

MICROSOFT SENTINEL SIEM

Project Title: Microsoft Sentinel SIEM Implementation on Azure

Author: Bhargav Pavan Sai Suriseti

Date: 08-10-2025

Project Description

The project aims to **implement Microsoft Sentinel**, a cloud-based **Security Information and Event Management (SIEM)** and **Security Orchestration, Automation, and Response (SOAR)** solution on **Microsoft Azure**.

Microsoft Sentinel helps monitor your IT environment, collect security data from different sources (like Azure resources, Microsoft 365, servers, firewalls, etc.), and detect suspicious activities using analytics and automation.

This project will guide you through setting up Microsoft Sentinel from scratch — creating necessary Azure resources, connecting data sources, setting up alerts, and building automated response playbooks.

Simple Requirements

1. **Azure Account** – Active subscription to use Azure services.
2. **Resource Group** – To organize all Sentinel-related resources.
3. **Log Analytics Workspace** – Stores logs and data for Sentinel.
4. **Enable Microsoft Sentinel** – Turn on Sentinel in your workspace.
5. **Permissions** – Need Owner or Contributor access to set up.
6. **Data Sources** – Connect Azure AD, Microsoft 365, or server logs.
7. **Basic Knowledge** – Some understanding of Azure and security monitoring.

Step 1: Create SIEM on Azure using Microsoft Sentinel GitHub Repo

Objective

Deploy Microsoft Sentinel automatically using Microsoft's **Sentinel All-In-One** template from GitHub.

Steps

1. Open the GitHub repository:

👉 <https://github.com/Azure/Azure-Sentinel/tree/master/Tools/Sentinel-All-In-One>

2. On that page, scroll down and click the **“Deploy to Azure”** button.
 - This will redirect you to your **Azure Portal** in a new browser tab.
 - It automatically loads the **Sentinel All-In-One ARM template** for deployment.
3. In the Azure Portal deployment form, fill in the required fields:
 - **Subscription:** Choose your active Azure subscription.
 - **Resource Group:** Create a new one (e.g., *Sentinel-RG*) or select an existing one.
 - **Region:** Select your preferred Azure region.
 - **Workspace Name:** Example — *SentinelWorkspace*.
 - **Admin Email:** Enter your email for alerts or notifications.
4. Review the parameters and click **“Review + Create”** → then **“Create.”**
5. Wait for the deployment to complete (it may take a few minutes).

The tool will automatically create:

- A **Log Analytics Workspace**
- **Microsoft Sentinel** enabled on it
- Optional **Automation Account** and **Playbooks**

6. Once completed, go to:

Azure Portal → Microsoft Sentinel → [Your Workspace Name]

Here you'll see your Sentinel dashboard ready to use.

Custom deployment

Deploy from a custom template

Can I deploy multiple resources within a single ARM template?

Aut

New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now →

Microsoft Sentinel All-In-One deployment, see more information about this project [here](#).

Project details

Deploying templates at subscription scope enables scenarios like applying policies and assigning roles at the subscription level. Subscription scope deployments are also used for creating resource groups and deploying resources in it. You can change the deployment scope by updating the schema in the template.

Subscription *

Azure subscription 1

Instance details

Location *

North Europe

Resource Group name *

SEC-Monitoring

Workspace Name *

SEC-Monitoring

Daily ingestion limit in GBs. Enter 0 for no limit. *

10

Number of days of retention *

90

Select pricing tier for Sentinel and Log Analytics *

Pay-as-you-go

Resource Manager

Default Directory

Export resource groups using Bicep or Terraform

Search

Create Manage view Refresh Export to CSV Open query Assign tags

Group by none

You are viewing a new version of Browse experience. Click here to access the old experience.

Filter for any field... Subscription equals all Location equals all Add filter

<input type="checkbox"/>	Name ↑	Subscription	Location
<input type="checkbox"/>	SEC-Monitoring	Azure subscription 1	North Europe

Step 2: Add Diagnostic Settings to Microsoft Sentinel

Objective

Send logs and activity data from Azure resources (like Azure AD, Key Vault, Storage Accounts, etc.) into your Microsoft Sentinel workspace for monitoring and analysis.

