Alessio Ragazzi

Alerts Monitoring and Response with Microsoft Sentinel and Microsoft 365 Defender

---

A day in the life of a SOC analyst (Microsoft Security Environment)

Table of Contents

1. Introduction - About me and the Microsoft exams

The Microsoft SC-900 and SC-200 are two exams by Microsoft that require the candidate to have a solid understanding of the Microsoft Azure services capabilities and Microsoft Security solutions. In October 2022 I was able to achieve the SC-900 successfully. Regarding the SC-200, despite being able to describe and utilize Microsoft 365 Defender and Microsoft Defender for Cloud to mitigate threats and respond to alerts, I'm still mastering Microsoft Sentinel. Therefore, I haven't attempted the exam yet.

1.1 Skill measured

SC-900

- Describe the concepts of security, compliance, and identity
- Describe the capabilities of Microsoft Azure Active Directory (Azure AD)
- Describe the capabilities of Microsoft Security solutions
- Describe the capabilities of Microsoft compliance solutions

SC-200

- Mitigate threats using Microsoft 365 Defender
- Mitigate threats using Microsoft Defender for Cloud
- Mitigate threats using Microsoft Sentinel

1.2 Microsoft Learn and this writeup/walkthrough

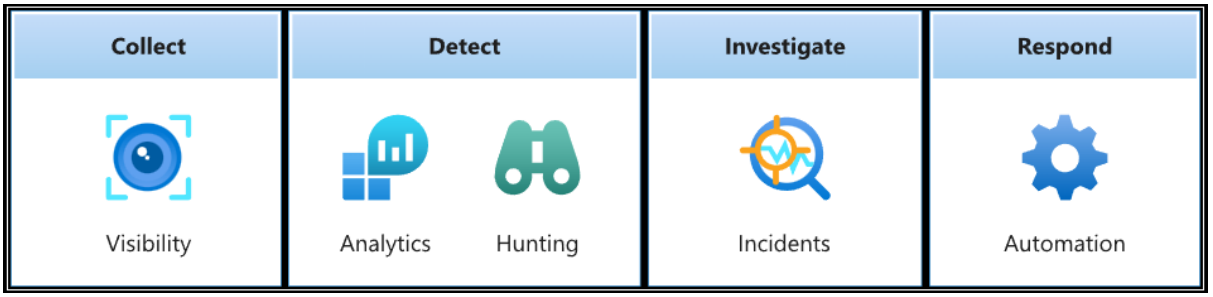
Microsoft Learn does a great job of providing you with detailed documentation to outline the efficacy of their Security solution in a modern SOC environment.
Going through the Microsoft resources I was able not only to gain fundamental theoretical knowledge but also to practice with extensive hands-on interactive guides that represent real-world scenarios.
For this writeup/walkthrough, I chose an interactive guide that demonstrates how Microsoft 365 Defender with XDR capabilities and Microsoft Sentinel enable organizations to monitor, detect, protect and respond to threats and attacks. This exercise was helpful to understand some of the day-to-day duties of a SOC analyst.

2. Microsoft Security solutions overview

2.1 Microsoft Sentinel

It's a cloud-native SIEM system that a security operations team can use to:

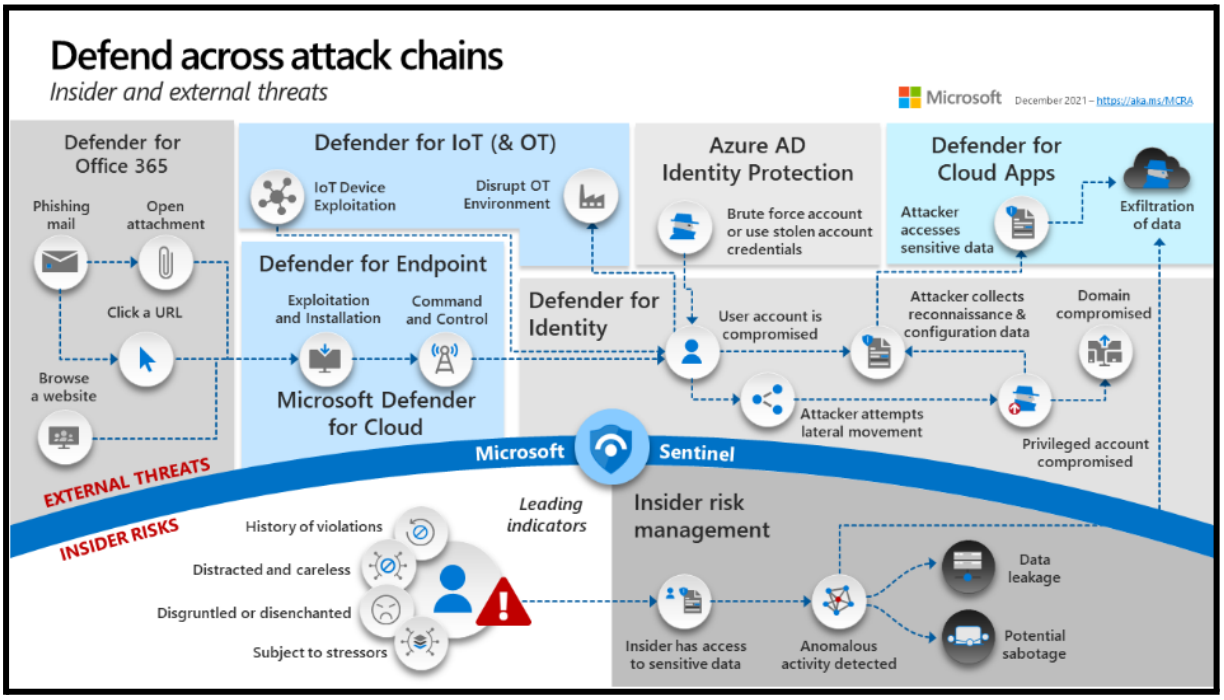
Get security insights across the enterprise by collecting data from virtually any source.
Detect and investigate threats quickly by using built-in machine learning and Microsoft threat intelligence.
Automate threat responses by using playbooks and by integrating Azure Logic Apps.
Unlike traditional SIEM solutions, to run Microsoft Sentinel, you don't need to install any servers either on-premises or in the cloud. Microsoft Sentinel is a service that you deploy in Azure. You can get up and running with Sentinel in just a few minutes in the Azure portal.



2.2 Microsoft 365 Defender

It's an integrated threat protection suite with solutions that detect malicious activity across email, endpoints, applications, and identity. These solutions provide a complete attack chain compromise story that enables a complete understanding of the threat. And, enables you to remediate and protect your organization from future attacks.

