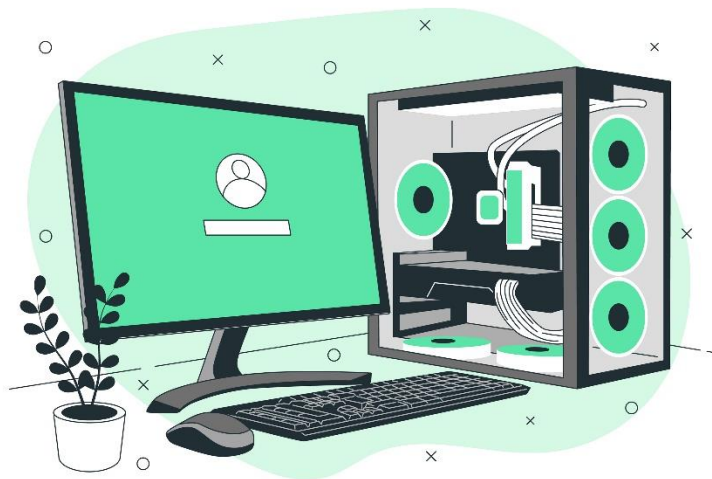


CyberSight - Enhancing SIEM with Microsoft Sentinel Detection Lab and SOAR Automation

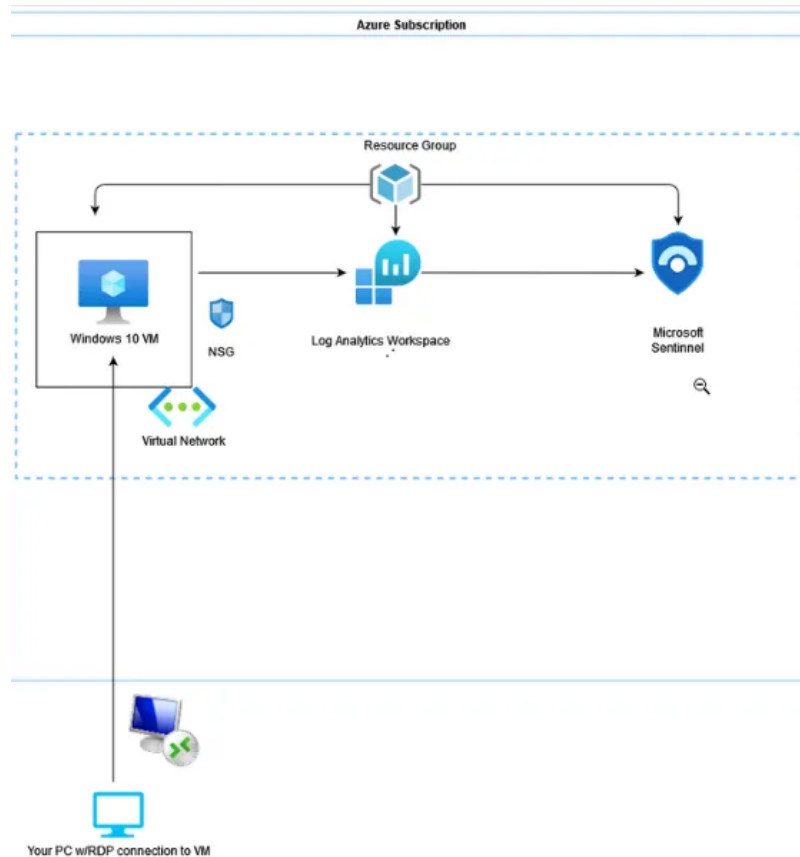


CyberSight is a project aimed at enhancing Security Information and Event Management (SIEM) capabilities using Microsoft Sentinel and Security Orchestration, Automation, and Response (SOAR) techniques. This project provides hands-on experience and practical exercises to familiarize cybersecurity enthusiasts with Azure Sentinel, enabling them to effectively defend against cyber threats and strengthen organizational security posture.

