Introduction to Microsoft Defender XDR

Vlad Catrinescu

Microsoft MVP | Independent Consultant

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

Overview

Introduction to Microsoft Defender XDR

Microsoft Defender portal

Microsoft Secure Score

Introduction to Microsoft Defender XDR

Microsoft Defender XDR

Microsoft Defender XDR is a unified pre- and post-breach enterprise defense suite that natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks.

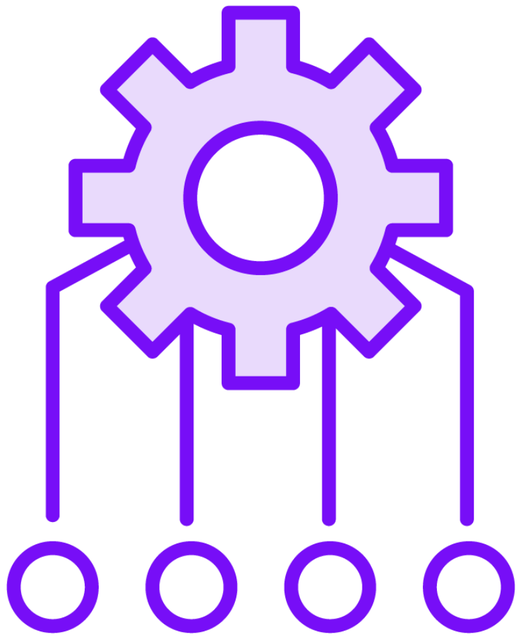
https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender

Microsoft Defender XDR was previously named Microsoft 365 Defender. You might still see references to the old name it in documentation today.

Microsoft Defender XDR Services

- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Microsoft Defender Vulnerability Management
- Microsoft Defender Threat Intelligence
- Microsoft Defender for Cloud Apps

