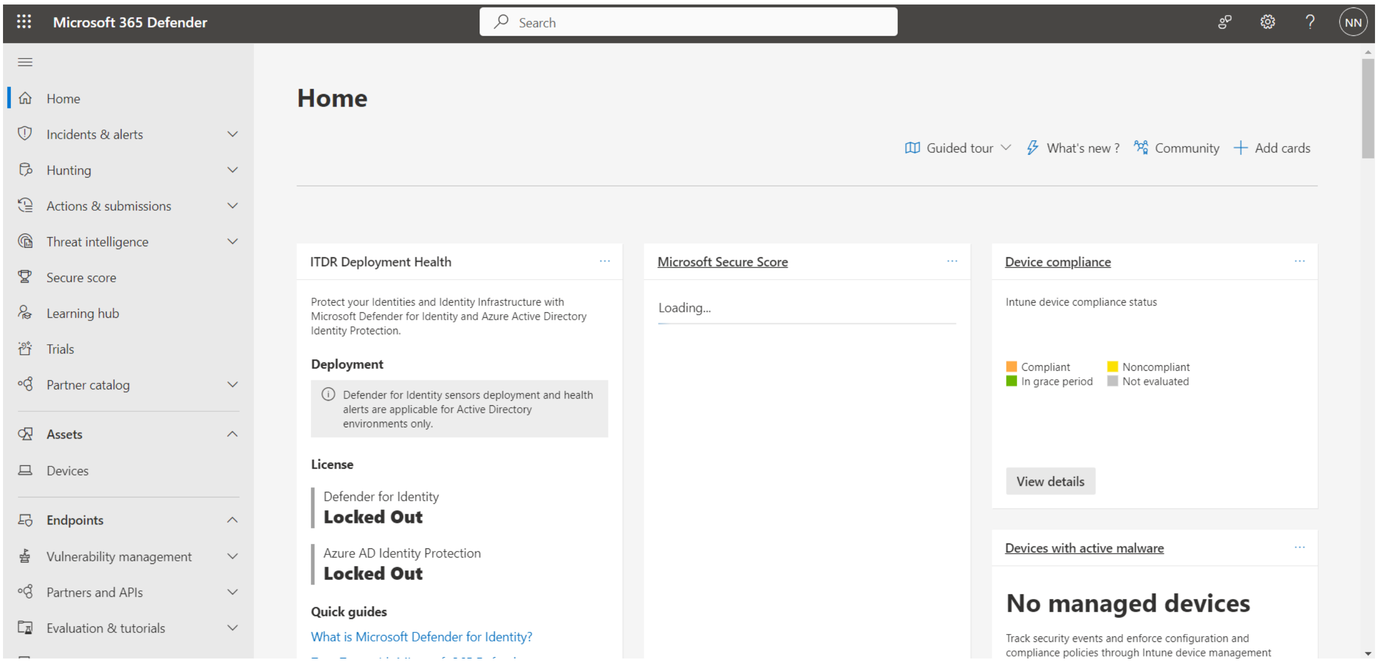
Microsoft 365 Defender

By

N Nithish

Introduction

Microsoft 365 Defender is an EDR Tool to maintain security in the devices and also help to prevent insider hackers from attacking the organization it will work on integrating with Microsoft Defender antivirus which will be present in every Windows OS and windows server. The are a lot of features and processes for deploying the package we will call deploying of package device onboarding where we will try to install the package in the client system now, we will see all things in detail as we can see in the below picture its home page of Microsoft



Home

ITDR Deployment Health

Protect your Identities and Identity Infrastructure with Microsoft Defender for Identity and Azure Active Directory Identity Protection.

Deployment

Defender for Identity sensors deployment and health alerts are applicable for Active Directory environments only.

License

Defender for Identity
Locked Out

Azure AD Identity Protection
Locked Out

Quick guides

What is Microsoft Defender for Identity?

Microsoft Secure Score

Loading...

