Azure Sentinel: 5-day Proof of Concept

What is Azure Sentinel?

Microsoft Sentinel or Azure Sentinel is a scalable, cloud-native, **security information and event management (SIEM)** and **security orchestration, automation, and response (SOAR)** solution. Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for attack detection, threat visibility, proactive hunting, and threat response.

Microsoft Sentinel is your birds-eye view across the enterprise alleviating the stress of increasingly sophisticated attacks, increasing volumes of alerts, and long resolution time frames.

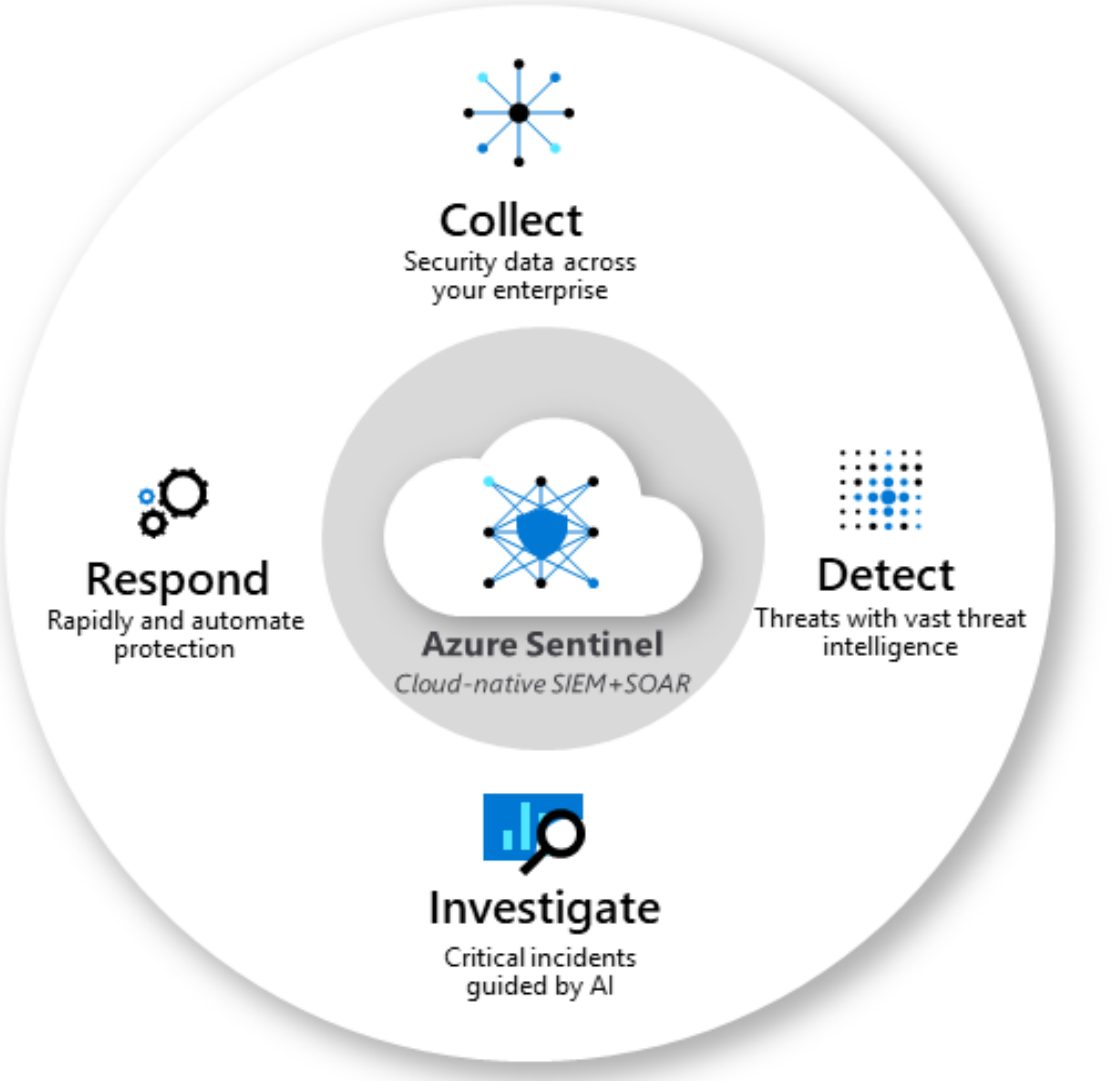
Features: -

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

2. **Detect previously undetected threats** and minimize false positives using Microsoft's analytics and unparalleled threat intelligence.

