



Microsoft Defender Advanced Threat Protection

Attack simulation

Scenario 4: Automated investigation
(fileless attack)

February 2019

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.

© 2019 Microsoft. All rights reserved.

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

All other trademarks are property of their respective owners.

Our detection philosophy

It's simple.

We make sure that known advanced persistent threat (APT) indicators or techniques are visible in our telemetry, that we recognize them, and that we are able to raise the relevant alerts.

When we raise an alert near real-time, 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, including known threat components previously observed on real machines, 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 generated mainly by Microsoft's own APT hunting and research teams, but enriched by collaboration with partners and shared 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) analyst to validate and address. With the help of information about proximate events on the same machine and other relevant machines, 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: Automated investigation of a fileless attack

In this scenario, we simulate a fileless attack executed in memory, and let the *automated investigation* in Microsoft Defender ATP kick in, providing automated SOC attack response: triage, investigate, and remediate. During the response, automated investigation identifies and removes known attack artifacts from the affected machine. It can also automatically pivot to other machines that may be affected and apply the same response actions.

To trigger automated investigation, we leverage the same attack from [Scenario 2: PowerShell script in fileless attack](#). In this scenario, the simulated attack leverages advanced techniques to stay under the detection radar. These attacks “live off the land” by using only existing system and administrative tools and injecting their code into system processes to hide their execution and persist.

We will also explore how exploit protection in Windows 10 can help prevent attackers from being able to carry out some of their activities.

In this simulation, our example scenario starts with a PowerShell script. A user may be tricked into executing such a script, or the script may be executed remotely from another machine in the organization that was previously infected, with the attacker attempting to move laterally in the network. Detection of such scripts is difficult because administrators also often run scripts remotely to carry out various administrative activities.

During the simulation, the attacker goes on to inject some shellcode into a seemingly innocent process, in this case *notepad.exe*. We chose this process for the simulation, but attackers will more likely target a long-running system process like *svchost.exe*. The shellcode then goes on to contact the attacker’s command-and-control (C&C) server to receive instructions on how to proceed.

Following the detection of this fileless attack, automated investigation will kick in, analyzing the memory context of the entities involved and then automatically incriminating the malicious process and remediating it.

The test machine require for this simulation should:

- Be onboarded to Microsoft Defender ATP
- Run [Windows 10 version 1809 preview](#)
- Have PowerShell turned on
- Have [Windows Defender Antivirus](#) turned on

For onboarding instructions, [read to the product guide](#). We recommend running the local onboarding script to onboard the test machine.

Run the simulation

To run this attack scenario, follow these steps:

1. On the designated test machine, log in to the Microsoft Defender ATP portal and go to **Help (?) > Simulations & tutorials**.

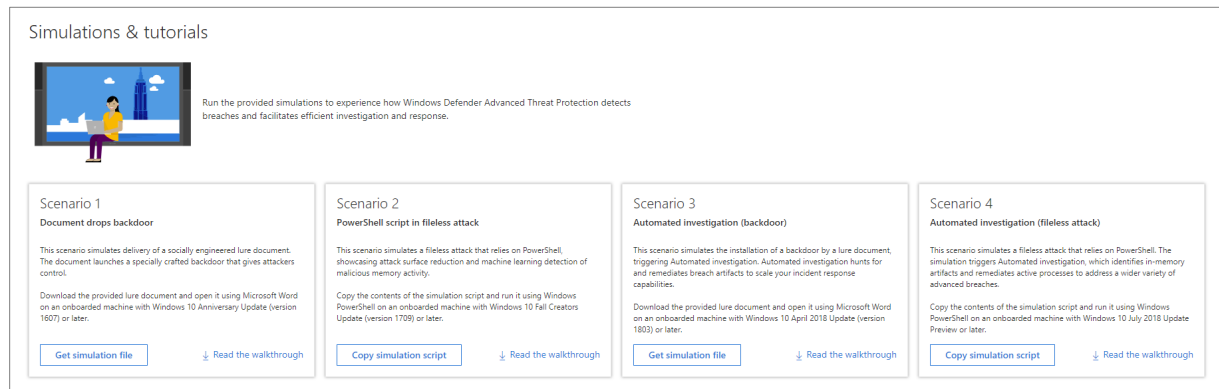


Figure 1. Simulation scenarios in the portal


2. Click the **Copy simulation script** button under **Scenario 4: Automated investigation (fileless script)** to copy the PowerShell script.
3. Open a Windows PowerShell window with administrative privileges on the test machine.
4. At the prompt, paste and run the provided script.

