Microsoft Defender for Endpoint

Microsoft Defender for Endpoint : Microsoft Defender for Endpoint is Microsoft's enterprise endpoint security platform which is created to prevent, investigate, detect, and respond to threats. . Microsoft Defender for Endpoint is a security solution that includes risk-based vulnerability management and assessment, attack surface reduction, behavioral-based and cloud-powered next-generation protection, endpoint detection and response (EDR), automatic investigation and remediation, managed hunting services, rich APIs, and unified security management.

Advance features of Microsoft Defender :

Enable advance features :

1. in navigation pane ,select Settings > Endpoints > Advanced features
2. select the advanced features you want to configure and toggle the setting between on or off
3. select save preferences

- Automated investigation
  - which Enables the automation capabilities for investigation and response.
- Enabling EDR in block mode
  - it provides extra added protection from the malicious artifacts when Microsoft Defender Antivirus is not the primary antivirus product and is running in passive mode.
  - EDR in block mode works behind the scenes to remediate malicious behavioral-based applications that were detected by EDR
  - EDR in block mode allows Microsoft Defender Antivirus to take actions on post-breach, behavioral EDR detection.

EDR in block mode does not provide all the protection when user using Microsoft antivirus real-time protection

- automatically resolve alerts
  - if Automated investigation finds no threats or has successfully remediated all malicious artifacts. It resolves an alerts
- Enabling Allow or block file
  - this feature enable you to block potential malicious files in your network. Blocking file will prevent it from being read written or executed on devices in your organization

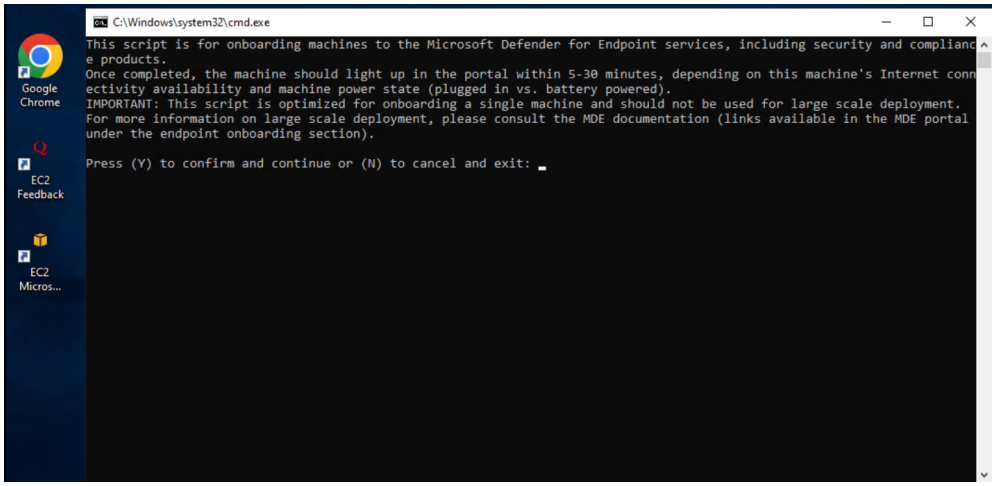
Blocking is only available if the user using Microsoft Defender as a active anti-malware solution
cloud-based protection feature should be enabled

