Extended Detection and Response with Microsoft Defender XDR

Vlad Catrinescu

Microsoft MVP | Independent Consultant

@vladcatrinescu | VladTalksTech.com | YouTube.com/@VladTalksTech

Overview

- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Microsoft Defender Vulnerability Management
- Microsoft Defender Threat Intelligence
- Microsoft Security Copilot

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint

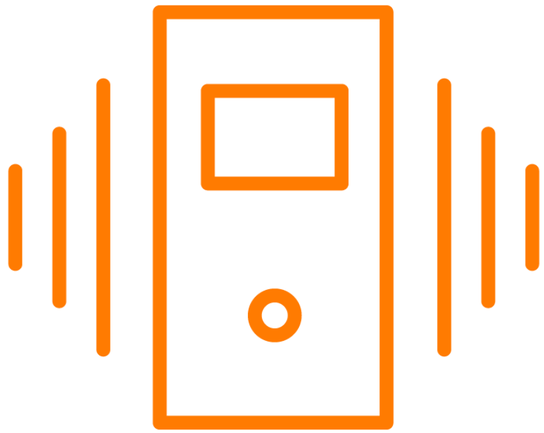
Microsoft Defender for Endpoint is a platform designed to help enterprise networks protect endpoints including laptops, phones, tablets, PCs, access points, routers, and firewalls. It does so by preventing, detecting, investigating, and responding to advanced threats.

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint

Microsoft Defender for Endpoint Key Areas

- Core Defender Vulnerability Management
- Attack surface reduction
- Next-generation protection
- Endpoint detection and response
- Automated investigation and remediation
- Microsoft Threat Experts

Core Defender Vulnerability Management



Risk-based approach to

- Discovery
- Prioritization
- And remediation of endpoint vulnerabilities

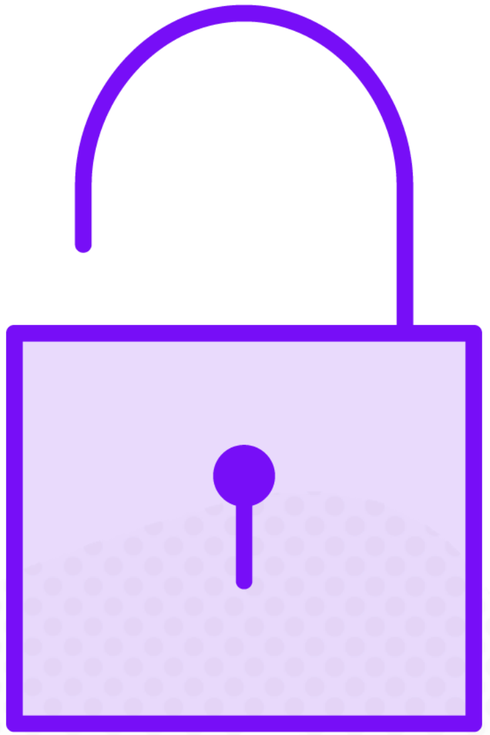
Uses sensors for real-time discovery

- No agents/scans needed

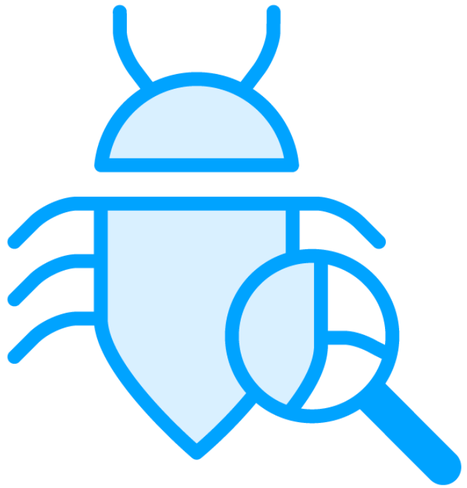
Attack Surface Reduction

Reduce the places where your organization is vulnerable

- Provides a first line of defense
- Ensures configurations are properly set
- Network and web protection



Next-generation Protection



Microsoft Defender Antivirus

- Behavior-based and real-time antivirus protection
- Cloud-delivered protection
- Protection and product updates

Endpoint Detection and Response

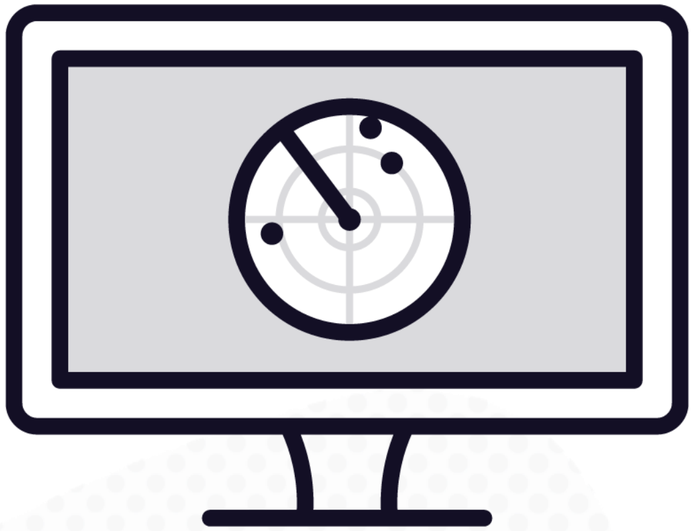
Advanced attack detection

- Near real-time
- Actionable

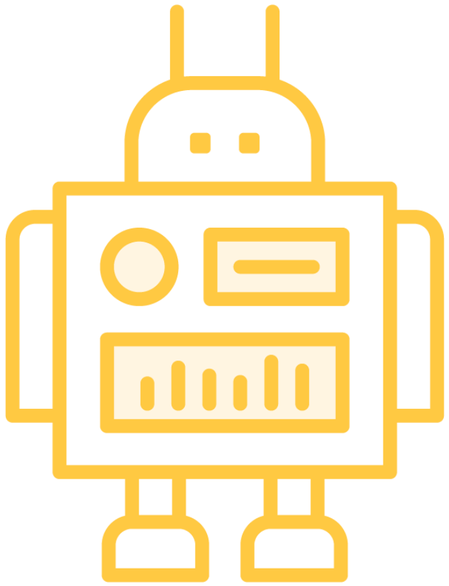
Prioritize alerts and gain visibility into the full scope of a breach