3. **Investigate threats with artificial intelligence**, and hunt for suspicious activities at scale, tapping into years of cyber security work at Microsoft.

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



Microsoft Sentinel enriches your investigation and detection with Artificial Intelligence (AI) and provides Microsoft's threat intelligence stream and enables you to bring your own threat intelligence.

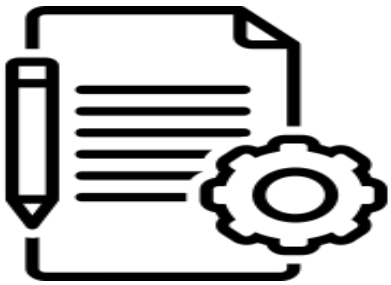
Planning of POC: -

We will help you get started with Azure Sentinel with its Proof of Concept offering and the program running over 5 days. Before deployment we will check prerequisites for the project.

Prerequisites: -

Azure Tenant Requirements: -

1. An Azure Active Directory license and tenant, or an individual account with a valid payment method, are required to access Azure and deploy resources.
2. After you have a tenant, you must have an Azure subscription to track resource creation and billing.
3. After you have a subscription, you will need the relevant permissions to begin using your subscription. If you are using a new subscription, an admin or higher from the AAD tenant should be designated as the owner/contributor for the subscription.
4. To maintain the least privileged access available, assign roles at the level of the resource group.
5. For more control over permissions and access, set up custom roles.
6. For extra separation between users and security users, you might want to use resource-context or table-level RBAC.
7. A Log Analytics workspace is required to house all the data that Microsoft Sentinel will be ingesting and using for its detections, analytics, and other features.



Deployment plan: -

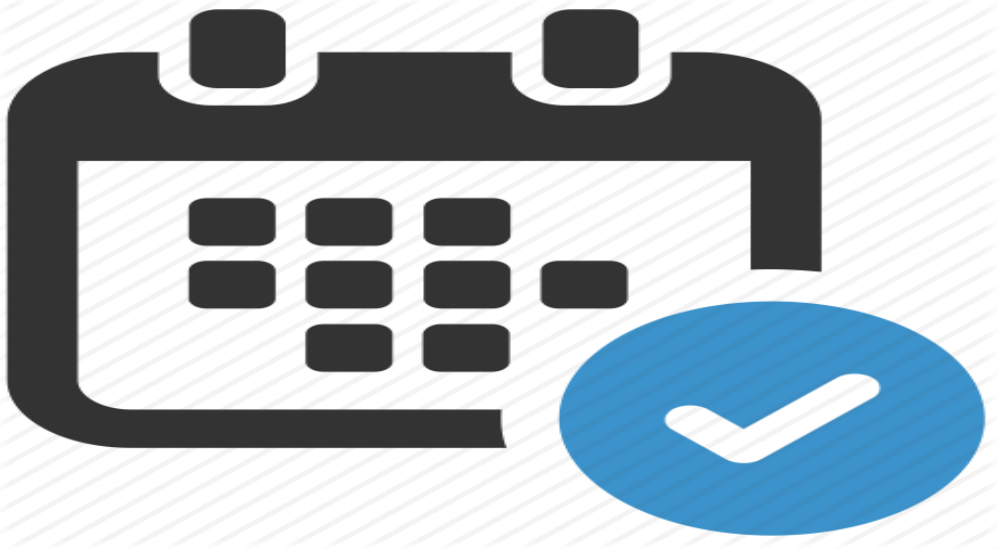
We will be providing deployment plan based on day and activities carried out on that day. In the kick-off meeting we will be finalising the Scope Of Work (SOW) before starting of project.

Day 1: We will help you to integrate with supported sources by deploying sentinel agents or using sentinel data connectors.

Day 2 & Day 3: We will help you to detect threats using Microsoft's analytics and threat intelligence.

Day 4: We will help you to hunt for the malicious threats at scale in your organisation.

