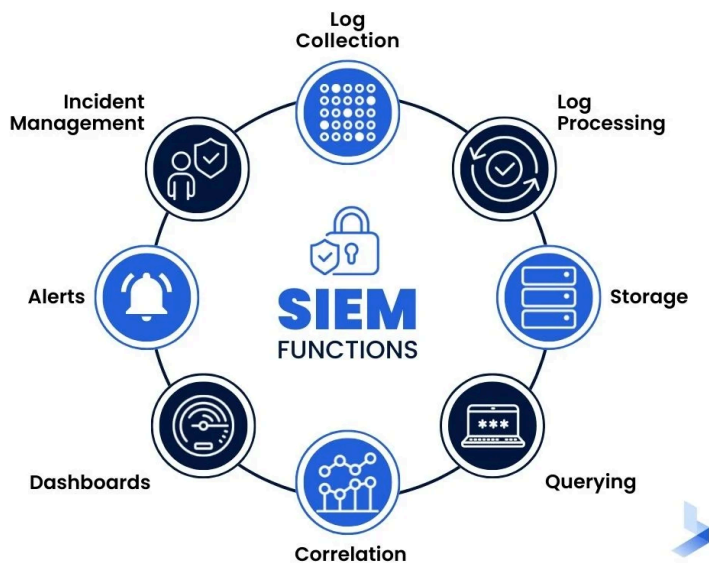


Microsoft Sentinel



- *Microsoft Sentinel* = A cloud-based security system that both detects threats (*SIEM*) and automatically responds to them (*SOAR*).
- *Microsoft Sentinel* = *Collect* → *Detect* → *Investigate* → *Respond* — all in one cloud security platform with the help of AI integration(*copilot*).

1. What Is SIEM?



SIEM = Security Information and Event Management

Think of SIEM as a **central security brain** that collects logs and alerts from everywhere in your network.

Simple Meaning:

- SIEM **collects data** from devices, apps, servers, firewalls, cloud, etc.
- SIEM **analyzes** the data for suspicious behavior.
- SIEM **alerts** you when something is wrong.

SIEM does:

- Collect logs
- Correlate events
- Detect anomalies
- Generate alerts
- Help with investigations

2. What Is SOAR?



SOAR = Security Orchestration, Automation, and Response

Think of SOAR as a **security robot** that helps you respond faster.

Simple Meaning:

- SOAR **automates tasks** (no need to do everything manually).
- SOAR **runs playbooks** to fix issues automatically.
- SOAR **connects different security tools** to respond quickly.

SOAR does:

- Automate repetitive actions
- Run playbooks (scripts + workflows)
- Speed up incident response
- Reduce manual work

3. What Is Microsoft Sentinel?

Microsoft Sentinel = **Cloud-based SIEM + SOAR combined in one tool**

It is a **scalable, cloud-native security platform** that helps SOC teams:

- Collect security data
- Detect threats
- Investigate incidents
- Automate responses

Sentinel Works ?

SIEM part of Sentinel:

- ✓ Collects logs
- ✓ Queries logs with KQL
- ✓ Correlates events
- ✓ Detects anomalies
- ✓ Creates alerts & incidents

SOAR part of Sentinel:

- ✓ Supports playbooks
- ✓ Automates response actions
- ✓ Blocks IPs, disables users, triggers notifications
- ✓ Integrates with many security tools

4.Sentinel's Purpose

Sentinel is a **one-stop security solution** that gives:

1. **Attack detection**
2. **Threat visibility**
3. **Proactive hunting**
4. **Automated response**

4 Pillars of Microsoft Sentinel

1. Collect

Gather logs from on-prem, cloud, applications, networks, and security tools.

2. Detect

Correlate data, find threats, and generate alerts/incidents.

3. Investigate

Use dashboards, KQL, AI-assisted analysis to understand what happened.

4. Respond

Use playbooks, automation, and workflows to contain/fix incidents.

5. Microsoft Sentinel

Sentinel works in **4 phases**.

Everything starts with **logs**.