Alerts with same technique/attacker are aggregated into an incident

- Easier to investigate and respond to a threat



Automated Investigation and Remediation (AIR)



Inspection algorithm and processes to examine alerts and take quick remediation

Remediation can occur automatically or only upon approval

- Depending on your organization configuration

Microsoft Threat Experts

Managed threat hunting service

Expert level monitoring and analysis

Targeted attack notification

Access to experts on demand

Customers need to apply for the Microsoft Threat Experts program

- Extra cost

Other Features

Microsoft Secure Score for Devices

Dynamically assess the security state of your enterprise network, identify unprotected systems, and take recommended actions to improve the overall security of your organization

Management and APIs

Offers an API model designed to expose entities and capabilities through a standard Microsoft Entra ID-based authentication and authorization model

Microsoft Defender for Office 365

Microsoft Defender for Office 365

Microsoft Defender for Office 365 , safeguards your organization against malicious threats posed by email messages, links , and collaboration tools, including Microsoft Teams, SharePoint Online, OneDrive for Business, and other Office clients

https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-security-center-mdo

Microsoft Defender for Office 365 Key Areas

Threat protection policies

Reports

Threat investigation and response capabilities

Automated investigation and response capabilities

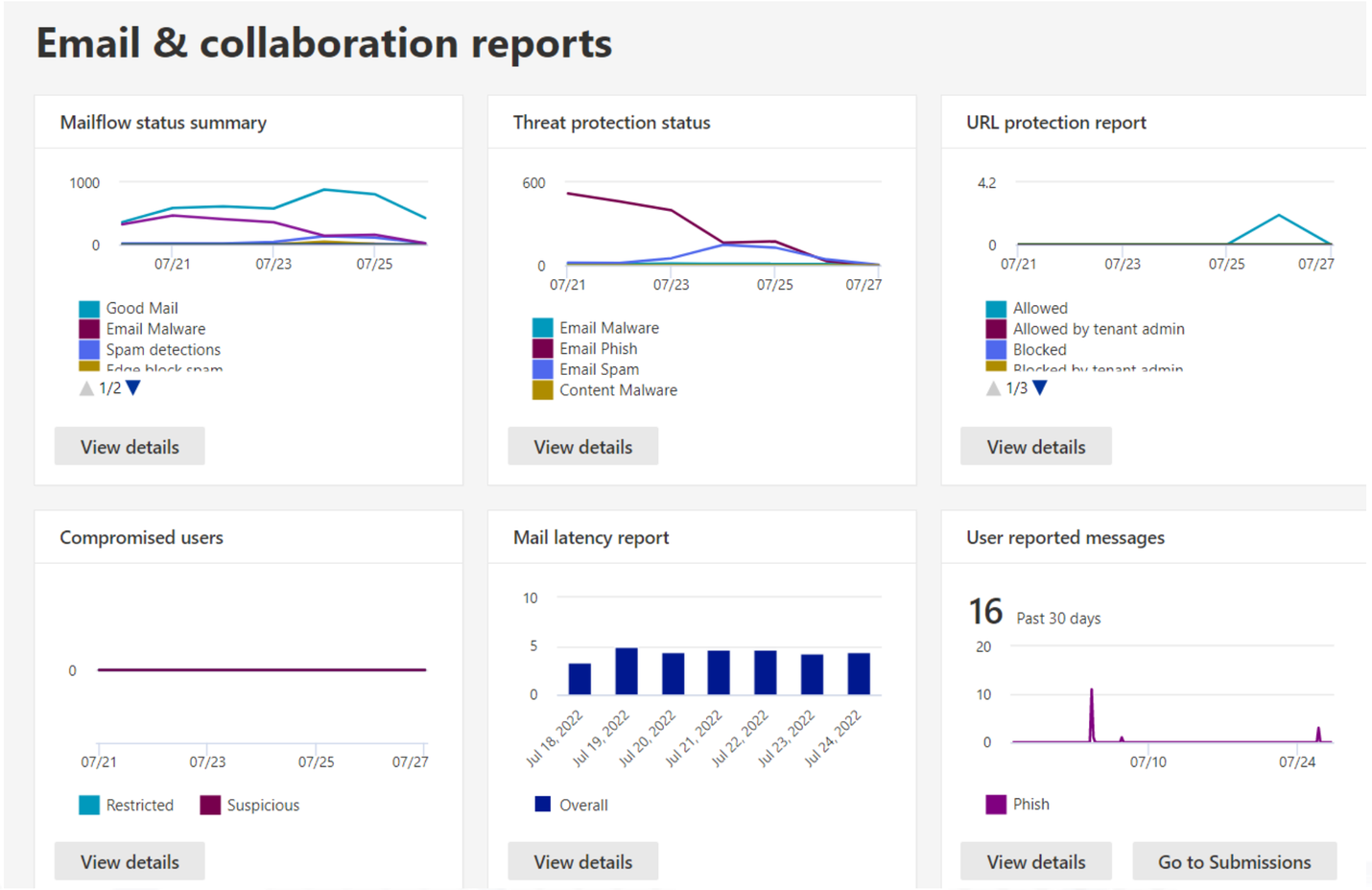
Threat Protection Policies

Safe Attachments	Provides zero-day protection to safeguard your messaging system, by checking email attachments for malicious content
Safe Links	Provides time-of-click verification of URLs, for example, in emails messages and Office files
Anti-phishing protection	Detects attempts to impersonate your users and internal or custom domains
Safe Attachments for SharePoint, OneDrive, and Teams	Protects your organization when users collaborate and share files, by identifying and blocking malicious files in document libraries

Microsoft Defender for Office 365 Reports

Real-time reports to monitor performance

- URL protection report
- Threat protection status
- User reported messages



Threat Investigation and Response Capabilities

Threat trackers

Threat explorer/real-time detections

- Identify and analyze recent threats

Attack simulator

- Run realistic attack scenarios in your organization
  - Spear phishing
  - Attachment attack
  - Password spray