Parts Overview:

1. **Setup Lab Resources:** This part focuses on creating necessary Azure resources, including a virtual machine, resource groups, and networking configurations, to establish the foundation for the CyberSight lab.
2. **Getting Data into Sentinel:** Connecting Windows 10 VMs to Azure Sentinel using data connectors and data collection rules, enabling the ingestion of security events for analysis.
3. **Remote Accessing and Generating Security Events in our VM:** Exploring to remotely access a Windows 10 VM, generating security events, and observe them in Event Viewer to understand Windows security event logging.
4. **Kusto Query Language:** Demonstrates how to query and analyze security events stored in Azure Sentinel logs using Kusto Query Language (KQL).
5. **Writing Analytic Rule and Generating Scheduled Task:** Creates analytic rules in Azure Sentinel to detect specific security events and set up scheduled tasks in Windows VMs to simulate potential threat scenarios.
6. **Scheduled Task and Persistence Techniques:** Delves into scheduled tasks as a persistence technique, create custom rules to detect malicious activity, and explore mitigation strategies based on MITRE ATT&CK framework.
7. **MITRE ATT&CK:** Discussion about MITRE ATT&CK framework, its relevance to cybersecurity, and how it guides detection and mitigation efforts in the context of the CyberSight project.

Topology



Procedure

Part 1: Setup Lab Resources

1. Follow the provided link to create your Azure Account. This process will automatically set up your account and associated Azure Subscription. <https://azure.microsoft.com/en-us/free/>

Create a Resource Group

2. Navigate to the Azure Portal and search for "Resource Group" in the search bar.
3. Follow the on-screen prompts to create a lab named Cyber_Sight_Lab.
4. Skip to "review and create" after filling out the basic information and click on create.

Home > Resource groups >

Cyber_Sight_Lab

Search

Create Manage view Delete resource group Refresh Export to CSV Open query Assign tags Move Delete Export template Open in mobile

Overview

Activity log

Access control (IAM)

Tags

Resource visualizer

Events

Settings

Deployments

Security

Deployment stacks

Policies

Properties

Locks

Cost Management

Cost analysis

Cost alerts (preview)

Budgets

Advisor recommendations

Monitoring

Insights (preview)

Alerts

Metrics

Diagnostic settings

Essentials

Subscription (move) : Azure subscription 1

Subscription ID :

Tags (edit) : Add tags

Deployments : 14 Succeeded

Location : East US

Resources Recommendations

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

Showing 1 to 3 of 3 records. Show hidden types

No grouping List view

Name	Type	Location
CyberSightWorkspace	Log Analytics workspace	East US
SecurityEvent	Data collection rule	East US
Securityinsights(cybersightworkspace)	Solution	East US

< Previous Page 1 of 1 Next >

Give feedback

Deploy a Virtual Machine

5. Use the previously created resource group and fill out the required fields to create your virtual machine.
6. Type "Virtual machine" in the search bar.
7. Fill in the appropriate fields, including adding the VM to your resource group.
8. Use all the default settings on the Basics Tab and fill in the appropriate field.
9. For Disks, Networking, Management, Advanced, and Tags, the default settings are sufficient.
10. Remember the admin username and password for authentication.
11. Click on "Review + create" and create your virtual machine.

Home >

CyberSightVM

Virtual machine

Search

Connect Start Restart Stop Hibernate (preview) Capture Delete Refresh Open in mobile Feedback CLI / PS

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect

Connect

Bastion

Networking

Network settings

Load balancing

Application security groups

Network manager

Settings

Disks

Extensions + applications

Configuration

Advisor recommendations

Properties

Locks

Availability + scale

Size

Availability + scaling

Essentials

Resource group (move) : CyberSight

Status : Stopped (deallocated)

Location : East US (Zone 1)

Subscription (move) : Azure subscription 1

Subscription ID :

Availability zone : 1

Tags (edit) : Add tags

Operating system : Windows

Size : Standard D2s v3 (2 vcpus, 8 GiB memory)

Public IP address :

Virtual network/subnet : CyberSightVM-vnet/default

DNS name : Not configured

Health state : +

Properties Monitoring Capabilities (7) Recommendations Tutorials

Virtual machine

Computer name	CyberSightVM
Operating system	Windows
Image publisher	MicrosoftWindowsDesktop
Image offer	Windows-10
Image plan	win10-22h2-pro-g2
VM generation	V2
VM architecture	x64
Hibernation	Disabled
Host group	-
Host	-
Proximity placement group	-
Colocation status	N/A
Capacity reservation group	-
Disk controller type	SCSI

