
6/17/
Azure WAF - Guided investigatic
Microsoft
Investigation
6/17/
Configuring your Notebook Envi
Microsoft
Configuration
6/17/
Clone notebook
See documentation for detailed instructions.
Name your notebook
A Getting Started Guide For Microsoft Sentinel ML Notebooks
Overwrite the existing file?
Save
Cancel

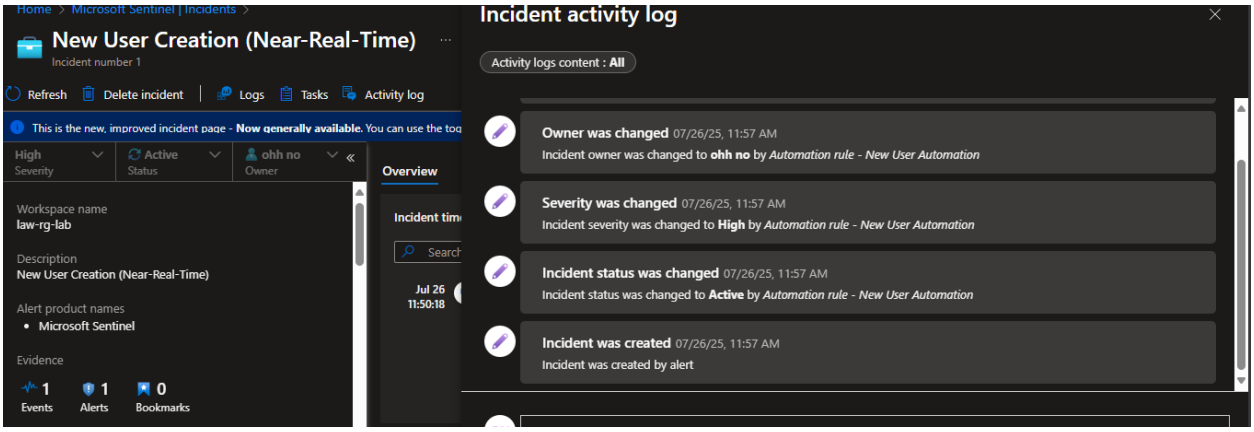

Home > Microsoft Sentinel
Microsoft Sentinel | Incidents
Selected workspace: 'law-rg-lab'
Search
Create incident (Preview)
Refresh
Last 24 hours
Actions
Delete
Security efficiency workbook
Columns
Guides & Feedback
General
Overview
Logs
Guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
2
Open incidents
1
New incidents
1
Active incidents
Open incidents by severity
High (1)
Medium (1)
Low (0)
Informational (0)
Search by ID, title, tags, owner or product
Severity : All
Status : 2 selected
Incident Provider name : All
More (2)
Auto-refresh incidents
Severity
Incident number
Title
Alerts
Incident provider na...
Alert product name
Created time
Medium
2
New User Created: A...
1
Azure Sentinel
Microsoft Sentinel
07/26/25, 02:32 PM
High
1
New User Creation (...
1
Azure Sentinel
Microsoft Sentinel
07/26/25, 11:57 AM

