A screenshot of a computer

Description automatically generatedMicrosoft Azure Threat Detection Lab

Published by AS on November 25,2024

Earlier in the year, I deepened my understanding of cloud computing and its core concepts. I successfully completed the Microsoft Azure Fundamentals AZ-900 exam back in April. One of the key factors that influenced my decision to opt for Azure is its integration with Microsoft Sentinel, a cutting-edge cloud-based SIEM/SOAR solution equipped with advanced intelligence tools designed to enhance security for both cloud and on-premises resources.

Presently, I’m in the process of developing my skills as a security analyst, with the goal of securing a role in defensive security operations and ultimately specializing in cloud security. Many security roles require expertise in SIEMs like Splunk and Microsoft Sentinel. Sentinel, being a unified platform encompassing security analytics, threat intelligence, threat response, and more, presents a valuable opportunity for me to gain hands-on experience, making this lab an excellent stepping stone toward my career objectives.

Getting Started

In July 2022, I registered for a Microsoft Azure free account; however, I didn’t fully utilize the $200 free credit available for the first month as I was focused on studying for my CCNA certification and honing my tech fundamentals.

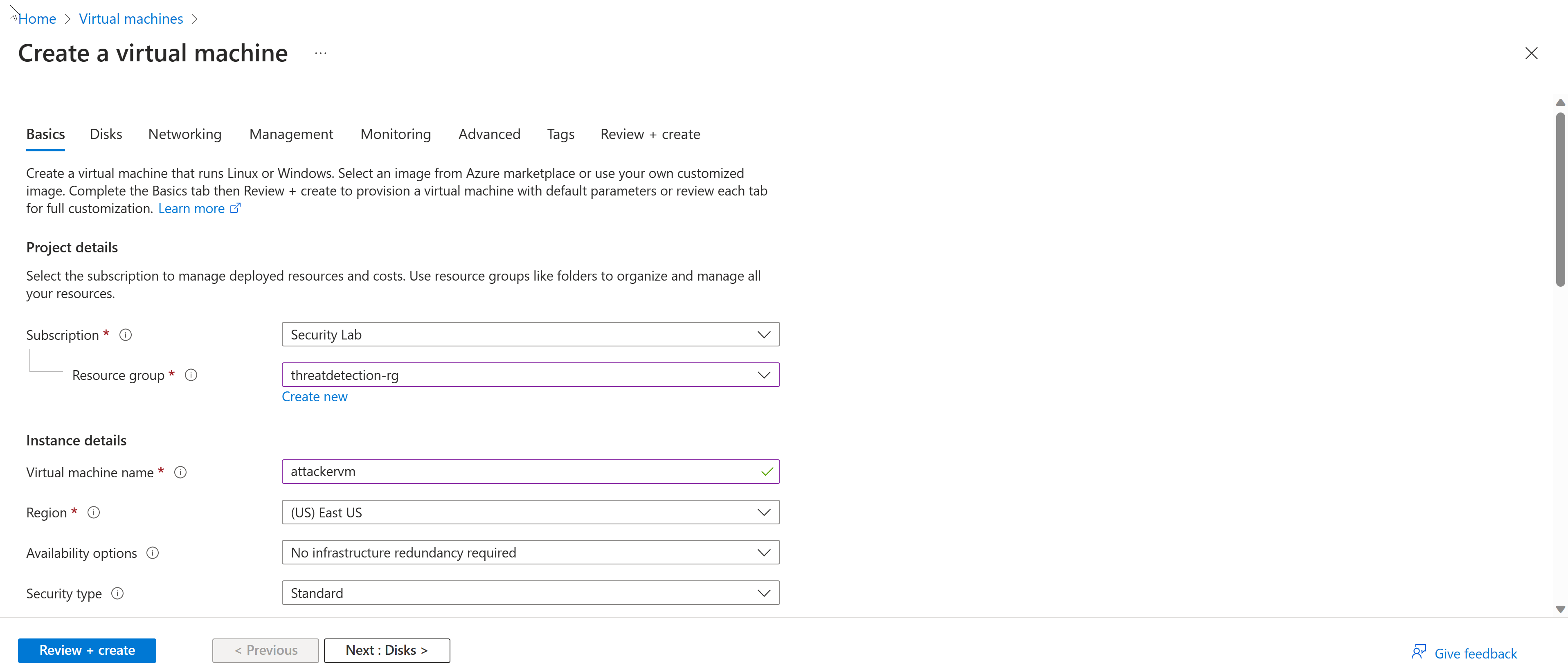
Step 1 – Create a Resource Group

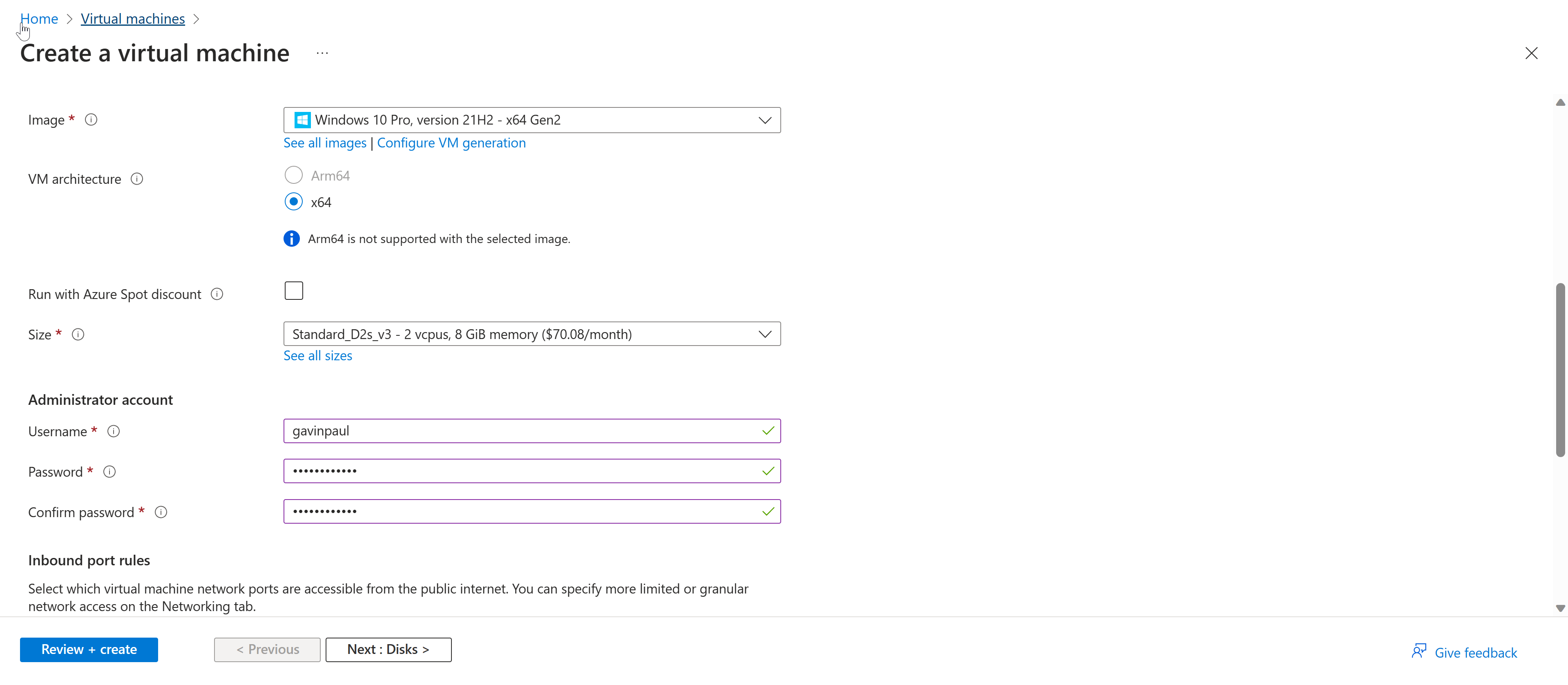
The first step was creating the resource group which will contain all of the resources that I used for this lab:

* Windows 10 Virtual Machine
* Log Analytics Workspace
* Microsoft Sentinel

Step 2 – Deploy Virtual Machine

Next, I deployed a Windows 10 Virtual Machine using the default settings.







I didn’t worry about configuring the network settings since this was just a basic lab. When a Virtual Machine is deployed in Azure it is connected to Virtual Network (VNet). I left the Remote Desktop Protocol (RDP) port open because that is how I will connect to the virtual machine. This alone isn’t recommended as threat actors actively hunt accessible machines with open management ports, like RDP or SSH. All of your virtual machines are potential targets for an attack. When a VM is successfully compromised, it’s used as the entry point to attack further resources within your environment.

