Microsoft Defender Advanced Threat Protection

Attack simulation

Scenario 2: PowerShell script in 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.

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: PowerShell script in fileless attack

In this scenario, we move up a notch to more sophisticated attack that leverage advanced techniques to stay under the detection radar. This category of attacks usually doesn't include files dropped on the victim's machine—they occur solely in memory. They "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 on the box.

We will simulate such an attack and explore how exploit protection capabilities 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.

The test machine require for this simulation should:

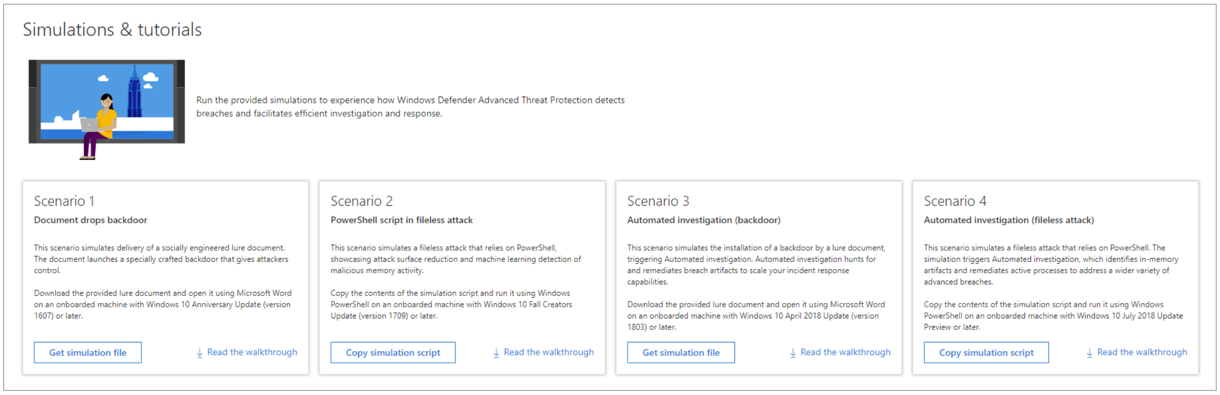
- Be onboarded to Microsoft Defender ATP
- Run Windows 10 Fall Creators Update (version 1709)
- Have PowerShell turned on
- Have Windows Defender Antivirus turned on

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**.



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

This scenario simulates delivery of a socially engineered lure document. The document launches a specially crafted backdoor that gives attackers control.

Download the provided lure document and open it using Microsoft Word on an onboarded machine with Windows 10 Anniversary Update (version 1607) or later.

Scenario 2

PowerShell script in fileless attack

This scenario simulates a fileless attack that relies on PowerShell, showcasing attack surface reduction and machine learning detection of malicious memory activity.

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.

Scenario 3

Automated investigation (backdoor)

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.

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.

Scenario 4

Automated investigation (fileless attack)

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.

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.

Figure 1. Simulation scenarios in the portal

2. Click the **Copy simulation script** button under **Scenario 2: PowerShell script in fileless attack** 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.

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.

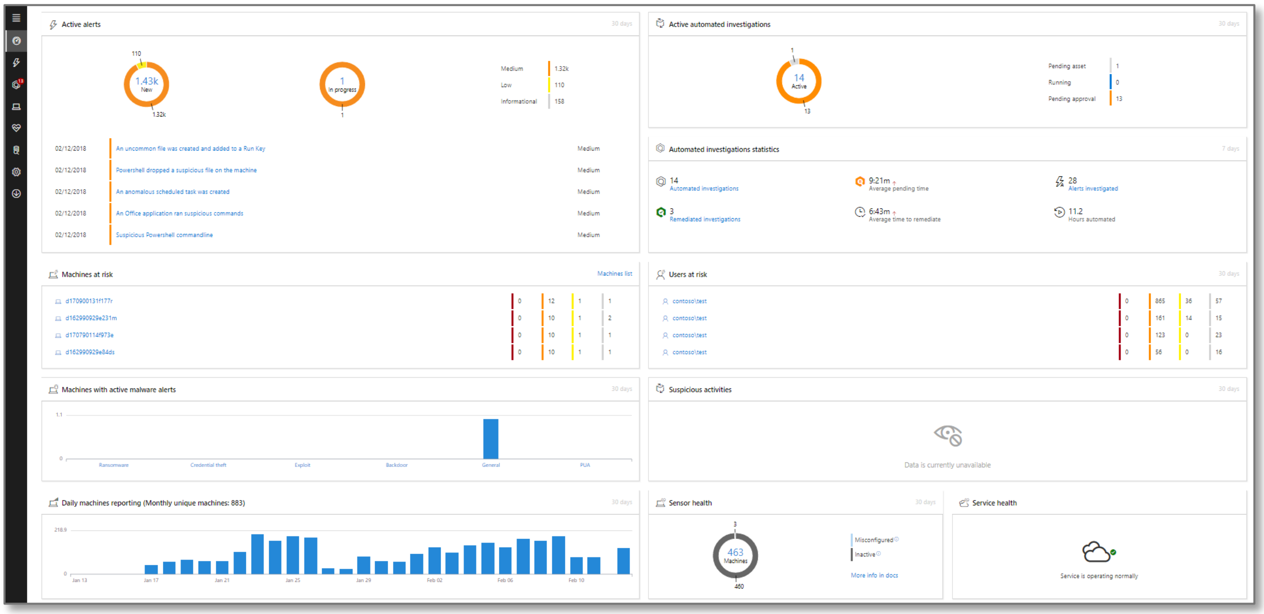
Investigate the attack in the portal

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 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.



