



Microsoft Defender Advanced Threat Protection

Attack simulation

Scenario 3: Automated investigation
(backdoor)

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 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. This library is constantly updated 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 to the automated incident response scenario

In this scenario, we simulate an attack that triggers the new Microsoft Defender ATP automated investigation capabilities. This capability automates the 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 provide the same attack lure document used in *Scenario 1: Document drops backdoor*. Scenario 1 simulates attacks that are launched using a socially engineered lure document in a spear-phishing email. The lure is designed to ensure that the receiver doesn't suspect a thing and unwittingly opens the document.

The document, however, is weaponized with crafted macro code that silently drops and loads an executable file onto the machine. Although this simulation uses a document that drops a benign executable, the executable behaves as if it is a backdoor attempting to gain persistence—it writes to a registry Run key and creates a scheduled task, both commonly known autostart extensibility points (ASEPs).

The attack simulation ends when the ASEPs are created. In the real world, however, the attacker is expected to use the implanted backdoor to perform other actions within the compromised network, such as moving laterally to other machines, gathering credentials to gain privileges, and exfiltrating stolen data.

The test machine required for this simulation should:

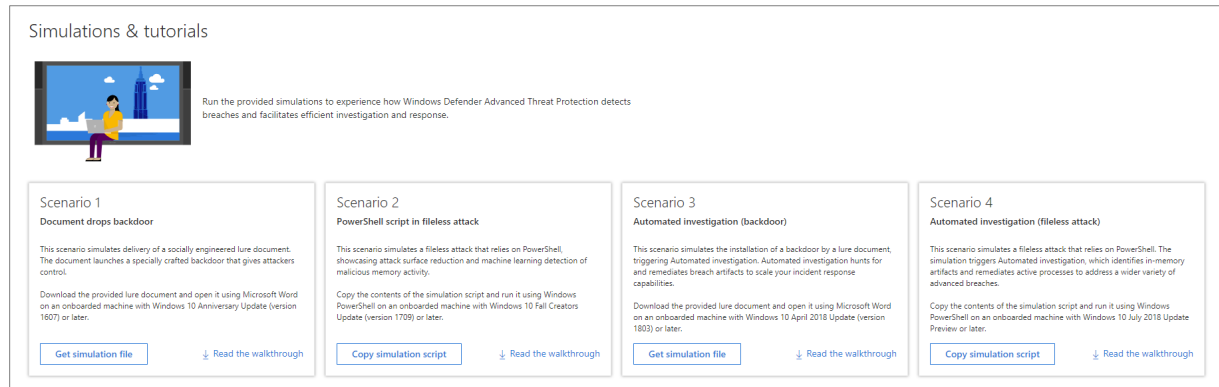
- Be onboarded to Microsoft Defender ATP
- Run Windows 10 Spring Creators Update preview
- Have PowerShell turned on
- Have Windows Defender Antivirus turned on
- Have Microsoft Word installed

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 the attack simulation:

1. Log in to the Microsoft Defender ATP portal and go to **Help (?) > Simulations & tutorials**.



2. Click **Get simulation file** under **Scenario 3: Automated incident response** to download the lure document **WinATP-Intro-Invoice.docm**.
3. Copy the lure document to the test machine.
4. To simulate typical user interaction with the lure document, double-click the copy of the document on the test machine. Microsoft Word will prompt for a password to open the document. To open the password-protected document, use the password **WDATP!diy#**.
5. Click **Enable Editing** if the document opens in Protected View. If you see a subsequent security warning about macros being disabled, click **Enable Content**. With the right lure content, many users are actually enticed to bypass these security safeguards when opening malicious Office documents.

 **Note:** If your organization blocks macros in documents from the internet, you might need to unblock this specific document for the **Enable Content** option to work. To unblock the document, navigate to its location in File Explorer. In File Explorer, right-click the document, select **Properties**. In the **General** tab, mark the **Unblock** option under **Security**.

 **Note:** You might encounter difficulties running the scenario if you have third party security products. We recommend using an onboarded test machine with the default out-of-box Windows 10 configuration and Windows Defender AV turned on.