Steps

1. Open the Azure Portal

Go to <https://portal.azure.com> and sign in with your Azure account.

2. Go to the Resource you want to Monitor

Example: Azure Activity Log, Key Vault, Storage Account, or any other resource.

3. Open Diagnostic Settings

- In the left menu of the resource, select “**Diagnostic settings**”.
- Click “**Add diagnostic setting.**”

4. Name the Diagnostic Setting

- Give it a clear name (e.g., *SendToSentinel* or *ActivityLogsToSentinel*).

5. Select Logs to Send

- Check the boxes for the types of logs you want to collect.

Example:

- *AuditLogs* • *SignInLogs* • *Security* • *Performance*

6. Choose the Destination

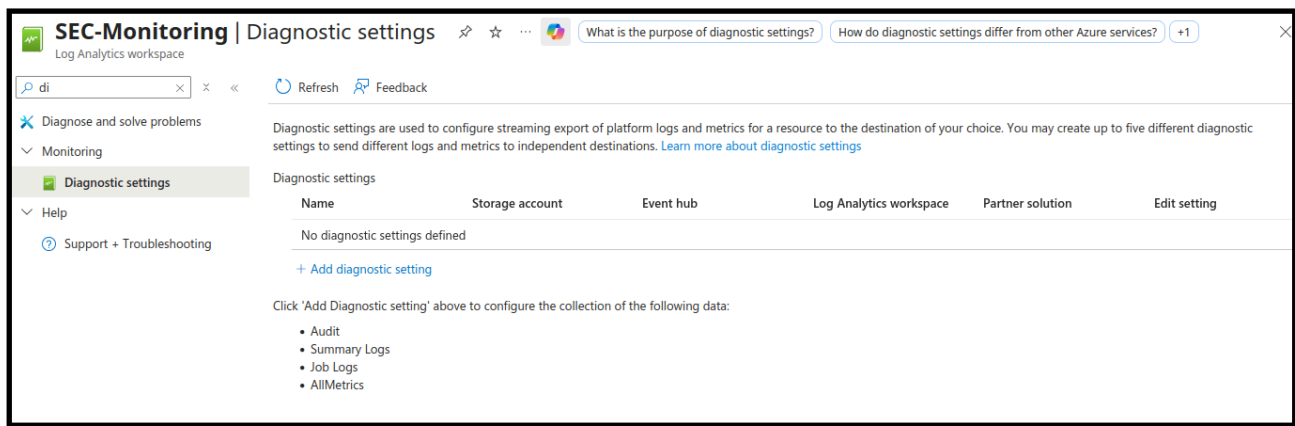
- Under “**Destination details**”, select:

Send to Log Analytics workspace

- Then, choose the **Log Analytics workspace** you created for Sentinel (e.g., *SentinelWorkspace*).

7. Save the Configuration

- Click **Save**.
- Azure will now start streaming logs from this resource into your Sentinel workspace.



Diagnostic setting

Save Discard Delete Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

A more flexible, faster, and robust way to collect metrics is in preview! Click [here](#) to configure platform metrics collection from microsoft.operationalinsights/workspaces to storage account, event hubs, and Log Analytics workspace. [Learn more.](#)

Diagnostic setting name * Sentinel

Logs

Category groups ⓘ

☐ audit ☒ allLogs

Categories

☒ Audit

☒ Summary Logs

☒ Job Logs

Metrics

☒ AllMetrics

Destination details

☒ Send to Log Analytics workspace

Subscription

Azure subscription 1

Log Analytics workspace

SEC-Monitoring (northeurope)

☐ Archive to a storage account

☐ Stream to an event hub

☐ Send to partner solution

Result

✅ Diagnostic settings are configured, and logs are now being collected in your Microsoft Sentinel workspace for analysis and alerting.

Step 3: Enable AI in SIEM (Turn On UEBA Feature)

Objective

Enable **User and Entity Behavior Analytics (UEBA)** in Microsoft Sentinel to use AI-based insights for detecting abnormal user or entity behavior — such as suspicious logins, unusual access patterns, or compromised accounts.

Steps

1. Open Microsoft Sentinel

- In the **Azure Portal**, go to **Microsoft Sentinel** → [Your Workspace Name].

