

Microsoft Defender ATP

Demo Guide

Updated: 03/10/2020

This document is provided “as-is”. Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

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.

© 2020 Microsoft. All rights reserved.

**Table of Contents**

[Before you begin 3](#_Toc34727152)

[Demo Home Page and login 3](#_Toc34727153)

[Devices 3](#_Toc34727154)

[User Accounts 3](#_Toc34727155)

[Pre-demo Setup Steps 3](#_Toc34727156)

[Microsoft Defender ATP Demo 3](#_Toc34727157)

[Deployment and Onboarding 4](#_Toc34727158)

[Detection and Investigation of Alerts 4](#_Toc34727159)

[Investigating MDATP Security Alerts 5](#_Toc34727160)

[MDATP File Investigation 7](#_Toc34727161)

[MDATP File-less Attack Investigation 8](#_Toc34727162)

[MDATP Machine Investigation & Analyzing Email Threats with Office 365 Threat Intelligence 10](#_Toc34727163)

[MDATP Threat Analytics 14](#_Toc34727164)

[MDATP Threat & Vulnerability Management (TVM) 16](#_Toc34727165)

[Section 1: Review the TVM dashboard 16](#_Toc34727166)

[Section 2: Reviewing Security recommendations 18](#_Toc34727167)

[Section 3: Submitting a Remediation request or creating an Exception 19](#_Toc34727168)

[Section 4: Monitoring remediation activities and exceptions 20](#_Toc34727169)

[Section 5: Reviewing Software inventory and Software page 20](#_Toc34727170)

[Section 6: Machine page 21](#_Toc34727171)

[Section 7: Weaknesses page 22](#_Toc34727172)

[Section 8: Advanced Hunting for Threat Vulnerabilities 23](#_Toc34727173)

[Section 9: Global TVM search 24](#_Toc34727174)

[Section 10: Machine group filtered TVM context 24](#_Toc34727175)

[MDATP Live Response 25](#_Toc34727176)

[Get a mini memory dump using a PowerShell script 25](#_Toc34727177)

[Use forensic tools to gather forensic information 28](#_Toc34727178)

[MDATP Power BI reports 30](#_Toc34727179)

[Conclusion 33](#_Toc34727180)

[[Optional] Building MDATP Power BI reports 33](#_Toc34727181)

[Reset Instructions 37](#_Toc34727182)

# Before you begin

## Demo Home Page and login

You will need to log into a shared MTP Demos tenant at the following URL: <https://securitycenter.windows.com/> to complete this demo.

**IMPORTANT NOTE: This is a shared tenant. Please refrain from making any changes to the tenant or the user’s profile, else it will hamper the demo experience of your colleagues!**

This shared demo environment has numerous endpoints perpetually connected to it. These endpoints are used to generate alerts based on user and machine activity simulations of both good and bad actors. These activities are repeated on a recurring basis (weekly and monthly) so alerts remain fresh on the appropriate dashboards/reports and are always demo ready. Due to the changing nature of the product and the environment, the exact alert or click step described in this demo guide may not appear in the tenant for your demo session.

## Devices

For the **Optional** section below, you will need to use your own demo environment configured and equipped with the following:

A **Windows 10** (Build 1903 or greater) **endpoint** with [**PowerBI Desktop**](https://www.microsoft.com/en-us/download/confirmation.aspx?id=58494&6B49FDFB-8E5B-4B07-BC31-15695C5A2143=1) **client** app installed which is **MDATP On-Boarded**, as well as **Azure AD joined** to an **MDATP enabled tenant** with some **pre-populated device and user activity**.

## User Accounts

* **SecOps user**: (**MTPGlobalReader@mtpdemos.net**) is a Security Operations Center (SOC) analyst in a hypothetical organization’s IT Department. They have Security Reader access to the demo tenant.
* **Password**: MTPz@p!MTPz@p!

# Pre-demo Setup Steps

Launch a browser session (**InPrivate**, if necessary) and sign in to the shared demo tenant’s **Microsoft Defender** Security Center portal, <https://securitycenter.windows.com> using the **SecOps user** credentials above.

# Microsoft Defender ATP Demo

**Microsoft Defender ATP** is a unified endpoint security platform for preventative protection, post-breach detection, automated investigation, and response. Microsoft Defender ATP protects endpoints from cyber threats, detects advanced attacks and data breaches, automates security incidents, and improves security posture. In this demo, you will shadow the path of a SecOps user who is performing a routine check on their organization’s security posture.

## Deployment and Onboarding

| **What to say** | **What to show** |
| --- | --- |
| **Microsoft Defender ATP** is built into Windows 10, not bolted on, so there is nothing to deploy. All it requires is to run a small onboarding script on each of the endpoint machines to onboard them to the service. The script sets the registry on the machines to report activities to the MDATP service. There’s no agent to install/run on the machines.  Besides Windows, MDATP can onboard and monitor non-Windows endpoints, including Linux, Mac OS, iOS and Android.  The SecOps team can also choose the deployment method that’s convenient for the organization, such as System Center Config Manager, MDM/Intune or Group Policy. | * + 1. Restore the admin user’s browser session, signed in to <https://securitycenter.windows.com>.     2. In the left navigation, go to **Settings** > **Machine management** > **Onboarding**.     3. Open the **Select operating system…** drop-down menu to show options.   A screenshot of a cell phone  Description automatically generated   * + 1. Open the **Deployment method** drop-down menu to show options. |

## Detection and Investigation of Alerts

|  |  |
| --- | --- |
| **What to say** | **What to show** |
| Here, in the MDATP Dashboard, is an operational view of the organization’s endpoints and users which gives the SecOps user an aggregated view of the latest alerts, their severity and when they were observed. It also provides a listing of the machines most at risk with several alerts related to each machine and indicates users at risk, providing insight into the activities, actions, and relationships to the machine. .  The security operations dashboard in MDATP provides a single pane of glass and centralized management. | * + 1. At the top under the URL, click **Microsoft Defender Security Center** label to navigate to the **Security Operations** dashboard.      * + 1. Scroll down the page, and point to the following reports:        1. **Active alerts**        2. **Active automated investigations**        3. **Automated investigation statistics**        4. **Machines at risk**        5. **Users at risk** |

