



# Microsoft Defender Advanced Threat Protection

## Attack simulation

Scenario 1: Document drops backdoor

July 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: Document drops backdoor scenario

---

Attacks that introduce file-based malware using socially engineered email are quite common. Recipients are tricked into launching a backdoor that gives attackers control over what is now a compromised machine.

This scenario simulates such an attack on your selected test machine. You can then explore and understand how Microsoft Defender ATP detects the attack and enables prompt investigation and response.

This scenario 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 auto-start 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:**

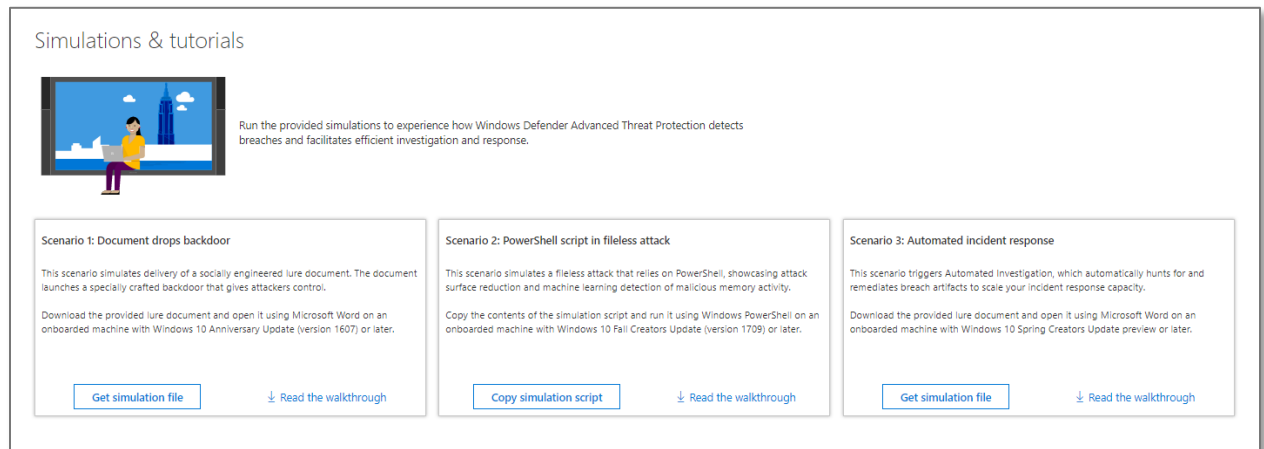
- Be onboarded to Microsoft Defender ATP
- Run Windows 10 Anniversary Update (version 1607) or later
- Have PowerShell turned on
- Have Windows Defender Antivirus turned on
- Have Microsoft Word installed

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**.

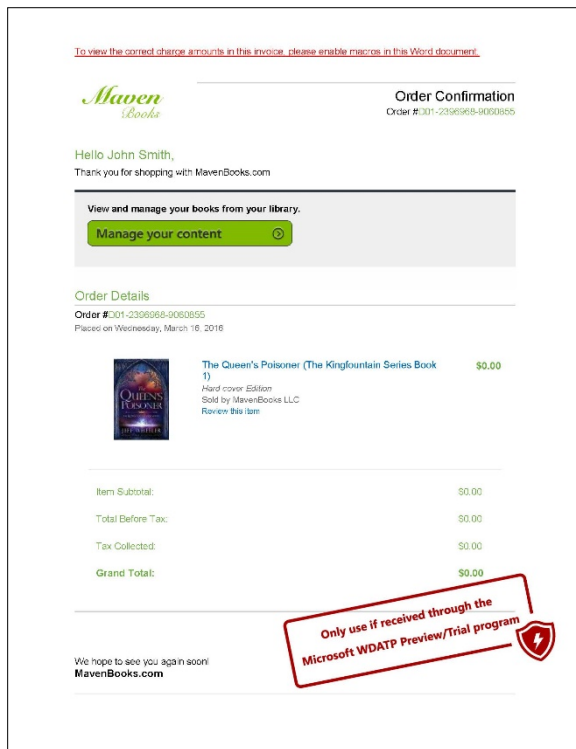


## *Simulation scenarios in the portal*

2. Click **Get simulation file** under **Scenario 1: Document drops backdoor** 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.

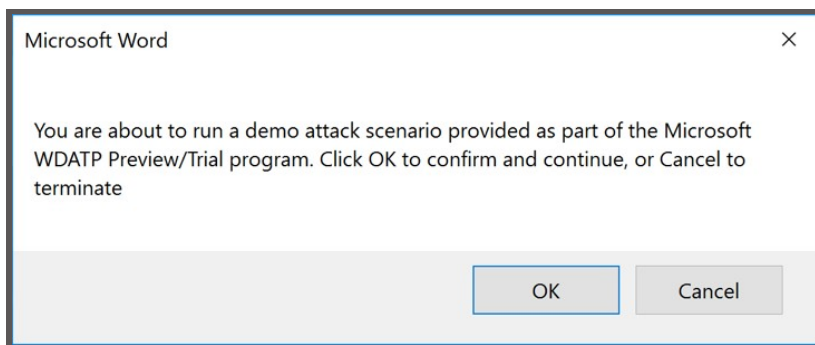
 **Note:** If your organization blocks macros in documents from the internet, you might need to unblock this specific document for the **Enable Content** option to work. To unblock the document, navigate to its location in File Explorer. In File Explorer, right-click the document, select **Properties**.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



*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 auto-start 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.

