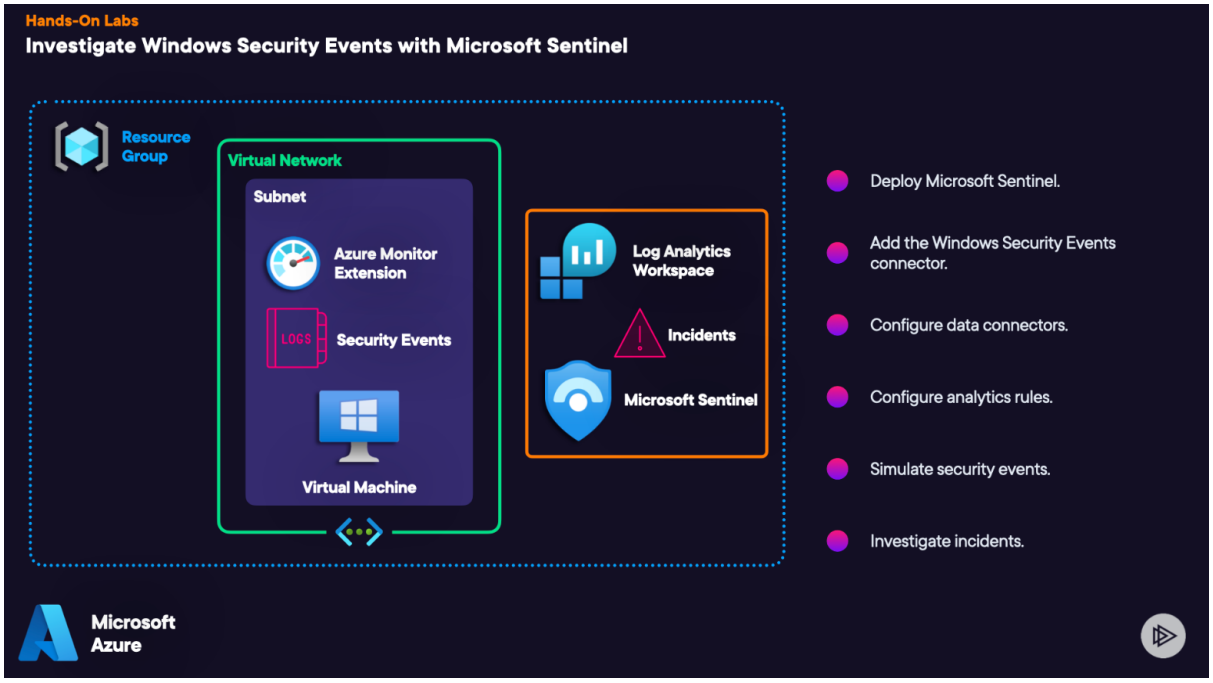
Investigate Windows Security Events with Microsoft Sentinel

Introduction

Microsoft Sentinel is a cloud-native SIEM (security information and event management) solution with SOAR (security orchestration, automation, and response) capabilities. You can use Microsoft Sentinel to collect, detect, investigate, and respond to security threats across your infrastructure. In this lab, you will deploy Microsoft Sentinel, generate some security alerts, and investigate those alerts.