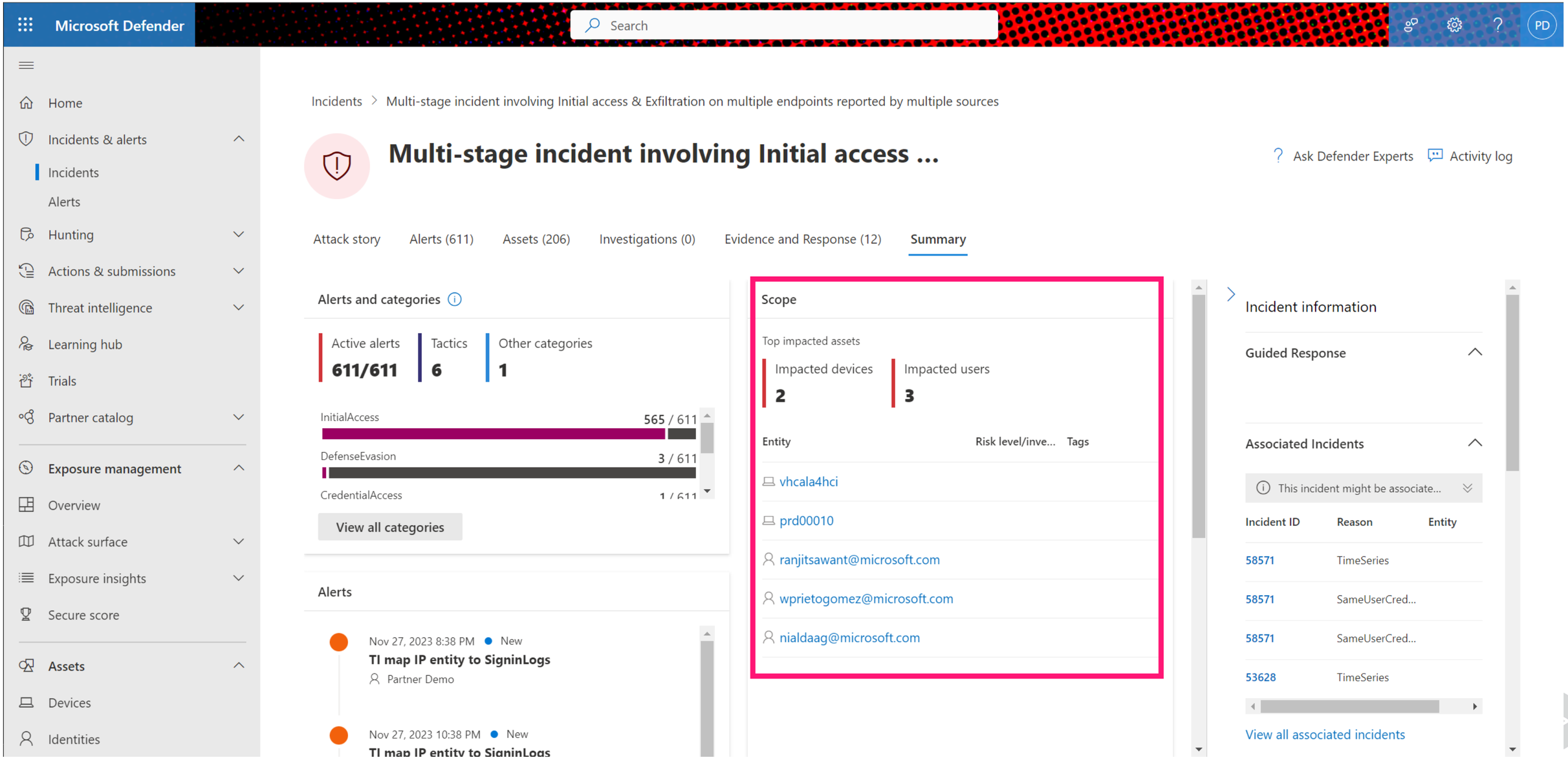
An Integrated Solution



