Getting Started with Microsoft Azure Sentinel

What is Azure Sentinel?

Azure Sentinel is a **SIEM** (security information event management) and **SOAR** (security orchestration automated response) system in Azure. This means that incidents and security threats can be detected and alerted. You can use it to investigate and mitigate threats. You can gain insight into collected data, events and potential harmful incidents through overviews, dashboards and custom queries. Once an accident occurs, you can choose to launch the Azure Sentinel Playbook, a logical application that begins the automatic mitigation process.

Azure Sentinel four crucial areas or stages:

- **Collect.** Collecting data from multiple sources and clouds, on-premises, applications, infrastructure, users, services, and others.
- **Detect.** Detect threats to protected and monitored resources as they happen, minimizing the time to react to threats.
- **Investigate.** Powered with artificial intelligence, search for and discover malicious activities across all protected assets.
- **Respond.** Once a threat is known, avoid manual actions and respond to threats with automating tasks.

What does it cost?

- **Capacity Reservation based pricing**
  - Capacity Reservation is a fixed-fee license, where you pay for capacity (and receive discounts based on the amount of capacity you purchase).
  - Purchasing capacity for 100 GB per day will cost you 109.63 € ($123)/day
- **Pay-As-You-Go**
  - The first 5 GB is free, then per GB you'd pay 2.522 € ($2.99).
  - Pay-As-You-Go is based on Log Analytics pricing, and it's set at 2.20 € ($2.60)/GB.

What data can you ingest in azure sentinel at no cost.?

- Azure Activity Logs
- Office 365 Activity Logs
- Alerts from Microsoft Threat Protection Are available at no cost.

What about Azure Security Center?

- **ASC** is more about getting and understanding how to best configure your Azure assets
- **Azure Sentinel** is all about detecting bad actors from accessing your data.

Data Retention

Once Azure Sentinel is enabled on your Azure Monitor Log Analytics workspace, every GB of data ingested into the workspace can be retained at no charge for the first 90 days. Retention beyond 90 days will be charged per the standard Azure Monitor Log Analytics retention prices.

Advanced multistage attack detection in Azure Sentinel

- Anomalous login leading to O365 mailbox exfiltration
- Anomalous login leading to suspicious cloud app administrative activity
- Anomalous login leading to mass file deletion
- Anomalous login leading to mass file download
- Anomalous login leading to O365 impersonation
- Anomalous login leading to mass file sharing
- Anomalous login leading to ransomware in cloud app

On-board Azure Sentinel

To on-board Azure Sentinel, you first need to enable Azure Sentinel, and then connect your data sources. Azure Sentinel comes with a number of connectors for Microsoft solutions, you'll need to create a new Log Analytics-based workspace. If you have any existing ones, you can choose to use one of those, or just create a new empty one.

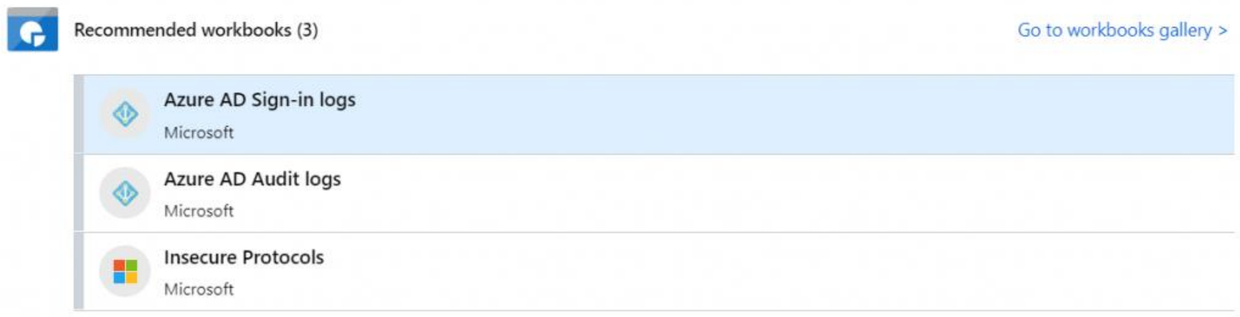
Global prerequisites

- Active Azure Subscription
- Log Analytics workspace.
- Contributor permissions

Connect data sources

- **Machines and virtual machines:** you can install the Azure Sentinel agent that collects the logs and forwards them to Azure Sentinel.
- **Firewalls and proxies:** Azure Sentinel utilizes a Linux Syslog server. The agent is installed on it and from which the agent collects the log files and forwards them to Azure Sentinel.

Once a connector has been configured, you can click on *Next steps* to see additional guidance on how to best utilize the connector. For Azure Active Directory, the options include additional workbooks, and a few query samples using Log Analytics' query language, KQL (also sometimes known as Kusto).



