



Windows Defender Advanced Threat Protection

Attack simulation

Scenario 5: Custom detections

August 2018

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.

© 2018 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 this scenario

In this scenario, we simulate an attack that triggers an alert based on a custom detection rule. By creating a custom detection rule, you can tailor your monitoring activities towards specific attacks or attack patterns. The query itself gives you extremely granular control over the indicators and events you want to cover. Saving the query as a custom detection rule periodically checks all recorded events for matches and raises corresponding alerts for these matches.

To trigger the custom detection rule, 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.

This simulation requires a test machine that:

- Has been onboarded to Windows Defender ATP
- Is running Windows 10 Anniversary Update (version 1607) or later
- Has PowerShell turned on
- Has Microsoft Word installed

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

About custom detections

By leveraging the power of advanced hunting on Windows Defender ATP, custom detections can periodically hunt for a range of possible breach behaviors, including suspicious activities and activities associated with emerging threats.

Custom detections run every 24 hours and can be configured so that when it meets specified criteria set by the user, alerts are triggered and are surfaced in Windows Defender Security Center. These alerts are treated like any other alert in the system.

This capability is particularly useful when you want to proactively respond to certain threats and be notified quickly of emerging threats.

Run the simulation

To run the attack simulation:

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

Simulations & tutorials





Run the provided simulations to experience how Windows Defender Advanced Threat Protection detects breaches and facilitates efficient investigation and response.

Scenario 1 Document drops backdoor <p>This scenario simulates delivery of a socially engineered lure document. The document launches a specially crafted backdoor that gives attackers control.</p> <p>Download the provided lure document and open it using Microsoft Word on an onboarded machine with Windows 10 Anniversary Update (version 1607) or later.</p> <p>Get simulation file Read the walkthrough</p>	Scenario 2 PowerShell script in fileless attack <p>This scenario simulates a fileless attack that relies on PowerShell, showcasing attack surface reduction and machine learning detection of malicious memory activity.</p> <p>Copy the contents of the simulation script and run it using Windows PowerShell on an onboarded machine with Windows 10 Fall Creators Update (version 1709) or later.</p> <p>Copy simulation script Read the walkthrough</p>	Scenario 3 Automated investigation (backdoor) <p>This scenario simulates the installation of a backdoor by a lure document, triggering Automated investigation. Automated investigation hunts for and remediates breach artifacts to scale your incident response capabilities.</p> <p>Download the provided lure document and open it using Microsoft Word on an onboarded machine with Windows 10 April 2018 Update (version 1803) or later.</p> <p>Get simulation file Read the walkthrough</p>
Scenario 4 Automated investigation (fileless attack) <p>This scenario simulates a fileless attack that relies on PowerShell. The simulation triggers Automated investigation, which identifies in memory artifacts and remediates active processes to address a wider variety of advanced breaches.</p> <p>Copy the contents of the simulation script and run it using Windows PowerShell on an onboarded machine with Windows 10 July 2018 Update Preview or later.</p> <p>Copy simulation script Read the walkthrough</p>	Scenario 5 Custom detections <p>In this scenario, we create a custom Advanced hunting query to find specific attack activity and periodically check for subsequent activity. To simulate the attack, we use a specially crafted lure document that drops simulated malware.</p> <p>Refer to the walkthrough and create the query, and then use Microsoft Word to open the simulation file on an onboarded machine with Windows 10 Anniversary Update (version 1607) or later.</p> <p>Get simulation file Read the walkthrough</p>	

2. Click **Get simulation file** under **Scenario 5: Advanced hunting query** 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.