- Enabling custom network indicator

    - this feature allows you to create indicators for IP addresses, domains, or URLs, which determine whether they'll be allowed or blocked based on your custom indicator list.
- Tamper protection
    - during attack some kind off malicious software tries to disable security features like disabling real-time protection turning off third party anti-viruses. On your machine these kind of applications like to disable your security features to get easier access your data to install malware or to exploit your devices or breach the data , identity.
    - Tamper protection essentially locks Microsoft defender anti-virus and prevent from security settings being changed
- Enabling skype for business integration
    - Enabling the Skype for Business integration gives you the ability to communicate with users using Skype for Business, email, or phone. This activation can be handy when you need to communicate with the user and mitigate risks.
- Microsoft Defender for identity integration
    - The integration with Microsoft Defender for Identity allows you to pivot directly into another Microsoft Identity security product. Microsoft Defender for Identity augments an investigation with more insights about a suspected compromised account and related resources. By enabling this feature, you'll enrich the device-based investigation capability by pivoting across the network from an identify point of view.
- Web content filtering
    - Block access to websites containing unwanted content and track web activity across all domains.
- Download quarantined files
    - Backup quarantined files in a secure and compliant location so they can be downloaded directly from quarantine. The download file button will always be available in the file page
- Authenticated telemetry
    - Turning on Authenticated telemetry to prevent spoofing telemetry into your dashboard.
- Microsoft Intune Connection
    - Enabling this feature shares of device information , additional information about manged device and enhanced policy enforcement
- Device discovery
    - this help you to find un-managed devices connected to you network without the need for extra appliances Using onboarded devices, you can find unmanaged devices in your network and assess vulnerabilities and risks

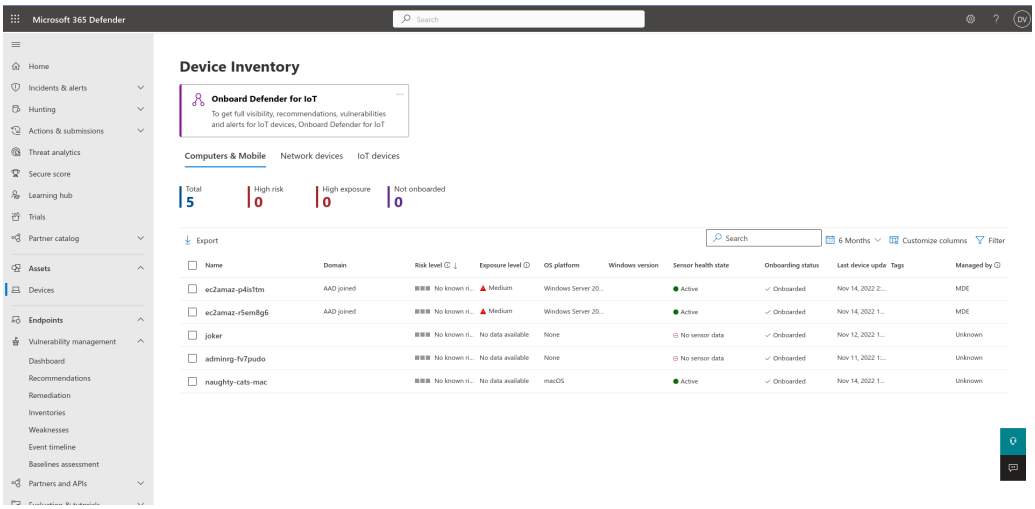
Onboarding Devices :

1) In navigation pane select Setting > Endpoints > Device Management > Onboarding.
2) Select Platform OS that you want to connect to EDR
3) Onbording a device **Select Deployment method | Download Onboarding package**
4) Extract on device that you want to get connected to EDR
5) Run the application as a administrator and enter Y to configure Windows Defender onboarding package
6) Wait till the onboarding process complete

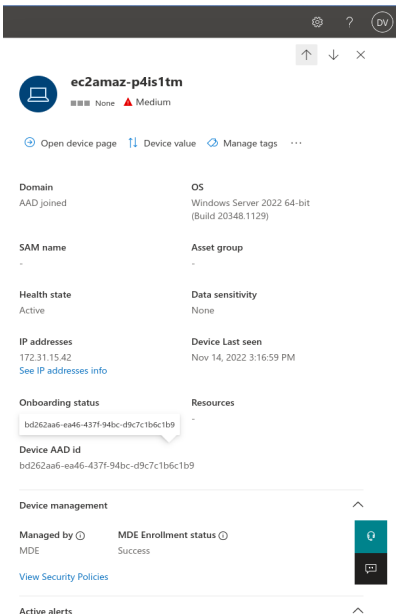


7) Run a **detection test**
   a) open a Command prompt Window
   b) powershell.exe -NoExit -ExecutionPolicy Bypass -WindowStyle Hidden $ErrorActionPreference= 'silentlycontinue';(New-Object System.Net.WebClient).DownloadFile('http://127.0.0.1/1.exe', 'C:\\test-WDATP-test\\invoice.exe');Start-Process 'C:\\test-WDATP-test\\invoice.exe'
   c) copy paste the command the command prompt window close automatically