Active alerts — 30 days

Medium	1.32k
Low	110
Informational	158

02/12/2018	An uncommon file was created and added to a Run Key	Medium
02/12/2018	Powershell dropped a suspicious file on the machine	Medium
02/12/2018	An anomalous scheduled task was created	Medium
02/12/2018	An Office application ran suspicious commands	Medium
02/12/2018	Suspicious Powershell commandline	Medium

Active automated investigations — 30 days

Pending asset	1
Running	0
Pending approval	13

Automated investigations statistics — 7 days

14 Automated investigations

9:21m Average pending time

28 Alerts investigated

3 Remediated investigations

6:43m Average time to remediate

11.2 Hours automated

Machines at risk — Machines list

d170900131f177r	0	12	1	1
d162990929e231m	0	10	1	2
d170790114f973e	0	10	1	1
d162990929e84ds	0	10	1	1

Users at risk — 30 days

contoso\test	0	865	36	57
contoso\test	0	161	14	15
contoso\test	0	123	0	23
contoso\test	0	56	0	16

Suspicious activities — 30 days

Data is currently unavailable

Service health

Service is operating normally

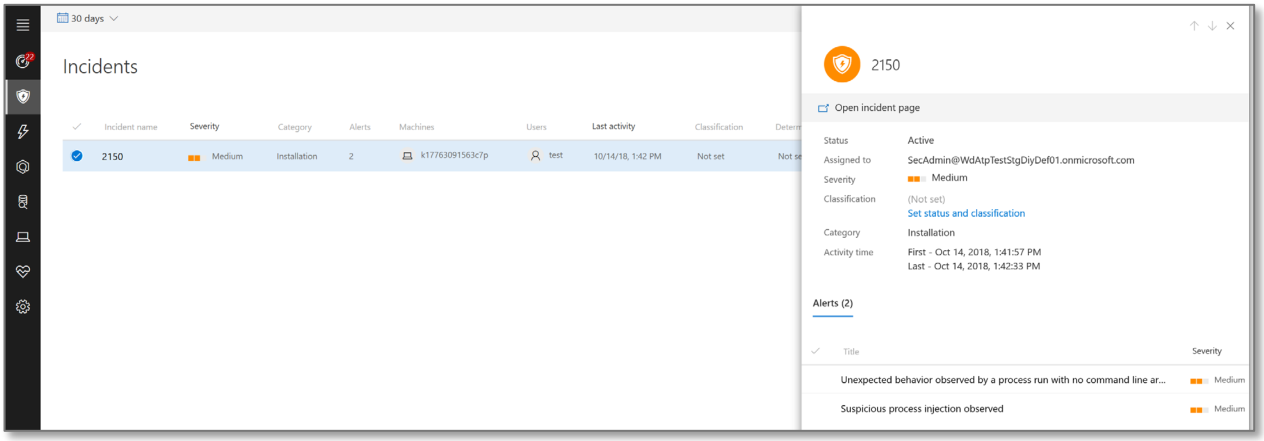
Figure 2. Dashboard view showing the alerts

Investigate the attack as a single incident

Microsoft Defender ATP applies correlation analytics and aggregates all related alerts and investigations into one “incident” entity. By doing so, Microsoft Defender ATP narrates a broader attack story, allowing the SOC analyst to understand and deal with complex threats across the org with the right visuals—through the enhanced incident graph—and data representations.

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, go to the **Incidents** queue and select the relevant item as shown below. A side panel displays additional information about the incident, including all the related alerts.



Incidents

✓	Incident name	Severity	Category	Alerts	Machines	Users	Last activity	Classification	Determ
✓	2150	Medium	Installation	2	k17763091563c7p	test	10/14/18, 1:42 PM	Not set	Not se

2150

Open incident page

Status	Active
Assigned to	SecAdmin@WdAtpTestStgDiyDef01.onmicrosoft.com
Severity	Medium
Classification	(Not set) Set status and classification
Category	Installation
Activity time	First - Oct 14, 2018, 1:41:57 PM Last - Oct 14, 2018, 1:42:33 PM

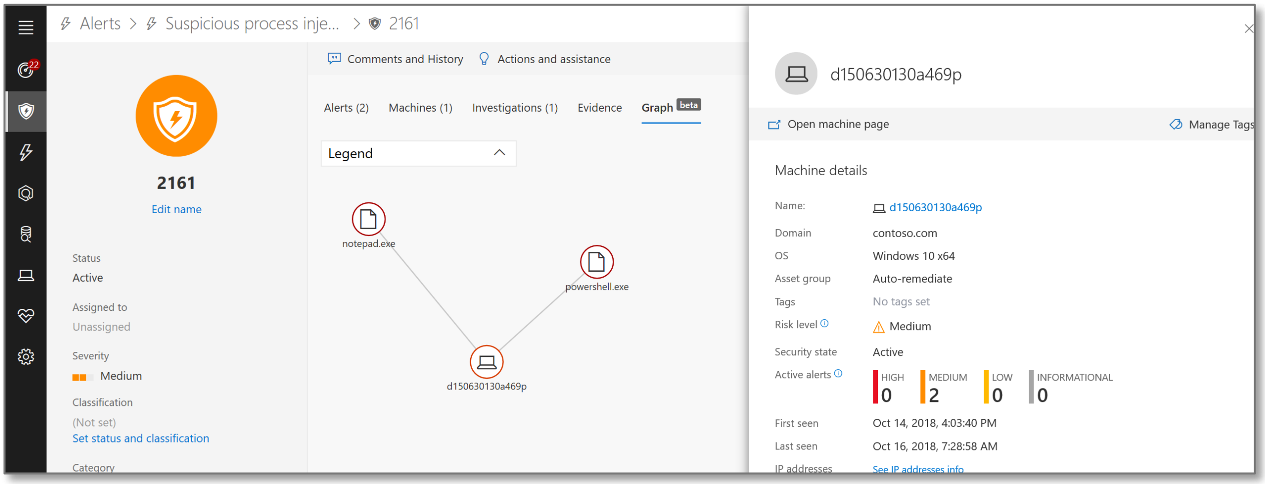
Alerts (2)

✓	Title	Severity
	Unexpected behavior observed by a process run with no command line ar...	Medium
	Suspicious process injection observed	Medium

Figure 3. Incident aggregating alerts generated during the simulation

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

In the incident page, you can check all the affected machines and the related alerts. For a broader view of the entities involved in the incident, select **Graph**.