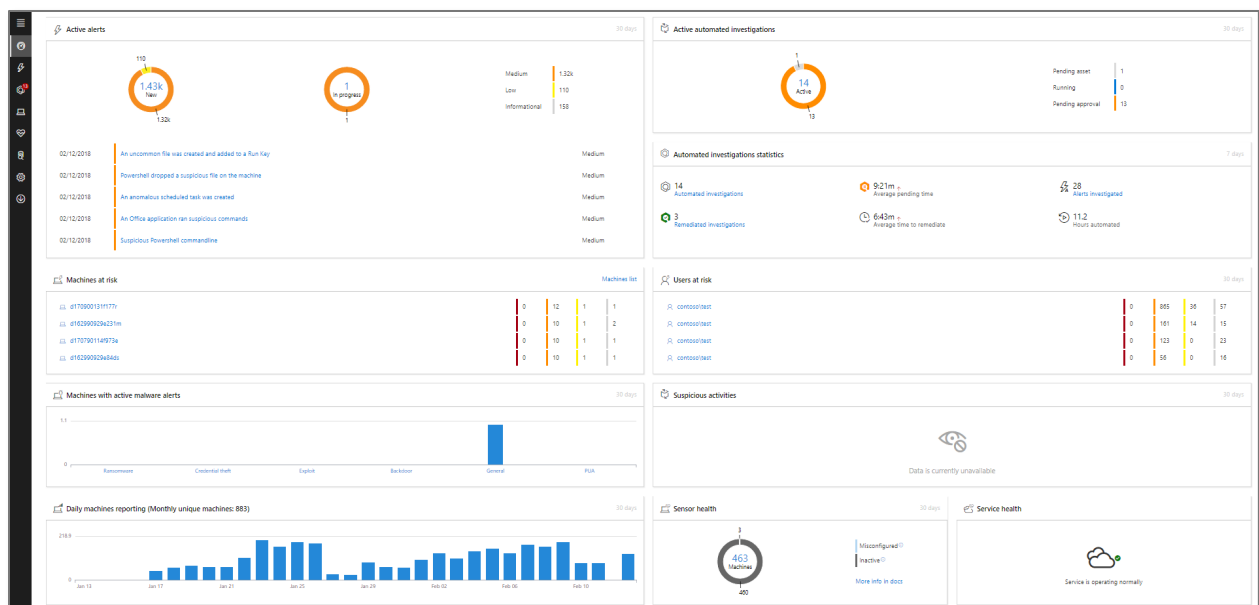
Next, let’s review and investigate the Microsoft Defender ATP alerts that surface the simulated attack.

 **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.



*Dashboard view showing the alerts*

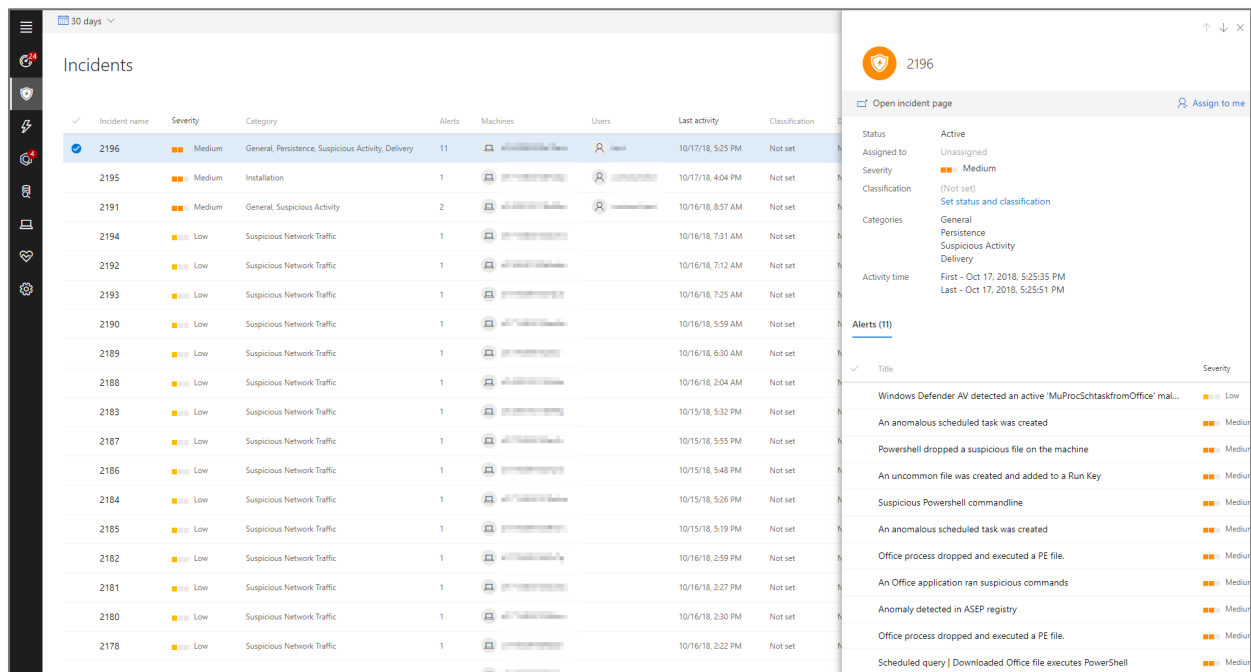


## Investigate the attack as a single incident

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.