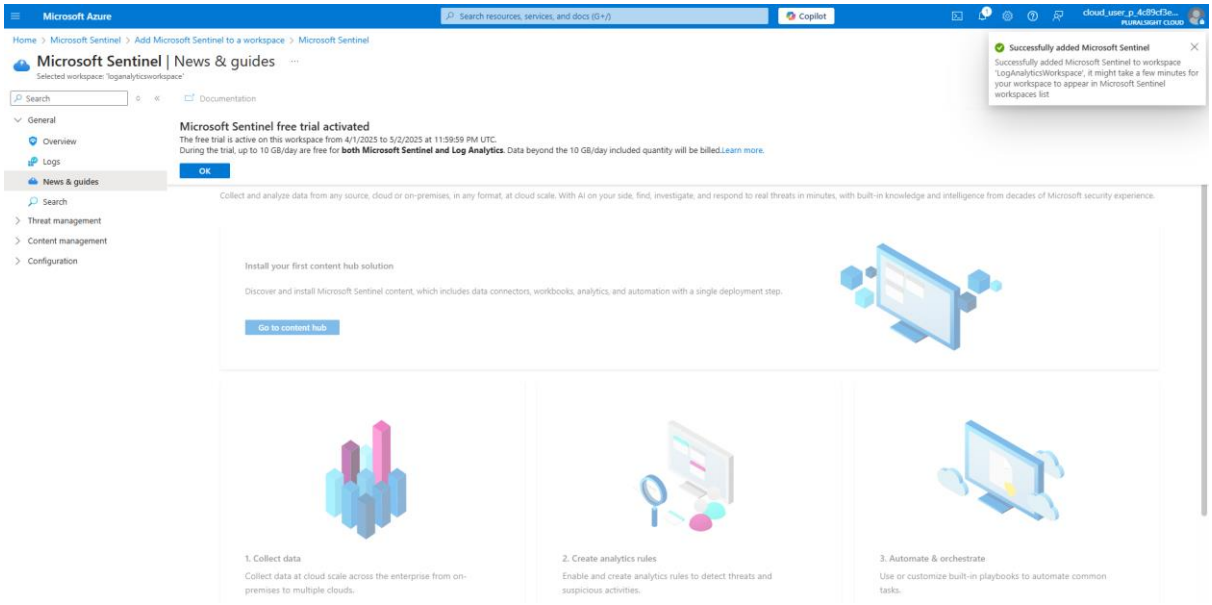


Deploy Microsoft Sentinel

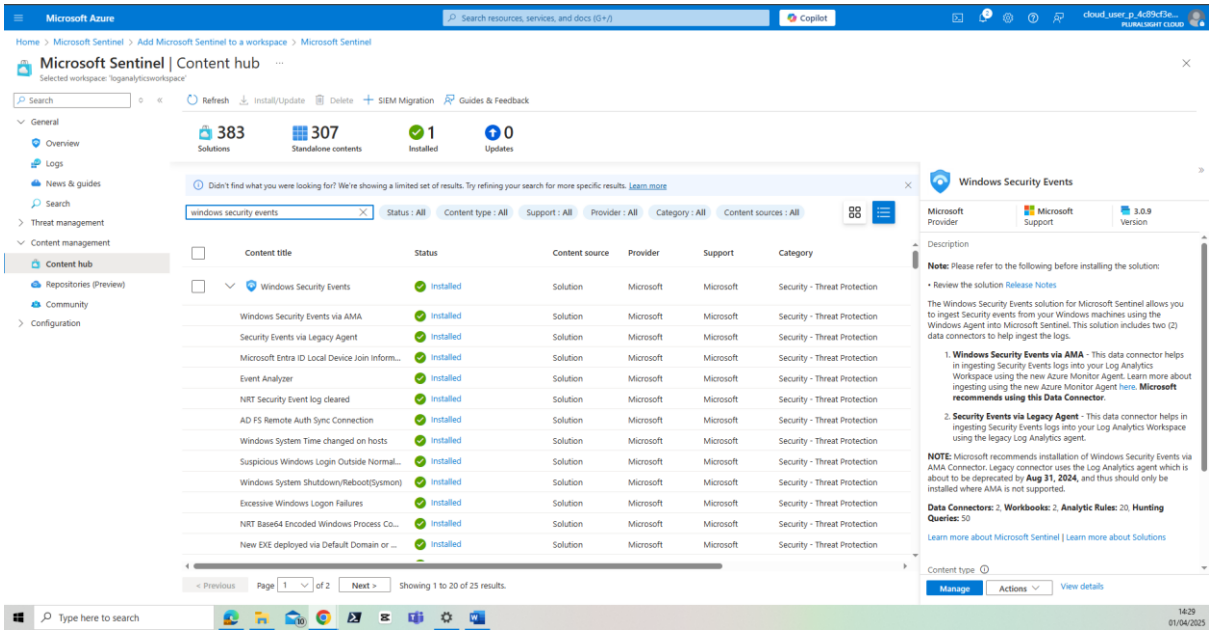
A. From the top search bar, search for and navigate to **Microsoft Sentinel**.