Day 5: We will help you to respond to the threat rapidly using built-in orchestration and automation

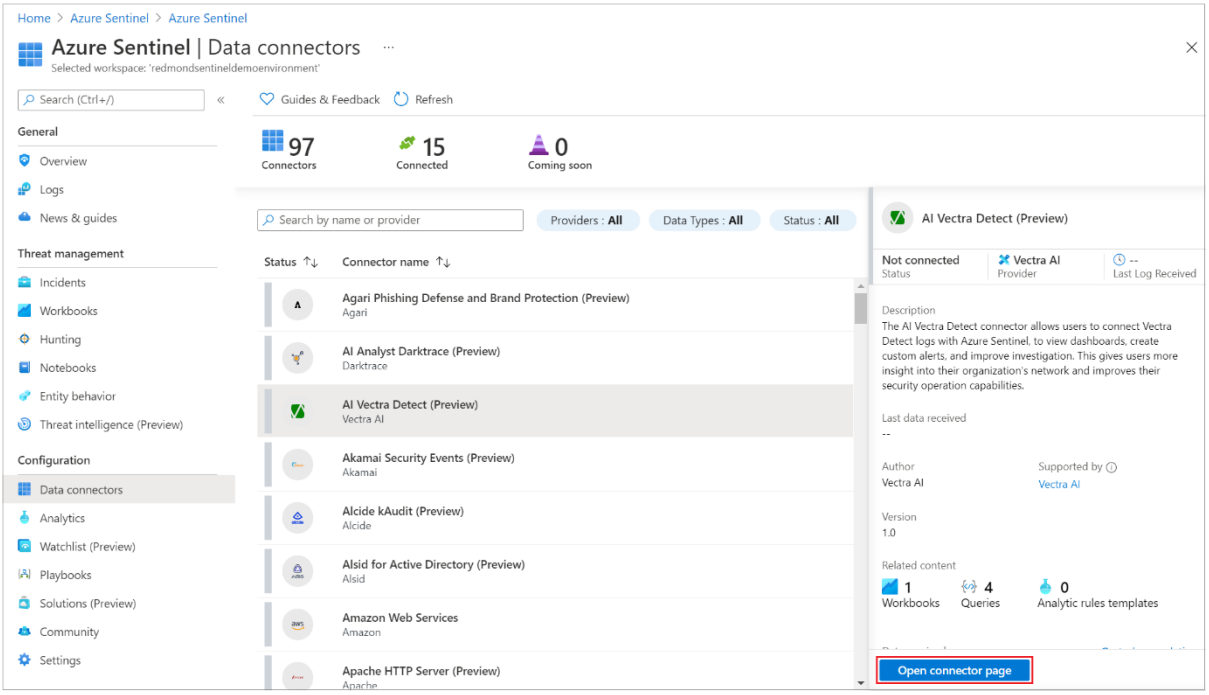


Phases of deployment

Phase 1: Sentinel agents and sentinel data connectors

Data connectors: Microsoft Sentinel comes with several connectors for Microsoft solutions, available out of the box and providing real-time integration, including Microsoft 365 Defender (formerly Microsoft Threat

Protection) solutions, and Microsoft 365 sources, including Office 365, Azure AD, Microsoft Defender for Identity (formerly Azure ATP), and Microsoft Defender for Cloud Apps, and more. In addition, there are built-in connectors to the broader security ecosystem for non-Microsoft solutions. You can also use common event format, Syslog or REST-API to connect your data sources with Microsoft Sentinel as well.