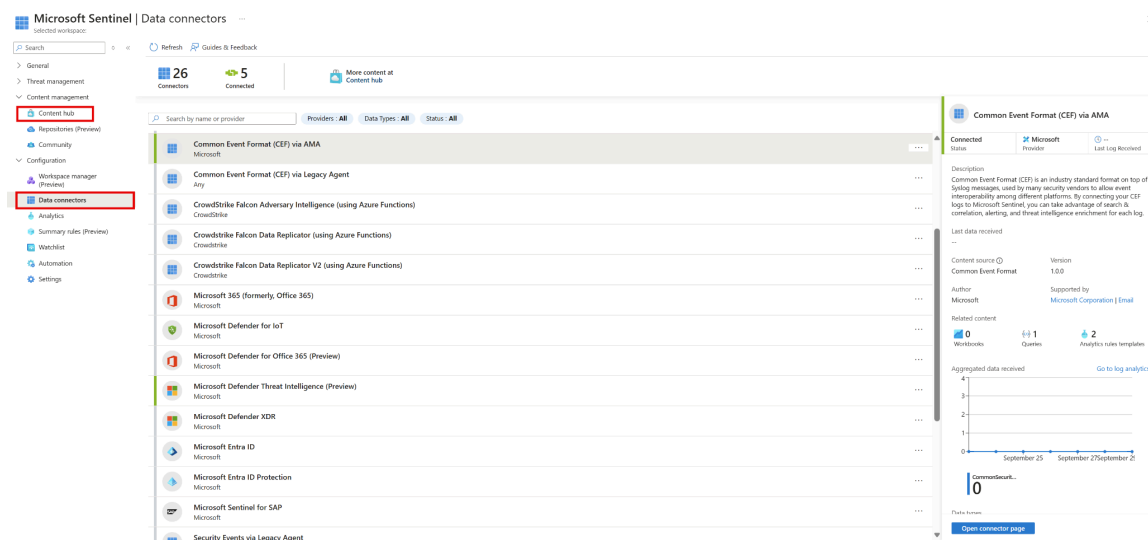
No logs → no detection → no alerts → no response.

Phase 1: Collect (SIEM Part)

Goal: Get visibility into what is happening.

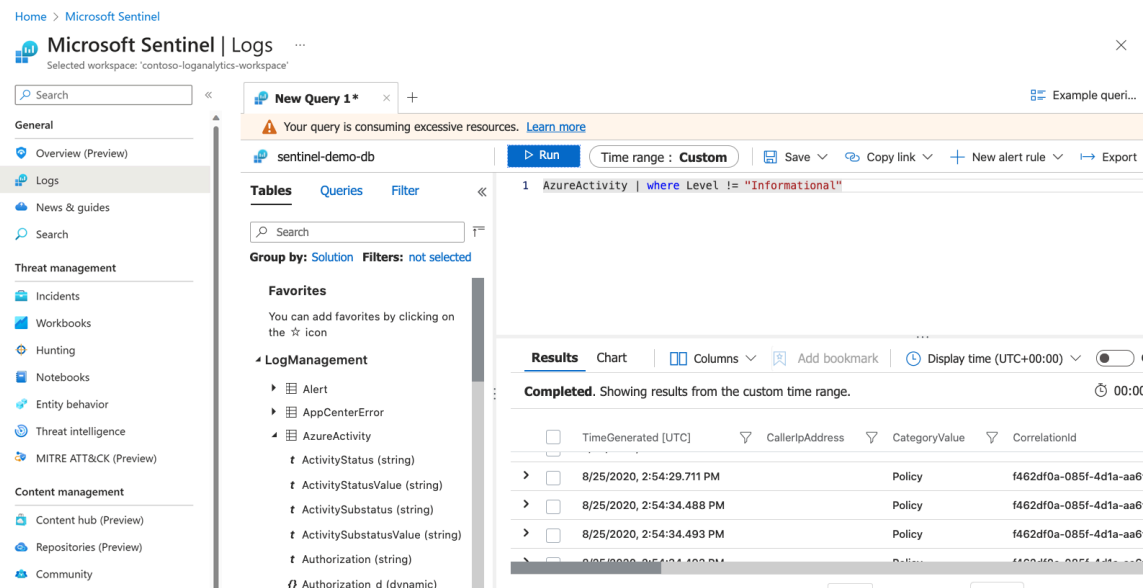
1. Data Connectors

- The first step is to **ingest data** into Microsoft Sentinel. This is exactly what data connectors are for. It collect from various data sources and scenarios.
- Microsoft provides **100+ connectors** (Azure AD, Office 365, Firewalls, Endpoints, AWS, etc.).