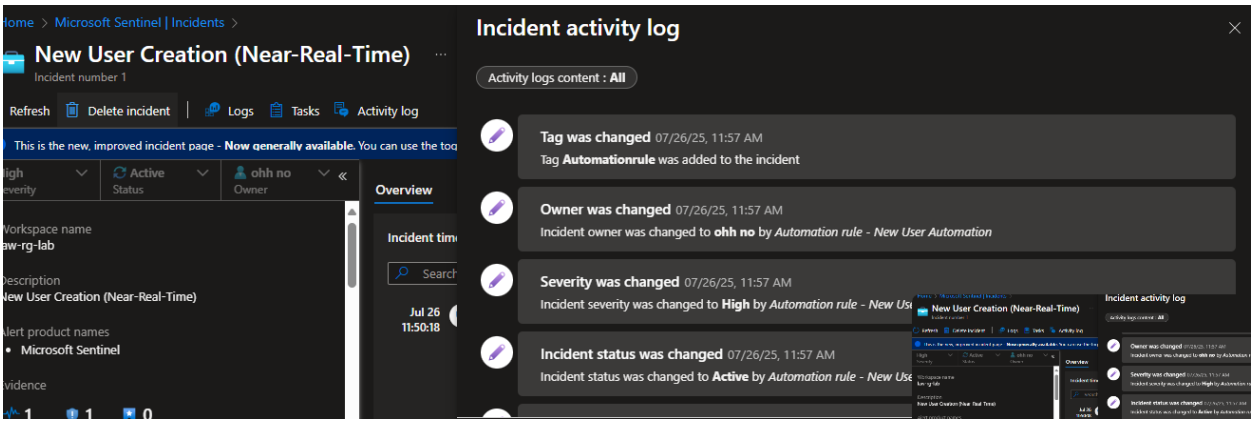

Home > Microsoft Sentinel
Microsoft Sentinel | Logs
Selected workspace: 'law-rg-lab'
Search
General
Overview
Logs
Guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Run
Time range : Last 24 hours
Show : 1000 results
KQL mode
1 SecurityIncident
Results
Chart
Add bookmark
TimeGenerated [UTC]
IncidentName
Title
Description
7/26/2025, 7:32:39.015 PM
cfc7221e-0993-4167-9852-ed2fac781837
New User Created: AutomationRule@ohhno961gmail.onmi...
A new user (Automation
7/26/2025, 4:57:16.934 PM
17d96058-5f8a-4eba-b7ba-cfdd7a7df755
New User Creation (Near-Real-Time)
7/26/2025, 4:57:14.684 PM
7/26/2025, 4:57:12.457 PM
7/26/2025, 4:57:10.132 PM
7/26/2025, 4:57:09.784 PM
Columns