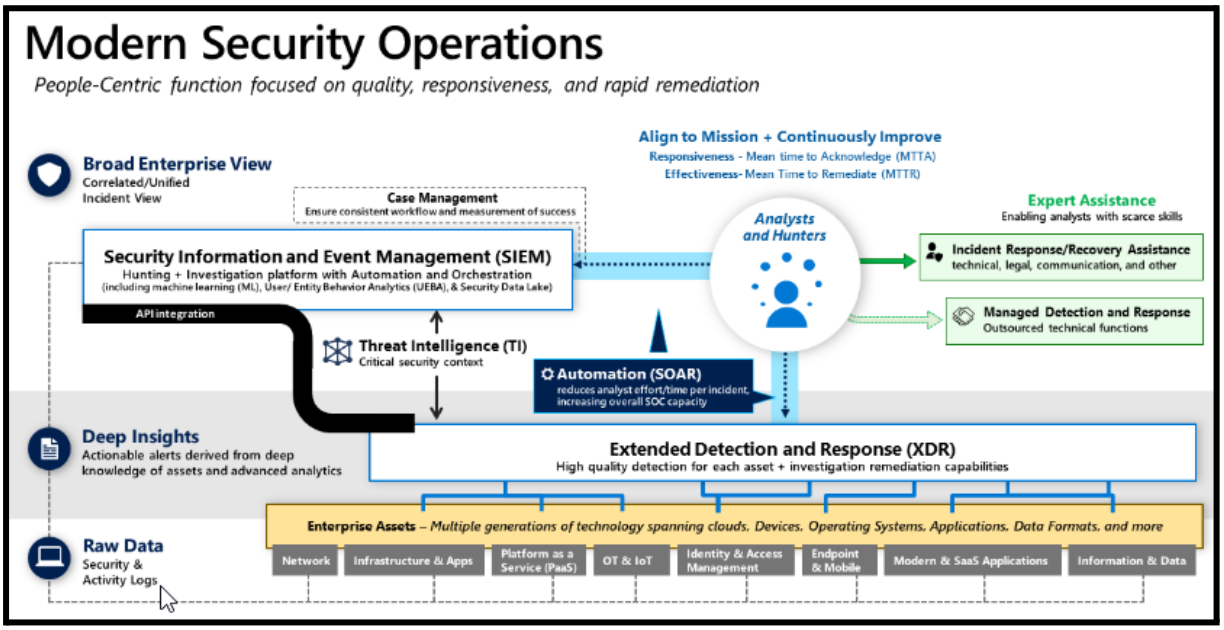
You're a Security Operations Analyst working at a company that is implementing Microsoft 365 Defender solutions. You need to understand how Extended Detection and Response (XDR) combines signals from endpoints, identity, email, and applications to detect and mitigate threats.



2.3 Microsoft Defender and Microsoft Sentinel in a Security Operation Center

---

The following graphic provides an overview of how Microsoft 365 Defender and Microsoft Sentinel are integrated in a Modern Security Operations Center (SOC).

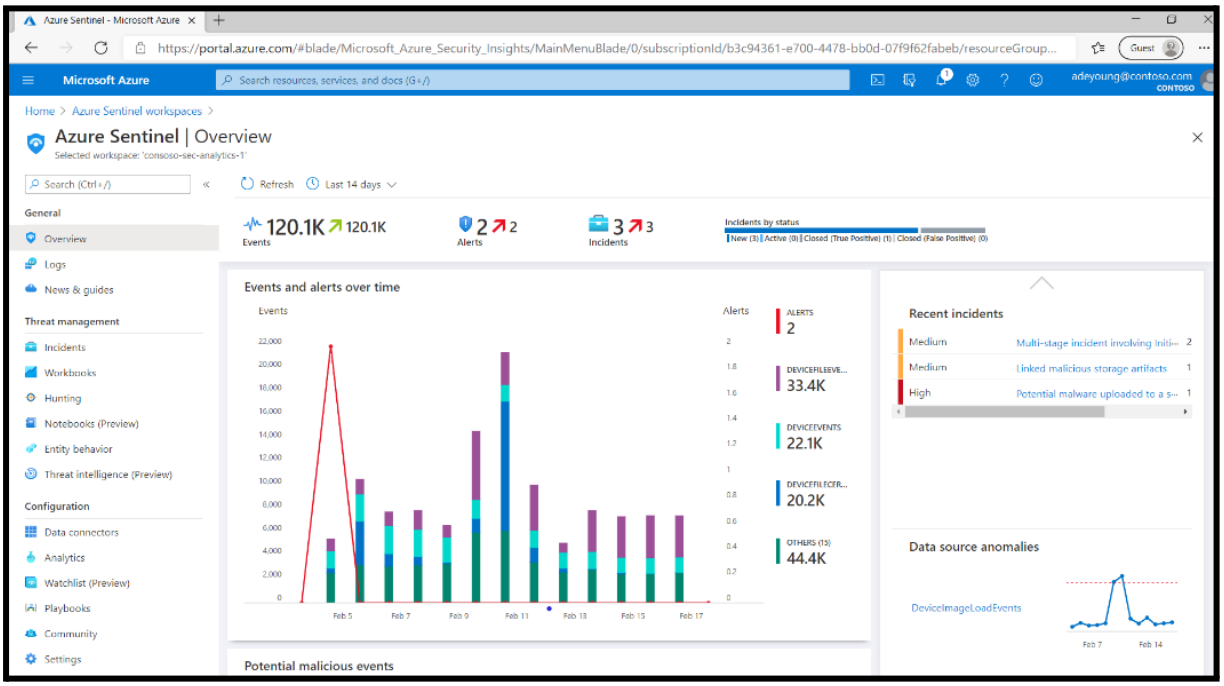


3. Alerts detection and response as a SOC analyst

In the following scenario:

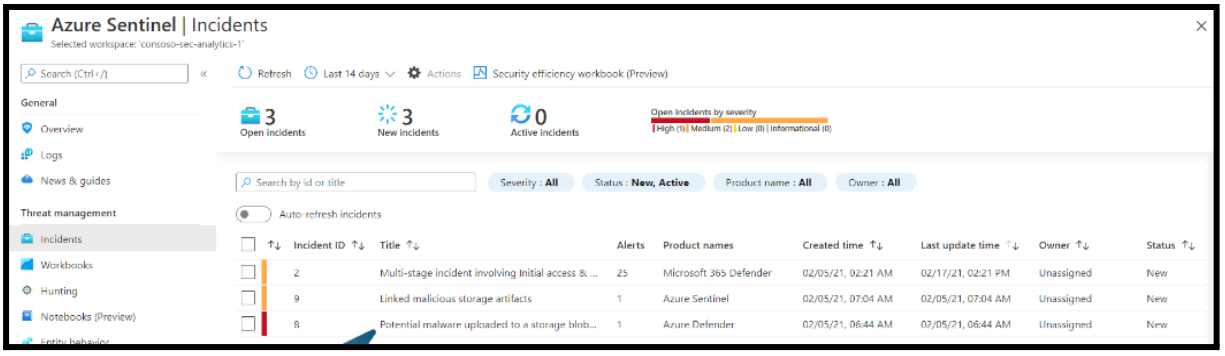
- I'll review alerts and incidents generated in Microsoft Sentinel.
- I'll try to remediate threats by running automatic remediations scripts using Azure Defender
- I'll trigger playbooks to share custom threat intelligence indicators
- I'll Investigate alerts and Incidents using Microsoft 365 Defender
- I'll show how an automation rule can trigger an automatic playbook

3.1 Reviewing Alerts and Incidents with Microsoft Sentinel



In the Microsoft Sentinel Dashboard, we can have a look at our organization's events and alerts status with rich visualizations and quick reports.
From the dashboard, we can navigate to different tabs and pages.

If we navigate to the Incident page we can have an overview of all incidents detected across the organization

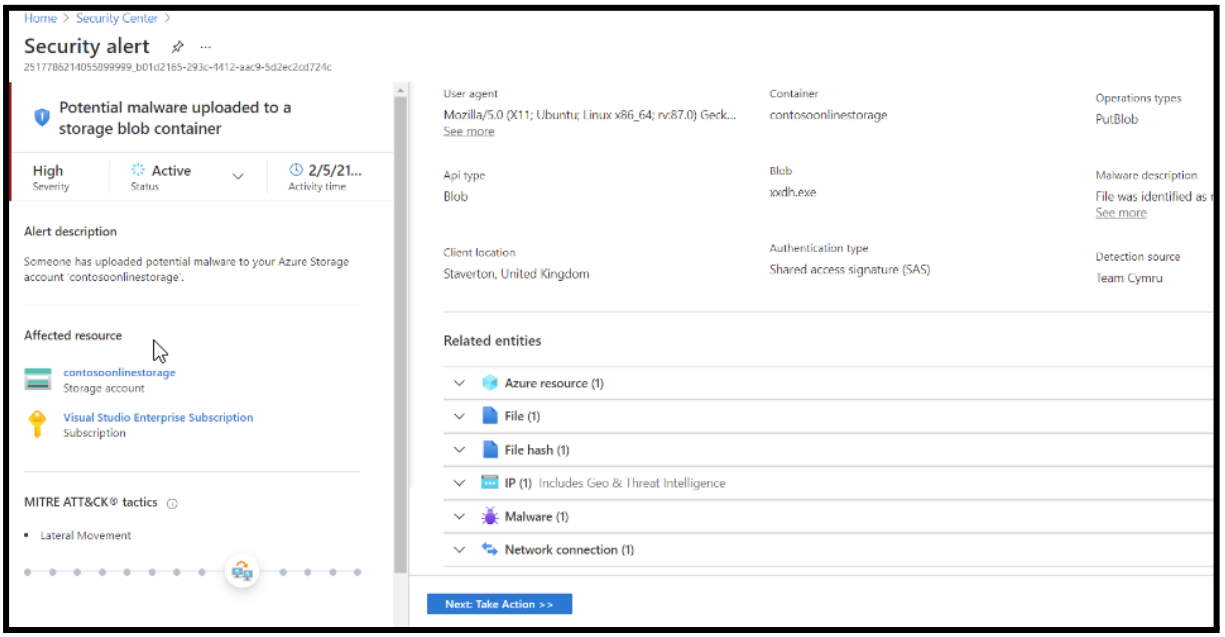


We can see a high-severity alert titled "*Potential malware uploaded to a storage blob container*" generated from Azure Defender.

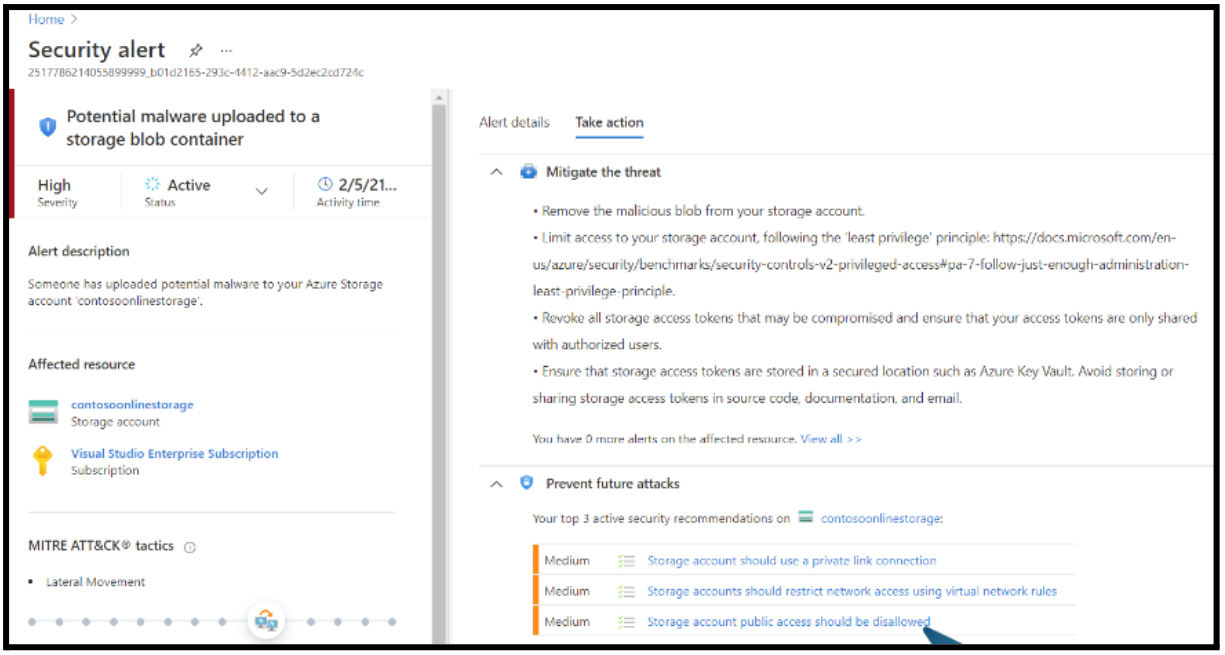
3.2 Remediate threats by running automatic remediation scripts using Azure Defender