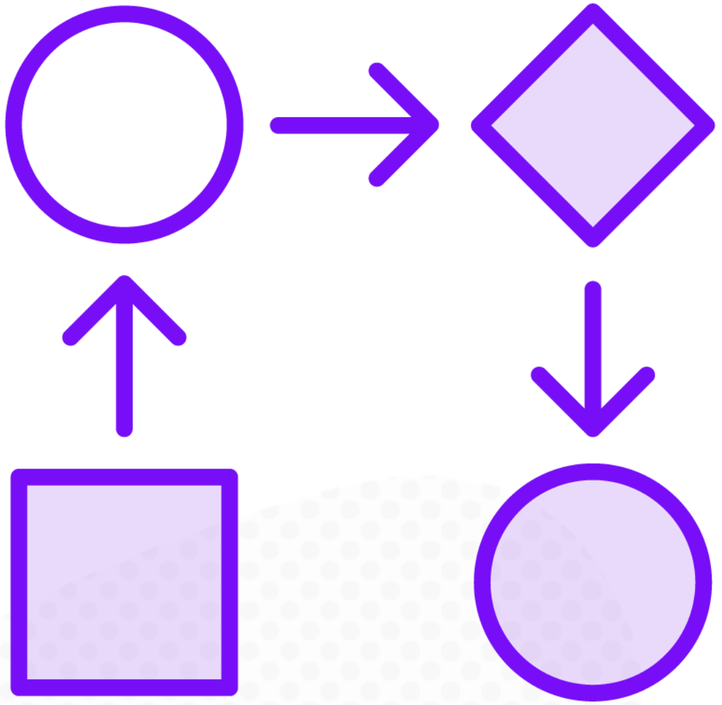
Automated Investigation and Response (AIR)

Set of security playbooks

Can be launched manually or automatically

Remediation actions are proposed

Security team approves or rejects them



Microsoft Defender for Identity

Microsoft Defender for Identity

Microsoft Defender for Identity is a cloud-based security solution that helps secure your identity monitoring across your organization. Defender for Identity is fully integrated with Microsoft Defender XDR, and leverages signals from both on-premises Active Directory and cloud identities to help you better identify, detect, and investigate advanced threats directed at your organization.

https://docs.microsoft.com/en-us/defender-for-identity/what-is

Microsoft Defender for Identity Key Areas

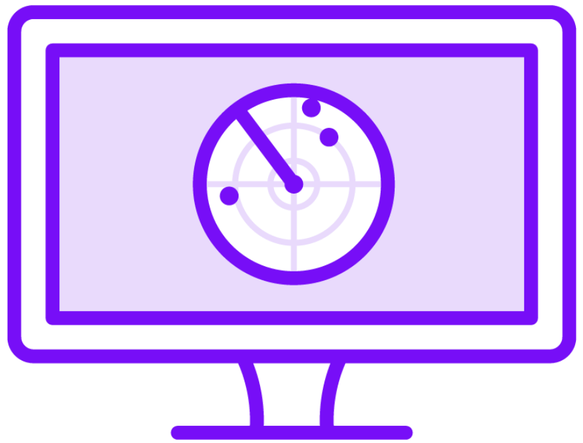
Monitor and profile user behavior and activities

Protect user identities and reduce the attack surface

Identify suspicious activities and advanced attacks across the cyber-attack kill-chain

Investigate alerts and user activities

Monitor and Profile User Behavior and Activities



Monitors and analyzes

- User activities
- Permissions
- Group membership

Creates a behavioral baseline for each user

Identify anomalies in user behavior

- Insights into suspicious activities and events

Protect User Identities and Reduce the Attack Surface

Insights on identity configurations and security best practices

Reduce your organizational attack surface

Visual Lateral Movement Paths

Quickly understand how attackers can move laterally inside your network

Security reports to identify users and devices authenticating with clear-text passwords

Identify Suspicious Activities and Advanced Attacks

Reconnaissance

Identify rogue users and attackers' attempts to gain information

Compromised credentials

Identify attempts to compromise user credentials using brute force attacks, failed authentications, and other methods

Lateral movements

Detect attempts to move laterally inside the network to gain further control of sensitive users

Domain dominance

Highlighting attacker behavior if domain dominance is achieved, through remote code execution on the domain controller and other methods

Investigate Alerts and User Activities

Provide only relevant security alerts

Real-time organizational attack timeline

Microsoft Defender Vulnerability Management

Microsoft Defender Vulnerability Management

Defender Vulnerability Management delivers asset visibility, intelligent assessments, and built-in remediation tools for Windows, macOS, Linux, Android, iOS, and network devices.

Leveraging Microsoft threat intelligence, breach likelihood predictions, business contexts, and devices assessments, Defender Vulnerability Management rapidly and continuously prioritizes the biggest vulnerabilities on your most critical assets and provides security recommendations to mitigate risk.

https://learn.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/defender-vulnerability-management

Microsoft Defender Vulnerability Management Key Areas

Continuous asset discovery and monitoring

Risk-based intelligent prioritization

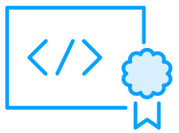
Remediation and tracking

Continuous Asset Discovery and Monitoring

Visibility into software and vulnerabilities

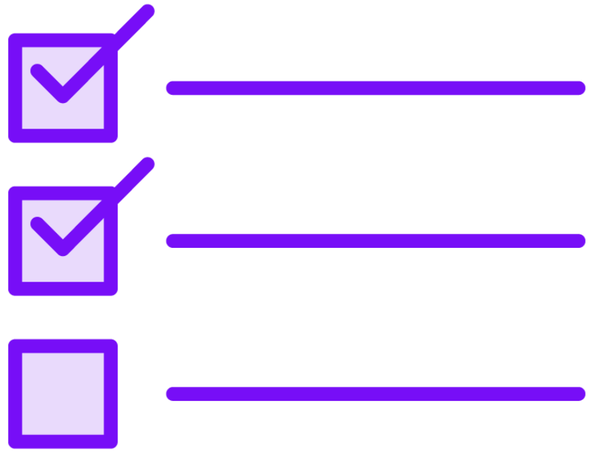
Network share assessment

Browser extensions assessment



Digital certificates assessment

Risk-based Intelligent Prioritization



Prioritizes recommendations for your assets to reduce the biggest vulnerabilities

