Introducing Microsoft 365 Defender

At the end of this episode, I will be able to:

1. Describe Microsoft 365 Defender

Learner Objective: *Describe Microsoft 365 Defender*

Description: In this episode, you will learn the basics about Microsoft 365 Defender and what powers this security solution from Microsoft.

- Microsoft 365 Defender is a unified pre- and post-breach enterprise defense suite.
- Microsoft 365 Defender natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks.
- Microsoft 365 Defender works with:

    - MS Defender for Endpoint
    - MS Defender for Office 365
    - MS Defender for Identity
    - MS Defender for Cloud Apps
    - MS Defender for Vulnerability Management
    - Azure Active Directory Identity Protection
    - Microsoft Data Loss Prevention
    - App Governance

- A great feature of the MS 365 Defender is the ability to correlate alerts from all of these different products
- Another selling point is automated remediations to stop attacks and heal effected components
- Seeks to protect:

    - Endpoints
    - Assets
    - Email
    - Collaboration
    - Identities
    - Applications

- The product includes:

    - Single pane of glass
    - Combined incidents queue
    - Automatic response to threats
    - Self-healing
    - Cross-product threat hunting

Additional Resources:

What is Microsoft 365 Defender
https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender?view=o365-worldwide