Recommended workbooks (3)

Go to workbooks gallery >

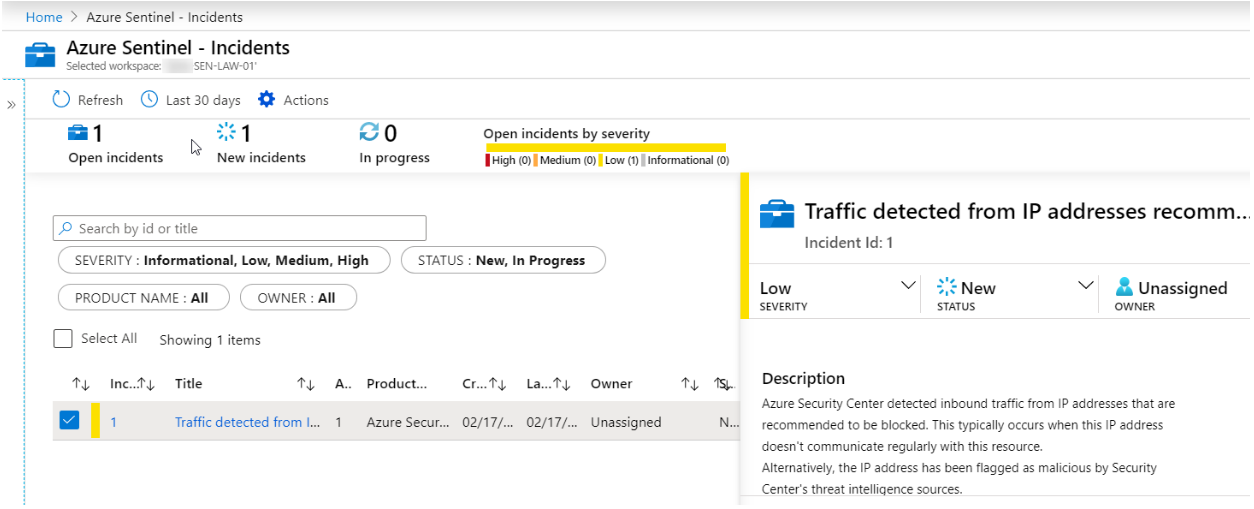
Azure AD Sign-in logs
Microsoft

Azure AD Audit logs
Microsoft

Insecure Protocols
Microsoft

Azure Sentinel: Incidents

Azure Sentinel can collect data from all sorts of data sources, like the Azure Security Center, Azure Active Directory, Office 365, Amazon Web Services, CyberArk and more. It can detect incidents in the data from those data sources and alert you that something needs your attention. Once an accident occurs, you can choose to launch the Azure Sentinel Playbook, a logical application that begins the automatic mitigation process.



Home > Azure Sentinel - Incidents

Azure Sentinel - Incidents

Selected workspace: [redacted] SEN-LAW-01'

1 Open incidents

1 New incidents

0 In progress

Open incidents by severity

High (0) | Medium (0) | Low (1) | Informational (0)

SEVERITY : **Informational, Low, Medium, High**

STATUS : **New, In Progress**

PRODUCT NAME : **All**

OWNER : **All**

□ Select All   Showing 1 items

	Inc...↑↓	Title	↑↓	A..	Product...	Cr...↑↓	La...↑↓	Owner	↑↓	⇅...
☑	1	Traffic detected from I...		1	Azure Secur...	02/17/...	02/17/...	Unassigned		N...

Traffic detected from IP addresses recomm...