## Investigating MDATP Security Alerts

|  |  |
| --- | --- |
| **What to say** | **What to show** |
| Alerts are any security-related incidents collected from the organization’s endpoints and flagged by the MDATP service. MDATP applies correlation analytics and aggregates all related alerts and investigations into one “**Incident**” entity. By doing so, MDATP narrates a broader attack story, allowing the SecOps user to understand and deal with complex threats across the org with the right visuals.  Our SecOps user can see the latest alerts from all machines that are onboarded in the entire organization, along with the severity of each alert.  Severity in this context is the potential impact the associated malware may have on an organization as a whole – not just to a single endpoint or a single user.  Dropping into the Incidents queue, and then selecting an incident, allows the user to see an alert where a PowerShell dropped a suspicious file on the End Users’ machine.  It is marked as a “medium” severity alert, however, the SecOps team wants to understand the context and see what actions we might need to take.  Microsoft Defender Security Center allows the SecOps user to set alert status, set classification types, or create a rule to suppress the alert next time it occurs in a specific machine or anywhere in the organization.  The alert story takes alert triage and investigation to the next level, displaying the alert and related evidence, together with other events that occurred within the same execution context and time. This rich triage context of the alert and surrounding events is available on the alert page.  At the top of the alert, the SecOps user can see how this incident has affected the entire org. What users and machines were involved, in this alert.  Tracing down the malware related to this alert, SecOps can see that PowerShell was used to schedule an unusual task to run an unknown executable on the PC!  Looking into the Alert story, The SecOps user can see that the file that was dropped is called **WinATP-Intro-Backdoor.exe** and that file name sounds very suspicious, but the SecOps user does not yet know if it is truly a malicious file or not. The SecOps Team can easily find out more by visiting the detailed file investigation page. | **Note:** If you see an alert in the top-right corner prompting for action, click **Snooze for 1 hour** to dismiss.   * + 1. In the left navigation, click **Incidents***.* (Shield Icon)     2. If necessary (i.e. you don’t see items in the current view), change the range of incidents to **6 months**.      * + 1. Select an incident corresponding to the machine, **MDATP Incident - <Most Recent Date>**.   **NOTE:** ([direct link to the incident](https://securitycenter.windows.com/incidents/4809/overview)).     * + 1. From within the incident click the **Alerts** tab.     2. From the list of **Alerts**, locate and click on alert titled: **Powershell dropped a suspicious file on the machine**.     3. Point out the Machine(s) and User(s) at the top of the alert.      * + 1. If needed, in the **Details** pane to the right, click to expand the **Alert details**.     2. Point out **Alert description** within the **Alert details**.     3. Scroll down to the **Alert story**.      * + 1. In the **Alert story**, point out the item **schtasks.exe**.     2. In the **Alert story**, point out the item **WinATP-Intro-backdoor.exe**.     3. At the top of the page toggle the **New alert experience** to the **off** position.     4. Scroll down in the Alert process tree, and click the file **WinATP-Intro-Backdoor.exe** to launch the **File Investigation**. |

## MDATP File Investigation

|  |  |
| --- | --- |
| **What to say** | **What to show** |
| Our SecOps user can investigate the details of a file associated with a specific alert, behaviour, or event to help determine if the file exhibits malicious activities, identify the attack motivation, and understand the potential scope of the breach.  To enrich the data related to the file, SecOps can submit the file for **deep analysis**.  The deep analysis feature executes a file in a secure, fully instrumented cloud environment. Deep analysis results show the file's activities, observed behaviours, and associated artifacts, such as dropped files, registry modifications, and communication with IPs.  Here SecOps can see that the suspect file makes a system file ‘talk’ with an external IP address.  The **Observed in the organization** section provides details on the name of the file as it is observed in the organization, and its prevalence in specific user machines. | **Note:** [Here is a link](https://securitycenter.windows.com/files/daa3d1f83a37ca3f8b818f949becd4948f3c5f52;name=WinATP-Intro-Backdoor.exe/deep_analysis) to a recent file investigation page.   1. At the top of the **File overview** page, on the far right, note the **File** **prevalence** details. 2. Click the **Deep analysis** tab. 3. Click a **Deep analysis summary** to expand.   **Note:** If a Deep analysis summary is not available, click **Submit** next to **Deep analysis request**. Deep Analysis Summary will typically be available within 10 minutes.     1. In the **Deep analysis** tab, under **Behaviors**, click **Communication** to expand. 2. Click **A system file communicates with an external IP address** to expand. 3. Note the IP addresses in the **Target** column. 4. In the left-hand navigation bar, click the **Machines list.**(PC icon) |

## MDATP File-less Attack Investigation

|  |  |
| --- | --- |
| **What to say** | **What to show** |
| Attackers need not inject a physical file in a victim’s machine to take control – attacks can happen through scripts.  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 automated investigation, Microsoft Defender ATP identified the notepad.exe process, which was injected into, as one of the artifacts requiring remediation.  By default, Microsoft Defender ATP will wait for the SecOps approval before proceeding, but they could also configure it under the machine group settings to skip this step and apply remediation automatically. | * + 1. Select the **andrewf-pc** machine name.      * + 1. Within the machine page, click the **Alerts** tab.      * + 1. Click the alert title, **Suspicious process injection observed**.   **Note:** Here is a direct link to a [recent alert](https://securitycenter.microsoft.com/alerts/da637229366612137916_-1203295796/details).     * + 1. Point out the **Alert Details**.     2. Point out the sequence of events in the **Alert story**     3. Return to the Alert Details pane of the page and locate the **Automated investigation details**.     4. Click the **ID:** [**Suspicious process injection observed**](https://securitycenter.microsoft.com/investigation/589)     **Note:** The alert investigation page remains in an active state for up to 7 days. If you visit the page after this time has elapsed, the alert will be auto remediated. You can go back and find another alert that is still pending     * + 1. Note the investigation graph and the list of known threats found in the attack.     2. If available: click the **Actions** tab and note the **Quarantine file** actions recommended by MDATP. |

