

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

2 Topics 1 Quiz

SI(4) Correlation

6 Topics 1 Quiz

SI(5) Using Splunk

5 Topics 2 Quizzes

INCIDENT RESPONSE DOMAIN

IR(1) Introduction to Incident Response

8 Topics 1 Quiz

Section Introduction, Incident Response

What is Incident Response?

Why is Incident Response Needed?

Security Events vs Security Incidents

Incident Response Lifecycle (NIST SP 800 61r2)

CSIRT and CERT Explained

Further Reading Material, Incident Response

[Incident Response Glossary](#)

Activity) End of Section Review, Incident Response

IR(2) Preparation Phase

10 Topics 2 Quizzes

IR(3) Detection and Analysis Phase

Incident Response Glossary

Blue Team Level 1 Certification (Standard) > IR(1) Introduction to Incident Response > Incident R...

IN PROGRESS



We have created a PDF that contains all of the terms and phrases used in this domain of Blue Team Level 1. While we work to ensure we declare full names of acronyms before they're used in a lesson, this document may help you remember them better and make studying easier. This PDF can either be viewed digitally or printed.

[Download BTL1_Incident_Response_Glossary.pdf](#)

[Previous Topic](#)

[Mark Complete](#)

[Back to Lesson](#)

[Privacy & Cookies Policy](#)

