Alert_Rule_Configuration

Overview

Alert rules define the conditions under which the SOC is notified of suspicious events.
Well-configured alerts are crucial to effective security monitoring.

Poorly tuned alerts lead to false positives or missed threats, overwhelming analysts or leaving them blind to attacks.

Learning Approach

Students should learn the balance between sensitivity and specificity when creating rules.

Studying common detection use-cases such as brute force, privilege escalation, and unusual traffic helps in rule formulation.

Example / Use-Case

An alert rule triggers when more than 10 failed logins occur within 5 minutes. This helps detect brute-force attempts before compromise.