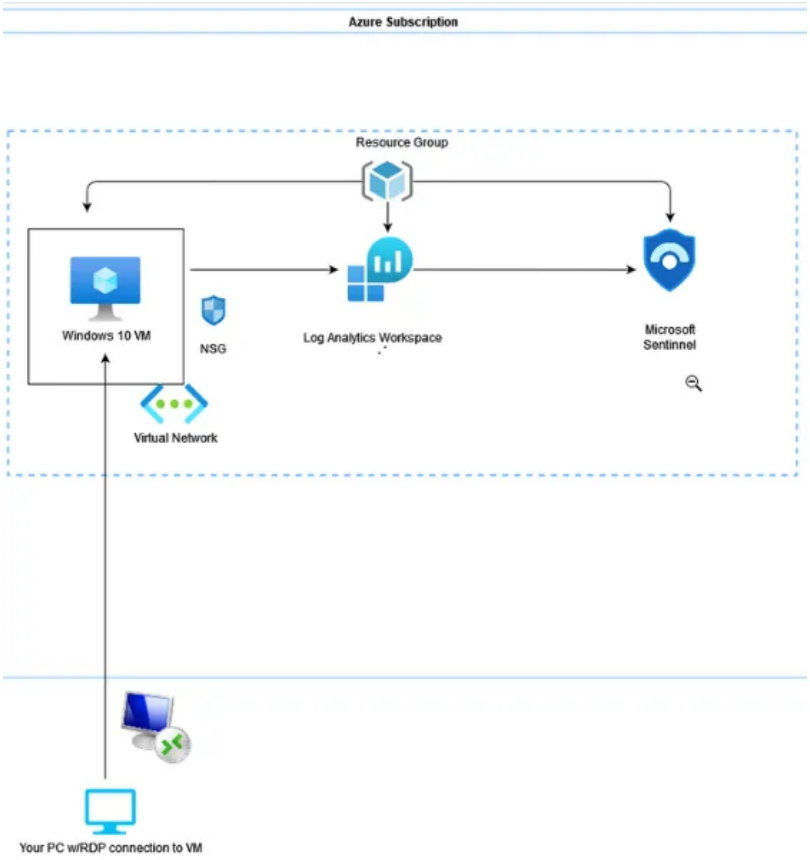
CyberSight - Enhancing SIEM with Microsoft Sentinel Detection Lab and SOAR Automation