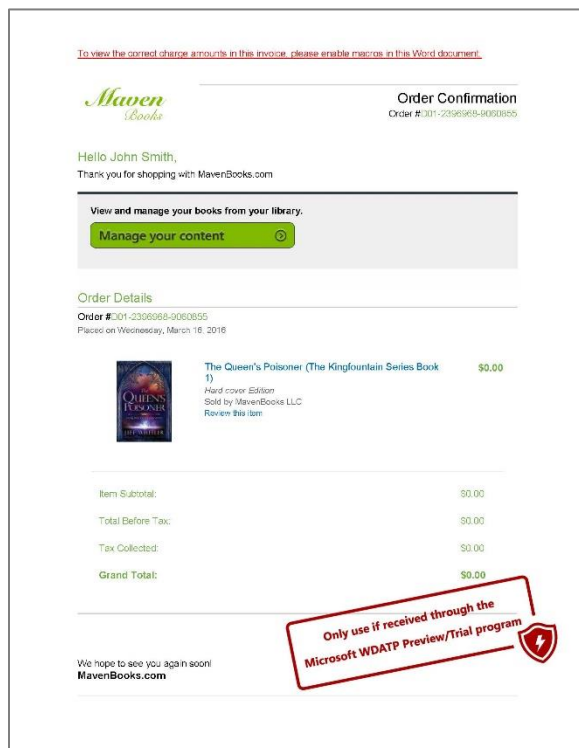
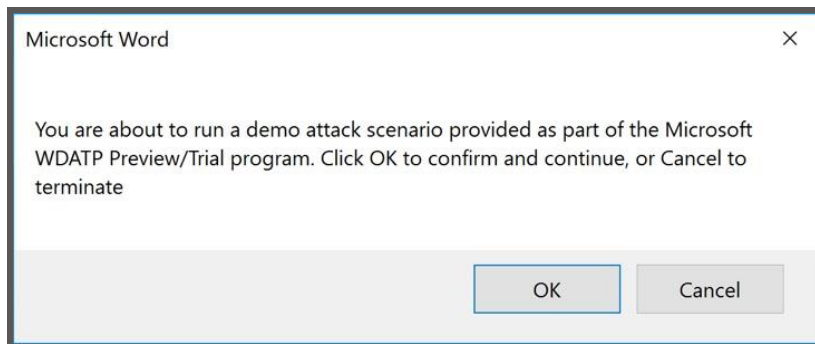


Figure 1. The lure document

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



7. 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.
8. 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 create a scheduled query and experience how alerts are triggered based on manually specified alerting criteria.

Create a Custom Detection

Let's switch from being an attacker to a SOC defender. In this stage, you will create a query designed to match the simulated attack behavior. You will also schedule the query so that it runs periodically and automatically raises an alert.

1. Open the Windows Defender ATP portal on <https://securitycenter.windows.com> from any machine.
2. Log in with your Windows Defender ATP credentials. Default global administrator credentials are provided with your signup email.
3. Go to the **Advanced hunting** page.
4. To capture the simulated attack, create a query that can detect events wherein a downloaded Microsoft Office file executes a PowerShell command. You can use this sample query:

```
DeviceProcessEvents
| where InitiatingProcessFileName in~ ("winword.exe","excel.exe","powerpnt.exe")
// For more detailed query, that find a document file that was downloaded from the
// internet, comment out the following line. Also modify the following line if the
// document resides in a folder other than "downloads"
// | where InitiatingProcessFolderPath contains "downloads"
| where FileName =~ "powershell.exe"
| where Timestamp > ago(30d)
```