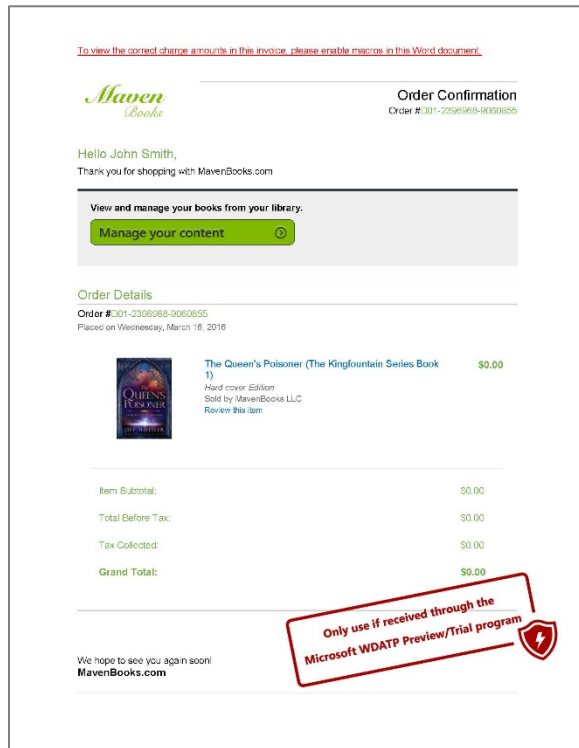
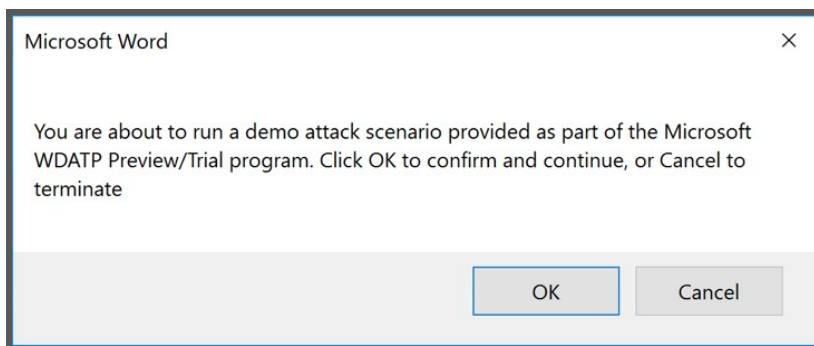


Figure 1. The lure document

- Click OK on the message box to confirm that you wish to run the attack simulation.



- A few seconds later, a new file **WinATP-Intro-Backdoor.exe**, which represents the backdoor, is dropped onto the Desktop folder by a PowerShell script launched from the document's malicious macro.
- The script goes on to create a scheduled task to launch the backdoor at a predefined time. This mechanism of indirect process launch is sometimes used for stealth, as it is harder to trace back to the document.

9. When the backdoor is launched, it creates an autostart entry under the registry Run key, allowing it to stay persistent by starting automatically with Windows. A Command Prompt window opens, indicating that the simulated backdoor is running.
10. Close the Command Prompt window to end the **WinATP-Intro-Backdoor.exe** process.

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.

View the alerts and the automated response

Let's switch from being an attacker to a SOC defender.