Device compliance

Intune device compliance status

🟧 Compliant 🟨 Noncompliant
🟩 In grace period ⬜ Not evaluated

View details

Devices with active malware

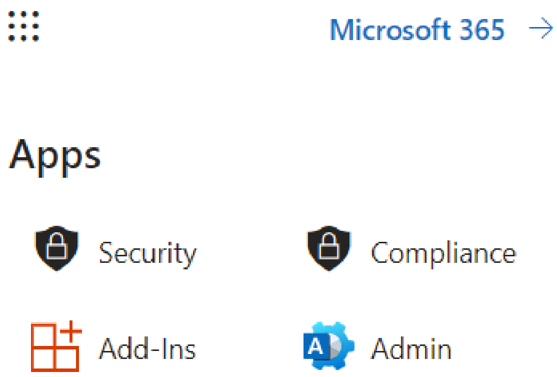
No managed devices

Track security events and enforce configuration and compliance policies through Intune device management

365 defender

The home page of Microsoft 365 defender

Now we will see step-by-step onboarding of the device and we will see how that will respond when a malware package is tried to enter the device and features provided by Microsoft 365 Defender.



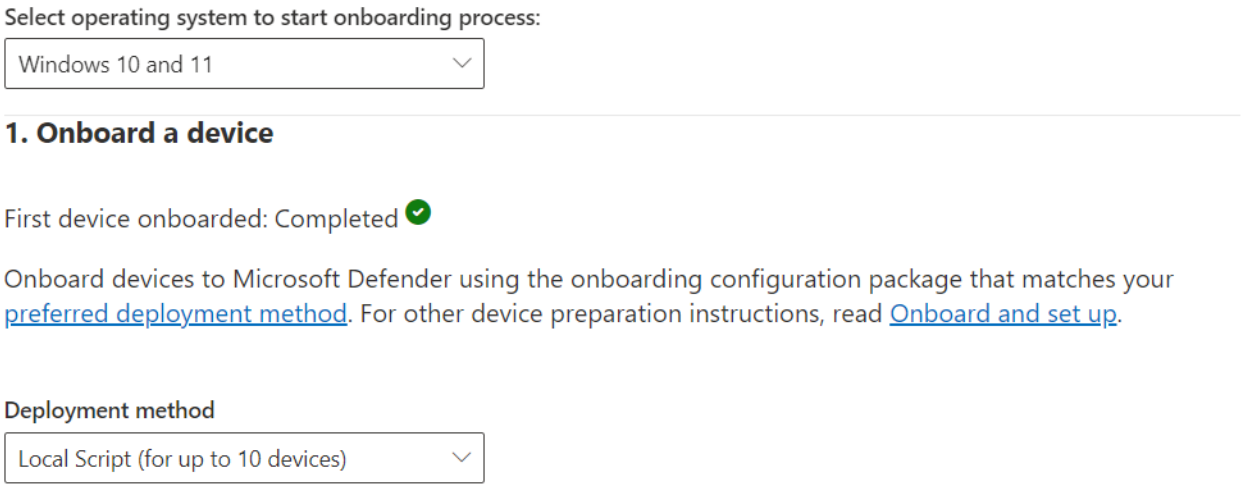
These are the Applications provided by Microsoft 365 Defender

Device onboarding:

Now we will see the exact process of deploying the EDR (Endpoint Detection and Response).

Here are the steps to deploy:

1. From the Home page we need to select the security as shown in the above picture
2. We need to go to the settings options and we need to select the Endpoints.
3. As we can see all the options on that we need to select device management
4. After going to that option, we need to select an option Device onboarding.
5. Now we need to select the version and it will give the package for that version as shown in the below picture.