A few seconds later, *notepad.exe* is started and the simulated attack code is injected into it. The simulated attack code attempts communication to an external IP address simulating the C&C server.

Simulate the attack with exploit protection

With [exploit protection](#) introduced with Windows 10 Fall Creators Update (version 1709), policies can be applied to restrict how code runs on machines, mitigating many exploit-based attacks. Exploit protection detections are surfaced as alerts by Microsoft Defender ATP to provide SOC personnel with visibility into these events.


In this section, we will configure *exploit protection* so that it disallows dynamic code execution in our process of interest, *notepad.exe*, and then run the simulated attack again.

 **Note:** This section demonstrates how exploit protection stops attempts at process injection and other in-memory attack activities. You can proceed to explore automated investigation without completing this section.

To simulate the attack with exploit protection:

1. Open a Windows PowerShell window with administrative privileges.
2. At the prompt, run the following commands to configure exploit protection:

```
$path = "HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\notepad.exe";  
$value = ([byte[]](0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x11,0x11,0x01,0x01,0x00,0x00));  
New-Item -Path $path -Force;  
New-ItemProperty -Path $path -Name "MitigationOptions" -Value $value -PropertyType Binary -Force
```

 **Note:** The exploit protection configuration provided here is solely to illustrate pertinent functionality. This configuration should not be applied to other machines in production without proper analysis of its impact.

3. Now run the provided attack PowerShell script from the [Simulations & tutorials](#) page again.

The script starts *notepad.exe* again, injects its malicious shellcode into it, and attempts to execute it as before. This time, however, it is stopped by exploit protection, which causes *notepad.exe* to be terminated.


4. [Optional] To restore exploit protection settings on the test machine, run the following command in the PowerShell window:

```
Remove-ItemProperty -Path $path -Name "MitigationOptions" -Force
```

Congrats – you’re done running the attack!

The attack simulation ends here. A real attacker, if successful, would likely continue to scan for information, send collected reconnaissance information to a command-and-control (C&C) server, and use this information to move laterally and pursue other attractive targets.

Next, let’s review and investigate the Microsoft Defender ATP alerts that surfaced the simulated attack.

 **Note:** Alerts should start to appear 15-30 minutes after the simulated backdoor is launched.

Investigate the attack in the portal

Let's switch into our defender role and explore the attack from the SOC point of view in the Microsoft Defender ATP portal.

1. Open the Microsoft Defender ATP portal on <https://securitycenter.windows.com> from any machine.
2. Log in with your Microsoft Defender ATP credentials. Default global administrator credentials are provided with your signup email.
3. After 15-30 minutes of the simulated attack, you should find several new alerts on the dashboard.