2. Log Analytics Workspace

- Once the data has been ingested into Microsoft Sentinel, it must be stored for further **correlation** and **analysis**.
- This log storage mechanism is called **Log Analytics workspaces**.
- Data stored in these workspaces can be queried to gain further insights using **Kusto Query Language (KQL)**.



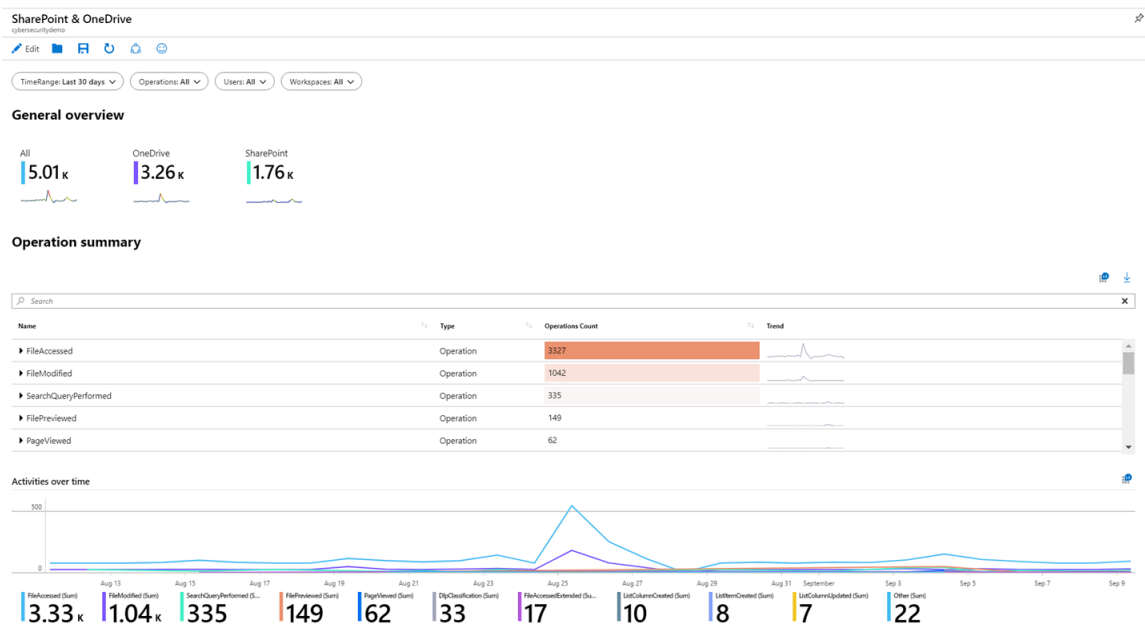
- **Simple Understanding:**
Connect data → Store it → Query it
This gives **visibility** to SOC analysts.

Phase 2: Detect (SIEM + Proactive Hunting)

Goal: Detect threats from collected logs.

1. Workbooks (Dashboards)

- Visual dashboards that show security patterns.
- Useful for **quick threat visibility**, charts, graphs, trends.



2. Analytics Rules

- Rules created to automatically detect suspicious activity.
- These rules turn logs into **alerts and incidents**.
- Example: “Multiple failed logins → Possible brute force attack.”

The screenshot displays the Microsoft Sentinel Analytics workspace. The left sidebar contains navigation links for General, Threat management, Content management, and Configuration. The main area shows a list of active rules under the 'Active rules' tab. A rule titled 'Create incidents based on Azure Defender a...' is selected, and its details are shown on the right.

Rules by severity: High (2), Medium (0), Low (0), Informational (1)

Severity	Name	Rule type	Status	Tactics
High	Create incidents ba...	Microsoft Security	Enabled	
Informational	Ingestion Rule Test	Scheduled	Enabled	Discover
High	Advanced Multista...	Fusion	Enabled	Discover, Investigate

Create incidents based on Azure Defender a...