## MDATP Machine Investigation & Analyzing Email Threats with Office 365 Threat Intelligence

|  |  |
| --- | --- |
| **What to say** | **What to show** |
| Here the SecOps user is going to take a closer look at a machine with an alert.  The machine view page provides SecOps with an overview of security-relevant details such as logged on users, high-level machine status and risk profile.  Here they can also see that the Microsoft Defender Security Center supports multiple endpoint types Including Windows Server 2019, Linux Machines, as well as Apple clients running macOS.  **Clicking into a machine**  SecOps is also able to see a summary of all relevant alerts related to this machine.  Additionally, they can view a rich and detailed timeline that shows all events observed from this machine, back as far as 6 months. Additionally, they can interactively hunt, search and explore historical data across all the endpoints.  SecOps can reduce the verbosity by using search or filter functionality.  Drilling in, the detailed view of the alert shows the SecOps team what services were involved in the alert, as well as what files are affected.  Here SecOps can see that the malware in question was introduced via an email, and with the deep integration with Office ATP we can also get more details on who else in the organization received this mail, including **Delivery Actions** (Delivered, Delivered to Junk, or Blocked) as well as the **Delivery Location** (Inbox, Junk, or Quarantine).  The SecOps user then heads back to the Microsoft Defender portal, to take a look at the organization's threat analytics. | * + 1. Navigate to the **Machines list**   A screenshot of a computer screen  Description automatically generated   * + 1. Click the machine named **lolas-pc**.   A screenshot of a computer  Description automatically generated   * + 1. On the machine info page, point to the machine metadata located on the left-hand side.     2. Click the **Alerts** tab. Note the “New” and “Resolved” alerts under Status.   A screenshot of a computer screen  Description automatically generated   * + 1. Click the **Timeline** tab.   A screenshot of a computer screen  Description automatically generated   * + 1. On the right, click **Filters** (Show filters) to show the **Filters** pane if not already showing.     2. Under **Event group**, check **File events**.     3. Click **Apply**.     4. Click **Search events** and type the phrase,.**doc** then press <Enter>.     5. Locate and click on an Event labelled **WINWORD.EXE created file <HASH>.docm**.   (Example: WINWORD.EXE modified 8ABF035E.docm)  A screenshot of a computer screen  Description automatically generated   * + 1. On the task pane, click on the file name label, **<HASH>.doc**. (Example: 8ABF035E.docm)   A screenshot of a computer screen  Description automatically generated   * + 1. Click the **Open File page**.   A screenshot of a computer screen  Description automatically generated   * + 1. Under **File prevalence**, note the occurrence of this file elsewhere in the organization, including **Email inboxes**.   A screenshot of a cell phone  Description automatically generated   * + 1. Under **Email inboxes**, Click **Open in Office 365**.   A screenshot of a computer  Description automatically generated   * + 1. In the Office 365 Security & Compliance report, scroll down to the bottom of the list of Email tab,     2. Point Out: **Delivery action** and **Delivery location** columns.     3. Click the browsers **Back** button to return to the MDATP portal. |

## MDATP Threat Analytics

|  |  |
| --- | --- |
| **What to say** | **What to show** |
| **View the threat analytics dashboard**  Cyberthreats are emerging more frequently and prevalently. It is critical for organizations to quickly assess their security posture, covering the impact of emerging threats and their organizational resilience.  Threat analytics is a set of reports published by Microsoft security researchers as soon as emerging threats and outbreaks are identified. The reports help the SecOps team assess the impact of threats to the environment and identify actions that can contain them.  The threat analytics dashboard is a great jump-off point for getting to the reports that are most relevant to the organization. It provides several overviews about the threats covered in the reports:   * Latest threats — lists the most recently published threat reports, along with the number of machines with resolved and unresolved alerts. * High-impact threats — lists the threats that have had the highest impact on the organization in terms of the number of machines that have had related alerts, along with the number of machines with resolved and unresolved alerts. * Threat summary — shows the number of threats among the threats reported in threat analytics with actual alerts.   **View a threat analytics report**  Each threat report generally provides an overview of the threat and an analysis of the techniques and tools used by the threat. It also provides worldwide impact information, mitigation recommendations, and detection information. It includes several cards that show dynamic data about how the organization is impacted by the threat and how prepared it is to stop the threat.  **Organizational impact**  Each report includes cards designed to provide information about the organizational impact of a threat:   * Machines with alerts — shows the current number of distinct machines in the organization that have been impacted by the threat. A machine is categorized as **Active** if there is at least 1 alert associated with that threat and **Resolved** if all alerts associated with the threat on the machine have been resolved. * Machines with alerts over time — shows the number of distinct machines with Active and Resolved alerts over time. The number of resolved alerts indicates how quickly the organization responds to alerts associated with a threat. Ideally, the chart should be showing alerts resolved within a few days.   **Organizational resilience**  Each report also includes cards that provide an overview of how resilient the organization can be against a given threat:   * Mitigation status — shows the number of machines that have and have not applied mitigations for the threat. Machines are considered mitigated if they have all the measurable mitigations in place. * Vulnerability patching status — shows the number of machines that have applied security updates or patches that address vulnerabilities exploited by the threat. * Mitigation recommendations — lists specific actionable recommendations to improve SecOps visibility into the threat and increase the organizational resilience. This card lists only measurable mitigations along with the number of machines that don't have these mitigations in place. | * + 1. In the left navigation menu of MDATP, click **Dashboards**, select **Threat analytics**.     2. Click on an item under **High-impact threats,** e.g. **Living-off-the-land binaries**.     3. Note the **Overview** writeup and the organizational impact report on the right side. |

