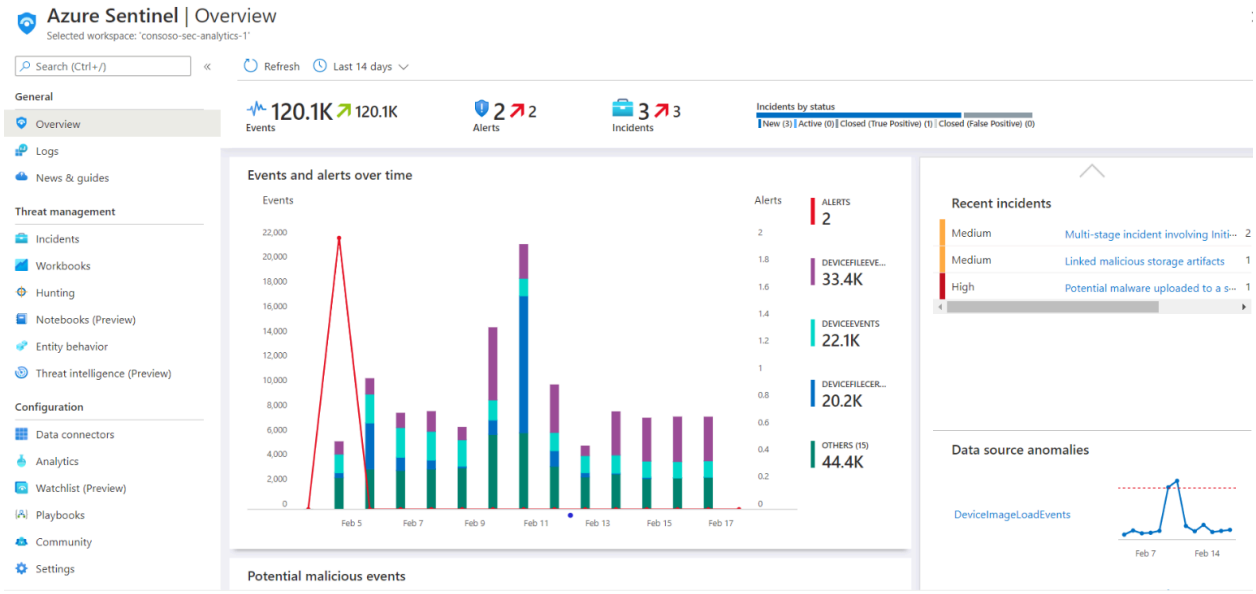
Detect and respond to modern attacks with unified SIEM and XDR capabilities

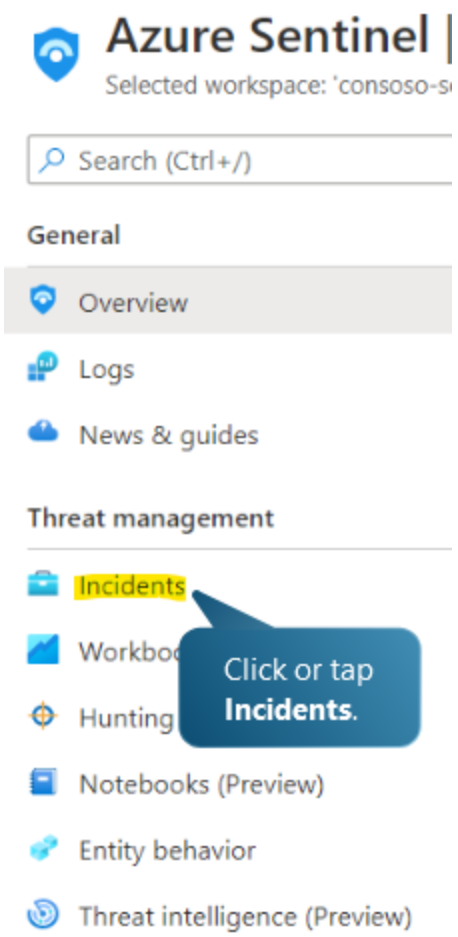
By: Ryan Stewart

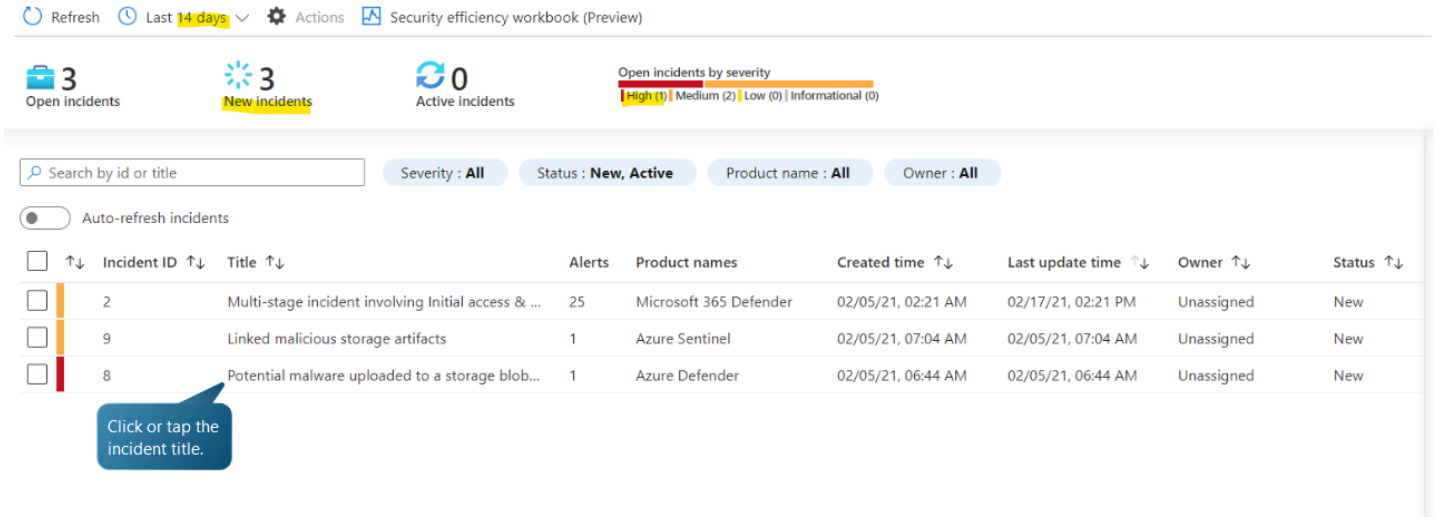
Unified Experience

- Automates threat investigations
- Helps close critical gaps
- Empowers rapid response

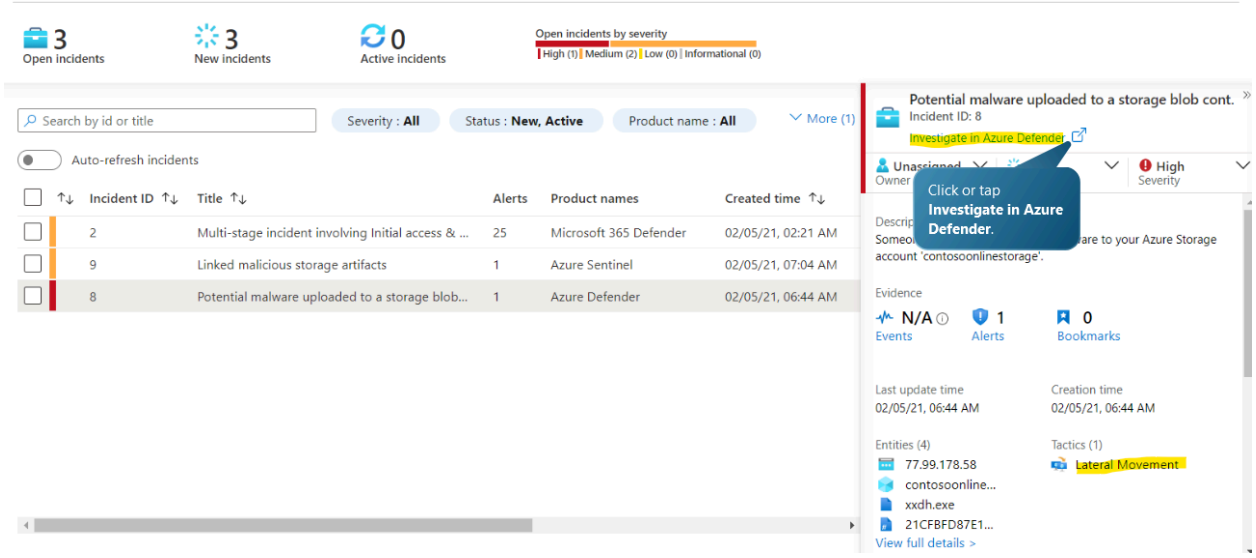


Azure Sentinel is a cloud-native SIEM solution that delivers intelligent security analytics across the entire organization. It collects data at cloud scale across all users, devices and apps, infrastructures and on-premise or multiple clouds. Most importantly to me it enables SOC teams to make threat detection, investigation, and response more efficient with AI and automation.

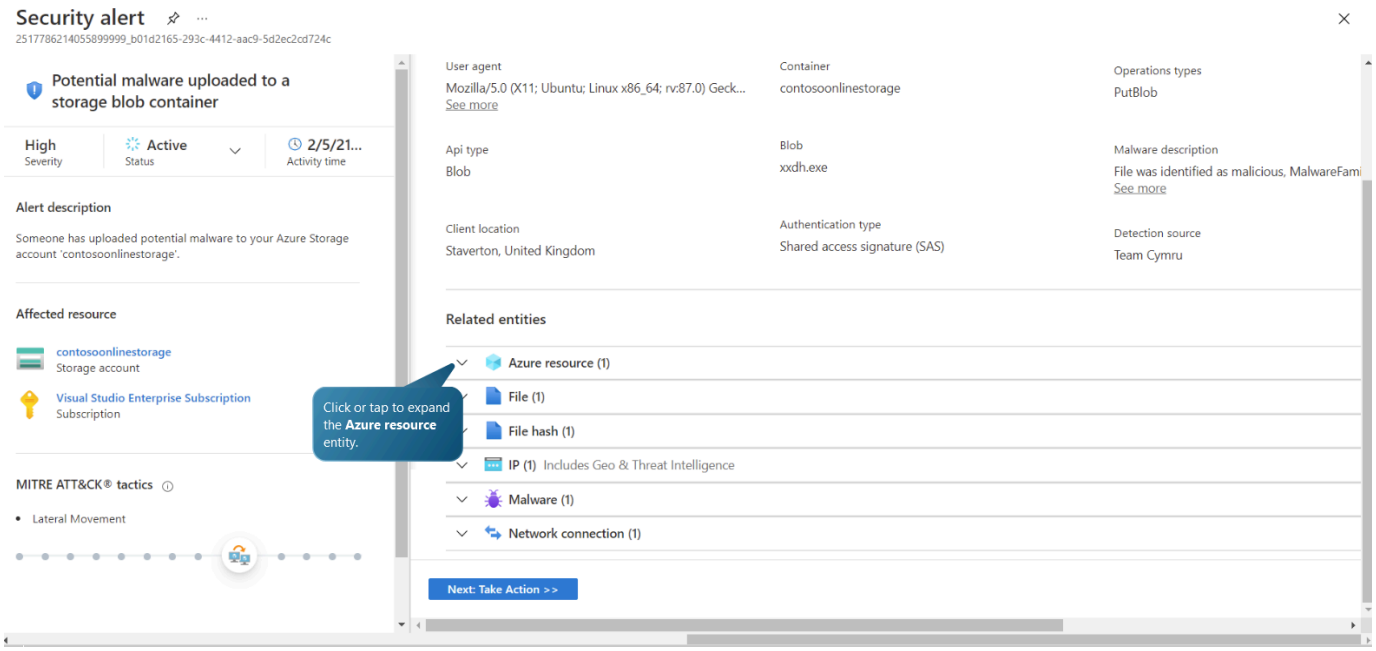

Azure Sentinel |
Selected workspace: 'consoso-s
Search (Ctrl+/)
General
Overview
Logs
News & guides
Threat management
Incidents
Workboo
Hunting
Notebooks (Preview)
Entity behavior
Threat intelligence (Preview)
Click or tap Incidents.


Refresh
Last 14 days
Actions
Security efficiency workbook (Preview)
3
Open incidents
3
New incidents
0
Active incidents
Open incidents by severity
High (1) Medium (2) Low (0) Informational (0)
Search by id or title
Severity : All
Status : New, Active
Product name : All
Owner : All
Auto-refresh incidents
Incident ID
Title
Alerts
Product names
Created time
Last update time
Owner
Status
2 Multi-stage incident involving Initial access & ... 25 Microsoft 365 Defender 02/05/21, 02:21 AM 02/17/21, 02:21 PM Unassigned New
9 Linked malicious storage artifacts 1 Azure Sentinel 02/05/21, 07:04 AM 02/05/21, 07:04 AM Unassigned New
8 Potential malware uploaded to a storage blob... 1 Azure Defender 02/05/21, 06:44 AM 02/05/21, 06:44 AM Unassigned New
Click or tap the incident title.