2161

Edit name

Status: Active

Assigned to: Unassigned

Severity: Medium

Classification: (Not set)

Set status and classification

Category

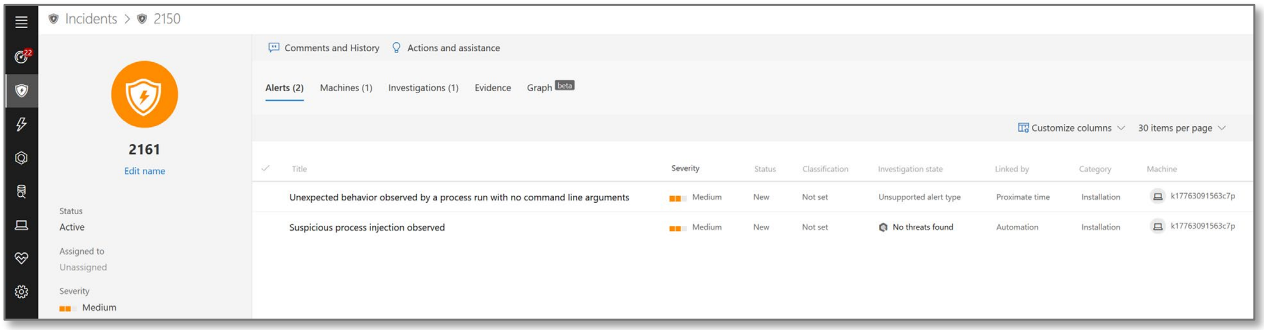
d150630130a469p

Machine details

Name:	d150630130a469p
Domain	contoso.com
OS	Windows 10 x64
Asset group	Auto-remediate
Tags	No tags set
Risk level	⚠ Medium
Security state	Active
Active alerts	HIGH 0 MEDIUM 2 LOW 0 INFORMATIONAL 0
First seen	Oct 14, 2018, 4:03:40 PM
Last seen	Oct 16, 2018, 7:28:58 AM
IP addresses	See IP addresses info

Figure 4. Graph of the incident

Reviewing the incident alert list unfolds the progression of the attack. From this view you can dive into the individual alerts



2161

Edit name

Status: Active

Assigned to: Unassigned

Severity: Medium

Title	Severity	Status	Classification	Investigation state	Linked by	Category	Machine
Unexpected behavior observed by a process run with no command line arguments	Medium	New	Not set	Unsupported alert type	Proximate time	Installation	k17763091563c7p
Suspicious process injection observed	Medium	New	Not set	No threats found	Automation	Installation	k17763091563c7p

Figure 5. Incident related alerts

Review generated alerts

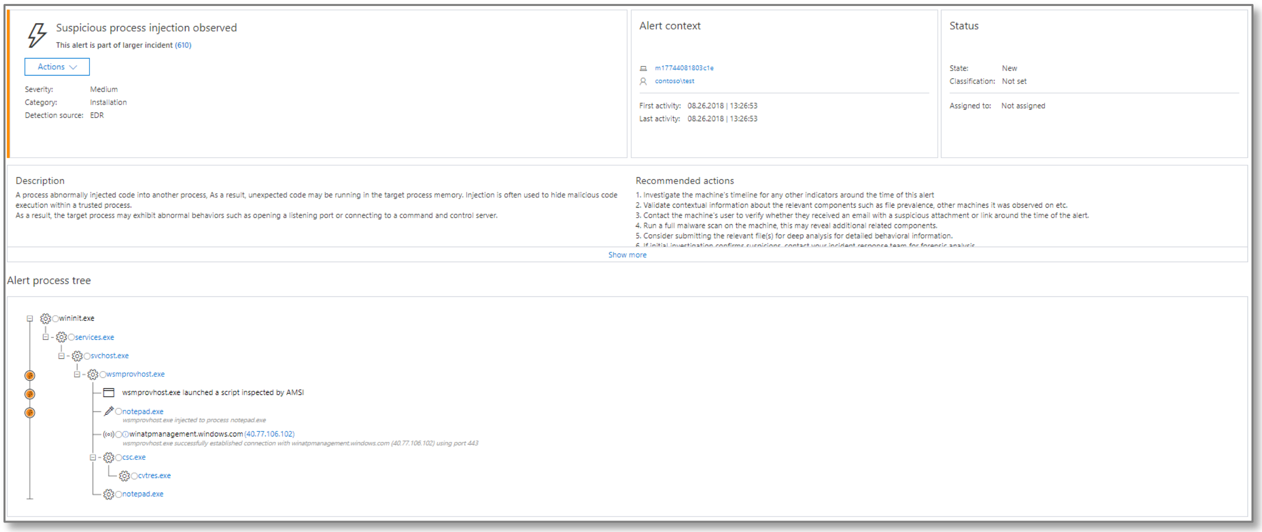
Let's look at some of the alerts generated during the simulated attack.

Note: We will walk through only a few of the alerts generated during the simulated attack. Depending on the version of Windows and the Windows Defender Antivirus protection updates running on your test machine, you might see more alerts and they might appear in a slightly different order.