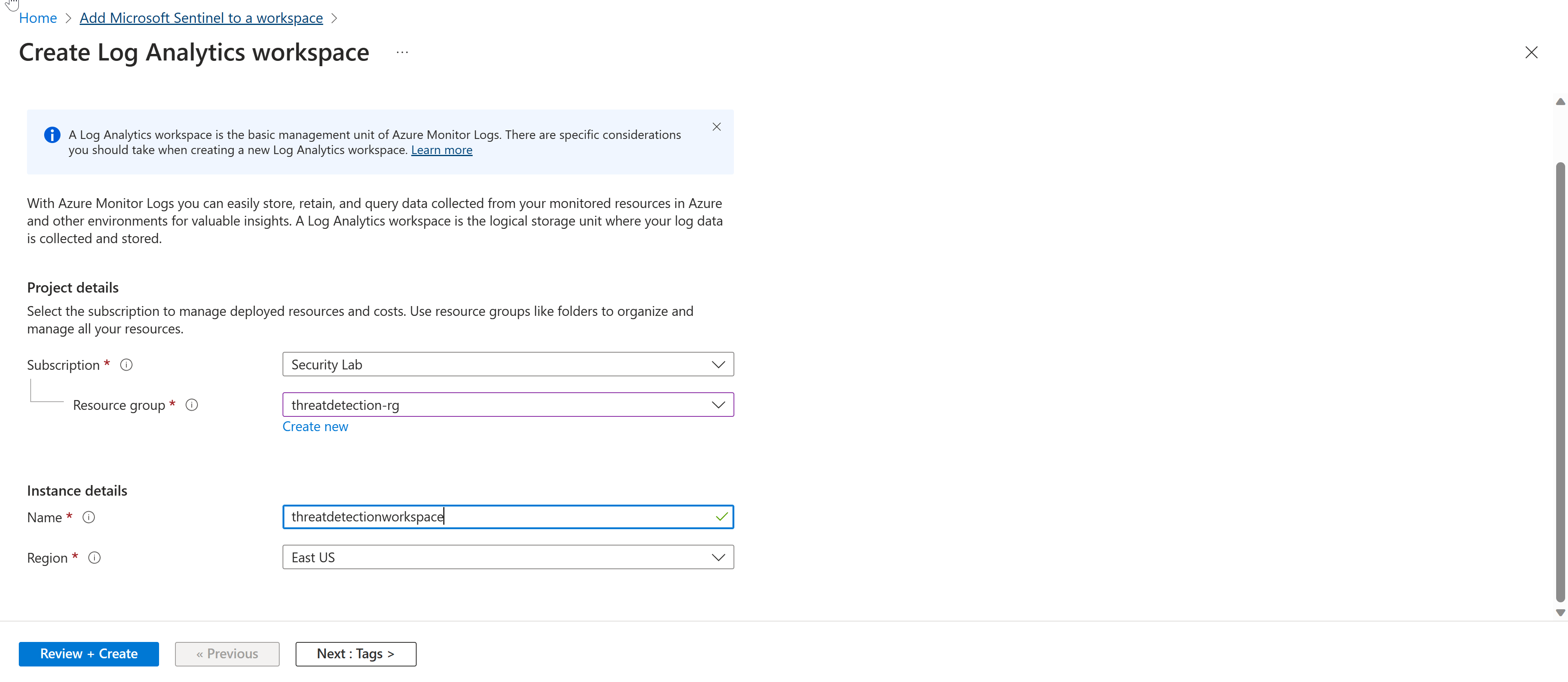
Our goal should be to reduce the attack surface. In this case, that means having fewer open ports, especially management ports. Legitimate users also use these ports, so it’s not practical to keep them closed.

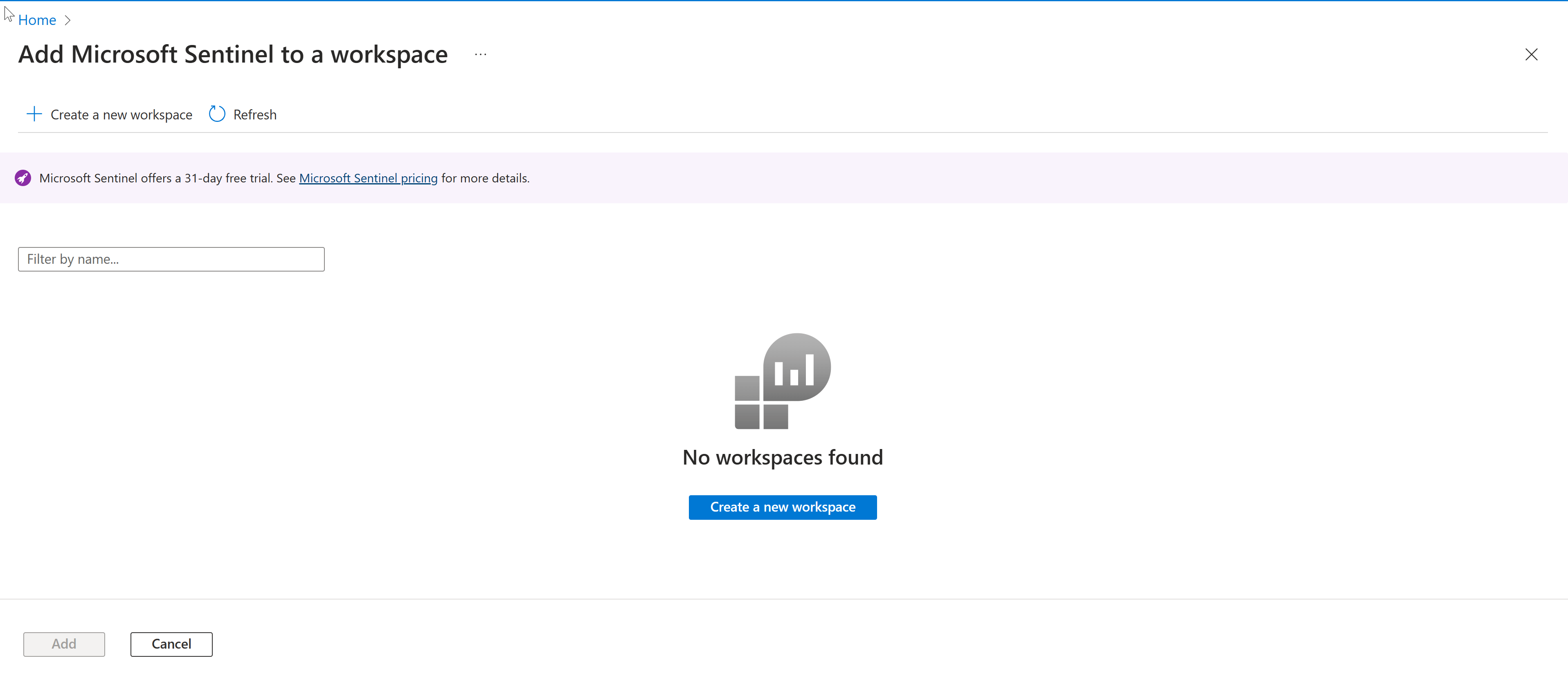
To solve this dilemma, Microsoft Defender for Cloud offers Just-In-Time (JIT). With JIT, you can lock down the inbound traffic to your VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.

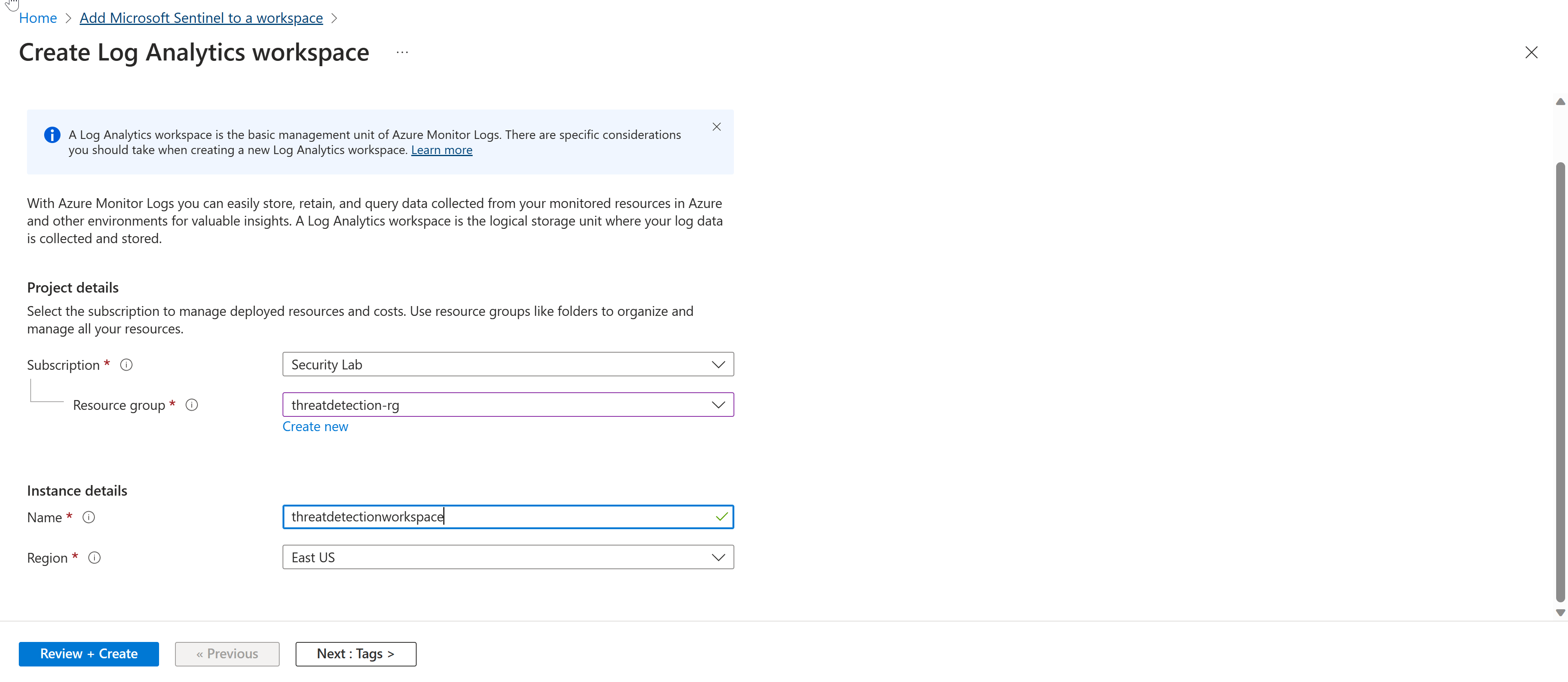
When a user requests access to a VM, Defender for Cloud checks that the user has Azure role-based access control (Azure RBAC) permissions for that VM. If the request is approved, Defender for Cloud configures the Network Security Groups (NSGs) and Azure Firewall to allow inbound traffic to the selected ports from the relevant IP address (or range), for the amount of time that was specified.