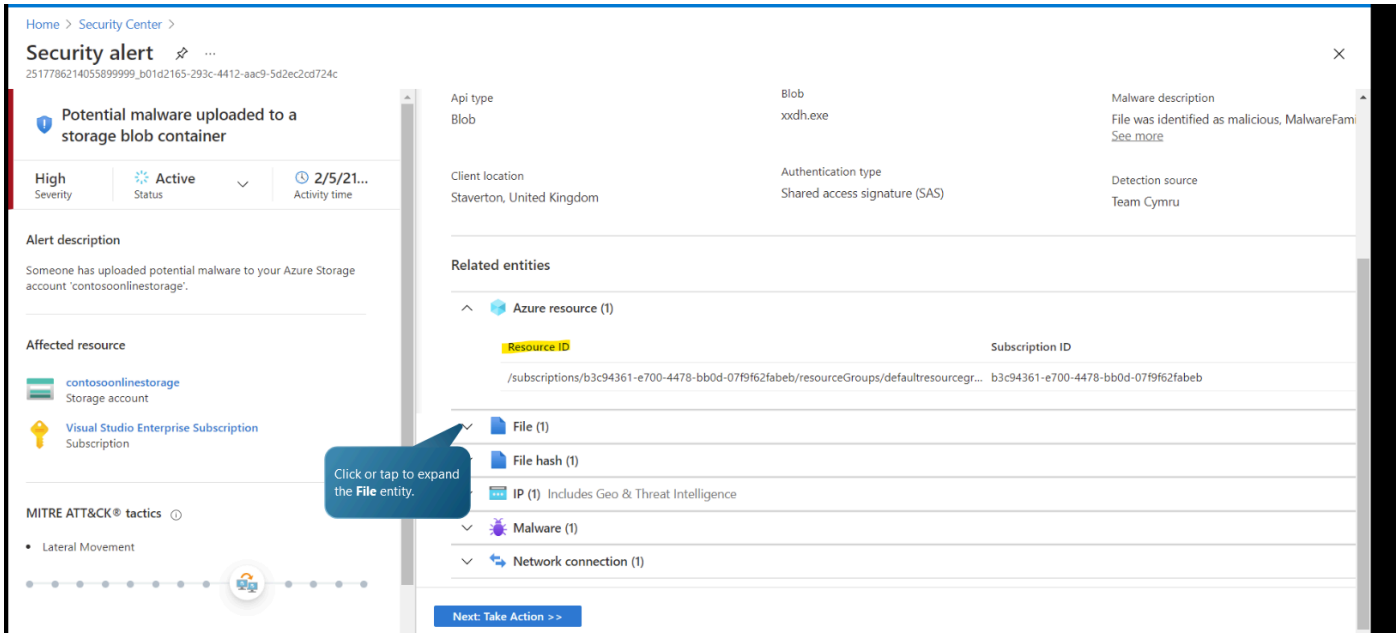
Let's investigate the high severity alert title “Potential malware uploaded to a storage blob container.”



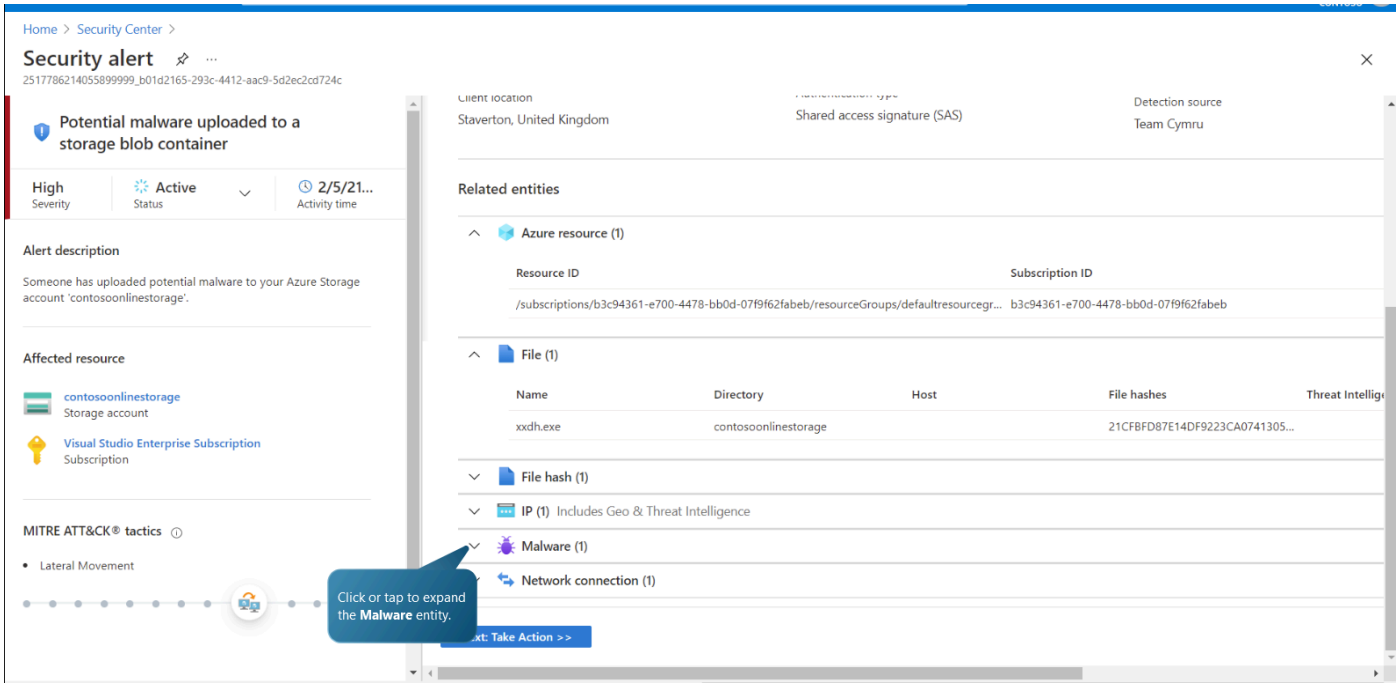
To see if there is any immediate action that needs to be taken to protect the organization, we can investigate this alert in Azure defender.



Expand the **Azure resource** entity.

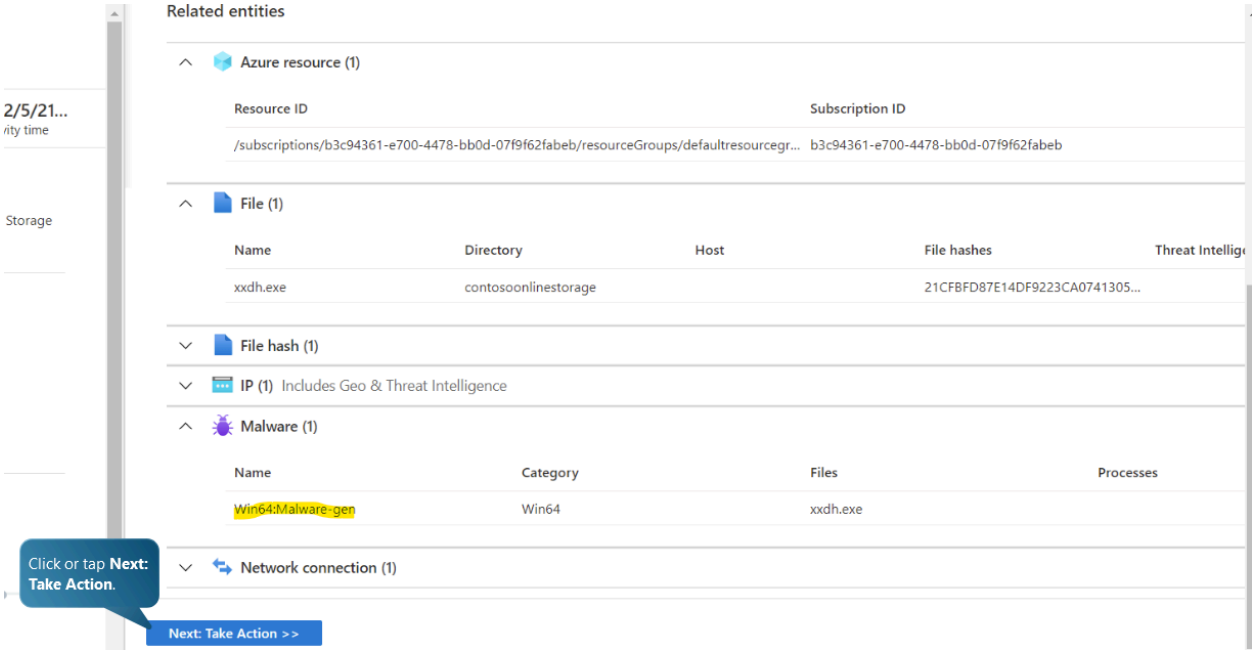


Here, we can see the resource ID of the affected storage account.

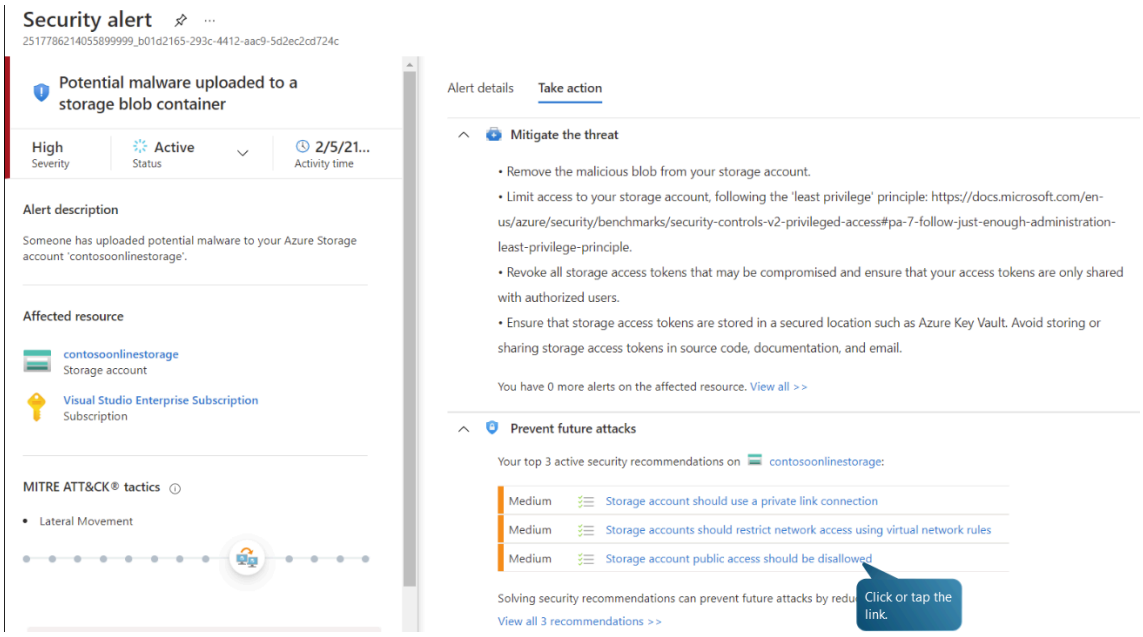


Here we can view details on the potential malware file that was detected in the storage account.

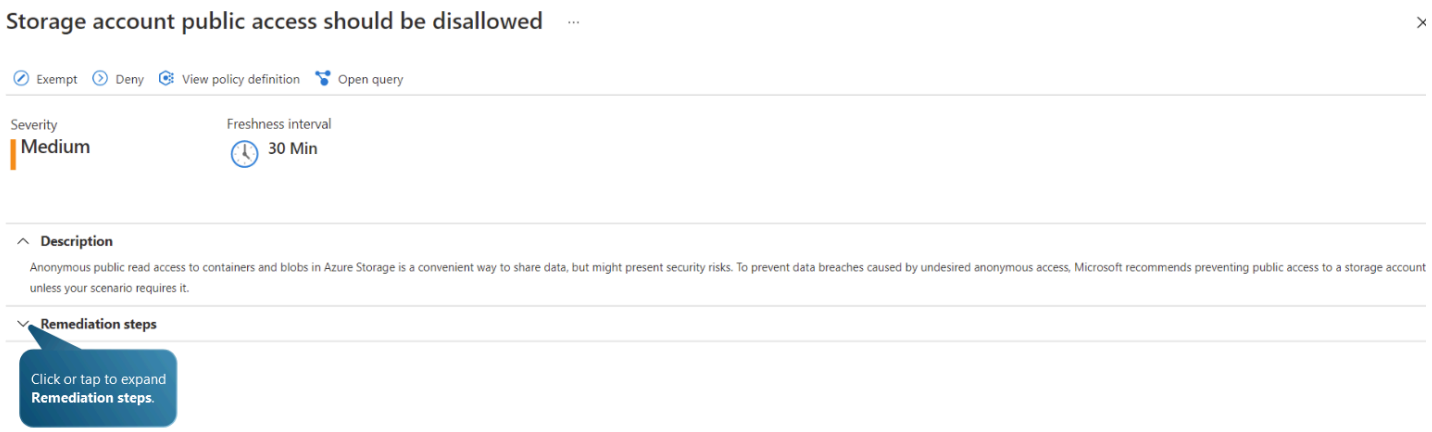
Note that **Microsoft Sentinel** “file hashes” can be used to query VirusTotal for additional threat information. VirusTotal aggregates antivirus scan engines and security tools, indicating if a file hash is flagged as malicious. While useful, it's essential to rely on multiple sources for comprehensive threat intelligence. Microsoft Sentinel integrates with various services, allowing cross-referencing with VirusTotal for enhanced threat understanding.