Alert: Suspicious process injection observed

Advanced attackers will use more 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 allows SOC personnel to catch such advanced attacks, deep memory sensors in Microsoft Defender ATP provide our cloud service with unprecedented visibility into a variety of cross-process code injection techniques. As show below, Microsoft Defender ATP detected and alerted on the attempt to inject code to notepad.exe.



Suspicious process injection observed

This alert is part of larger incident (610)

Severity: Medium
Category: Installation
Detection source: EDR

Alert context

m17744081803c1e
contoso\test

First activity: 08.26.2018 | 13:26:53
Last activity: 08.26.2018 | 13:26:53

Status

State: New
Classification: Not set

Assigned to: Not assigned

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.

Recommended actions

1. Investigate the machine's timeline for any other indicators around the time of this alert
2. Validate contextual information about the relevant components such as file prevalence, other machines it was observed on etc.
3. Contact the machine's user to verify whether they received an email with a suspicious attachment or link around the time of the alert.
4. Run a full malware scan on the machine, this may reveal additional related components.
5. Consider submitting the relevant file(s) for deep analysis for detailed behavioral information.
6. If initial investigation confirms suspicions, contact your incident response team for forensic analysis

Alert process tree

```
wininit.exe
  services.exe
    svchost.exe
      wsmprovhost.exe
        wsmprovhost.exe launched a script inspected by AMSI
        notepad.exe
          wsmprovhost.exe injected to process notepad.exe
        winatpmanagement.windows.com (40.77.106.102)
          wsmprovhost.exe successfully established connection with winatpmanagement.windows.com (40.77.106.102) using port 443
        csc.exe
          cvtres.exe
        notepad.exe
```

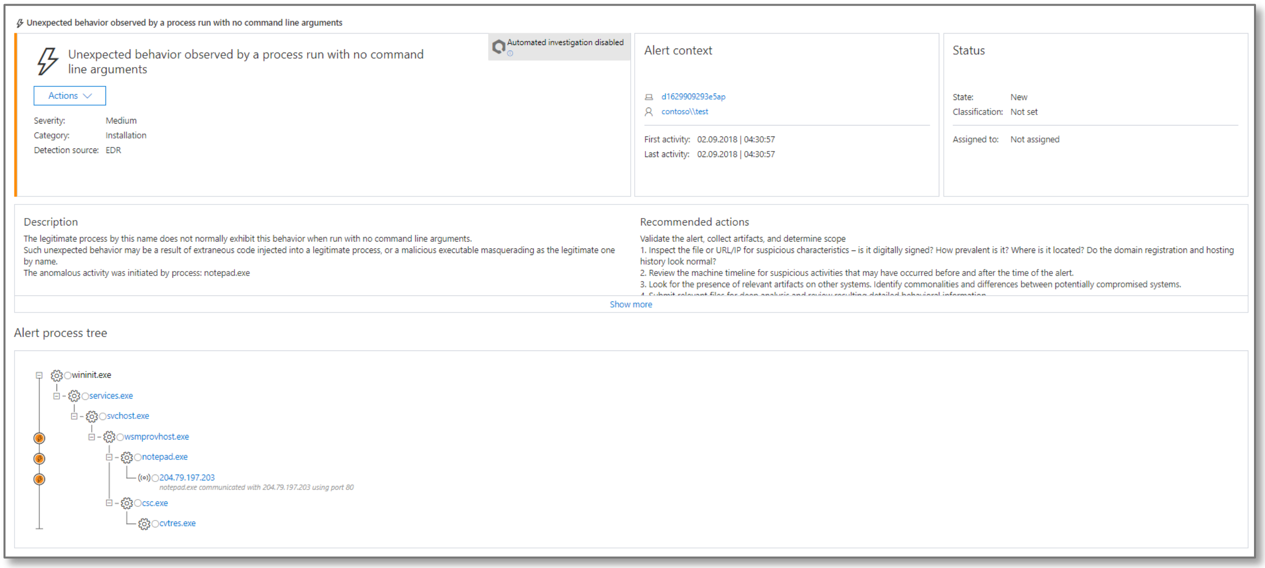
Figure 6. Alert for injection of potentially malicious code

Alert: Unexpected behavior observed by a process run with no command line arguments

Microsoft Defender ATP detections are often targeting the most invariant aspect of an attack technique. This ensures durability and raises the bar for attacker's 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 running in the otherwise trusted process.

In our case, the well-known process *notepad.exe* is exhibiting abnormal behavior, involving communication with an external location. Note that this outcome is independent of the specific method used to introduce and execute the malicious code.



Unexpected behavior observed by a process run with no command line arguments

Unexpected behavior observed by a process run with no command line arguments

Severity: Medium
Category: Installation
Detection source: EDR

Alert context

d1629909293e5ap
contoso\\test

First activity: 02.09.2018 | 04:30:57
Last activity: 02.09.2018 | 04:30:57

Status

State: New
Classification: Not set

Assigned to: Not assigned

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.
The anomalous activity was initiated by process: notepad.exe