## MDATP Threat & Vulnerability Management (TVM)

|  |  |
| --- | --- |
| **What to say** | **What to show** |
| Section 1: Review the TVM dashboard The **Threat & Vulnerability Management (TVM**) component of Microsoft Defender ATP provides real-time endpoint vulnerabilities and misconfigurations assessment for both OS and third-party software, prioritized by and correlated with external threat landscape insights, internal threat insights (EDR context) and business context.  TVM also includes the ability to create remediation and mitigation requests and monitor their progress in real-time, bridging the gap between Security Admins and IT. Here in the MDATP TVM Dashboard, populated with several key overviews, the following data provided helps enable the SecOps user:   * + - * **Exposure Score** - Reflects the current exposure associated with machines in the organization. Reduce the exposure score by addressing what needs to be remediated based on the prioritized security recommendations.       * **Configuration Score** - Reflects the collective security configuration posture of all the organizational machines across OS, Application, Network, Accounts and Security Controls. Increase the configuration score by addressing what needs to be remediated based on the prioritized security recommendations.   Configuration Score serves as the **Microsoft Secure Score** for Devices. This score and its related configuration assessments comprise the Device pillar in Microsoft Secure Score.   * + - * **Exposure Distribution** – Reflects the exposure level distribution of machines in the organization.       * **Top Security Recommendations** – The top security recommendations for organizations prioritized based on the dynamic threat landscape factors, breach likelihood and business context (machine value). Useful icons with hover tooltip context also quickly call attention to possible active alerts Possible active alert, associated threats and public exploits Threat insight, and recommendation insights Recommendation insight.       * **Top Vulnerable Software** - Real-time visibility into the organizational software inventory, with a stack-ranked list of vulnerable software installed on an organizations network’s devices and how they impact your organizational exposure score.       * **Top Exposed Machines** - See the exposed machine names and their exposure level. The SecOps team can click each machine name from the list and it will take your Secops User to the machine page, where They can view TVM context for the exposed machine - security recommendations, installed software, discovered vulnerabilities and missing KBs. *l*       * **Remediation Activities** - Track the remediation activities generated from the security recommendations. | * + 1. In the left navigation menu of MDATP, select **Threat & Vulnerability Management**, then **Dashboard**.     2. Scroll down the page, noting the following scores and charts:        - **Exposure score**        - **Microsoft Secure Score for Devices**        - **Machine exposure distribution**        - **Top security recommendations**        - **Top vulnerable software**        - **Top exposed machines**        - **Remediation activities** |
| Section 2: Reviewing Security recommendations Diving into security recommendations, The SecOps user can see that MDATP is providing a list of actionable recommendations to improve the vulnerability posture of the organization, both in relation to software vulnerabilities as well as endpoint misconfigurations.  This page contains a dynamic prioritized list of security recommendations for the entire organization across all operating systems and software.  These recommendations are prioritized based on the potential exposure improvement impact that applying them would generate, to help security admins focus on the vulnerabilities that are currently posing the highest exposure risk.  By clicking on a recommendation, SecOps can view further details about the recommendation (exposed machines, related CVEs, etc.).  This capability also includes integration with MDATP Threat Analytics, where threats covered in TA are linked to vulnerabilities discovered by TVM – clicking on a threat link will open the related Threat Analytics report. | * + 1. In the left navigation menu under **Threat & Vulnerability Management**, click **Security recommendations**.     2. Locate the recommendation **Update Rarlab Winrar to version X.Y.Z**.   **Note**: The recommendation version will change as new versions come out.     * + 1. Hover over the bug icon (Threat insight) in the Threats column and note the exploits/threats related to this recommendation, affecting its prioritization.      * + 1. Click on the recommendation row to open the **recommendation details** side pane.     2. Point out the various fields in the pane, including the lists (Exposed machines, CVEs addressed, etc.). Note: Each of these lists can be exported to a CSV.        - *Optional #1 – expand the* ***Exposed machines*** *list to show the ability to view the list of specific machines.*        - *Optional #2 – expand the* ***CVEs address*** *list to show the ability to view the list of vulnerabilities that machines are currently exposed to due to this software. Clicking on a CVE will open a side pane with CVE details.*   **Note**: The security recommendation pane also includes a button that opens the related software page – the software page scenario is described in section 5 below. |
| Section 3: Submitting a Remediation request or creating an Exception To complement the scenario described in Section 2 (“Reviewing security recommendations”), the next step after reviewing a recommendation is to apply the mitigation.  There are two types of mitigating actions that can be taken:   1. Creating a remediation request – this is the primary mitigation option for a security recommendation. 2. Creating an exception – in some cases, it is not possible to apply the primary remediation, and security admins can choose to create an exception instead. | * + 1. Click the **Remediation options** button at the top of the Security recommendation pane to open the remediation request side pane.      * + 1. Point out **Remediation options** - This provides the ability to create a remediation activity in TVM and monitor its progress, as well as open a remediation task in InTune.     2. Point out **Exemption options** Security admins can choose to create an exception instead. |
| Section 4: Monitoring remediation activities and exceptions This area of Threat & Vulnerability Management (TVM) provides the ability to view, monitor and manage the progress/status of remediation requests and exceptions that were created in the organization.  The remediation progress is a real-time reflection of the endpoint patch state that is continuously assessed by the MDATP sensor.  The SecOps user can view activities that are currently active/in progress, as well as expired and completed activities. | * + 1. In the left navigation menu under **Threat & Vulnerability Management**, click **Remediation**.     2. In the **Remediation activities** tab, click the **Update Winrar to version 5.71.0.0** activity.     3. Point out the various fields.     4. Point out but do not click the **Mark as completed** and **Export to CSV** buttons.     5. Click the **Exceptions** tab at the top of the page.     6. Click an existing exception.     7. Point out the fields.     8. **Point out** but do not click the ability to cancel an existing exception. |
