

Blue Team Level 1 Certification
(Standard)

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

☐ 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

☐ Exam Preparation☐ Using RDP and SSH☐ How to Start Your Exam

Further Reading Material, Incident Response

Blue Team Level 1 Certification (Standard) > IR1) Introduction to Incident Response > Further R...

IN PROGRESS

Incident Response Domain FURTHER READING



This lesson is designed to provide students with additional reading material on different aspects of incident response in case you didn't fully understand a specific part of the course, or you just want to read more about this area of cybersecurity to strengthen your skills ready for the BTL1 practical exam. **We suggest that students come back to this lesson once they have completed this domain.**

If you have any resources you would like us to add to this list, please reach out to us via email at BTL1@securityblue.team with the subject line "Incident Response Domain Further Reading".

RESOURCES

- Incident Response Resources (Runbooks, books, frameworks, careers)
[// https://www.incidentresponse.com/resources/](https://www.incidentresponse.com/resources/)
- Incident Response Resources From Infosec Institute
[// https://resources.infosecinstitute.com/category/incident-response-resources/](https://resources.infosecinstitute.com/category/incident-response-resources/)
- A Curated List of Tools for Incident Response
[// https://github.com/meirwah/awesome-incident-response](https://github.com/meirwah/awesome-incident-response)
- Incident Response Tools by AT&T Cybersecurity
[// https://cybersecurity.att.com/resource-center/ebook/insider-guide-to-incident-response/incident-response-tools](https://cybersecurity.att.com/resource-center/ebook/insider-guide-to-incident-response/incident-response-tools)
- Proactive Incident Response by Secureworks
[// https://www.secureworks.com/centers/proactive-incident-response](https://www.secureworks.com/centers/proactive-incident-response)
- Incident Handler's Handbook by SANS
[// https://www.sans.org/reading-room/whitepapers/incident/paper/33901](https://www.sans.org/reading-room/whitepapers/incident/paper/33901)
- Ultimate Guide to Cybersecurity Incident Response by TechTarget
[// https://searchsecurity.techtarget.com/Ultimate-guide-to-incident-response-and-management](https://searchsecurity.techtarget.com/Ultimate-guide-to-incident-response-and-management)
- A Beginners Guide to Open Source Incident Response Tools and Resources by Cybersecurity Insiders
[// https://www.cybersecurity-insiders.com/beginners-guide-to-open-source-incident-response-tools-and-resources/](https://www.cybersecurity-insiders.com/beginners-guide-to-open-source-incident-response-tools-and-resources/)

< Previous Topic

Mark Complete ✓

Back to Lesson

Next Topic >