Recommended actions

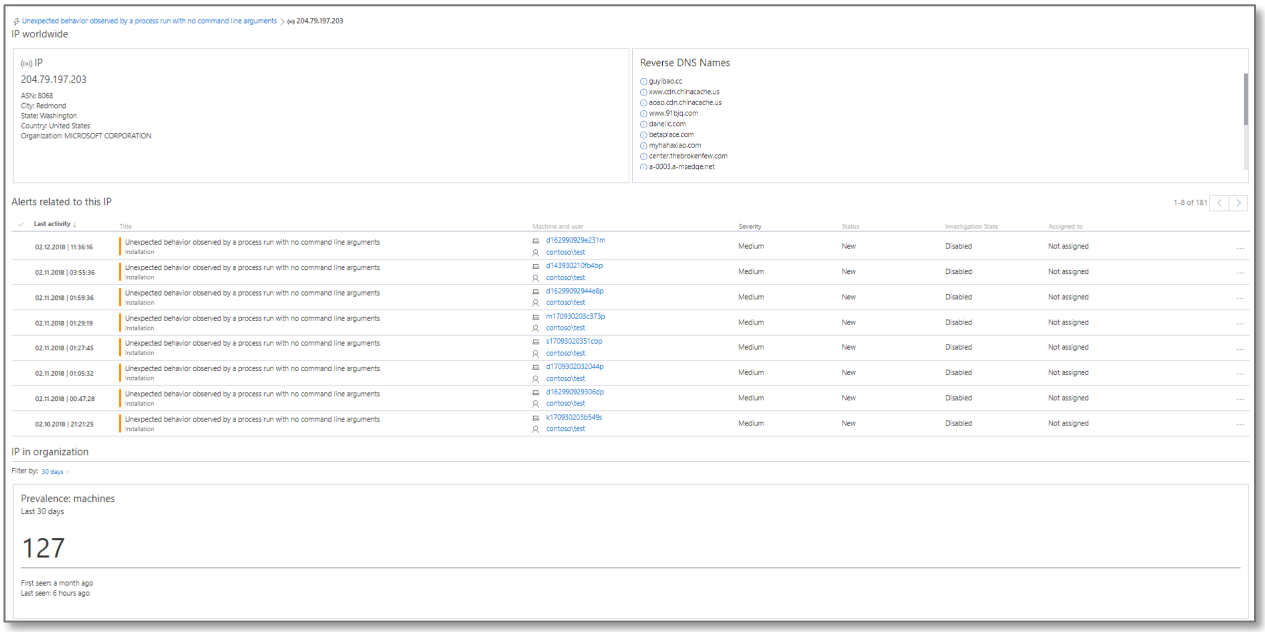
Validate the alert, collect artifacts, and determine scope
1. Inspect the file or URL/IP for suspicious characteristics – is it digitally signed? How prevalent is it? Where is it located? Do the domain registration and hosting history look normal?
2. Review the machine timeline for suspicious activities that may have occurred before and after the time of the alert.
3. Look for the presence of relevant artifacts on other systems. Identify commonalities and differences between potentially compromised systems.
4. Submit relevant files for deep analysis and review resulting detailed behavioral information.

Alert process tree

Figure 7. Alert for unexpected behavior by a process run with no command line arguments

✎ **Note**: Because this alert is based on machine-learning models that require some backend processing, it might take some time before it is actually generated on the portal.

Notice that the alert details include the external IP address—an indicator 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.



Unexpected behavior observed by a process run with no command line arguments > 204.79.197.203

IP worldwide

IP
204.79.197.203
ASN: 8068
City: Redmond
State: Washington
Country: United States
Organization: MICROSOFT CORPORATION

Reverse DNS Names

- guyibao.cc
- xww.cdn.chinacache.us
- aoao.cdn.chinacache.us
- www.91bjq.com
- danellc.com
- betaplace.com
- myhahaxiao.com
- center.thebrokenfew.com
- a-0003.a-msedge.net

Alerts related to this IP

1-8 of 181

Last activity ↓	Title	Machine and user	Severity	Status	Investigation State	Assigned to	
02.12.2018 | 11:36:16	Unexpected behavior observed by a process run with no command line arguments Installation	d162990929e231m contoso\test	Medium	New	Disabled	Not assigned	...
02.11.2018 | 03:55:36	Unexpected behavior observed by a process run with no command line arguments Installation	d143930210fb4bp contoso\test	Medium	New	Disabled	Not assigned	...
02.11.2018 | 01:59:36	Unexpected behavior observed by a process run with no command line arguments Installation	d16299092944e8p contoso\test	Medium	New	Disabled	Not assigned	...
02.11.2018 | 01:29:19	Unexpected behavior observed by a process run with no command line arguments Installation	m170930203c373p contoso\test	Medium	New	Disabled	Not assigned	...
02.11.2018 | 01:27:45	Unexpected behavior observed by a process run with no command line arguments Installation	s17093020351cbp contoso\test	Medium	New	Disabled	Not assigned	...
02.11.2018 | 01:05:32	Unexpected behavior observed by a process run with no command line arguments Installation	d1709302032044p contoso\test	Medium	New	Disabled	Not assigned	...
02.11.2018 | 00:47:28	Unexpected behavior observed by a process run with no command line arguments Installation	d162990929306dp contoso\test	Medium	New	Disabled	Not assigned	...
02.10.2018 | 21:21:25	Unexpected behavior observed by a process run with no command line arguments Installation	k170930203b549s contoso\test	Medium	New	Disabled	Not assigned	...

