Section Introduction, SIEM

In the first section of the SIEM domain, we're going to cover the history of SIEM, and how the two components, SIM and SEM, come together to provide a platform that allows central logging for an organizations assets so that security analysts can identify and respond to security events and suspicious behaviour on specific systems and across multiple networks in one panel.

LEARNING OBJECTIVES

By the end of this section of the SIEM domain, you will be able to:

- Understand what Security Information Management (SIM) is, and how it features within SIEM.
- Understand what Security Event Management (SEM) is, and how it features within SIEM.
- Understand what SIEM is, and how it's used by security teams to aggregate, correlate, and normalise logs from a wide range of sources such as proxies, firewalls, IDPS, anti-virus, EDR, and various system logs.