- From multiple sources including Microsoft's threat intelligence

Remediation and Tracking

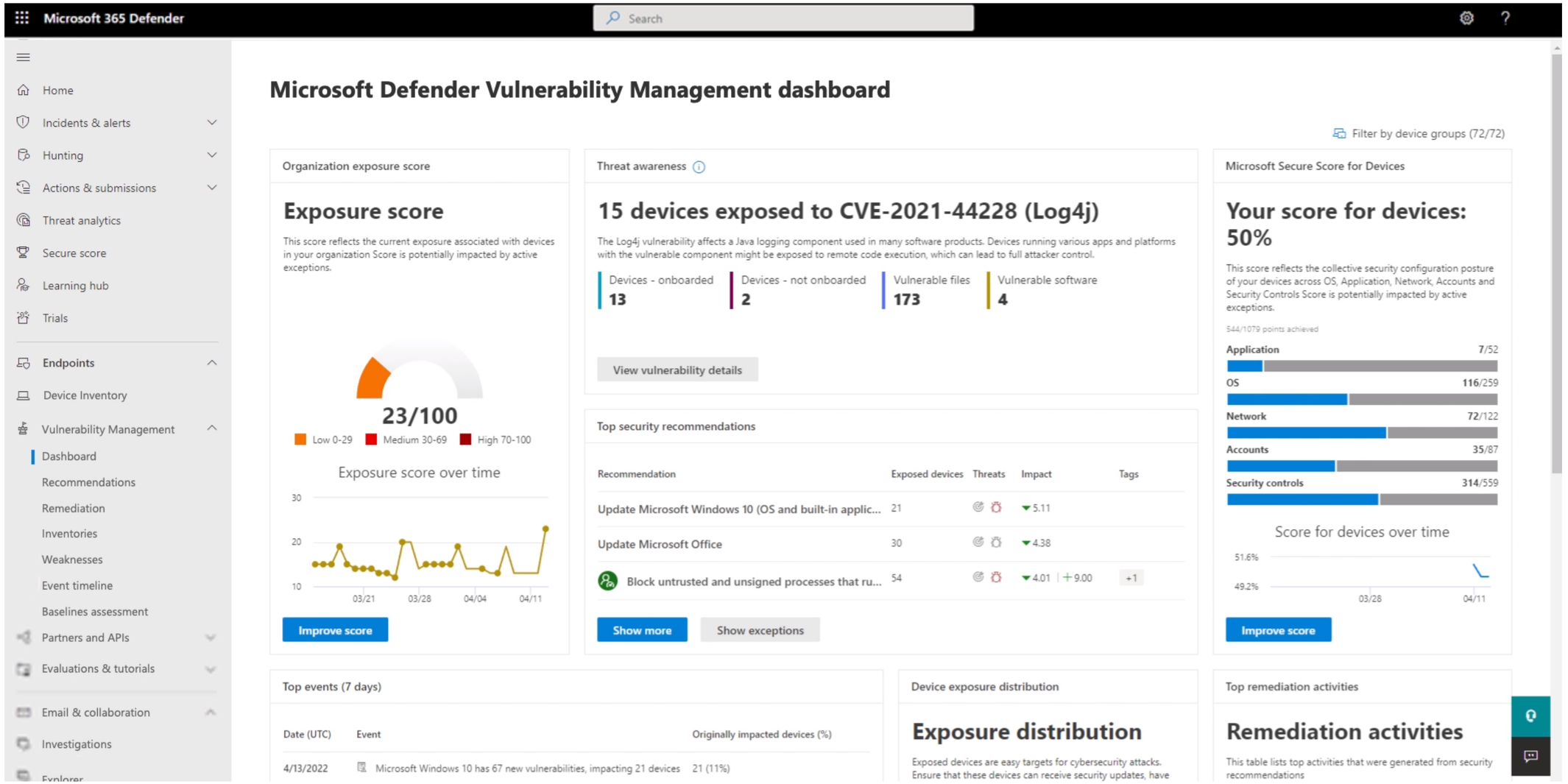
Create remediation tasks in Microsoft Intune

Block vulnerable applications for specific device groups

Configure mitigations

Real-time monitoring of remediation activities

Microsoft Defender Vulnerability Management Dashboard



Source: https://www.microsoft.com/security/business/threat-protection/microsoft-defender-vulnerability-management

Microsoft Defender Threat Intelligence

Microsoft Defender Threat Intelligence (Defender TI)

Microsoft Defender Threat Intelligence (Defender TI) is a platform that streamlines triage, incident response, threat hunting, vulnerability management, and cyber threat intelligence analyst workflows when conducting threat infrastructure analysis and gathering threat intelligence.

Analysts spend a significant amount of time on data discovery, collection, and parsing, instead of focusing on what actually helps their organization defend themselves--deriving insights about the actors through analysis and correlation.