Incident Id: 1

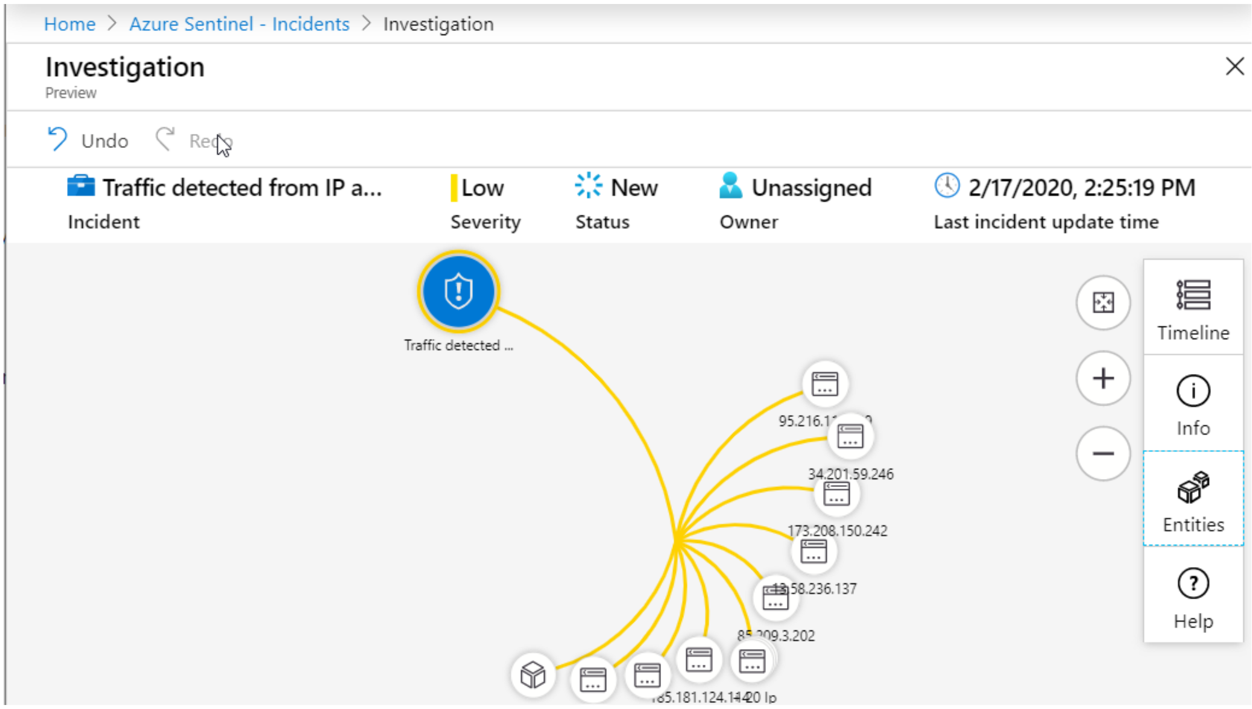
Low
SEVERITY

New
STATUS

Unassigned
OWNER

Description

Azure Security Center detected inbound traffic from IP addresses that are recommended to be blocked. This typically occurs when this IP address doesn't communicate regularly with this resource.
Alternatively, the IP address has been flagged as malicious by Security Center's threat intelligence sources.



Home > Azure Sentinel - Incidents > Investigation

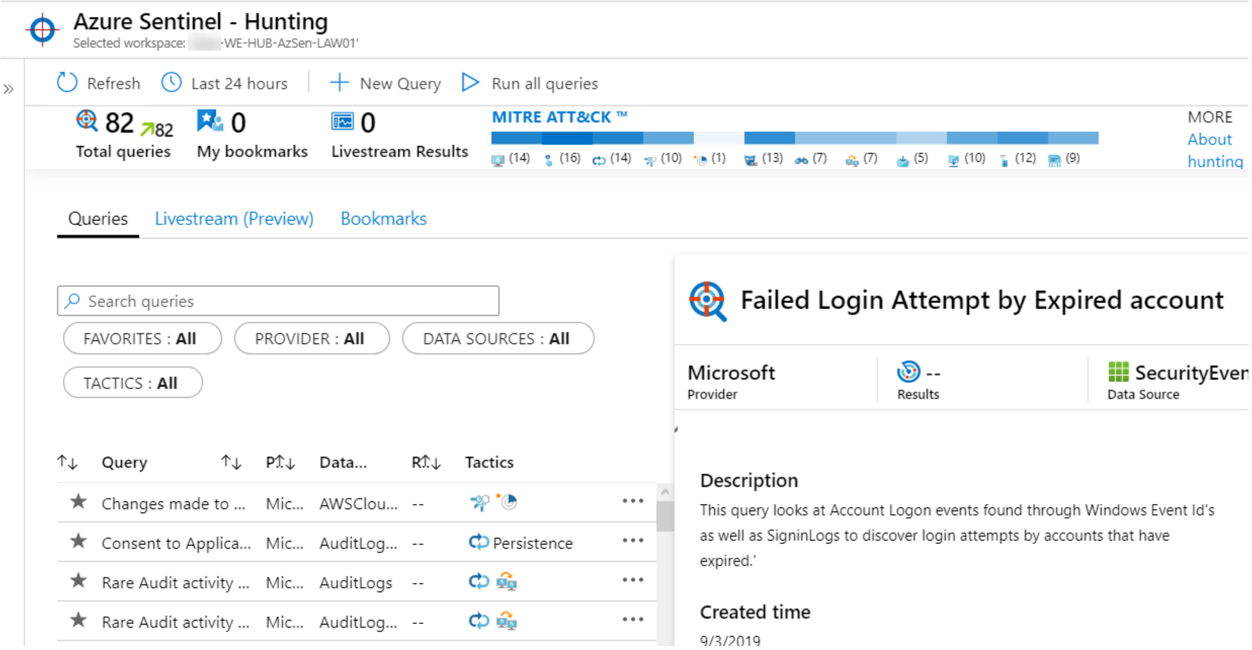
Investigation

Preview

Traffic detected from IP a...	Low	New	Unassigned	2/17/2020, 2:25:19 PM
Incident	Severity	Status	Owner	Last incident update time

Azure Sentinel: Hunting

Hunting in this context means that investigators run queries, investigate and use playbooks (known as notebooks in Azure Sentinel lingo) to proactively look for security threats.