1. Open the Microsoft Defender ATP portal 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.

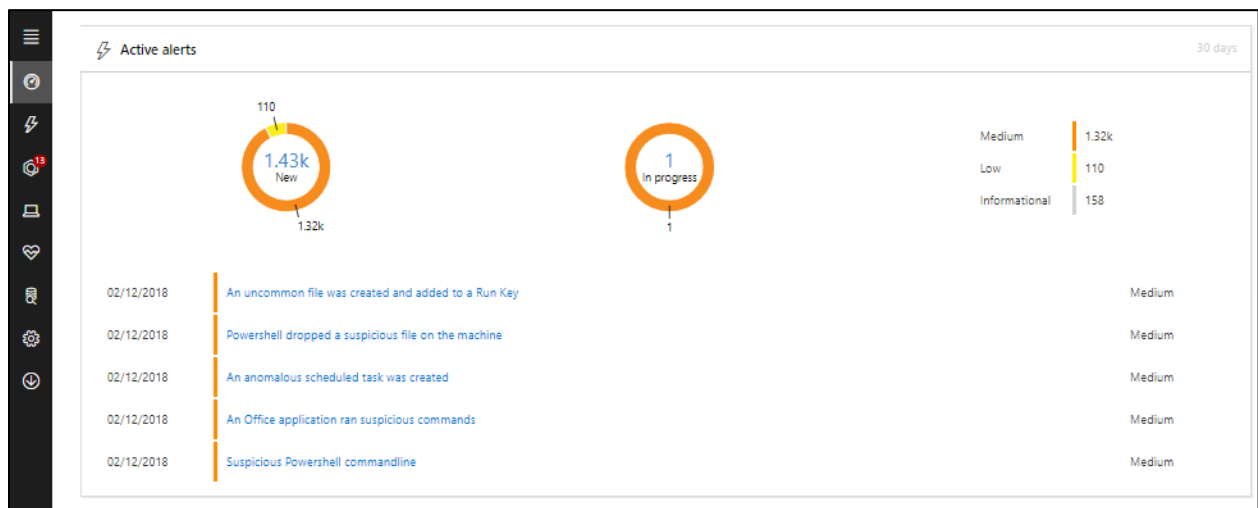



Figure 2. Dashboard view showing the triggered alerts

 **Note:** In this simulation we will focus on the automated investigation and response aspects related to the simulated attack. If you would like to learn more about the individual alerts raised in this attack and some of the manual investigation features available to analyze them, see the walkthrough document for **Scenario 1: Document drops backdoor**.

4. Select the item **PowerShell dropped a suspicious file on the machine** to navigate the corresponding [alert details page](#). In the alert details page, a badge will indicate that automated investigation has been started and the current status of the investigation.

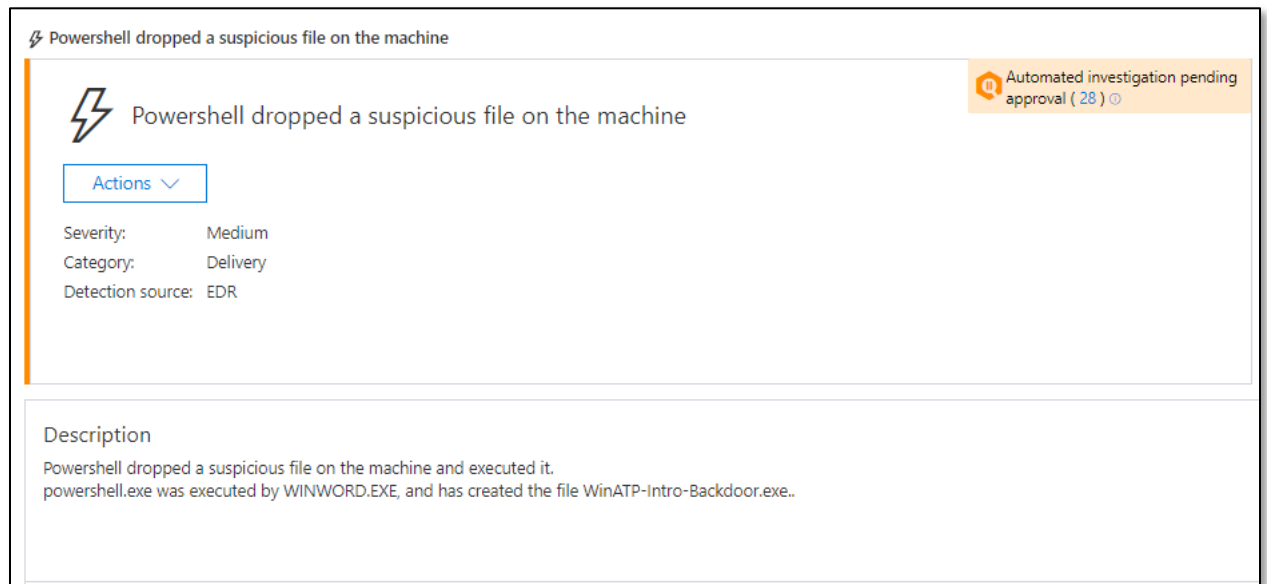


Figure 3. Alert page showing that automated investigation has been started

Explore the 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.