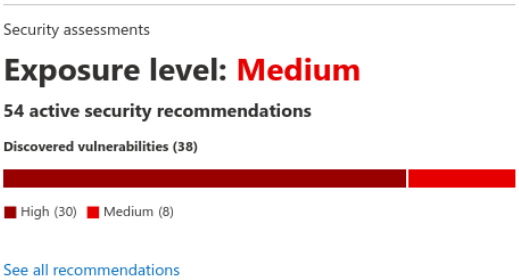
after few min you can see the devices in Home or Devices in navigation pane



click on the device to see device details
opening device page is going to give more information about the user
Exposure Level , Risk Level , user login



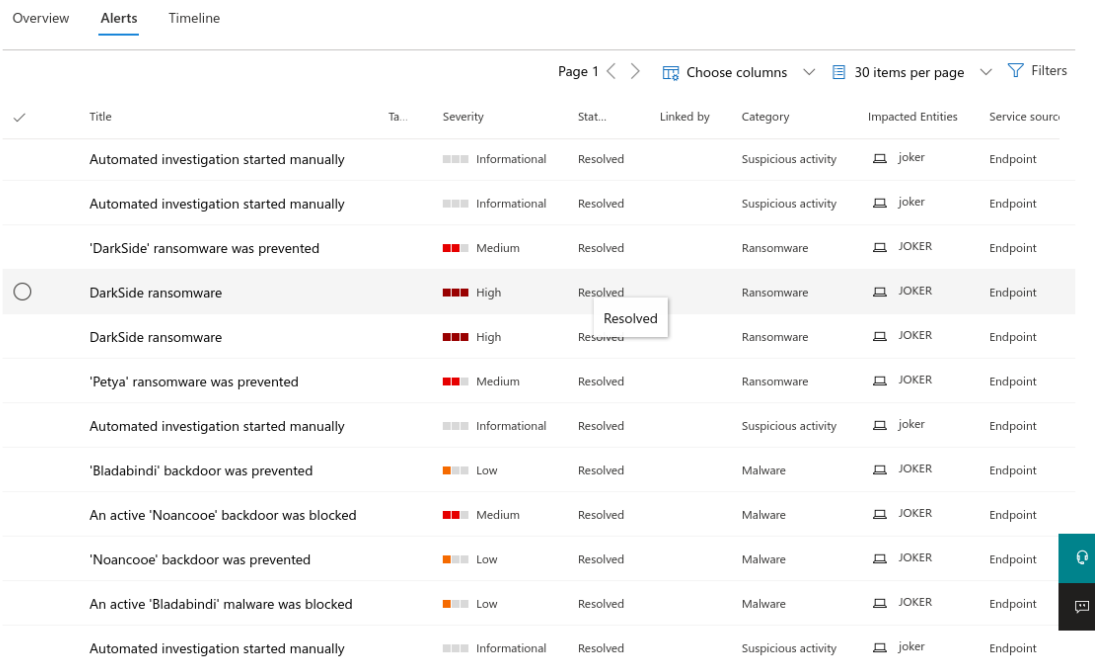
Exposure level shows vulnerability exposure lowering the vulnerability exposure by remediating security recommendations



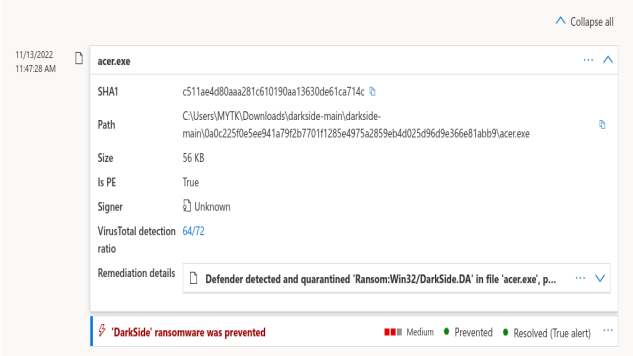
make the most impact to the device Each software has weaknesses that are going to be transformed into recommendations and prioritized based on
risk to the organization