---

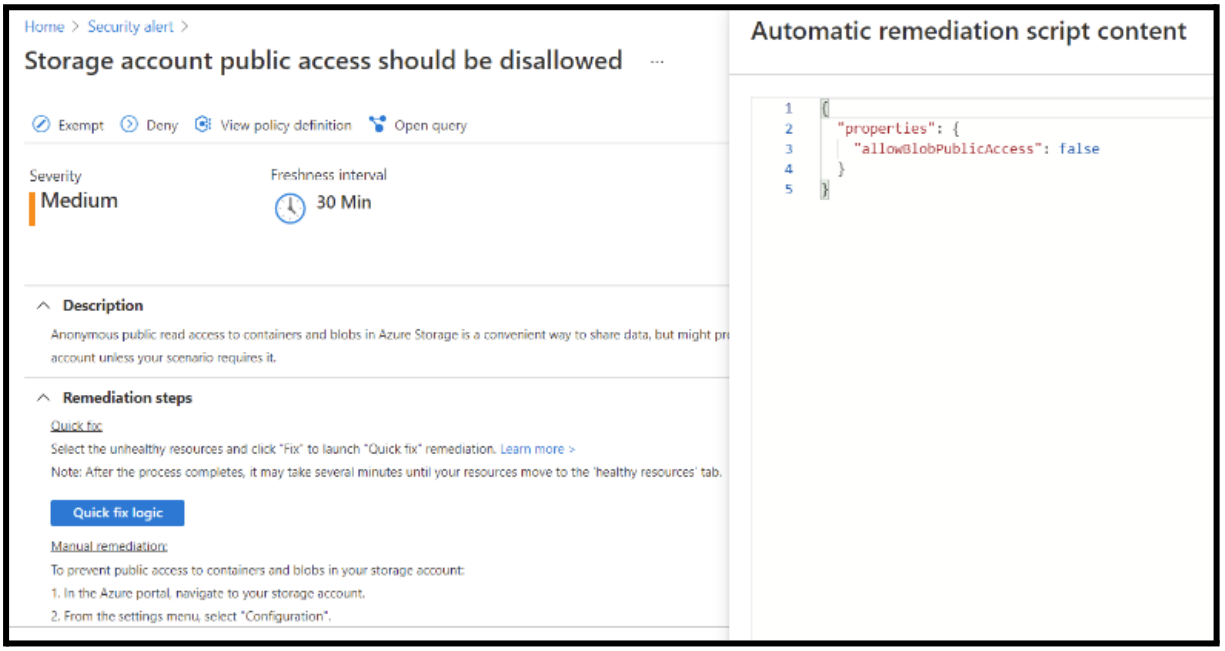
If we click on the alert, we can decide to continue the investigation on Azure Defender.
Azure defender will give us additional information and related entities to further analyze. In this case, Azure Defender was able to recognize the malware name because the file has a known hash, saving us time from checking the hash against VirusTotal.



If we look at the bottom, we can also see that is possible to take immediate action to mitigate the threat.



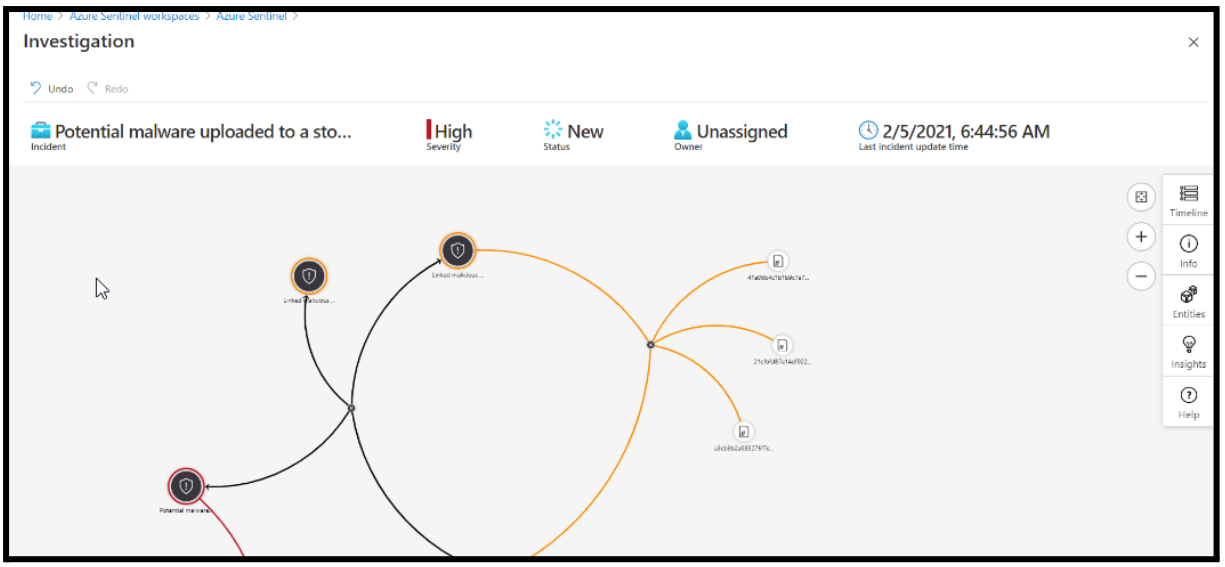
We can see the recommendation *Storage account public access should be disallowed* from the *Prevent future attack* list.
We can choose to go ahead with this recommendation and run the automatic script.



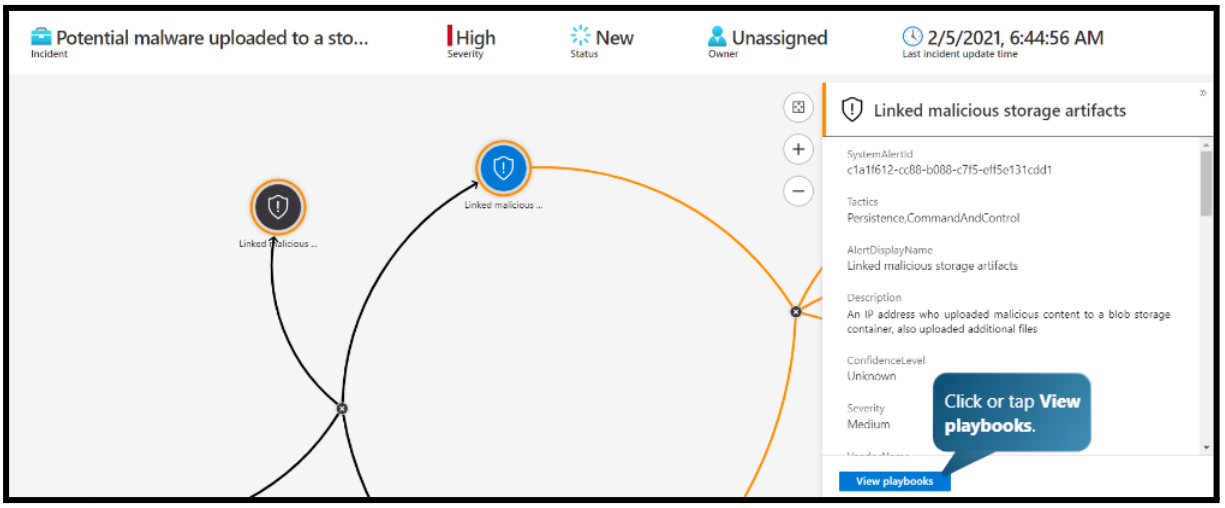
3.3 Triggering playbooks to share custom threat intelligence indicators