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



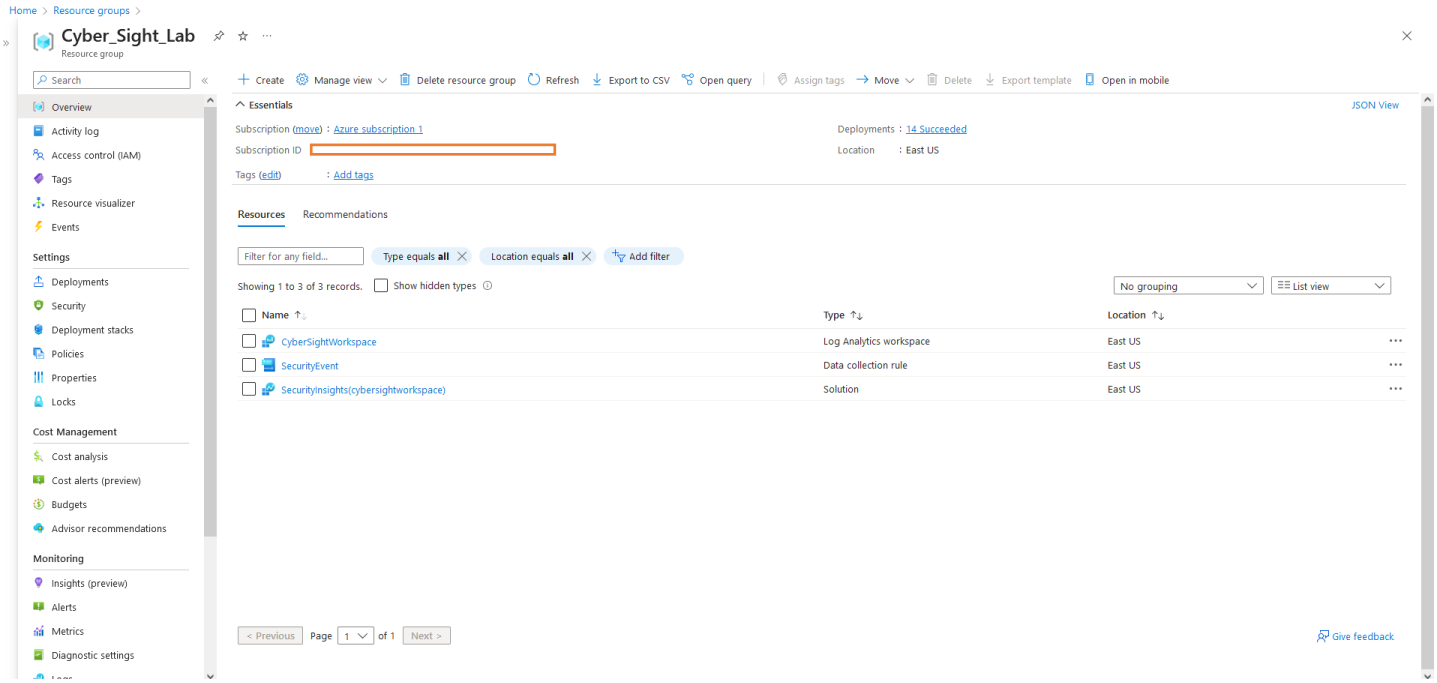
Procedure

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/

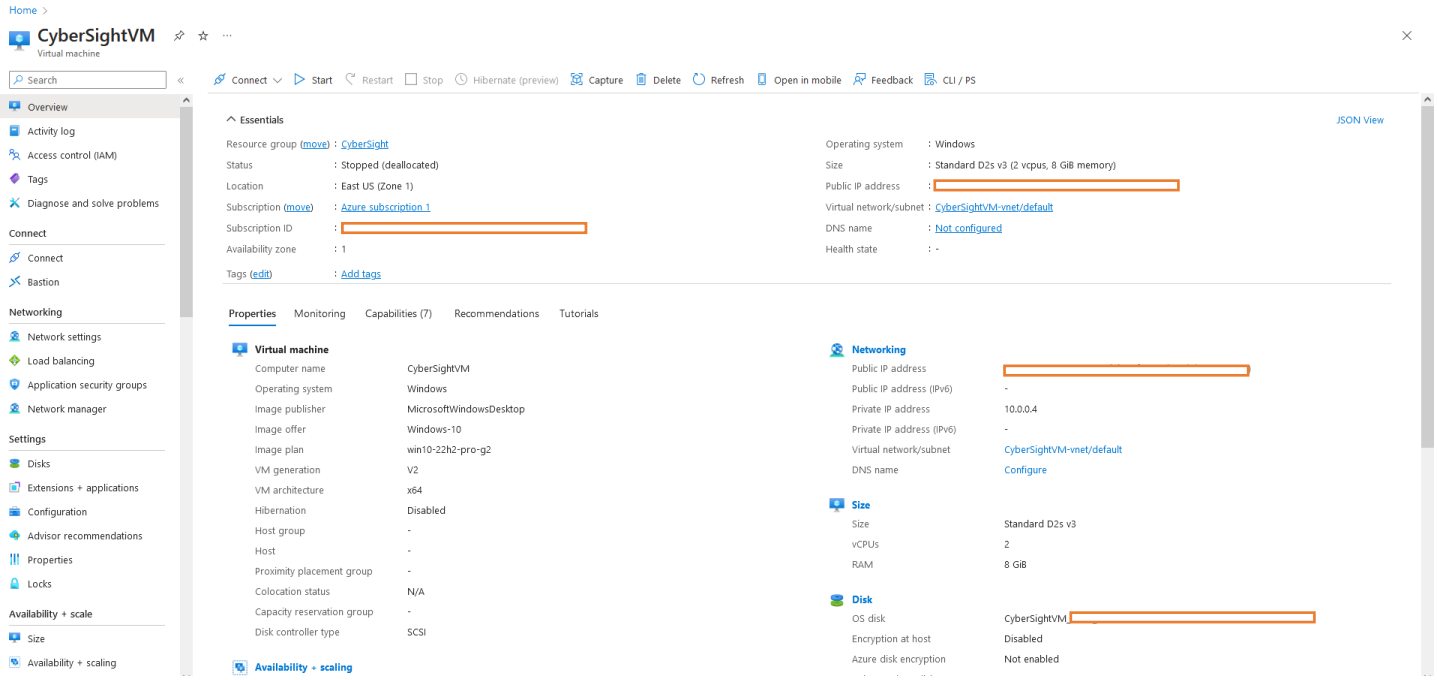
Create a Resource Group

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.