2. Go to UEBA Settings

- In the left-hand menu, under **Configuration**, click “**Entity behavior**” or “**UEBA.**”

3. Enable UEBA

- Click “**Enable**” (or “**Turn on**”) to activate the **User and Entity Behavior Analytics** feature.
- This may take a few minutes to initialize.

4. Select Data Sources for UEBA

- UEBA uses identity and activity logs to analyze behavior.
- Make sure the following connectors are enabled:
 - **Azure Active Directory (SignInLogs, AuditLogs)**
 - **Microsoft Defender for Cloud Apps**
 - **Microsoft 365 Defender**
- UEBA automatically starts learning from these connected logs.

5. Wait for Data Collection

- After enabling UEBA, it takes **a few hours** for initial insights and profiles to appear.
- Sentinel will start building behavioral baselines using AI/ML models.

6. View AI Insights


- Go to **Microsoft Sentinel** → **Entity Behavior** → **Entity** page.
- Here, you'll see:

- User profiles and entities.
- Suspicious behavior scores.
- Related incidents and anomalies.


Home >

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

Apply

Home > Microsoft Sentinel

Microsoft Sentinel | Settings

Selected workspace: 'sec-monitoring'

Search

Workspace usage report

[Microsoft Sentinel](#)

- Enable Azure Lighthouse if you're managing workspaces across multiple Microsoft Sentinel workspaces [at scale](#).

Make this workspace a central workspace.

☐ Off

Playbook permissions

What is it?
Automation rules allow you to centrally manage all the automation of incident handling in Microsoft Sentinel and enable you to simplify complex workflows for your incident orchestration.

Playbook permissions
Microsoft Sentinel automation rules can run Logic App playbooks to integrate with other services. Explicit permissions are required to use this functionality.

[Configure permissions](#)

How do we use your data?

Auditing and health monitoring


Remove Microsoft Sentinel

Manage permissions

Choose the resource groups that contain the playbooks you want to give Microsoft Sentinel permissions to run

Browse Current permissions

Search

Name ↑↓	Subscription ↑↓
<input checked="" type="checkbox"/> SEC-Monitoring	 Azure subscription 1

Apply **Cancel**

✅ **AI-based behavior analytics (UEBA)** is enabled.

Microsoft Sentinel will now automatically analyze user and entity activity using machine learning to detect anomalies and potential insider threats.

Step 4: Create a Watchlist to Detect Cybersecurity Threats

Objective

Create and use a **Watchlist** in Microsoft Sentinel to detect, monitor, or alert on specific items — such as suspicious IP addresses, user accounts, or high-value assets.

Steps

1. Open Microsoft Sentinel

- Go to **Azure Portal** → **Microsoft Sentinel** → **[Your Workspace Name]**.

2. Navigate to Watchlists

- In the left menu, under **Configuration**, click **“Watchlists.”**
- Select **“+ Add new”** to create a new watchlist.

3. Enter Basic Details

- **Name:** (e.g., *CyberThreatIPs* or *HighValueUsers*)
- **Description:** A short explanation like *“List of known malicious IPs for threat detection.”*

4. Upload Data File

- Prepare a simple **CSV file** with your data.

Example format:

IPAddress,Description

192.168.1.10,Suspicious internal IP

8.8.8.8,External DNS to monitor

10.0.0.5,High-value server

•Click **“Upload file”** and select your CSV file.

- Choose the column (like IPAddress) that will act as the **search key**.

5. Save and Create

- Click **“Next → Review + Create.”**
- Once validated, click **“Create.”**

✓ Created watchlist [Top-IP-Adresses]



Successfully submitted watchlist [Top-IP-Adresses]. It may take a few minutes for the 49 watchlist items to be created, validated and become available.

a few seconds ago

Watchlists

0
Watchlists

0
Watchlist Items

My Watchlists Templates (Preview)

+ New Delete Update watchlist Columns

Search by name, alias and description

Add filter

<input type="checkbox"/>	Name	Alias	Source	Created...	Last up...
<input type="checkbox"/>	Top-IP-Adresses	Top-IP-Adr	Tor+Exit+N	10/8/2025,	10/8/2025,

Result

✓ Watchlist successfully created through **Microsoft Defender Portal** and connected to Microsoft Sentinel for threat detection and monitoring.

