

Blue Team Level 1 Certification
(Standard)

2 Topics 1 Quiz

SI4) Correlation

6 Topics 1 Quiz

SI5) Using Splunk

5 Topics 2 Quizzes

INCIDENT RESPONSE DOMAIN

IR1) 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

IR2) Preparation Phase

10 Topics 2 Quizzes

IR3) Detection and Analysis Phase

7 Topics 4 Quizzes

IR4) Containment, Eradication, and Recovery
Phase

5 Topics 1 Quiz

IR5) Lessons Learned and Reporting

7 Topics

IR6) MITRE ATT&CK

13 Topics 2 Quizzes

BTL1 EXAM

Activity) End of Section Review,
Incident Response

Blue Team Level 1 Certification (Standard) > IR1) Introduction to Incident Response > Activity) End of Section Re...

Introduction to Incident Response
END OF SECTION REVIEW

This quiz has been created to test the knowledge we've covered in this section of the course. You will answer a number of questions and select or provide the correct answer. If you get stuck, you can use the Hints feature for some guidance. You are able to retake this quiz as many times as you wish.

KNOWLEDGE REVIEW

What benefits does an incident response program bring to an organization?

- ☐ Ensuring a timely recovery of affected systems to ensure business operations continuity
- ☐ Reducing the damage that can be done by successfully cyberattacks by containing and limiting the actions conducted by attackers
- ☐ Learning from previous incidents to improve overall defenses, making it easier to protect against and contain future attacks
- ☐ All of the above

Check

Privacy & Cookies Policy