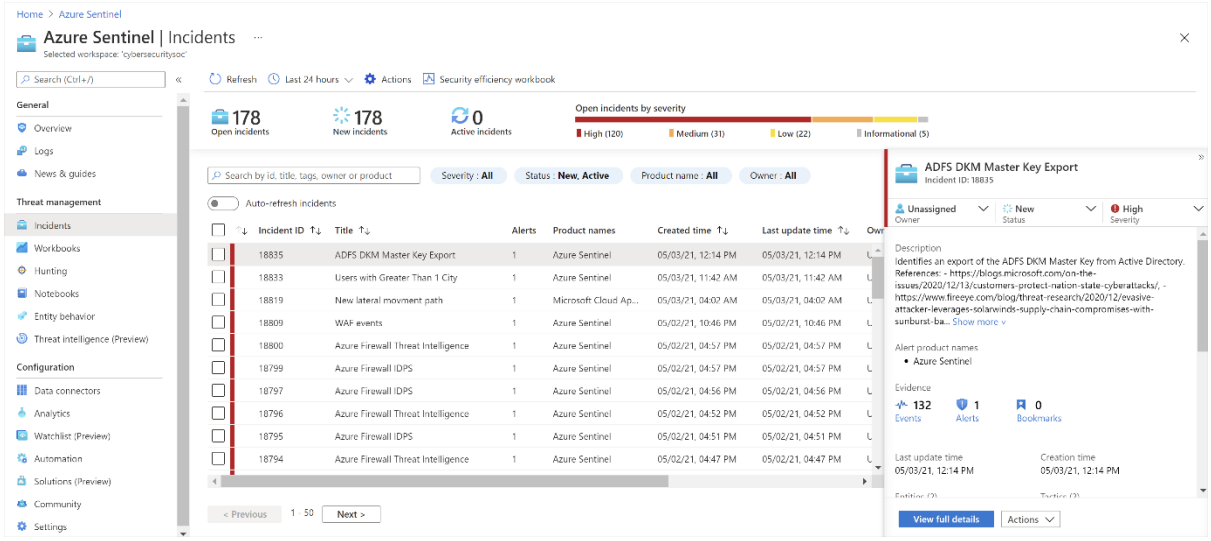


Phase 2: Microsoft Analytics and Threat Intelligence

Analytics:

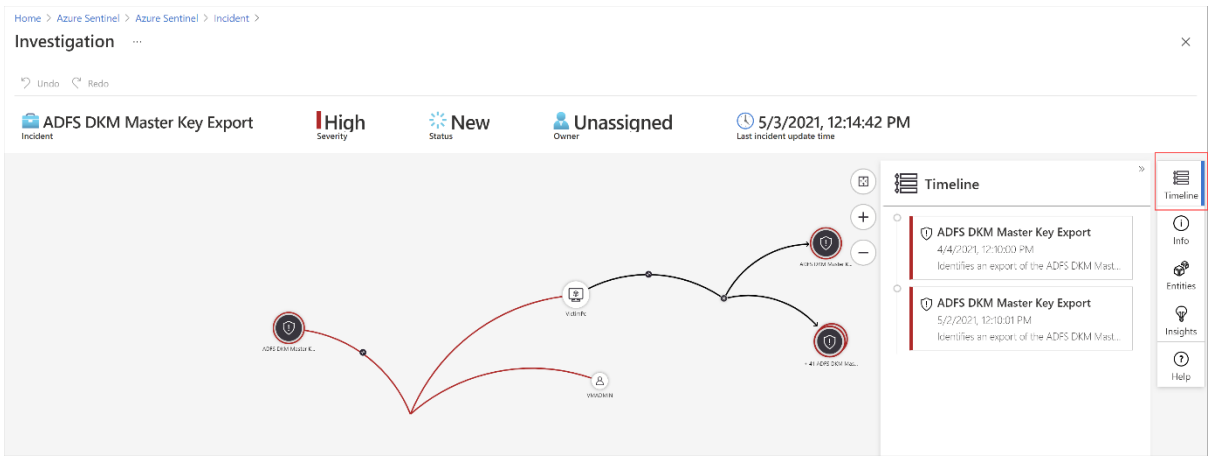
Microsoft Sentinel uses analytics to correlate alerts into **incidents**. These are groups of related alerts that together create an actionable possible threat that you can investigate and resolve. Use the built-in correlation rules as-is or use them as a starting point to build your own.

Microsoft Sentinel also provides machine learning rules to map your network behaviour and then look for anomalies across your resources. These analytics connect the dots, by combining low fidelity alerts about different entities into potential high-fidelity security incidents.



Investigation:

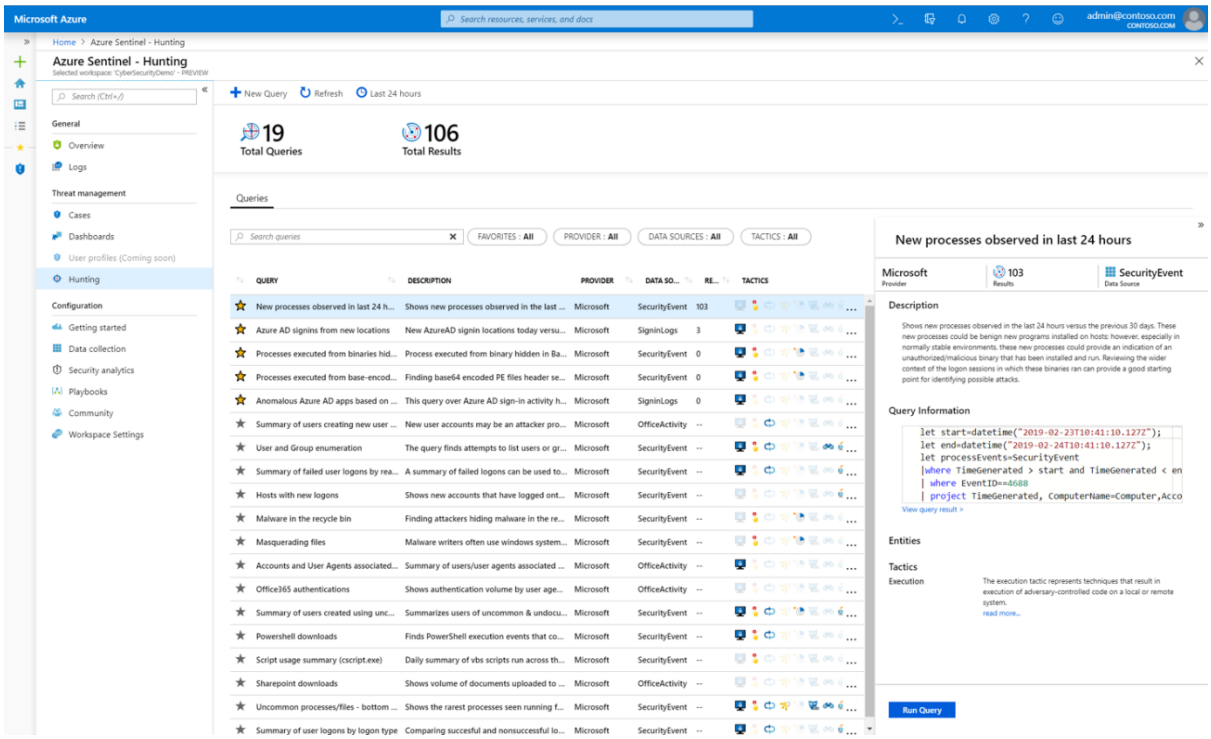
Currently in preview, Microsoft Sentinel deep investigation tools help you to understand the scope and find the root cause, of a potential security threat. You can choose an entity on the interactive graph to ask interesting questions for a specific entity, and drill down into that entity and its connections to get to the root cause of the threat.



Phase 3: Hunting malicious threats in scale

Hunting: Use Microsoft Sentinel's powerful hunting search-and-query tools, based on the MITRE framework, which enable you to proactively hunt for security threats across your organization's data sources, before an alert is

triggered. After you discover which hunting query provides high-value insights into possible attacks, you can also create custom detection rules based on your query and surface those insights as alerts to your security incident responders.