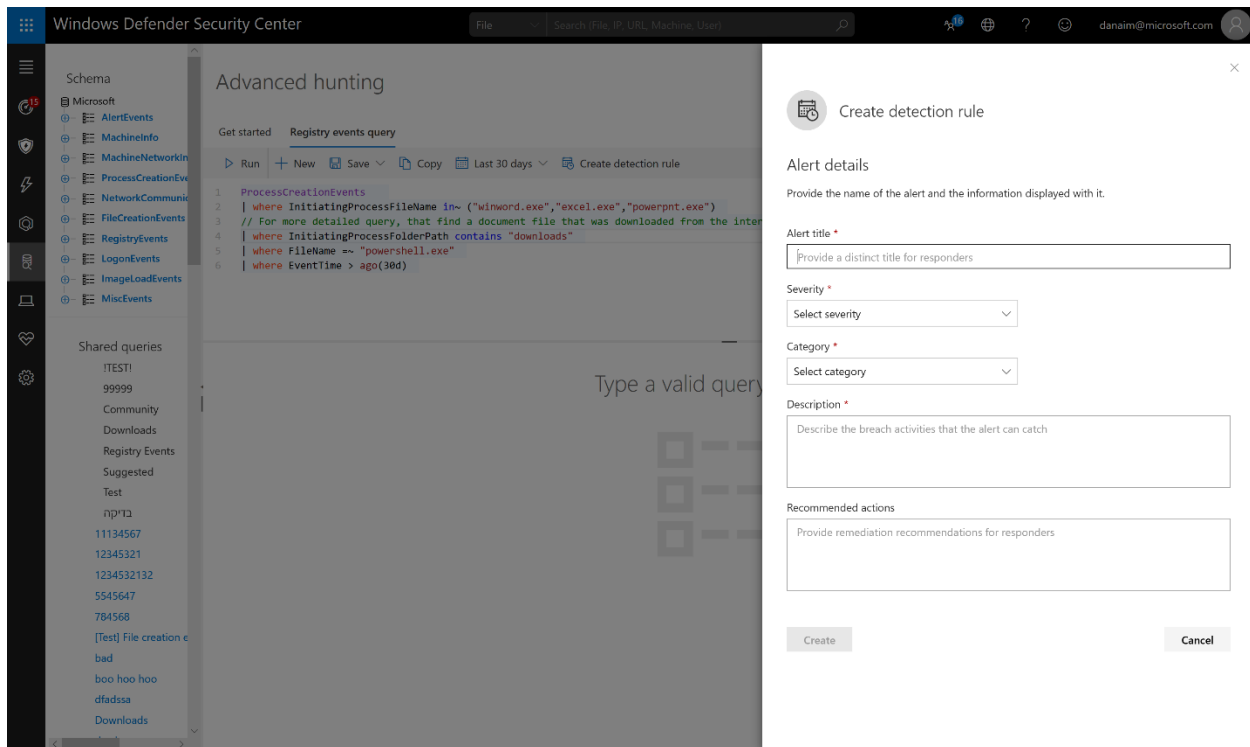
5. For a more extensive and comprehensive query you can use the following:

```
let wordProcessesOpeningDownloadedDocuments =
DeviceProcessEvents
| where FileName =~ "winword.exe" and ProcessCommandLine contains @"\\"
// Parse the document name from the winword commandline.
// Document name comes after the /n argument.
| parse ProcessCommandLine with * " /n \" DocumentPath "\""
| project DeviceName, OpenDocTime=Timestamp, DocumentPath, ReportId, DeviceId;
let wordProcessesRunningPowershell =
DeviceProcessEvents
| where InitiatingProcessFileName =~ "winword.exe" and FileName =~ "powershell.exe"
| project ReportId, DeviceId, DeviceName, Timestamp,
PowershellCommandline=ProcessCommandLine,
WordProcessCreationTime=InitiatingProcessCreationTime;
wordProcessesRunningPowershell
| join kind=inner (wordProcessesOpeningDownloadedDocuments) on DeviceName
```



```
// Look for documents opened up to 5 minutes before the suspicious Powershell was run,
// but only if opened after this winword process was run already.
| where OpenDocTime between (max_of(Timestamp-5m, WordProcessCreationTime) ..
Timestamp)
| summarize makeset(DocumentPath) by ReportId, DeviceId, DeviceName,
PowershellCommandline, bin(Timestamp, 1tick)
```