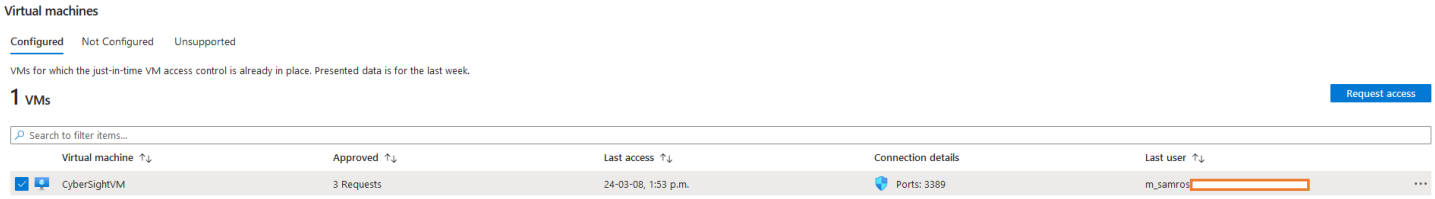
Deploy a Virtual Machine

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.



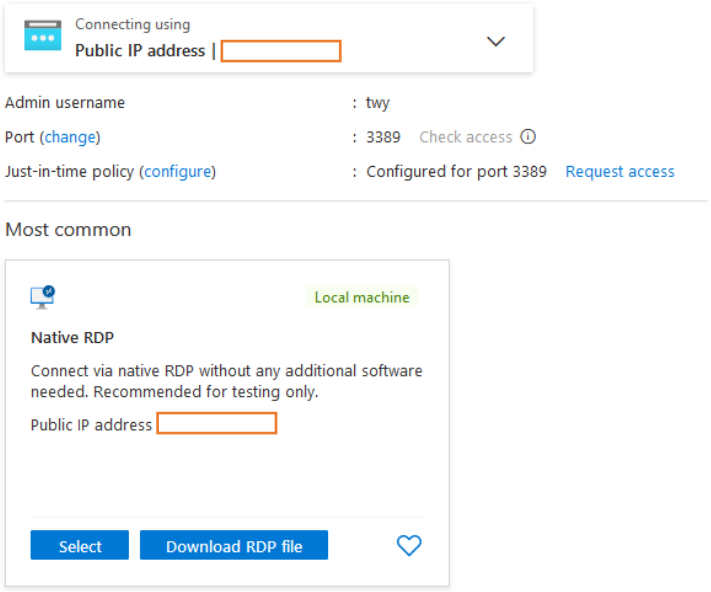
Windows Defender

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.