Networking

Public IP address	
Public IP address (IPv6)	-
Private IP address	10.0.0.4
Private IP address (IPv6)	-
Virtual network/subnet	CyberSightVM-vnet/default
DNS name	Configure

Size

Size	Standard D2s v3
vCPUs	2
RAM	8 GiB

Disk

OS disk	CyberSightVM
Encryption at host	Disabled
Azure disk encryption	Not enabled

Availability + scaling

Windows Defender

12. Enable Just in Time access:

- Search for "Microsoft Defender for Cloud" in the Azure Portal and select the service.
- Select your Azure Subscription and enable all Microsoft Defender for Cloud Plans.
- Navigate to Workload Protections > Just in time VM access and enable JIT on VM.

Virtual machines

Configured Not Configured Unsupported

VMs for which the just-in-time VM access control is already in place. Presented data is for the last week.

1 VMs Request access				
Search to filter items...				
Virtual machine ↑↓	Approved ↑↓	Last access ↑↓	Connection details	Last user ↑↓
<input checked="" type="checkbox"/> CyberSightVM	3 Requests	24-03-08, 1:53 p.m.	Ports: 3389	m_samros Request access

Setting up Just-In-Time, Networking Security Groups Access (Firewall Rules)

13. Use default Just in Time settings and click save.

14. In VM settings, click Connect > My IP as Source IP Request Access > Request access.

Connecting using
Public IP address

Admin username : twy

Port (change) : 3389 [Check access](#)

Just-in-time policy (configure) : Configured for port 3389 [Request access](#)

Most common

Local machine

Native RDP
Connect via native RDP without any additional software needed. Recommended for testing only.
Public IP address

[Select](#) [Download RDP file](#) [Heart icon](#)

Create Log Analytics Workspace and Deploy Sentinel

15. Create a Log Analytics Workspace:

- Search for "Microsoft Sentinel" in the Azure Portal.
- Create a Log Analytics Workspace using the same resource group as the Azure Virtual Machine.
- Click "review and create" to create the Log Analytics Workspace.

Home > Log Analytics workspaces >

CyberSightWorkspace

Log Analytics workspace

Search Delete

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Logs
- Settings
- Tables
- Agents
- Usage and estimated costs
- Data export
- Network isolation
- Linked storage accounts
- Properties
- Locks
- Classic
- Legacy agents management
- Legacy activity log connector
- Legacy storage account logs
- Legacy computer groups
- Legacy solutions
- System center
- Workspace summary (deprecated)

Essentials

Resource group (move) : [cyber_sight_lab](#)

Status : Active

Location : East US

Subscription (move) : [Azure subscription 1](#)

Subscription ID :

Tags (edit) : [Add tags](#)

Workspace Name : CyberSightWorkspace

Workspace ID :

Pricing tier : Pay-as-you-go

Access control mode : Use resource or workspace permissions

Operational issues : [OK](#)

Get Started Recommendations

Get started with Log Analytics

Log Analytics collects data from a variety of sources and uses a powerful query language to give you insights into the operation of your applications and resources. Use Azure Monitor to access the complete set of tools for monitoring all of your Azure resources.

- 1 Connect a data source**
Select one or more data sources to connect to the workspace
[Azure virtual machines \(VMs\)](#)
[Windows and Linux Agents management](#)
[Storage account log](#)
[System Center Operations Manager](#)
- 2 Configure monitoring solutions**
Add monitoring solutions that provide insights for applications and services in your environment
[View solutions](#)
- 3 Monitor workspace health**
Create alerts to proactively detect any issue that arise in your workspace
[Learn more about monitor workspace health](#)

Useful links

[Documentation site](#)
[Community](#)

Maximize your Log Analytics experience

- Search and analyze logs**
Use Log Analytics rich query language to analyze logs
[View logs](#)
- Manage alert rules**
Notify or take action in response to important information in your data
- Manage usage and costs**
Understand your usage of Log Analytics and estimate your costs for each month
- Create and Share Workbooks**
Use Workbooks to create rich interactive reports with your data
[Create Workbooks](#)

16. Deploy Azure Sentinel:

- Search for "Sentinel" in the Azure Portal.
- Scroll to the bottom of the page and select Add.