6. Save the query and select **Create detection rule**.

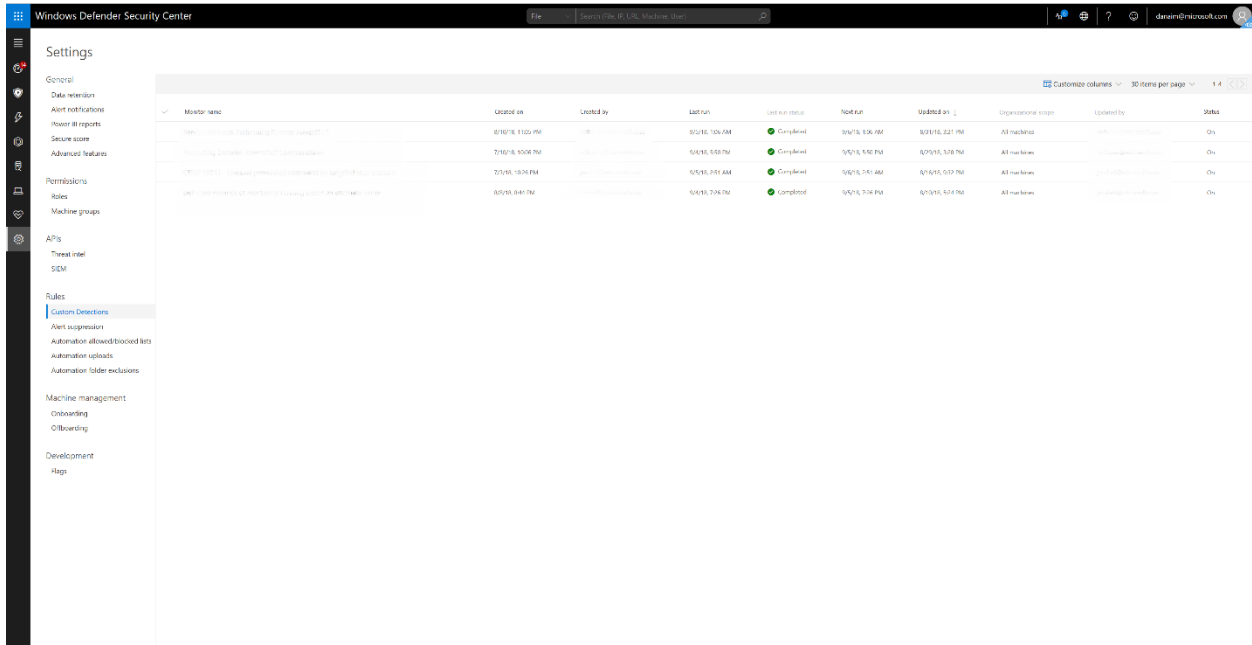


7. Create a custom detection rule with the following details:

- Alert title: "Custom Detection | Downloaded Office file executes PowerShell"
- Severity: Medium
- Category: Suspicious behavior
- Description: "A downloaded Microsoft Office file executed PowerShell commands. This alert is based on a scheduled Advanced hunting query."
- Recommended actions: Check the Microsoft Office file and determine if the PowerShell activity is expected.

After the custom detection rule is created, it will run for the first time. (Note that it might take a few minutes before any alerts are raised.) From this point on, the monitor will automatically run every 24 hours.

You can access all the existing custom detection in Settings > Custom Detections.



The screenshot shows the Windows Defender Security Center interface. The left sidebar contains various settings categories. The main pane displays the 'Custom Detections' section, which lists three custom detection rules. Each rule entry includes its name, creation and last run timestamps, status (Completed), next run time, scope (All machines), and a toggle switch to enable or disable the rule.

Custom Detection	Created on	Updated by	Last run	Last run status	Next run	Quarantined on	Operational scope	Updated by	Status
Block all incoming connections to the network	8/18/18 11:00 PM	Microsoft Defender	8/18/18 10:00 AM	Completed	8/18/18 1:00 PM	8/18/18 1:00 PM	All machines	Microsoft Defender	On
Prevent all incoming connections to the network	8/18/18 11:00 PM	Microsoft Defender	8/18/18 10:00 AM	Completed	8/18/18 1:00 PM	8/18/18 1:00 PM	All machines	Microsoft Defender	On
Prevent all incoming connections to the network	8/18/18 11:00 PM	Microsoft Defender	8/18/18 10:00 AM	Completed	8/18/18 1:00 PM	8/18/18 1:00 PM	All machines	Microsoft Defender	On

Explore the alerts triggered by the custom detection

Let's investigate the attack in Windows Defender Security Center using the alerts triggered by the scheduled query. The dashboard should display several new alerts for the test machine resulting from the simulated attack.