Step 5: Create a User Account in Azure for SIEM Investigation

Objective

Create a **dedicated Azure AD user account** for security analysts to access Microsoft Sentinel and perform investigations, while following the **least-privilege principle**.

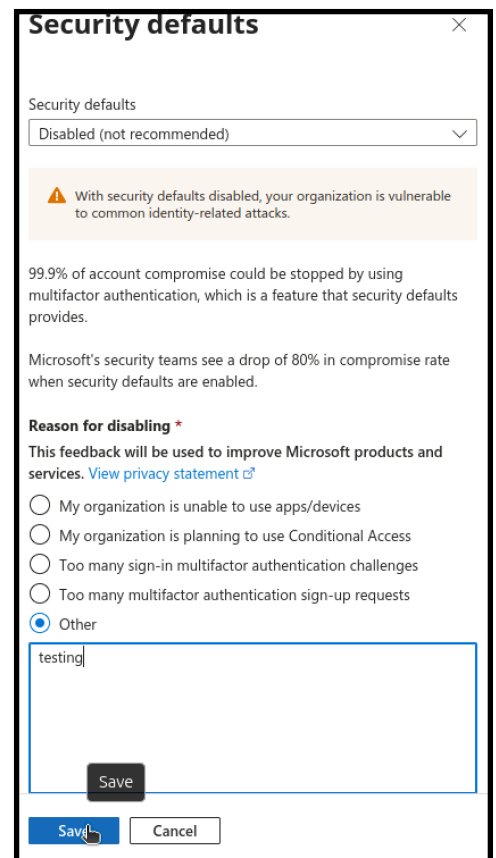
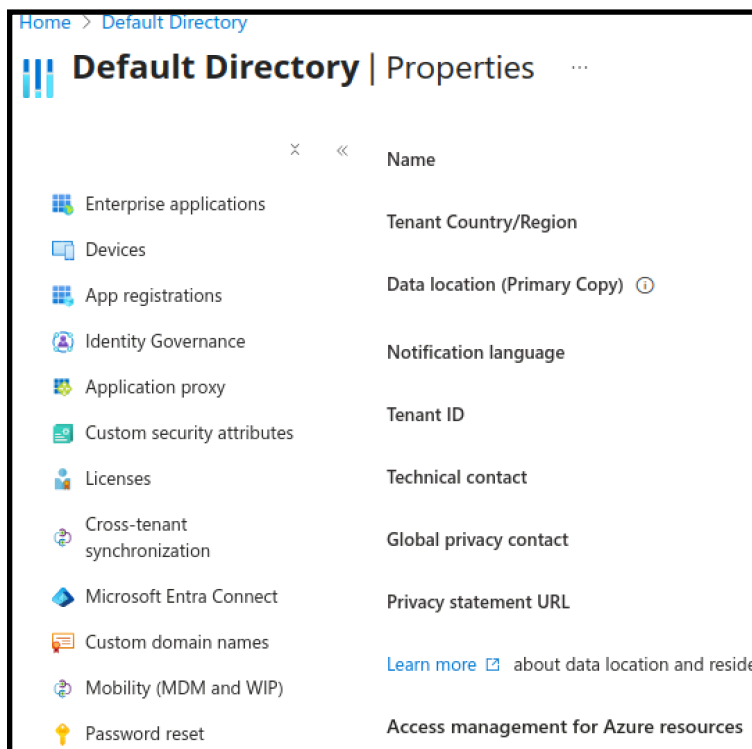
Steps

1. Open Azure Active Directory

- Go to https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview.

2. Disable Security Defaults (if enabled)

- In Azure AD, go to **Properties** → **Manage Security Defaults**
- Turn **Security Defaults** to **Off**.
- This allows you to create custom roles and accounts without enforcing default MFA policies (optional, based on lab/testing needs).