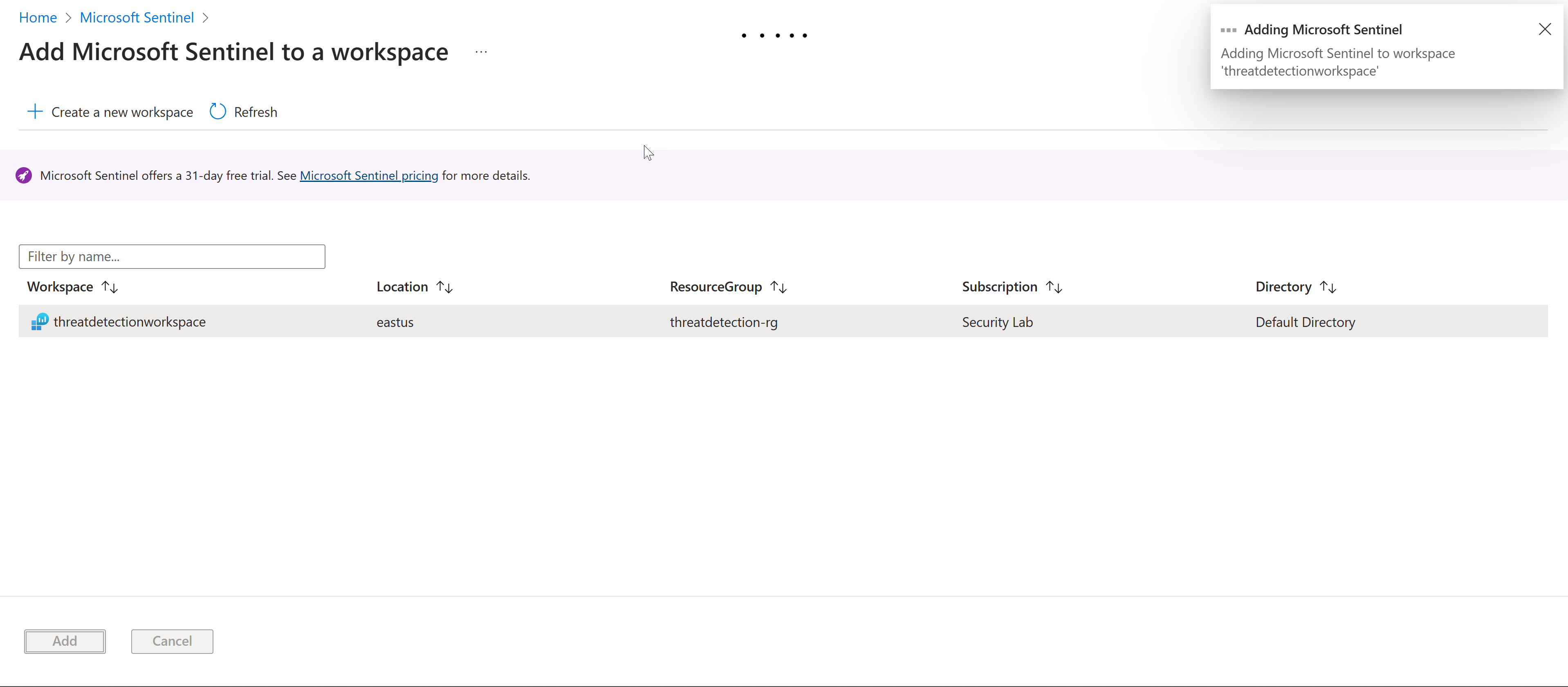
Step 3 – Creating a Log Analytics Workspace and Deploying Sentinel

When working with Log Data in Azure we need somewhere to store/operate that data. Log Analytics workspace is used to collect and store log data from Azure Resources.









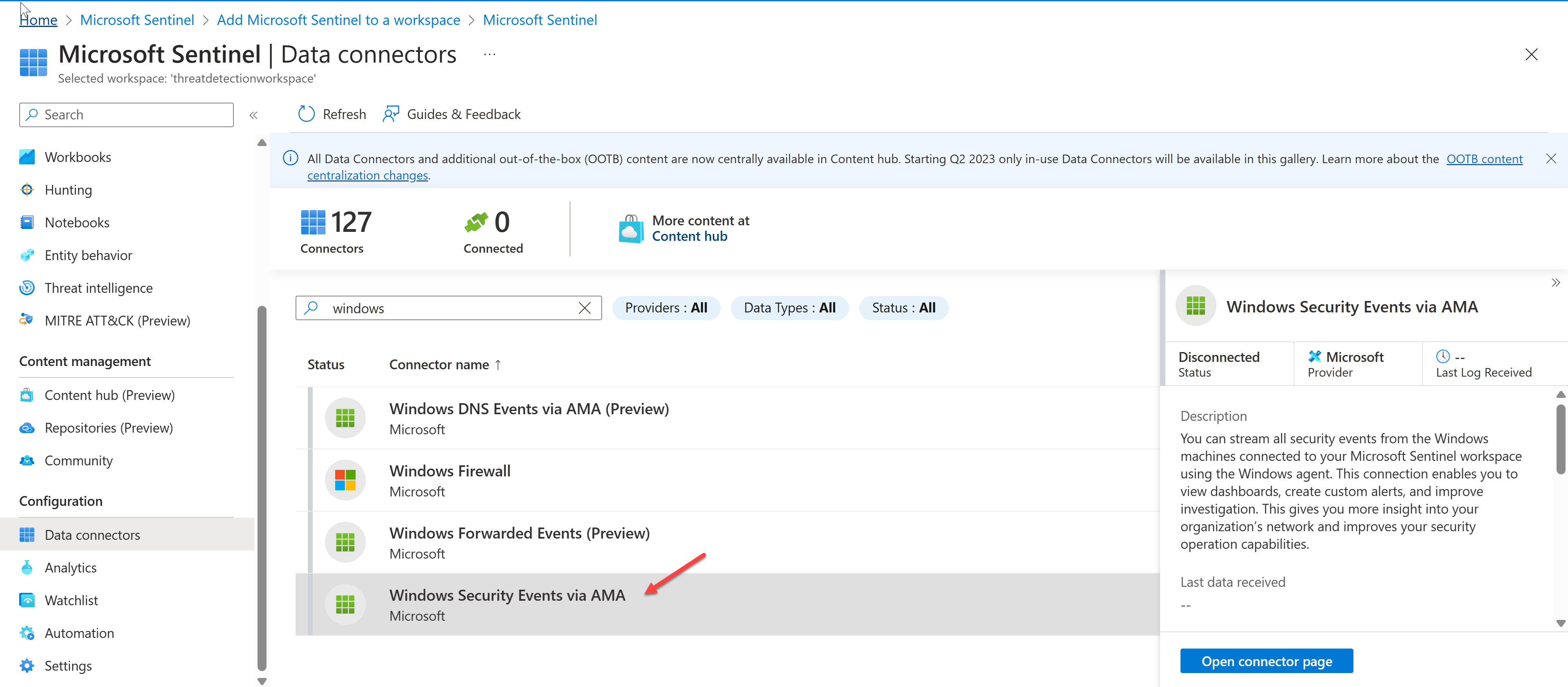
Step 4: Adding Data Connectors

Now that I’ve added Microsoft Sentinel to my log analytics workspace, I can now navigate to Microsoft Sentinel to add Microsoft Sentinel to add the data connectors to bring data into Sentinel for analysis. Azure Data Connectors are integration tools that allow you to collect, ingest, and analyze data from various sources, including cloud services, on-premises systems, and third-party platforms. They simplify the process of data ingestion into Azure services like Azure Monitor, Azure Sentinel, and Azure Logic Apps, enabling organizations to gain insights and take action on their data more efficiently.

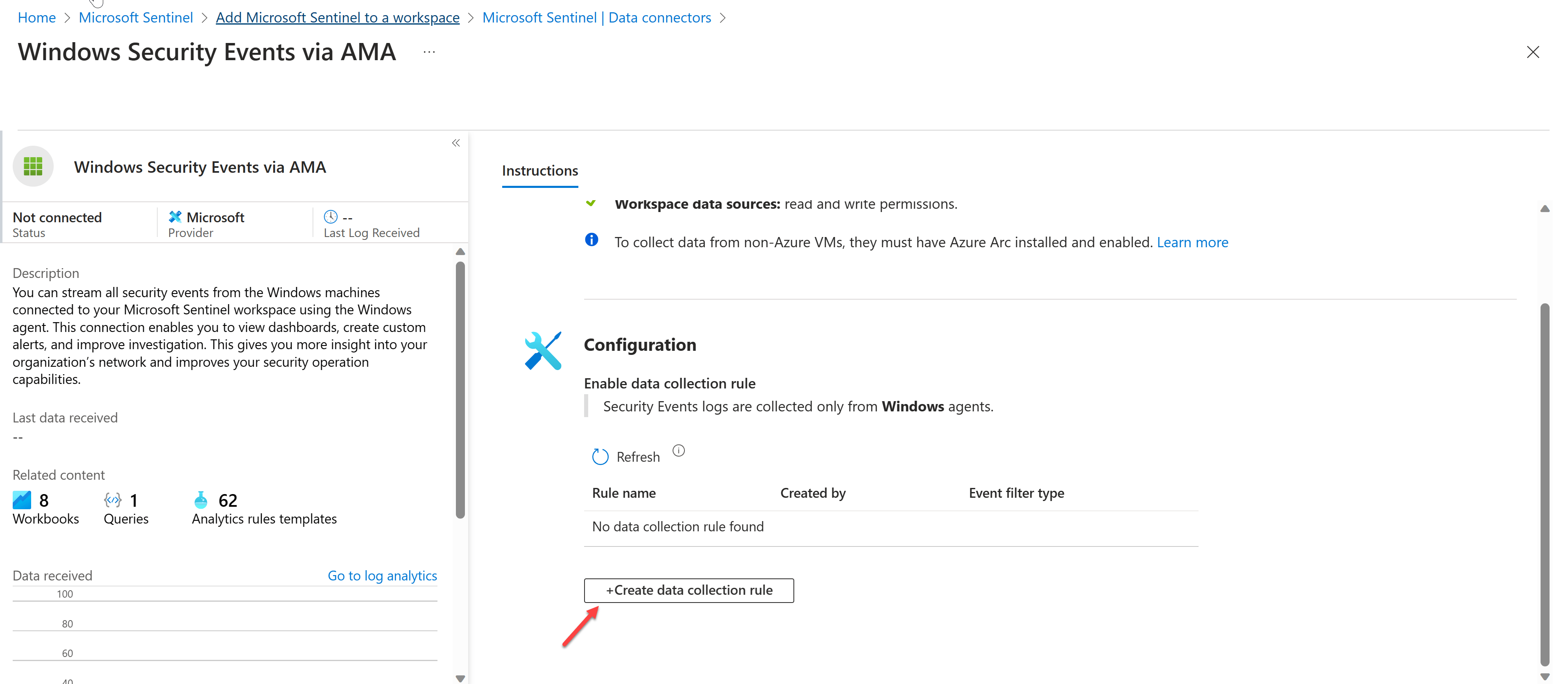
A screenshot of a computer

Description automatically generated

Typing Windows in the search box and selecting **Windows Security Events via AMA** allows you to stream all security events from the Windows 10 VM to the Microsoft Sentinel workspace.