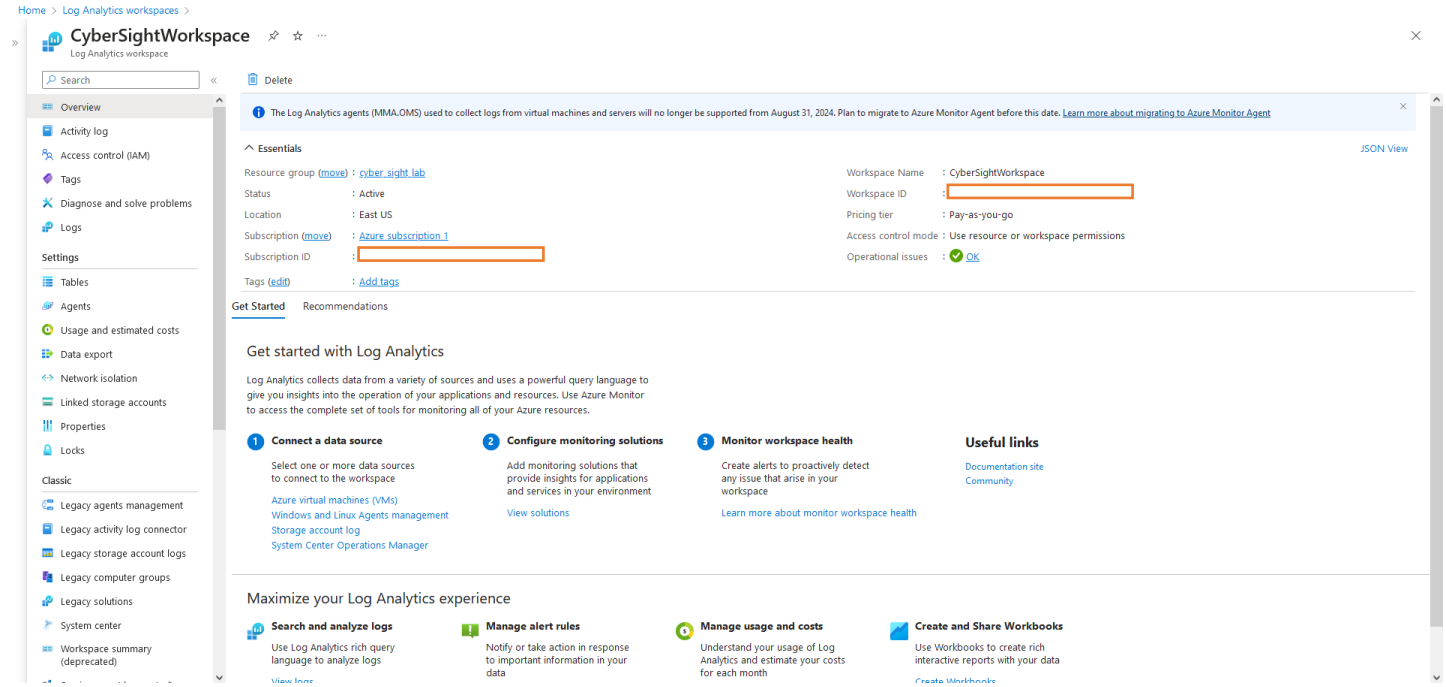
Setting up Just-In-Time, Networking Security Groups Access (Firewall Rules)

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.