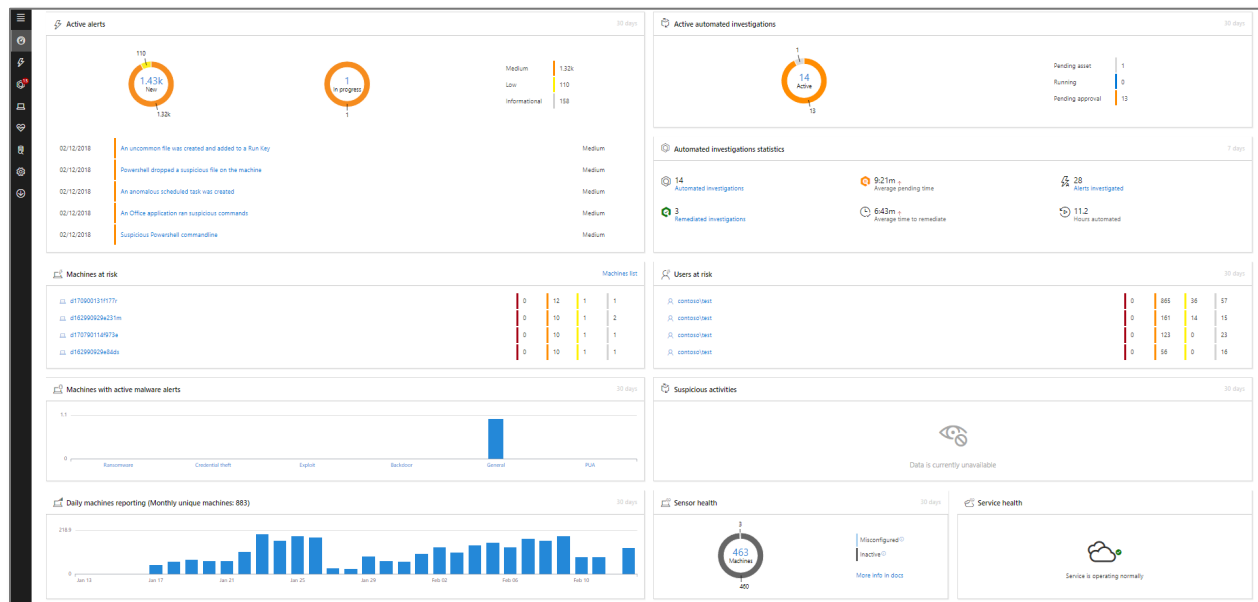



Figure 2. Dashboard view showing the alerts

- Select the item **Suspicious process injection observed** to navigate the corresponding [alert details page](#). In the alert details page, a badge will indicate that automated investigation has been started and the status of the investigation.



Suspicious process injection observed


This alert is part of larger incident [\(2489\)](#)

Actions

Severity: Medium

Category: Installation

Detection source: EDR



Automated investigation is waiting for user approval ([3587](#)) ⓘ

Description

A process abnormally injected code into another process, As a result, unexpected code may be running in the target process memory. Injection is often used to hide malicious code execution within a trusted process.

As a result, the target process may exhibit abnormal behaviors such as opening a listening port or connecting to a command and control server.

Figure 3. Alert page showing that an automatic investigation has been started

Explore the automated investigation and approve pending remediation actions

Microsoft Defender ATP provides detailed information about each investigation. By default, it waits for user approval before performing corresponding remediation actions.