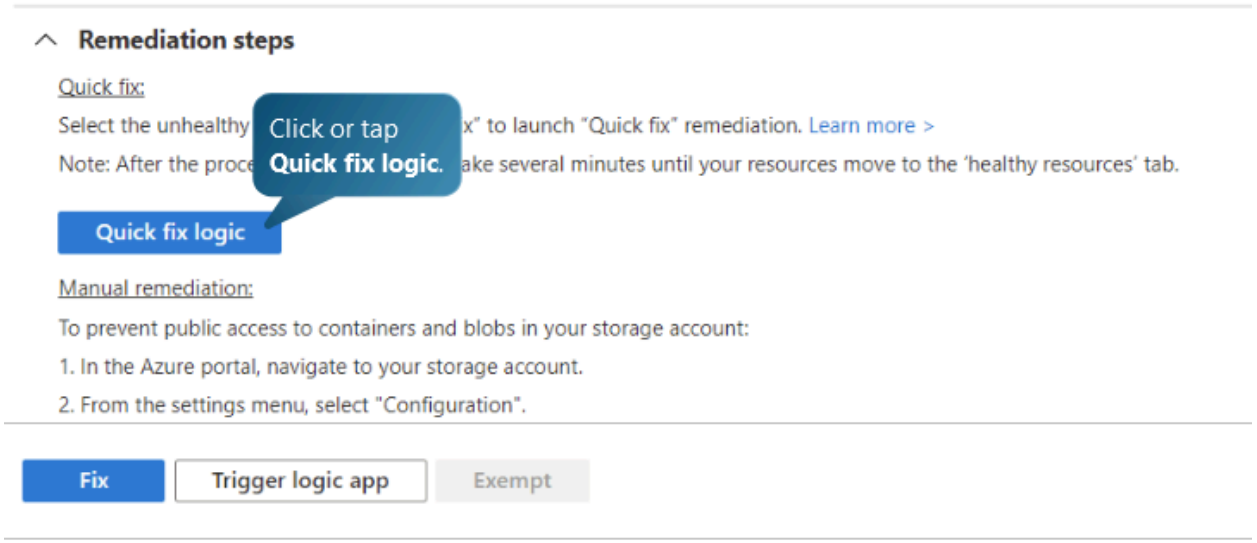
Here we see the name of the malware that was detected in the scanned file. Azure defender was able to detect this file because it used a known bad hash. Now lets see how we can use **Azure Defender** to take action.



Azure Defender provides recommended steps that an **administrator** can take to mitigate this threat.



Lets view one of the recommendations:



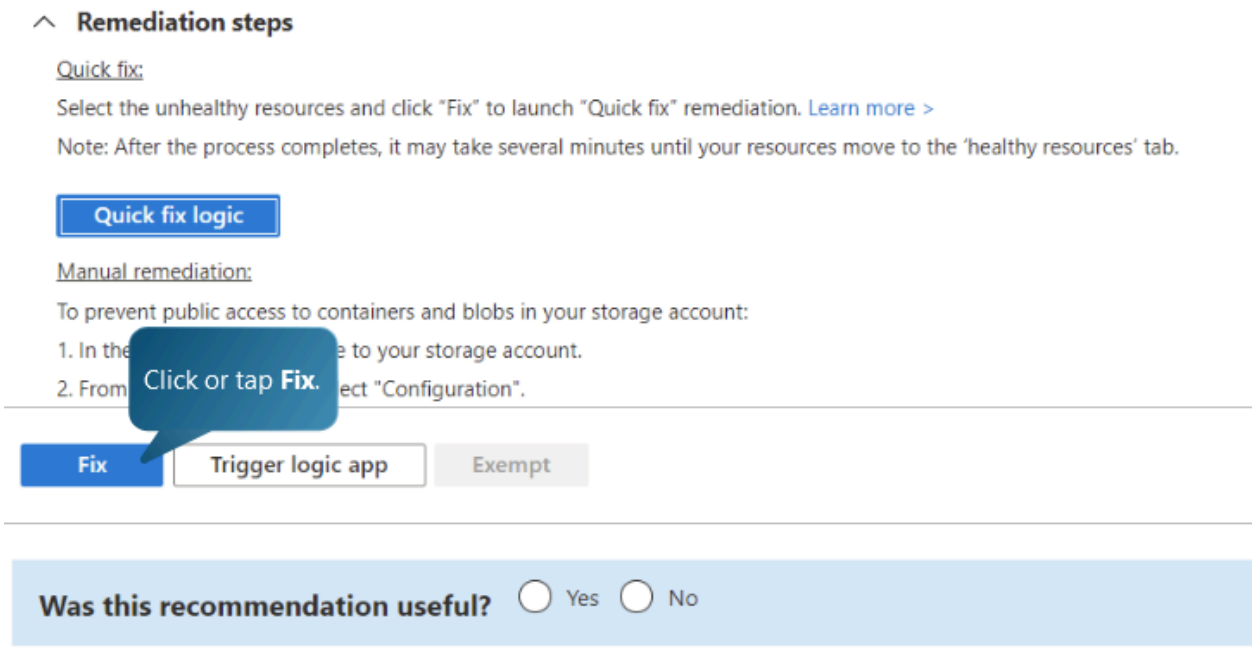
This recommendation includes both **quick fix** and **manual** remediation options.

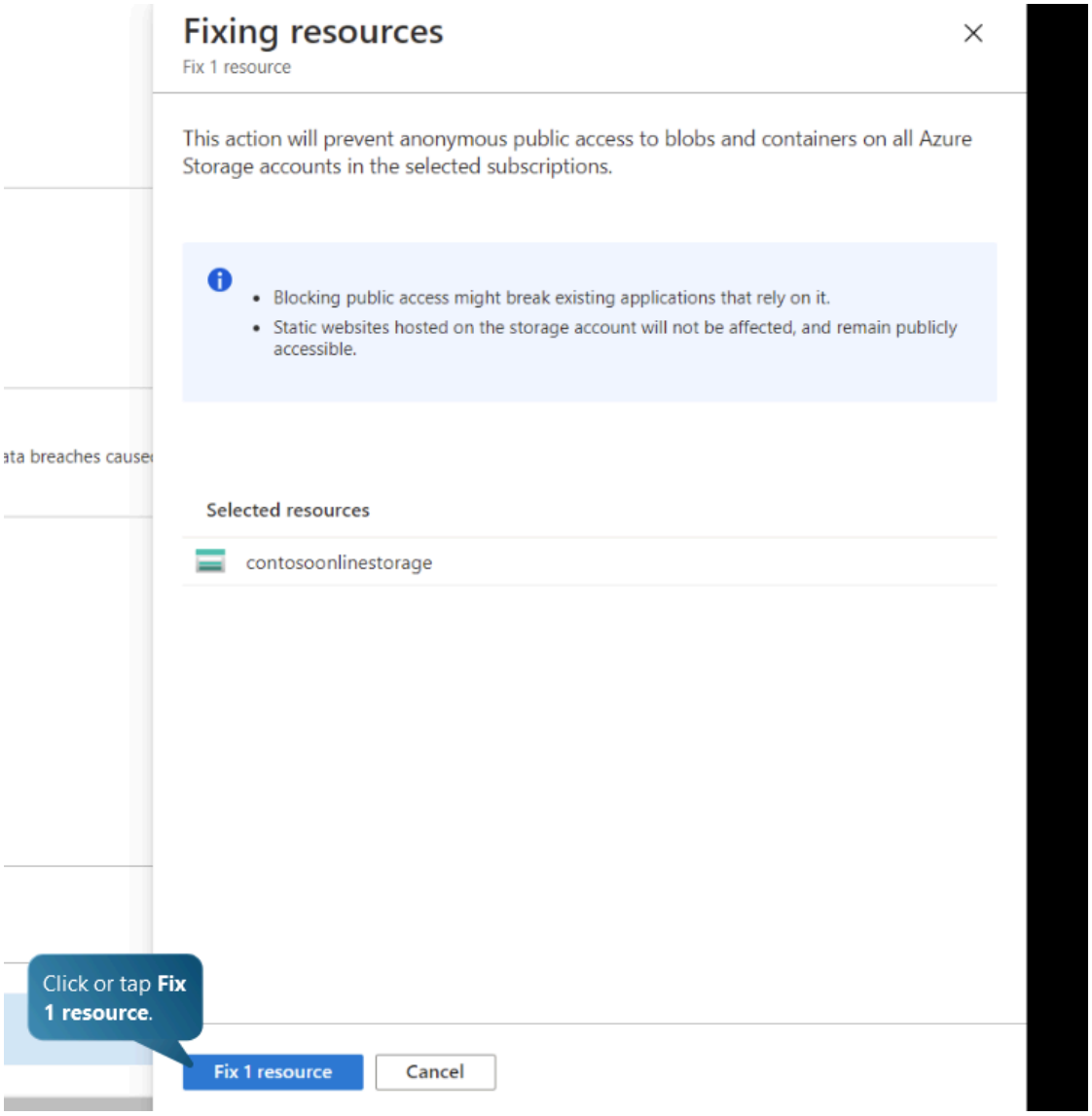
Azure Defender, which is part of **Azure Security Center,** employs a feature called Azure Policy for automatic remediation scripts. Remediation actions are implemented using Azure Policy initiatives with associated remediation tasks.

The remediation tasks are defined using Azure Resource Manager (ARM) templates, which can include **PowerShell scripts**, **Azure CLI commands**, or other applicable configurations based on the specific requirements. These templates are executed automatically when a non-compliant resource is identified.

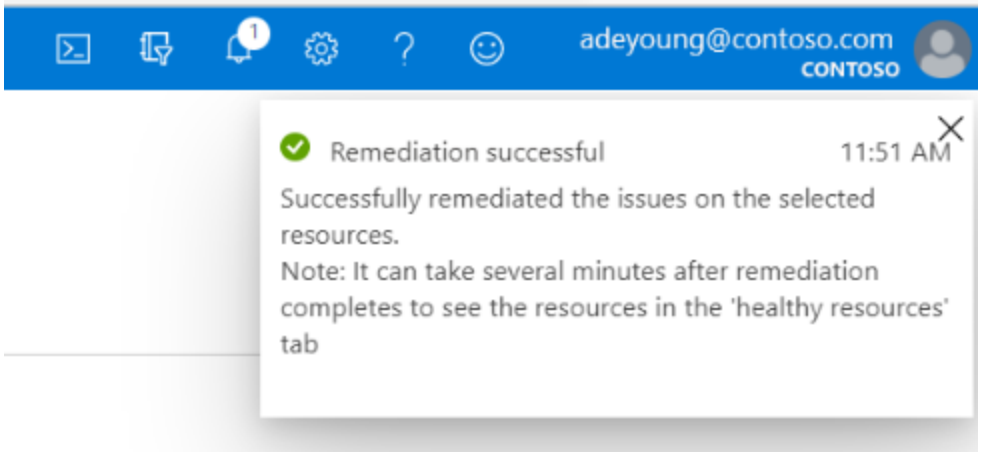
Here is an example of what an Azure Policy initiative with remediation might look like. This script disallows public access to the Azure storage account.

It's important to tailor the remediation scripts according to your specific security and compliance requirements.

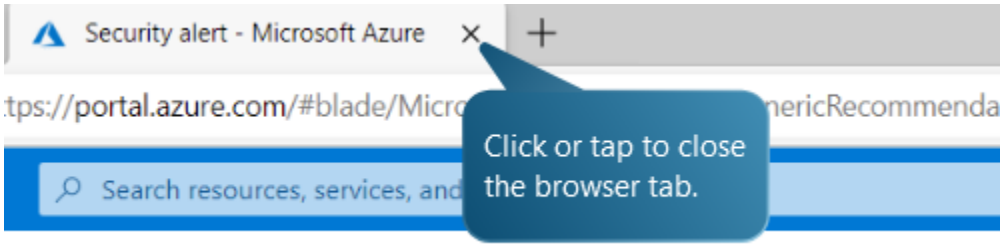




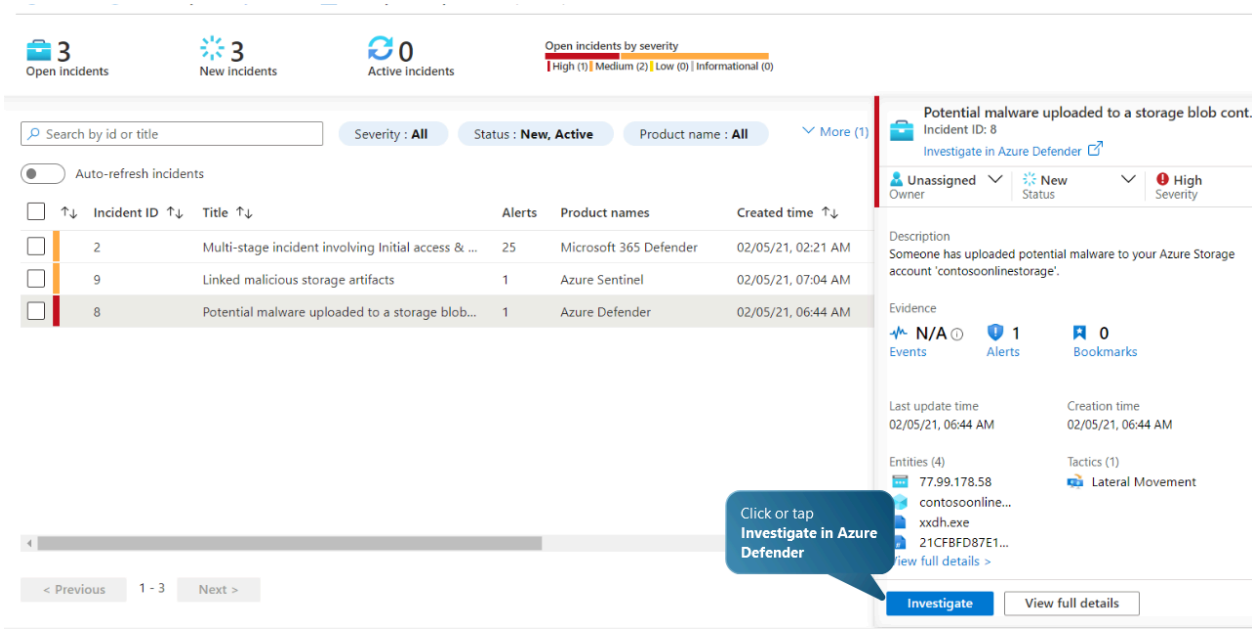
Let's use the quick fix option to resolve the issue.