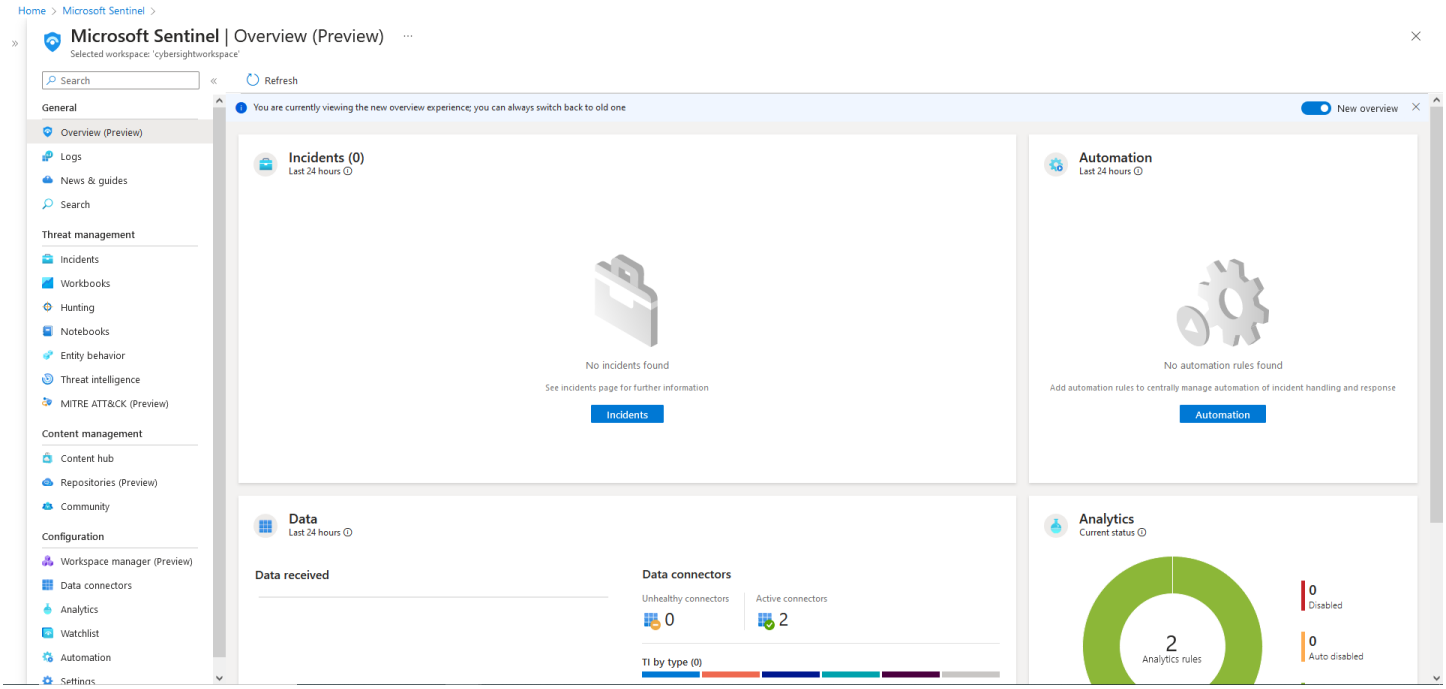


Create Log Analytics Workspace and Deploy Sentinel

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.



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

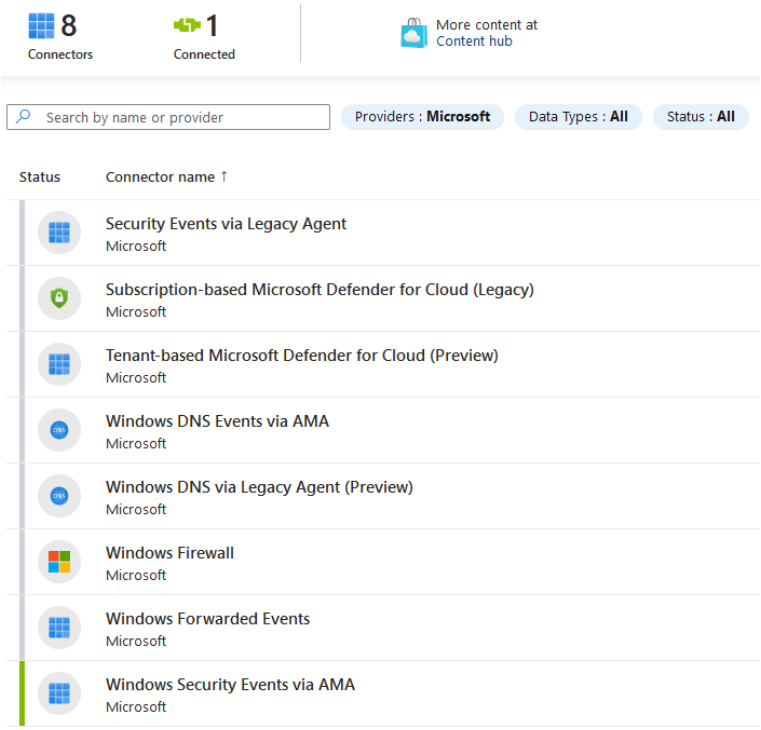


Part 2: Getting Data into Sentinel

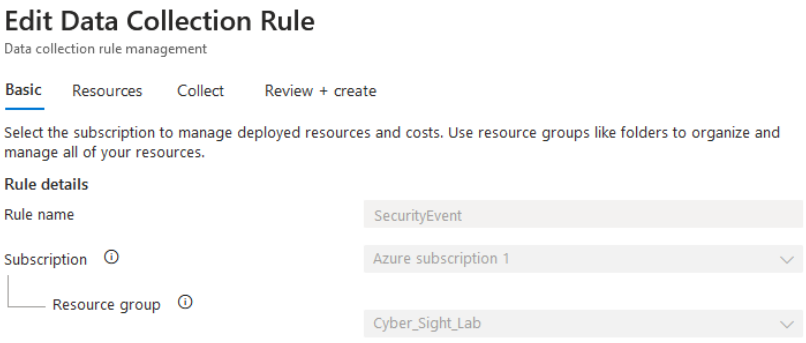
After the Sentinel Deployment, navigate to the incidents tab on the left. Since there is no data being fed into Sentinel, we need to utilize data connectors and create a data collection rule to bring in data from our Windows 10 VM.

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.



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.