Incident name	Severity	Category	Alerts	Machines	Users	Last activity	Classification
2196	Medium	General, Persistence, Suspicious Activity, Delivery	11			10/17/18, 5:25 PM	Not set
2195	Medium	Installation	1			10/17/18, 4:04 PM	Not set
2191	Medium	General, Suspicious Activity	2			10/16/18, 9:57 AM	Not set
2194	Low	Suspicious Network Traffic	1			10/16/18, 7:31 AM	Not set
2192	Low	Suspicious Network Traffic	1			10/16/18, 7:12 AM	Not set
2193	Low	Suspicious Network Traffic	1			10/16/18, 7:25 AM	Not set
2190	Low	Suspicious Network Traffic	1			10/16/18, 5:59 AM	Not set
2189	Low	Suspicious Network Traffic	1			10/16/18, 6:30 AM	Not set
2188	Low	Suspicious Network Traffic	1			10/16/18, 2:04 AM	Not set
2183	Low	Suspicious Network Traffic	1			10/15/18, 5:32 PM	Not set
2187	Low	Suspicious Network Traffic	1			10/15/18, 5:55 PM	Not set
2186	Low	Suspicious Network Traffic	1			10/15/18, 5:48 PM	Not set
2184	Low	Suspicious Network Traffic	1			10/15/18, 5:26 PM	Not set
2185	Low	Suspicious Network Traffic	1			10/15/18, 5:19 PM	Not set
2182	Low	Suspicious Network Traffic	1			10/16/18, 2:59 PM	Not set
2181	Low	Suspicious Network Traffic	1			10/16/18, 2:27 PM	Not set
2180	Low	Suspicious Network Traffic	1			10/16/18, 2:30 PM	Not set
2178	Low	Suspicious Network Traffic	1			10/16/18, 2:22 PM	Not set

**Incident 2196 Details:**

- Status: Active
- Assigned to: Unassigned
- Severity: Medium
- Classification: (Not set)
- Categories: General, Persistence, Suspicious Activity, Delivery
- Activity time: First - Oct 17, 2018, 5:25:35 PM; Last - Oct 17, 2018, 5:25:51 PM

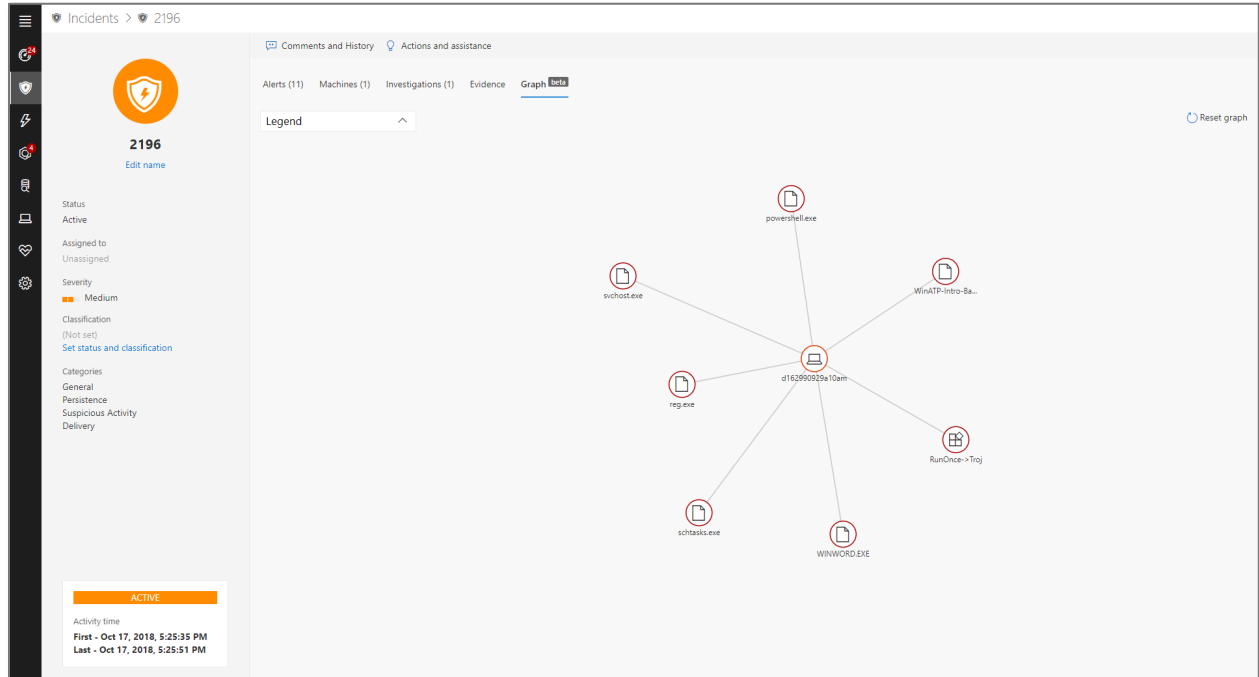
**Alerts (11):**

Title	Severity
Windows Defender AV detected an active 'MuProcSchtaskfromOffice' mal...	Low
An anomalous scheduled task was created	Medium
Powershell dropped a suspicious file on the machine	Medium
An uncommon file was created and added to a Run Key	Medium
Suspicious Powershell commandline	Medium
An anomalous scheduled task was created	Medium
Office process dropped and executed a PE file.	Medium
An Office application ran suspicious commands	Medium
Anomaly detected in ASEP registry	Medium
Office process dropped and executed a PE file.	Medium
Scheduled query   Downloaded Office file executes PowerShell	Medium