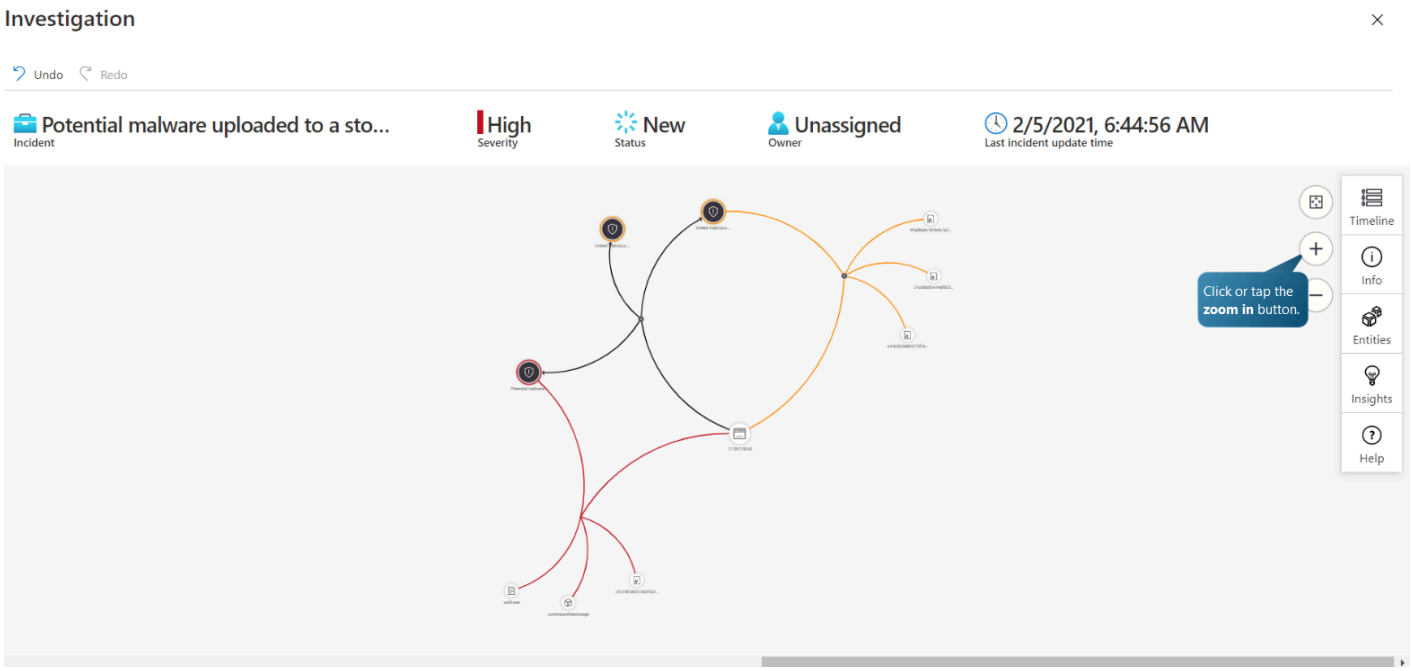
Remediation success!



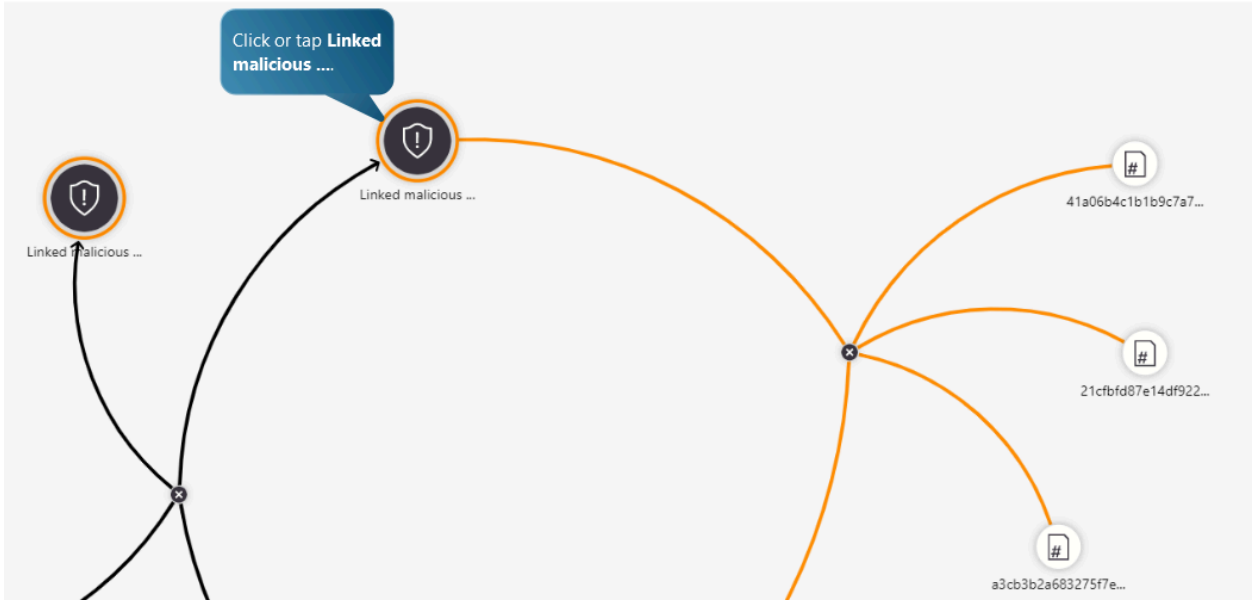
Let's return to Azure Sentinel.



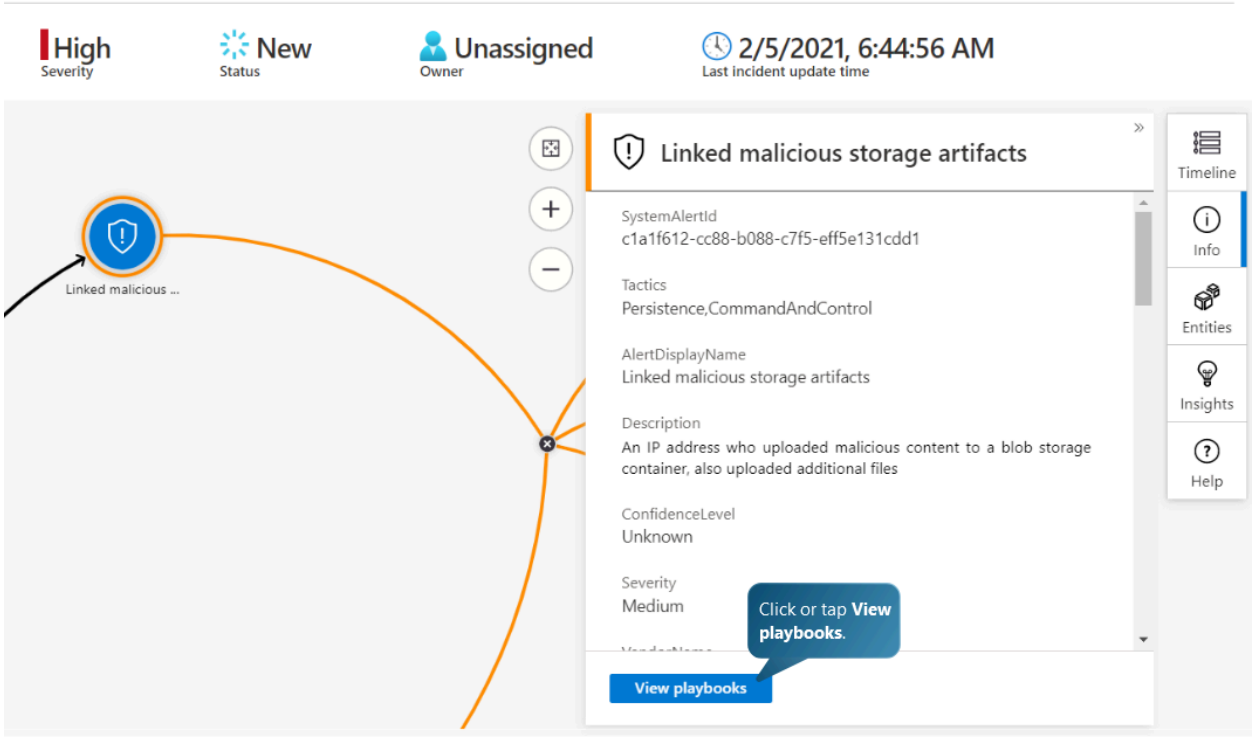
Lets perform a deeper investigation into the impact this attack had.



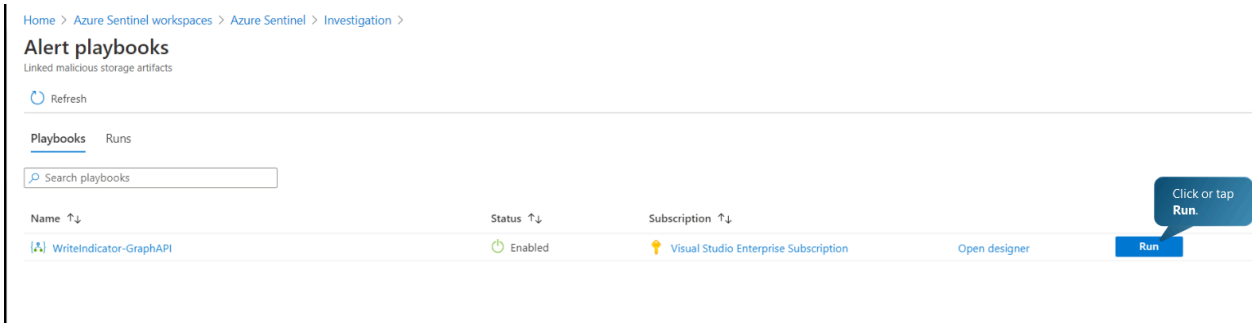
The image above is the investigation graph for the incident. This graph helps an analyst understand the scope, and identify the root cause, of a potential security threat by correlating relevant data with any involved entity.



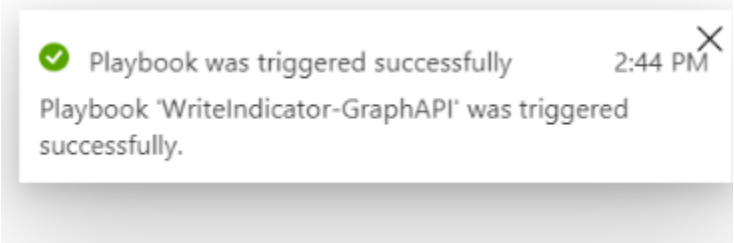
Open the Linked malicious storage artifacts alert detail.

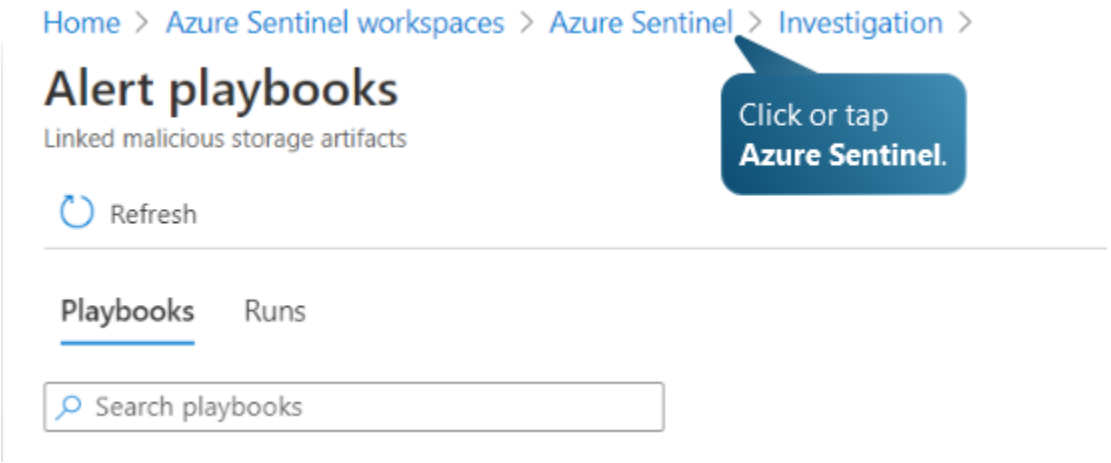


Use these playbooks to share these additional hashes as custom threat intelligence indicators.