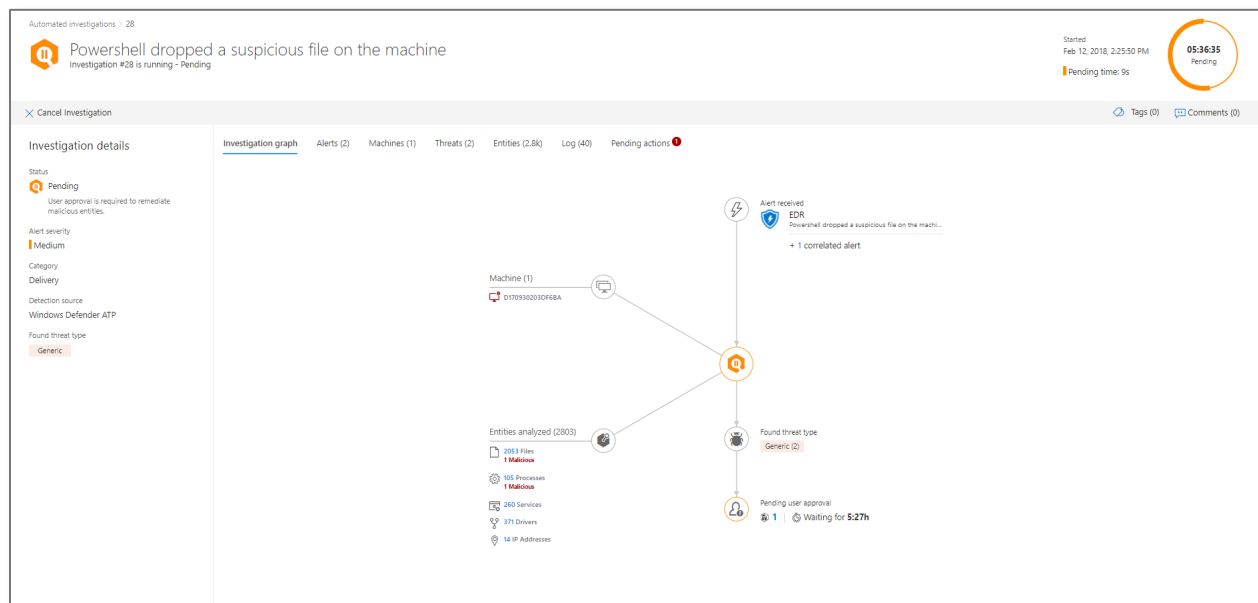



Figure 4. Investigation details page

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 automated 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.

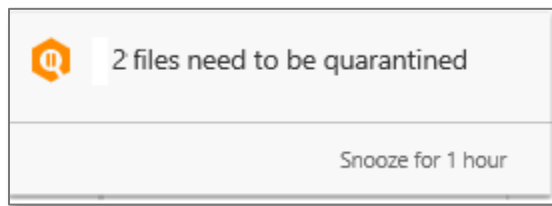


Figure 5. Notification for pending remediation actions

- 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 all artifacts requiring remediation: the backdoor, the ASEPs—the registry entry and scheduled task—and even the lure document. Microsoft Defender ATP will await your approval before proceeding, but you can [configure it to skip this step and apply remediation automatically](#).