Azure Sentinel - Hunting

Selected workspace: '[redacted]-WE-HUB-AzSen-LAW01'

82 ↗82 Total queries

0 My bookmarks

0 Livestream Results

FAVORITES : **All** PROVIDER : **All** DATA SOURCES : **All** TACTICS : **All**

↑↓	Query ↑↓	P↑↓	Data...	R↑↓	Tactics
★	Changes made to ...	Mic...	AWSClou...	--	
★	Consent to Applica...	Mic...	AuditLog...	--	Persistence
★	Rare Audit activity ...	Mic...	AuditLogs	--	
★	Rare Audit activity ...	Mic...	AuditLog...	--	

Failed Login Attempt by Expired account

Microsoft Provider | -- Results | SecurityEven Data Source

Description

This query looks at Account Logon events found through Windows Event Id's as well as SigninLogs to discover login attempts by accounts that have expired.'

Created time

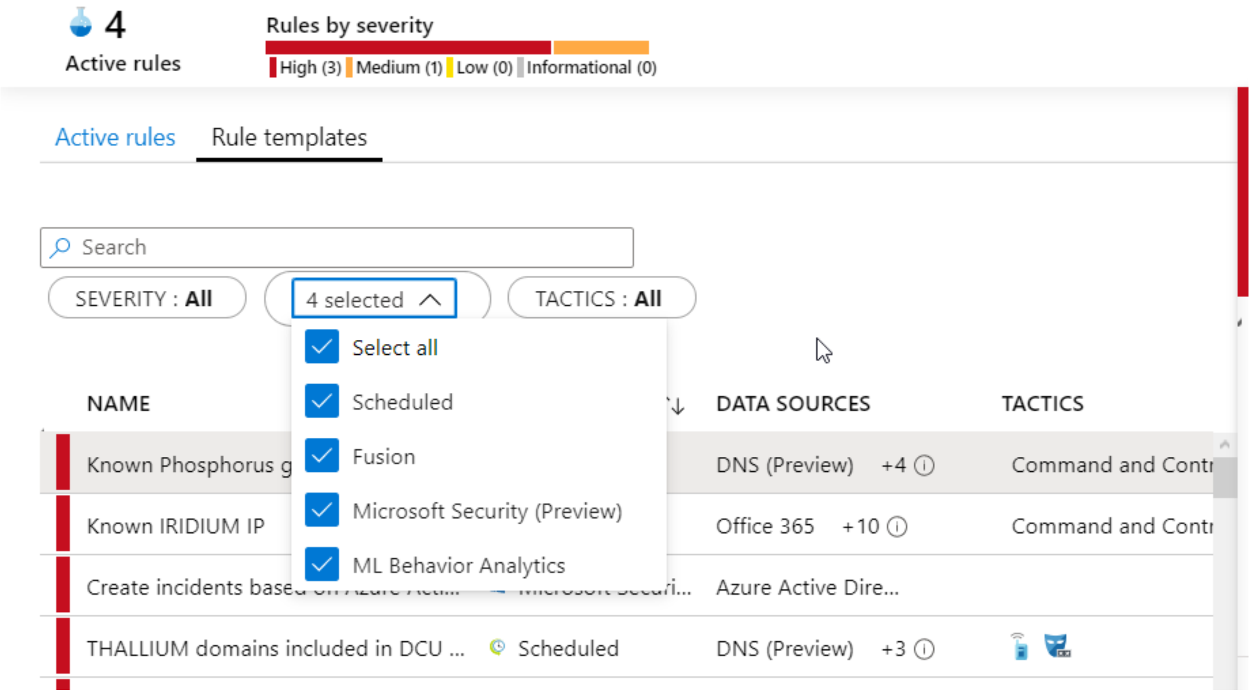
9/3/2019

Azure Sentinel: Detecting threats

After you connected your data sources to Azure Sentinel, you want to be notified when something suspicious happens. To enable you to do this, Azure Sentinel provides you with out-of-the-box built-in templates.

- Use out-of-the-box detections
- Automate threat responses

You can choose between Azure Security Center, Cloud App Security, Azure ATP, and Azure AD Identity Protection.