1. Click the investigation ID on the automated investigation badge to view detailed investigation information.

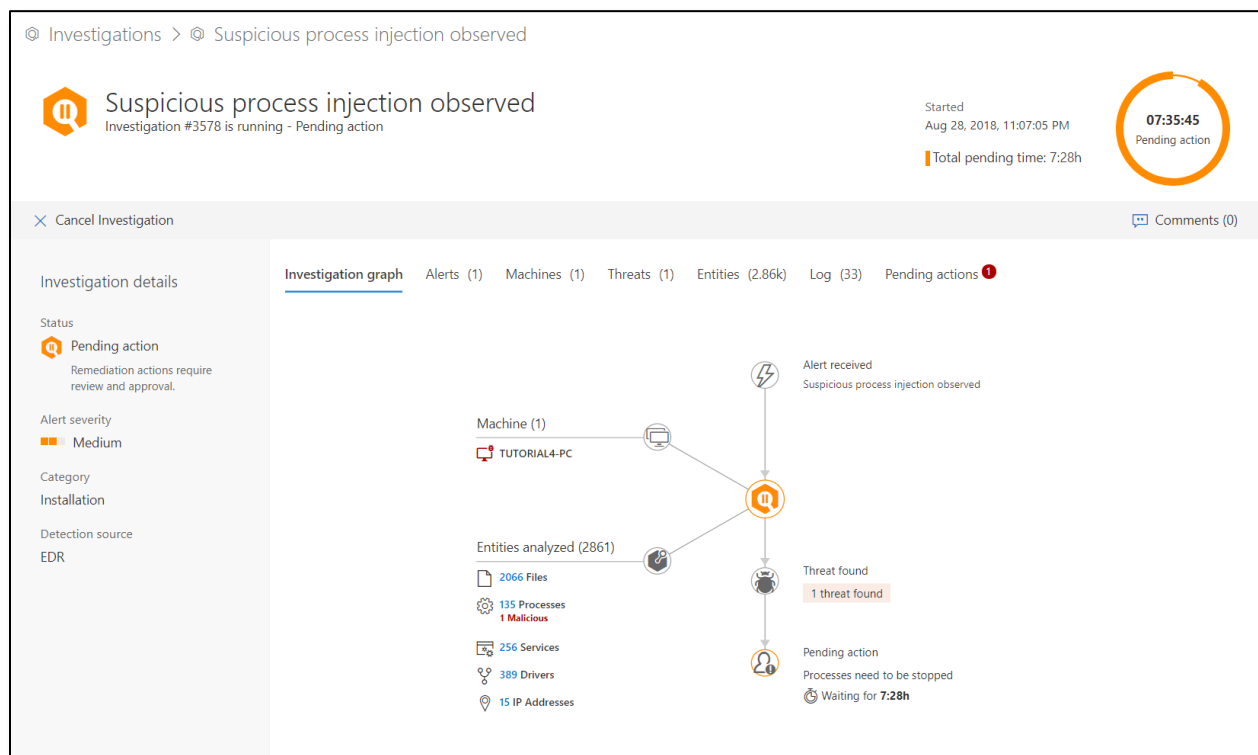



Figure 4. Investigation details page

The [investigation details](#) page shows:

- The alert(s) that triggered the automated investigation
- The machines involved. If indicators are found on additional machines, these additional machines will be listed as well.
- The entities or artifacts found and analyzed: files, processes, services, drivers, and network addresses. These entities have been analyzed for possible relationships to the alert and have been rated as benign or malicious.