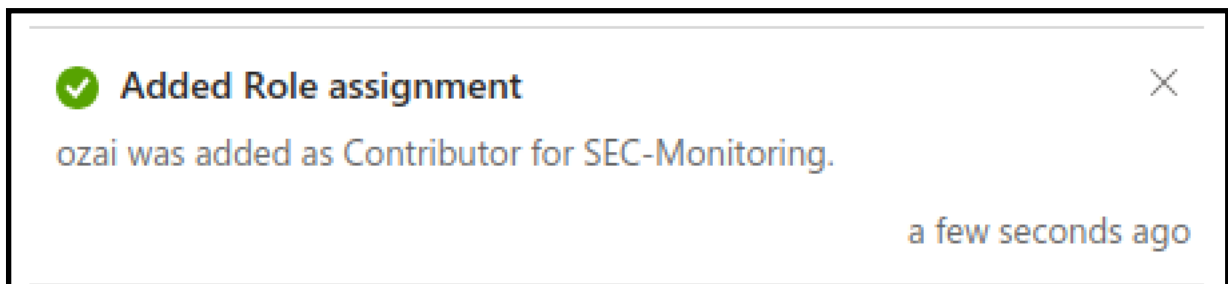


3. Create a New User

- Navigate to **Users** → **+ New User** → **Create User**.
- Fill in the details:
 - **Username:** siem.investigator@yourdomain.com
 - **Name:** SIEM Investigator
 - **Password:** Auto-generate or set a strong temporary password

4. Assign Roles for Sentinel Access


- Go to **Microsoft Sentinel** → **[Your Workspace]** → **Access Control (IAM)** → **+ Add role assignment**
- Select a **role**:
 - Microsoft Sentinel Reader – read-only access
 - Microsoft Sentinel Contributor – full access to analytics rules and playbooks
- Assign the role to the newly created user and save.



5. Verify Account Access

- Log in with the new account at <https://portal.azure.com>
- Navigate to **Microsoft Sentinel** → **[Your Workspace]**
- Confirm the user can view dashboards, logs, and alerts according to assigned role.

Result

 The **SIEM investigation user account** is ready and has proper access through **Access Control (IAM)** for secure investigation in Sentinel.

Step 6: Generate Test Incidents for SIEM Investigation

Objective

Generate incidents so SOC analysts can practice investigations and validate detections, playbooks, and runbooks — using safe, controlled methods.

Steps

1. Use a test account

- Ensure you have a dedicated test user (e.g., siem.testuser@yourdomain.com) — do not use a real SOC or admin account.

2. Open Azure Active Directory → Users

- Portal: Azure Portal → Azure Active Directory → Users
- Select the test user.

3. Reset password

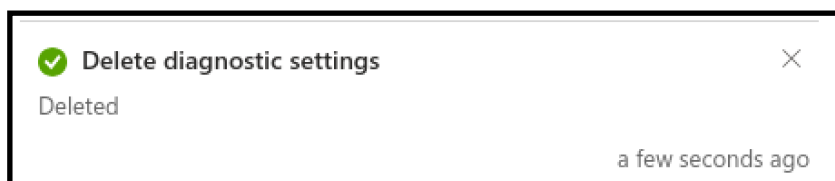
- Click **Reset password** → choose **Auto-generate password** or set a strong temporary password → **Reset**.
- Note the temporary password so you can sign in with it.

4. Perform a test sign-in (optional)

- Sign in to <https://portal.azure.com> (or another test app) with the test user using the new password to generate sign-in logs.
- You can also attempt a failed sign-in from a different IP/device to generate additional suspicious sign-in events (again: only against accounts you control).

5. Delete the diagnostic setting (test resource only)

- Portal: **Open the resource** → **Diagnostic settings** → **select the diagnostic setting** → **Delete**
- Confirm the deletion.



6 . Delete Diagnostic Settings / Manage Auditing and Health Monitoring (Test Resources Only)

- Open the test resource in **Azure Portal**.
- Navigate to **Diagnostic settings** → select the diagnostic setting → **Delete** → confirm

The screenshot shows the 'Diagnostic setting' page in the Azure Portal. At the top, there are buttons for 'Save', 'Discard', 'Delete', and 'Feedback'. A 'Delete' confirmation dialog is open, asking 'Are you sure you want to delete?' with 'Yes' and 'No' buttons. The 'Logs' tab is selected, showing 'Category groups' with 'allLogs' checked and 'Categories' with 'Analytics', 'Automation', and 'Data Collection - Connectors' checked. The 'Destination details' section shows 'Send to Log Analytics workspace' checked, with 'Subscription' set to 'Azure subscription 1' and 'Log Analytics workspace' set to 'SEC-Monitoring (northeurope)'. Other options like 'Archive to a storage account', 'Stream to an event hub', and 'Send to partner solution' are unchecked.