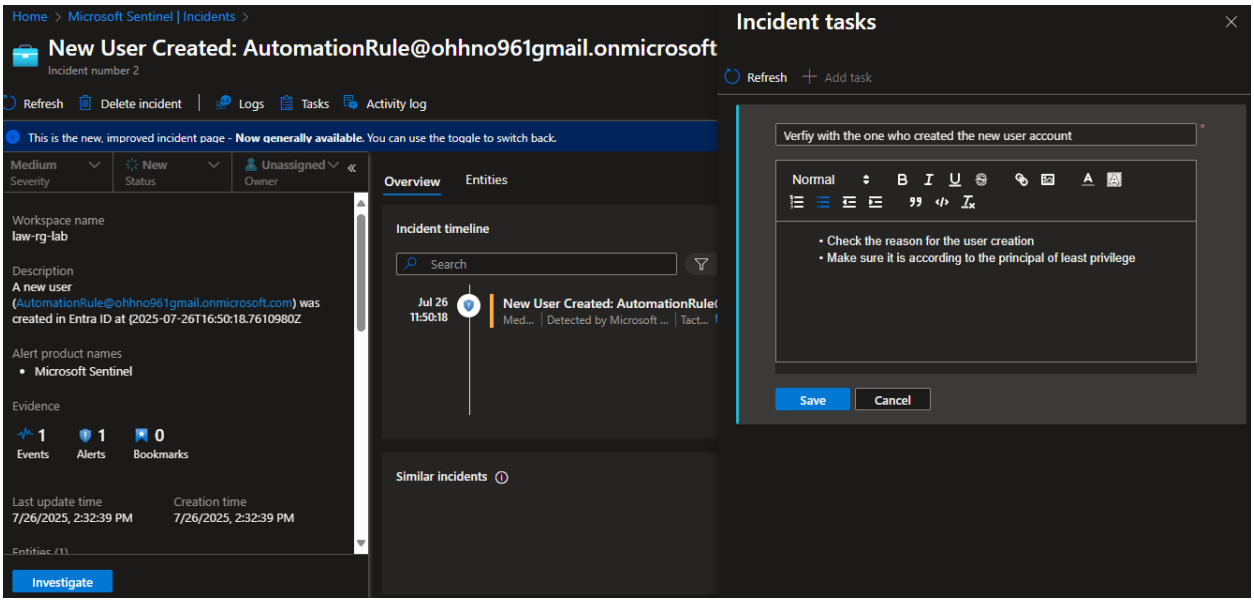

Home > Microsoft Sentinel
Microsoft Sentinel | Incidents
Selected workspace: 'law-rg-lab'
Create incident (Preview)
Refresh
Last 24 hours
Actions
Delete
Security efficiency workbook
Columns
Guides & Feedback
2 Open incidents
1 New incidents
1 Active incidents
Open incidents by severity
High (1)
Medium (1)
Low (0)
Informational (0)
Search by ID, title, tags, owner or product
Severity : All
More (4)
Auto-refresh incidents
Severity
Incident number
Title
Alerts
Medium
2
New User Created: ...
1
High
1
New User Creation (...
1
< Previous
1 - 2
Next >
New User Creation (Near-Real-Time)
Incident number 1
ohh no
Owner
Active
Status
High
Severity
Privilege Escalation (0)
Incident workbook
Incident Overview
Analytics rule
New User Creation (Near-Real-Time)
Tags
The investigation graph requires that your incident includes entities (for example: user, host, IP, etc.). Use the entity mapping option when defining your alerts. Learn more >
View full details
Actions