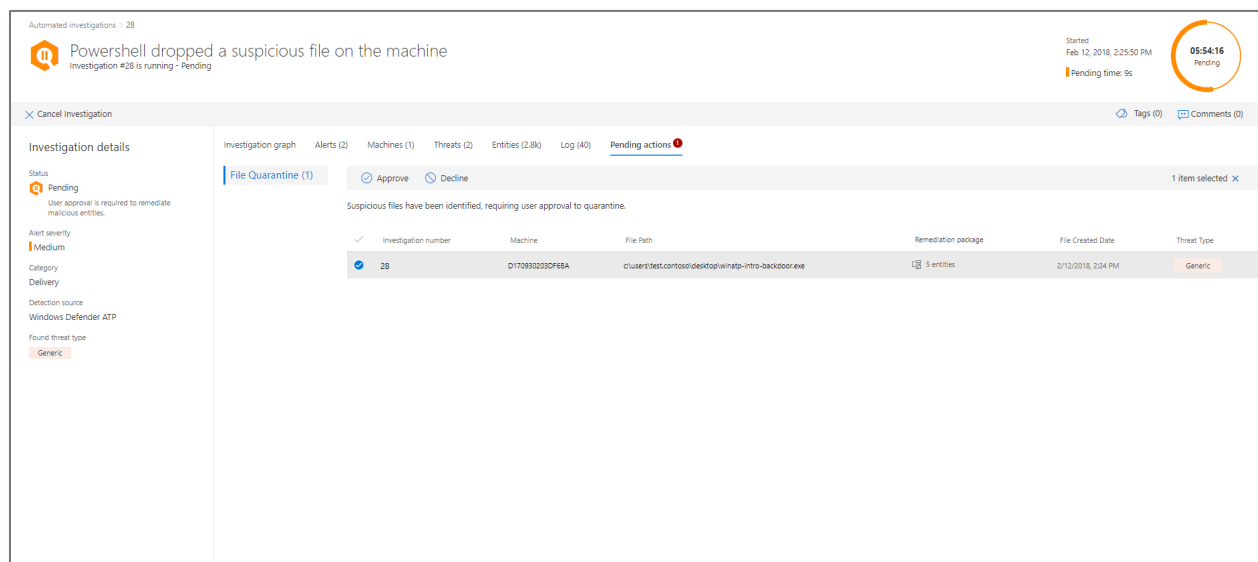


Figure 6. Pending actions

- Click on **Approve** to approve the remediation action for all artifacts linked to the attack. Once you approve, automated investigation stops relevant process, quarantines suspicious files (the backdoor and the lure document), and deletes the ASEPs.

When completed, the investigation status changes to **Fully remediated**.

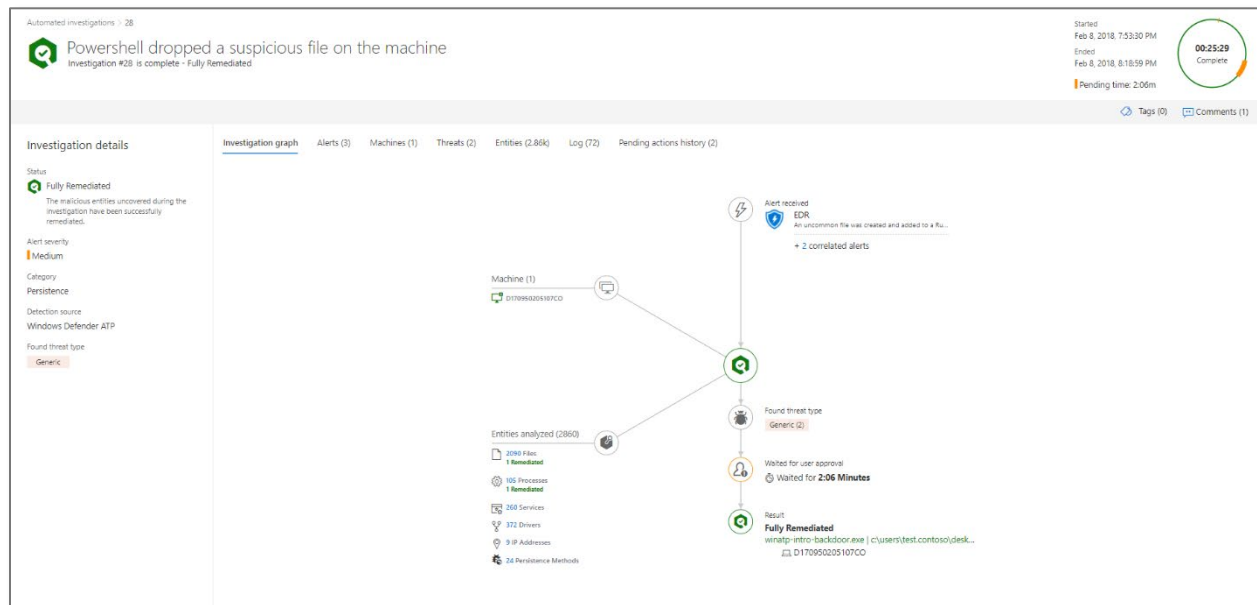


Figure 7. The investigation details page after full remediation

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.