SEVERITY : **All**

4 selected

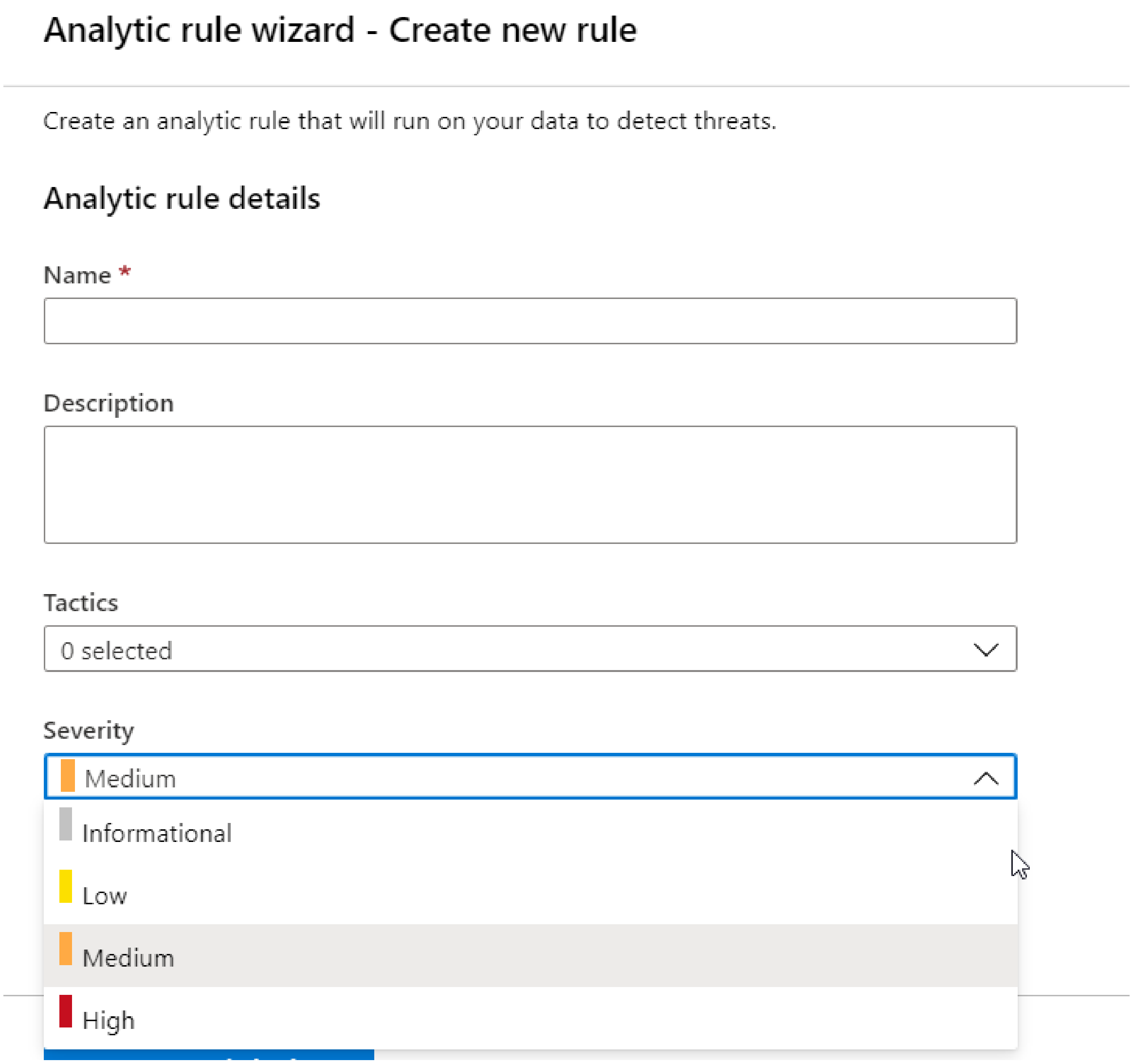
TACTICS : **All**

☑ Select all
☑ Scheduled
☑ Fusion
☑ Microsoft Security (Preview)
☑ ML Behavior Analytics

NAME		DATA SOURCES	TACTICS
Known Phosphorus g		DNS (Preview) +4 ⓘ	Command and Contr
Known IRIDIUM IP		Office 365 +10 ⓘ	Command and Contr
Create incidents based on Azure Acti...	Microsoft Securi...	Azure Active Dire...	
THALLIUM domains included in DCU ...	Scheduled	DNS (Preview) +3 ⓘ	

If you want more freedom, use ***Scheduled query rule*** when creating the rule. This will allow you to select which tactics to watch for, and what severity level we're interested in.

To build your detection rules, click *Azure Sentinel > Analytics*. Click **+ Create** to add a new rule.