Home > Microsoft Sentinel >

Microsoft Sentinel | Overview (Preview)

Selected workspace: 'cybersightworkspace'

Search Refresh

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

You are currently viewing the new overview experience; you can always switch back to old one ☒ New overview

Incidents (0)

Last 24 hours

No incidents found

See incidents page for further information

[Incidents](#)

Automation

Last 24 hours

No automation rules found

Add automation rules to centrally manage automation of incident handling and response

[Automation](#)

Data

Last 24 hours

Data received

Data connectors

Unhealthy connectors: 0

Active connectors: 2

TI by type (0)

Analytics

Current status

2 Analytics rules

0 Disabled

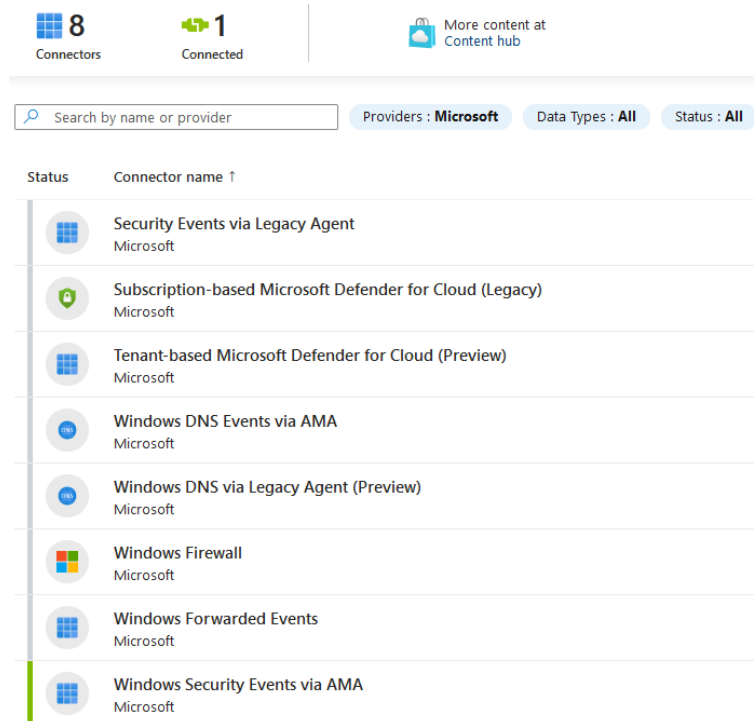
0 Auto disabled

Part 2: Getting Data into Sentinel

After the Sentinel Deployment, navigate to the incidents tab on the left. Since there is no data being fed into Sentinel, we need to utilize data connectors and create a data collection rule to bring in data from our Windows 10 VM.

Content Hub

1. In the Search bar, type in “Windows” and select Windows Security Events via AMA.
2. Click “Open Connector Page”.
3. Click “Add Data collection” listed at the bottom of the page.



4. Give your rule a name and connect it to your resource group used for all resources thus far.

Edit Data Collection Rule

Data collection rule management

Basic Resources Collect Review + create

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all of your resources.

Rule details

Rule name	SecurityEvent
Subscription ⓘ	Azure subscription 1 ▼
Resource group ⓘ	Cyber_Sight_Lab ▼

5. Click “Add resources” and select the Virtual Machine created in Step 2.
6. Select “All Security Events”.
7. Refresh the page until the “Connected” status is shown.

8. Click "Add resources".
9. Select your VM and click "Apply".
10. Click "Next".
11. Review and create.

Part 3: Remote Accessing and Generating Security Events in our VM, and Mitigating TA0003 Persistence using MITRE ATT&CK

Now that our VM is connected to Sentinel and our Log Analytics Workspace, we need to transport data from our Logs. To do this, we need to perform some action on the Windows 10 events that will generate security alerts.

Observing Windows Security Events

1. Utilize the Azure Portal to navigate to the VM created earlier in the lab.
2. Click on the virtual machine.
3. Click "Start" at the top page if it's not on already.
4. Enable Just in Time Access if necessary.
5. Use RDP on your PC Client such as Remote Desktop Connection to access your VM by entering the public IP address.
6. Enter the username and password created when you made the VM.
7. Open Event Viewer and navigate to "Security" to observe the event 4624.
8. We see that 4624 ID is indicative of a successful logon.