Exposure Scoring level :

- 0-29 Low exposure score
- 30-69 medium exposure score
- 70 – 100 high exposure score



If user click on any kind of application with a malicious behavior which is pop some alerts based on threat activity of malicious files and threat level
in EDR



Microsoft Defender for Endpoint (MDE, previously known as Microsoft Defender Advanced Threat Protection) is Microsoft's endpoint security platform that goes far and beyond the traditional anti-malware engine and firewall to protect against the modern cybersecurity threats an organization faces

Creating policy in MDE anti-virus endpoint security :

creating new policy can make can make accurate monitor on incoming outgoing files

- scanning of mails
- File extensions to exclude from scans and real-time protection
- Enabling mapped network drives be scanned during a full scan

- Allowing Intrusion Prevention System
- Blocking user access to Microsoft Defender app
- Scanning network files
- CPU usage limit per scan
- Turn on behavior monitoring
- Enable on access protection
- Turn on real-time protection
- Disable Catchup Quick Scan
- Cloud-delivered protection level
- Day of week to run a scheduled scan
- Disable Catch-up Full Scan
- Scan removable drives during full scan
- Check For Signatures Before Running Scan (Device)
- Scan all downloaded files and attachments
- Scan scripts that are used in Microsoft browsers
- Scan archive files
- Turn on cloud-delivered protection
- Defender Cloud Extended Timeout In Seconds
- Enable low CPU priority for scheduled scans
- Submit Samples Consent
- Actions for detected threats
- Action to take on potentially unwanted apps
- Scan Type
- Allow users to view the full History results
- Create a system restore point before computers are cleaned
- Randomize scheduled scan and security intelligence update start times

Review and Save the settings

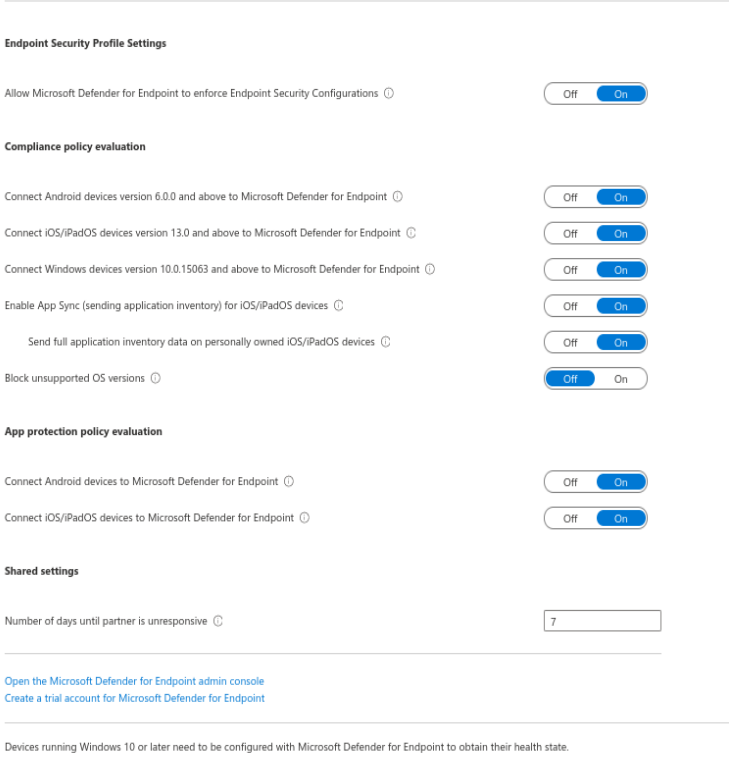
Creating policy for firewall

- creating rules for inbound and outbound traffic
- services names of protocols that can be allowed on organization
- ports ranges to include to scan the traffic
- accepting RDP port addresses through
  - remote access
  - wireless connection
  - LAN
  - Mobile broadband

only mentioned interface can be accepting as remote access agents

- The EdgeTraversal property indicates that specific inbound traffic is allowed to tunnel through NATs

Configuring Microsoft defender for Endpoint



Allow Microsoft Defender for Endpoint to enforce Endpoint Security Configurations

Microsoft Endpoint Manager can enforce Endpoint Security profiles and configuration via supported agents independently of the device being managed by MDM or ConfigMgr.