High Severity | Custom Content Source | Enabled Status

Id: b8da0949-524b-472c-bd02-a9911d4fe9e9

Description: Create incidents based on all alerts generated in Azure Defender

Microsoft security service
Microsoft Defender for Cloud

Filter by severity
Low, Medium, High

Include by alert name(s)
Any

Exclude by alert name(s)
None

Page 1 of 1 | Showing 1 to 3 of 3 results.

3. Threat Hunting

- Instead of waiting for alerts, analysts do **proactive searching**.
- Sentinel has **200+ built-in hunting queries**.
- Helps find hidden threats that rules may miss.

The screenshot shows the Microsoft Sentinel Hunting interface. The top navigation bar includes 'Home > Microsoft Sentinel' and 'Microsoft Sentinel | Hunting'. Below this, there's a search bar and a 'Refresh' button. The main content area displays a summary of 155/211 active queries, 0/0 result count / queries run, 0 livestream results, and 0 my bookmarks. A table of hunting queries is shown, with columns for Query, Content source, Data source, and Results. The first query, 'Changes made to AWS IAM policy', is selected, and its details are shown on the right. The query text is 'AWSCloudTrail | where EventName in~ ('AttachGroupPolicy','. The interface also includes a sidebar with navigation options like General, Threat management, and Content management.

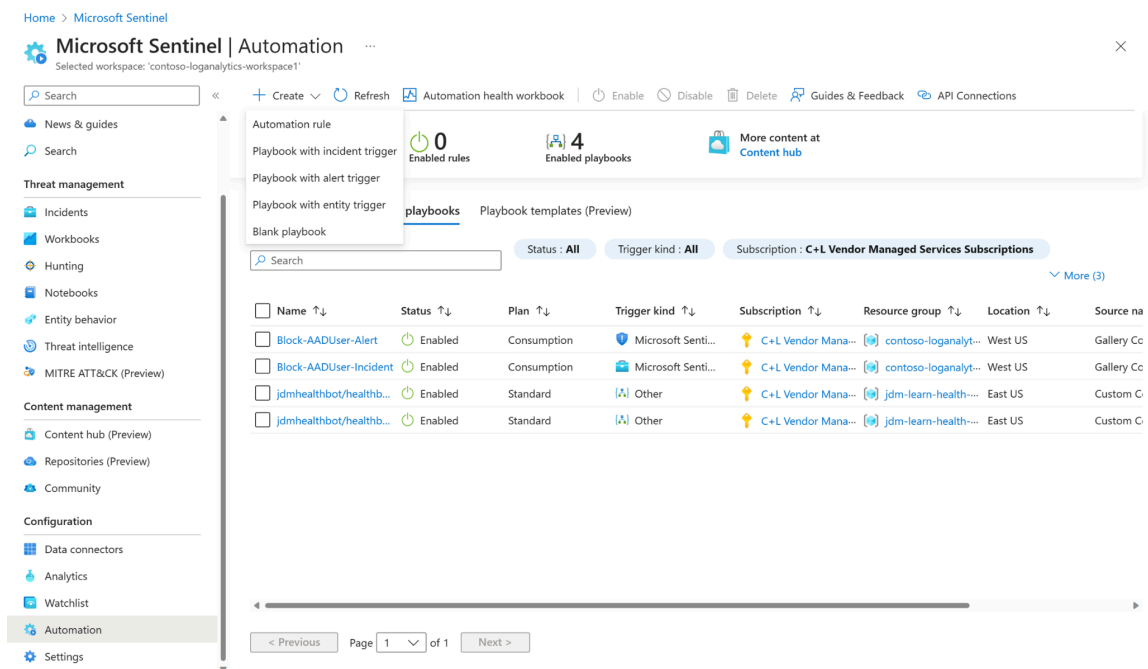
- **Simple Understanding:**
Visualize data → Detect attacks → Hunt hidden threats

Phase 3: Investigate (SOC L1/L2 Work)

Goal: Study alerts, check what happened, and decide next steps.

1. Incidents

- When Analytics rules detect something → **Incidents** are created.
- SOC analysts review incidents to confirm if it's real or false.