7 . Restore Settings

- Re-enable deleted diagnostic settings or auditing after testing.
- Ensure normal telemetry resumes for monitoring and SIEM ingestion.

Result

✅ Auditing and health monitoring events are generated safely on **test resources**, allowing Sentinel to detect and create incidents for training and validation purposes.

Step 7: Explore and Investigate Incidents in Microsoft Sentinel (SIEM)

Objective

Investigate alerts and incidents detected by Microsoft Sentinel to understand threats and take response actions.

Steps

1. Open Incidents Page

- Go to **Azure Portal** → **Microsoft Sentinel** → **[Your Workspace]** → **Incidents**.
- You'll see a list of all active and past incidents.

2. View Incident Details

- Click on any incident to open the **Incident Details** page.
- Review:
 - **Overview:** Summary, severity, status, and owner.
 - **Alerts:** Specific detections that triggered the incident.
 - **Entities:** Users, IP addresses, or devices involved.
 - **Investigation Graph:** Visual view showing how entities and alerts are connected.
 - **Evidence & Response:** Logs, playbooks, and actions related to the incident.

3. Analyze the Data

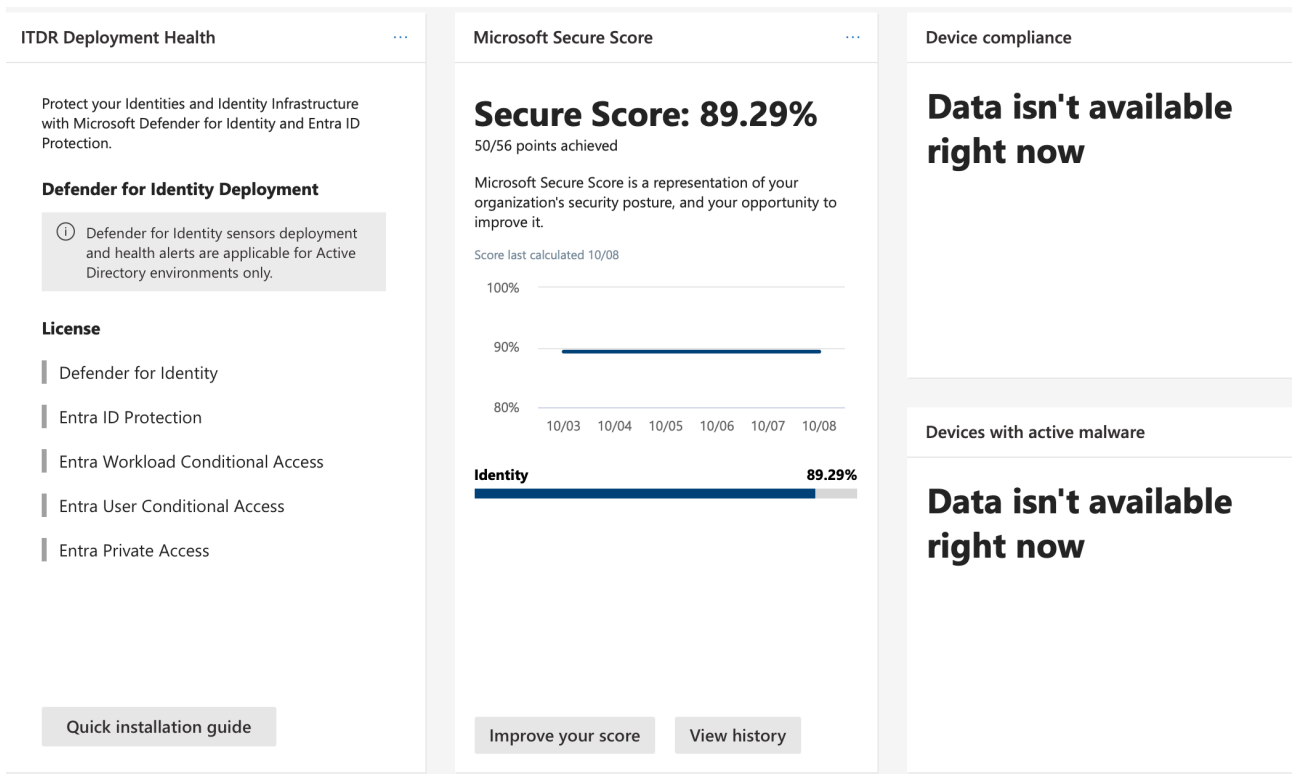
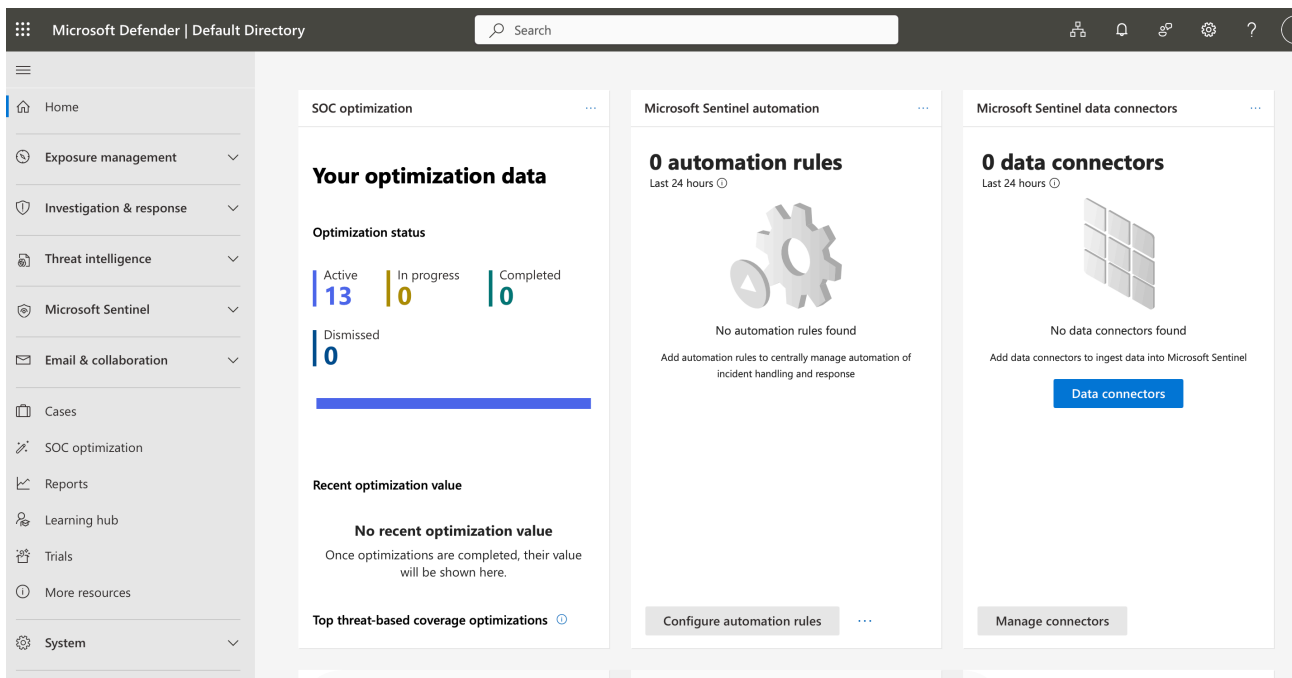
- Use the **Logs** tab to run **KQL queries** for deeper investigation.
- Correlate alerts with other data sources (like Sign-in logs, Audit logs, etc.).
- Identify root cause, affected users, and suspicious behavior patterns.

4. Take Action

- Update the **incident status** (Active → Resolved → Closed) based on your findings.
- Assign incidents to SOC analysts or team members.
- Trigger playbooks or manual actions if response automation is configured.