Select operating system to start onboarding process:

Windows 10 and 11

1. Onboard a device

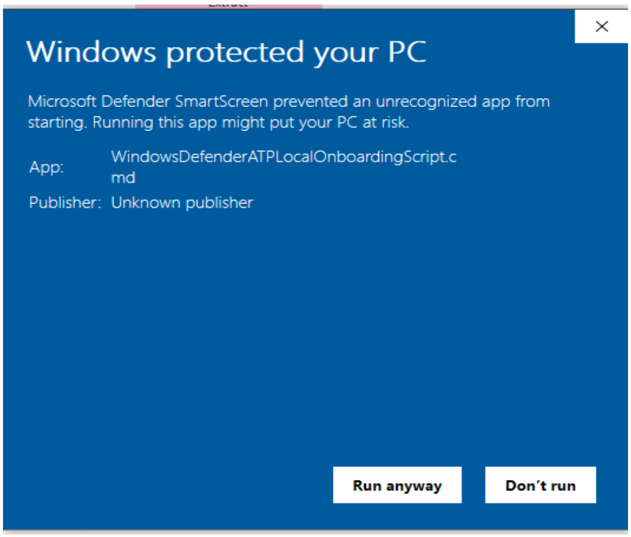
First device onboarded: Completed ✓

Onboard devices to Microsoft Defender using the onboarding configuration package that matches your preferred deployment method. For other device preparation instructions, read Onboard and set up.

Deployment method

Local Script (for up to 10 devices)

6. The same package can be deployed for 10 devices and we can go for more devices to deploy the same package.
7. After downloading to the client device, we need to start the installation process.
8. Make sure that installation must be done with admin privilege so that the package will have maximum access to the client device.
9. At first Microsoft Defender will try to block it but we need to give the run anyway option to install.

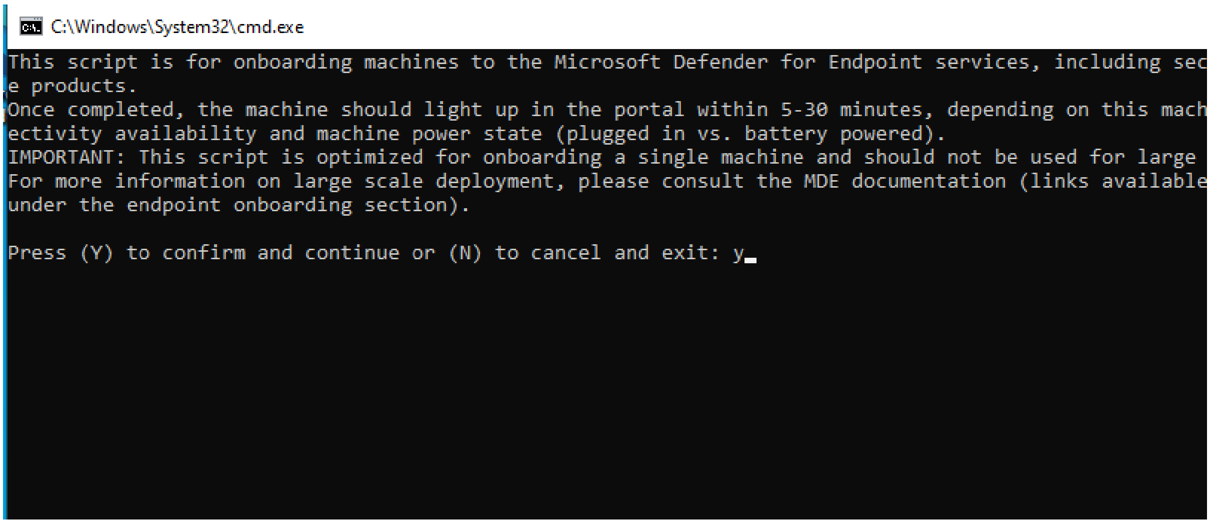


Windows protected your PC

Microsoft Defender SmartScreen prevented an unrecognized app from starting. Running this app might put your PC at risk.

