Mitigate incidents using Microsoft 365 Defender Intro

By: Ryan Stewart

Learn how the Microsoft 365 Defender portal provides a unified view of incidents from the Microsoft 365 Defender family of products.

Learning objectives

Upon completion of this module, the learner will be able to:

- Manage incidents in Microsoft 365 Defender
- Investigate incidents in Microsoft 365 Defender
- Conduct advanced hunting in Microsoft 365 Defender

Introduction

Microsoft Defender XDR is a comprehensive enterprise defense suite designed for both pre- and post-breach scenarios. It seamlessly integrates detection, prevention, investigation, and response capabilities across various domains, including endpoints, identities, email, and applications, providing a unified defense against sophisticated cyber attacks.

The integrated **Microsoft Defender XDR** solution empowers security professionals by streamlining the coordination of threat signals received by products like Defender for Endpoint, Defender for Identity, and Microsoft Defender for Cloud Apps. This unified approach enables security teams to comprehensively assess the scope and impact of a threat, determining its point of entry, affected areas, and current impact on the organization.

As a **Security Operations Analyst** in a company that has implemented Microsoft Defender XDR solutions, including the aforementioned components, your role involves consolidating related alerts from all these solutions into a single incident view. This consolidated view allows you to analyze the incident's complete impact and conduct a root cause investigation efficiently. **Leveraging the Microsoft Defender portal**, which offers a unified perspective on incidents and actions taken, enhances your ability to manage and respond to security incidents effectively.