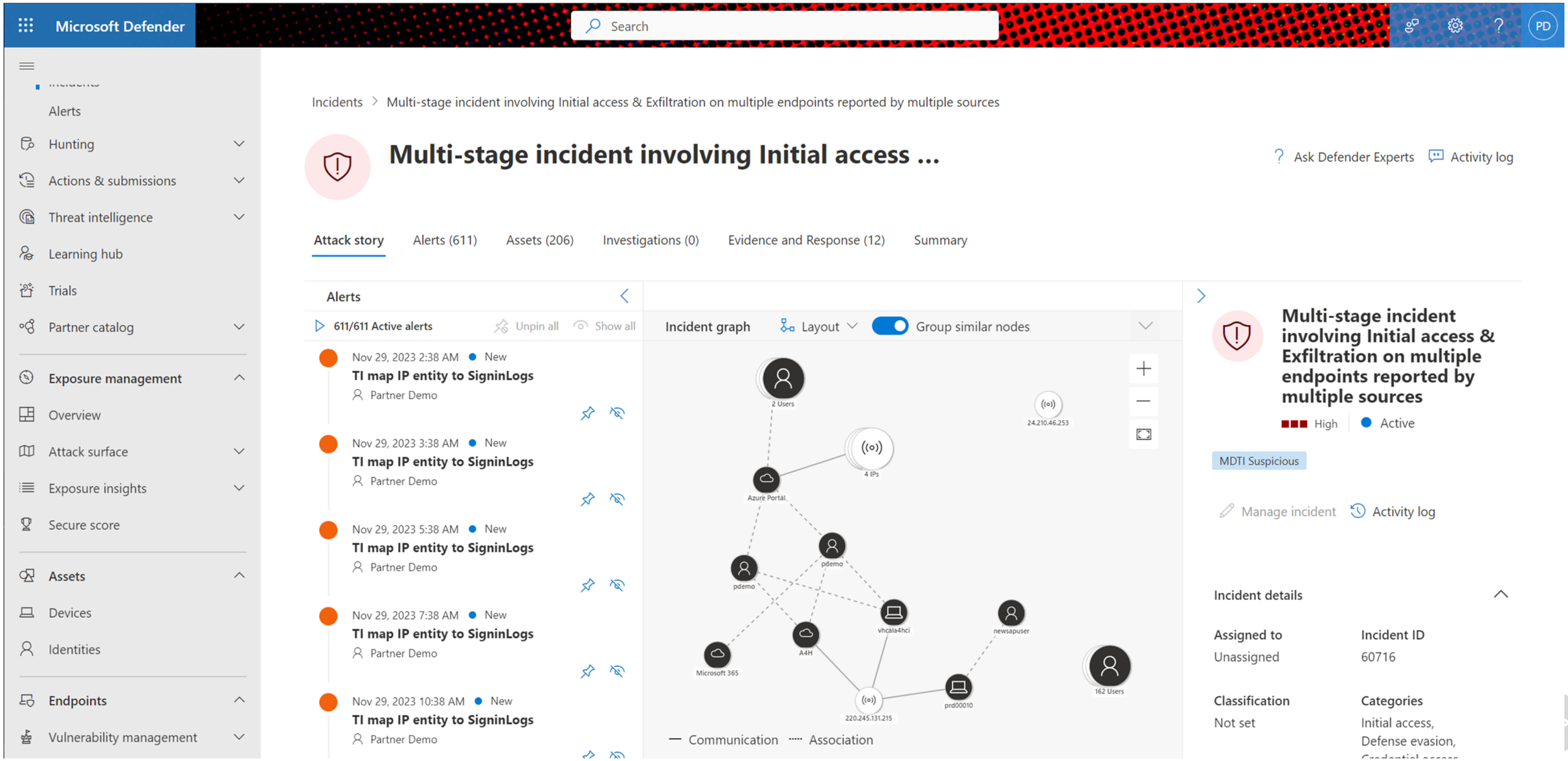
Microsoft Defender XDR is an integrated – cross domain solution