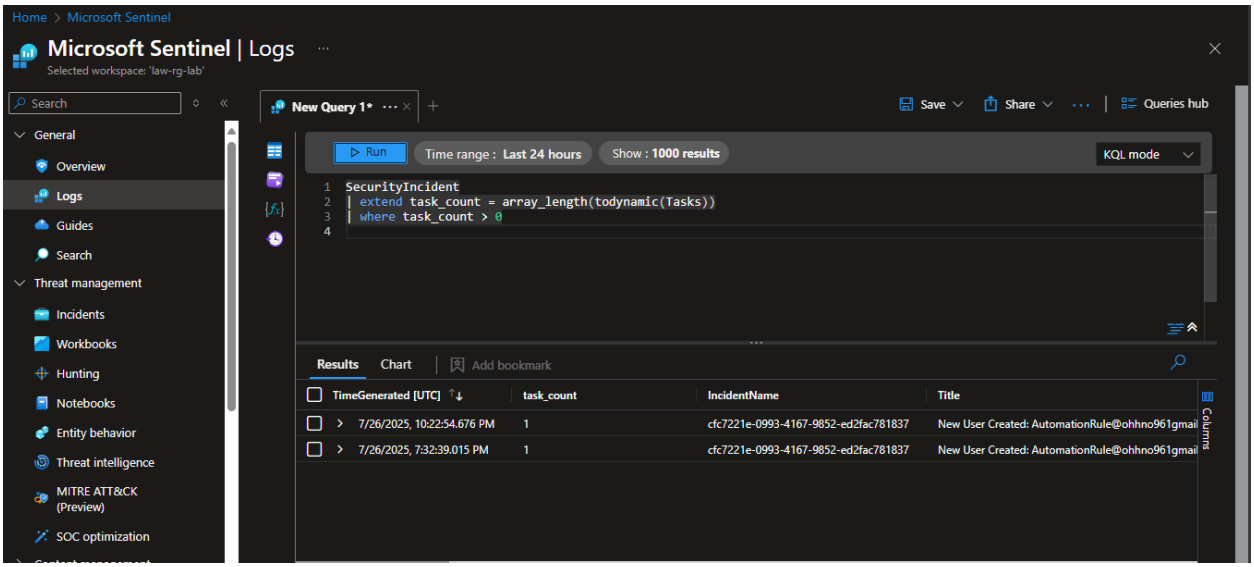

New User Creation (Near-Real-Time)
Incident number 1
Refresh
Delete incident
Logs
Tasks
Activity log
This is the new, improved incident page - Now generally available. You can use the toggle to switch back.
New experience
High
Severity
Active
Status
ohh no
Owner
Overview
Entities
Incident actions
New
Active
Closed
Select classification
True Positive - Suspicio...
Benign Positive - Suspi...
False Positive - Incorrec...
False Positive - Inaccura...
Undetermined
Incident workbook
Incident Overview
Analytics rule
New User Creation
Incident Team
Incident timeline
Search
Add filter
Jul 26
11:50:18
New User Creation (Near-Real-Time)
Entities
No Entities
No entities found
Similar incidents