Select **+ Create data collection rule**



Data Collection Rules specify what data should be collected, how to transform that data, and where to send that data.

A screenshot of a computer

Description automatically generated

From here I selected **+Add resource(s)**



… and added the Virtual Machine (**attackervm**) as the scope that I deployed earlier.

A screenshot of a computer

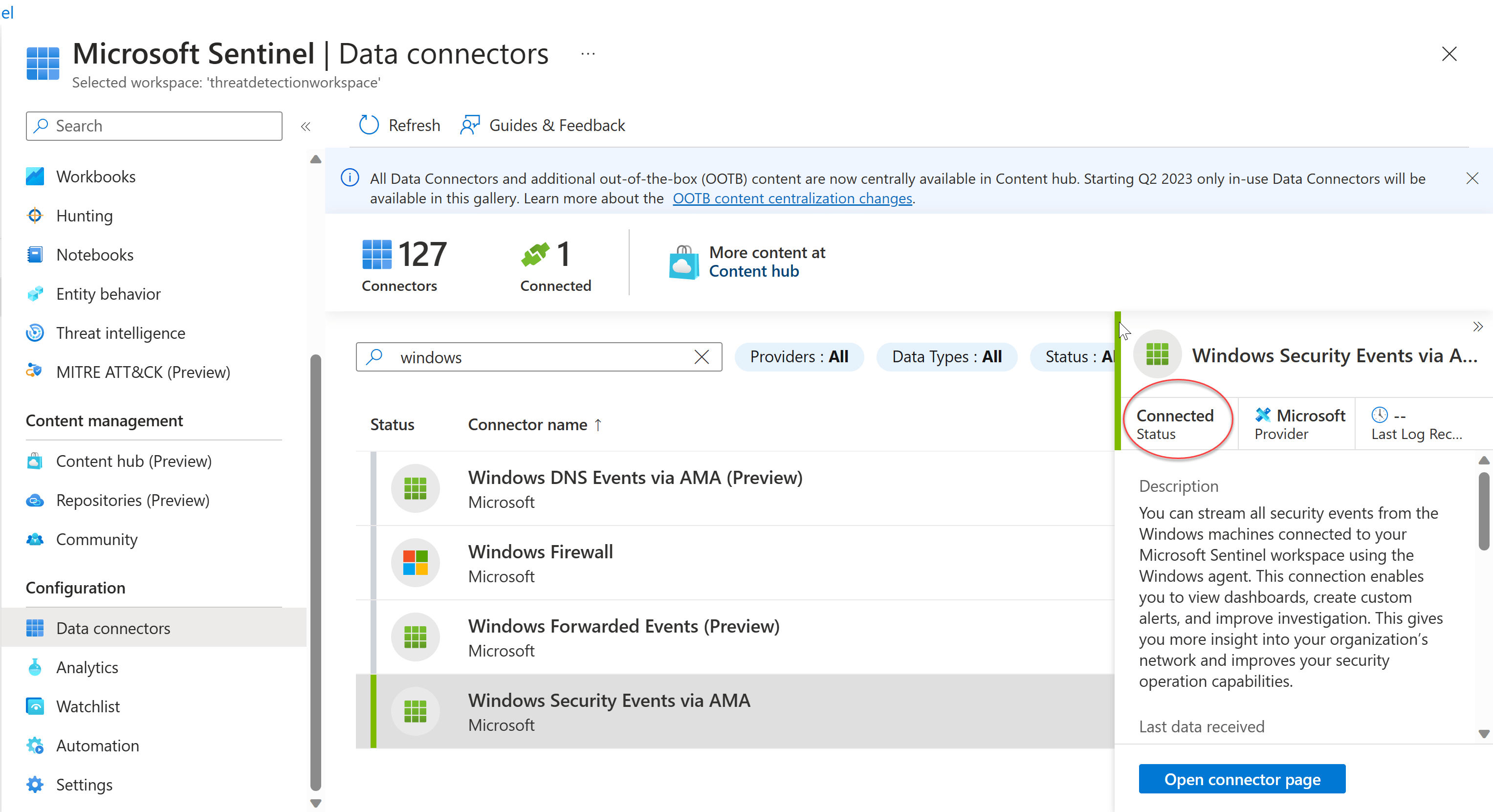
Description automatically generated

This should be the end result:

A screenshot of a computer

Description automatically generated

After navigating back to the Data Connectors page in Microsoft Sentinel you should see the status of **Connected**.



Step 5: Generating Security Events

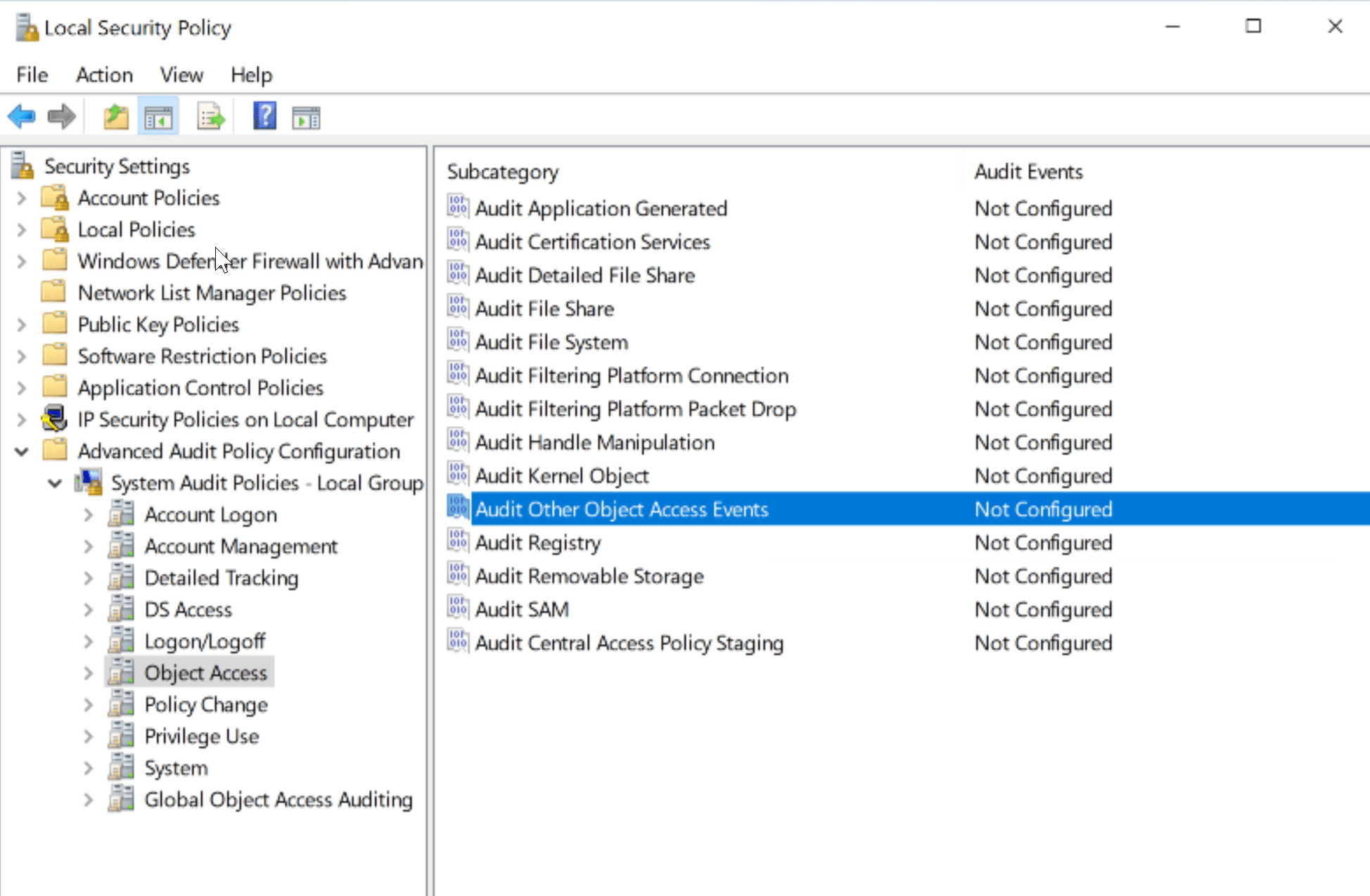
Now that the VM is connected to Sentinel and Log Analytics Workspace we need to transport data from my logs. To do this I accessed my VM via RDP to generate security events.