*Incident aggregating alerts generated during the simulation*

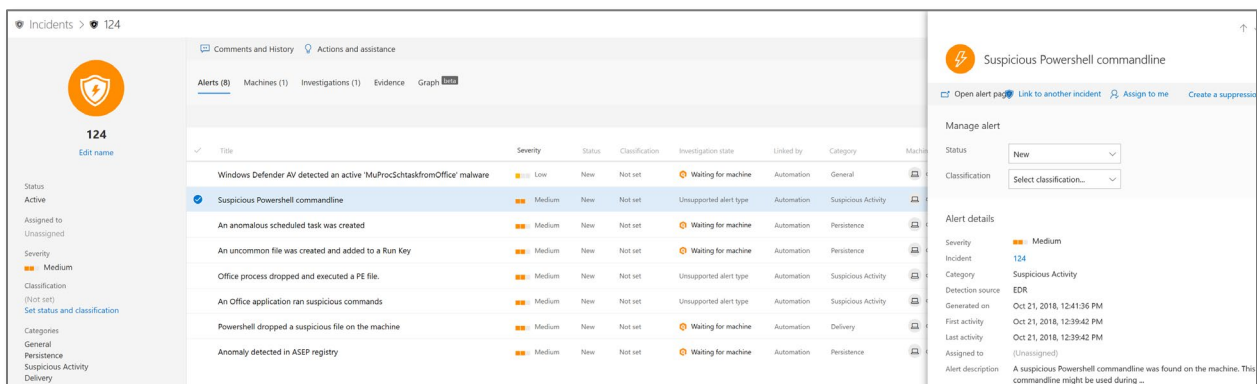
Select **Open incident page** to get more information about the incident.

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**.



*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




Title	Severity	Status	Classification	Investigation state	Linked by	Category
Windows Defender AV detected an active 'MuProcSchtaskfromOffice' malware	Low	New	Not set	Waiting for machine	Automation	General
<b>Suspicious Powershell commandline</b>	Medium	New	Not set	Unsupported alert type	Automation	Suspicious Activity
An anomalous scheduled task was created	Medium	New	Not set	Waiting for machine	Automation	Persistence
An uncommon file was created and added to a Run Key	Medium	New	Not set	Waiting for machine	Automation	Persistence
Office process dropped and executed a PE file.	Medium	New	Not set	Unsupported alert type	Automation	Suspicious Activity
An Office application ran suspicious commands	Medium	New	Not set	Unsupported alert type	Automation	Suspicious Activity
Powershell dropped a suspicious file on the machine	Medium	New	Not set	Waiting for machine	Automation	Delivery
Anomaly detected in ASEP registry	Medium	New	Not set	Waiting for machine	Automation	Persistence

*Actions and assistance options for managing the incident*

## Review generated alerts

---

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

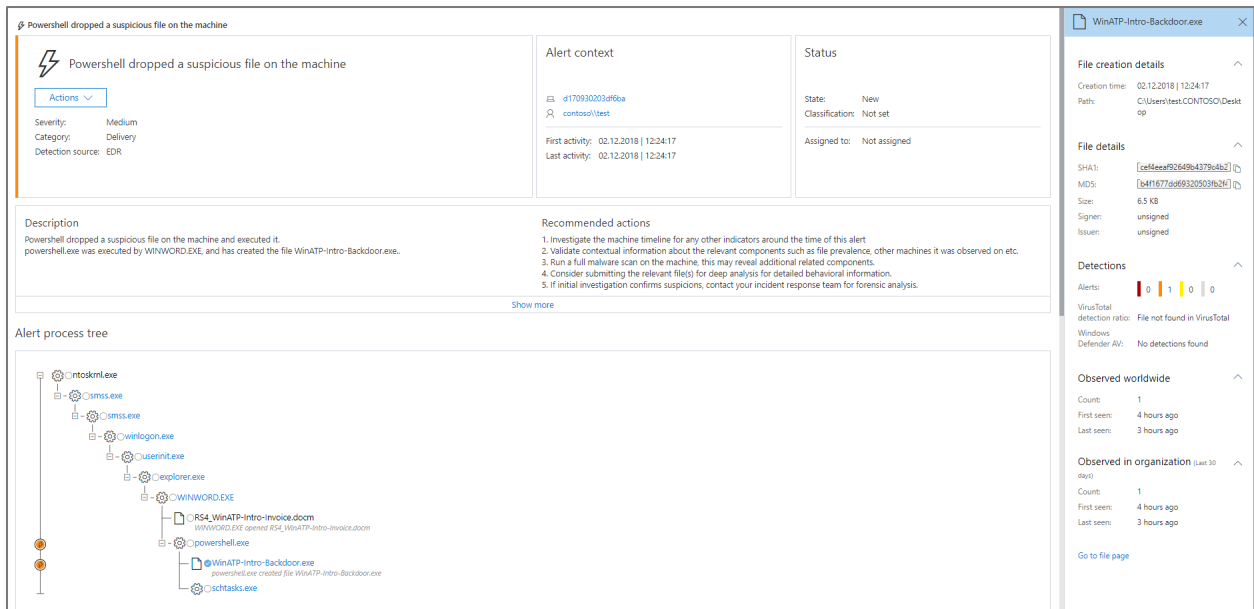
 **Note:** We will walk through only a few of the alerts generated during the simulated attack. Depending on the version of Windows and the Windows Defender Antivirus protection updates running on your test machine, you might see more alerts and they might appear in a slightly different order.

