Respond to Alerts in MS 365 Defender

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

1. Review and respond to security incidents and alerts in Microsoft 365 Defender

Learner Objective: *Respond to security incidents and alerts*

Description: In this episode, you will learn to review and respond to alerts that can appear in Microsoft 365 Defender. You will also learn how Microsoft 365 Defender correlates alerts into incidents. You also learn how to respond to and investigate these incidents.

- Alerts are are created by services and apps when they detect suspicious or malicious activity.
- Microsoft 365 Defender automatically aggregates the alerts and the associated information into what is called an incident.
- Grouping alerts into incidents helps you see:
    - Where the attack started
    - What tactics were used
    - How far the attack has done into your tenant
    - The scope of the attack
    - All of the data associated with the attack
- Incidents offer tabs for more details:
    - Attack story
    - Alerts
    - Assets
    - Investigations
    - Evidence and response
    - Summary

Additional Resources:

Investigate and Respond with Microsoft 365 Defender
https://learn.microsoft.com/en-us/microsoft-365/security/defender/incident-response-overview?view=o365-worldwide

Incident Response with Microsoft 365 Defender
https://learn.microsoft.com/en-us/microsoft-365/security/defender/incidents-overview?view=o365-worldwide