B. Click **Create Microsoft Sentinel**.

C. Select the provisioned Log Analytics workspace and click **Add**



Installed Microsoft Security Events



Configure Data Connectors

A. On the left menu, under **Configuration**, select **Data connectors**.

B. Select **Windows Security Events via AMA**.

C. Click **Open connector page**.

D. Under **Configuration**, click **+Create data collection rule**.

E. In the **Create Data Collection Rule** wizard, under **Rule Name**, enter *All_Windows_Security_Events*.

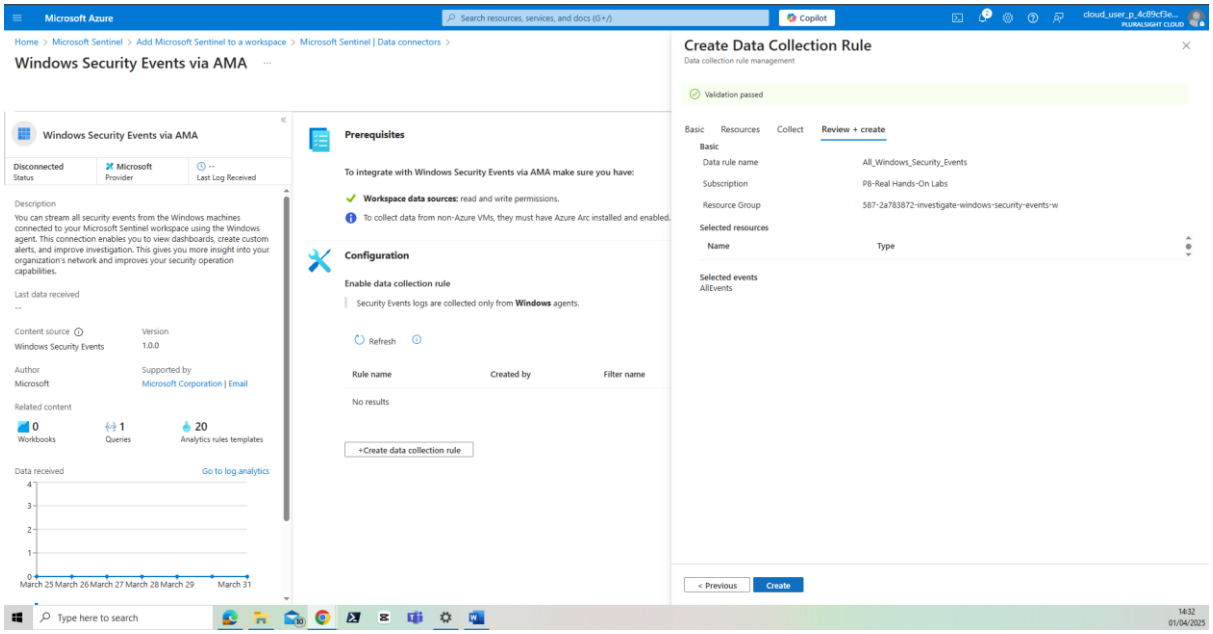
F. Leave the rest of the settings as their default and click **Next: Resources**.

G. Click **+Add resource(s)**.

H. Select the provisioned virtual machine and click **Apply**.

I. Click **Next: Collect** > **Next: Review + create**.

J. Click **Create**.



Configure Analytics Rules

Configure the Analytics Rule to Search for When Scheduled Tasks Are Hidden

A. At the top of the page, click **Microsoft Sentinel**.

B. On the left menu under **Configuration**, select **Analytics**.

C. Select the **Rule templates** tab.

D. In the search bar, type *Scheduled Task Hide*.

E. Select the rule underneath, and click **Create rule**.

F. Leave the default settings and click **Next: Set rule logic**.

G. Scroll down to **Query scheduling**, and set the following values:

- **Run query every**: **5 Minutes**
- **Lookup data from the last**: **5 Minutes**