### Alert: PowerShell dropped a suspicious file on the machine

A macro in the Word document we opened used PowerShell to write an executable to disk. Microsoft Defender ATP monitors executables created by Office applications, including executables dropped using PowerShell, and looks for files that are rare relative to your organization or to everyone else.

On the machine details page or any of the alert queues, click the name of this alert to see details such as:

- Detailed description and recommended actions
- The process tree related to the files and processes in the alert, including command lines, times of execution, and other details shown in the side pane for selected processes
- The incident graph, including other machines in the organization this file was observed on
- The artifact timeline, providing details of the event(s) that triggered the alert on this machine, including time observed, as well as the name, path and SHA1 hash of the dropped file.



**PowerShell dropped a suspicious file on the machine**

**Alert context**

- Alert ID: d170930203df6ba
- First activity: 02.12.2018 | 12:24:17
- Last activity: 02.12.2018 | 12:24:17

**Status**

- State: New
- Classification: Not set
- Assigned to: Not assigned

**Description**

PowerShell dropped a suspicious file on the machine and executed it. powershell.exe was executed by WINWORD.EXE, and has created the file WinATP-Intro-Backdoor.exe.

**Recommended actions**

1. Investigate the machine 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. Run a full malware scan on the machine, this may reveal additional related components.
4. Consider submitting the relevant file(s) for deep analysis for detailed behavioral information.
5. If initial investigation confirms suspicions, contact your incident response team for forensic analysis.

[Show more](#)

**Alert process tree**

```

graph TD
    ntoskrnl.exe --> smss.exe
    smss.exe --> csrss.exe
    csrss.exe --> winlogon.exe
    winlogon.exe --> csrssinit.exe
    csrssinit.exe --> Explorer.exe
    Explorer.exe --> WINWORD.EXE
    WINWORD.EXE --> RS4_WinATP-Intro-Invoice.docm
    RS4_WinATP-Intro-Invoice.docm --> powershell.exe
    powershell.exe --> WinATP-Intro-Backdoor.exe
    WinATP-Intro-Backdoor.exe --> schtasks.exe
  
```

**File creation details**

- Creation time: 02.12.2018 | 12:24:17
- Path: C:\Users\test\CONTOSO\Desktop

**File details**

- SHA1: [ce4f5ea952649b4379c4b2]
- MD5: [bd4f1677d689320503b26f]
- Size: 6.5 KB
- Signer: unsigned
- Issuer: unsigned

**Detections**

Alerts: 0 1 0 0

VirusTotal detection ratio: File not found in VirusTotal

Windows Defender AI: No detections found

**Observed worldwide**

Count: 1

First seen: 4 hours ago

Last seen: 3 hours ago

**Observed in organization** (Last 30 days)

Count: 1

First seen: 4 hours ago

Last seen: 3 hours ago

[Go to file page](#)

### Alert details page

Select the file in the alert process tree (checking the circle next to it) to display the File Details pane at right. Here you can see details about the file, including hashes, size, Virus Total summary, and more.



To inspect the file further, select **Go to file page**. For more information about the file page, read [Inspect and download the backdoor file](#).

The PowerShell invocation pattern used in the macro exhibited traits indicating stealth and intent to evade detection. This attempt to remain stealthy triggered this alert.

Suspicious Powershell commandline
Automated investigation disabled

### Suspicious Powershell commandline

**Actions**

Severity: Medium  
Category: Suspicious Activity  
Detection source: EDR

### Description

A suspicious Powershell commandline was found on the machine. This commandline might be used during installation, exploration, or in some cases with lateral movement activities which are used by attackers to invoke modules, download external payloads, and get more information about the system. Attackers usually use PowerShell to bypass security protection mechanisms by executing their payload without touching the disk and leaving any trace. The process powershell.exe was executing suspicious commandline

```
powershell.exe -WinAuto -FreeDnsGet -Command cd &'FileDecatProfile' -> &'FileDecatProfile' -FileDecatProfile
```

### Alert context

d170930203df6ba  
contoso/test

---

First activity: 02.12.2018 | 12:24:06  
Last activity: 02.12.2018 | 12:24:06

### Status

State: New  
Classification: Not set

---

Assigned to: Not assigned

### Recommended actions

- Examine the PowerShell commandline to understand what commands were executed. Note: the script may need to be decoded if it is base64-encoded
- Search the script for more indicators to investigate - for example IP addresses (potential C&C servers), target computers etc.
- Explore the timeline of this and other related machines for additional suspect activities around the time of the alert.
- Look for the process that invoked this PowerShell run and their origin. Consider submitting any suspect files in the chain for deep analysis for detailed behavior information.

[Show more](#)

### Attack simulation scenario 1: Document drops backdoor

A common technique used by attackers to obtain long-term persistence on victim machines is to register for automatic start after reboot using one of several ASEP (Automatic Start Extensibility Point) registry keys. Microsoft Defender ATP monitors for such anomalous auto-start registrations, as we see performed on this machine to install our simulated backdoor.

Alert details showing the file and the registry Run key

## Alert: An anomalous scheduled task was created

Attackers also commonly use scheduled tasks as a persistence technique. However, these can also be used for other purposes, such as to delay the next phases of an attack, remaining quiet and stealthy in the process. Regardless of its usage, Microsoft Defender ATP detects anomalous scheduled tasks—including ones that are rare and not seen elsewhere in the organization—and alerts about it.