---

If we come back to the Microsoft Sentinel Dashboard, we can choose to investigate the incident further by visualizing the Investigation graph.



Thanks to custom detection rules previously crafted, we can see that the malicious actor has uploaded more than one malicious file. If we click on the Icon representing the other files we can trigger playbook to share threat intelligence Indicators with Microsoft 365 Defender.

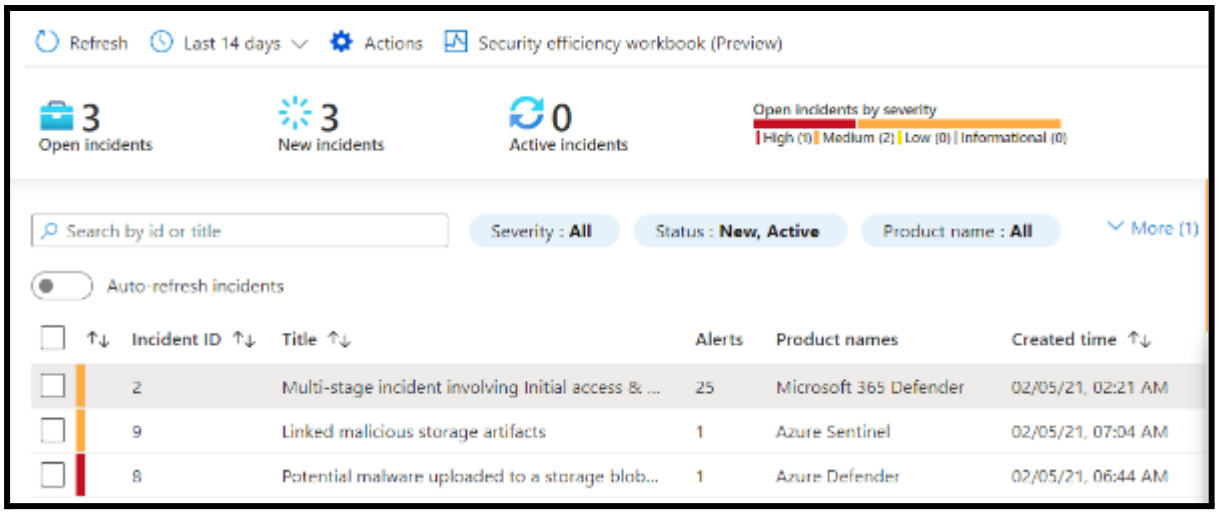


3.4 Investigating alerts and Incidents using Microsoft 365 Defender

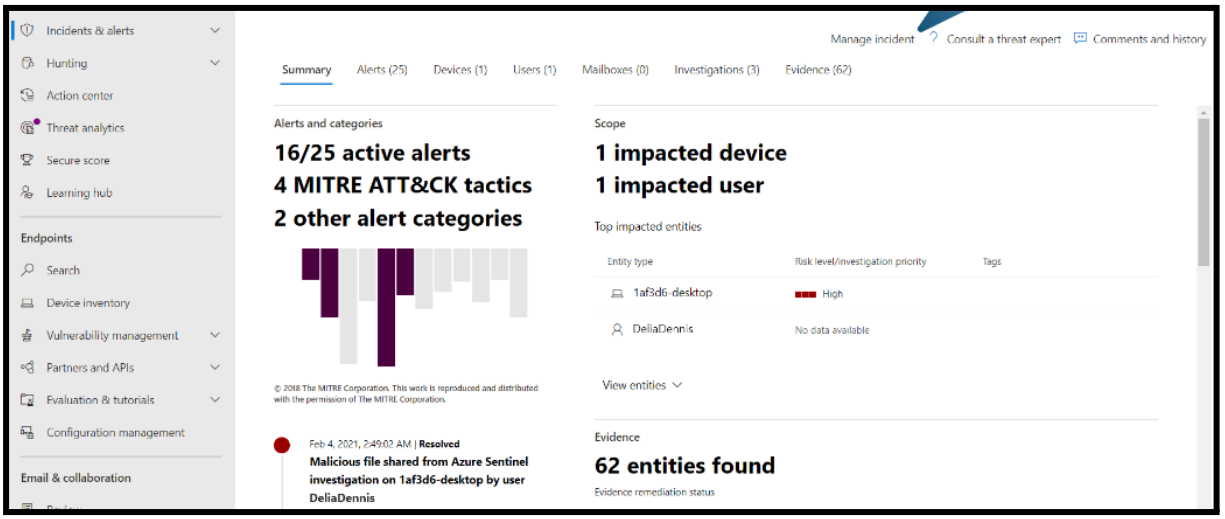
---

After investigating and taking action on the highest-severity alert, it's time to dive into the medium-severity one and see if there are correlations between incidents.
If we come back to the Microsoft Sentinel Dashboard, we can now take a look at the first alert on the list: *Multi-stage incident involving Initial Access and Credential Access.*

