

Blue Team Level 1 Certification
(Standard)

✓ PA4) Investigating a Phishing Email

8 Topics 2 Quizzes

✓ PA5) Analysing URLs, Attachments, and Artifacts

8 Topics 1 Quiz

○ PA6) Taking Defensive Actions

12 Topics 1 Quiz

○ PA7) Report Writing

7 Topics 1 Quiz

○ PA8) Phishing Response Challenge

3 Topics 1 Quiz

THREAT INTELLIGENCE DOMAIN

○ TI1) Introduction to Threat Intelligence

7 Topics

○ TI2) Threat Actors & APTs

6 Topics 2 Quizzes

○ TI3) Operational Threat Intelligence

7 Topics 1 Quiz

○ TI4) Tactical Threat Intelligence

7 Topics 1 Quiz

○ TI5) Strategic Threat Intelligence

5 Topics 1 Quiz

○ TI6) Malware and Global Campaigns

6 Topics 1 Quiz

DIGITAL FORENSICS DOMAIN

○ DF1) Introduction to Digital Forensics

5 Topics

○ DF2) Forensics Fundamentals

10 Topics 5 Quizzes

○ DF3) Digital Evidence Collection

8 Topics 1 Quiz

○ DF4) Windows Investigations

3 Topics 3 Quizzes

○ DF5) Linux Investigations

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

Preparation: Incident Response Teams

Blue Team Level 1 Certification (Standard) > IR2) Preparation Phase > Preparation: Incident Res...

IN PROGRESS

Incident Response Domain INCIDENT RESPONSE TEAMS



Incident response teams are responsible for handling incidents when they occur. This lesson will cover the need for these specialist teams, who should be included in them, and how they should operate.

WHY DO WE NEED THEM?

A dedicated incident response team is crucial to be able to respond to confirmed incidents properly and reduce the impact they have on the business, working to ensure continuity and reduce costs as a result of the successful attack. By bringing together people with all the skills that are needed, this specialist team can be activated when an incident occurs, minimizing the time that damage can be caused. Larger organizations tend to opt for a full-time staff that focuses purely on preparation, testing, and incident response, whilst smaller organizations may have team members that have other roles but can step up when an incident is discovered.

I.R TEAM MEMBERS

Incident response teams are made up of skilled individuals from a wide range of departments, **not just security analysts!** In this section, we'll cover everyone that *should* be included in an IR team.

Incident Commander

This is the name given to the individual that is in charge of dealing with the incident, typically a dedicated Incident Response Manager. It is their job to coordinate response efforts and ensure communication is maintained between all relevant parties throughout. They will be the point of contact for all departments, and will typically provide periodic updates to management and the C-suite.

Security Analysts

The most obvious individuals that should be included in the team are Security Analysts, individuals with a deep technical understanding of networks, and how to triage and investigate security alerts generated by platforms such as IDPS or SIEM. These guys and girls will provide first-hand analysis of incidents and collect information such as the systems affected, the time, and the specific activity that is happening.

Forensic Analysts

Arguably the most technically-knowledgeable analysts are those with a skill for digital forensics and incident response (also known as DFIR). It is their job to take a deeper dive into the incident, retrieve and preserve digital evidence so that it can be used in court if there is a legal prosecution as a result of the incident.

Threat Intelligence Analysts

As you know from the Threat Intelligence domain, work in this field can help to provide context around an incident, such as working to identify the actor(s) behind the attack, performing further exposure checks using IOCs and artifacts collected by forensic analysts, and relaying intelligence to other organizations so they can prepare for similar attacks to the one currently being dealt with.

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: Assest 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

As mentioned previously, it's not just cybersecurity professionals that should be included in this team. Below is a list of other individuals that should be included.

Management/C-Suite

Having members of the company's management board such as Chief Information Security Officer (CISO), Chief Operations Officer (COO), and Chief Technology Officer (CTO) is important so that responders have the resources they need to both prevent and respond to incidents properly.

Human Resources (HR)

If an employee is the cause of an incident, individuals from the HR department will need to be involved, as they will coordinate the organization's response to discipline the employee, whether that's to take legal action, fire them, or give them a warning.

Public Relations

If an incident affects the public, employees, or customers (such as a data breach) then by law this needs to be announced as soon as possible. The PR department will handle how the news should be announced, what information to include, and who needs to be notified. They will also likely communicate with stakeholders to inform them of any important events.

Legal


Members of this department will provide legal advice, and support forensic analysts, HR, and public relations to ensure that everything that happens is legal and the organization has completed any tasks it is required to do by law, such as notifying affected persons, and ensuring digital evidence is forensically sound.

< Previous Topic

Mark Complete ✓
Back to Lesson

Next Topic >

Privacy & Cookies Policy

Privacy & Terms