5. Document Findings

- Record investigation details, timeline, and remediation steps.
- Use these insights to improve detection rules and response strategies.



Result

✓ You have successfully **investigated incidents** in Microsoft Sentinel, analyzed related alerts, and taken appropriate response actions.

Step 8: Perform Remediation in Microsoft Sentinel (SIEM)

Objective

Take corrective actions to contain and resolve security incidents detected by Microsoft Sentinel.

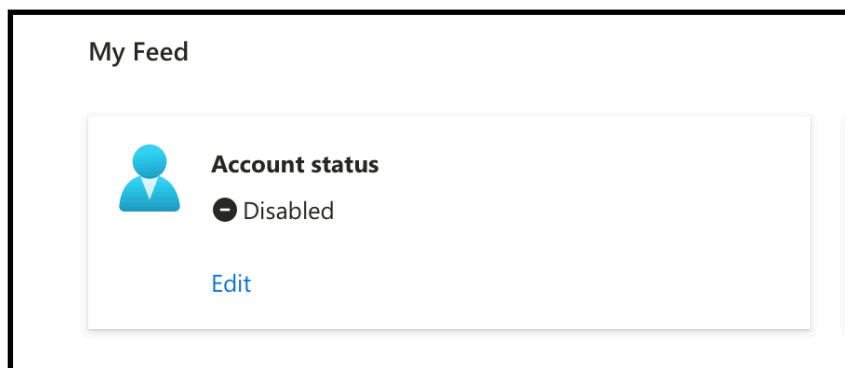
Steps

1. Open the Incident for Remediation

- Go to **Azure Portal** → **Microsoft Sentinel** → **[Your Workspace]** → **Incidents**.
- Select the incident you need to remediate.
- Review all related **alerts, users, and affected resources** under the **Entities** tab.

2. Disable the Compromised User Account

- Navigate to **Azure Portal** → **Azure Active Directory** → **Users**.
- Search for the affected user (e.g., the one involved in the incident).
- Click on the user's name → **Block sign-in** → select **Yes** → click **Save**.
- This action immediately prevents the user from accessing Azure resources.
- Note the action in your incident documentation for auditing.



3. Check and Restore Diagnostic Settings

- Go to **Azure Portal** → **Resource Group** → **Select affected resource (VM, Storage, etc.)** → **Diagnostic settings**.
- Ensure diagnostic logs are still connected to **Log Analytics / Sentinel Workspace**.
- If diagnostic settings were deleted or modified during testing:

- Click **+ Add diagnostic setting**.
- Choose **Send to Log Analytics workspace**.
- Select your **Sentinel workspace** and **Save**.
- This ensures continued log collection and visibility for Sentinel.

4.Enable Auditing and Health Monitoring

- Go to the affected resource (e.g., SQL Server, Storage Account, or VM).
- Open **Auditing & Health Monitoring** (under **Monitoring** in the left pane).
- Turn **Auditing** → **ON** and configure it to send logs to your **Log Analytics workspace**.
- Enable **Health Monitoring** to track performance and availability.
- Save the configuration to ensure logs flow into Sentinel for continuous monitoring.

Step 9: Conclusion and Project Summary

Objective

Summarize the outcomes of the Microsoft Sentinel SIEM project and ensure all configurations, monitoring, and security operations are functioning properly.

Final Conclusion

The **Microsoft Sentinel SIEM Project** successfully demonstrates how to deploy, configure, and manage a cloud-based security monitoring solution on **Microsoft Azure**.

Throughout this project, Sentinel was integrated with diagnostic logs, data connectors, and analytics rules to detect and investigate potential threats.

User and Entity Behavior Analytics (UEBA), watchlists, and automated playbooks enhanced visibility and response efficiency.

By simulating security incidents and performing remediation actions such as disabling compromised accounts, enabling auditing, and restoring diagnostic settings, this project showcased a complete **end-to-end SOC workflow** — from detection to investigation and response.

With Microsoft Sentinel in place, organizations gain **real-time threat detection**, **automated incident response**, and **centralized visibility** across Azure resources, ensuring a stronger and more proactive security posture in the cloud environment.

THANK YOU