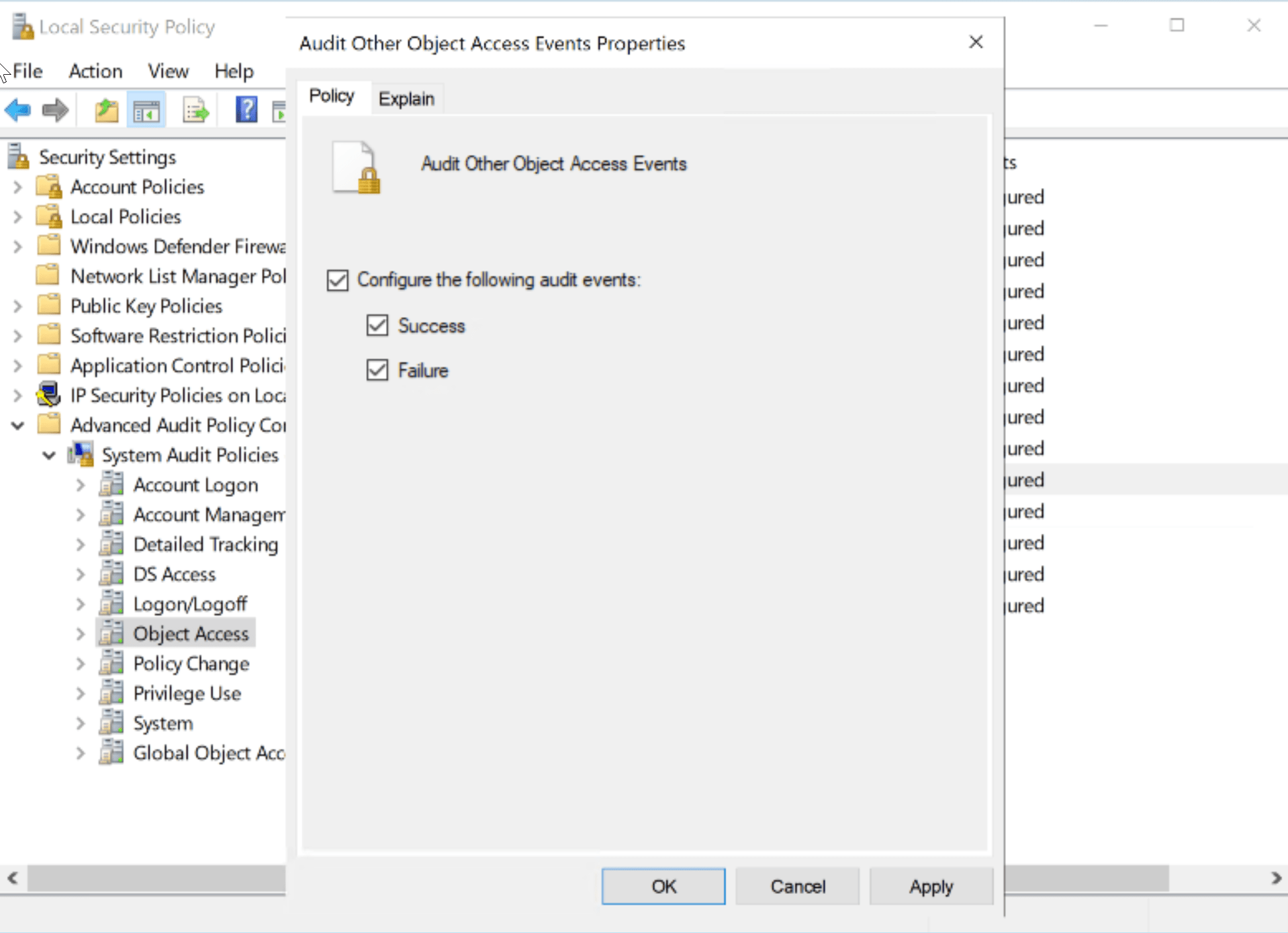
A screenshot of a computer program

Description automatically generated

A screenshot of a computer error

Description automatically generated

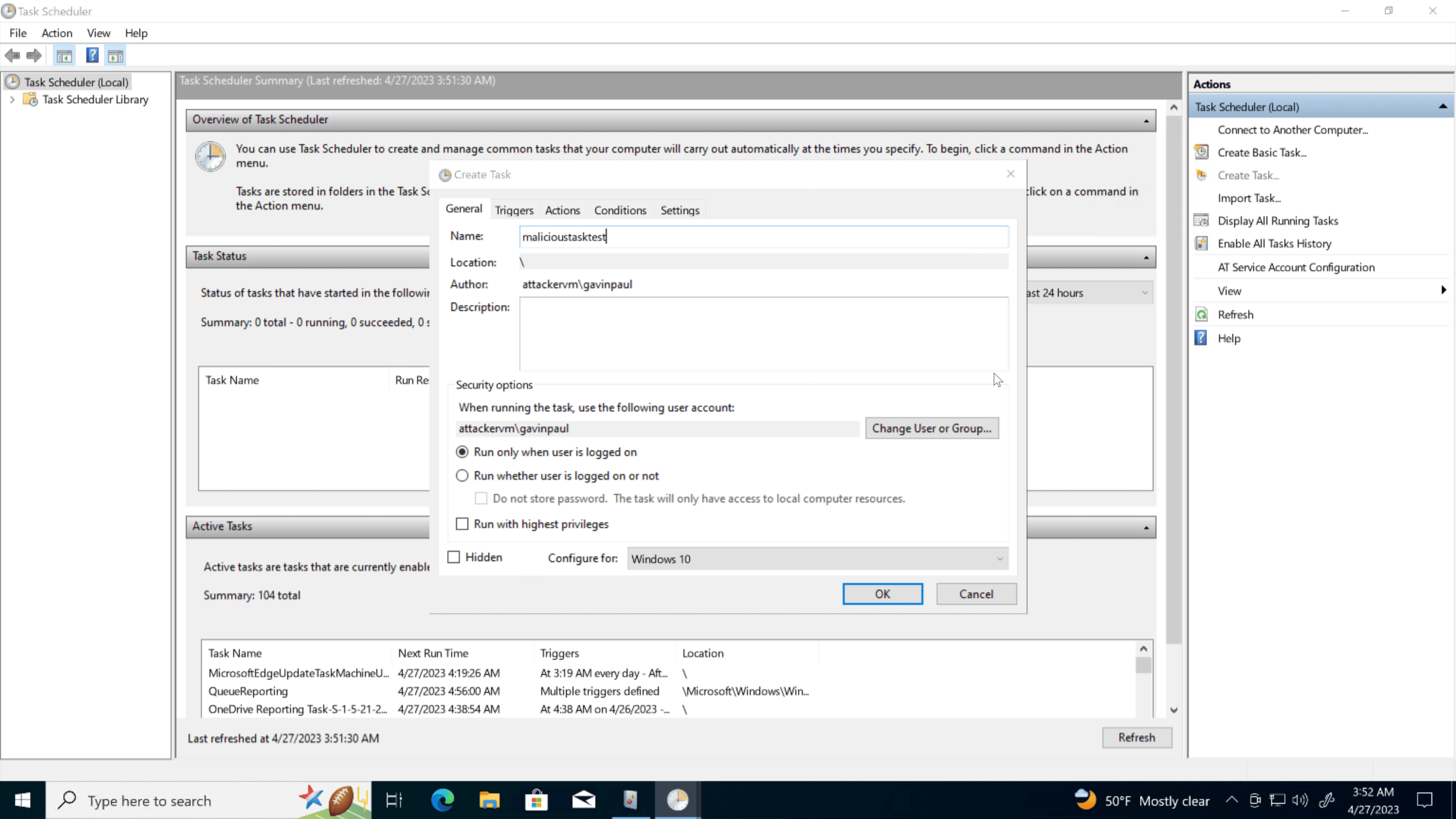