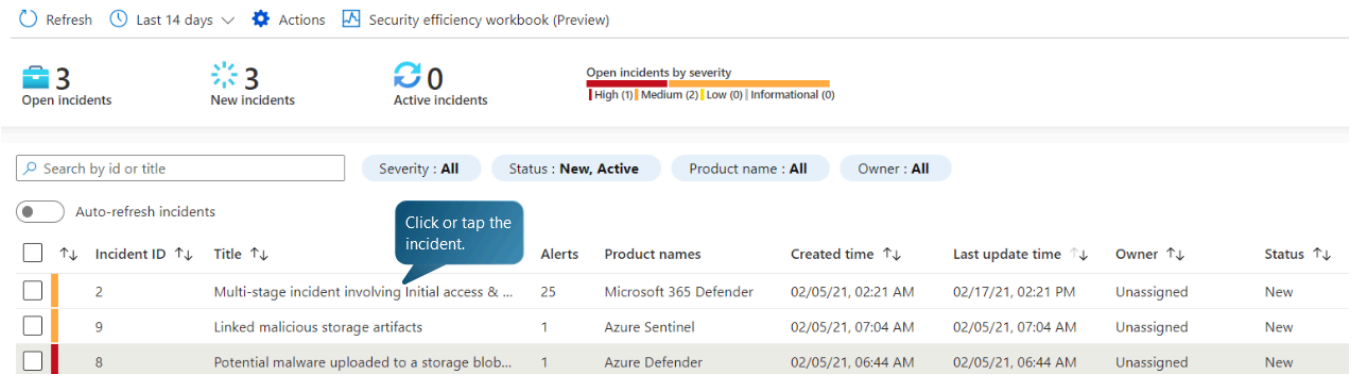


When executed, this playbook will share the new file hashes with Microsoft 365 Defender, enabling Defender to detect the presence of these hashes on machines within our network.

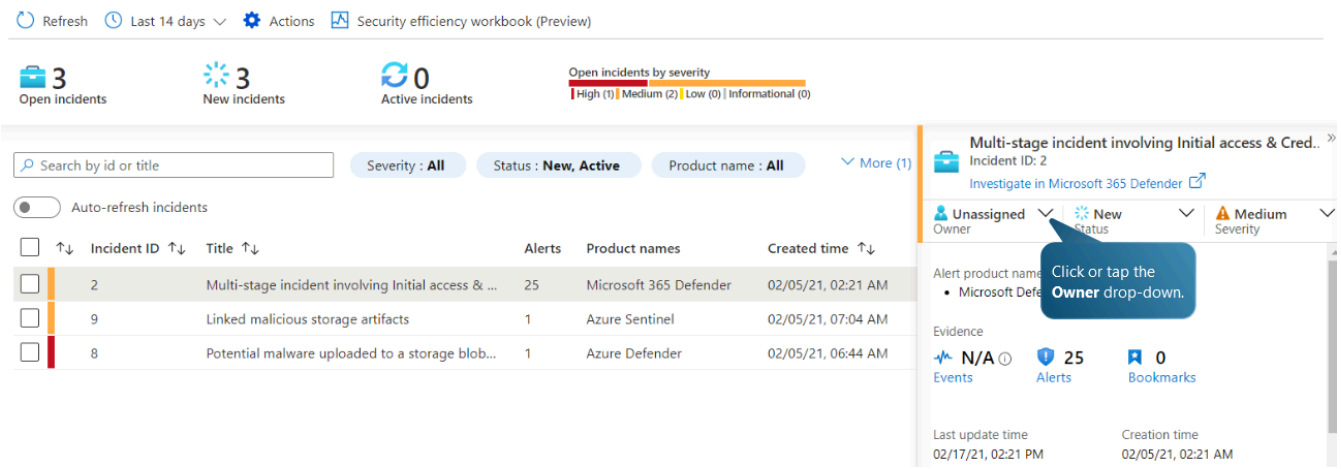




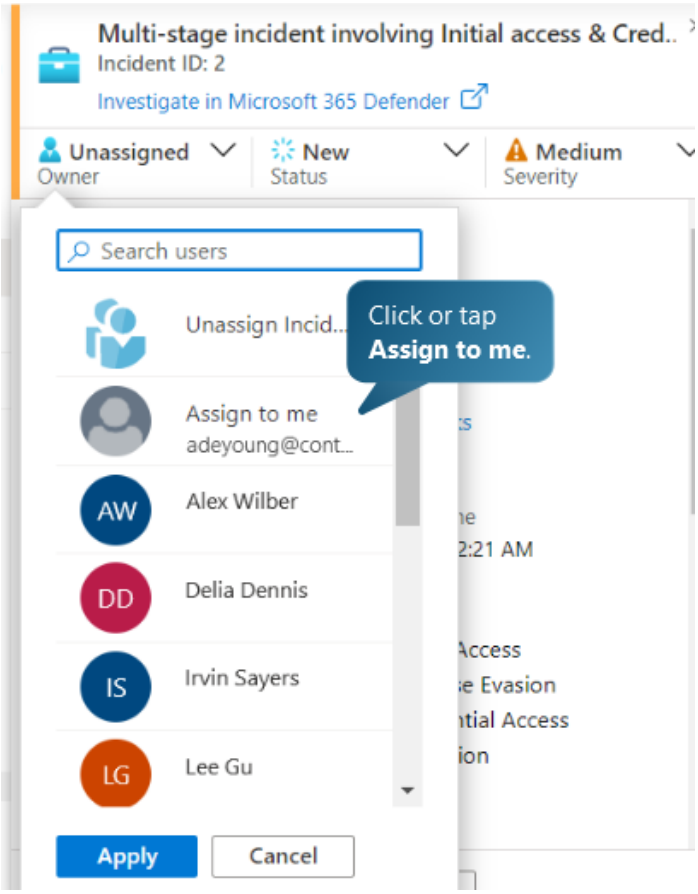
Let's return to the Incidents page to figure out how an attacker gained access to our environment.

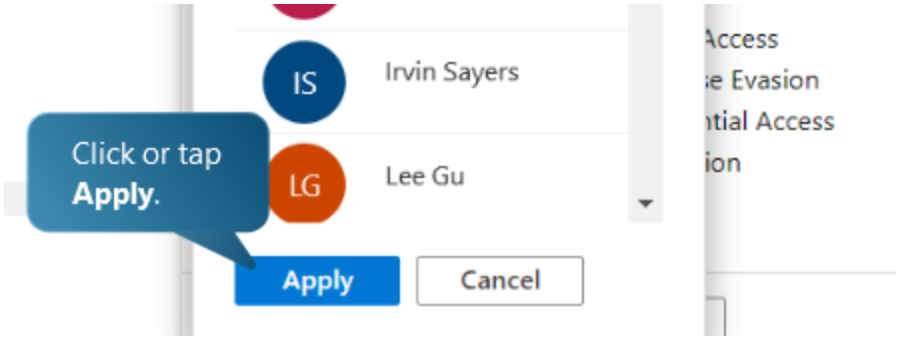


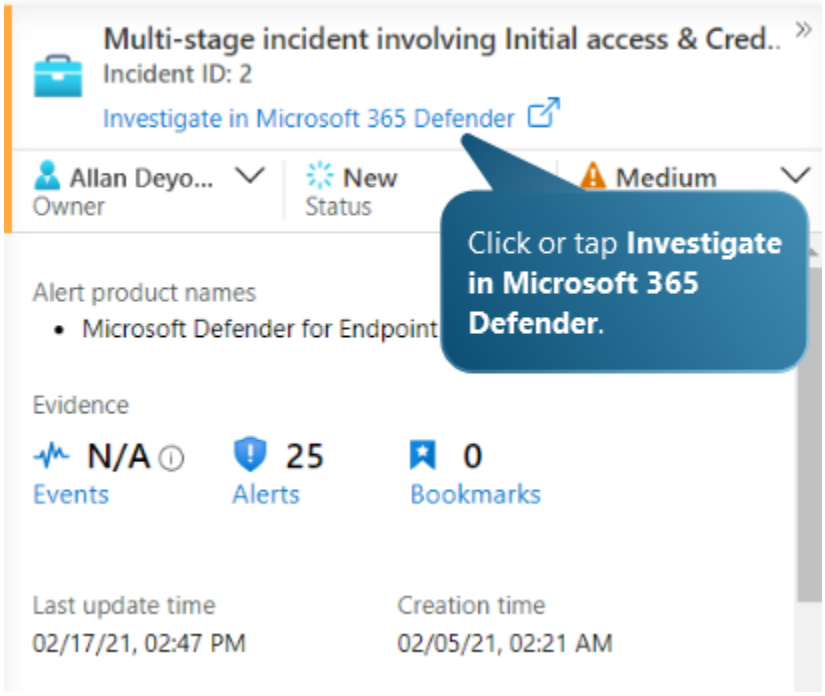
We can see that Microsoft 365 Defender has created an endpoint incident for initial access and credential access. This might tell us how the actor gained a foothold in the network.



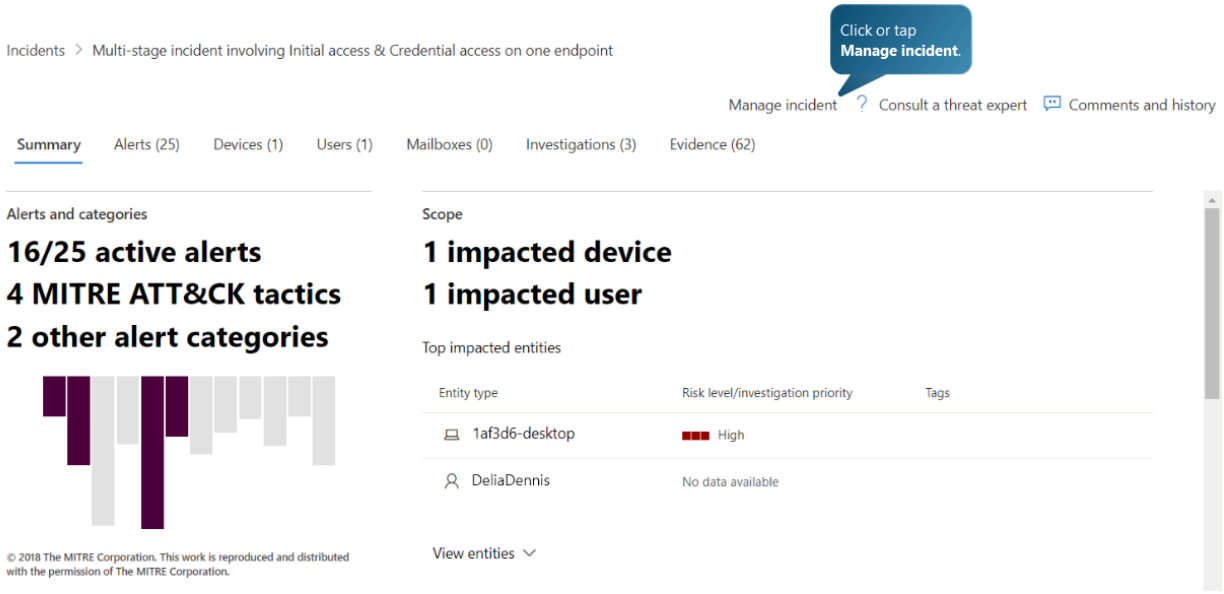
Let’s take ownership of the incident since we’ll be investigating it.



