Blue Team Level 1 Certification (Standard)
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
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

Network Security

This lesson will introduce you to some basic network defenses, and what they do to protect networks and systems from attacks. These security controls will be expanded on in future domains of this course, this lesson is purely designed to provide a foundation which will be constantly built on.

NETWORK INTRUSION DETECTION

Network intrusion detection systems, also known as NIDS, can come in the form of software or physical devices that tap monitor network traffic in order to generate alerts for human analysts to investigate (hence the name network intrusion "detection" system). NIDS can be positioned in the following positions:

- **Inline –** The system running the NIDS software is sitting directly in the path of network traffic, meaning all traffic will pass through the NIDS. In this case, the system will actually by definition become a Network Intrusion Prevention system, as it is able to perform defensive measures such as blocking or resetting connections.
- **Network Tap –** The NIDS will be connected to the network by tapping into a physical connection, such as a cable.
- **Passive –** The NIDS is connected to a SPAN port on a network device. This physical port allows all traffic passing through the device to be mirrored to the SPAN port, so the NIDS will get a copy of all network activity.

The purpose of NIDS is purely to generate alerts so that human analysts can investigate and take action if needed. If an attack is happening, the NIDS will generate an alert, and it will eventually be investigated.

NETWORK INTRUSION PREVENTION

Whilst similar to NIDS, network intrusion prevention systems, or NIPS, is able to automatically take defensive actions based on the activity that has been identified (hence the name network intrusion "prevention" system). So a NIDS can detect activity and generate an alert, but NIPS can detect activity and take actions to defend against it. As an example, if an internal system begins scanning other systems, which would be classed as unusual activity in most networks, we can pre-program the NIPS to block any communications that originate from the suspicious system, and generate an alert so human analysts can investigate further.

FIREWALLS

Firewalls are used to separate parts of a network to create private zones by restricting the traffic that can come in or go out. The most obvious example is having a physical firewall between the internet and your network, only allowing common protocols in such as HTTP, HTTPS, and DNS. This prevents random hosts from connecting to your systems, which could allow them to be exploited and compromised. There are different types of firewalls, which we will cover later in the course, with the three main being;

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

- Standard firewalls that run on dedicated hardware and sit at key points of the network.
- Local firewalls in software form that run on endpoints (such as Windows firewall).
- Web application firewalls in software form that sit on internet-facing web servers that host websites or web applications.

EVENT MONITORING

Network devices can generate logs, and these logs can be sent to a SIEM platform. By having logs come from systems across the environment, the SIEM is able to provide a dashboard that analysts can utilize to monitor activity and respond to alerts that are generated when suspicious or malicious traffic is detected. Network devices can provide very valuable information, let's take a look at a couple of examples:

- **Web Proxy Logs –** This device processes web-based requests to the internet, and will contain a list of sites visited by employees. This can be combined with a blacklist to generate SIEM alerts when an employee tries to visit a malicious website or explicit website.
- **Perimeter Firewalls –** If a malicious actor starts port scanning the organization, the perimeter firewalls will pick this activity up first as they get smashed with requests from the scanning IP(s). By sending this to a SIEM an alert can be generated when a port or vulnerability scanning is being conducted, or when distributed denial-of-service attacks (DDoS) start.

NETWORK ACCESS CONTROL

Network Access Control (NAC) can work to prevent rogue or non-compliant devices from connecting to a private network. Security teams could require that any devices connecting to the network need the latest patches and security updates, and must be running anti-virus. NAC is able to enforce this, and not let devices connect to the network until they have met all of the requirements. This is typically used for Bring Your Own Device (BYOD) or guest networks, where non-corporate devices will be connecting such as employee mobile phones and personal laptops, which may potentially be infected as they aren't protected by company security tools.

Ever been to a restaurant or shopping center that offers free wifi, but you need to sign up? That's NAC in action, allowing the network administrators to restrict access and manage sessions, such as networks that have time limits, like public transport and commercial flights.

Privacy & Cookies Policy
Privacy - Terms