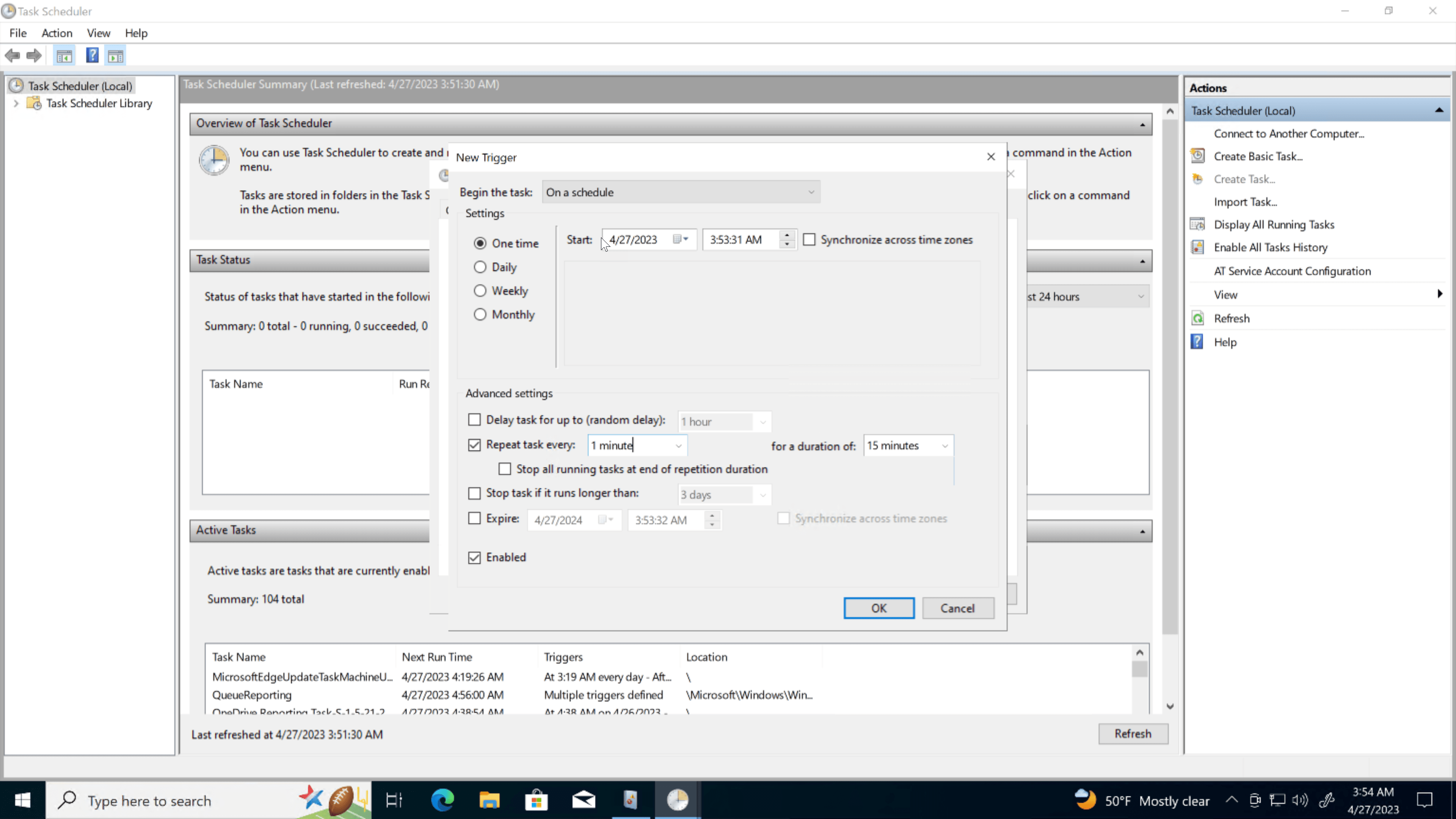


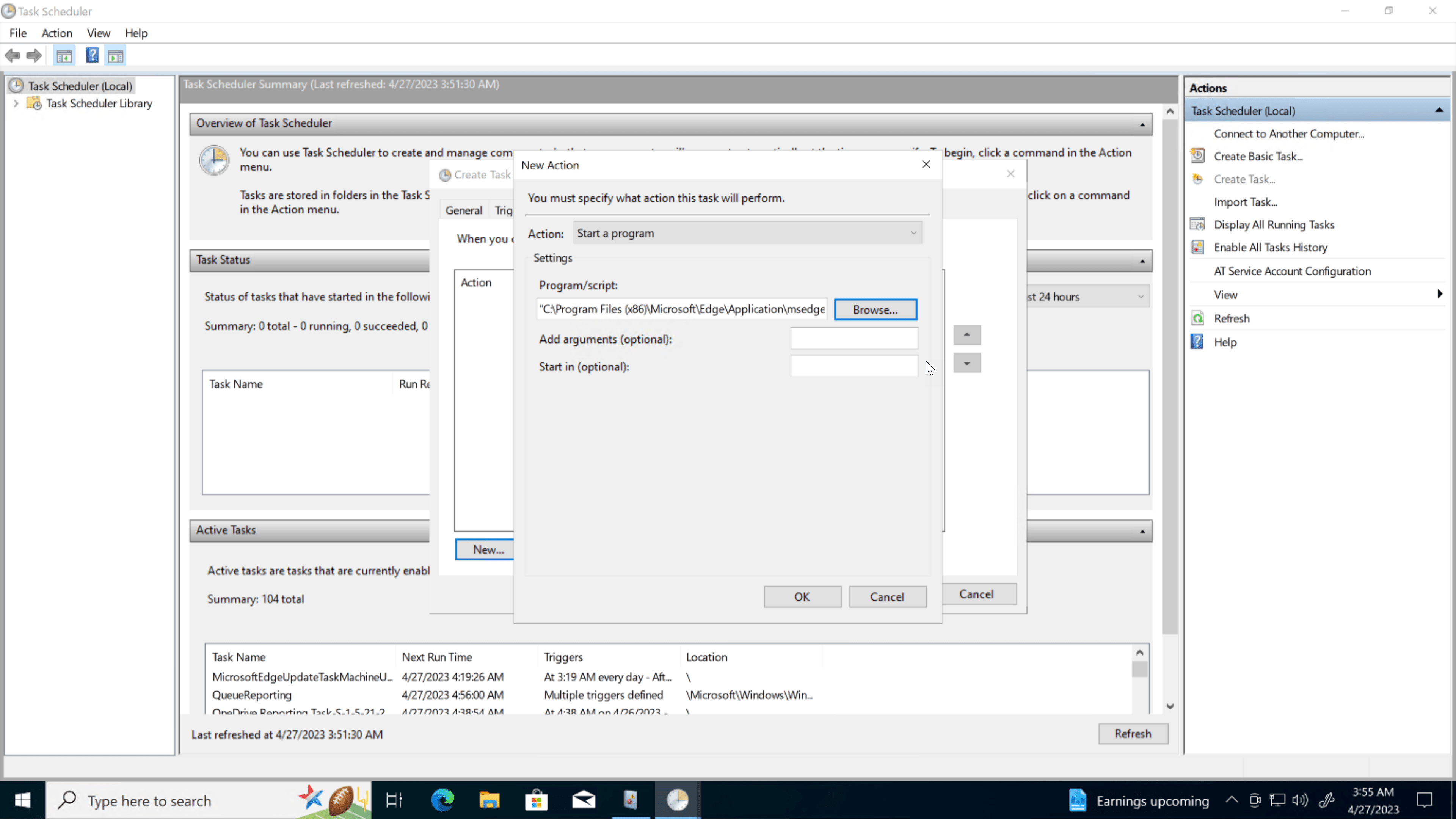
Next, I opened up Task Scheduler to generate activity on the VM. For the purpose of this lab, I created a task for Microsoft Edge to be opened every 3 minutes for 15 minutes.