App: WindowsDefenderATPLocalOnboardingScript.cmd

Publisher: Unknown publisher

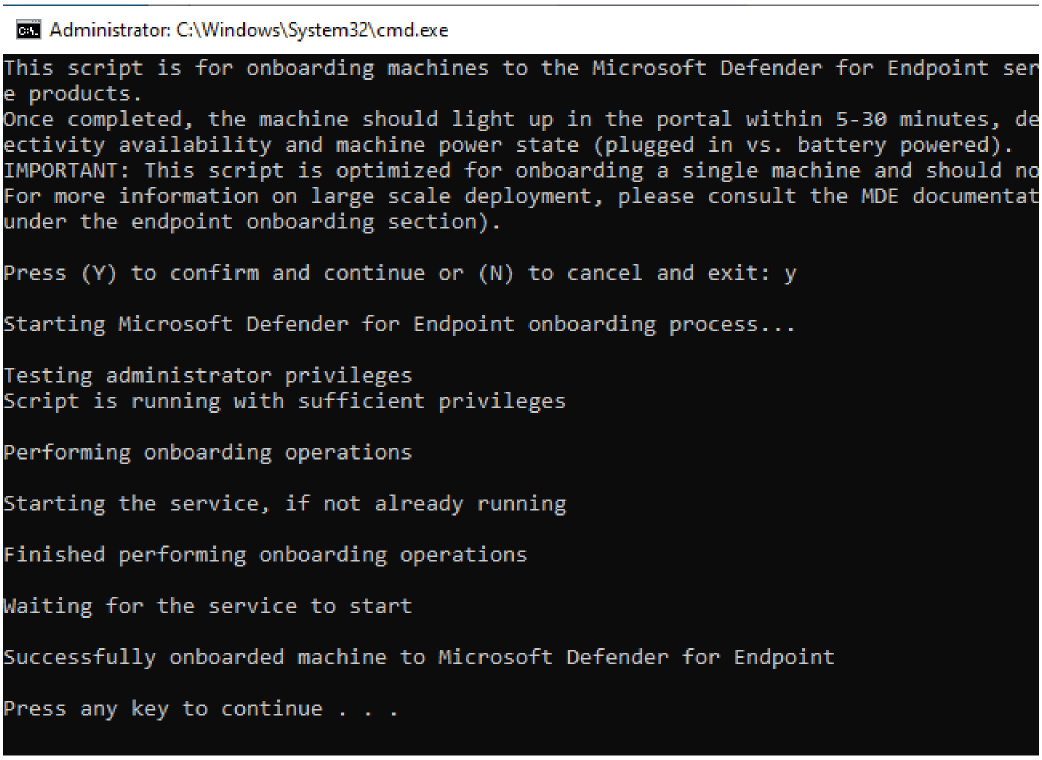


C:\Windows\System32\cmd.exe

```
This script is for onboarding machines to the Microsoft Defender for Endpoint services, including sec
e products.
Once completed, the machine should light up in the portal within 5-30 minutes, depending on this mach
ectivity availability and machine power state (plugged in vs. battery powered).
IMPORTANT: This script is optimized for onboarding a single machine and should not be used for large
For more information on large scale deployment, please consult the MDE documentation (links available
under the endpoint onboarding section).

Press (Y) to confirm and continue or (N) to cancel and exit: y
```

We need to y option to deploy the EDR in the client device



Administrator: C:\Windows\System32\cmd.exe

```
This script is for onboarding machines to the Microsoft Defender for Endpoint ser
e products.
Once completed, the machine should light up in the portal within 5-30 minutes, de
ectivity availability and machine power state (plugged in vs. battery powered).
IMPORTANT: This script is optimized for onboarding a single machine and should no
For more information on large scale deployment, please consult the MDE documentat
under the endpoint onboarding section).

Press (Y) to confirm and continue or (N) to cancel and exit: y

Starting Microsoft Defender for Endpoint onboarding process...

Testing administrator privileges
Script is running with sufficient privileges

Performing onboarding operations

Starting the service, if not already running

Finished performing onboarding operations

Waiting for the service to start

Successfully onboarded machine to Microsoft Defender for Endpoint

Press any key to continue . . .
```