The screenshot displays the Microsoft Sentinel Automation interface. The left sidebar contains navigation options: News & guides, Search, Threat management (Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence, MITRE ATT&CK), Content management (Content hub, Repositories, Community), and Configuration (Data connectors, Analytics, Watchlist, Automation, Settings). The main area shows the 'Automation' section with a search bar and a dropdown menu for creating automation rules. Below this, there are statistics for 'Enabled rules' (0) and 'Enabled playbooks' (4). A table lists the enabled playbooks with columns for Name, Status, Plan, Trigger kind, Subscription, Resource group, Location, and Source name.

Name	Status	Plan	Trigger kind	Subscription	Resource group	Location	Source name
Block-AADUser-Alert	Enabled	Consumption	Microsoft Senti...	C+L Vendor Mana--	contoso-loganalyt...	West US	Gallery Co
Block-AADUser-Incident	Enabled	Consumption	Microsoft Senti...	C+L Vendor Mana--	contoso-loganalyt...	West US	Gallery Co
jdmhealthbot/healthb...	Enabled	Standard	Other	C+L Vendor Mana--	jdm-learn-health...	East US	Custom C
jdmhealthbot/healthb...	Enabled	Standard	Other	C+L Vendor Mana--	jdm-learn-health...	East US	Custom C

2. Investigation Process

Analysts usually do:

- Change incident status (New → Active → Closed)
- Assign to other analysts
- View timeline of the attack
- Map entities (user, IP, device, file)
- Use investigation maps to see how the attack happened
- Add comments and notes
- **Simple Understanding:**
Alerts → Incidents → Investigation → Decision

Phase 4: Respond (SOAR Part)

Goal: Reduce workload + automate actions.

! Problem: Alert Fatigue

- SOC teams get **too many alerts**.
- They get tired, slow, or miss real threats.
- Automation is needed.

1. Playbooks (Automated Response)

Playbooks = automated workflows

(Example: **If incident is created → Send email → Block IP → Notify SOC**)

Playbooks can automate:

- Incident updates
- Threat intelligence enrichment
- Investigation steps
- Remediation actions (disable user, delete email, block IP)
- **Simple Understanding:**
Automation saves time → Fix issues faster → Reduce alert load

6. When Should You Use Microsoft Sentinel?

- Use Microsoft Sentinel when you need to **monitor cloud + on-premise environments** for security threats **from one single place**.
- Many tools can monitor security, but **Sentinel stands out** because it gives a **360-degree bird's-eye view** and lets SOC teams do almost everything from one dashboard.

7. What Does Sentinel Help With?

Microsoft Sentinel helps SOC teams:

-  **Visualize log data**
-  **Detect anomalies / suspicious behavior**
-  **Do threat hunting**
-  **Investigate incidents**
-  **Automate responses** using playbooks

In short: **Collect → Detect → Investigate → Respond** from one tool.

8. Why Choose Microsoft Sentinel?

Choose Sentinel if the organization wants to:

✓ **Collect data from many different sources**

(Azure, Office 365, AWS, firewalls, endpoints, servers, etc.)

✓ **Find suspicious activity using built-in analytics and ML**

✓ **Run complete SOC operations without managing servers**

9. Key Extra Benefits of Sentinel

1. Cloud-native SIEM

No servers to deploy → automatically scalable.

2. Built-in & easy integrations

100+ data connectors → Azure services integrate instantly.

3. Automated incident response

Playbooks can block IPs, disable users, send alerts.

4. Advanced threat detection

Uses Microsoft global threat intelligence + machine learning.

5. Supports hybrid & multi-cloud

Azure + AWS + GCP + On-prem → all can be monitored.