A screenshot of a computer

Description automatically generated





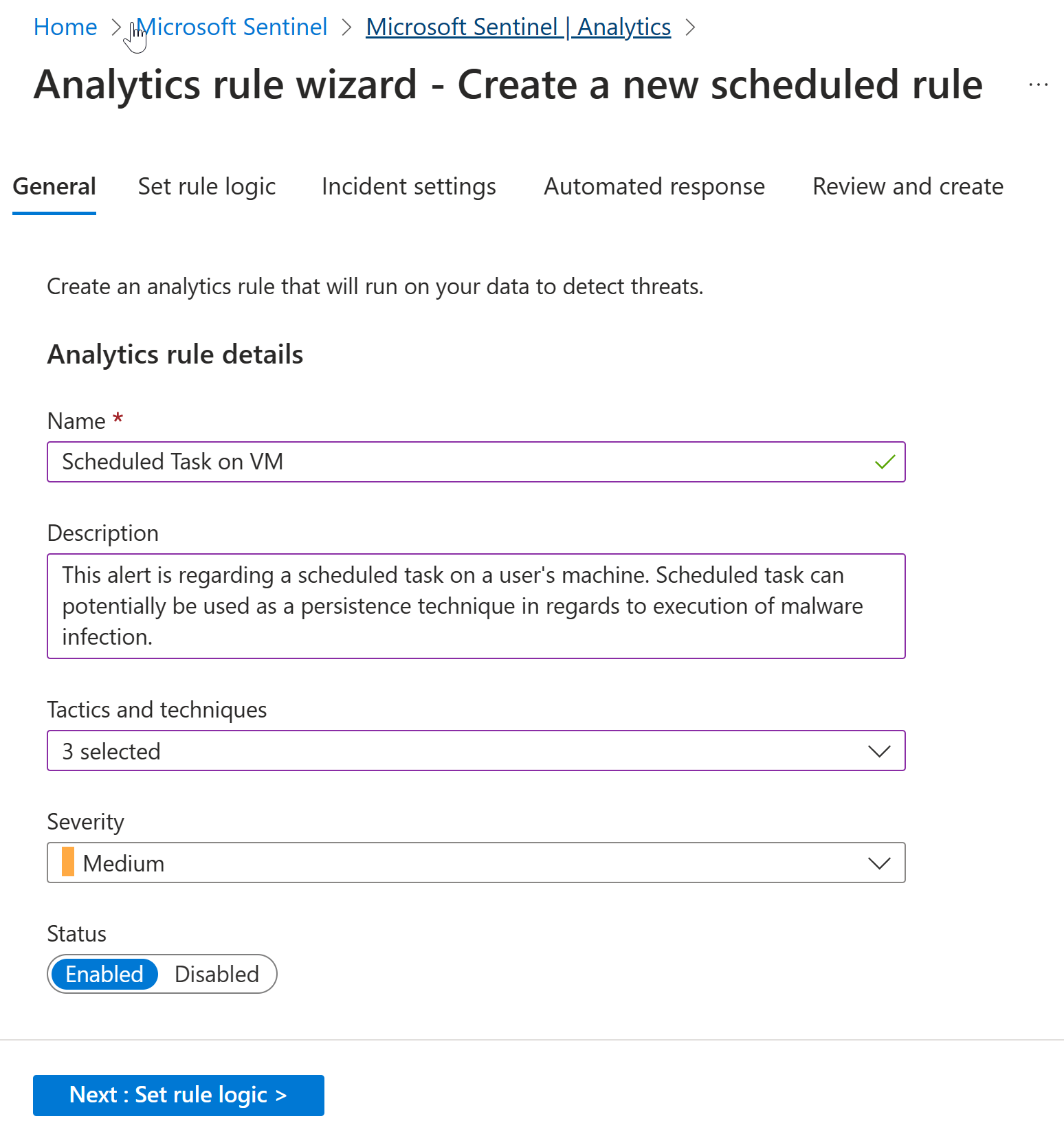


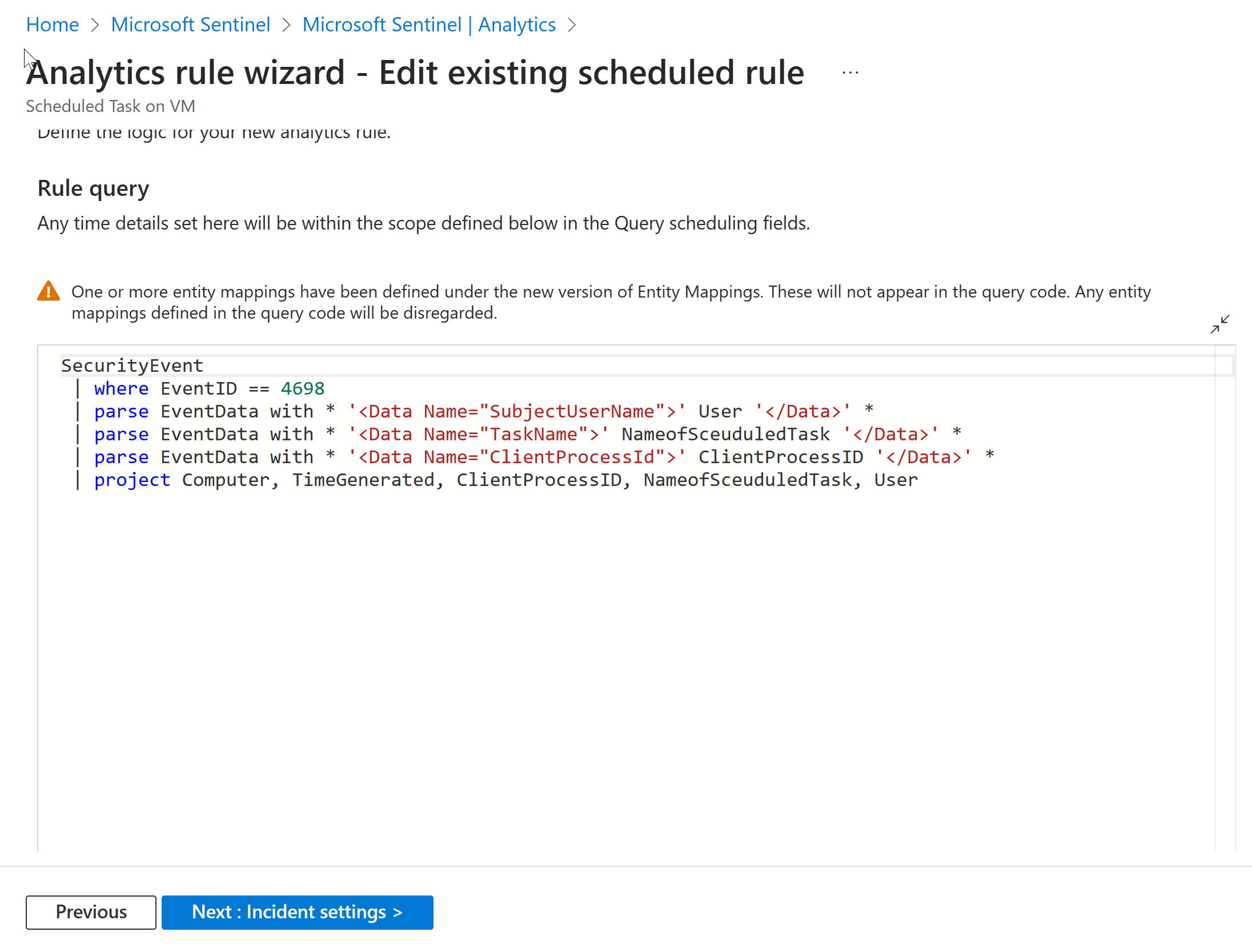
Step 6: **Writing an Analytic Rule**

### FinallStep 6: **Writing an Analytic Rule**

Finally, we must craft KQL logic to trigger alerts when a scheduled task is generated.

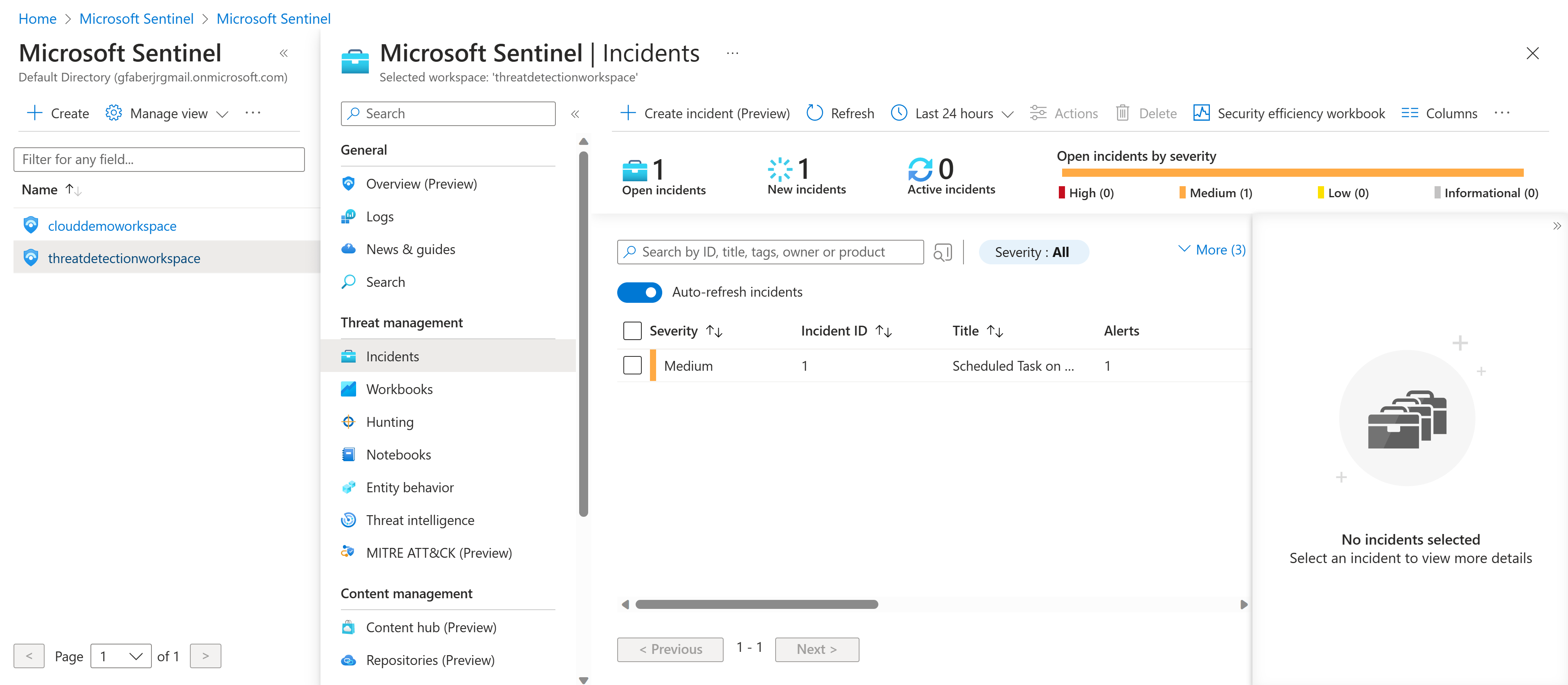
y, we must craft KQL logic to trigger alerts when a scheduled task is generated.