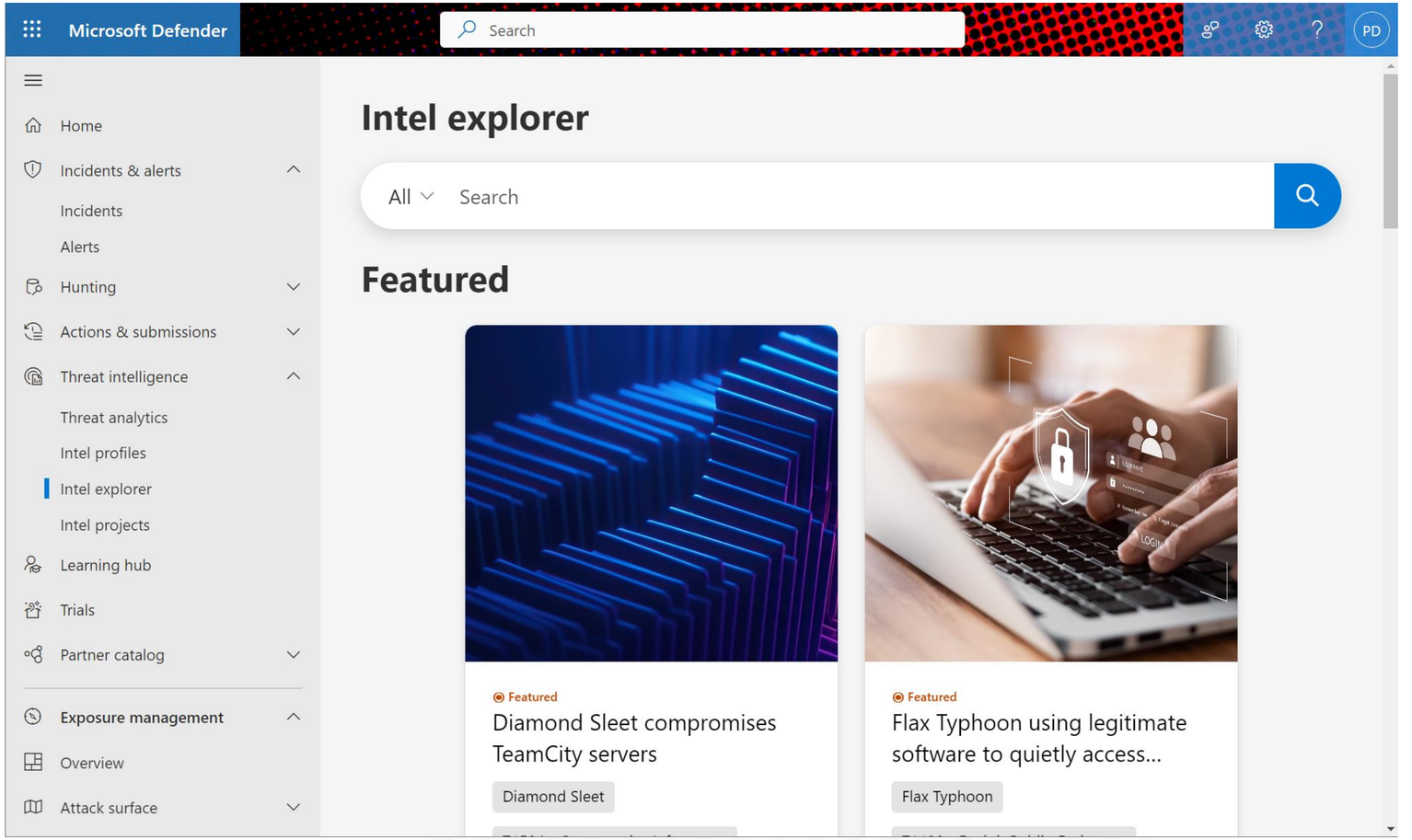
https://learn.microsoft.com/en-us/defender/threat-intelligence/what-is-microsoft-defender-threat-intelligence-defender-ti

Defender TI articles

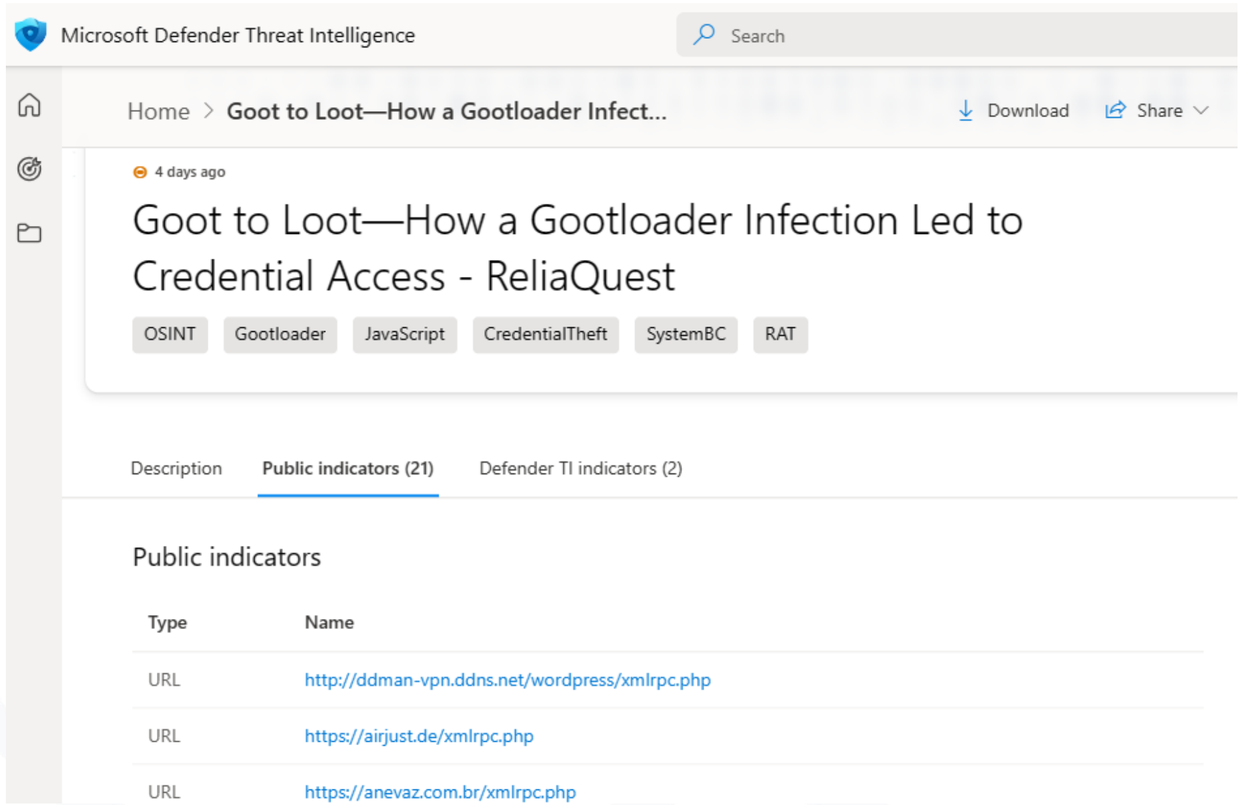
Narratives by Microsoft that provide insights into:

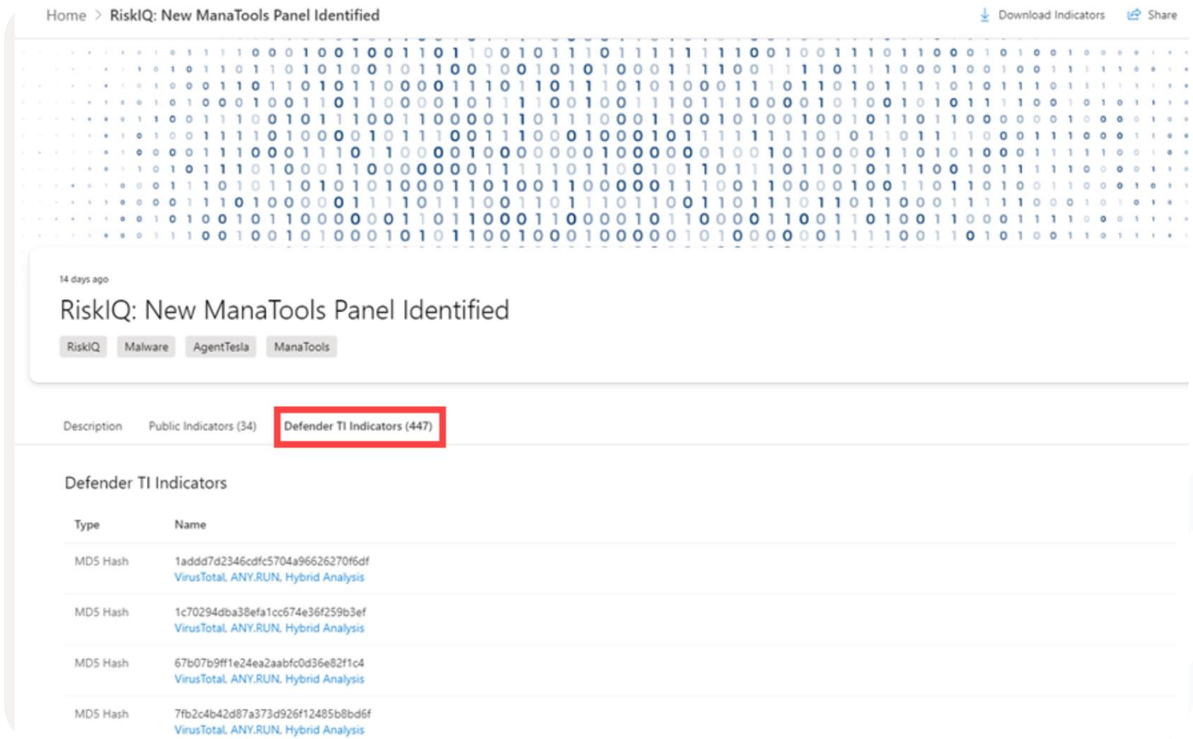
- Threat actors
- Tooling
- Attacks
- Vulnerabilities

Link to actionable content and key indicators of compromise



Indicators



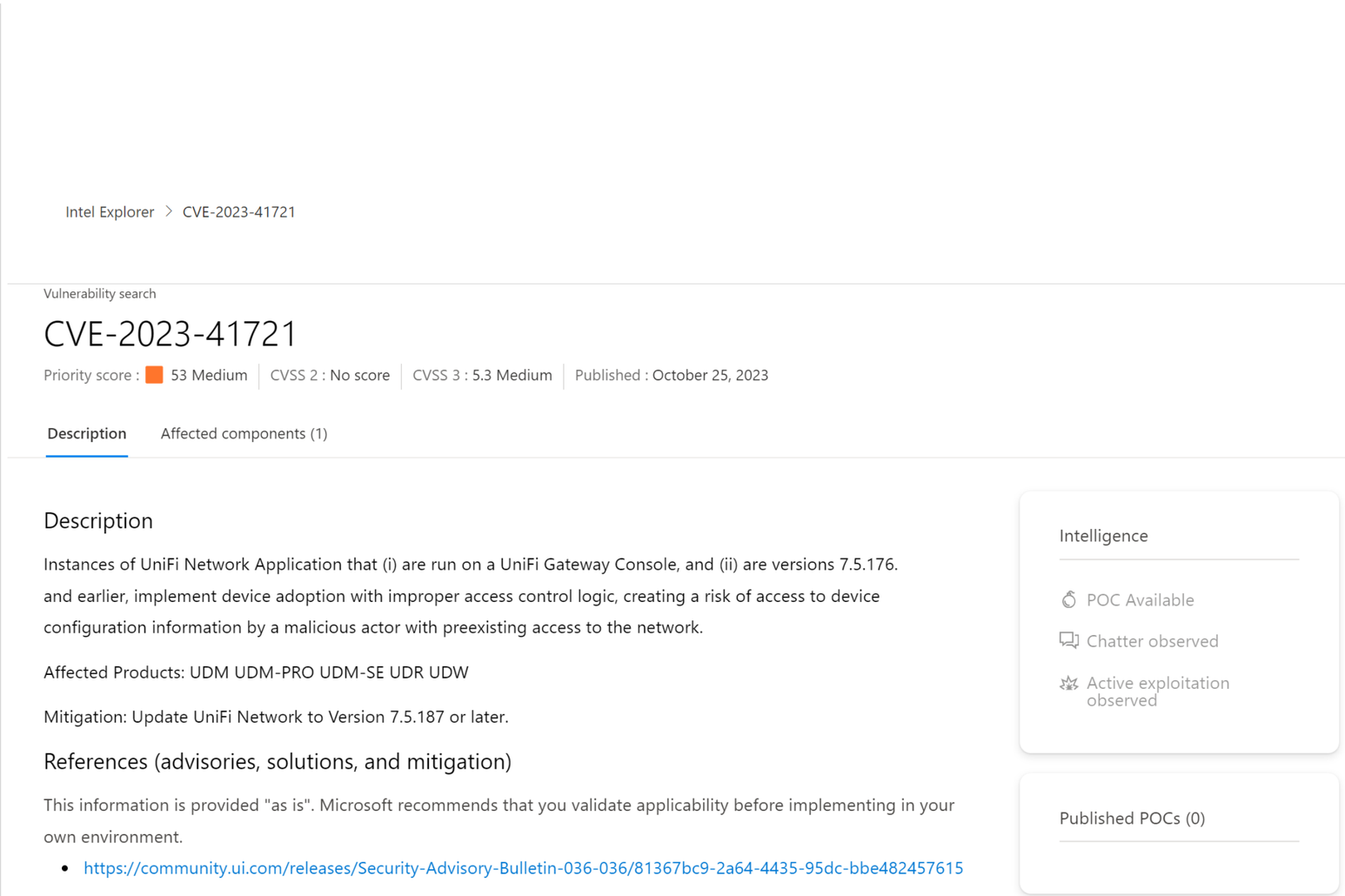


Source: https://learn.microsoft.com/en-us/defender/threat-intelligence/what-is-microsoft-defender-threat-intelligence-defender-ti