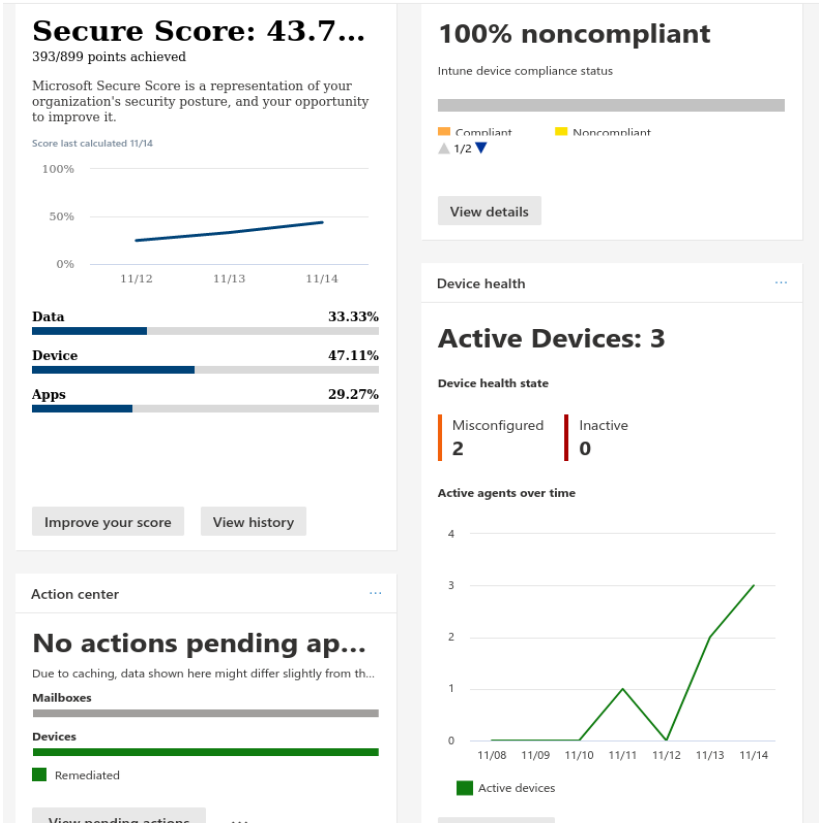
Enabling this setting allows supported agents to report the status of applied profiles to Microsoft Endpoint Manager, and agents will appear in device views and reports relevant to Endpoint Security profile management.

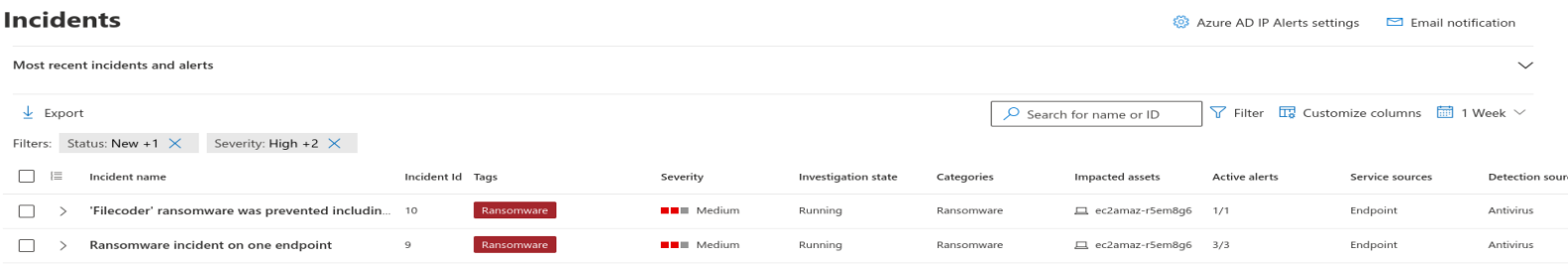
INCIDENTS :

if there is any Malware detected in user device or suspicious or malicious event or activity it is going to provide clues and extra information about completed or ongoing attack the defender automatically trigger the alerts and associated information into an incident