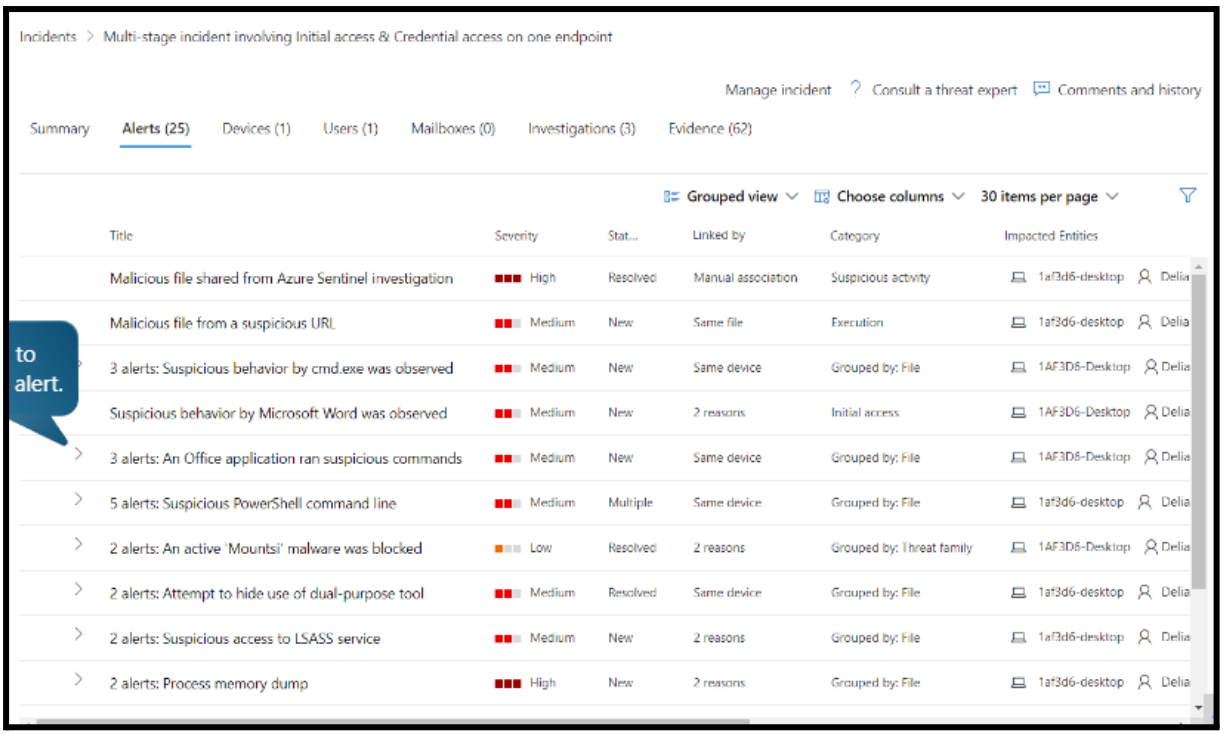
We can investigate this alert usign Microsoft 365 Defender for deep analysis of Endpoint Exploitation.



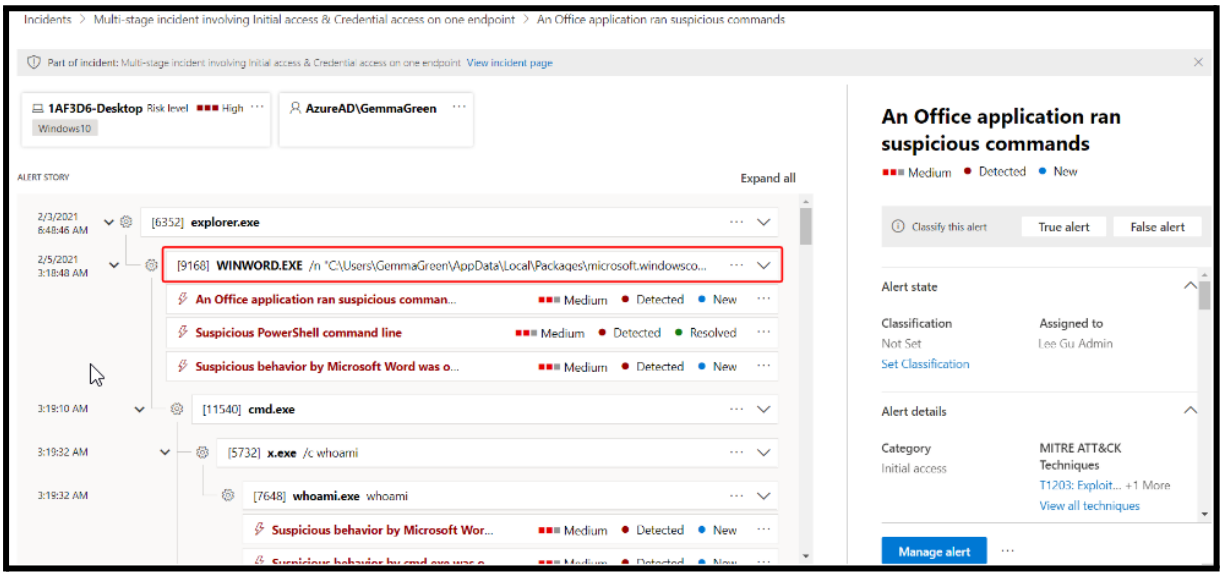
From the Microsoft 365 defender Dashboard, we can navigate between Alerts and Incidents pages, Configuration management, Secure score, Threat Hunting, and many other features.



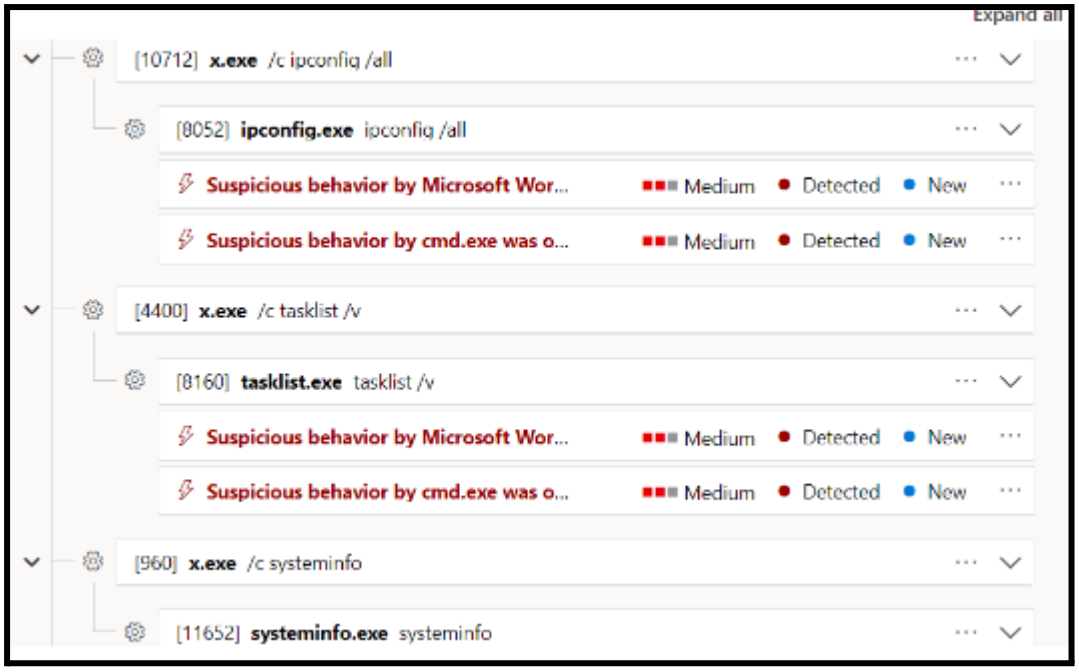
If we navigate to the Alerts page we can see what threats is our organization exposed to, ranked by severity. We'll choose the investigate the medium-severity alert: *An office application ran suspicious commands*.