AZURE -SIEM

COLLECT- data connector

**Microsoft Sentinel** | Data connectors

Selected workspace: 'cybersecuritysoc'

[Refresh](#) [Guides & Feedback](#)

News & guides

Search

Threat management

Incidents

Workbooks

Hunting

Notebooks

Entity behavior

Threat intelligence

MITRE ATT&CK (Preview)

Content management

Content hub

Repositories (Preview)

Community

Configuration

Workspace manager (Preview)

Data connectors

Analytics

Azure Active Directory (Azure AD) is now Microsoft Entra ID. [Learn more](#)

**190**
Onboarded Connectors

**38**
Connected

**0**
Updates

 More content at
[Content hub](#)

Providers : **Microsoft** Data Types : **All**

Status : **All**

Status	Connect...	Content Source	Updates
	Azure Act... Microsoft	Solution Azure Activity	
	Azure Bat... Microsoft	Solution Azure Batch Account	
	Azure Co... Microsoft	Solution Azure Cognitive Search	
	Azure Dat... Microsoft	Solution Azure Data Lake Storage Gen1	
	Azure DD... Microsoft	Solution Azure DDoS Protection	

Detect threats

Microsoft Azure

Search resources, services, and docs (G+V)

Copilot

Home > Microsoft Sentinel > Microsoft Sentinel

Microsoft Sentinel | MITRE ATT&CK (Preview)

Selected workspace: 'cybersecuritysoc'

Search

Search by technique...

Matrices type view: 13 selected

Sentinel detections: All

Active

Active scheduled query...

Simulated

Select options

General

Overview (Preview)

Logs

News & guides

Search

Threat management

Incidents

Workbooks

Hunting

Notebooks

Entity behavior

Threat intelligence

MITRE ATT&CK (Preview)

Content management

Content hub

Repositories (Preview)

Community

Configuration

Workspace manager (Preview)

Data connectors

Analytics

Watchlist

Automation

Settings

Legend

0 1-5 6-10 11+

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
10 techniques	8 techniques	9 techniques	14 techniques	19 techniques	13 techniques	42 techniques	17 techniques	31 techniques
1 Active Scanning	Acquire Access	3 Drive-by Compromise	11 Command and Scripting...	30 Account Manipulation	5 Abuse Elevation Control...	2 Abuse Elevation Control...	1 Man-in-the-Middle	5 Account Discovery
Gather Victim Host...	Acquire Infrastructure	20 Exploit Public-Facing...	8 Exploitation for Client Execution	1 BITS Jobs	1 Access Token Manipulation	1 Access Token Manipulation	21 Brute Force	Application Window...
Gather Victim Identity...	Compromise Accounts	5 External Remote Services	1 Inter-Process Communication	1 Boot or Logon Autostart...	1 Boot or Logon Autostart...	1 BITS Jobs	Credentials from Password Stores	Browser Bookmark...
Gather Victim Network...	Compromise Infrastructure	1 Hardware Additions	Native API	1 Boot or Logon Initialization...	1 Boot or Logon Initialization...	1 Debugger Evasion	1 Exploitation for Credential...	Debugger Evasion
Gather Victim Org Information	Develop Capabilities	10 Phishing	Scheduled Task/job	Browser Extensions	2 Create or Modify System...	4 Declofuscate/De code Files or...	Forced Authentication	Device Driver Discovery
Phishing for Information	Establish Accounts	1 Replication Through...	Shared Modules	2 Compromise Client Software...	4 Domain Policy Modification	1 Direct Volume Access	Forge Web Credentials	Domain Trust Discovery
Search Closed Sources	Obtain Capabilities	4 Supply Chain Compromise	1 Software Deployment...	7 Create Account	1 Escape to Host	1 Domain Policy Modification	Input Capture	File and Directory...
		1	2	2	1		1	

Brute Force ID T1110

21 Sentinel Detections

0 Incidents

51 Alerts

Description

Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism. Brute forcing passwords can take place via interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes.

View full technique details on the official MITRE ATT&CK site >

Tactic

Credential Access

Incidents and alerts

Last 24 hours

8

6

4

2

0

May 2 May 3

SecurityAlert (51)

SecurityIncident (0)