- where the attack started
- what kind of tactics were used
- threat of the code
- how many devices , users , mailboxes impacted from the threat
- all of the associated with the attack

The defender is going to automatically investigate and resolves alert through automation and AI(artificial intelligence).
By adding new policy we can also perform additional remediation steps to resolve the attack

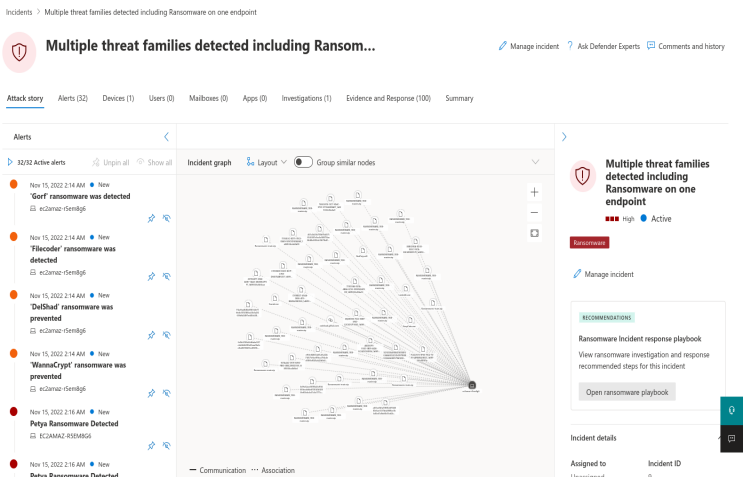




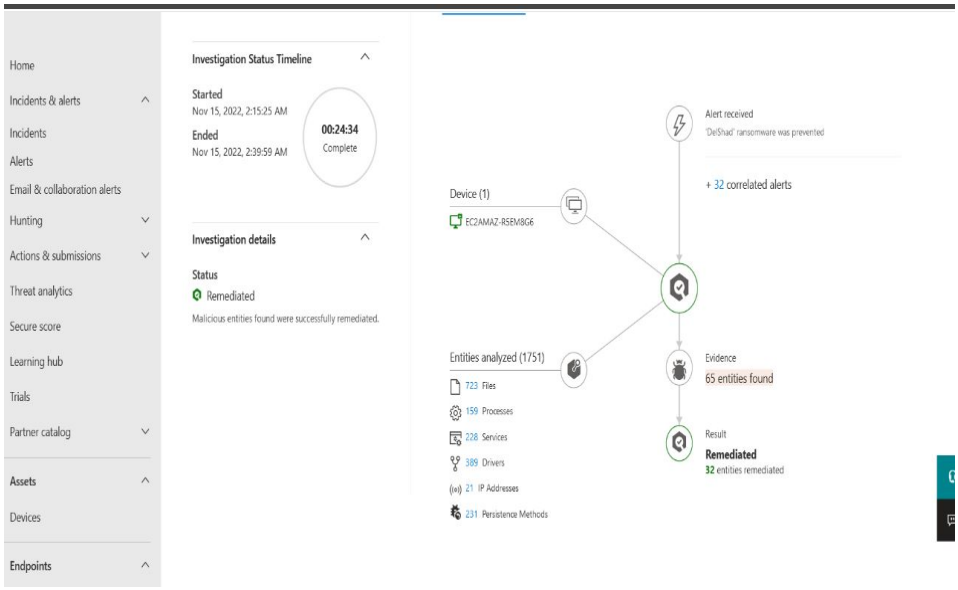
selecting an incident name displays the entire attack chain including alert and a graph of chain which shows process of the entity that follows

viewing the attack story to get entity details from the graph and deleting the file or isolating the device

alerts – alerts are related to the incident and their information
devices – all the devices that are identified who are related to incident
mailboxes – how many mailboxes all associated with the attack



investigation – an automated investigation going perform and generate information which are triggered by alerts in the incident
evidence and response – we can able see all kind of supported events and suspicious entities and attack chain.
Summary – a quick overview of the impact assets got damaged