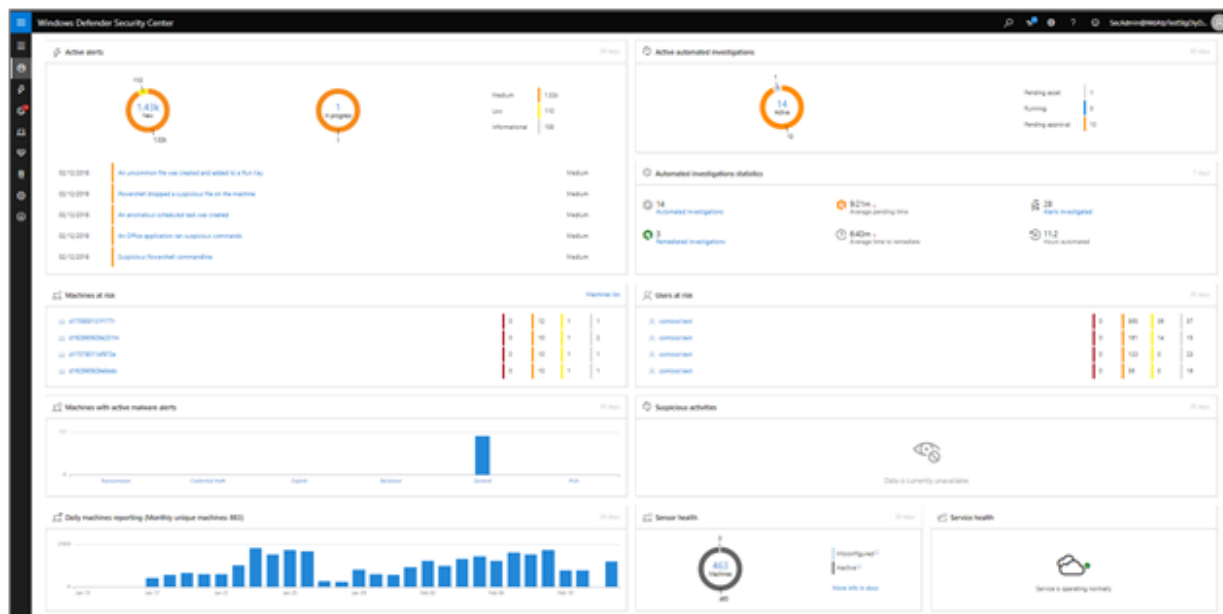


Figure 2. Dashboard showing alerts

In the **Machines at risk widget**, click the test machine to see the details of that machine and all the alerts associated alerts.