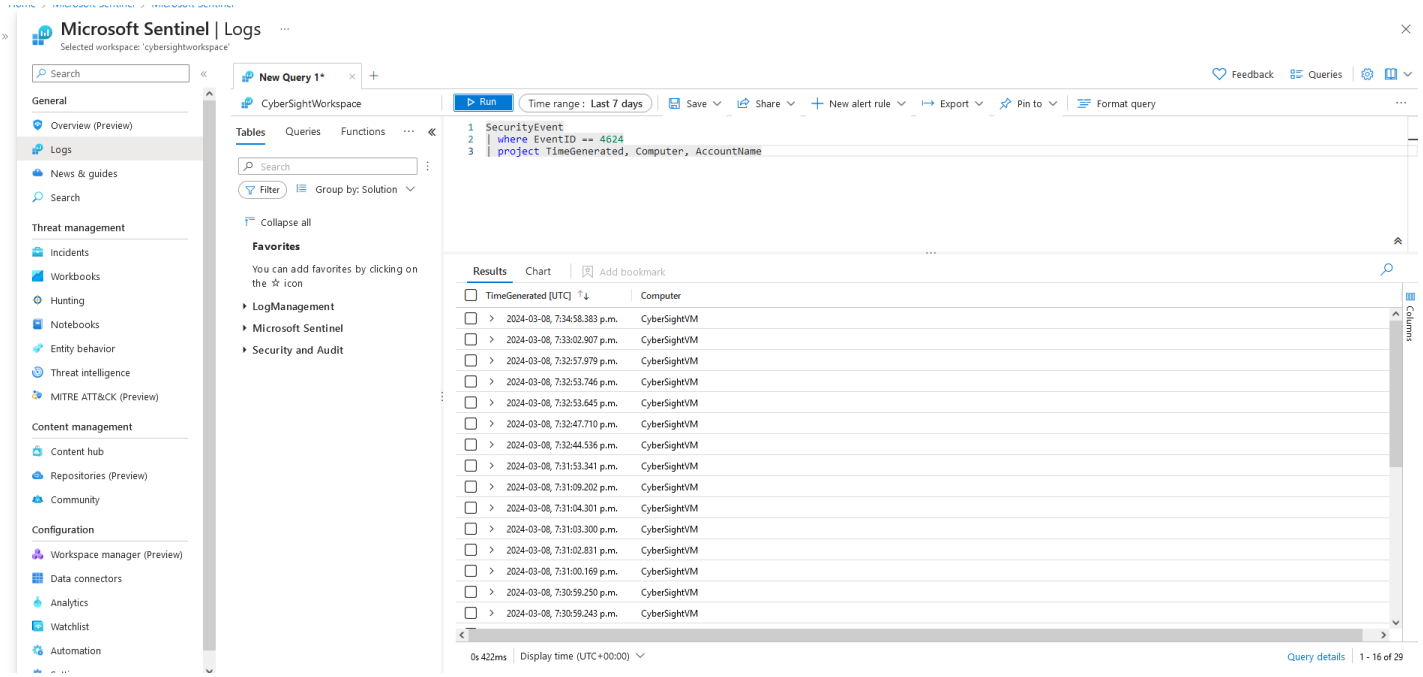
Observing Windows Security Events

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
```



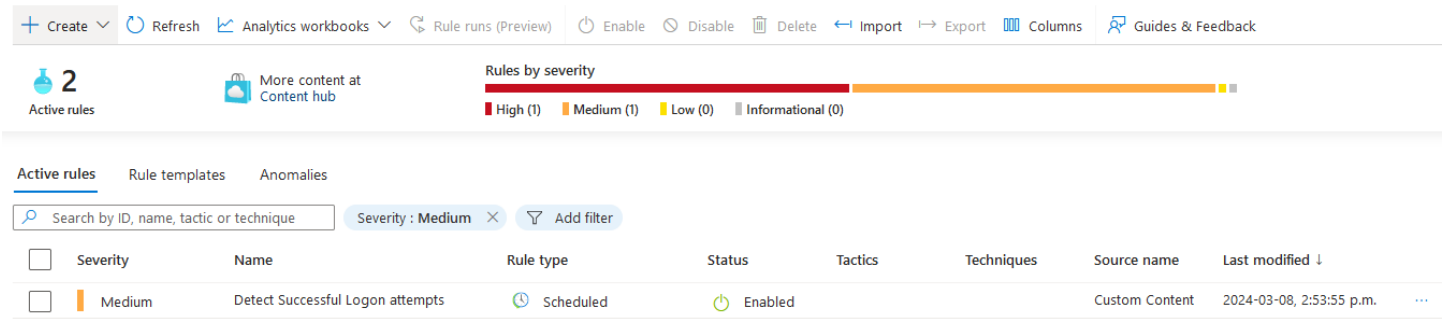
Part 5: Writing Analytic Rule and Generating Scheduled Task

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

Writing Analytic Rule

1. Go to the Sentinel Home Page and click “Analytics Rules”.
2. Click create at the top of the page and select the scheduled query option.
3. Provide information about the alert to the analyst.
4. 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
```

