Section Introduction, Correlation

Blue Team Level 1 Certification (Standard) > SI4) Correlation > Section Introduction, Correlation IN PROGRESS

This section of the SIEM domain will introduce you to SIEM correlation, and how the aggregated data is used to identify security events, incidents, and anomalies, generating alerts that can be investigated by human analysts. We will cover the normalization process, the application of regular expression (regex) queries, and how SIEM rules are written to aid security monitoring and detection.

LEARNING OBJECTIVES

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

- Understand what normalization means in regard to SIEM, and how aggregated logs can be normalized.
- Understand why regex is used in security, and be able to write regex queries.
- Develop your understanding of how SIEMs actually detect security events using rulesets.

< Previous Lesson

Mark Complete ✓

Next Topic >

Back to Lesson