- Threats found—known threats that are identified found during the investigation

 **Note:** Depending on timing, the automatic investigation may be still running. Give it a few minutes to fully collect and analyze evidence and prepare the results. Refresh the investigation page to get the latest findings.

- When the automated investigation has completed, a notification message indicates remediation actions that require analyst action.

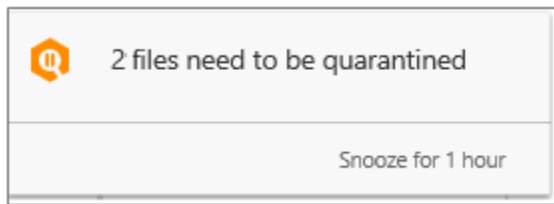
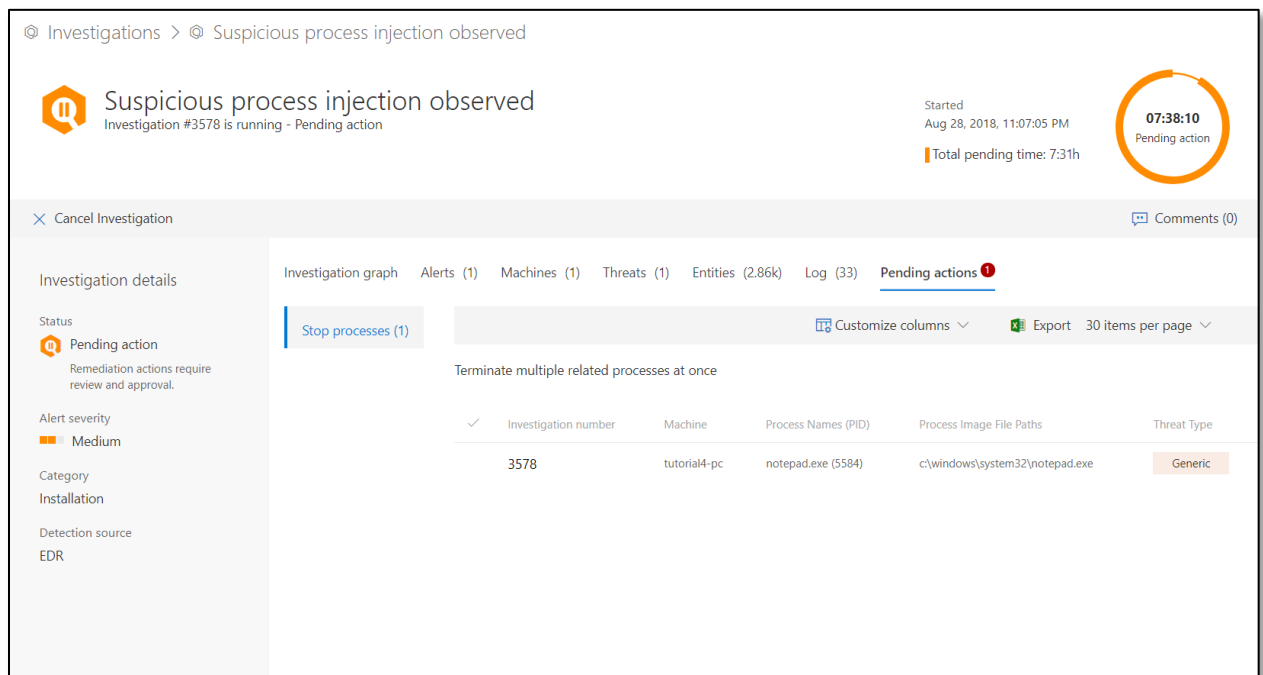