| Section 5: Reviewing Software inventory and Software page The Software Inventory area of Threat & Vulnerability Management (TVM) provides visibility into all the 1st and 3rd party software installed across all devices in the organization.  This page provides a list of all the 1st and 3rd party applications that were discovered by TVM across all devices in the org, ranked based on the level of vulnerability/exposure that each software product is currently introducing into the organization.  Also, the SecOps user can drill down into any of the software products listed in the software inventory for a detailed full overview of this software and its related TVM information – security recommendations, exposed machines, related vulnerabilities, version distribution, missing security updates (KBs), and more.  This page provides all available information related to the vulnerabilities that software is introducing into the organization, their exposure impact and related security recommendations. | * + 1. In the left navigation menu under **Threat & Vulnerability Management**, click **Software inventory**.     2. Point out the table columns.     3. Hover over the bug icon (Threat insight) in the Threats column for either **WinRAR** or **Windows 10** and note the exploits/threats related to this software, affecting its exposure impact on the organization.     4. Open the **Windows 10** software page by doing one of the following:        - Click the **Windows 10** text in the **Name** column of the inventory table.        - Click the **Windows 10** row to open the software side pane, then click the **Open software page** button at the top of the pane.     5. Point out the general information related to the software on the left-hand area of the page, and the summarized data at the top (discovered vulnerabilities and misconfigurations).     6. Click the tabs at the middle of the page and point out the important data provided there:        - **Security recommendations** tab – A list of all security recommendations related to this software across all machines in the org. Click any recommendation to view additional information.        - **Discovered vulnerabilities** tab – A list of all vulnerabilities (CVEs) that exist for this software across all machines in the org. Click any vulnerability to view additional information.        - **Installed machines** tab – A list of all machines that have this software installed.        - **Version distribution** tab – A distribution list of all versions of this software installed on machines in the organization. Click any vulnerability to view additional information.        - **Missing KBs** tab – A list of all missed security updates (KBs) for this software. Click any KB item to view additional information |
| Section 6: Machine page The machine page in MDATP has been enriched with Threat & Vulnerability Management (TVM) data, providing full vulnerability context for the machine entity – security recommendations, software vulnerabilities, software inventory, missing security updates (KBs) and overall exposure level.  This enrichment serves both the SecOps, as well as SecOps, who can now easily see any gaps in a machine's defenses while investigating an alert and gain insights into possible weaknesses that were exploited by an attacker. | * + 1. In the left navigation menu under **Threat & Vulnerability Management**, click **Dashboard**.     2. Scroll down to the **Top exposed machines** list and click the following PC name: **deborahp-pc**.   **Note**: The list is dynamic, you may need to expand the list by clicking **Show more**.   * + 1. In the **Overview** tab, point out the Security assessment summary.     2. **Point out** the TVM tabs to show the TVM context that now exist in the machine page:      * + - * **Security recommendations** tab – A list of all TVM security recommendations related to this machine. If available, you can click any recommendation to view additional information.       * **Software inventory** tab – A list of all software products identified on this machine, including vulnerability related information. If available, you can click any software to view additional information.       * **Discovered vulnerabilities** tab – A list of all vulnerabilities (CVEs) discovered on this machine. If available, you can click any vulnerability to view additional information.       * **Missing KBs** tab – A list of all missed security updates (KBs) on this machine. If available, you can click any KB item to view additional information. |
| Section 7: Weaknesses page The **Weaknesses** page is essentially a knowledge base listing all the vulnerabilities (CVEs) that are known to TVM – both CVEs that apply to your organization at this time, as well as those that aren’t. The SecOps team is interested to understand how exposed the organization is to a specific CVE – so this is the place to review it.  For each vulnerability, the SecOps user can view the severity using the **Common Vulnerability Scoring System (CVSS)** rating. This includes the **Vulnerability description** for the CVE. As well as its prevalence within the organization, any related software, or a corresponding breach.  The SecOps user can also review the **Vulnerability details** which include detailed information on severity, age, and any known related software.  The SecOps team has access to detailed **Threat insights**, which includes Information relating to the threat landscape for this vulnerability, such as public exploits, exploit kits.  Also, with endpoint management – you have detailed data as an exportable list on any **Exposed machines** exposed to this vulnerability from within the organization. | * + 1. In the left navigation menu under **Threat & Vulnerability Management**, click **Weaknesses**.     2. Point out the fields shown for each vulnerability.   *Optional – identify a vulnerability where the bug icon (*Threat insight*) is lit up and hover over it, note the exploits/threats related to this vulnerability, affecting its exposure impact on the organization.*   * + 1. Click one of the CVEs to open the vulnerability side pane.     2. Point out the various sections in the side panel:        - **Vulnerability description** –        - **Vulnerability details**      * + - * **Threat insights**      * + - * **Exposed machines** |
| Section 8: Advanced Hunting for Threat Vulnerabilities The SecOps team can take advantage of the advanced hunting capabilities on MDATP with TVM.  Here they have a saved query for identifying machines that have an active High Alert status for software threat vulnerabilities.  They are then able to run this query to see what machines in the environment need remediation.  The results are not great for the Operations Team. There are quite a few machines that need some attention.  The SecOps user then goes ahead and sees what they can do with one of these alerts.  On this Alert window, they can see how this vulnerability in software has allowed for some malicious activity.  Under actions, the SecOps user has the option to consult a **Microsoft Threat Expert.** If they choose to submit a request, a Microsoft expert would review the alert and give detailed recommended actions. | * + 1. In the Microsoft Defender Security Center’s left navigation, select **Advanced Hunting**.     2. Under **Shared Queries**, expand **TVM**, then click **Vulnerable machine with alerts**.     3. Click **Run query**.   **Scenario 1**   * + 1. From the list of results, click on an **Alert ID**.     2. Under **Actions**, **point out** but do not click **Consult a threat expert**. |
| Section 9: Global TVM search Threat & Vulnerability Management (TVM) data is also reachable via the global search option of MDATP by choosing one of the following TVM entities:   * Vulnerability * Software * Recommendation   The TVM Software Inventory page will open showing a filtered view of related software products. | * + 1. In the global search, click the drop-down box and choose **Software**.      * + 1. In the search box, type: **Adobe** and press **Enter**. |
| Section 10: Machine group filtered TVM context All Threat & Vulnerability Management (TVM) pages can be viewed in the context of specific machine groups – this provides the ability to understand your vulnerabilities and exposure for different parts of the organization.  The machine group filter remains persistent when moving across and drill downing through different TVM pages. | * + 1. From the top of any page in the TVM section, click the **Selected machine groups** icon to open the selector side pane.      * + 1. Choose the **Semi-Auto** machine group and click **Apply**.     2. Point out that all TVM views will now change to reflect only this specific machine group.     3. To return to full organizational view, open the selector side pane again and choose the **Any** option. |