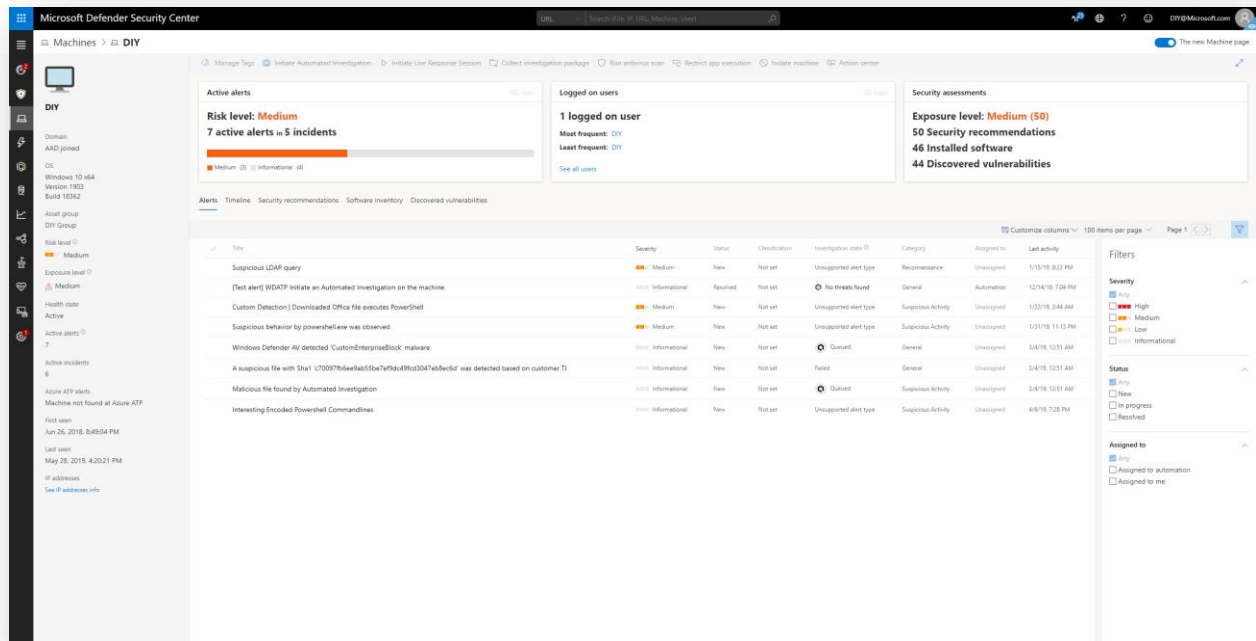


Figure 3. Test machine with alerts

Note: In this scenario, we focus on the alerts triggered by the custom detection rule. If you'd like to learn more about other alerts triggered by the simulated attack and manual investigation features available to analyze them, see the walkthrough document for *Scenario 1: Document drops backdoor*.

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.

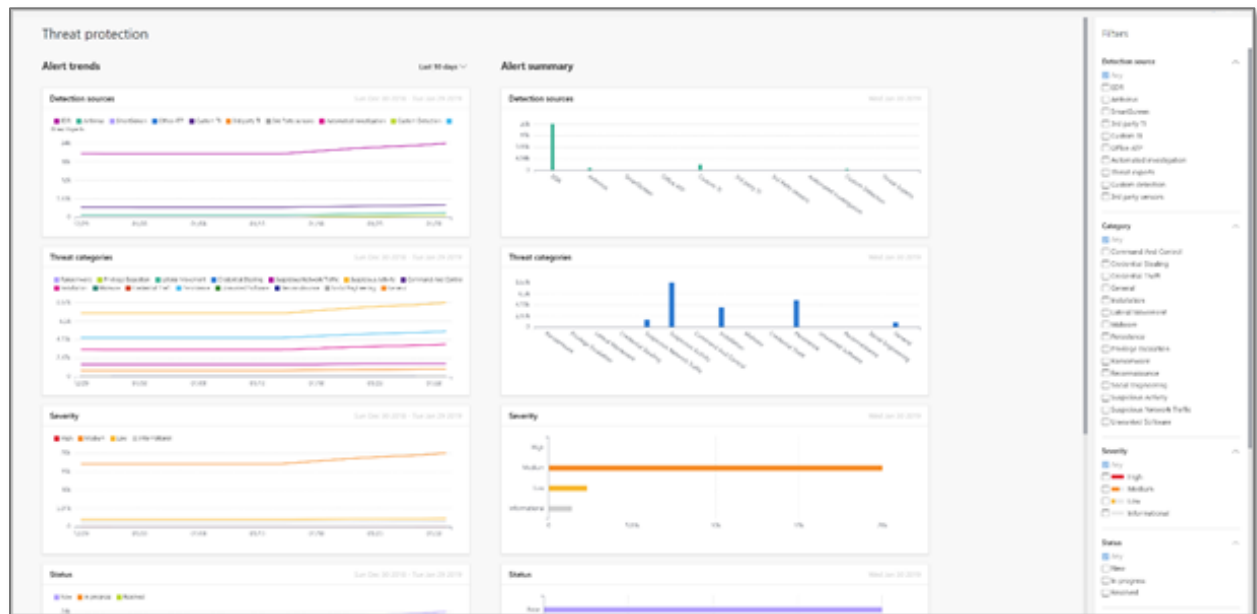


Figure 4. Threat protection report page

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 Windows Defender ATP surfaces that attack using a custom detection mechanism. This simulation emphasizes how Advanced hunting can provide highly customizable query capabilities that can be used to monitor for emerging attacks.

We hope you enjoyed this simulation and are now encouraged to explore Advanced hunting 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 Windows 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!