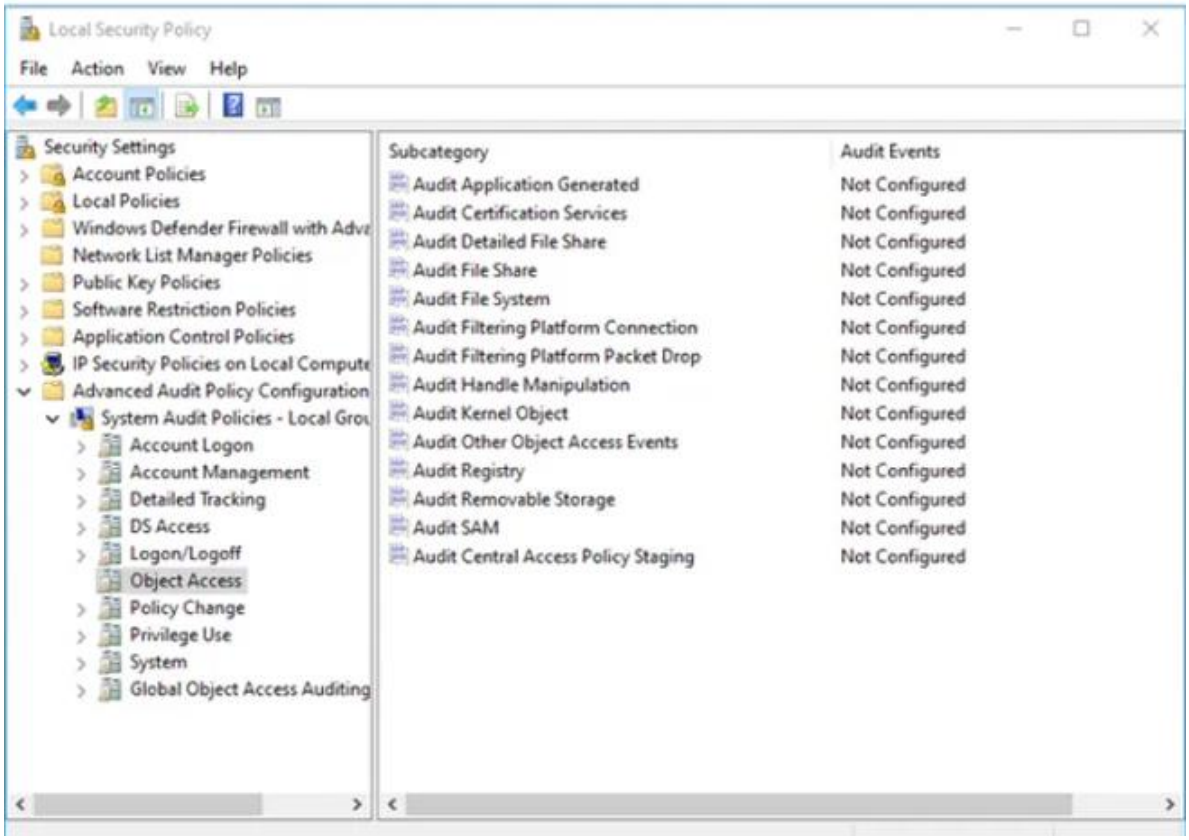


Part 6: Scheduled Task and Persistence Techniques

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

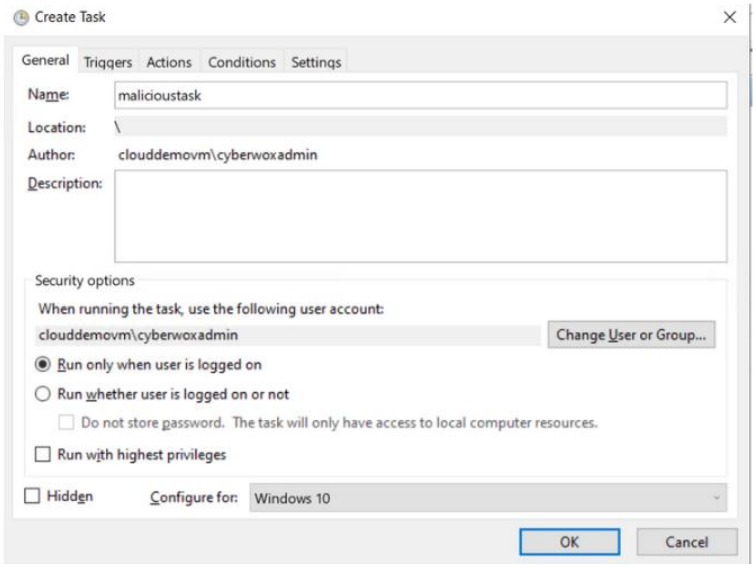
Enable Logging on Windows 10 VM:

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.*



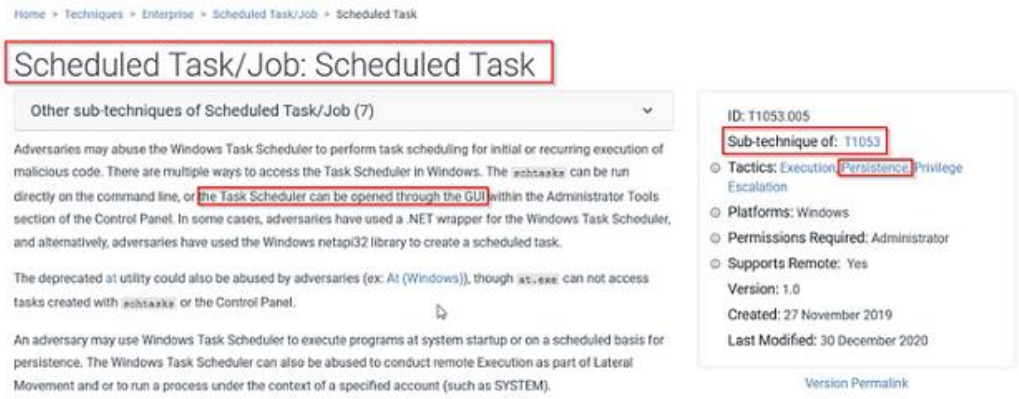
3. *Navigate to triggers and click "new" and schedule the task for a time close to your current time. Then select "OK"*
4. *Navigate to the action tap and select start a program.*
5. *Then open program or script and select a program to run every time this task runs. I will select* ***Internet Explorer.***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

Part 7: MITRE ATT&CK

Detection

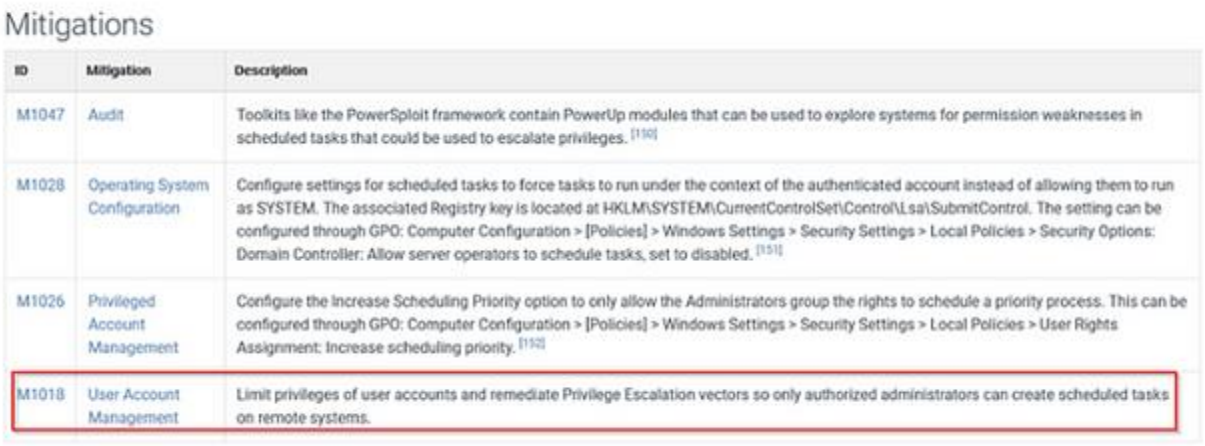
As observed. monitoring and logging of specific windows event id was used to detect this activity. However, MITRE also has more recommendations for detection.

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.



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. [110]
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. [111]
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. [112]
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.