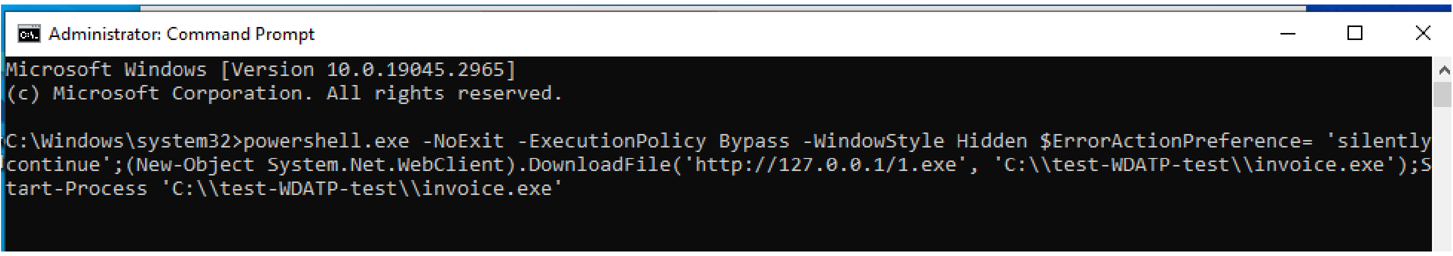
10. So, the deployment of the onboarding device is complete.

Working of EDR

Since we deployed the package now, we will see how it will give alerts to us. For this, Microsoft has a test command that will make sure to check whether the EDR is properly deployed or not.

Command: powershell.exe -NoExit -ExecutionPolicy Bypass -WindowStyle Hidden $ErrorActionPreference= 'silentlycontinue';(New-Object System.Net.WebClient).DownloadFile('http://127.0.0.1/1.exe', 'C:\\test-WDATP-test\\invoice.exe');Start-Process 'C:\\test-WDATP-test\\invoice.exe'

So, this is the command to test in the client device for that we will open the command prompt in the admin mode to make sure to check.

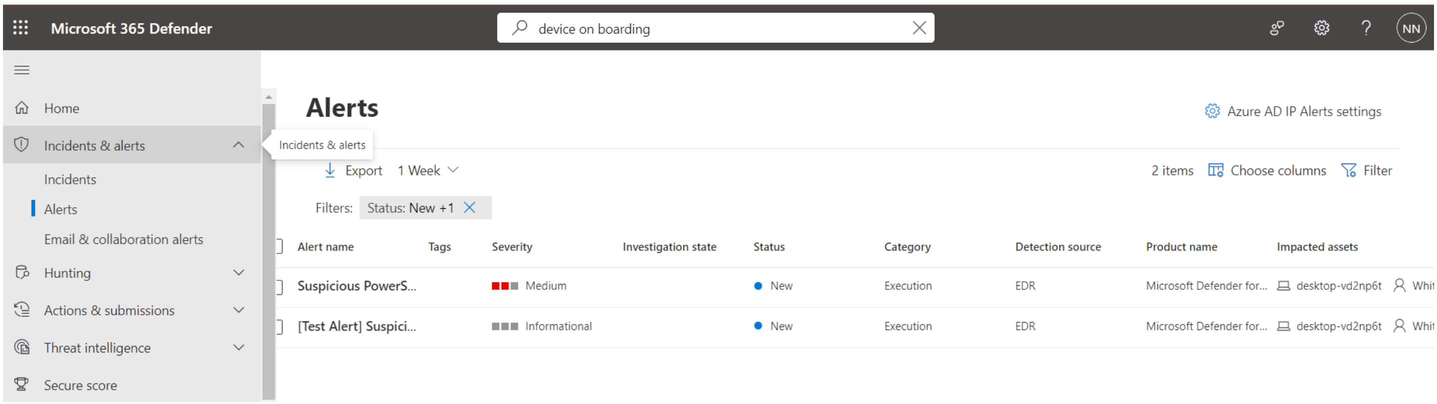


```
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>powershell.exe -NoExit -ExecutionPolicy Bypass -WindowStyle Hidden $ErrorActionPreference= 'silently
continue';(New-Object System.Net.WebClient).DownloadFile('http://127.0.0.1/1.exe', 'C:\\test-WDATP-test\\invoice.exe');S
tart-Process 'C:\\test-WDATP-test\\invoice.exe'
```