Defender TI includes a database of CVE

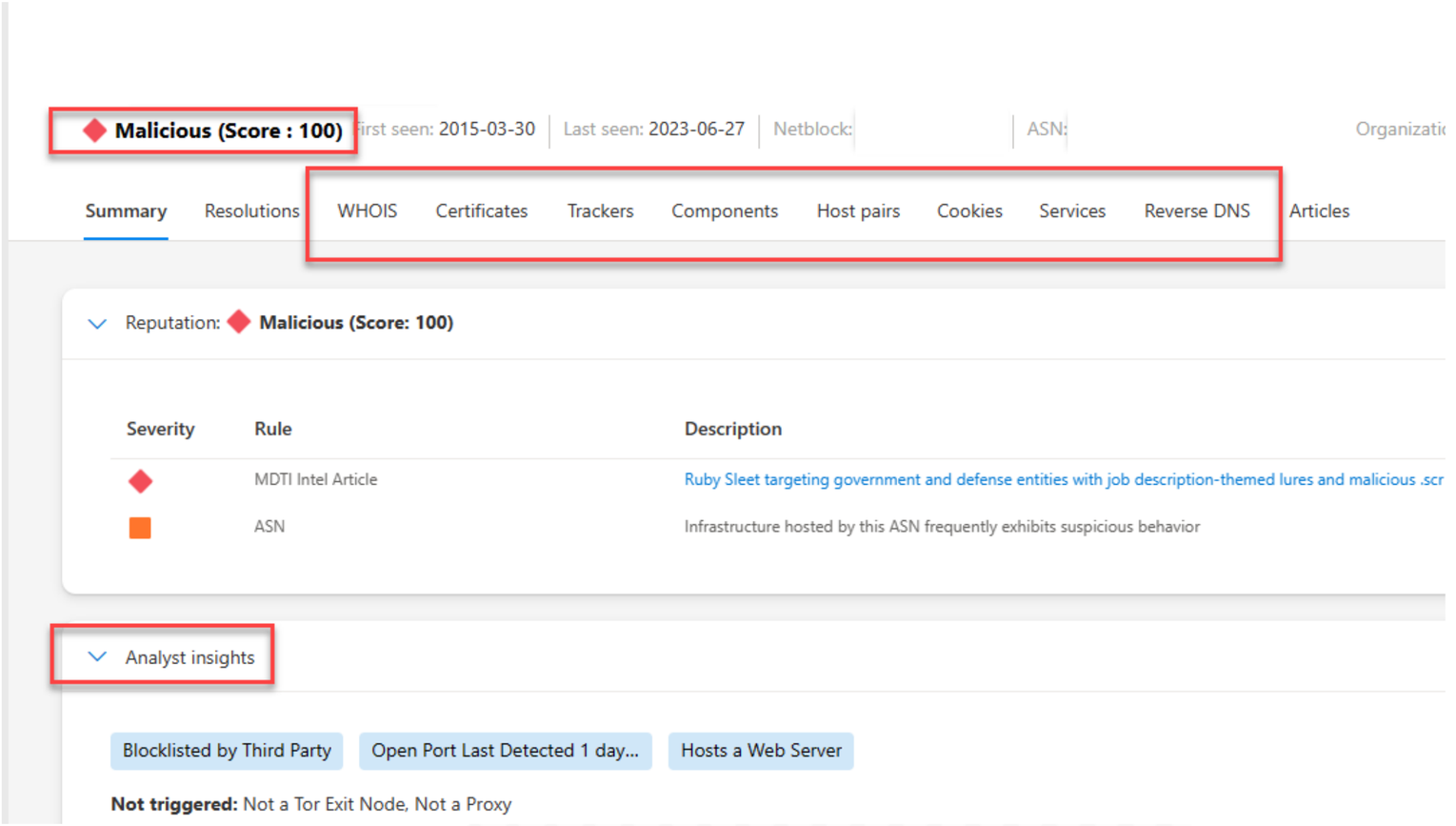
Common vulnerabilities and exposures

Allows you to quickly find information on CVE including key context and priority score



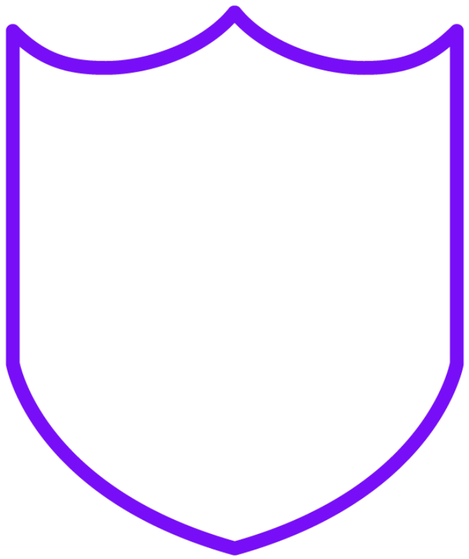
Data sets give you access to search for any domain, IP and find information from a wide variety of sources

Defender TI provides reputation scoring and analyst insights



Microsoft Security Copilot

Microsoft Security Copilot



Amplify your security team with the power of AI

Combines the power of large language models (LLMs) with a security-specific model from Microsoft

- Security specific model is trained by Microsoft and over 65 trillion daily signals