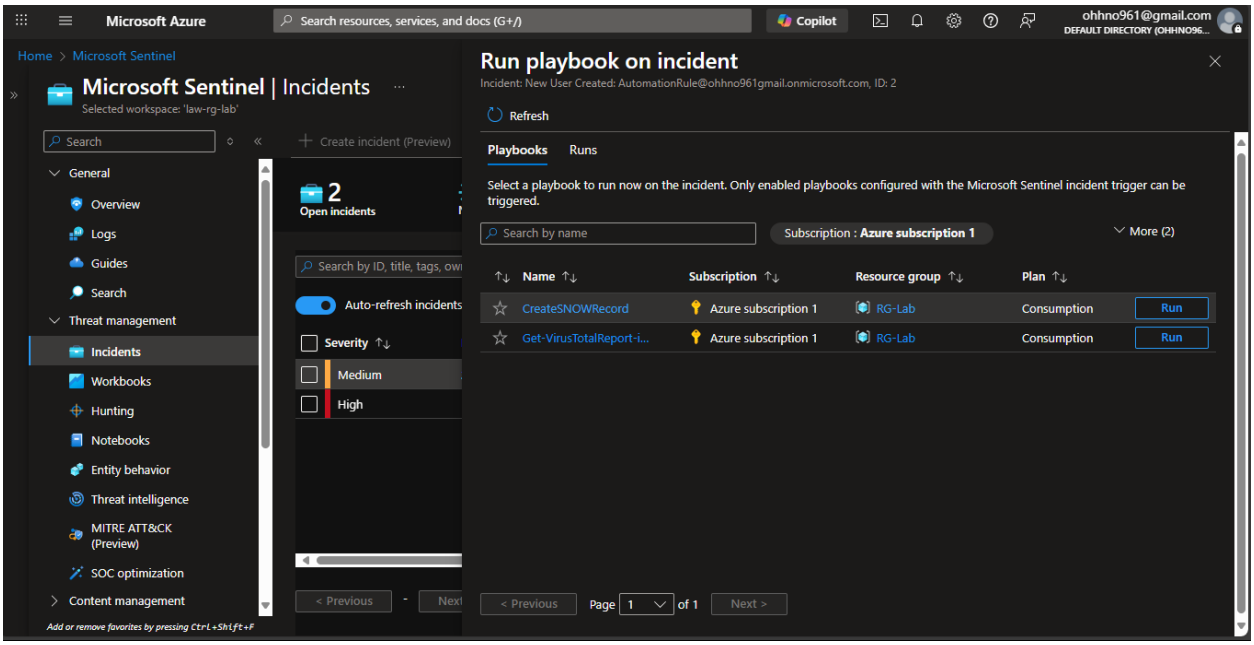

New User Creati
Incident number 1
Refresh
Delete incident
This is the new, improved incident pa
High
Severity
Active
Status
Tactics and techniques
Initial Access
Privilege Escalation
Incident workbook
Incident Overview
Analytics rule
New User Creation (Near-Real-Time)
Incident Team
The investigation graph requires
includes entities (for example: us
entity mapping option when defi
LAW-RG-lab
User Query
Time range : Last 24 hours
Show : 1000 results
Add
Simple mode
Results
Chart
Add bookmark
TimeGenerated [UTC]
IncidentName
Title
Description
7/26/2025, 7:32:39.015 ...
cfc7221e-0993-4167-9852-ed2fac781837
New User Created: AutomationRule@ohhno961gmail.on...
A new user (AutomationRule@ohhno
TenantId
f5496e57-1177-4c2b-a209-436d46e60ee5
TimeGenerated [UTC]
2025-07-26T19:32:39.0151586Z
TimeGenerated [UTC]
cfc7221e-0993-4167-9852-ed2fac781837
Title
New User Created: AutomationRule@ohhno961gmail.onmicrosoft.com
Description
A new user (AutomationRule@ohhno961gmail.onmicrosoft.com) was created in Entra ID at {2025-07-26T16:50:18.7610980Z
Severity
Medium
Status
New
Owner
{"objectId":null,"email":null,"assignedTo":null,"userPrincipalName":null}
ProviderName
Azure Sentinel
ProviderIncidentId
2
FirstActivityTime [UTC]
2025-07-26T16:50:18.761098Z
Columns
11s 502ms
Display time (UTC+00:00)
1 - 1 of 6

