Event_Documentation_Template

Overview

Documentation of events ensures accountability and transparency in SOC operations.

An event template provides a consistent structure for recording incident details such as event type, severity, affected systems, and analyst notes.

Learning Approach

Students should learn the key fields required in documentation: event ID, timestamp, event description, and mitigation steps.

Practice filling in event records using simulated alerts to build consistency.

Example / Use-Case

When an endpoint triggers a malware detection alert, an analyst documents the event ID, time detected, malware type, and response actions taken.