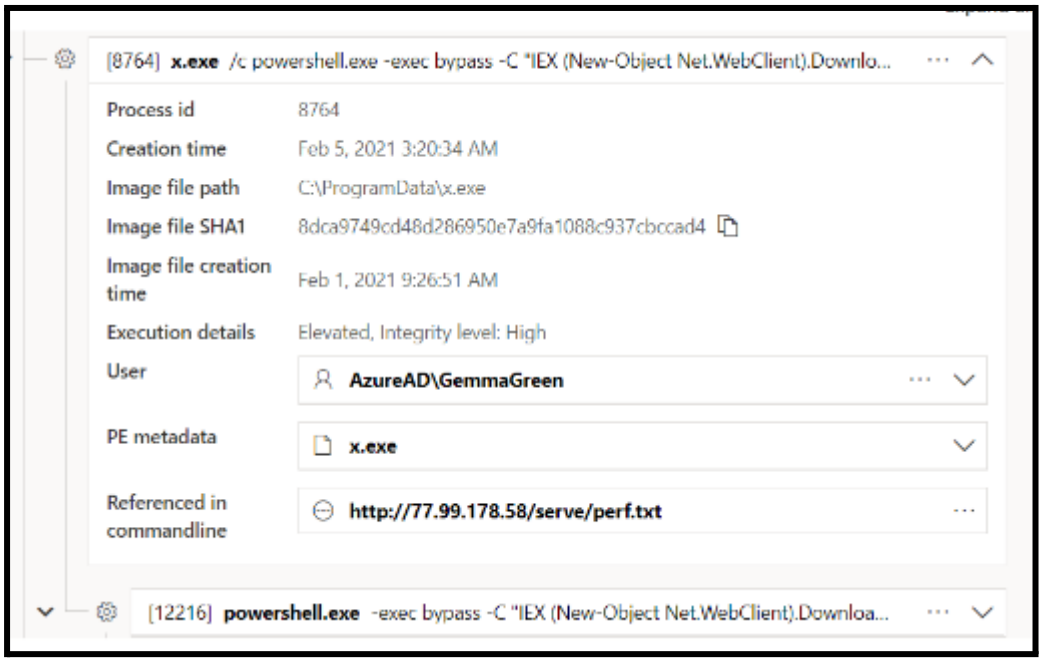
To investigate the alerts and understand the root cause and the scope of the attack, we can start by analyzing the *Alert Story*. We can collect the information we needed. For example, we can see that Microsoft Word was used to open an attachment, probably delivered by spear phishing. After opening the attached file, various PowerShell commands were executed, eventually causing the spawning of command.exe and x.exe.



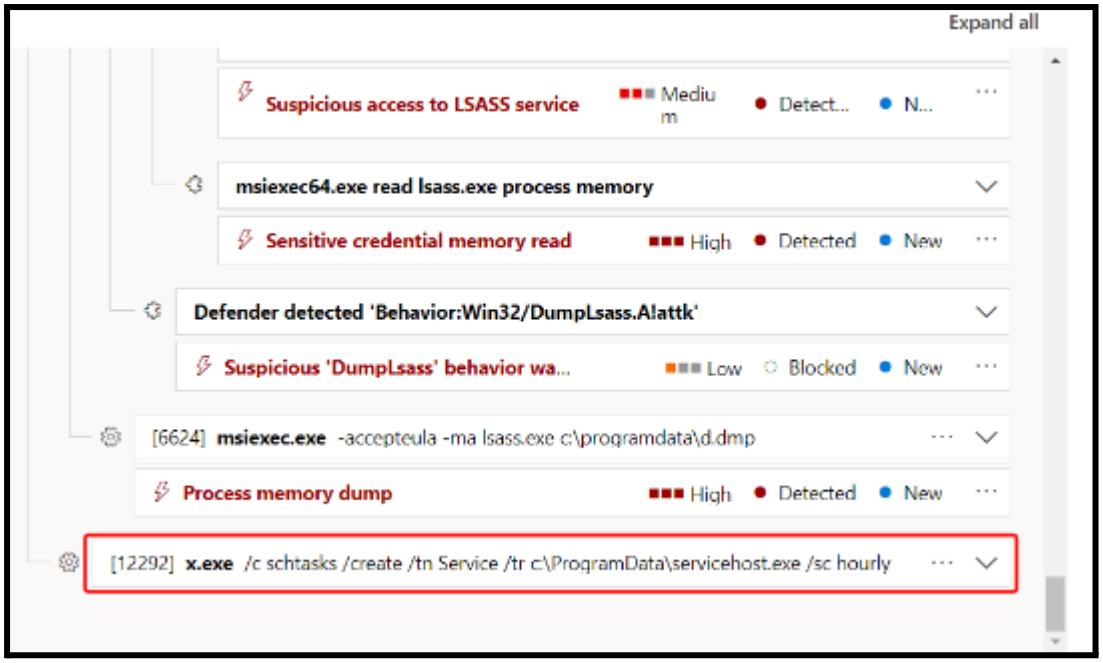
Furthermore, several reconnaissance commands were executed.



We can collect two more pieces of information by analyzing the alert story. First, we can see a PowerShell executable calling out the same IP address implicated in the high-severity alert previously discussed in the blob storage account. This can be the indicator we were looking for to connect the two incidents.