**An anomalous scheduled task was created**

Severity: Medium  
Category: Persistence  
Detection source: EDR

**Alert context**

Source: d170930203@fiba  
Target: contoso\test

First activity: 02.12.2018 | 12:24:11  
Last activity: 02.12.2018 | 12:24:11

**Status**

State: New  
Classification: Not set  
Assigned to: Not assigned

**Description**

An anomalous scheduled task was created. This may be used by an attacker to obtain persistence on the machine.

**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.

[Show more](#)

**Alert process tree**

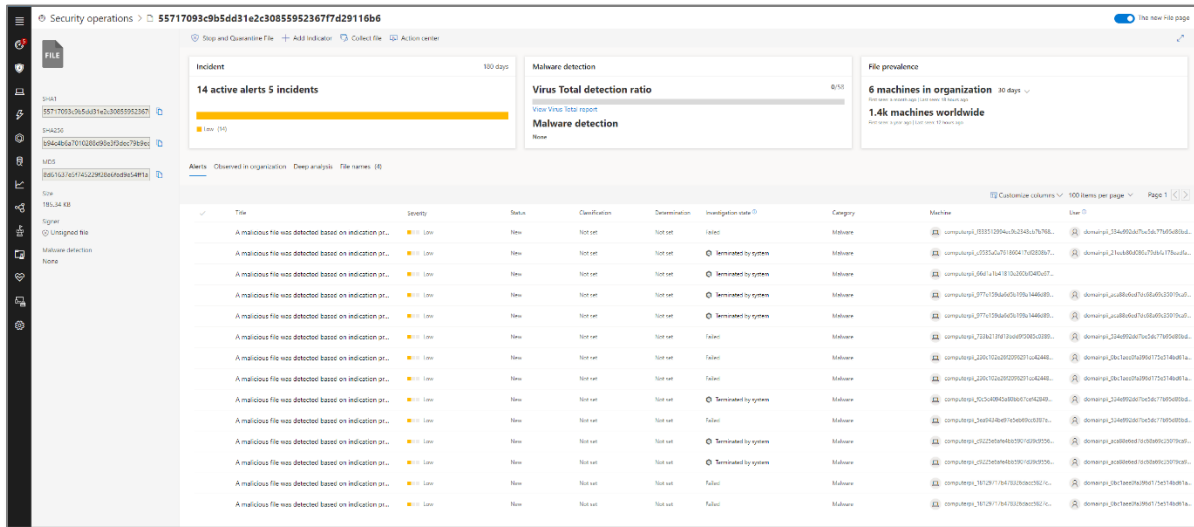
```

graph TD
    ntoskrnl.exe --> smss.exe
    smss.exe --> csrss.exe
    csrss.exe --> winlogon.exe
    winlogon.exe --> userinit.exe
    userinit.exe --> explorer.exe
    explorer.exe --> WINWORD.EXE
    WINWORD.EXE --> RS4_WinATP-intro-invoice.docm
    RS4_WinATP-intro-invoice.docm --> powershell.exe
    powershell.exe --> schtasks.exe
    
```

*Alert for anomalous creation of a scheduled task*

# Inspect and download the backdoor file

In this simulation, you can inspect the simulated backdoor by selecting its file name, **WinATP-Intro-Backdoor.exe**, on the alert **PowerShell dropped a suspicious file on the machine**. Selecting **Go to file page** takes you to a full page about the file.



The screenshot shows the Microsoft Defender ATP interface. On the left, there's a sidebar with navigation options like 'Incident', 'Alerts', 'File', 'Process', 'Network', 'Device', 'User', 'Group', 'Machine', 'Process', 'Network', 'Device', 'User', 'Group', 'Machine'. The main area displays a list of alerts. The selected alert is 'A malicious file was detected based on indication pr...'. The details pane on the right shows the file's properties, including its name, size, and a list of machines it was observed on. The file is identified as 'WinATP-Intro-Backdoor.exe'.

File page for the simulated backdoor

## Get detailed information about the file

In the file page, you get comprehensive information about the simulated backdoor, including:

- File hashes
- Signer name, if it is validly signed
- Alerts raised on this file
- The number of machines it was observed on, in the organization and worldwide
- Names used by the same file in the organization
- Machines in the organization it was observed on, indicating its origins and the footprint in the organization

To perform further forensics on the file itself, submit the file for deep analysis, which provides automated analysis in a controlled environment. Or you can download the file.




## Download the file

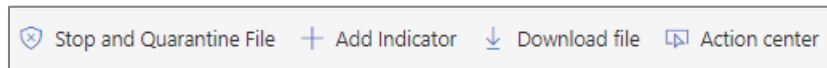
To download a file, it must already be in Microsoft Defender ATP sample storage. If the file is not in storage, the action bar shows a **Collect file** option.



Select **Collect file** to gather the file from one of your machines.

 **Note:** File collection might take several hours depending on the availability of machines.

As soon as the file has been collected, select **Download file** to obtain a copy of the file.



# 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.

The screenshot shows the Microsoft Defender ATP interface for a specific machine named 'jedawant'. The left sidebar contains machine details: 'jedawant', 'Circum: AAD joined', 'OS: Windows 10 x64', 'Version: 19H2', 'Build: 18362', 'Local group: WANDisque\_1', 'Risk level: Medium', 'Exposure level: Medium', 'Health state: Active', 'Action alerts: 7', 'Active incidents: 6', 'Azure AD alerts: Machine not found at Azure ATP', 'First seen: Jun 26, 2018, 8:45:04 PM', 'Last seen: May 28, 2019, 4:20:21 PM', and 'IP addresses: See IP addresses info'.

