Blue Team Level 1 Certification (Standard)

Introduction to BTL1

- ~~Welcome to Blue Team Level 1!~~
  - 4 Topics
- ~~Lab and Forum Access~~

SECURITY FUNDAMENTALS DOMAIN

- ~~Introduction to Security Fundamentals~~
  - 1 Topic
- ~~Soft Skills~~
  - 7 Topics
- ~~Security Controls~~
  - 5 Topics | 1 Quiz
  - ~~Section Introduction, Security Controls~~
  - ~~Physical Security~~
  - ~~Network Security~~
  - ~~Endpoint Security~~
  - ~~Email Security~~
  - ~~Activity) End of Section Review, Security Controls~~
- ~~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

Physical Security

Physical security controls are used to prevent unauthorized access to a building, or areas within. These controls help to make intrusion as hard as possible. The three main controls are deterrents, monitoring controls, and access controls. Examples can include locked doors, security guards, CCTV, and barriers. Although this is not usually the responsibility of a cyber team, it is still very important to know and may come in useful during investigations.

WHY IS IT IMPORTANT?

Usually, if an attacker has physical access to systems, it's game over. This could include terminal access to servers, physical data theft in the form of paper documents or hard drives, or even physical damage to systems causing a denial of service.

By using **Access Controls**, we can make it hard for unauthorized individuals to gain access to protected areas. An example of this would be turnstiles at the main entrance that require an RFID badge to unlock and pass through. Using this control, only employees that have a badge with the correct digital keys will be able to pass through.

Monitoring Controls such as CCTV are useful for live monitoring and keeping a record of any malicious behavior so that it can be used in the event of prosecution. CCTV can also be classed as a deterrent, because if people know they're being recorded, they may be less likely to commit a crime or malicious act.

Deterrents are designed to deter people; an example would be warning signs telling people that if they go any further, they will be trespassing. This may be enough to prevent some people from continuing.

ACCESS CONTROLS

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

- **Mantraps:** These are a slow but effective security control, where an individual wanting to access a protected

TI4) Tactical Threat Intelligence
7 Topics | 2 Quizzes
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
IR1) Introduction to Incident Response
8 Topics | 1 Quiz
IR2) Preparation Phase
10 Topics | 3 Quizzes
IR3) Detection and Analysis Phase
7 Topics | 5 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

area must go through an initial door into a holding room, where they are inspected from a window or 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.

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 detect and respond to intruders or insider threats.

- **CCTV:** Closed-circuit television allows monitoring from multiple interconnected cameras. This gives 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. An example of this would be a sound detection system that can recognize the sound of glass smashing (such as an intruder breaking a window to gain access to the building) and trigger an alarm.

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 be climbed over and requires more effort for attackers to bypass, slowing them down, and giving more

How to Start Your Exam

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.
- **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 solution.
- **CCTV Cameras:** If individuals believe they are being filmed (even if the cameras do not work) then this is likely to deter them from conducting any illegal or malicious activity, as there may be recorded evidence of them conducting a crime.

Previous Topic

Back to Lesson

Next Topic