- Stiches together signals from
  - Endpoints
  - Identities
  - Data
  - Applications
- Groups signals from all domains in incidents
  - Allows security teams to see the full picture

Microsoft Defender XDR Incident

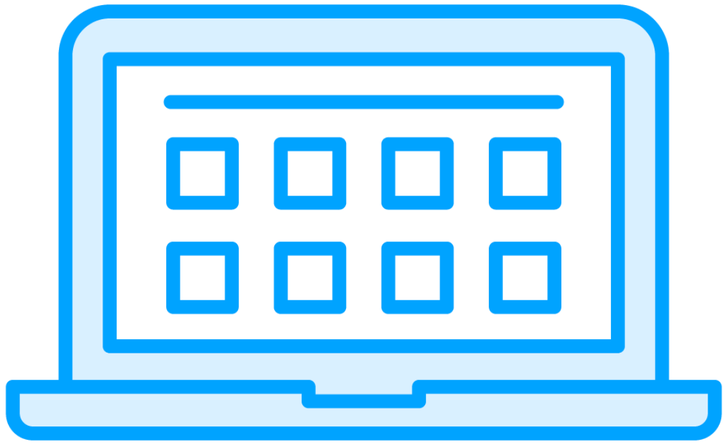


Microsoft Defender XDR Incident



The Microsoft Defender Portal

The Microsoft Defender Portal



Central location for monitoring and managing security services

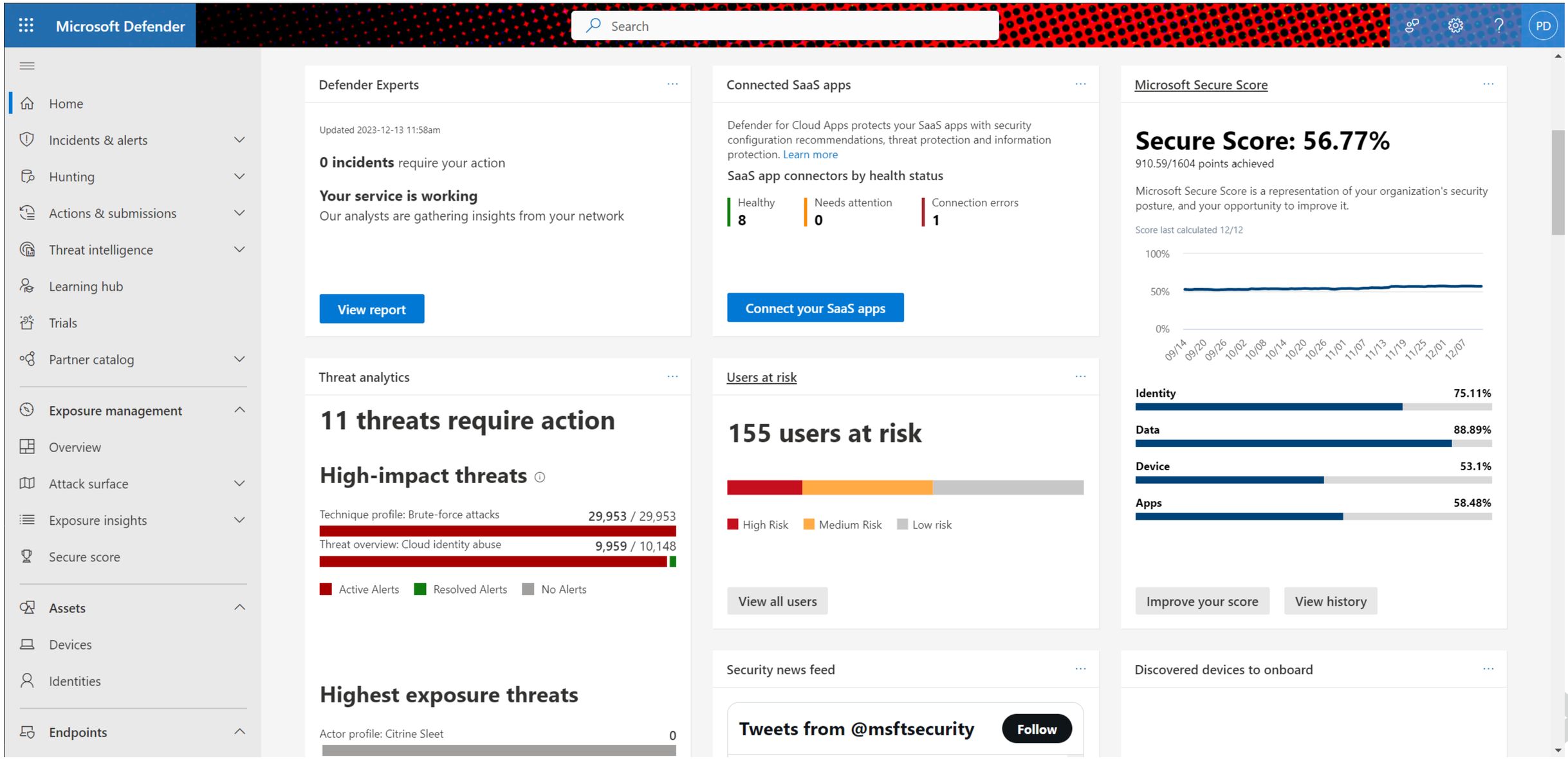
- Identities
- Data
- Devices
- Apps
- Infrastructure

Accessible at https://security.microsoft.com

Only Certain Roles Have Access to the Defender Portal

- Global Administrator
- Security Administrator
- Security Operator
- Security Reader

Microsoft Defender Portal



Microsoft Defender Portal: Customization

Customize your navigation pane

Show or hide navigation items in your navigation pane. Other admins won't see your changes.

Selected items appear in the navigation pane

Don't worry, you can find these hidden items by selecting **Show all** from the navigation pane.

