Section Introduction, Detection & Analysis

This section of the IR domain will cover how incidents are detected via different tools such as SIEM and IDPS, and how potential and confirmed incidents are analyzed via log and PCAP analysis to gather indicators of compromise which can be used in threat exposure checks and shared with other organizations.

LEARNING OBJECTIVES

By the end of this section you will have achieved the following objectives:

- Understand common events and incidents faced by organizations.
- Understand what baselines are, and how they can be used to detect unusual behavior from users, systems, and network traffic.
- Understand and perform log analysis and PCAP analysis.