

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

☐ 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

Why is Incident Response Needed?

Blue Team Level 1 Certification (Standard) > IR1) Introduction to Incident Response > Why is Inc...

IN PROGRESS



Incident response benefits the wider business by reducing the impact of successful attacks and allowing business operations to remain as uninterrupted as possible. It's impossible to completely prevent any incident from occurring, so incident response helps to minimize the impact. Successful cyberattacks can have a number of adverse consequences, such as data breaches, events where information an organization stores is exfiltrated. Data breaches can cause immense damage in terms of lost customer trust and business, monetary losses from recovering damaged or infected systems, stock prices dropping, hiring external security teams to help contain the breach, and legal or regulatory fines such as those under legislation including the [General Data Protection Regulation](#) (for EU countries, or organizations that process data belonging to EU data subjects). Just to give you an example of how heavy GDPR and regulatory fines can be, we have composed a list of some recent breaches:

- Uber fined £385,000 in November 2018 – [read more.](#)
- Equifax fined £500,000 in September 2018 – [read more.](#)
- Marriott proposed fine of £99m in July 2019 – [read more.](#)
- British Airways proposed fine of £183m in July 2019 – [read more.](#)

Legal and regulatory fines can be too much for smaller organizations and can result in them shutting down or having to change how they operate, such as no longer allowing customers from within EU countries.

Incident response isn't just about responding to data breaches, it involves responding to the aftermath of an attack such as:

- Employee credentials being leaked online
- Database leaks
- Malware infections, such as ransomware
- A stolen employee laptop
- Website defacement
- An employee trying to smuggle sensitive data out of the company

Having written plans to follow if these occur helps to reduce the risk by responding and containing the threat appropriately. We will cover incident response plans in the **Preparation: Incident Response Plan** lesson of the next section.

< Previous Topic

Mark Complete ✓

Back to Lesson

Next Topic >