- [x] Select all
- [x] Incidents & alerts
- [x] Hunting
- [x] Actions & submissions
- [x] Threat intelligence
- [x] Learning hub
- [x] Trials
- [x] Partner catalog
- [x] Overview
- [x] Attack surface
- [x] Exposure insights
- [x] Secure score
- [x] Devices
- [x] Identities
- [x] Vulnerability management

Save Cancel

Add cards to your home page

Attack simulation training

Devices with active malware

Intune-managed devices with active, unresolved malware. If a device has multiple malware detections, it may be counted more than once.

Device health

Devices discovered in the last 7 days

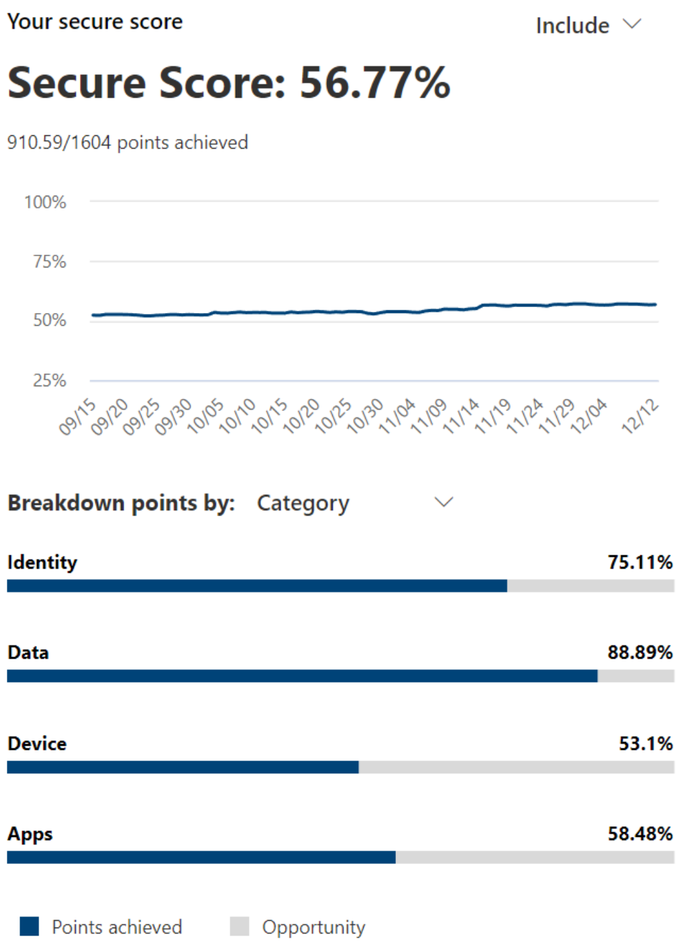
Microsoft Sentinel integration

Microsoft Secure Score

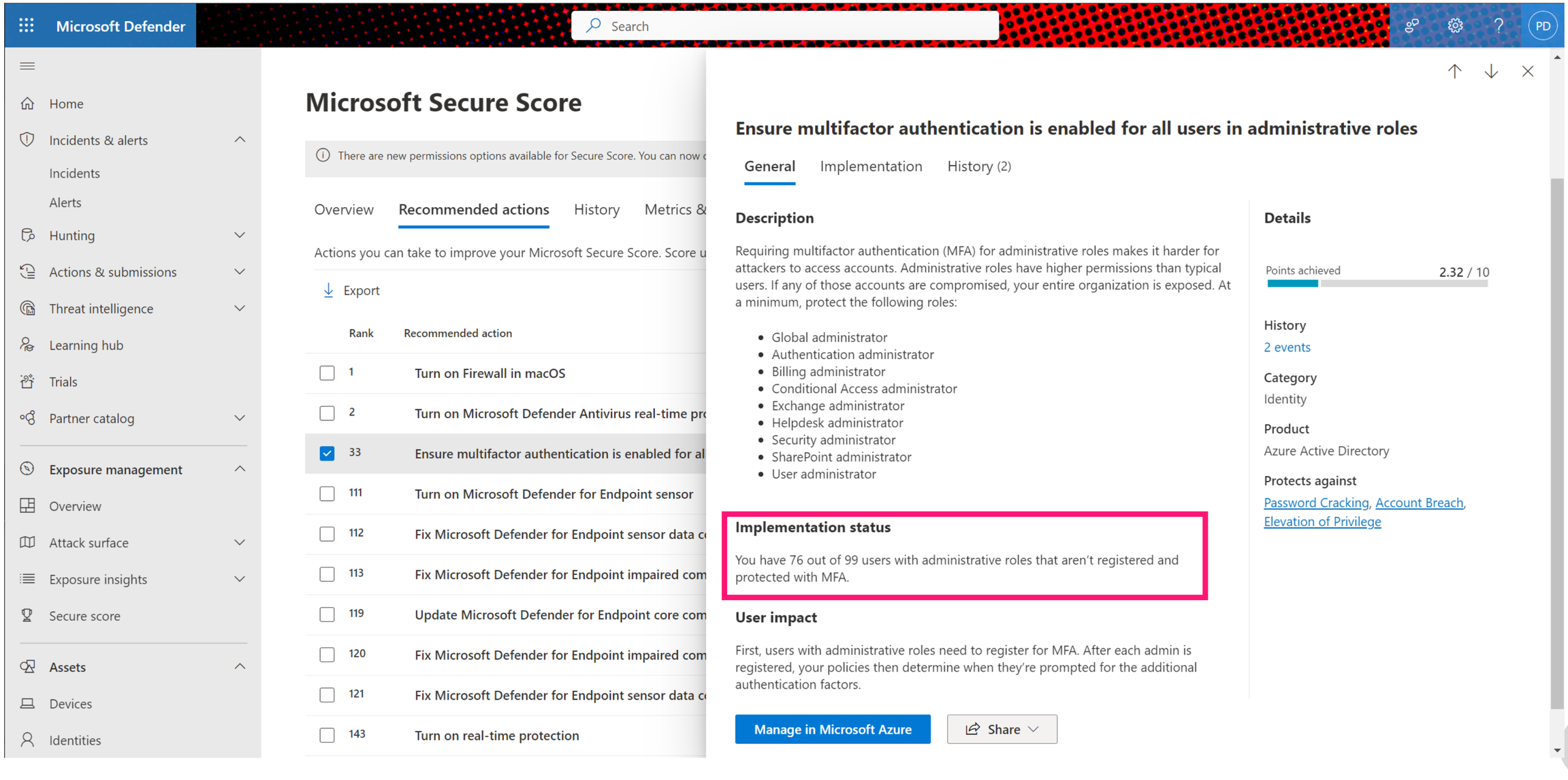
Quick way to understand your security posture

Helps prioritize actions based on potential to reduce risk

- Bigger the security impact – more points



Microsoft Secure Score Recommendation



Products included in Secure Score

Currently there are recommendations for the following products:

- App governance
- Microsoft Entra ID
- Citrix ShareFile
- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office
- Docusign
- Exchange Online
- Github
- Microsoft Defender for Cloud Apps
- Microsoft Information Protection
- Microsoft Teams
- Okta
- Salesforce
- ServiceNow
- SharePoint Online
- Zoom

Secure Score includes recommendations for both Microsoft and third-party products

Microsoft keeps adding supported products

Check out the latest available products at

- https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score#products-included-in-secure-score

Demo

Microsoft Defender portal

Microsoft Secure Score

Module Conclusion

Introduction to Microsoft Defender XDR

- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Microsoft Defender Vulnerability Management
- Microsoft Defender Threat Intelligence
- Microsoft Defender for Cloud Apps

Microsoft Defender Portal

- Central location to manage the security settings of your organization

Microsoft Secure Score

- Quick way to understand your security posture

Up Next:

Extended Detection and Response with Microsoft Defender XDR