

**Blue Team Level 1 Certification  
(Standard)**

10 Topics 5 Quizzes

☐ DF3) Digital Evidence Collection

8 Topics 1 Quiz

☐ DF4) Windows Investigations

3 Topics 3 Quizzes

☐ DF5) Linux Investigations

4 Topics 2 Quizzes

☐ DF6) Volatility

3 Topics 1 Quiz

☐ DF7) Autopsy

4 Topics 1 Quiz

**SECURITY INFORMATION AND EVENT  
MANAGEMENT DOMAIN**☐ SI1) Introduction to SIEM

7 Topics 1 Quiz

☐ SI2) Logging

6 Topics 2 Quizzes

☒ SI3) Aggregation

2 Topics 1 Quiz

[Section Introduction, Aggregation](#)☐ Log Aggregation Explained☐ Activity) End of Section Review,  
Aggregation☐ SI4) Correlation

6 Topics 1 Quiz

☐ SI5) Using Splunk

5 Topics 2 Quizzes

**INCIDENT RESPONSE DOMAIN**☐ IR1) Introduction to Incident Response

# Section Introduction, Aggregation

Blue Team Level 1 Certification (Standard) &gt; SI3) Aggregation &gt; Section Introduction, Aggregation

**IN PROGRESS**

This section of the SIEM domain will introduce you to aggregation, and how it is used to collect and manage logs coming from a range of log sources. In large businesses the volume of incoming logs can be extremely large, and the SIEM needs to be able to ingest and store these in a functional manner, and that's where aggregation comes in. Using techniques such as deduplication and combining logs we can reduce the total storage needed.

## LEARNING OBJECTIVES

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

- Understand what aggregation is, and the role it plays in SIEM.
- Understand the different formats of data going into a SIEM.

[Previous Lesson](#)[Mark Complete](#) ✓[Back to Lesson](#)[Next Topic](#) >