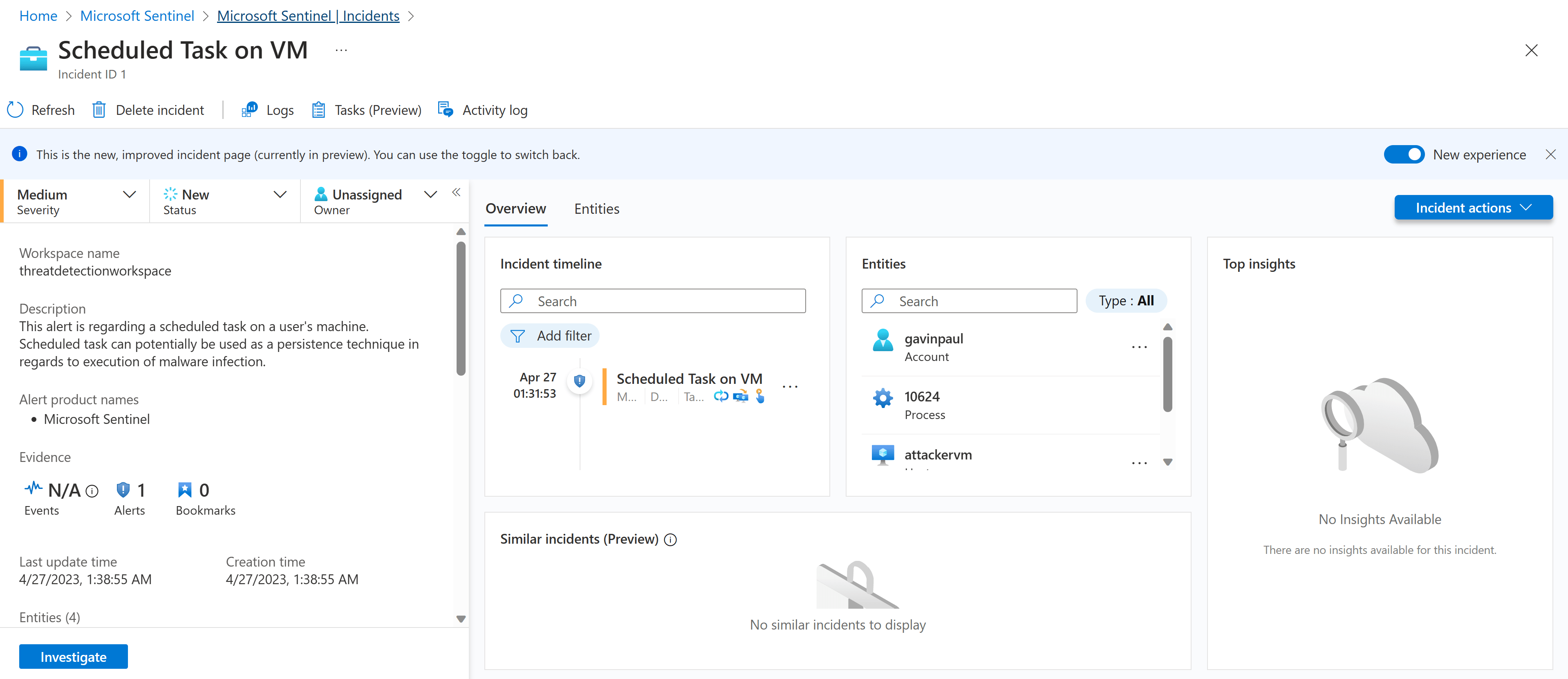


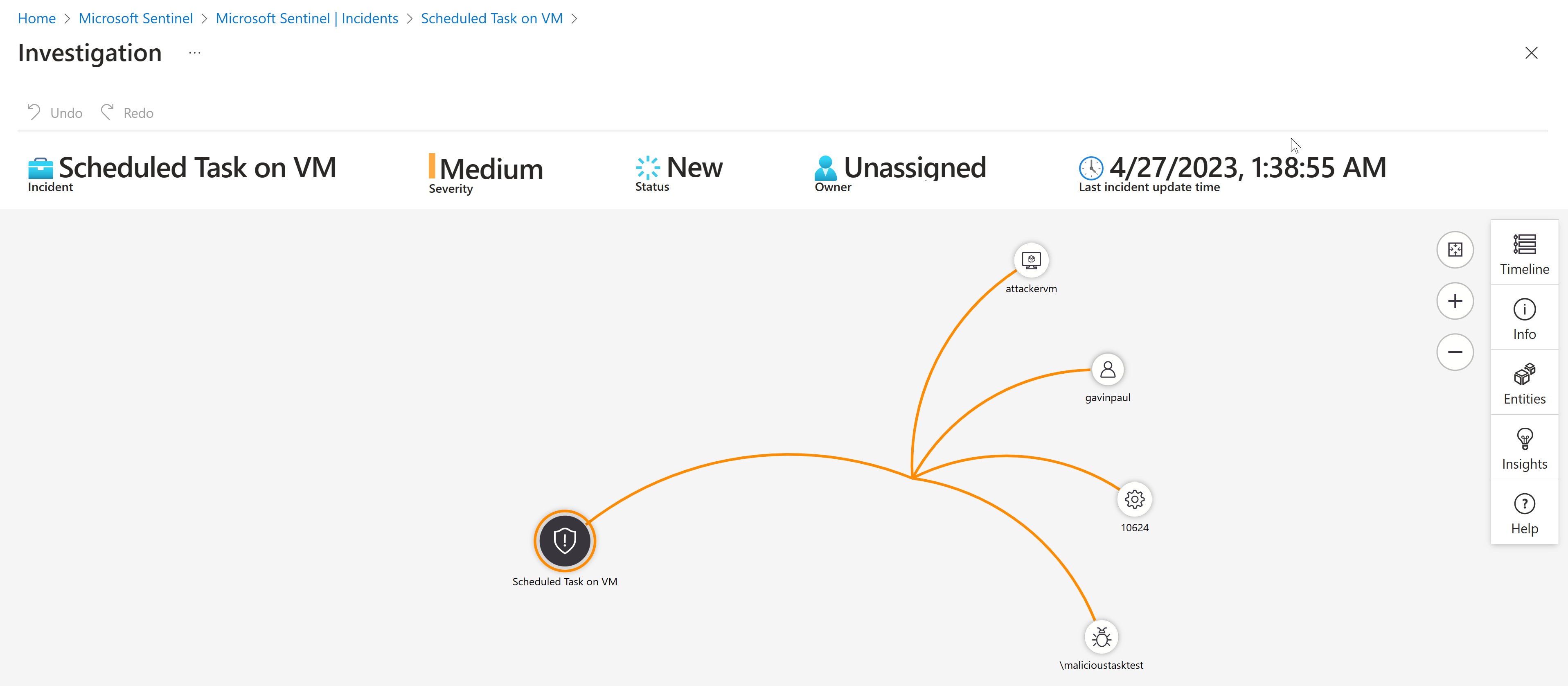


The query starts with a data source named “SecurityEvent.” This suggests that it’s querying a dataset related to security events. The first line filters the dataset using the where clause to include only records where the “EventID” is equal to 4698. The second line uses the parse statement to extract information from the “EventData” field. The third line similarly uses the parse statement to extract the name of a scheduled task. The fourth line again uses the parse statement to extract the client process ID. Finally, the query uses the project statement to select and display specific fields from the dataset, including “Computer,” “TimeGenerated,” “ClientProcessID,” “NameofScheduledTask,” and “User.” This means that the output will only include these columns from the filtered and parsed dataset.

After creating your analytic rule, the last step involves setting up a scheduled task on your Windows VM and patiently waiting for the alert to be activated within Sentinel and incident will be created. The below screenshot is the result:



Within the right-hand panel, we find all the essential details required to initiate an investigation into the alert, including information about the host machine, user account, task’s process ID, and the scheduled task’s name.



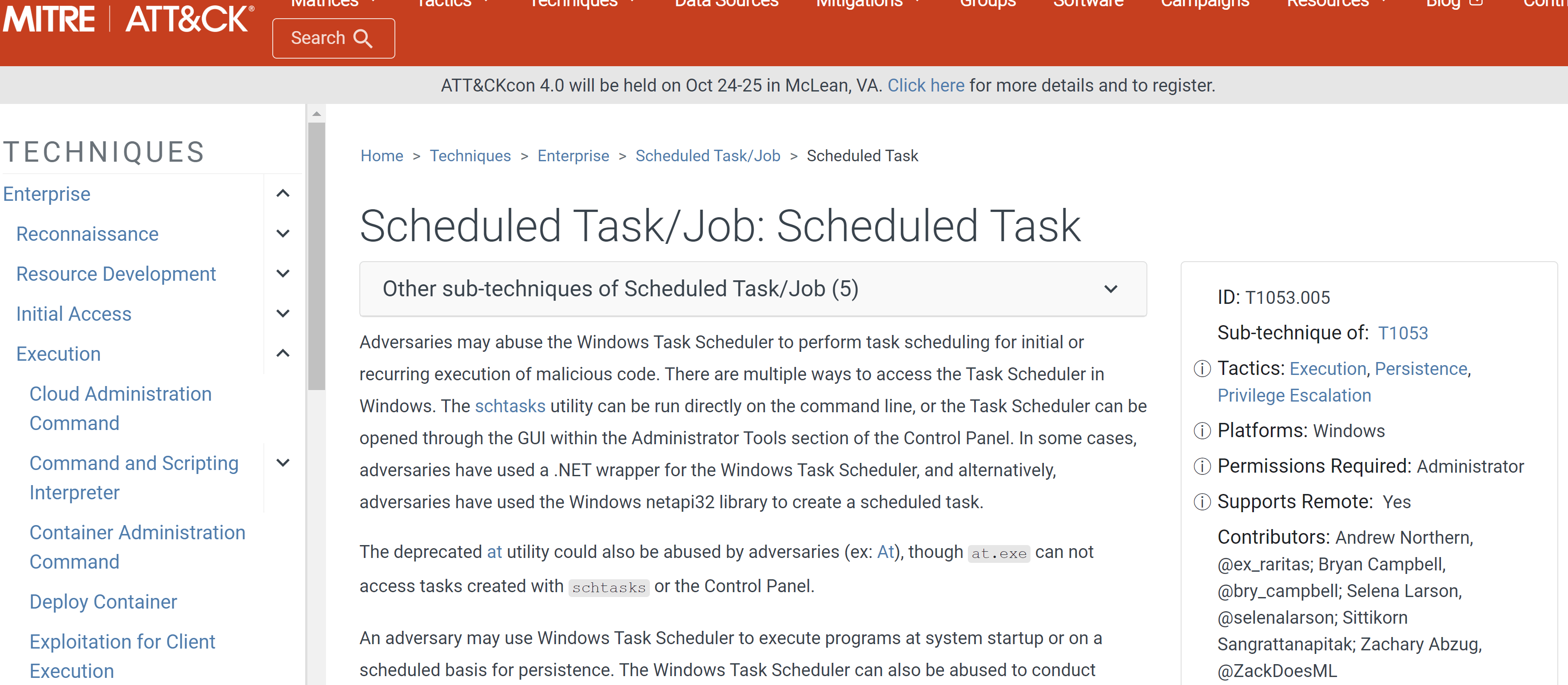
In this scenario, even though the scheduled task is benign, if it were potentially malicious, an analyst would proceed to investigate various elements, including the user account, the scheduled task, the host, and more. This investigation would typically involve utilizing additional security tools such as an EDR solution to determine whether the alert is a false positive or a true positive.

Step 7: MITRE ATT&CK

The MITRE ATT&CK framework is a comprehensive knowledge base that catalogs and categorizes real-world cyber threat tactics, techniques, and procedures (TTPs) used by adversaries during various stages of a cyberattack. It provides a standardized and detailed understanding of how cyberattacks occur, offering organizations insights into potential threats and attack vectors. Security professionals use MITRE ATT&CK to enhance threat detection, response, and mitigation strategies, ultimately improving cybersecurity defenses against a wide range of threats.

In the context of the MITRE ATT&CK framework and this lab, the tactic used was [**“Persistence”**](https://attack.mitre.org/tactics/TA0003/) which refers to a tactic used by adversaries to maintain access or control over a compromised system or network even after initial access has been achieved. It is one of the key tactics outlined in the framework and encompasses various techniques and methods that attackers employ to ensure their continued presence and influence within the targeted environment.

Persistence techniques may involve the use of backdoors, malware, scheduled tasks, registry modifications, or other means to establish mechanisms that allow attackers to regain access or control even if their initial point of entry is discovered and mitigated. Persistence is a critical aspect of many cyberattacks, as it enables attackers to maintain a foothold within a network, ensuring they can carry out their malicious activities over an extended period of time without being detected.



The MITRE ATT&CK framework categorizes and describes specific persistence techniques, offering organizations a comprehensive understanding of how attackers can maintain access and providing guidance on how to defend against such tactics. This knowledge is valuable for security professionals to enhance their threat detection and mitigation strategies.