H. Click **Next: Incident settings**.

I. For **Group related alerts, triggered by this analytics rule, into incidents**, select **Enabled**.

J. Ensure the **Grouping alerts into a single incident if all the entities match** option is also selected.

K. Click **Next: Automated response** > **Next: Review and Create**.

L. Click **Save**.

Configure the Rule for Detecting Excessive Windows Logon Values

A. On the **Analytics** page, select **Rule templates**.

B. In the search bar, type *Excessive Windows Logon Failures*.

C. Select the rule, and click **Create rule**.

D. Leave the default settings as-is, and click **Next: Set rule logic**.

E. Scroll down to **Query scheduling** and set the following values:

- **Run query every**: **5 Minutes**
- **Lookup data from the last**: **1 Days**

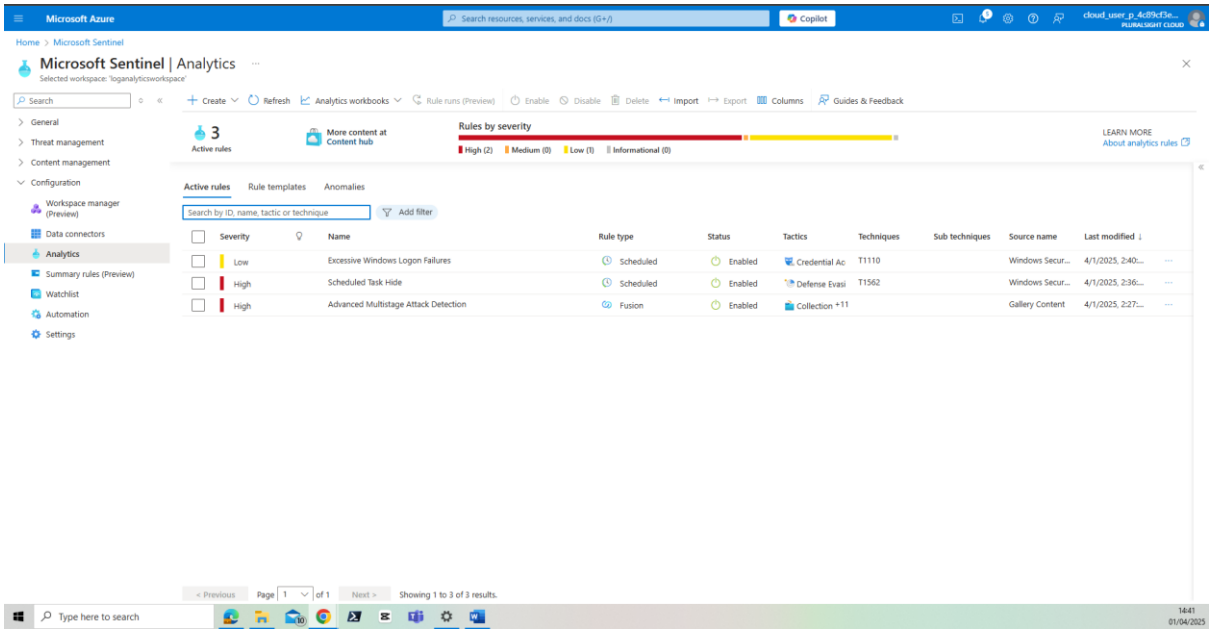
F. Click **Next: Incident settings**.

G. For **Group related alerts, triggered by this analytics rule, into incidents**, select **Enabled**.

H. Ensure the **Grouping alerts into a single incident if all the entities match** option is also selected.

I. Click **Next: Automated response** > **Next: Review and create**.

J. Click **Save**.



Enable Auditing of Object Access

A. Log in to the Windows virtual machine using the credentials provided for the lab-VM in your lab.

Note: When connecting to the virtual machine, you can ignore any certificate warnings.

B. Right-click the **Start** button, and select **Run**.

C. Type gpedit.msc, and click **OK**.

D. In the **Local Group Policy Editor** window, expand **Computer Configuration** > **Windows Settings** > **Security Settings** > **Advanced Audit Policy Configuration** > **System Audit Policies - Local Group**.

