

Blue Team Level 1 Certification (Standard) <

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

☐ 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

☐ 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

☐ Section Introduction, CER

☐ Incident Containment

☐ Taking Forensics Images

☐ Identifying and Removing Malicious Artifacts

☐ Identifying Root Cause and Recovery

☒ Activity) End of Section Review, CER

☐ IR5) Lessons Learned and Reporting

7 Topics

☐ IR6) MITRE ATT&CK

13 Topics 2 Quizzes

BTL1 EXAM

☐ Exam Preparation

☐ Using RDP and SSH

☐ How to Start Your Exam


29% COMPLETE 86/287 Steps

Activity) End of Section Review, CER

Blue Team Level 1 Certification (Standard) > IR4) Containment, Eradication, and Recovery Phase > Activity) End ...

Incident Response Domain

END OF SECTION REVIEW



Congratulations on completing this section of the Incident Response domain! This knowledge review is designed to test what you have learned about containing an incident, removing malicious artifacts, and remediating any affected systems so they can't be exploited in the same way again. You will be able to re-take the quiz as many times as you like, but you will need a score of 70% or above to pass. It is important that you feel confident answering these questions to ensure that you can complete tasks within the BTL1 exam and pass to become certified. If you get stuck, use the **Hint** feature!

Good luck!

KNOWLEDGE REVIEW

[1/5] Match the incident response activity descriptions with the appropriate headings.

Sort elements

Patching and hardening systems, deploying new IDPS rules and IOC watchlists.

Identifying and removing malicious artifacts such as attacker-created files and user accounts.

Isolating infected systems from the network by placing them on their own VLAN.

Recovery	
Containment	
Eradication	

Check

Privacy & Cookies Policy

