Respond to Threats Identified in Threat Analytics

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

1. Review and respond to threats identified in threat analytics

Learner Objective: *Respond to threats*

Description: In this episode, you will learn to review and respond to threats that might appear in the Microsoft 365 Defender dashboard.

- A threat intelligence solution that offers:

    - Active threat actors and their campaigns
    - Popular and new attack techniques
    - Critical vulnerabilities
    - Command attack surfaces
    - Prevalent malware

- High impact threats - greatest potential for harm
- High exposure threats - ones your assets are most vulnerable to
- This helps us:

    - Identify and react to emerging threats
    - Learn if you're currently under attack
    - Assess the impact of the threat to your assets
    - Review your resilience against or exposure to the threats
    - Identify the mitigation, recovery, or prevention actions you can take to stop or contain the threats

- Each threat analytics report provides information in sections:

    - Overview
    - Analyst report
    - Related incidents
    - Impacted assets
    - Prevented email attempts
    - Exposure and mitigations

- You can set up email notifications for report updates

Additional Resources:

Threat analytics in Microsoft 365 Defender
https://learn.microsoft.com/en-us/microsoft-365/security/defender/threat-analytics?view=o365-worldwide