The main content area is divided into several sections:

- Active alerts:** Risk level: Medium, 7 active alerts in 5 incidents. A bar chart shows the distribution of risk levels: Medium (7), Informational (0).
- Logged on users:** 1 logged on user. Most frequent: DIY, Least frequent: DIY. A link 'See all users' is available.
- Security assessments:** Exposure level: Medium (50), 50 Security recommendations, 46 Installed software, 44 Discovered vulnerabilities.
- Timeline:** A horizontal timeline from Dec 2018 to May 2019. Below it, a table lists events with columns for Event time, Event, Additional information, User, Action, and Action type.

Event time	Event	Additional information	User	Action	Action type
May 28, 2019, 4:20:21.727 PM	Multiple processes successfully established connection with 13.64.188.245.443 (outgoing...)		system	chrome.exe > Mapping.exe > 13.64.188.245.443 (outgoing...)	ConnectionSuccess
May 28, 2019, 4:20:21.626 PM	Multiple processes created process log (C:\ProgramData\Microsoft\Windows Defender\Signature\...)		system	chrome.exe > Mapping.exe > log (C:\ProgramData\Microsoft\Windows Defender\Signature\...)	ProcessCreated
May 28, 2019, 4:17:49.476 PM	The chrome.exe access token was modified		chrome	chrome.exe > chrome.exe > Access token modification	ProcessPrimaryTokenModified
May 28, 2019, 4:17:49.254 PM	chrome.exe successfully established connection with 93.184.215.201 (443) (outgoing...)		chrome	chrome.exe > chrome.exe > 93.184.215.201 (443) (outgoing...)	ConnectionSuccess
May 28, 2019, 4:17:49.156 PM	chrome.exe successfully established connection with 13.107.6.175.443 (outgoing...)		chrome	chrome.exe > chrome.exe > 13.107.6.175.443 (outgoing...)	ConnectionSuccess
May 28, 2019, 4:17:49.079 PM	chrome.exe created process chrome.exe		chrome	chrome.exe > chrome.exe > chrome.exe	ProcessCreated
May 28, 2019, 4:17:49.051 PM	chrome.exe created process chrome.exe		chrome	chrome.exe > chrome.exe > chrome.exe	ProcessCreated
May 28, 2019, 4:17:48.991 PM	chrome.exe opened link		chrome	chrome.exe > chrome.exe > https://www.microsoft.com/.../.../...	BrowserLaunchSuccessful
May 28, 2019, 4:17:48.914 PM	chrome.exe successfully established connection with 13.107.6.175.443 (outgoing...)		chrome	chrome.exe > chrome.exe > 13.107.6.175.443 (outgoing...)	ConnectionSuccess
May 28, 2019, 4:17:39.133 PM	The chrome.exe access token was modified		chrome	chrome.exe > chrome.exe > Access token modification	ProcessPrimaryTokenModified
May 28, 2019, 4:17:39.042 PM	chrome.exe successfully established connection with 13.107.6.175.443 (outgoing...)		chrome	chrome.exe > chrome.exe > 13.107.6.175.443 (outgoing...)	ConnectionSuccess
May 28, 2019, 4:17:39.012 PM	chrome.exe created process chrome.exe		chrome	chrome.exe > chrome.exe > chrome.exe	ProcessCreated
May 28, 2019, 4:17:37.724 PM	chrome.exe successfully established connection with 13.107.6.175.443 (outgoing...)		chrome	chrome.exe > chrome.exe > 13.107.6.175.443 (outgoing...)	ConnectionSuccess
May 28, 2019, 4:17:37.652 PM	The chrome.exe access token was modified		chrome	chrome.exe > chrome.exe > Access token modification	ProcessPrimaryTokenModified
May 28, 2019, 4:17:37.652 PM	chrome.exe created process chrome.exe		chrome	chrome.exe > chrome.exe > chrome.exe	ProcessCreated
May 28, 2019, 4:17:35.146 PM	chrome.exe successfully established connection with 13.107.6.175.443 (outgoing...)		chrome	chrome.exe > chrome.exe > 13.107.6.175.443 (outgoing...)	ConnectionSuccess

Machine timeline with behaviors

Expanding some of the more interesting behaviors provides useful details, such as process trees and file creation relationships. For example, clicking on the item **powershell.exe created WinATP-Intro-Backdoor.exe** displays the full process tree for this behavior.

