

Blue Team Level 1 Certification
(Standard)

5 Topics 2 Quizzes

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

Section Introduction, Preparation

Preparation: Incident Response Plan

Preparation: Incident Response Teams

Preparation: Asset Inventory and Risk Assessments

Prevention: DMZ

Prevention: Host Defenses

Prevention: Network Defenses

Legacy Activity) Setting up a Firewall

Prevention: Email Defenses

Prevention: Physical Defenses

Prevention: Human Defenses

Activity) End of Section Review, Preparation

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

Exam Preparation

Using RDP and SSH

How to Start Your Exam

Activity) End of Section Review,
Preparation

Blue Team Level 1 Certification (Standard) > IR2) Preparation Phase > Activity) End of Section Review, Preparation

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 the preparation stage of the incident response lifecycle, including the security controls that organizations use to reduce the likelihood of incidents occurring. You will be able to re-take the quiz as many times as you like, but 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] What is the name given to a network that is created between the internet and a private network?

☐ Honeynet☐ Secure Zone☐ DMZ☐ Buffer Net

Hint

Check

Privacy & Cookies Policy