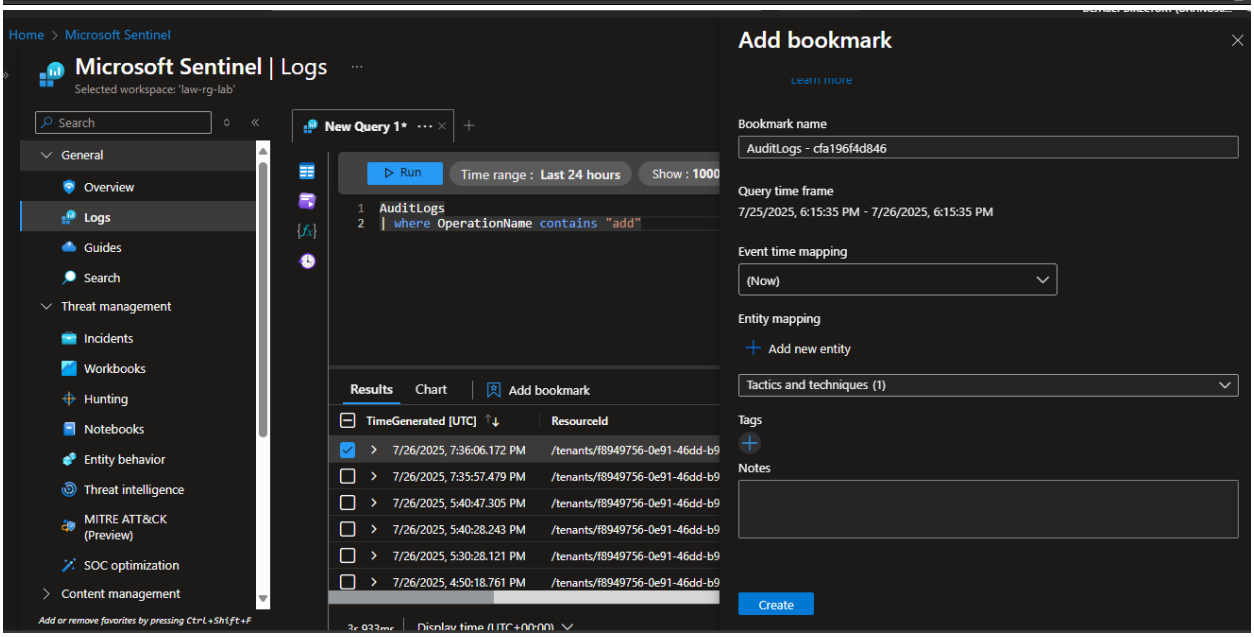

Home > Microsoft Sentinel | Incidents >
New User Creation (Near-Real-Time)
Incident number 1
Refresh
Delete incident
Logs
Tasks
Activity log
This is the new, improved incident page - Now generally available. You can use the too
High
Severity
Active
Status
ohh no
Owner
Overview
Workspace name
law-rg-lab
Description
New User Creation (Near-Real-Time)
Alert product names
Microsoft Sentinel
Evidence
1
Events
1
Alerts
0
Bookmarks
Incident activity log
Activity logs content : All
Owner was changed 07/26/25, 11:57 AM
Incident owner was changed to ohh no by Automation rule - New User Automation
Severity was changed 07/26/25, 11:57 AM
Incident severity was changed to High by Automation rule - New User Automation
Incident status was changed 07/26/25, 11:57 AM
Incident status was changed to Active by Automation rule - New User Automation
Incident was created 07/26/25, 11:57 AM
Incident was created by alert


Home > Microsoft Sentinel | Incidents >
New User Creation (Near-Real-Time)
Incident number 1
Refresh
Delete incident
Logs
Tasks
Activity log
This is the new, improved incident page - Now generally available. You can use the too
Active
Status
ohh no
Owner
Overview
Workspace name
law-rg-lab
Description
New User Creation (Near-Real-Time)
Alert product names
Microsoft Sentinel
Incident activity log
Activity logs content : All
Tag was changed 07/26/25, 11:57 AM
Tag Automationrule was added to the incident
Owner was changed 07/26/25, 11:57 AM
Incident owner was changed to ohh no by Automation rule - New User Automation
Severity was changed 07/26/25, 11:57 AM
Incident severity was changed to High by Automation rule - New Us
Incident status was changed 07/26/25, 11:57 AM
Incident status was changed to Active by Automation rule - New Use


Home > Microsoft Sentinel | Incidents >
New User Created: AutomationRule@ohhno961gmail.onmicrosoft
Incident number 2
Refresh
Delete incident
Logs
Tasks
Activity log
This is the new, improved incident page - Now generally available. You can use the toggle to switch back.
Medium
Severity
New
Status
Unassigned
Owner
Overview
Entities
Workspace name
law-rg-lab
Description
A new user (AutomationRule@ohhno961gmail.onmicrosoft.com) was created in Entra ID at (2025-07-26T16:50:18.7610980Z
Alert product names
Microsoft Sentinel
Evidence
1 Events
1 Alerts
0 Bookmarks
Last update time
7/26/2025, 2:32:39 PM
Creation time
7/26/2025, 2:32:39 PM
Investigate
Incident timeline
Search
Jul 26 11:50:18
New User Created: AutomationRule(
Similar incidents
Incident tasks
Refresh
Add task
Verfiy with the one who created the new user account
Normal
• Check the reason for the user creation
• Make sure it is according to the principal of least privilege
Save
Cancel


Home > Microsoft Sentinel
Microsoft Sentinel | Logs
Selected workspace: 'law-rg-lab'
Search
General
Overview
Logs
Guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
SOC optimization
New Query 1*
Save
Share
Queries hub
Run
Time range : Last 24 hours
Show : 1000 results
KQL mode
1 SecurityIncident
2 | extend task_count = array_length(todynamic(Tasks))
3 | where task_count > 0
4
Results
Chart
Add bookmark
TimeGenerated [UTC]
task_count
IncidentName
Title
7/26/2025, 10:22:54.676 PM
1
cfc7221e-0993-4167-9852-ed2fac781837
New User Created: AutomationRule@ohhno961gmail
7/26/2025, 7:32:39.015 PM
1
cfc7221e-0993-4167-9852-ed2fac781837
New User Created: AutomationRule@ohhno961gmail
Columns





Final Conclusion:

The successful implementation of Microsoft Sentinel's advanced features has significantly enhanced our cybersecurity capabilities. By automating incident response, integrating threat intelligence, and creating interactive workbooks, we have improved our threat detection and response mechanisms. These enhancements allow us to proactively identify and mitigate sophisticated threats, ensuring a more resilient and secure environment. Future efforts will focus on continuous monitoring, updating threat intelligence, and refining detection rules to stay ahead of emerging threats.