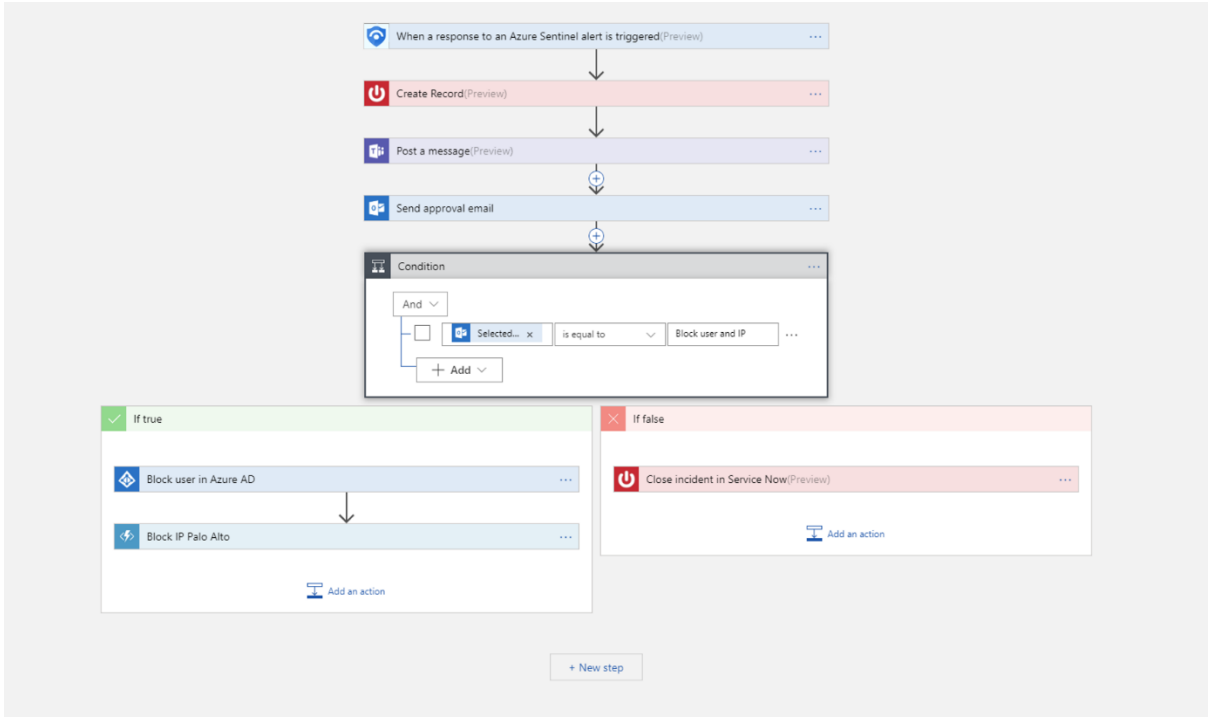


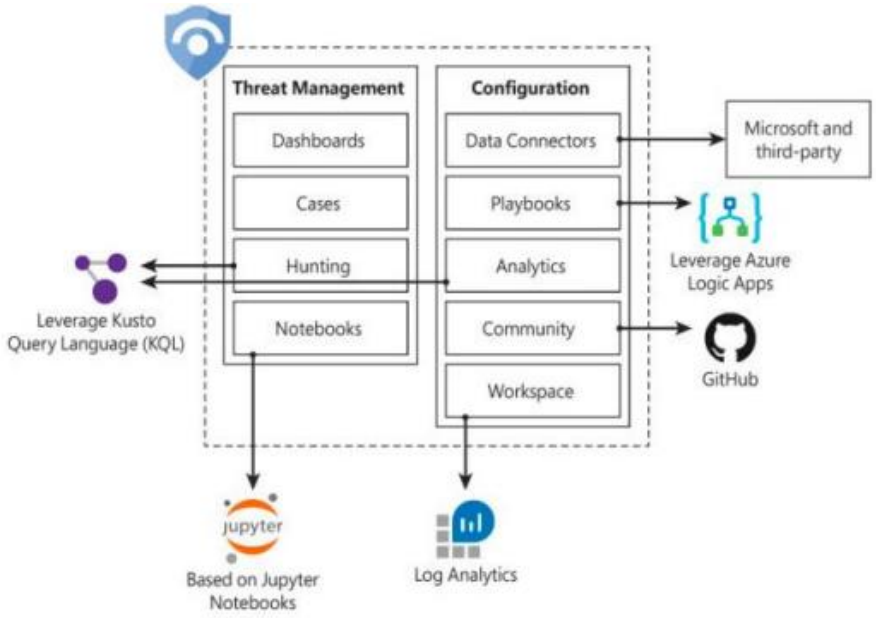
Phase 4: Respond to the threat rapidly using built-in orchestration and automation

Security Automation and Orchestration

Built on the foundation of Azure Logic Apps, Microsoft Sentinel's automation and orchestration solution provides a highly extensible architecture that enables scalable automation as new technologies and threats emerge. To build playbooks with Azure Logic Apps, you can choose from a growing gallery of built-in playbooks.

The connectors allow you to apply any custom logic in code, ServiceNow, Jira, Zendesk, HTTP requests, Microsoft Teams, Slack, Windows Defender ATP, and Defender for Cloud Apps.


When a response to an Azure Sentinel alert is triggered(Preview)
Create Record(Preview)
Post a message(Preview)
Send approval email
Condition
And
Selected...
is equal to
Block user and IP
Add
If true
Block user in Azure AD
Block IP Palo Alto
Add an action
If false
Close incident in Service Now(Preview)
Add an action
+ New step


Threat Management
Dashboards
Cases
Hunting
Notebooks
Configuration
Data Connectors
Playbooks
Analytics
Community
Workspace
Microsoft and third-party
Leverage Azure Logic Apps
GitHub
Leverage Kusto Query Language (KQL)
jupyter
Based on Jupyter Notebooks
Log Analytics