E. On the right side of the screen, double-click **Object Access**.

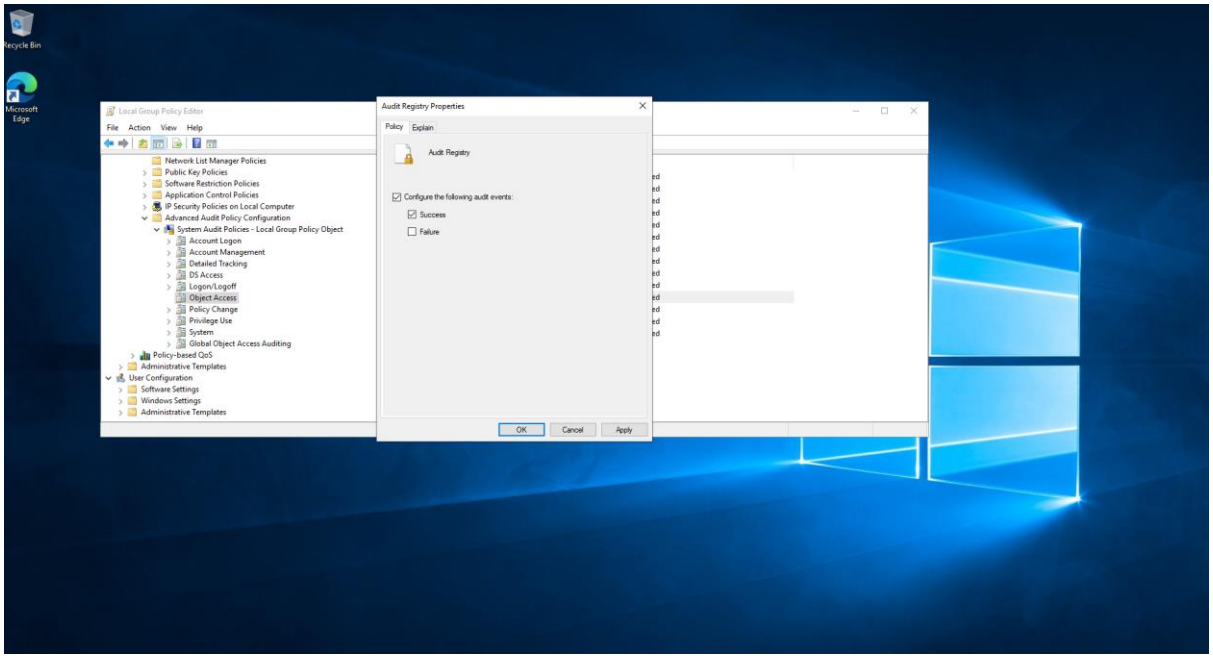
F. On the next screen, double-click **Audit Registry**.

G. Click the box next to **Configure the following audit events**.

H. Select **Success**, and click **OK**.

I. To update Group Policy locally, right-click the **Start** button and select **Run**.

J. Run GPUPDATE /FORCE. Click **OK**.



Enable Auditing Registry Settings for Scheduled Tasks

A. Click **Start** > **Windows Administrative Tools** > **Registry Editor**.

B. On Registry Editor, navigate to **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **Microsoft** > **Windows NT** > **CurrentVersion**.