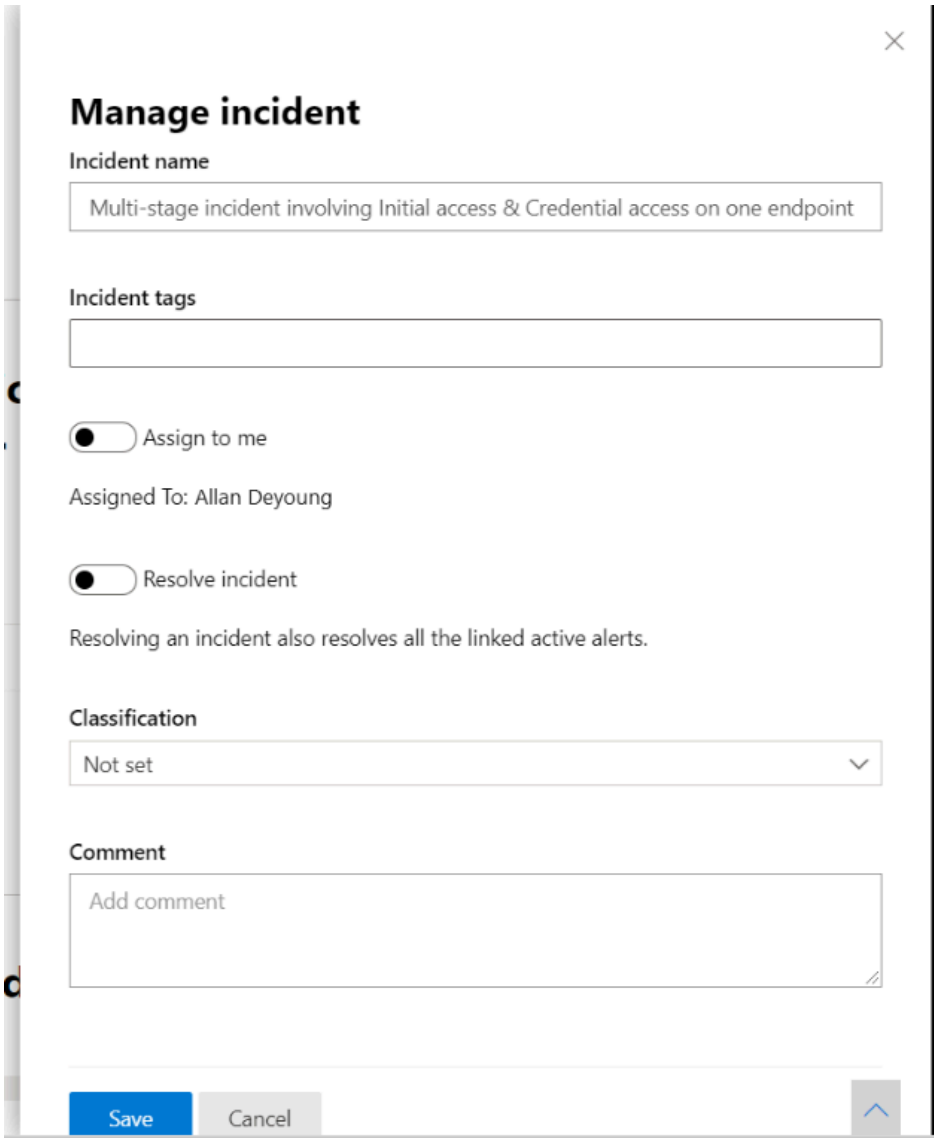

Access
e Evasion
tial Access
ion
IS
Irvin Sayers
LG
Lee Gu
Click or tap **Apply**.
Apply
Cancel


Multi-stage incident involving Initial access & Cred..
Incident ID: 2
Investigate in Microsoft 365 Defender
Allan Deyo...
Owner
New
Status
Medium
Click or tap **Investigate in Microsoft 365 Defender**.
Alert product names
Microsoft Defender for Endpoint
Evidence
N/A
Events
25
Alerts
0
Bookmarks
Last update time
02/17/21, 02:47 PM
Creation time
02/05/21, 02:21 AM

While Azure Sentinel provides a great breadth of information about attacks on the environment, Microsoft 365 Defender enables deep analysis of endpoint exploitation.



The Microsoft 365 Defender page provides a summary of the incident, including associated alerts and categories, the scope, evidence, and other important information about the incident. Before continuing the investigation, let's confirm that the change to the incident has been synchronized.



The incident has been changed to our assigned account!

Summary | Alerts (25) | Devices (1) | Users (1)

Click or tap **Alerts**.

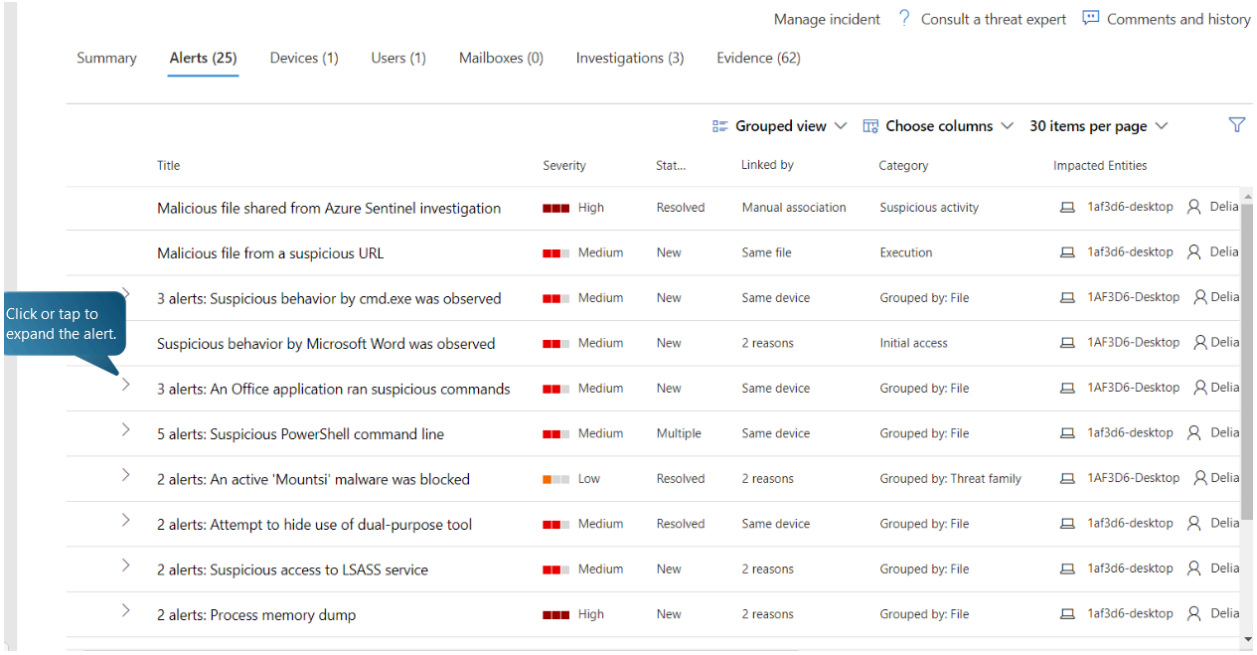
Alerts and categories

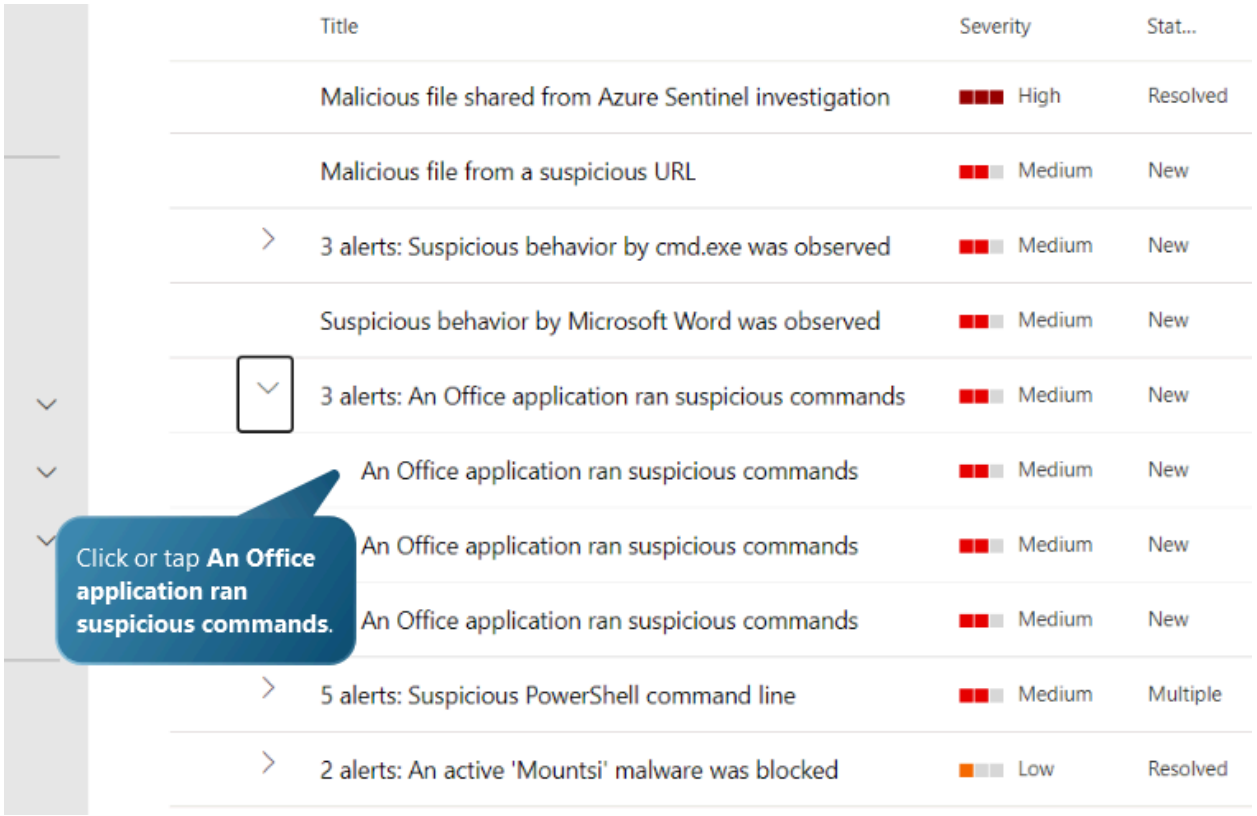
16/25 active alerts

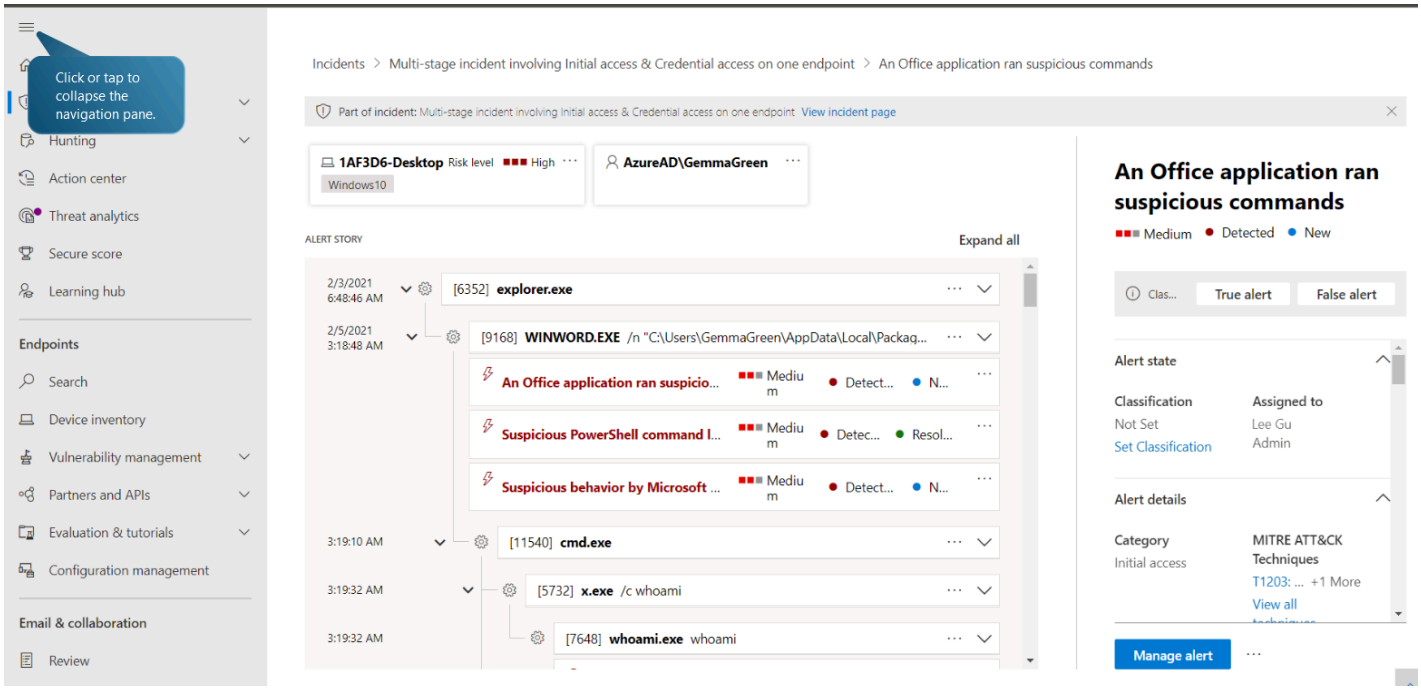
4 MITRE ATT&CK tactics

2 other alert categories

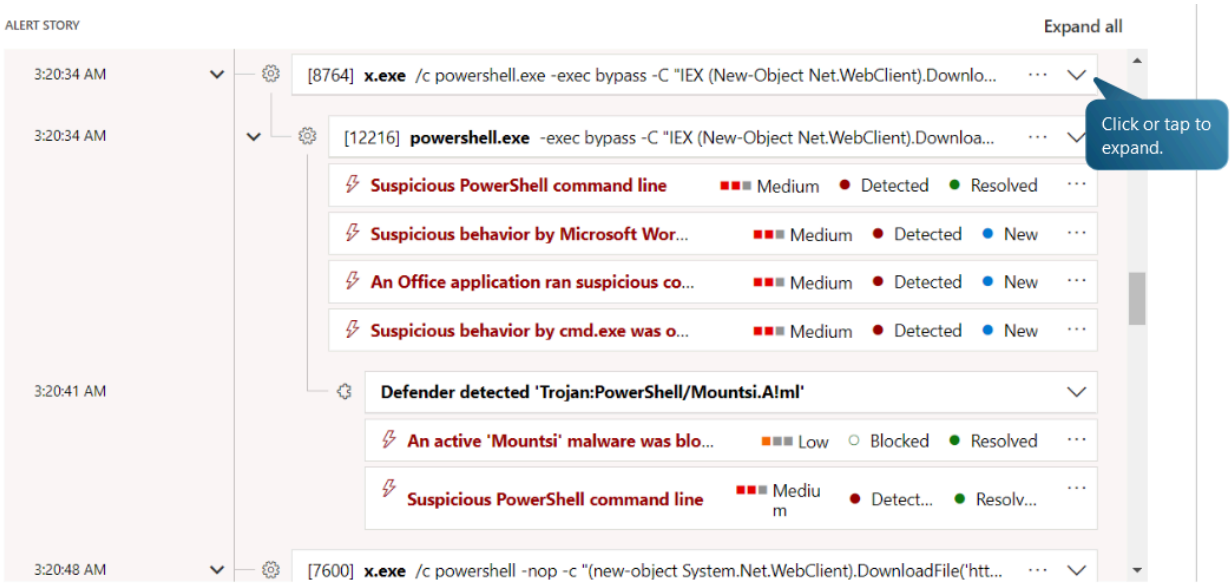
To establish how the attacker gained access to a machine on our network, let's investigate the alerts related to this incident.