Integrates with Microsoft Defender XDR and Microsoft Sentinel

Incident Response

<Vlad will insert MS provided short video in post editing similar as in Copilot course>

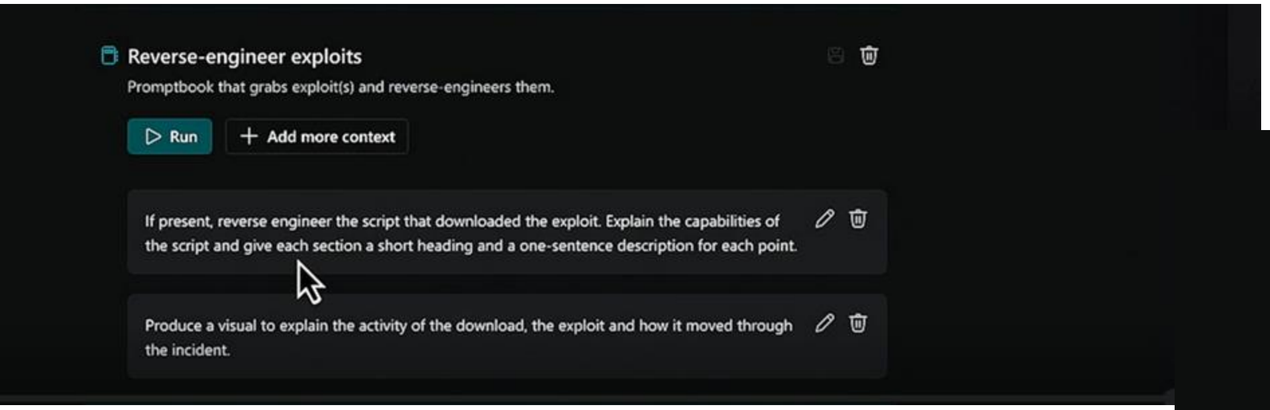
Threat Hunting

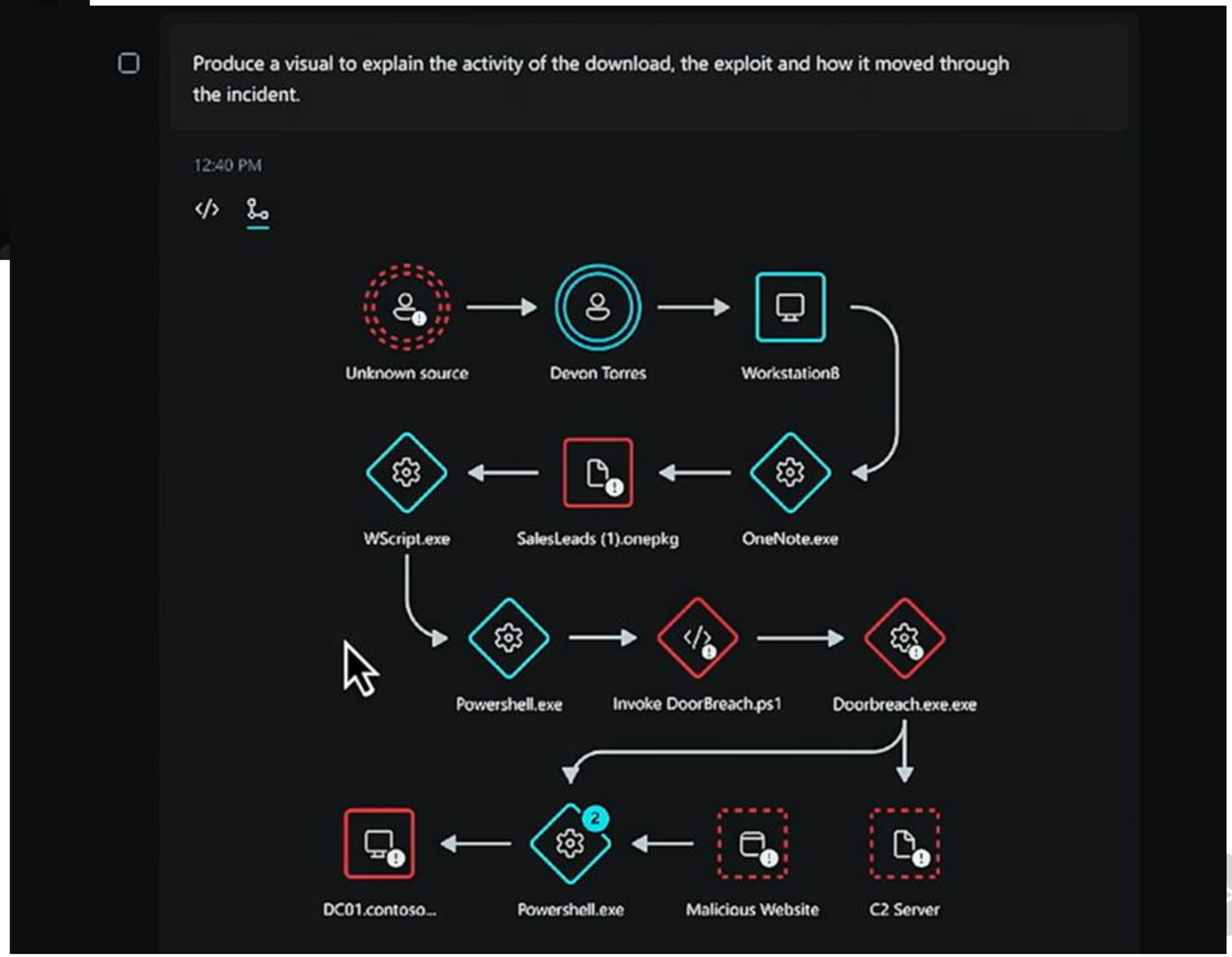
<Vlad will insert MS provided short video in post editing similar as in Copilot course>

Security Reporting

<Vlad will insert MS provided short video in post editing similar as in Copilot course>

Reverse Engineering





Module Conclusion

- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Microsoft Defender Vulnerability Management
- Microsoft Defender Threat Intelligence
- Microsoft Security Copilot

Up Next:

Discover and Control Shadow IT with Defender for Cloud Apps