The command execution in the command prompt on the client device

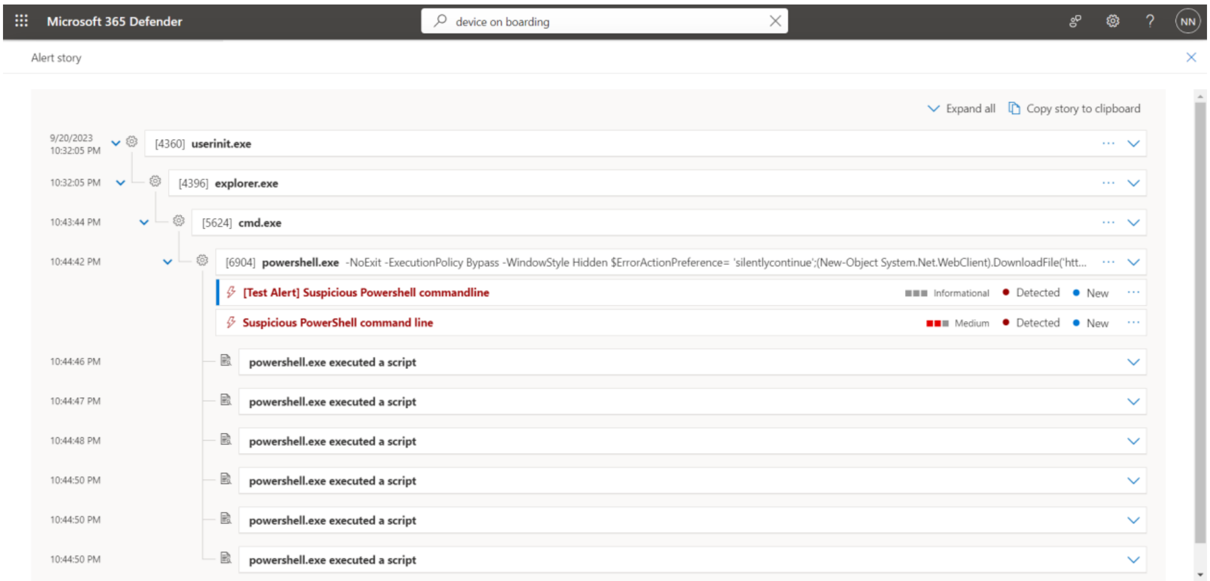
As we can see from the above picture the command the executed but it will do any action on the client device within a few minutes we will get an alert in the incidents and alerts.



Filters: Status: New +1

Alert name	Tags	Severity	Investigation state	Status	Category	Detection source	Product name	Impacted assets
Suspicious PowerS...		Medium		● New	Execution	EDR	Microsoft Defender for...	desktop-vd2np6t Whit
[Test Alert] Suspici...		Informational		● New	Execution	EDR	Microsoft Defender for...	desktop-vd2np6t Whit