Analytic rule wizard - Create new rule

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

Analytic rule details

Name *

Description

Tactics

0 selected

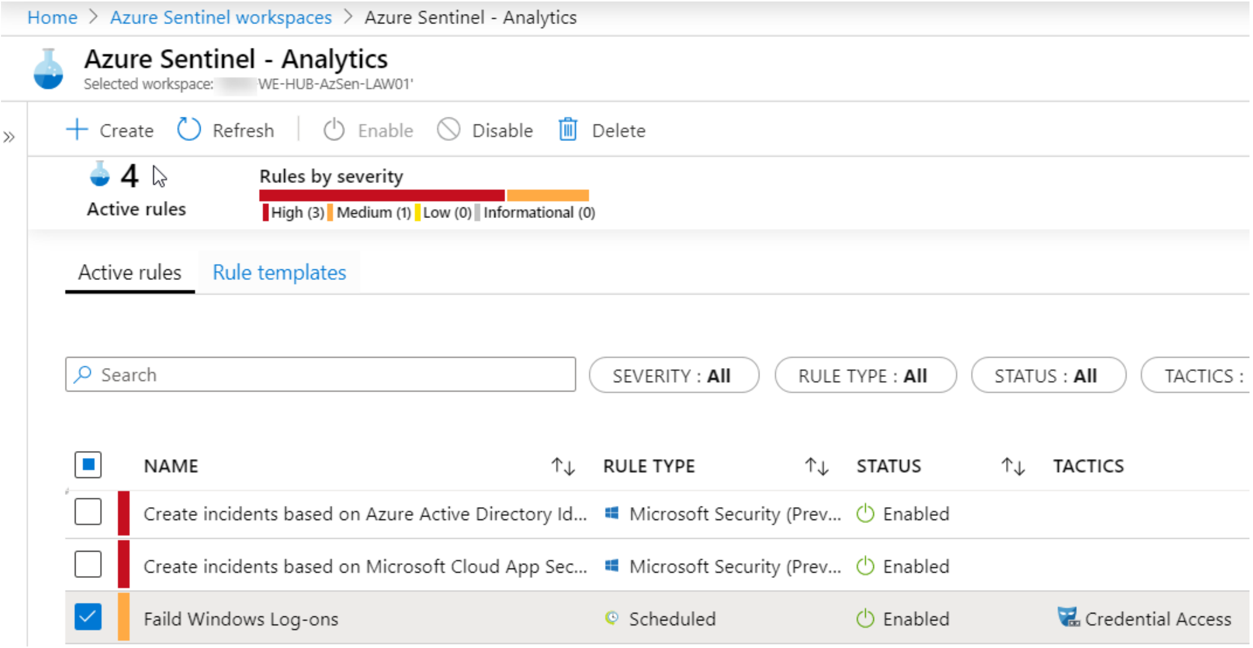
Severity

Medium

With the use of ***Scheduled query rule*** *you have to create a custom query, and set your scheduling as well as alerts threshold.*

Also, you can execute a playbook based on the triggered alert.

Azure Sentinel - Analytic rule



Azure Sentinel - Analytics

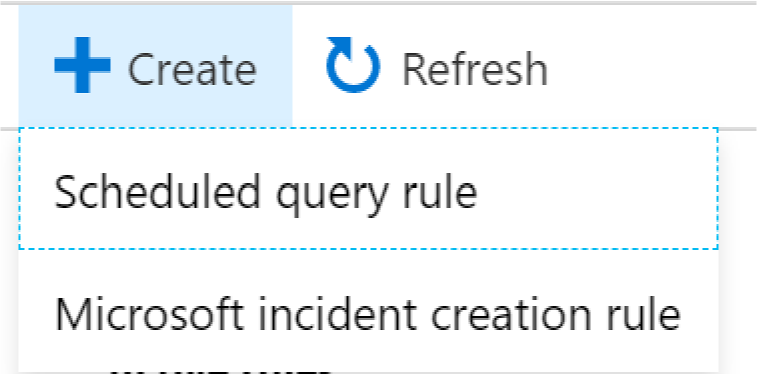
Selected workspace: [redacted] WE-HUB-AzSen-LAW01'