Part 4: Writing a KQL Query

1. In Azure Sentinel, click "Logs" on the main page.
2. In the section where it says, "Type your query", use the following logic to list out the successful logons:

```
SecurityEvent
| where EventID == 4624
| project TimeGenerated, Computer, AccountName
```

The screenshot shows the Microsoft Sentinel Logs interface. On the left is a navigation pane with categories like General, Threat management, Content management, and Configuration. The main area displays a query editor with the following KQL query:

```

1 SecurityEvent
2 | where EventID == 4624
3 | project TimeGenerated, Computer, AccountName
  
```

Below the query editor, the 'Results' tab shows a table of data. The first column is 'TimeGenerated [UTC]' and the second is 'Computer'. The results show multiple entries for 'CyberSightVM' with various timestamps from 2024-03-08.

Part 5: Writing Analytic Rule and Generating Scheduled Task

We can set up analytic rules to be alerted to certain events.

Writing Analytic Rule

- Go to the Sentinel Home Page and click “Analytics Rules”.
- Click create at the top of the page and select the scheduled query option.
- Provide information about the alert to the analyst.
- Set the alert logic using the following query:

```

SecurityEvent
| where EventID == 4698
| parse EventData with * '<Data Name="SubjectUserName">' User '</Data>' *
| parse EventData with * '<Data Name="TaskName">' NameofSceuduledTask '</Data>' *
| parse EventData with * '<Data Name="ClientProcessId">' ClientProcessID '</Data>' *
| project Computer, TimeGenerated, ClientProcessID, NameofSceuduledTask, User
  
```

The screenshot shows the Microsoft Sentinel Analytics Rules page. At the top, there's a toolbar with buttons like 'Create', 'Refresh', 'Analytics workbooks', 'Rule runs (Preview)', 'Enable', 'Disable', 'Delete', 'Import', 'Export', 'Columns', and 'Guides & Feedback'. Below this, there's a section for 'Active rules' showing 2 rules. A 'Rules by severity' bar chart shows 1 High, 1 Medium, 0 Low, and 0 Informational rules. The main table lists the rules:

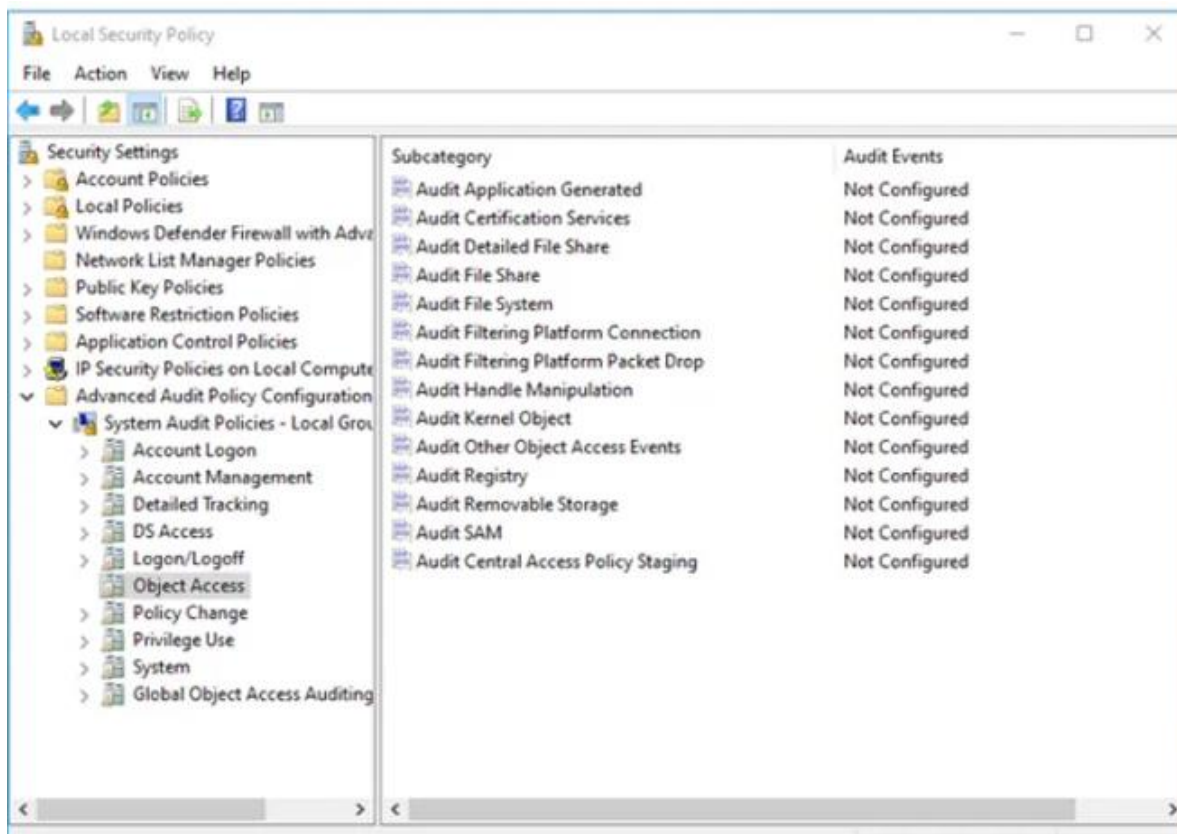
Severity	Name	Rule type	Status	Tactics	Techniques	Source name	Last modified ↓
Medium	Detect Successful Logon attempts	Scheduled	Enabled			Custom Content	2024-03-08, 2:53:55 p.m.