IP in organization

Filter by: 30 days

Prevalence: machines
Last 30 days

127

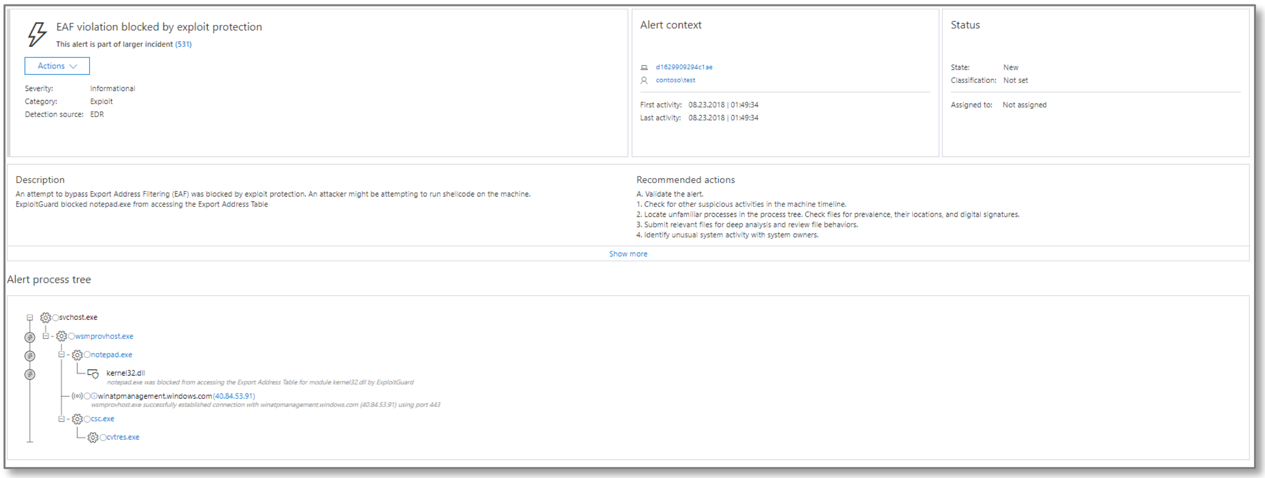
First seen: a month ago
Last seen: 6 hours ago

Figure 8. IP address details page

Alert: EAF violation blocked by exploit protection

By enabling exploit protection capabilities, we have hardened the victim machine against unexpected code execution. We have specifically enabled exploit protection rules that detect and prohibit unexpected code execution in *notepad.exe*. As a result, the simulated attempt to execute injected shellcode is detected and blocked, essentially stopping the attack's progression.

The exploit protection detection also results in a "EAF violation blocked by exploit protection" alert in the Microsoft Defender ATP portal. Note that the severity level of the alert is informational, because the attack was stopped. However, the security team is still notified that a possible exploitation attempt was made so they can take precautionary measures and be on the alert for a potentially persistent attacker.



EAF violation blocked by exploit protection

This alert is part of larger incident (531)

Severity: Informational
Category: Exploit
Detection source: EDR

Alert context

d1629909294c1ae
contoso\test

First activity: 08.23.2018 | 01:49:34
Last activity: 08.23.2018 | 01:49:34

Status

State: New
Classification: Not set

Assigned to: Not assigned

Description

An attempt to bypass Export Address Filtering (EAF) was blocked by exploit protection. An attacker might be attempting to run shellcode on the machine.
ExploitGuard blocked notepad.exe from accessing the Export Address Table

Recommended actions

A. Validate the alert.
1. Check for other suspicious activities in the machine timeline.
2. Locate unfamiliar processes in the process tree. Check files for prevalence, their locations, and digital signatures.
3. Submit relevant files for deep analysis and review file behaviors.
4. Identify unusual system activity with system owners.

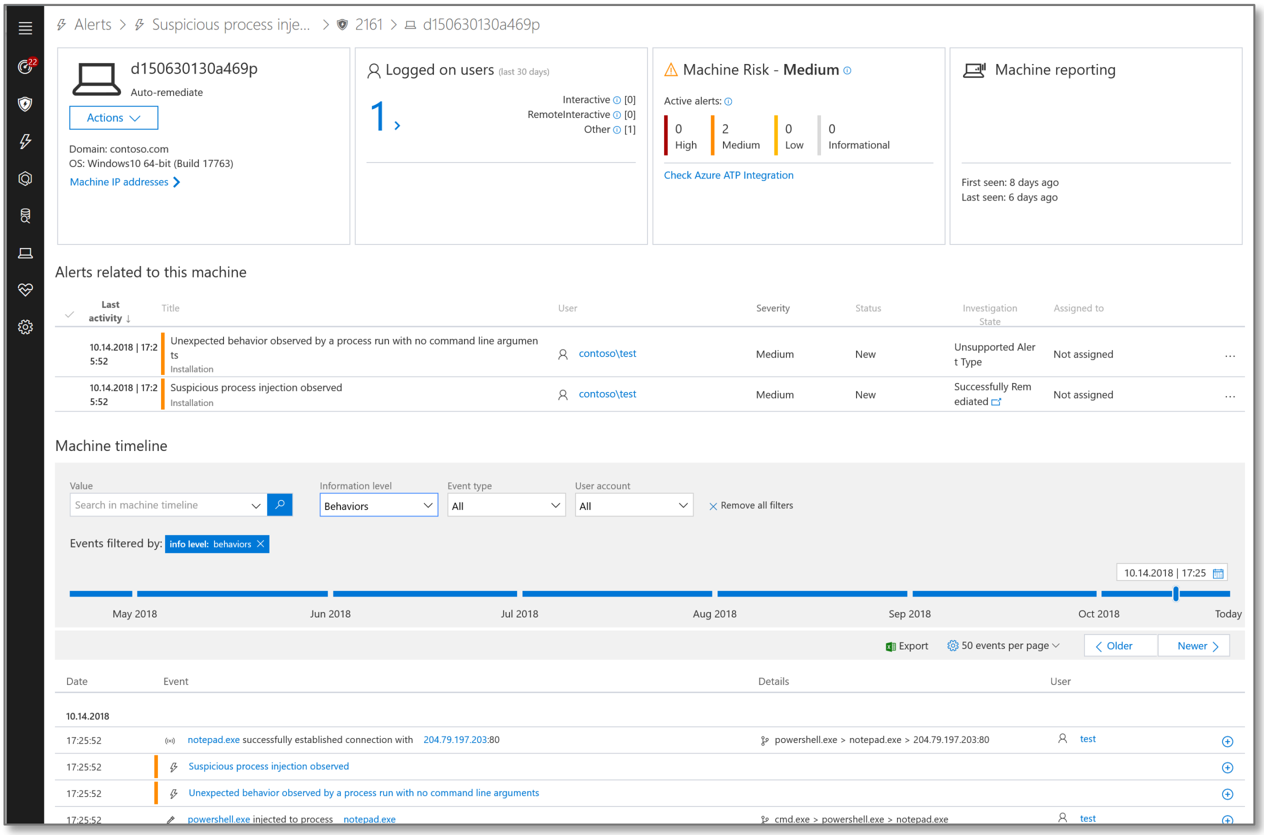
Alert process tree

```
svchost.exe
  wsmprovhost.exe
    notepad.exe
      kernel32.dll
      notepad.exe was blocked from accessing the Export Address Table for module kernel32.dll by ExploitGuard
    winatpmanagement.windows.com(40.84.53.91)
    wsmprovhost.exe successfully established connection with winatpmanagement.windows.com (40.84.53.91) using port 443
    csc.exe
      cvtres.exe
```

