

Blue Team Level 1 Certification
(Standard)

5 Topics 1 Quiz

✓ Networking 101

6 Topics 1 Quiz

✓ Management Principles

4 Topics 1 Quiz

PHISHING ANALYSIS DOMAIN

✓ PA1) Introduction to Emails and Phishing

7 Topics 1 Quiz

✓ PA2) Types of Phishing Emails

10 Topics 2 Quizzes

✓ PA3) Tactics and Techniques Used

12 Topics 2 Quizzes

✓ 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

Prevention: Physical Defenses

Blue Team Level 1 Certification (Standard) > IR2) Preparation Phase > Prevention: Physical Defenses

IN PROGRESS

Incident Response Domain PREVENTION: PHYSICAL DEFENSES



It's easy to only focus on cybersecurity controls, but if an attacker can get physical access to a system, it's usually game over. They can plug in malicious USBs, steal components such as hard drives, or damage systems so they can't be used. While this is not typically the responsibility of a cybersecurity team, it is definitely worth covering.

DETERRENTS



Security controls that act as deterrents include warning signs and barbed wire. Their purpose is to deter potential attackers and make them less likely to attempt to gain entry.

- **Warning Signs:** Signs such as "DO NOT ENTER" and "You Are Trespassing" can be enough to make people turn around, as they have been informed that any further activity may be illegal.
- **Fences:** Chain-link metal fences are very common, with barbed or razor wire on top. This creates a barrier that can't easily be climbed over and requires more effort for attackers to bypass, slowing them down and giving more time for them to be detected.
- **Guard Dogs:** Security dogs that are trained to bark and cause distress are a strong deterrent. Despite being highly trained, they still appear to be dangerous in the eyes of the attacker. They are also able to help detain any intruders by holding them down until physical security personnel can apprehend the suspect.
- **Security Guards:** Physical security staff can act as a strong deterrent, showing there is a human presence on the site, and that if intruders try to gain access, it is likely they will get caught. This deterrent is enhanced on sites where armed security personnel are present.
- **Security Lighting:** Lighting is used to prevent low visibility areas caused by darkness, which could allow an intruder to bypass security controls such as CCTV and Security Guards. Lighting the areas in conjunction with cameras is a great deterrent and monitoring.

ACCESS CONTROLS



Access controls are used to prevent unauthorized people from accessing specific areas of a building or area.

- **Mantraps:** These are a slow but effective security control, where an individual wanting to access a protected area must go through an initial door into a small holding room, where they are inspected from a window or

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
 - ☐ 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

camera before the second door is unlocked.

- **Turnstiles/Gates:** This efficient control is very common in office buildings and requires employees to tap their ID pass on a reader, which will unlock the gate and allow them to pass through.
- **Electronic Doors:** These secure doors should be used throughout the facility, to limit the areas that a person can access, based on their role. For example, it is highly unlikely that someone from Human Resources should have access to a Server room. Only allowing certain people in specific areas not only reduces the risk of malicious activity but can also help find the person accountable as the list of potential suspects is much shorter.
- **Security Guards:** Physical security staff is able to check IDs or manually allow employees to access certain areas of a site.

MONITORING CONTROLS



These controls, such as CCTV cameras and intrusion detection systems are implemented to provide real-time monitoring and give security personnel the ability to:

- **CCTV:** Closed-circuit television allows monitoring from multiple interconnected cameras, giving security teams expanded visibility.
- **Security Guards:** It's all good to have these technical measures in place, but there needs to be a team that is trained in their use and maintenance so they can fully utilize the security controls and respond to incidents.
- **Intrusion Detection Systems:** These systems have several different triggers that can generate alerts or set off alarms, including thermal (heat) detection, sound detection, and movement detection.

CONCLUSION

By employing all three types of physical controls, organizations can work to protect their buildings and places of work from physical intruders that seek to cause harm to information systems or other assets. If malicious actors know that the organization takes physical security seriously, it acts as a strong deterrent and can work to reduce the risk of physical intrusions.

[< Previous Topic](#)[Mark Complete ✓](#)[Back to Lesson](#)[Next Topic >](#)[Privacy & Cookies Policy](#)