C. Scroll down and right-click the **Schedule** folder, then select **Permissions**.

D. Click **Advanced**.

E. Select the **Auditing** tab.

F. Click **Add**.

G. Next to **Principal**, click **Select a principal**.

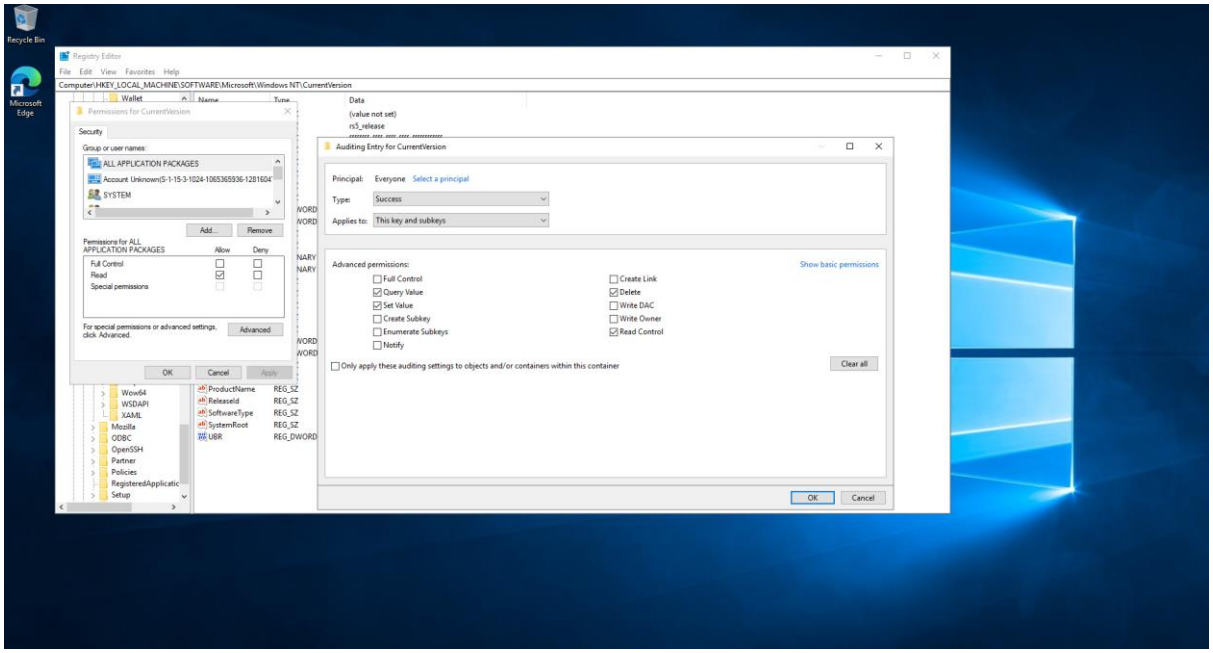
H. In the **Select User or Group** pop-up window, type *Everyone* in the bottom field.

I. Click **OK**.

J. Click the **Show advanced permissions** link.

K. Check the box next to **Query Value**, **Set Value**, and **Delete**. (**Read Control** can stay selected.)

L. Click **OK** > **OK** > **OK**.


Recycle Bin
Microsoft Edge
Registry Editor
File Edit View Favorites Help
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
Permissions for CurrentVersion
Security
Group or user names:
ALL APPLICATION PACKAGES
Account Unknown(S-1-15-3-1024-1065365936-1281604
SYSTEM
Add...
Remove
Permissions for ALL APPLICATION PACKAGES
Allow
Deny
Full Control
Read
Special permissions
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply
Auditing Entry for CurrentVersion
Principal: Everyone Select a principal
Type: Success
Applies to: This key and subkeys
Advanced permissions:
Show basic permissions
Full Control
Query Value
Set Value
Create Subkey
Enumerate Subkeys
Notify
Create Link
Delete
Write DAC
Write Owner
Read Control
Only apply these auditing settings to objects and/or containers within this container
Clear all
OK
Cancel
Wow64
WSDAPI
XAML
Mozilla
ODBC
OpenSSH
Partner
Policies
RegisteredApplicatic
Setup
ProductName REG_SZ
ReleaseId REG_SZ
SoftwareType REG_SZ
SystemRoot REG_SZ
UBR REG_DWORD