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.

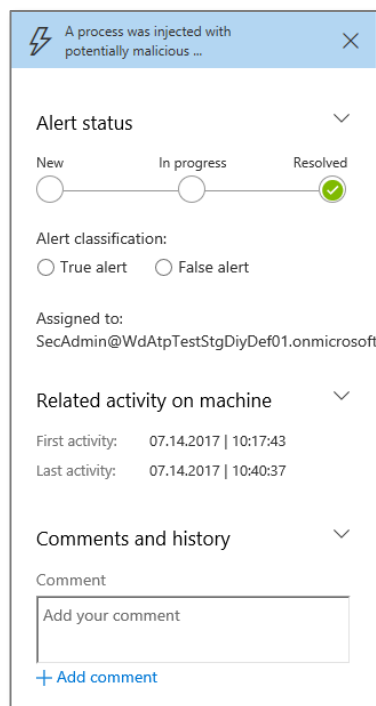


Figure 8. Alert management pane showing resolved alert

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.

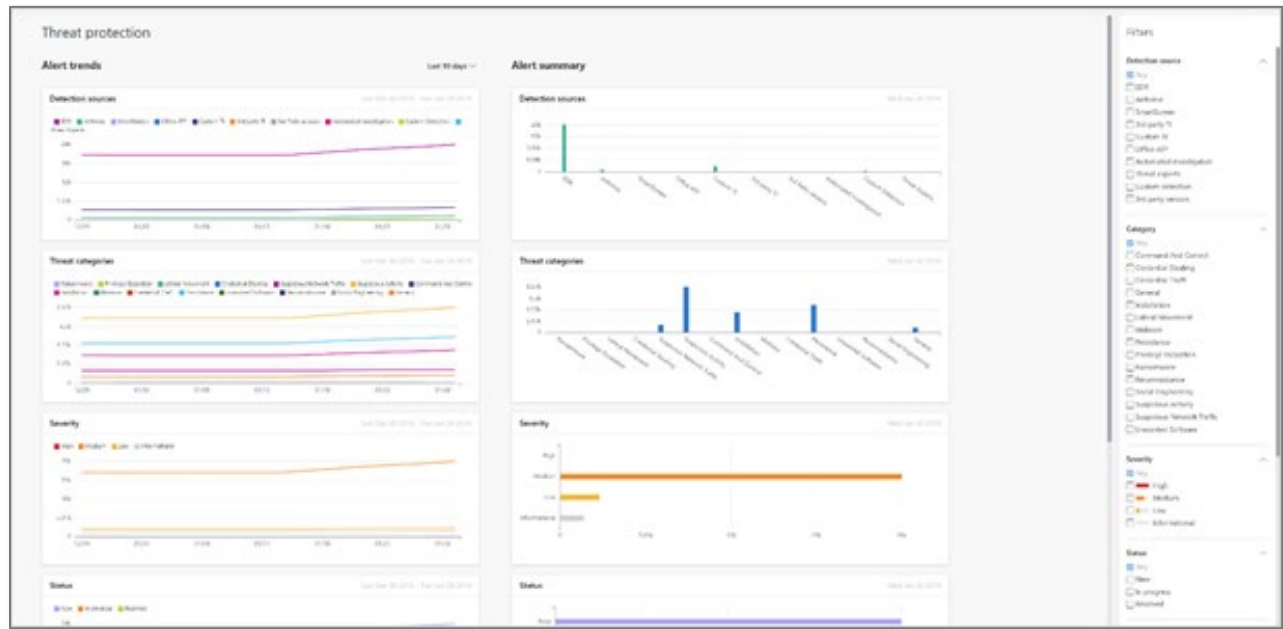


Figure 15. Threat protection report page

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 a common attack and walked through how Microsoft Defender ATP surfaces that attack and triggers an automated investigation in response. 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!