## MDATP Live Response

|  |  |
| --- | --- |
| **Talk Track** | **Click Steps** |
| The live response is a capability that gives instant access to a machine using a remote  shell connection. It gives the power to do in-depth investigative work and take immediate response actions to promptly contain identified threats – real-time.  The live response is designed to enhance investigations by enabling the SecOps user to quickly collect forensic data, run scripts, send suspicious entities for analysis, remediate threats, and proactively hunt for emerging threats.  While this example walks through investigation and remediation of a benign file (notepad.exe), SecOps users can use the Live Response tool to scan, analyze and act on any file or process running on the organization’s endpoints. | * + 1. In the left navigation of Microsoft Defender ATP, click **Machines list**.     2. Select a compromised machine (where Risk Level is **High** or **Medium**) to open the machine page. E.g. **lolas-pc.**     3. Click **Initiate Live Response Session**, found under the **Ellipsis** in the upper right.     4. In the **Command console**, type **help** and press **<Enter>**.     5. Locate suspicious files using **findfile** command, e.g. **findfile notepad.exe <Enter>**.     6. Run the remediate command on the file, e.g.  **remediate file** **C:\Windows\notepad.exe" -auto**.     7. Click the **Command log** tab at top of the page.     8. Point to the log of commands executed in the Command console session.     9. In the MDATP left navigation, expand **Automated investigations**, then choose **Action center**.     10. Go to the **History** tab.     11. Select the **Quarantine file** action at the top of the list.     12. Note the **Undo** action at the top of the pop-up pane. |
| Get a mini memory dump using a PowerShell script Before running a PowerShell script, first upload it to the library. If planning to use an unsigned script in the session, enable the setting in the Advanced features settings. | * + 1. Copy/paste the following PowerShell script snippet to a text editor:   $process\_arg=$args[0]    function MiniDumpWriteDump  {  [CmdletBinding()]  Param (  [Parameter(Position = 0, Mandatory = $True, ValueFromPipeline = $True)]  [System.Diagnostics.Process]  $Process  )  BEGIN  {  $WER = [PSObject].Assembly.GetType('System.Management.Automation.WindowsErrorReporting')  $WERNativeMethods = $WER.GetNestedType('NativeMethods', 'NonPublic')  $Flags = [Reflection.BindingFlags] 'NonPublic, Static'  $MiniDumpWriteDump = $WERNativeMethods.GetMethod('MiniDumpWriteDump', $Flags)  $MiniDumpWithFullMemory = [UInt32] 2  }  PROCESS  {  # get the process dump  $ProcessId = $Process.Id  $ProcessName = $Process.Name  $ProcessHandle = $Process.Handle  $ProcessFileName = "$($ProcessName)\_$($ProcessId).dmp"  $ProcessDumpPath = $env:TEMP + "\$([IO.Path]::GetRandomFileName())\_" + $ProcessFileName  $FileStream = New-Object IO.FileStream($ProcessDumpPath, [IO.FileMode]::Create)  $Result = $MiniDumpWriteDump.Invoke($null, @($ProcessHandle, $ProcessId, $FileStream.SafeFileHandle, $MiniDumpWithFullMemory, [IntPtr]::Zero, [IntPtr]::Zero, [IntPtr]::Zero))  $FileStream.Close()    if (-not $Result)  {  # Remove any partially written dump files. For example, a partial dump will be written  # in the case when 32-bit PowerShell tries to dump a 64-bit process.  $Exception = New-Object ComponentModel.Win32Exception  $ExceptionMessage = "$($Exception.Message) ($($ProcessName):$($ProcessId))"  Remove-Item $ProcessDumpPath -ErrorAction SilentlyContinue  throw $ExceptionMessage  }  # Compress to ZIP  $OutputFilePathZip = "$($ProcessDumpPath).zip"  Compress-Archive -Path $ProcessDumpPath -DestinationPath $OutputFilePathZip  Remove-Item -Path $ProcessDumpPath -ErrorAction SilentlyContinue    # write path to file and size  Write $OutputFilePathZip  Write "$([int]((Get-Item $OutputFilePathZip).length / 1024 / 1024)) MB"  }  END {}  }  try {  # by pid  $process\_id = [convert]::ToInt32($process\_arg, 10)  Get-Process -Id $process\_id | MiniDumpWriteDump  }  catch {  # by name  Get-Process $process\_arg | MiniDumpWriteDump  }   * + 1. Save the script file as a PowerShell, e.g. **Get-MiniDump.ps1**.     2. In the MDATP Live Response dashboard page, click **Upload file to library**, then point to the **Get-MiniDump.ps1** file to upload it. (ensure that the **Overwrite File** option is **selected**.)     3. In the Live Response Command console, type **library** and **<Enter>** to see the list of available scripts.     4. Execute the PowerShell script uploaded using the following console command: **run Get-MiniDump.ps1**   The file is saved in C:\WINDOWS\TEMP as the following file name format:  <Machine Name>-<Date ran the Mini-Dump>-<Random 4-digit number.log   * + 1. Navigate to the Windows\Temp folder by entering the following command:   **cd c:\windows\temp**   * + 1. List the contents of that directory, to locate the mini-dump by entering the following command:   **dir**   * + 1. Run the following command to enable the Mini-Dump for download   fileinfo c:\windows\temp\<Machine Name>-<Date you ran the Mini-Dump>-<Random 4 digit number>.log   * + 1. Download the recently created “mini memory dump” by typing: **download** <Machine Name>-<Date you ran the Mini-Dump>-<Random 4 digit number>.log   **NOTE:** After a few seconds, you should see the file being downloaded in your browser. Depending on your browser settings, it allows you to save the file automatically or asks where you’d like to save the file for further analysis. |
| Use forensic tools to gather forensic information This section will demonstrate how to use third-party forensic tools to gather forensic information from an endpoint machine. In this example, the SecOps user will demonstrate how to dump a Master File Table (MFT) using the NTFSInfo applet from Sysinternals.  Master file tables are file tracking systems that are used in the function of a Windows NT filing system. Considered to be an important part of the metadata files, they help to define the volume of an NTFS volume. Often referred to as the MFT, the table houses information about every file and directory that is found in the file system.  Now that the SecOps user has demonstrated how to initiate a live response session and perform basic remediation, get a mini memory dump using a PowerShell script, and use forensic tools such as Sysinternals to acquire forensic information on a machine.  This tutorial emphasizes the typical scenarios and commands that would be useful when an in-depth investigation and remediation is needed on a compromised device. | * + 1. Perform the following pre-demo steps on your local PC:        1. Download **NTFSInfo** from the [NTFSInfo](https://docs.microsoft.com/en-us/sysinternals/downloads/ntfsinfo) page.        2. Extract contents of the downloaded zip file locally.        3. **Upload** the content (**ntfsinfo64.exe**) to the machine’s Live Response **library**, as detailed in the previous section.        4. In Notepad. Copy and paste the following script:   .**\ntfsinfo64.exe /accepteula c:\**   * + - 1. Save the script file as **MFTdump.ps1**.       2. **Upload** this file to the machine’s Live Response **library**, as detailed in the previous section.       3. In the Live Response console, type **library** and **<Enter>** to verify the newly added files exist in the machine.     1. Type **putfile ntfsinfo64.exe -overwrite.** This command will download the file from the live response library to the "C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\Downloads\" local machine directory on the machine you are connected to.     2. Type **run MFTdump.ps**1 in the live response CLI. This command will run the PowerShell script on the machine.     3. The MFT dump will be created in the C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\Temp\PSScriptOutputs\ directory.   The output file is detailed as below:     * + 1. Navigate to the C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\Temp\PSScriptOutputs\ directory by entering the following commands:   **cd C:\ProgramData\Microsoft\**  **cd “Windows Defender Advanced Threat Protection”**  **cd Temp\PSScriptOutputs\**   * + 1. List the contents of that directory, to locate your MFTdump by entering the following command:   **dir**   * + 1. Run the following command to enable the MFTDump for download:   **fileinfo PSScript\_Transcript\_{Random GUID Value}.txt**   * + 1. Type **download PSScript\_Transcript\_{Random GUID Value}.txt** in Live response CLI window and a few seconds you will be asked to download the file. |