Simulate Security Events

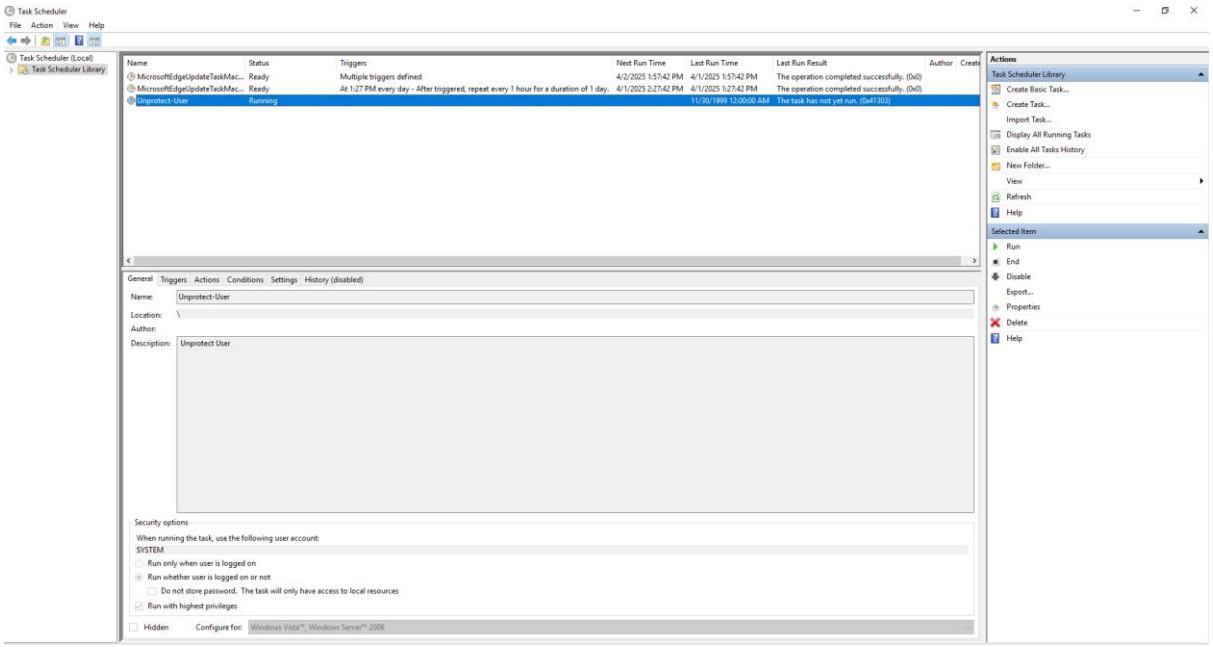
Start and Hide the Scheduled Task

A. Open Task Scheduler by clicking **Start** > **Windows Administrative Tools** > **Task Scheduler**.

B. On the left navigation, select the **Task Scheduler Library**.

C. In the middle pane, select the **Unprotect-User** task.

D. Right-click the task, and select **Run**.



Hide the Scheduled Task

A. Right-click the **Start** button, select **Run**, and run PSExec as system: C:\Scripts\PsExec64.exe -accepteula -i -s cmd.exe.

B. In the terminal window, type whoami to confirm you're running as system.

C. Delete the security descriptor for the scheduled task you just ran using the following command:

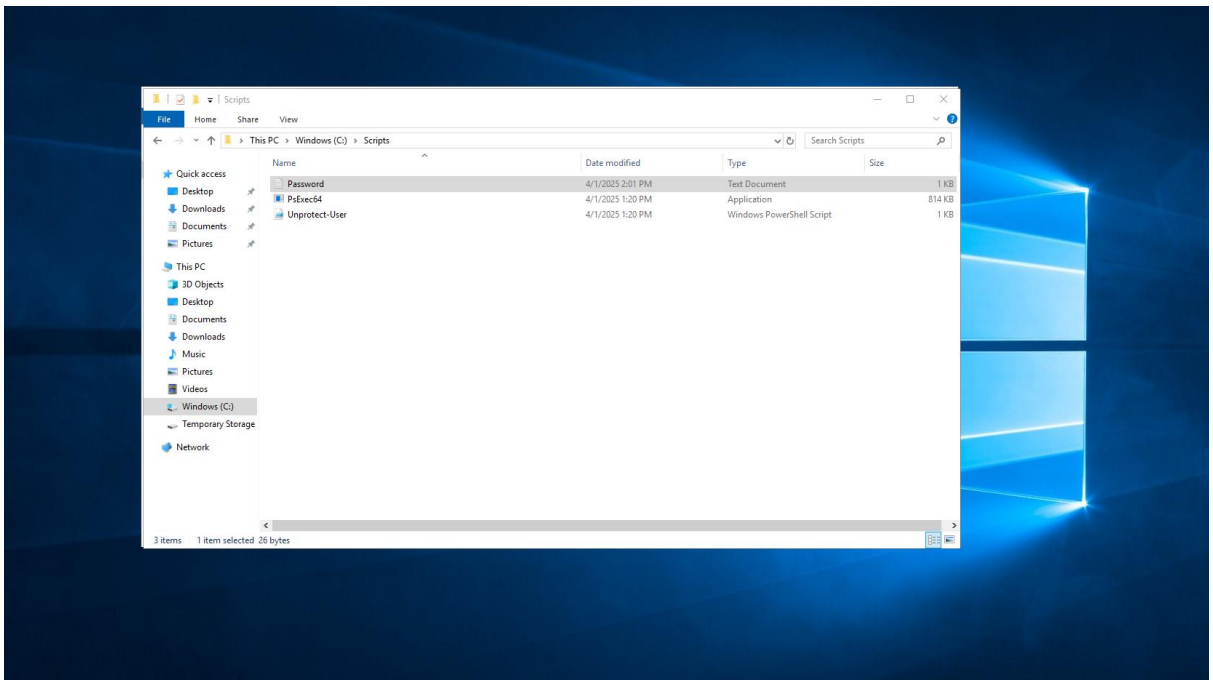
D. REG DELETE "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Unprotect-User" /v SD /f