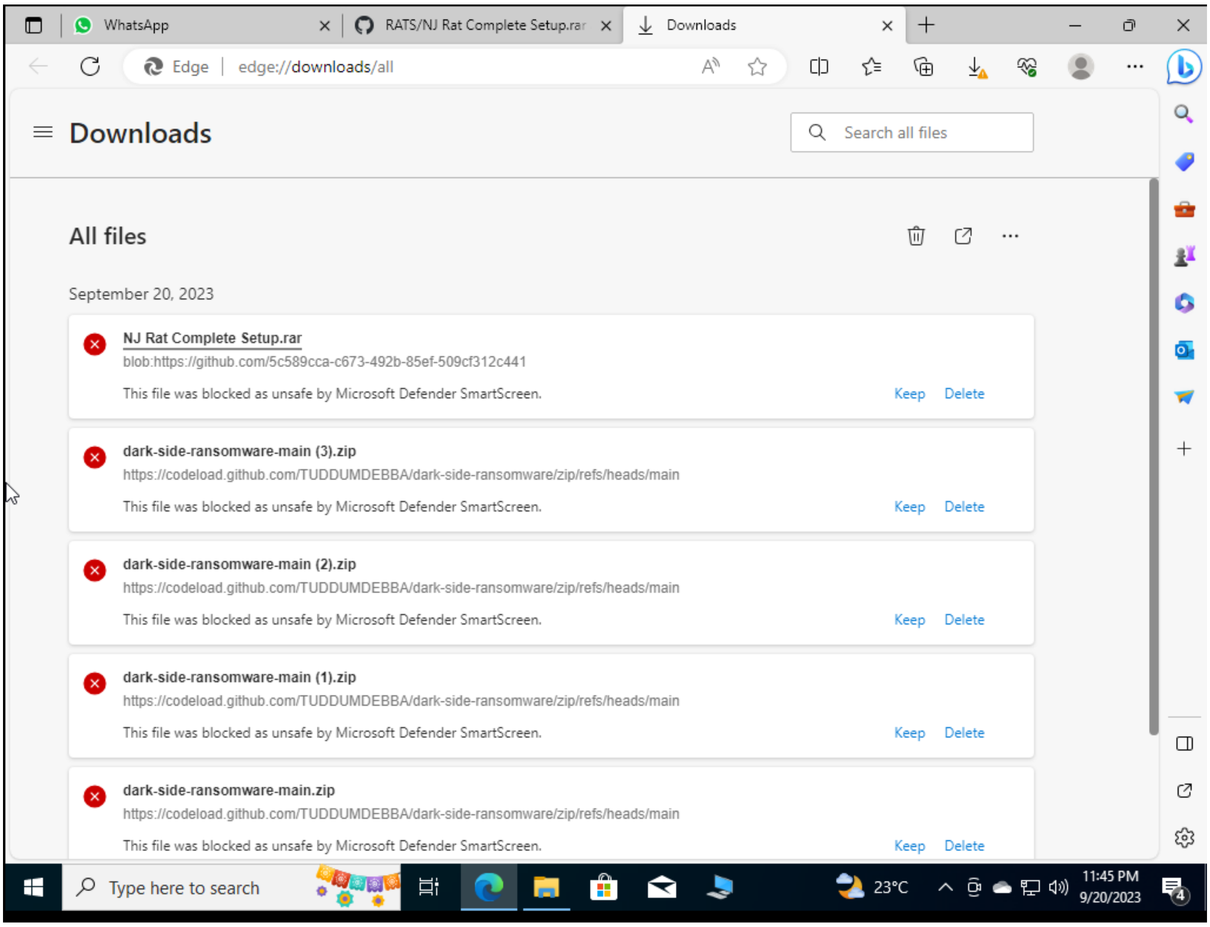
As shown in the above picture the alert has been received in the Microsoft 365 Defender. Now we will look into the alert by right-clicking the suspicious power command Line and it will give a detailed description of the command like the working methodology and motive of the command and where it will try to lead to reach but in the client device it will not be executed the alert will be sent within no time to Microsoft 365 defender.



```
9/20/2023 10:32:05 PM  [4360] userinit.exe
10:32:05 PM            [4396] explorer.exe
10:43:44 PM            [5624] cmd.exe
10:44:42 PM            [6904] powershell.exe -NoExit -ExecutionPolicy Bypass -WindowStyle Hidden $ErrorActionPreference= 'silentlycontinue';(New-Object System.Net.WebClient).DownloadFile('htt...
                       [Test Alert] Suspicious Powershell commandline    Informational  ● Detected  ● New
                       Suspicious PowerShell command line                Medium         ● Detected  ● New
10:44:46 PM            powershell.exe executed a script
10:44:47 PM            powershell.exe executed a script
10:44:48 PM            powershell.exe executed a script
10:44:50 PM            powershell.exe executed a script
10:44:50 PM            powershell.exe executed a script
10:44:50 PM            powershell.exe executed a script
```