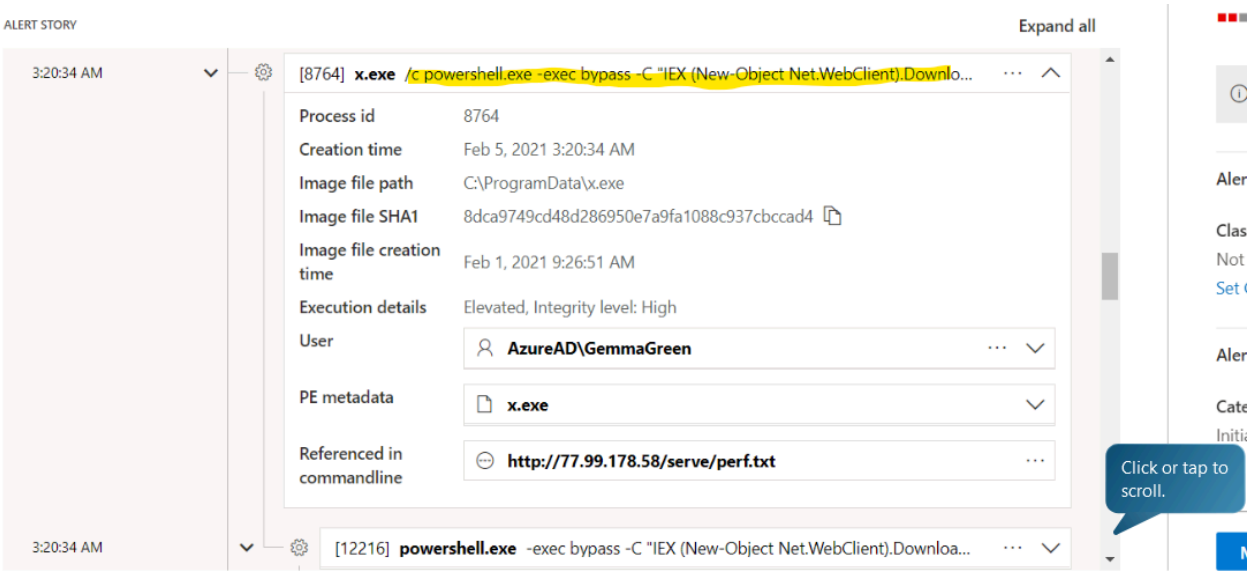




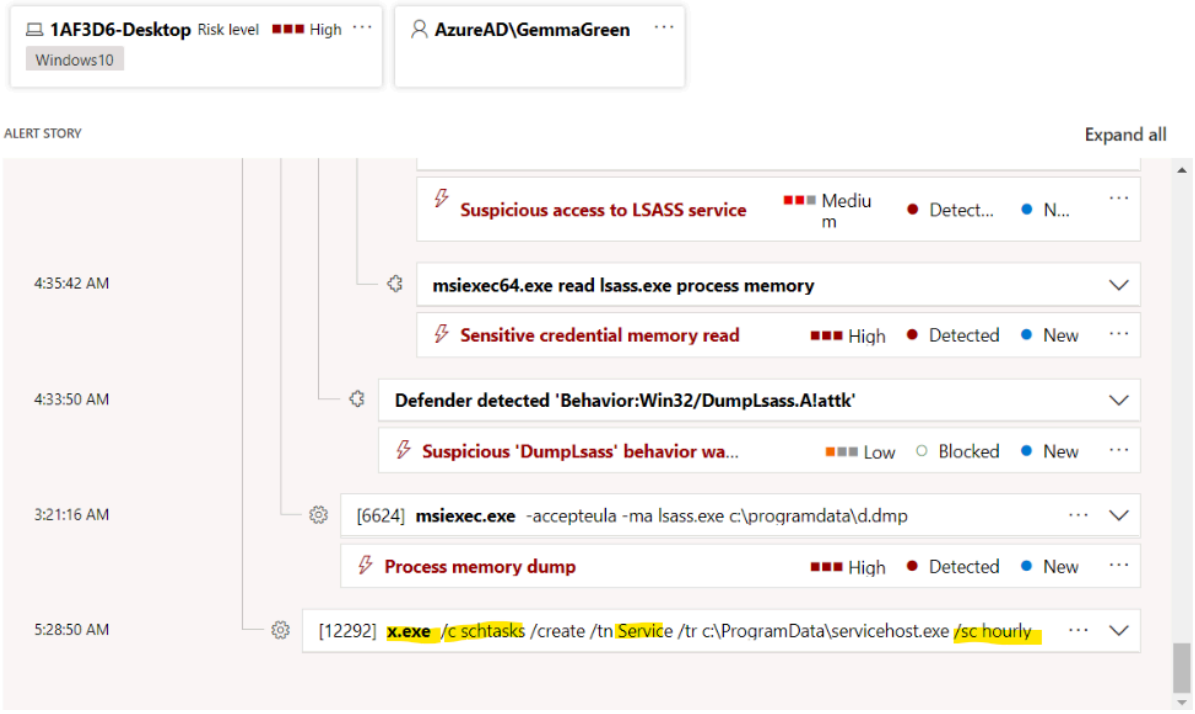
Three alerts were triggered when an application ran suspicious PowerShell commands, which might be when the initial access into our network occurred.



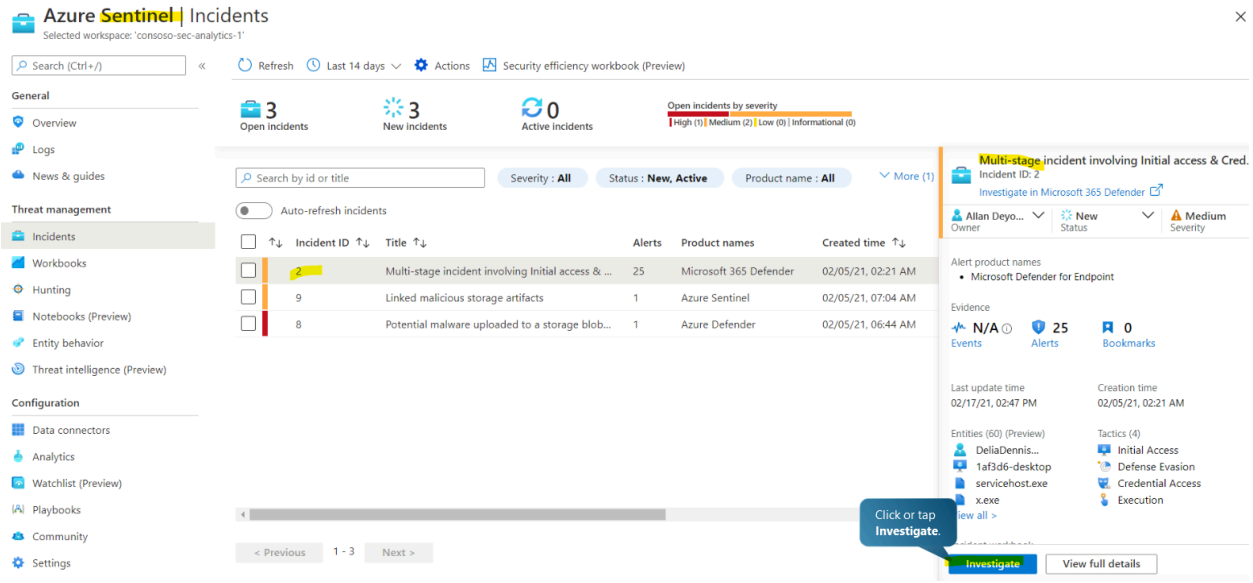
Several reconnaissance commands were executed!



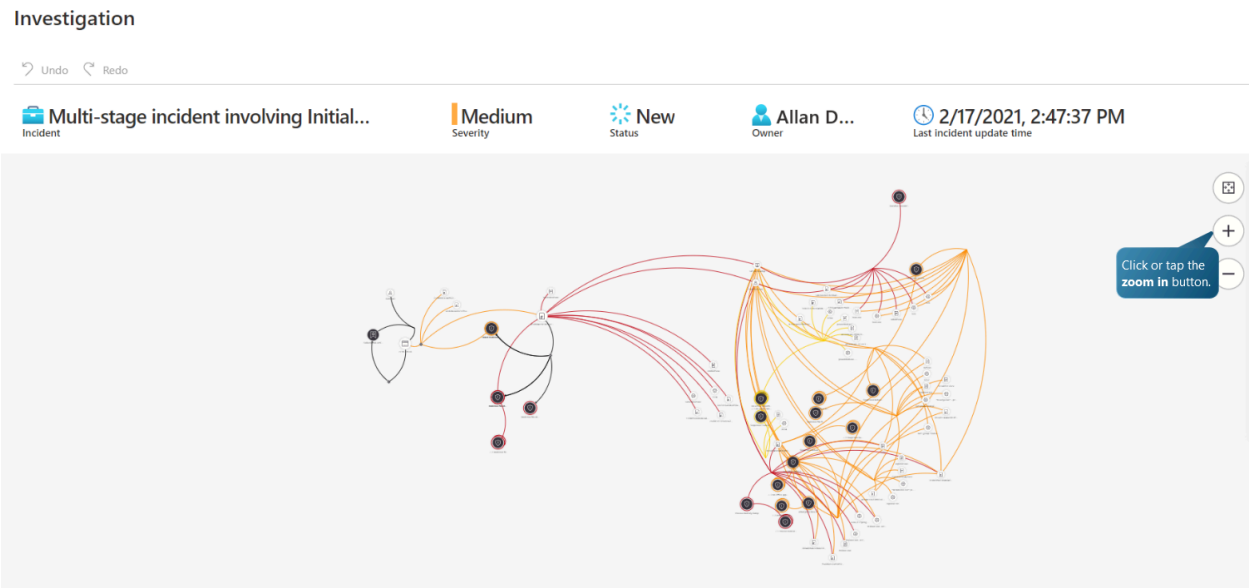
Also, a PowerShell execution occurred that called out to the same IP address we saw implicated in our Azure blob storage attack.