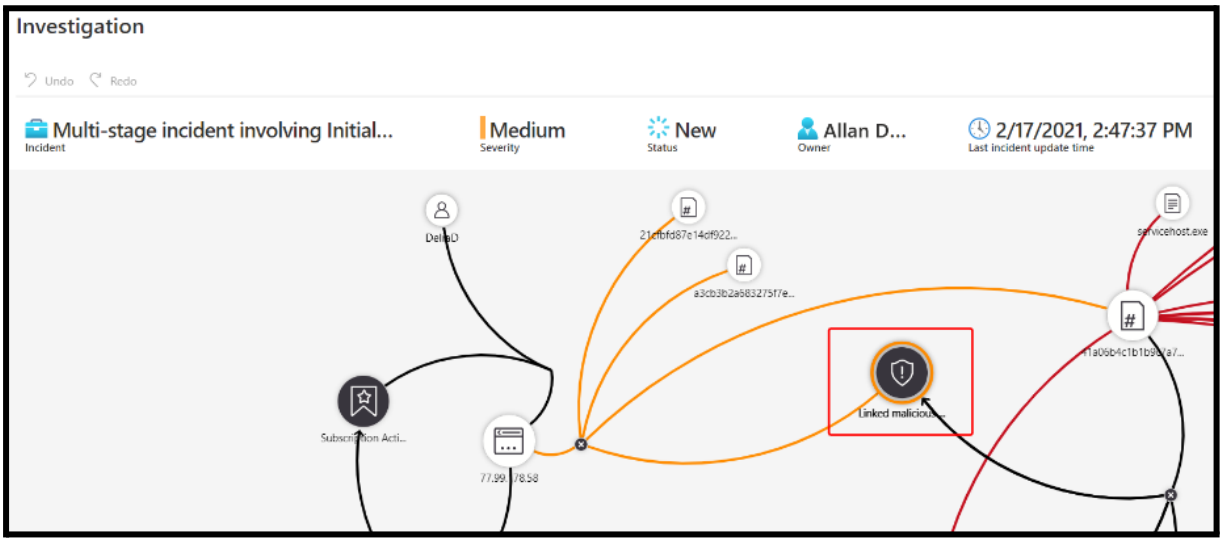


Finally, we can see that the binary servicehost.exe has been utilized to run tasks hourly.



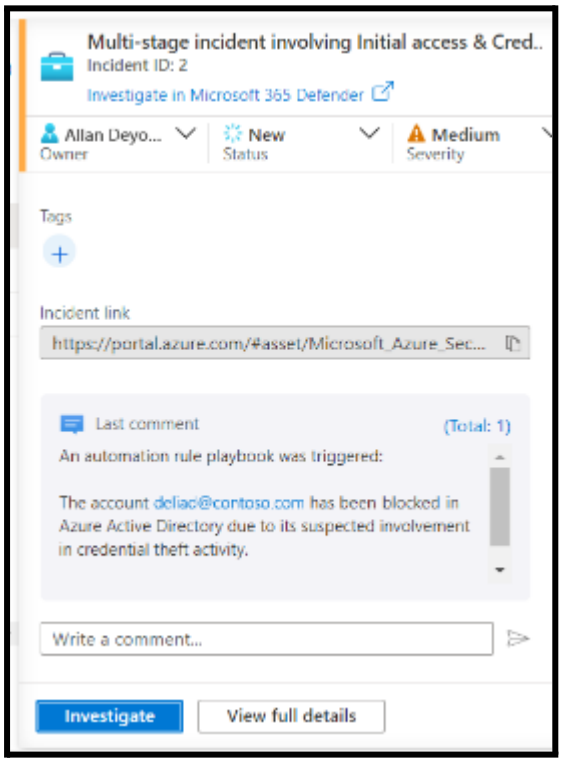
Now, as we did previously with the high-severity alert, we can investigate the medium-severity alert by visualizing the Investigation graph and checking for possible correlations between the two incidents.

If we take a look at the information laid out in the graph, we can see that, thanks to the customer threat sharing indicator we previously set, one of the file hashes we saw implicated in the blob storage incident can be associated with the Microsoft 365 Defender incident.

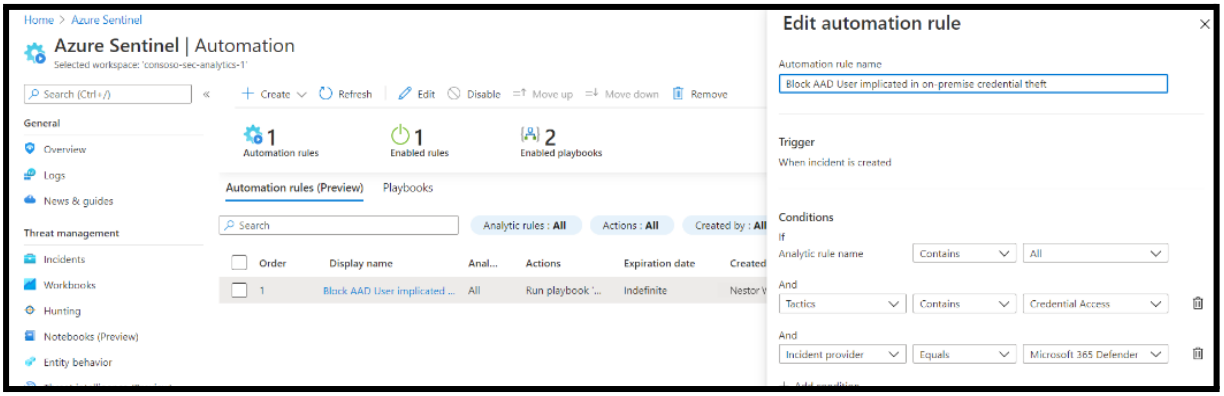


3.5 How an automation rule can trigger an automatic playbook

From the Microsoft Sentinel Dashboard we can click once again on the medium-severity alert to see if an automation rule has triggered an automatic playbook



Indeed it did. The AAD user has been blocked due to credential theft to mitigate the incident.



4. Conclusions

The subjects I was required to study in order to pass the Microsoft SC-900 exam, together with the modules from the SC-200 documentation, have given me the opportunity to understand what a day in the life of a SOC analyst (Tier 1) can look like. Apart

from the use of proprietary software/solutions, these resources allowed me to understand how to investigate alerts and incidents, share threat intelligence, how to apply quick remediation steps, and finally how to correlate different alert/incidents to understand the root cause of an attack and its scope using an integrated SIEM-XDR solution.

5. Resources

- Microsoft Learn: Microsoft SC-900
  https://learn.microsoft.com/en-us/training/paths/describe-concepts-of-security-compliance-identity/
- Microsoft Learn: Microsoft SC-200
  https://learn.microsoft.com/en-us/certifications/exams/sc-200
- Microsoft Learn: SC-200 Interactive guide
  https://mslearn.cloudguides.com/guides/Investigate%20security%20incidents%20in%20a%20hybrid%20environment%20with%20Azure%20Sentinel

Credit
Writeup/Walkthrough written by Alessio Ragazzi
Images from Microsoft Learn official website