As we can see in the above image, we can have a clear view of the command in detail the motive of the command including timestamps the red alerts are the most suspicious part of the command they will also tell us the level of command will try to damage.

Now we will try to deploy a malware in the client system:



September 20, 2023

NJ Rat Complete Setup.rar
blob:https://github.com/5c589cca-c673-492b-85ef-509cf312c441
This file was blocked as unsafe by Microsoft Defender SmartScreen. Keep Delete

dark-side-ransomware-main (3).zip
https://codeload.github.com/TUDDUMDEBBA/dark-side-ransomware/zip/refs/heads/main
This file was blocked as unsafe by Microsoft Defender SmartScreen. Keep Delete

dark-side-ransomware-main (2).zip
https://codeload.github.com/TUDDUMDEBBA/dark-side-ransomware/zip/refs/heads/main
This file was blocked as unsafe by Microsoft Defender SmartScreen. Keep Delete

dark-side-ransomware-main (1).zip
https://codeload.github.com/TUDDUMDEBBA/dark-side-ransomware/zip/refs/heads/main
This file was blocked as unsafe by Microsoft Defender SmartScreen. Keep Delete

dark-side-ransomware-main.zip
https://codeload.github.com/TUDDUMDEBBA/dark-side-ransomware/zip/refs/heads/main
This file was blocked as unsafe by Microsoft Defender SmartScreen. Keep Delete

As we can see above the image where the client tried to download malware on the client system. But we can see that each and every time the Microsoft Defender SmartScreen tried to stop the download of malware. It's one of the great features to stop entering malware Now will see in-depth in the features.

Features of Microsoft 365 Defender

I. EDR in block mode: This feature will block malicious behaviors at the endpoint detection. It will also give an alert to the defender.

II. Tamper Protection: It is one of the popular features to protect the client device by not allowing the device not to change any security settings on that device and they can't turn off the Microsoft Defender on that device.

III. Web content Filtering: In these, it will automatically restrict the client device not to accessing blocked domains and malicious websites and also help in tracking all web activities.

IV. Device Discovery: In these any unregistered device that wants to access the network and tries to communicate with the client devices immediately will block the device by not allowing it to enter that network.

V. Live Response: Role-based access control will come into the picture not to allow access by unauthorized users by shell connection like SSH or Telnet connection and it can also be implemented on the server.

VI. Quarantined Files: This feature will help to download the files and keep them in a restricted zone to make sure that files are safe and ready to back up at any time.

VII. Unsigned script execution: If any malicious command tries to execute in the command prompt it will stop execution and send an alert to Defender.

VIII. Sharing Endpoint Alerts: We can share the alerts with the compliance center to stop insider attackers in the organization.

IX. Custom network indicator: In this feature, we can give access to a particular IP address, URL and domains to be accessed by the client device and also monitor the logs and send logs to the Defender.

X. File access: In this feature, we can decide which file is to be given access or not in the client device.

APIs: SIEM (Security information and event management) is a feature that will monitor all the events in the client it's a new feature that will be officially available on December 31, 2023

Rules: we can write our own rules on the network, files, and security settings so that we can follow the CIA triad within the organization.

Permissions: We can create groups in the defender and we can monitor groups instead of the individual monitor and we can give or restrict the access within the organization.