Figure 5. Notification for pending remediation actions

- Click the notification to view the pending actions. Or go to the investigation details page and click **Pending actions**.

During the automated investigation, Microsoft Defender ATP identified *notepad.exe* process, which was injected into, as one of the artifacts requiring remediation. By default, Microsoft Defender ATP will await your approval before proceeding, but you can configure it under the [machine group settings](#) to skip this step and apply remediation automatically.



The screenshot shows the 'Suspicious process injection observed' investigation page. The status is 'Pending action' for investigation #3578. A timer indicates 07:38:10 remaining. The 'Pending actions' tab is active, showing a table of processes to be terminated.

Investigation number	Machine	Process Names (PID)	Process Image File Paths	Threat Type
3578	tutorial4-pc	notepad.exe (5584)	c:\windows\system32\notepad.exe	Generic

Figure 6. Pending actions

- Click on **Approve** to approve the remediation action for all artifacts linked to the attack. Once you approve, automated investigation stops the injected process.

You can see *notepad.exe* disappear from the list of running process on the test machine. When completed, the investigation status changes to **Fully remediated**.

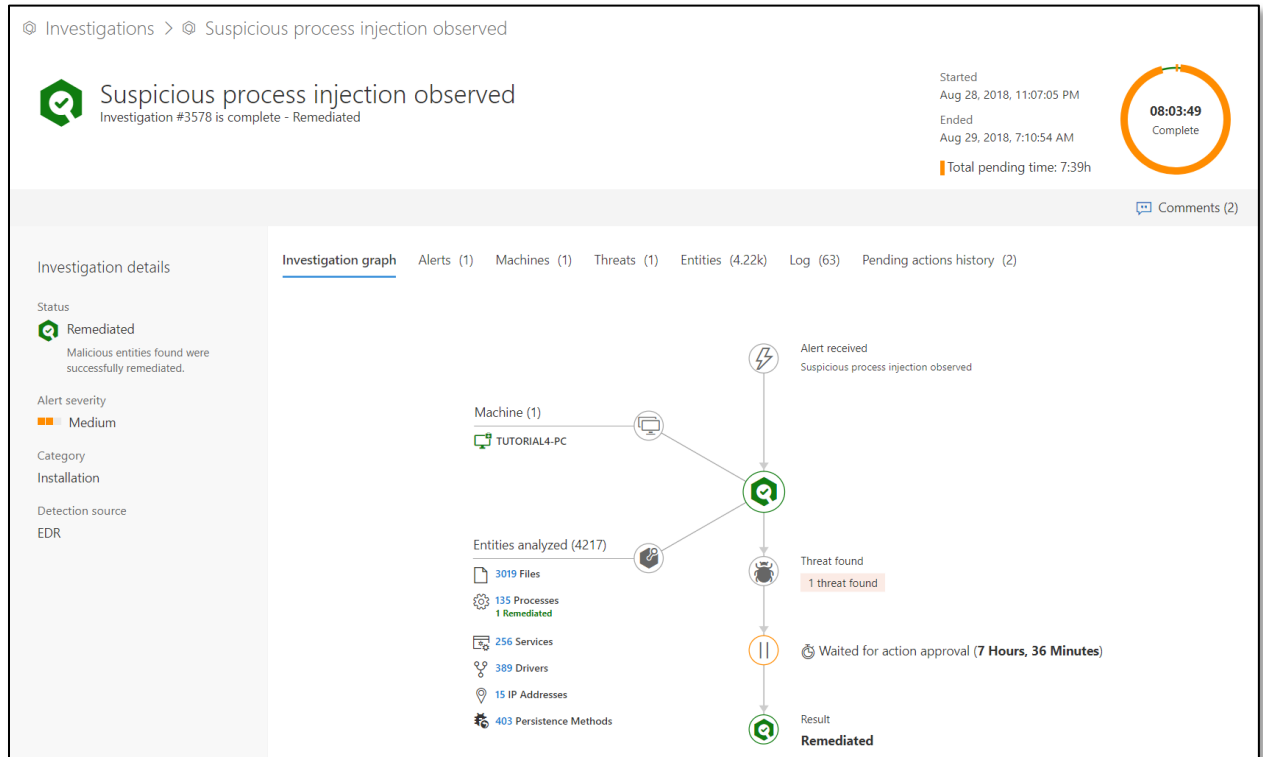


Figure 7. The investigation details page after full remediation

Resolve alerts

When you've completed investigating and remediating an alert, whether manually or automatically, you will want to resolve it. Resolving an alert removes it from the active alerts queue.

The simulated attack generates the following Microsoft Defender ATP alerts:

- Suspicious process injection observed
- Unexpected behavior observed by a process run with no command line arguments
- EAF violation blocked by exploit protection (not generated if the section about exploit protection is skipped)

For detailed information about these alerts, see the walkthrough document for [Scenario 2: PowerShell script in fileless attack](#).

To resolve an alert:

1. Locate the alert in **Alerts > New** or **Alerts > In progress**.
2. Select **Manage alert** from the **More [...]** menu that corresponds to the alert. The [alert management pane](#) opens.
3. Set the alert status to Resolved and classify the alert appropriately:
 - True alert – the alert correctly identified malicious activity
 - False alert – the alert incorrectly identified benign activity as malicious

In either case, provide additional information about the nature of the detection by choosing the most appropriate classification.

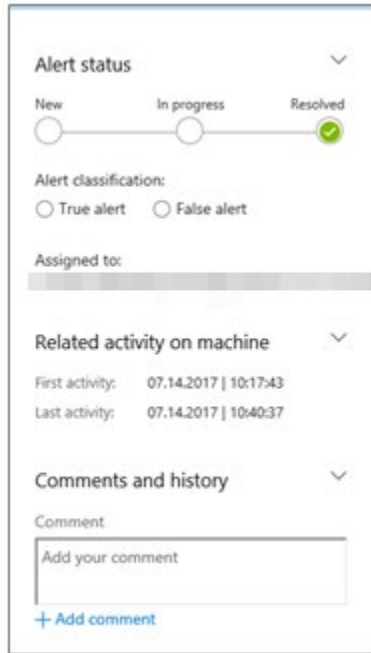


Figure 8. Alert management pane showing resolved alert

Review the reports

Before concluding the investigation, it's a good idea to look at the reports dashboard. It provides high-level information about alerts and machine related information generated in your organization. The report includes trends and summary information on alerts and machines.