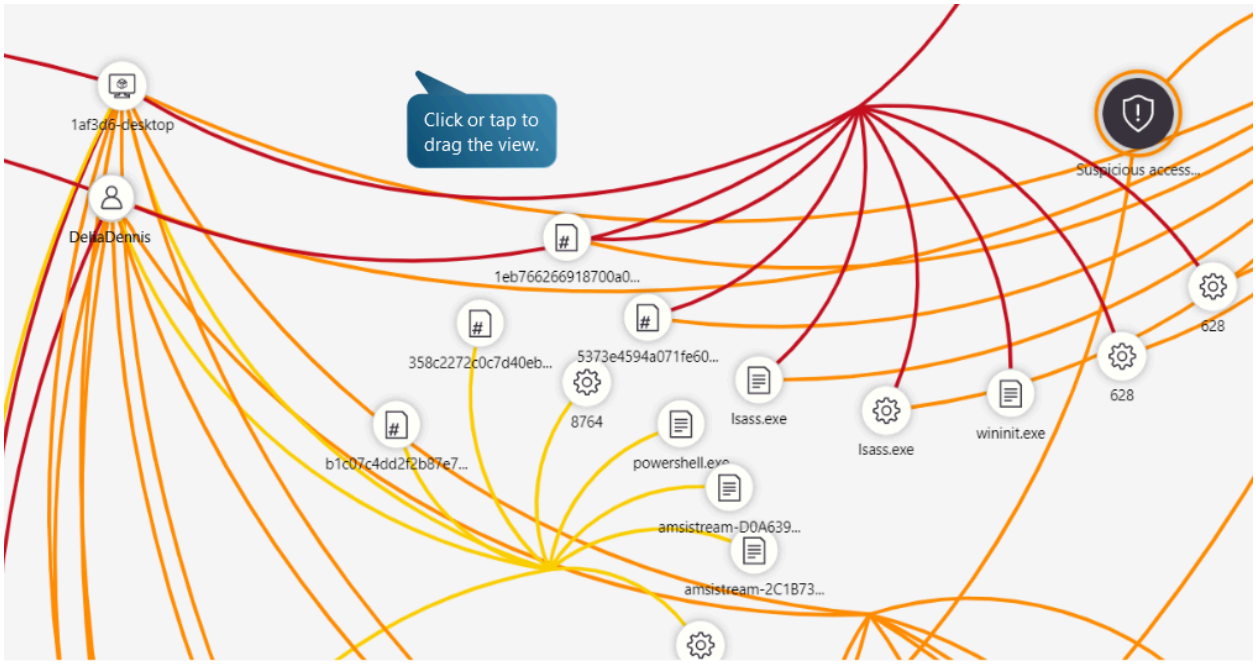
Tasks were then scheduled to run hourly using the binary servicehost.exe



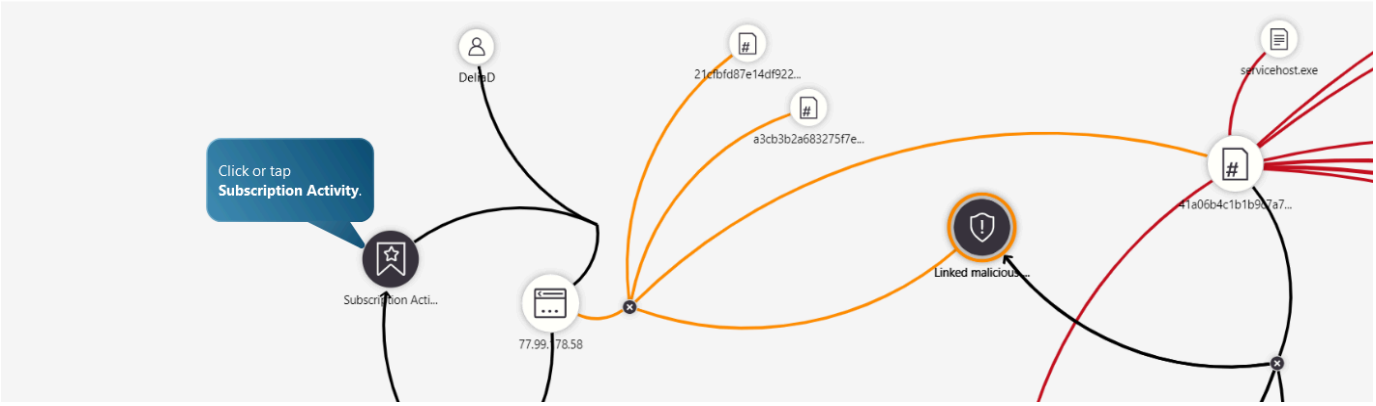
Now I'll return to Azure Sentinel to investigate whether servicehost.exe is associated with any other incidents in our network.



Back to the investigation graph that shows the full scope of the intrusion using first-party and third-party alerts and log sources.



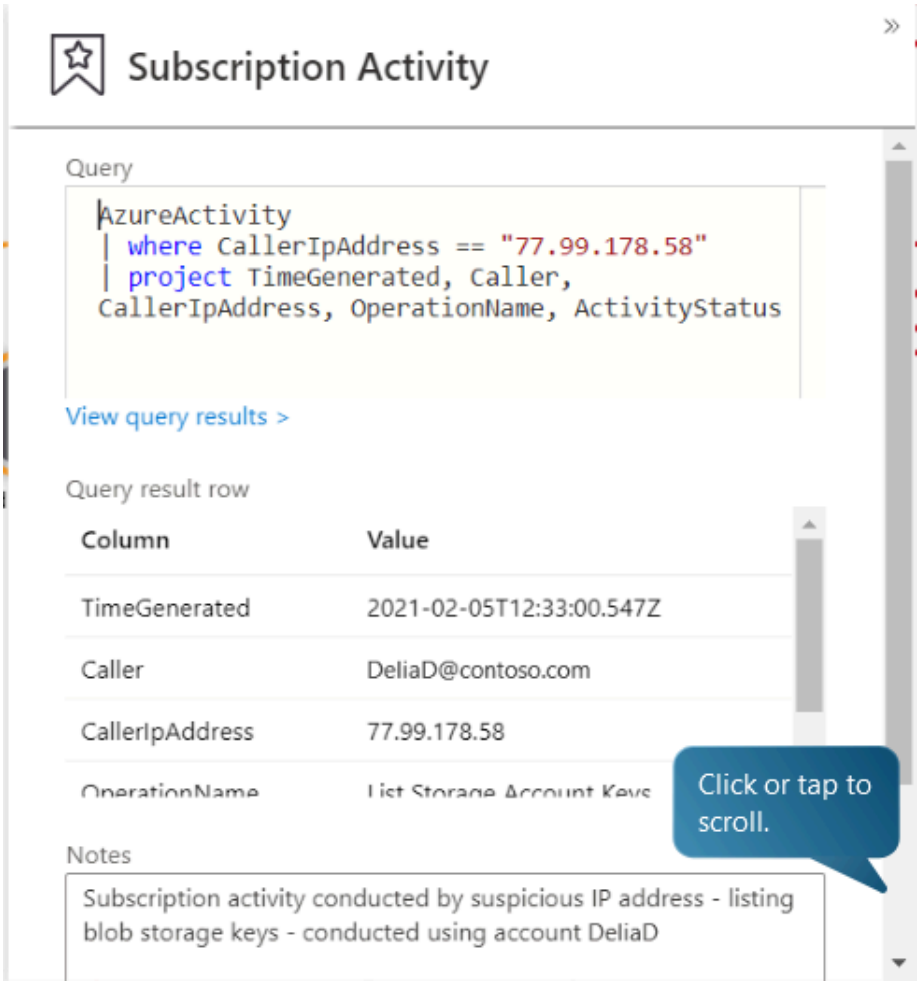
We can see the impacted machine and the user account in the center, as well as the Microsoft 365 Defender alert to the right.



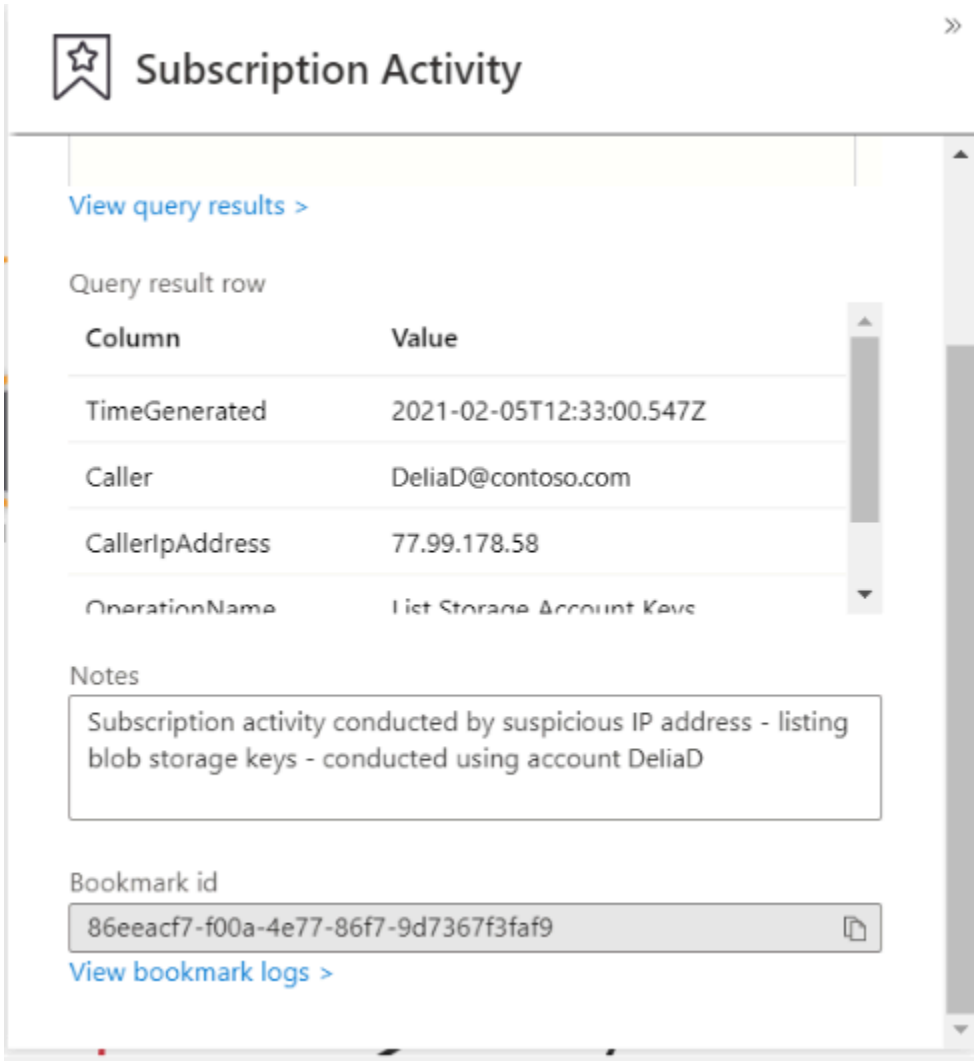
One of the file hashes I saw for the Azure Blob storage alert earlier has been associated with the Microsoft 365 Defender incident. This links the on-promises Microsoft 365 Defender alerts to the Azure Defender Blob storage alert.

The service host file used for persistence on-prem was uploaded to Blob storage by the attacker. The custom detection rule we saw earlier allowed indicator sharing with Microsoft 365 Defender, making this connection possible.

Furthermore, another analyst investigated Azure Activity logs for additional malicious IP activity and bookmarked the hunting query, which is linked to the malicious IP address.



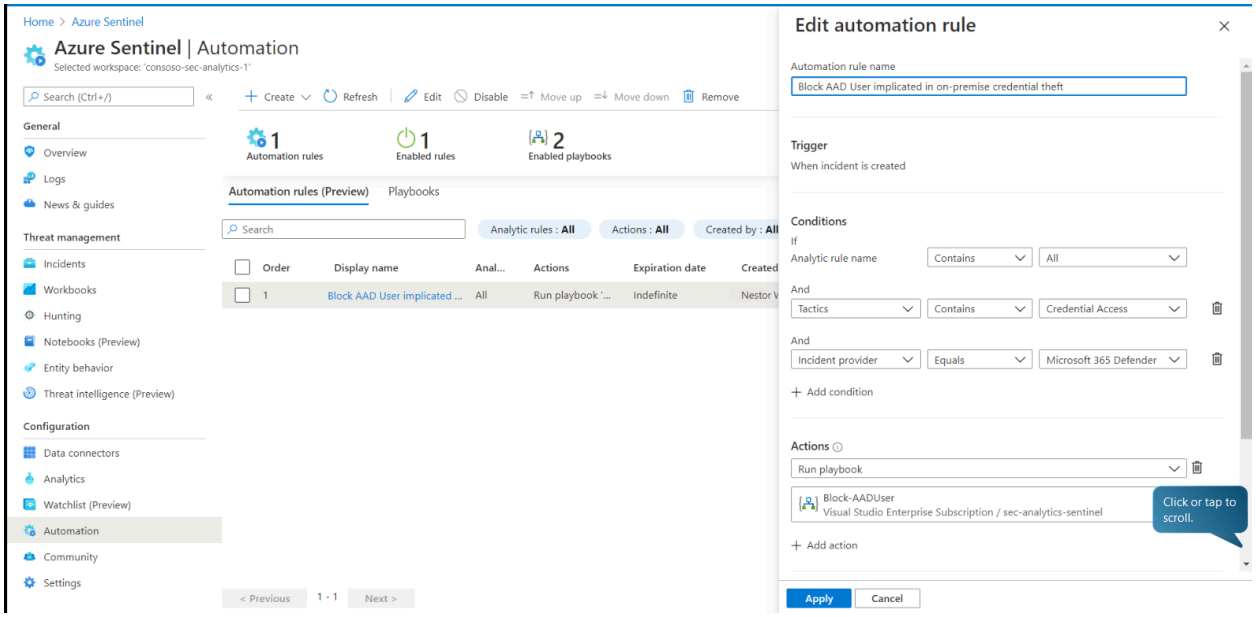
The query results show that the attacker used the user account to view Blob storage keys. The attacker then used the keys to upload files to our Blob storage, likely for use in future campaigns.



Azure Sentinel custom detection rules and custom indicator sharing made it possible to link the on-premises incident with the cloud incident.

If we wanted to, we could further enrich the attacker IP address details by bringing third-party logs and alerts into Azure Sentinel. For example, we could bring in Cisco ASA logs using the Cisco ASA connector, which would also allow us to determine if the attacker IP has been accessing our on-prem network.

Now that the incident was investigated, let's see what actions were taken in response to the attack.



When an incident is created, the rule checks if any analytic files have tactics containing credential access and if the incident provider was Microsoft 365 Defender. If so, the playbook will execute to block the Azure Active Directory user.

Summary:

This playbook automation blocked the compromised account in Azure Active Directory before our investigation even started, removing the attackers access, and allowing us time to investigate the scope of the attack.

This is a table-top exercise learning how to detect and respond to modern attacks with unified Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) capabilities.