Figure 9. Alert for EAF violation detected by exploit protection

Review the machine timeline

Clicking on the machine name on one of the alert pages opens the machine details page. On this page, the alert itself and related events on the machine are provided to ease investigation. You can scroll through the machine timeline and view all events and behaviors observed on the machine in chronological order, interspersed with the alerts raised. Note the different information levels available: *detections, behaviors, and verbose*.



Alerts > Suspicious process inje... > 2161 > d150630130a469p

d150630130a469p
Auto-remediate
Actions
Domain: contoso.com
OS: Windows10 64-bit (Build 17763)
Machine IP addresses

Logged on users (last 30 days)
1
Interactive [0]
RemoteInteractive [0]
Other [1]

Machine Risk - **Medium**
Active alerts:
0 High
2 Medium
0 Low
0 Informational
Check Azure ATP Integration

Machine reporting
First seen: 8 days ago
Last seen: 6 days ago

Alerts related to this machine

Last activity ↓	Title	User	Severity	Status	Investigation State	Assigned to
10.14.2018 | 17:25:52	Unexpected behavior observed by a process run with no command line arguments Installation	contoso\test	Medium	New	Unsupported Alert Type	Not assigned
10.14.2018 | 17:25:52	Suspicious process injection observed Installation	contoso\test	Medium	New	Successfully Remediated	Not assigned

Machine timeline

Value: Search in machine timeline
Information level: Behaviors
Event type: All
User account: All
Remove all filters

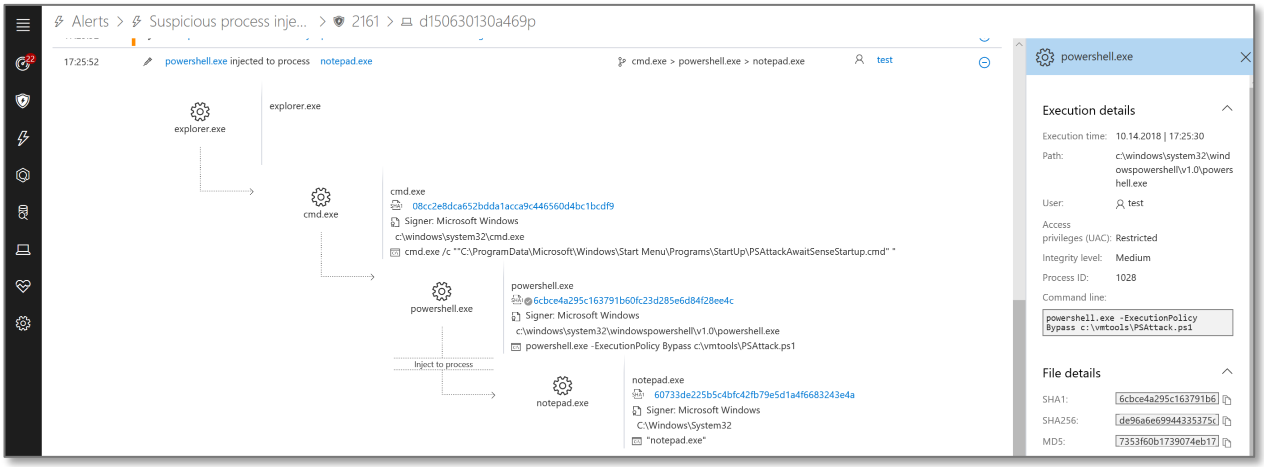
Events filtered by: info level: behaviors

10.14.2018 | 17:25

Date	Event	Details	User
10.14.2018			
17:25:52	notepad.exe successfully established connection with 204.79.197.203:80	powershell.exe > notepad.exe > 204.79.197.203:80	test
17:25:52	Suspicious process injection observed		
17:25:52	Unexpected behavior observed by a process run with no command line arguments		
17:25:52	powershell.exe injected to process notepad.exe	cmd.exe > powershell.exe > notepad.exe	test

Figure 10. Machine timeline with behaviors

Expanding some of the more interesting behaviors provides useful details, such as process trees. For example, clicking on the item **powershell.exe injected to process notepad.exe** displays the full process tree for this behavior. Selecting the powershell.exe will show more information on this specific execution



Alerts > Suspicious process inje... > 2161 > d150630130a469p

17:25:52 powershell.exe injected to process notepad.exe cmd.exe > powershell.exe > notepad.exe test

explorer.exe

cmd.exe
08cc2e8dca652bdda1acca9c446560d4bc1bcdf9
Signer: Microsoft Windows
c:\windows\system32\cmd.exe
cmd.exe /c ""C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\PSAttackAwaitSenseStartup.cmd" "

powershell.exe
6cbce4a295c163791b60fc23d285e6d84f28ee4c
Signer: Microsoft Windows
c:\windows\system32\windowspowershell\v1.0\powershell.exe
powershell.exe -ExecutionPolicy Bypass c:\vmtools\PSAttack.ps1

notepad.exe
60733de225b5c4bfc42fb79e5d1a4f6683243e4a
Signer: Microsoft Windows
C:\Windows\System32
"notepad.exe"

powershell.exe

Execution details

Execution time:	10.14.2018 | 17:25:30
Path:	c:\windows\system32\windowspowershell\v1.0\powershell.exe
User:	test
Access privileges (UAC):	Restricted
Integrity level:	Medium
Process ID:	1028