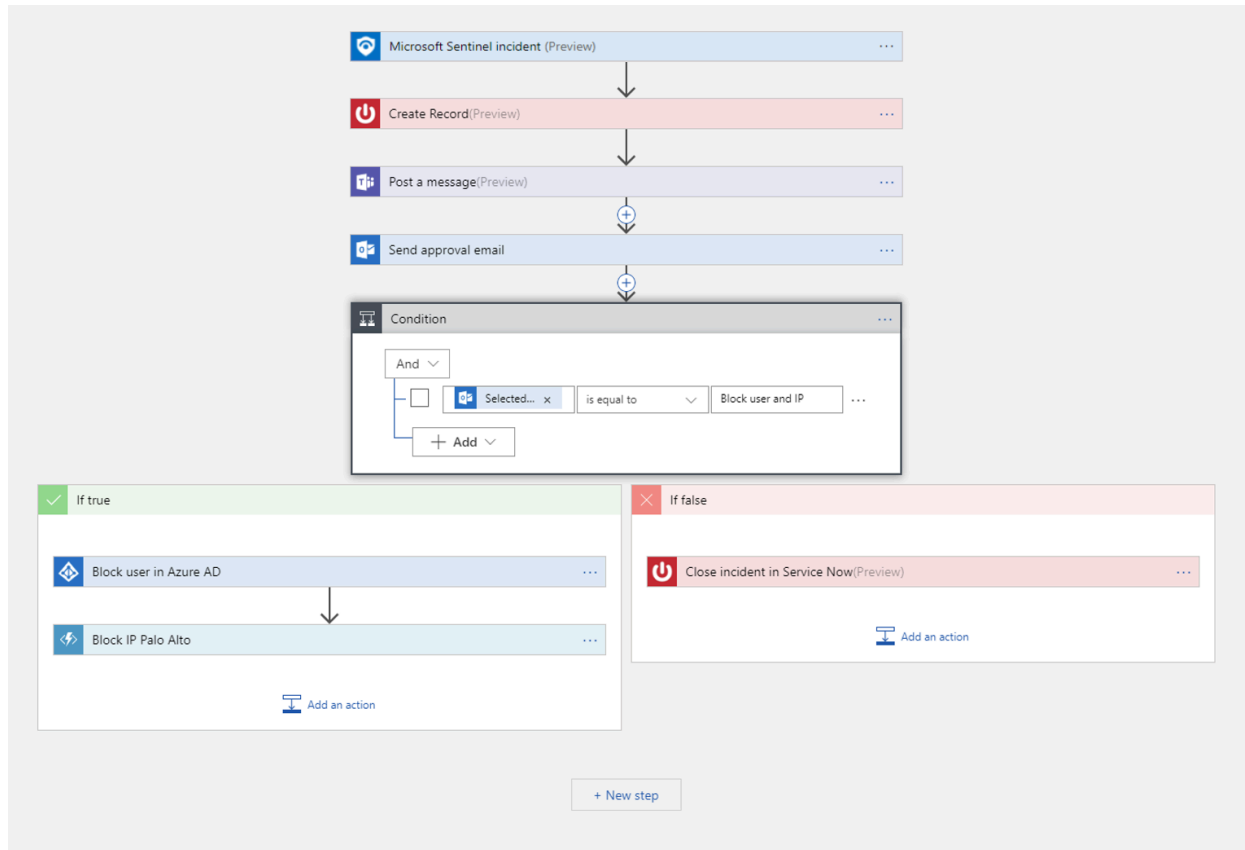
Coverage alerts (21)

Active coverage

Investigate threats

The screenshot displays the Microsoft Sentinel investigation interface. At the top, the breadcrumb navigation shows 'Home > Microsoft Sentinel > Microsoft Sentinel > Incident'. The main header area includes the incident title 'ADFS DKM Master Key Export' with a 'High' severity rating, a 'New' status, and an 'Unassigned' owner. The timestamp '5/3/2021, 12:14:42 PM' is also visible. The central part of the interface features a timeline diagram with nodes representing different entities and their relationships. The timeline is titled 'Timeline' and lists two events: 'ADFS DKM Master Key Export' on 4/4/2021 at 12:10:00 PM and 'ADFS DKM Master Key Export' on 5/2/2021 at 12:10:01 PM. The right sidebar contains navigation links for 'Timeline', 'Info', 'Entities', 'Insights', and 'Help'.

Respond to incidents



10.references:

- <https://learn.microsoft.com/en-us/azure/sentinel/overview?tabs=defender-portal>
- <https://github.com/azure/azure-sentinel/wiki>
- https://en.wikipedia.org/wiki/Security_information_and_event_management

-yuvaraj.D