E. Close the terminals and refresh Task Scheduler (right-click the center pane, and select **Refresh**).The task is now hidden and attempting to brute force a local user account.

F. Close Task Scheduler. From the **File Explorer**, click **This PC**.

G. Then, go to **Windows (C)** > **Scripts**.

H. Observe the **Password** file is available, meaning the password was brute-forced by the script.



Investigate the Incidents

A. Return to the Azure portal.

B. Under **Threat Management**, select **Incidents**.

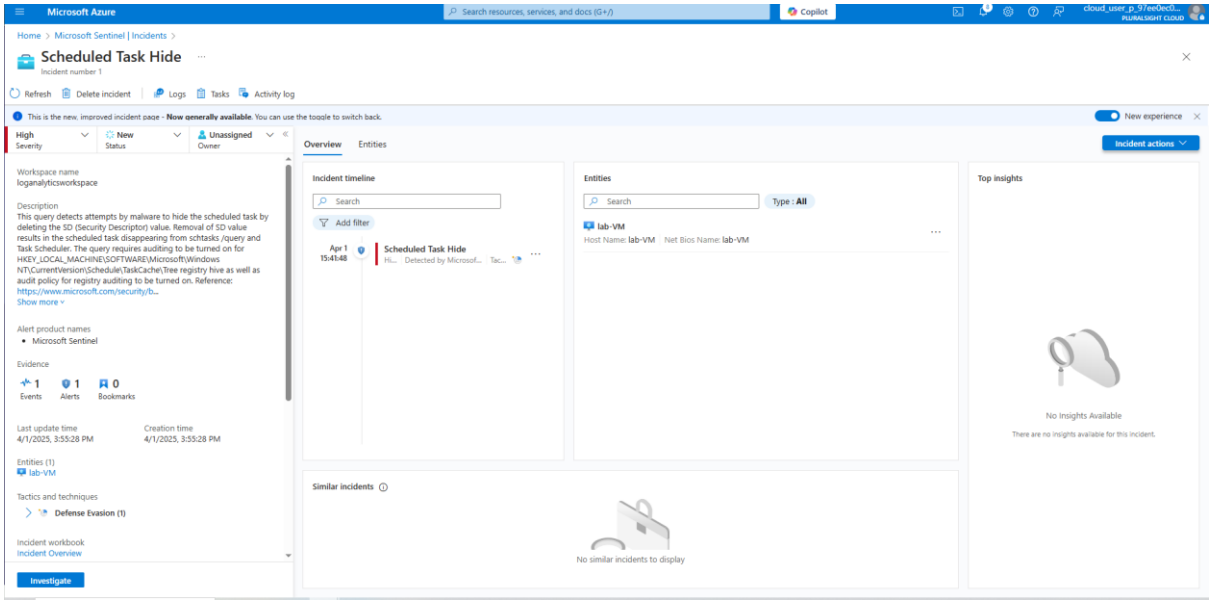
C. View the identified events, alerts, and incidents.

Note: It may take up to 10 minutes for all of the security events to populate to Microsoft Sentinel and for the alerts to be created.

D. Once incidents are available, select the first created incident, and click **View full details**.

E. Click **Investigate** on the bottom left to view the incident details

F. Click the **Incidents** link in the breadcrumb navigation to view any other incidents that come through.



Description

This query detects attempts by malware to hide the scheduled task by deleting the SD (Security Descriptor) value. Removal of SD value results in the scheduled task disappearing from schtasks /query and Task Scheduler. The query requires auditing to be turned on for HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree registry hive as well as audit policy for registry auditing to be turned on.