Command line:

```
powershell.exe -ExecutionPolicy
Bypass c:\vmtools\PSAttack.ps1
```

File details

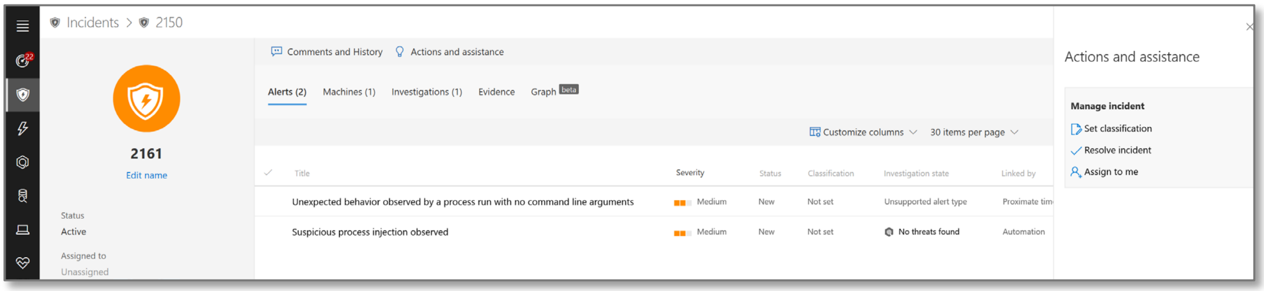
SHA1:	6cbce4a295c163791b6
SHA256:	de96a6e69944335375c
MD5:	7353f60b1739074eb17

Figure 11. Process tree for selected PowerShell file creation behavior

Resolve the incident

Now that the investigation is completed and, in our case, confirmed to be a benign activity, it is time to close the incident.

On the incident page, select **Actions and assistance** to get management options that apply to the entire incident and all related alerts.



Incidents > 2150

2161
Edit name

Status
Active

Assigned to
Unassigned

Title	Severity	Status	Classification	Investigation state	Linked by
Unexpected behavior observed by a process run with no command line arguments	Medium	New	Not set	Unsupported alert type	Proximate tim
Suspicious process injection observed	Medium	New	Not set	No threats found	Automation

Actions and assistance

Manage incident

Figure 14. Resolving the incident and related alerts

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.

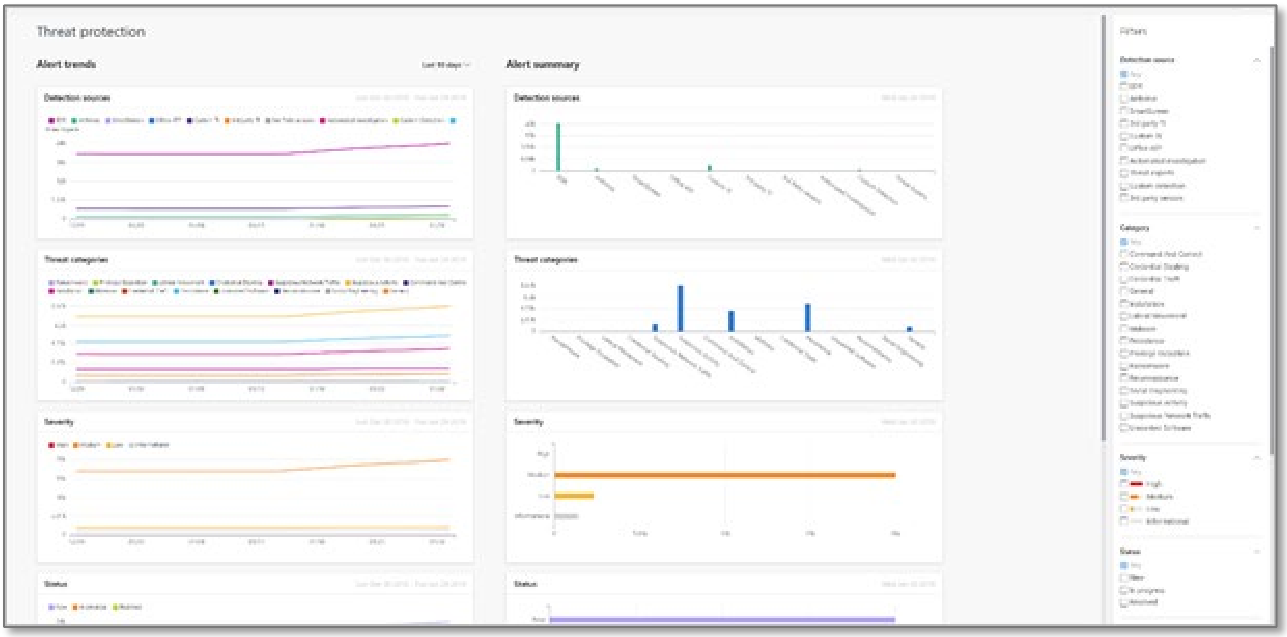


Figure 15. Threat protection report page

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 an advanced 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. We've seen how alerts are delivered along with other contextual information, enabling SOC personnel to investigate and take necessary action.

We hope you enjoyed this simulation and are now encouraged to explore other features and capabilities. For more information, read the product guide at 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!