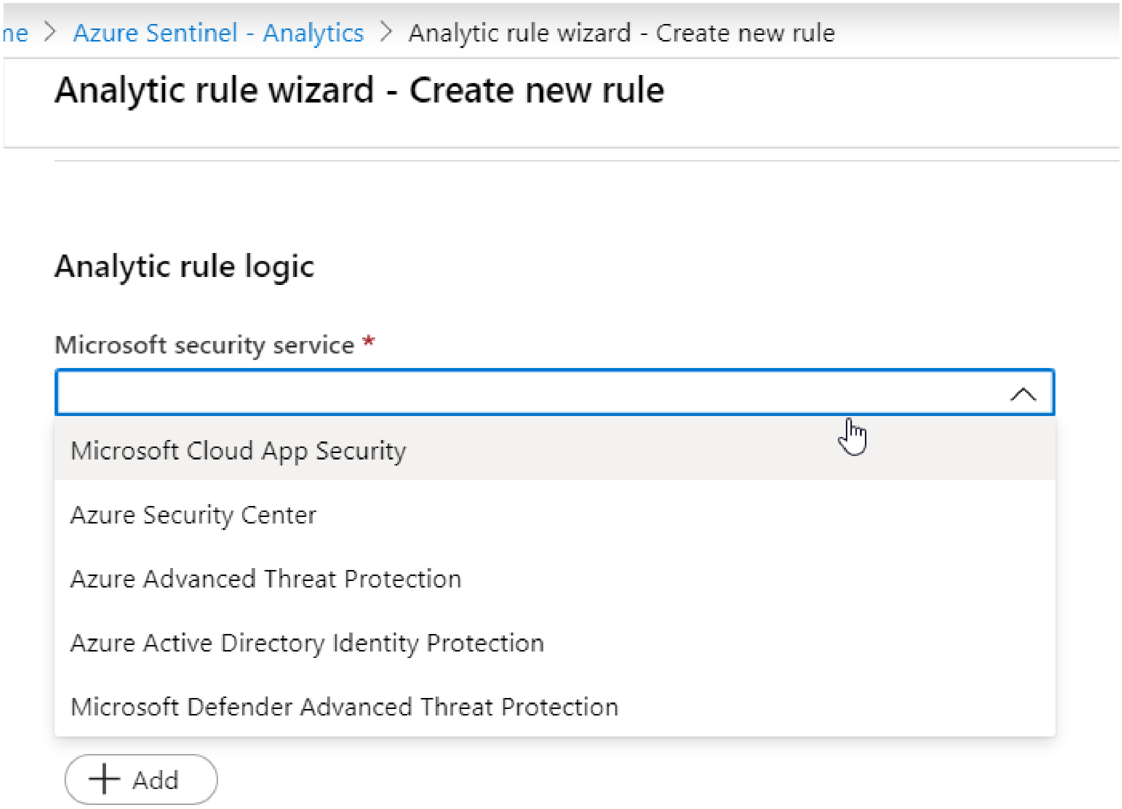
4 Active rules

Rules by severity: High (3) | Medium (1) | Low (0) | Informational (0)

☐	NAME	RULE TYPE	STATUS	TACTICS
☐	Create incidents based on Azure Active Directory Id...	Microsoft Security (Prev...	Enabled	
☐	Create incidents based on Microsoft Cloud App Sec...	Microsoft Security (Prev...	Enabled	
☑	Faild Windows Log-ons	Scheduled	Enabled	Credential Access

You can create a rule based on a scheduled query (using the query language in Log Analytics), or use a pre-defined service-triggered rule – such as an alert from Azure Security Center. I'll choose the latter – *Microsoft incident creation rule* – as it's a bit more explanatory to what happens when detecting a threat.





ne > Azure Sentinel - Analytics > Analytic rule wizard - Create new rule

Analytic rule wizard - Create new rule

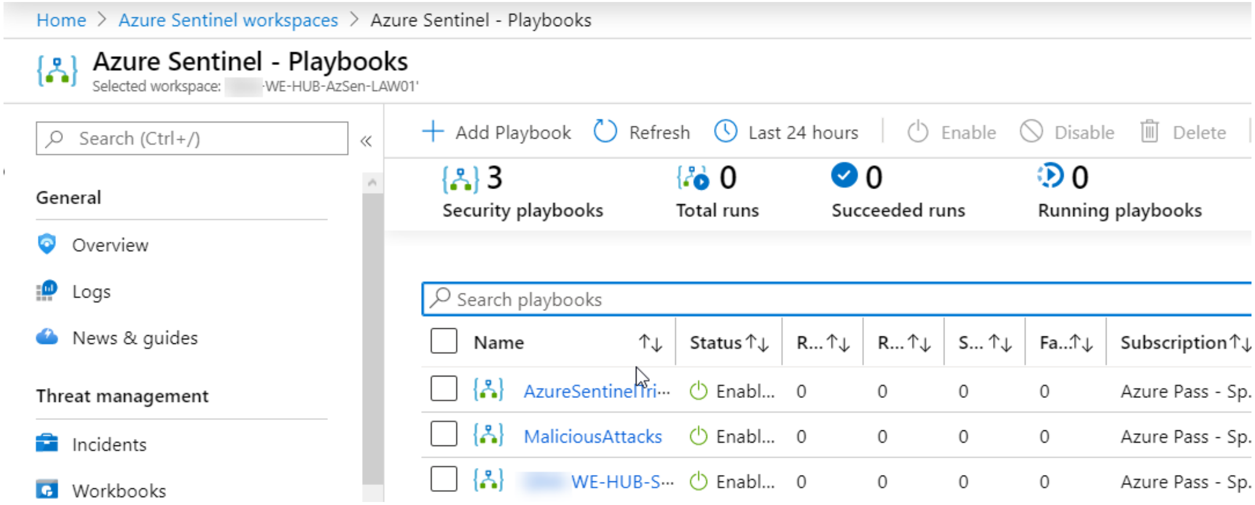
Analytic rule logic

Microsoft security service *

- Microsoft Cloud App Security
- Azure Security Center
- Azure Advanced Threat Protection
- Azure Active Directory Identity Protection
- Microsoft Defender Advanced Threat Protection