## MDATP Power BI reports

|  |  |
| --- | --- |
| **Using the Advanced Hunting API Connected to Power BI for Advanced Reports**  In this section, will be reviewing a few Power BI reports built using data collected by Microsoft Defender ATP services and exposed through MDATP APIs.  Typical enterprise security operation teams often rely on dependable reporting visualizations to make critical security decisions. While Microsoft Defender ATP provides extensive visibility on the security posture of your organization through built-in dashboards, custom reporting can help turn security data from multiple sources into insights to meet your analytical needs.  Power BI is a business analytics service that delivers insights to enable fast, informed decisions.  The first example demonstrates how Power BI can be leveraged to visualize the power of the MDATP Advanced Hunting API and the second example demonstrates a connection to OData APIs to visually showcase Machine Actions.  Here in the PowerBI home page, there is a dashboard pinned that contains some of our MDATP reporting data. SecOps digs into this data, by clicking into the **MDATP Reporting Group** workspace where reports are hosted.  Inside this Workspace, the SecOps user can see we have a pinned Dashboard where the data is easily accessible. Diving into this dashboard to check out the data.  Here in the MDATP dashboard, SecOps can see we have two reports being shown. The first one as we mentioned earlier, is the PowerBI Report that is leveraging the MDATP Advanced Hunting API, they then can take a closer look at this report by clicking the **Events Report**.  Here in this report, SecOps can see the Advanced Hunting Query they used to generate the report, in this case, it is polling anytime MDATP Action contained AntiVirus. As they can see in the example, the environment is quite busy. This report is a great way for the SecOps user to quickly determine if there is a rise in activity, and which machines are most impacted.  This report can be shared, exported, and even subscribed to as a feed, so the SecOps team can get this report directly into their inbox as part of the daily routine.  The SecOps user is then going to head back to the PowerBI Dashboard and take a look at that second report that uses the MDATP OData APIs to visually showcase Machine Actions.  Here in the Machine actions, the SecOps user can see what actions, both manually initiated as well as automatically initiated have been performed within the environment. It has a breakdown of these actions per machine so they can see which machines are most ‘active’, which can aid the SecOps user in identifying if there are machines that may be compromised. Here in this example, they can see that there is one active machine. This would lend to the probability that this machine has been compromised.  Like the other report, this report can also be shared, exported, and even subscribed to as a feed, so the SecOps team can get this report directly to their inbox as part of the SecOps daily routine.  Both Reports here have been configured to auto-refresh the data daily, so these reports are always up to date, allowing the SecOps user to be proactive. | 1. Open a new tab in the web browser, and navigate to <https://app.powerbi.com/>    1. If prompted use the [SecOps@mtpdemos.net](mailto:SecOps@mtpdemos.net) user to login. 2. Once in Power BI, expand **Workspaces**, then select the **MDATP Reporting Group**.      1. Click **MDATP Dashboard**.      1. Click the **Events** (bar graph) report.      1. Point out:    1. The **Advanced Hunting Query sample used**.    2. **Share**.    3. **Export**.    4. **Subscribe**. 2. Click the **MDATP Reporting…** breadcrumb at the top of the page to return to the MDATP Reporting workspace.      1. Click **MDATP Dashboard**.      1. Click **Action Count** (Pie Chart).      1. Point out:    1. The **Advanced Hunting Query sample used**.    2. **Share**.    3. **Export**.    4. **Subscribe**. 2. Point out:    1. **Data updated** date at the top center of the page. |