Part 6: Scheduled Task and Persistence Techniques

The final part is to create a custom rule to detect potentially malicious activity on our VM.

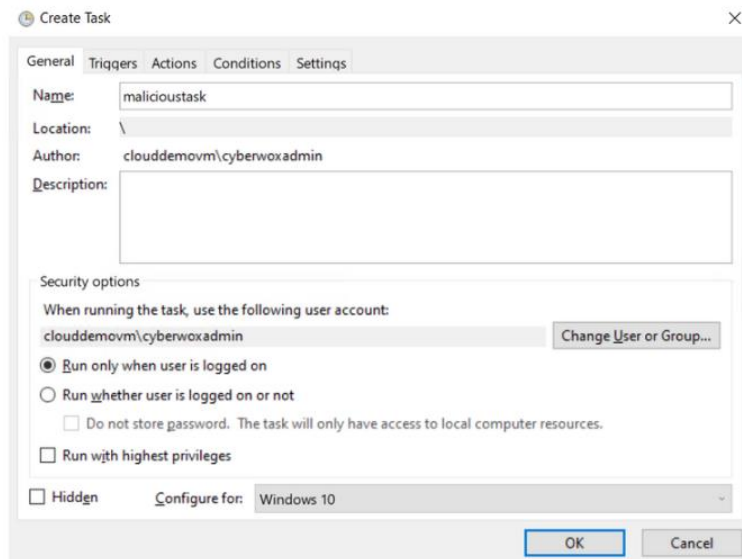
Enable Logging on Windows 10 VM:

1. Search for “Local Security Policy” in Windows 10 VM and expand “Advanced Audit Policy Configuration”
2. Expand “System Audit Policies” and “Select Object Access”. Then select the “Audit Other Object Access”
3. Enable “Success” and “Failure”.
4. Logging is now enabled for the scheduled task event.



Creating our scheduled task

1. To detect a scheduled task creation, some activity must be generated in the VM.
2. Open Windows Task Scheduler and navigate to “Create Task”. Add a name and change the “Configure For” Operating system to Windows 10.



3. Navigate to triggers and click “new” and schedule the task for a time close to your current time. Then select “OK”
4. Navigate to the action tab and select start a program.
5. Then open program or script and select a program to run every time this task runs. I will select **Internet Explorer**.
6. Keep the default settings and click “OK”.

Part 7: MITRE ATT&CK

Detection

As observed. monitoring and logging of specific windows event id was used to detect this activity. However, MITRE also has more recommendations for detection.