Azure Sentinel: Playbooks

After creating your detection rules and alerts, now it’s time to start creating your playbooks constructing logic app workflows. Also, you would be able to create an automated response to those detected threads.



Home > Azure Sentinel workspaces > Azure Sentinel - Playbooks

Azure Sentinel - Playbooks

Selected workspace: '[redacted]-WE-HUB-AzSen-LAW01'

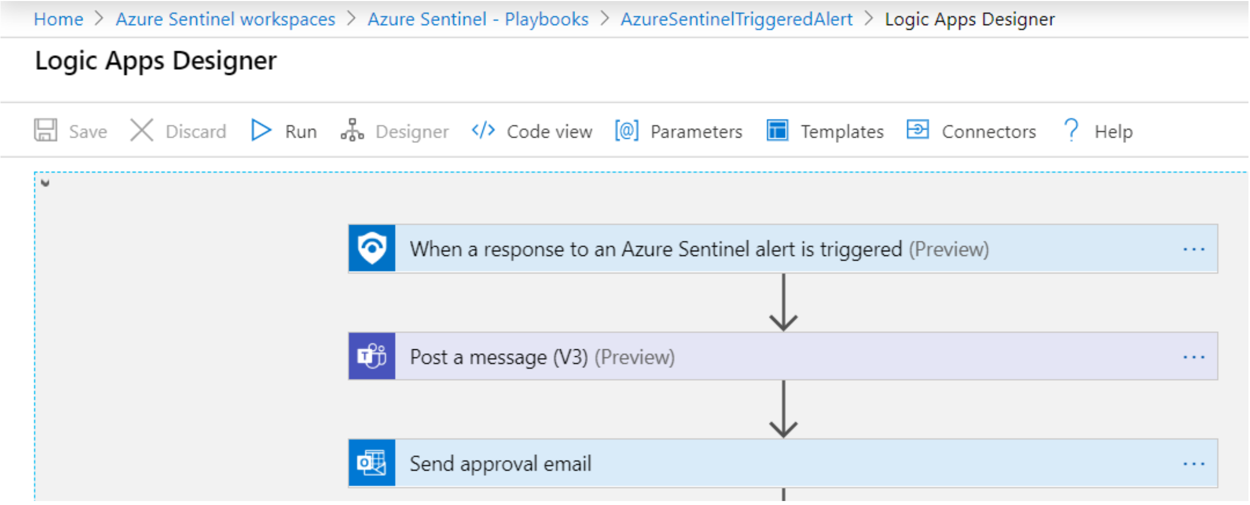
3 Security playbooks

0 Total runs

0 Succeeded runs

0 Running playbooks

□	Name ↑↓	Status ↑↓	R... ↑↓	R... ↑↓	S... ↑↓	Fa... ↑↓	Subscription ↑↓
□	AzureSentinelTri...	Enabl...	0	0	0	0	Azure Pass - Sp.
□	MaliciousAttacks	Enabl...	0	0	0	0	Azure Pass - Sp.
□	[redacted]WE-HUB-S...	Enabl...	0	0	0	0	Azure Pass - Sp.


Home > Azure Sentinel workspaces > Azure Sentinel - Playbooks > AzureSentinelTriggeredAlert > Logic Apps Designer
Save
Discard
Run
Designer
Code view
Parameters
Templates
Connectors
Help

Logic Apps Designer

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

Post a message (V3) (Preview)

Send approval email

Azure Sentinel – Workbooks Templates:

- AWS Network Activities
- AWS User Activities
- Azure Activity
- Azure AD Audit logs
- Azure AD Sign-in logs
- Azure Firewall
- Azure Information Protection
- Azure Network Watcher
- Check Point Software Technologies
- Cisco
- CyberArk Privileged Access Security
- DNS
- Exchange Online
- F5 BIG-IP ASM F5
- FortiGate
- Identity & Access
- Insecure Protocols
- Juniper
- Linux machines
- Microsoft Web Application Firewall (WAF)
- Office 365
- Palo Alto Networks
- Palo Alto Networks Threat
- SharePoint & OneDrive
- Symantec File Threats
- Symantec Security
- Symantec Threats
- Symantec URL Threats
- Threat Intelligence
- VM insights