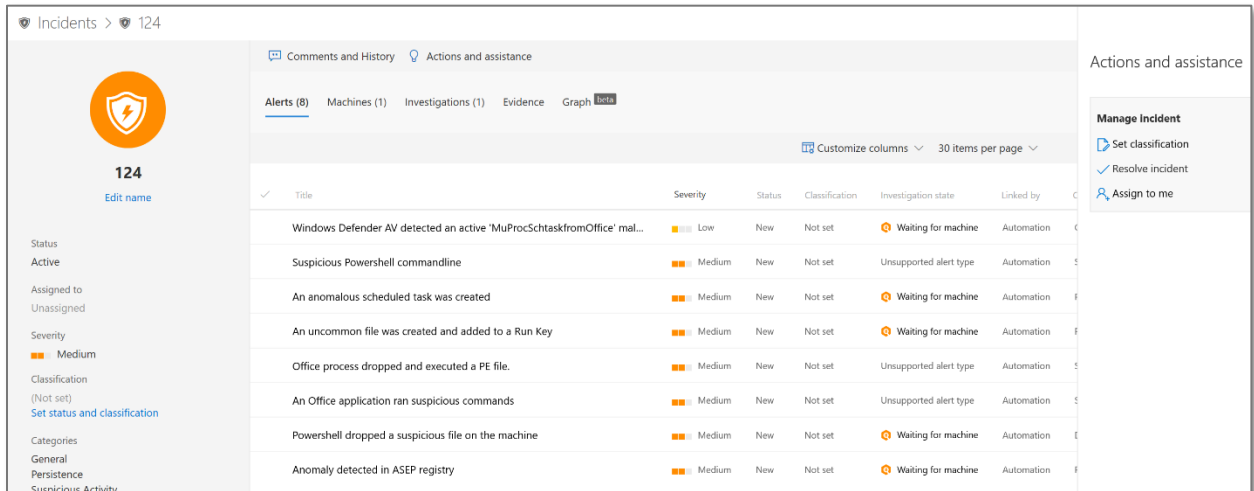
The screenshot displays the Microsoft Defender ATP console interface. On the left, a sidebar shows the machine 'daseeds-azrvm' with details like OS (Windows 10 x64) and version (19H1). The main area is divided into two panes. The left pane, titled 'Active alerts', shows a risk level of 'No known risks' and 3 active alerts. The right pane, titled 'powershell.exe created WinATP-Intro-Backdoor.exe', provides a detailed view of the event. It includes event information such as event time (May 25, 2019, 10:20:10.364 AM) and action type (ProcessCreated). Below this, a 'Process tree' graph shows the hierarchy of processes: powershell.exe created powershell.exe, which then created WinATP-Intro-Backdoor.exe. The WinATP-Intro-Backdoor.exe process is highlighted, showing its path (C:\Windows\System32\powershell.exe) and integrity level (System).

*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 > 124

Comments and History Actions and assistance

Alerts (8) Machines (1) Investigations (1) Evidence Graph **124**

Customize columns 30 items per page

✓	Title	Severity	Status	Classification	Investigation state	Linked by
	Windows Defender AV detected an active 'MuProcSchtaskfromOffice' mal...	Low	New	Not set	Waiting for machine	Automation
	Suspicious Powershell commandline	Medium	New	Not set	Unsupported alert type	Automation
	An anomalous scheduled task was created	Medium	New	Not set	Waiting for machine	Automation
	An uncommon file was created and added to a Run Key	Medium	New	Not set	Waiting for machine	Automation
	Office process dropped and executed a PE file.	Medium	New	Not set	Unsupported alert type	Automation
	An Office application ran suspicious commands	Medium	New	Not set	Unsupported alert type	Automation
	Powershell dropped a suspicious file on the machine	Medium	New	Not set	Waiting for machine	Automation
	Anomaly detected in ASEP registry	Medium	New	Not set	Waiting for machine	Automation

Actions and assistance

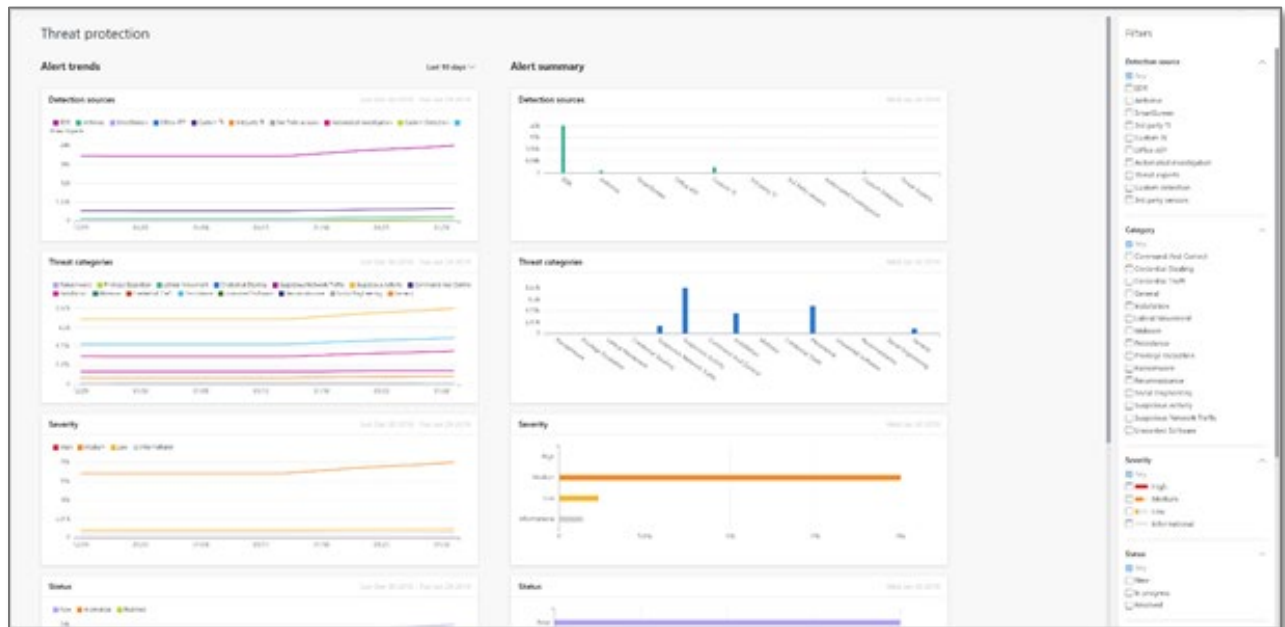
Manage incident

- Set classification
- Resolve incident
- Assign to me

*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.



*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. We saw what the alerts look like and the detailed contextual file, machine, and event information provided with each alert.

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](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!