## Conclusion

|  |  |
| --- | --- |
| **Talk Track** | **Click Steps** |
| Microsoft Defender Advanced Threat Protection is a platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.  With Microsoft Threat Protection, Microsoft Defender ATP and various Microsoft security solutions form a unified pre- and post-breach enterprise defense suite that natively integrates across endpoint, identity, email, and applications to detect, prevent, investigate and automatically respond to sophisticated attacks. |  |

## [Optional] Building MDATP Power BI reports

**Additional Note:** For the **Optional** section below, you will need to use your own demo environment configured and equipped with the following:

A **Windows 10** (Build 1903 or greater) **endpoint** with [**PowerBI Desktop**](https://www.microsoft.com/en-us/download/confirmation.aspx?id=58494&6B49FDFB-8E5B-4B07-BC31-15695C5A2143=1) **client** app installed which is **MDATP On-Boarded** as well as **Azure AD joined** to an **MDATP enabled tenant MDATP enabled tenant** with some **pre-populated device and user activity**.

| **What to say** | **What to show** |
| --- | --- |
| **Connect Power BI to Advanced Hunting API**  In this section, you will learn to create a Power BI report on top of Microsoft Defender ATP APIs.  Typical enterprise security operation teams often rely on dependable reporting visualizations to make critical security decisions. While Microsoft Defender ATP provides extensive visibility on the security posture of the organization through built-in dashboards, custom reporting can help turn security data from multiple sources into insights to meet analytical needs.  Power BI is a business analytics service that delivers insights to enable fast, informed decisions.  The first example demonstrates how to connect Power BI to Advanced Hunting API and the second example demonstrates a connection to OData APIs (e.g. Machine Actions, Alerts, etc..)  Now the results of the query will appear as a table and start to build visualizations on top of it!  You can duplicate this table, rename it and edit the Advanced Hunting query inside to get any data you would like. | 1. Log in to the Windows 10 endpoint PC configured as noted above. 2. In the PC, download and unzip [this sample Power BI report](https://github.com/microsoft/MicrosoftDefenderATP-PowerBI/releases/download/100616/MDATP_PowerBI_reports.zip) provided. 3. Launch the **Microsoft Power BI** desktop app. 4. If prompted, sign in to Power BI service as an administrative user in your tenant who has a Power BI license. 5. Close the **Open File** dialogue. 6. Click **Get Data** > **Blank Query**.      1. Click **Advanced Editor**.   .   1. **Copy** the below and **paste** it in the editor:   let  AdvancedHuntingQuery = "MiscEvents | where ActionType contains 'Anti'",  HuntingUrl = "https://api.securitycenter.windows.com/api/advancedqueries",  Response = Json.Document(Web.Contents(HuntingUrl, [Query=[key=AdvancedHuntingQuery]])),  TypeMap = #table(  { "Type", "PowerBiType" },  {  { "Double", Double.Type },  { "Int64", Int64.Type },  { "Int32", Int32.Type },  { "Int16", Int16.Type },  { "UInt64", Number.Type },  { "UInt32", Number.Type },  { "UInt16", Number.Type },  { "Byte", Byte.Type },  { "Single", Single.Type },  { "Decimal", Decimal.Type },  { "TimeSpan", Duration.Type },  { "DateTime", DateTimeZone.Type },  { "String", Text.Type },  { "Boolean", Logical.Type },  { "SByte", Logical.Type },  { "Guid", Text.Type }  }),  Schema = Table.FromRecords(Response[Schema]),  TypedSchema = Table.Join(Table.SelectColumns(Schema, {"Name", "Type"}), {"Type"}, TypeMap , {"Type"}),  Results = Response[Results],  Rows = Table.FromRecords(Results, Schema[Name]),  Table = Table.TransformColumnTypes(Rows, Table.ToList(TypedSchema, (c) => {c{0}, c{2}}))  in Table   1. Click **Done.** 2. Click **Edit Credentials.**      1. Select **Organizational account** > **Sign in.**      1. Enter your credentials and wait to be signed in. 2. Click **Connect.** |
| **Connect Power BI to OData APIs**  The only difference from the above example is the query inside the editor.  You also can use OData queries for queries filters, see [Using OData Queries](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/exposed-apis-odata-samples) | **Pre-demo Steps:**   * Download and save the following [sample reports](https://github.com/microsoft/MicrosoftDefenderATP-PowerBI/releases/download/100616/MDATP_PowerBI_reports.zip) on your demo endpoint machine with Power BI. * Setup the API´s in your tenant for connectivity <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/apis-intro>   + 1. Copy the below and paste it in the editor to pull all Machine Actions from your organization:   let  Query = "**MachineActions**",  Source = OData.Feed("https://api.securitycenter.windows.com/api/" & Query, null, [Implementation="2.0", MoreColumns=true])  in  Source   * + 1. Now update the Query for **Alerts**.     2. Once you have your results, update the Query again for **Machines**.     3. Once complete, **LOG OUT** from your remote desktop session. (Do NOT simply disconnect.) |

## Reset Instructions

**NOTE:** If you made no modifications to the demo environment during the demo, there are no reset steps.

1. If you did create any of the following during the demo, please remove/delete them so the shared environment is clean for the next demo user:

* Custom detection rule
* Live Response script