Configure event logging for scheduled task creation and changes by enabling the “Microsoft-Windows-TaskScheduler/Operational” setting within the event logging service. [154]

Several events will then be logged on scheduled task activity, including: [153][54]

- Event ID 106 on Windows 7, Server 2008 R2 - Scheduled task registered
- Event ID 140 on Windows 7, Server 2008 R2 / 4702 on Windows 10, Server 2016 - Scheduled task updated
- Event ID 141 on Windows 7, Server 2008 R2 / 4699 on Windows 10, Server 2016 - Scheduled task deleted
- Event ID 4698 on Windows 10, Server 2016 - Scheduled task created
- Event ID 4700 on Windows 10, Server 2016 - Scheduled task enabled

The observed MITRE ATT&CK tactic used in this lab is Persistence.
We can learn more about this technique by using a scheduled Task/Job.

Home > Techniques > Enterprise > Scheduled Task/Job > Scheduled Task

Scheduled Task/Job: Scheduled Task

Other sub-techniques of Scheduled Task/Job (7)

Adversaries may abuse the Windows Task Scheduler to perform task scheduling for initial or recurring execution of malicious code. There are multiple ways to access the Task Scheduler in Windows. The `schtasks` can be run directly on the command line, or the Task Scheduler can be opened through the GUI within the Administrator Tools section of the Control Panel. In some cases, adversaries have used a .NET wrapper for the Windows Task Scheduler, and alternatively, adversaries have used the Windows `netapi32` library to create a scheduled task.

The deprecated `at` utility could also be abused by adversaries (ex: `At (Windows)`), though `at.exe` can not access tasks created with `schtasks` or the Control Panel.

An adversary may use Windows Task Scheduler to execute programs at system startup or on a scheduled basis for persistence. The Windows Task Scheduler can also be abused to conduct remote Execution as part of Lateral Movement and/or to run a process under the context of a specified account (such as `SYSTEM`).

ID: T1053.005

Sub-technique of: T1053

- Tactics: Execution, Persistence, Privilege Escalation
- Platforms: Windows
- Permissions Required: Administrator
- Supports Remote: Yes

Version: 1.0

Created: 27 November 2019

Last Modified: 30 December 2020

[Version Permalink](#)

Mitigation

Additionally, we can delve deeper into the specific sub-technique labeled T1053.005. According to MITRE ID M1019, it is recommended that user account privileges be restricted to authorized administrators only, allowing them to create scheduled tasks on remote systems.

Mitigations

ID	Mitigation	Description
M1047	Audit	Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for permission weaknesses in scheduled tasks that could be used to escalate privileges. ^[150]
M1028	Operating System Configuration	Configure settings for scheduled tasks to force tasks to run under the context of the authenticated account instead of allowing them to run as SYSTEM. The associated Registry key is located at HKLM\SYSTEM\CurrentControlSet\Control\LSA\SubmitControl. The setting can be configured through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > Security Options: Domain Controller: Allow server operators to schedule tasks, set to disabled. ^[151]
M1026	Privileged Account Management	Configure the Increase Scheduling Priority option to only allow the Administrators group the rights to schedule a priority process. This can be configured through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Increase scheduling priority. ^[152]
M1018	User Account Management	Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create scheduled tasks on remote systems.

Conclusion

In conclusion, the CyberSight project has provided participants with invaluable hands-on experience and practical skills in leveraging Microsoft Sentinel and SOAR automation techniques to enhance SIEM capabilities. By completing the various parts of the lab, participants have gained proficiency in setting up Azure resources, collecting and analyzing security events, writing KQL queries, creating analytic rules, and simulating threat scenarios with scheduled tasks.

Skills Obtained:

1. **Azure Resource Management:** Participants have learned how to create and manage Azure resources, including virtual machines, resource groups, and networking configurations.
2. **Data Collection and Integration:** Skills have been developed in connecting Windows VMs to Azure Sentinel, configuring data connectors, and implementing data collection rules for comprehensive visibility of security events.
3. **Security Event Analysis:** Participants have gained proficiency in analyzing security events using tools like Event Viewer and querying logs with Kusto Query Language (KQL) to extract actionable insights.
4. **Analytic Rule Creation:** Knowledge and skills have been acquired in creating analytic rules in Azure Sentinel to detect specific security events and trigger alerts for proactive threat detection.
5. **Threat Simulation:** Through the creation of scheduled tasks and simulation of potential threat scenarios, participants have learned to identify and mitigate security risks, applying principles from the MITRE ATT&CK framework.

Overall, the CyberSight project has equipped participants with essential skills and knowledge to effectively defend against cyber threats, bolster organizational security, and advance their cybersecurity journey.