Alerts :

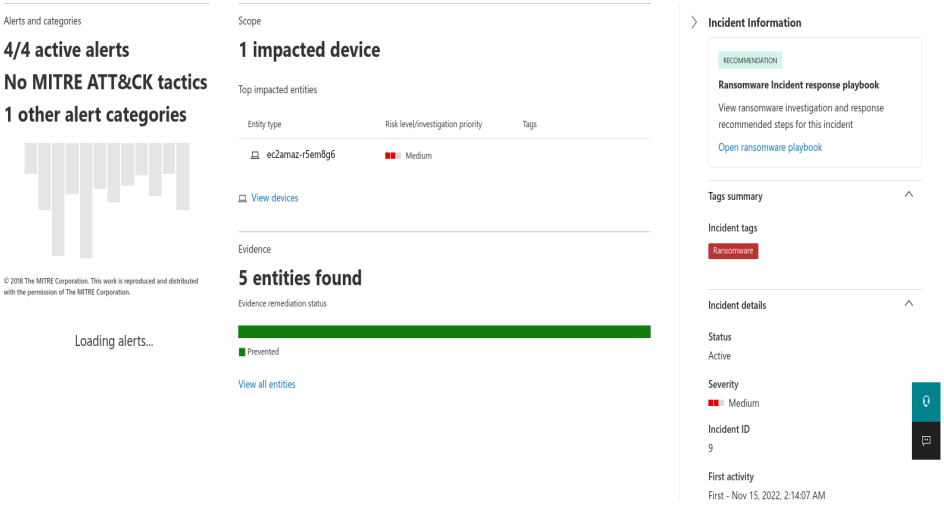
alerts are basis of all incidents to indicate the threat of malicious or suspicious event in environment it provide clues of incident.

All the alerts together to form an incident alerts are required for analyzing the incident for deeper analyzing

Analyzing an alert :

in alert page we can see a chain of events and alerts rated for the threat and summary details

opening the main alert from alert page action from manage alert pane. We can identify the source of a alert from different sources like windows defender , windows defender for end point microsoft data prevention microsoft defender for cloud apps etc



Managing an alert :

based to threat act we are going to c**h**ange alert status **t**o resolved or in progress

kind of the user that assigned to that alert

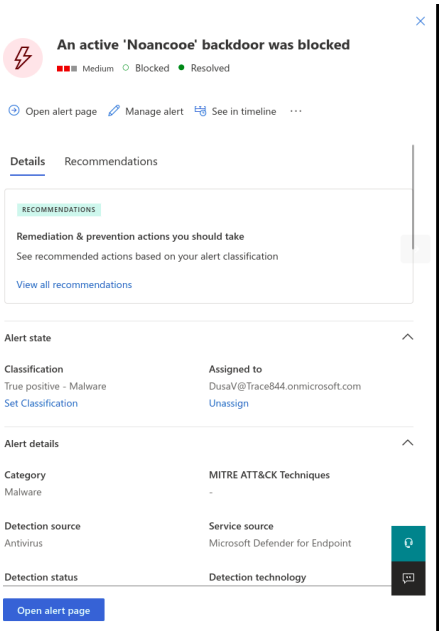
alert classifications :

not set will by default

True positive to ensure what type of threat it can be that can indicate a real threat . Specifying the type of threat and threat pattern to defend the organization

informational, expected activity using this option for alert which are accurate which are with normal behavior or self made threat activity (mainly used for automation investigation alert)

False positive if the alert is created even when there is no malicious behavior or malicious activity this kind of classification



can identify event as normal events that are triggered mistakenly identified . This will be using for catching real threats classifying alerts as false positive helps EDR to improve detection quality The **Recommendations** tab provides next-step actions and advice for investigation, remediation, and prevention.