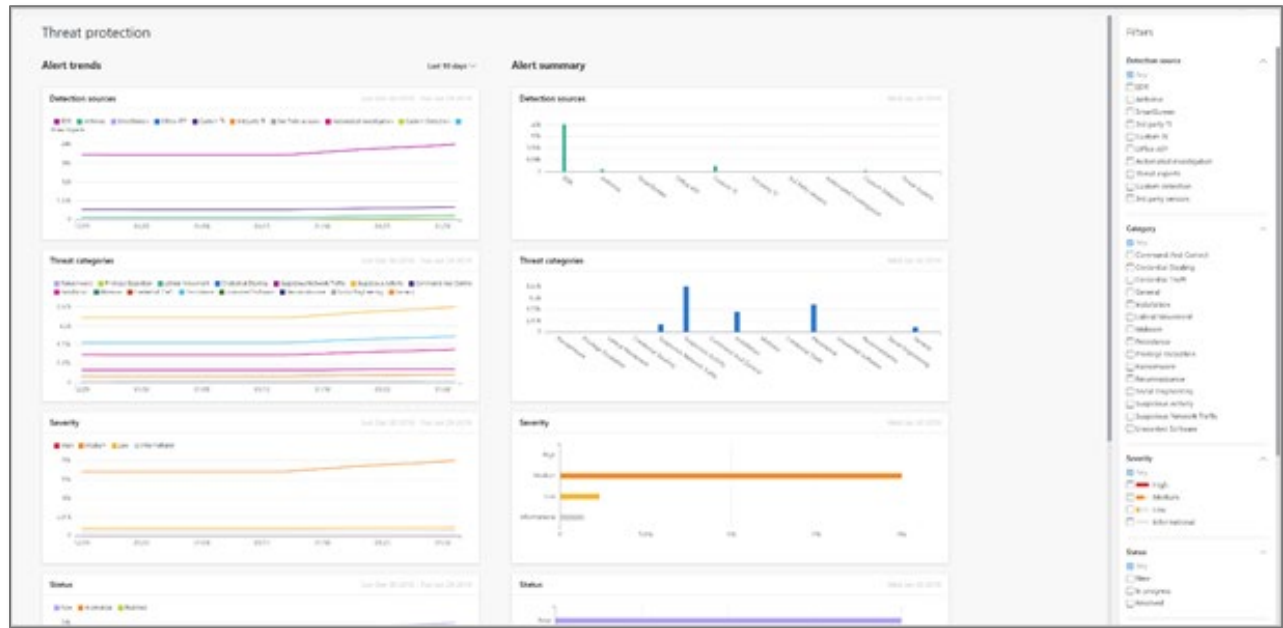


Figure 9. Threat protection report page

Knowing the trends and summaries related to alerts and machines in your organization can help identify where focused improvements can be made. For example, if you see a sudden spike in a specific kind of alert, you can drill down and start investigating directly from the relevant card to pivot into the alert or machine queue with the relevant filters applied and determine what action to take to address an issue.

Conclusion

We've simulated an advanced fileless or memory-only attack, and walked through how Microsoft Defender ATP detects and alerts on stealthy malicious activity with the help of deep OS sensors. We also experienced how exploit protection capabilities can stop advanced attacks and provide alert information in the portal.

In this simulation, we also experienced Microsoft Defender ATP automatically investigating and remediating artifacts involved in the memory-only attack. This simulation emphasizes how automated investigation can scale SOC capabilities by automatically hunting for attack artifacts across onboarded machines and by remediating suspicious artifacts. The feature safeguards machines from unwanted changes by requesting approval for remediation actions, but can also be configured to automatically apply these actions.

We hope you enjoyed this simulation and are now encouraged to explore automated investigation as well as other features and capabilities. For more information, [read the product guide at docs.microsoft.com](https://docs.microsoft.com).

Click the feedback icon on the Microsoft Defender ATP portal to let us know how you feel about this simulation or any other aspects of the product. We would love to hear your ideas about additional simulations and tutorials. Thank you!