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
  - ~~Blue Team Roles~~
- ~~Soft Skills~~ — 7 Topics
- ~~Security Controls~~ — 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 | 2 Quizzes
- TI5) Strategic Threat Intelligence — 5 Topics | 1 Quiz
- TI6) Malware and Global Campaigns — 6 Topics | 1 Quiz

Blue Team Roles

As you can imagine, the world of cybersecurity is huge. The defensive field, also known as 'blue team', is where we will be focusing in this course, however in some sections we will cover offensive (red) or hybrid (purple) practices. This lesson will introduce you to some of the most notoriously-known positions within defensive cybersecurity, including what tasks they are often responsible for, and further reading material. This content is designed to help inform individuals that aren't sure on which career path to take. Some of the most well-known defensive roles are:

- *SOC Analyst*
- *IT Security Analyst*
- *Incident Responder*
- *Threat Analyst*
- *Security Engineer*
- *Security Consultant*
- *Security Architect*
- *Forensic Computer Analyst*

SOC ANALYST

Arguably the most well-known position in the defensive realm is a ***SOC Analyst***. They are security professionals that typically work in the Security Operations Center *(SOC)* of an organization. The SOC team is in charge of protecting, monitoring, identifying, and eliminating threats in the IT systems of a company.

SOC analysts provide frontline incident handling and response, dealing with security events that are highlighted by tools such as a Security Information and Event Management (SIEM) platform, an Endpoint Detection and Response (EDR) solution, anti-virus, and intrusion detection systems (IDS). Analysts will deal with both common and anomalous event such as; external IP addresses performing port or vulnerability scans, login failures, phishing emails, administrator account usage, alerts generated from the above-mentioned tools, suspicious network connections, and more.

If you want to learn more about what a SOC is and what they do, take a look at the following links:

- *https://blog.eccouncil.org/soc-analysts-what-they-are-what-they-do-and-why-they-matter%E2%80%AF/*
- *https://www.csoonline.com/article/3537510/soc-analyst-job-description-salary-and-certification.html*

IT SECURITY ANALYST

Another important position is that of an ***information security analyst***. These professionals are in charge of safeguarding the organization's confidential and private information, avoiding at all costs any scenarios involving a breach of information.

Some example tasks carried out by individuals in this role can include hardening systems, identifying suspicious

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
How to Start Your Exam

activity, informing IT administrators of any risk, keeping systems updated, and more.

If you want to read more about this role, look at the following links:

- *https://digitalguardian.com/blog/what-security-analyst-responsibilities-qualifications-and-more*
- *https://www.infosecinstitute.com/career-profiles/security-analyst/*
- *https://www.careerexplorer.com/careers/information-security-analyst/*

INCIDENT RESPONDER

Continuing with this series of blue team roles, we have ***Incident Responders***. They are in charge of reacting immediately to any security incident, or any internal threat that occurs in the IT environment.

These highly-skilled individuals are extremely technically-capable, allowing the organization to respond to incidents that can be extremely damaging, such as ransomware outbreaks, website defacements, malware infections, DDoS attacks, and more.

If you want to know more about this role, you can visit the following links:

- *https://resources.infosecinstitute.com/job-titles/incident-responder/*
- *https://infosecaddicts.com/career-path/why-and-how-to-become-an-incident-responder/*

THREAT ANALYST

Another important position that exists in defensive environments is that of ***Threat Analyst***. These are professionals in charge of analyzing the data collected by the organization through various threat assessments *(Indicators of Compromise, Common/Known Vulnerabilities **(CVE)**, etc.)*, seeking to identify a possible threat that may affect the organization (whether it is happening now, or may happen in the future).

If you want to know more about this role, you can visit the following links:

- *https://digitalguardian.com/blog/what-does-insider-threat-analyst-do*
- *https://www.cybersecurity-insiders.com/role-of-cyber-threat-intelligence-analysts-in-an-organization-2/*
- *https://www.recordedfuture.com/threat-intelligence/*

SECURITY ENGINEER

In the security field you can also find the ***Security Engineers***. Professionals with this position are responsible for designing computer systems and implementing various types of security strategies *(network solutions, physical structures, etc.)*, in order to give them the ability to deal with various types of adversities and threats *(natural disasters, cyber-attacks, etc.)* and not die in the process.

Some of the responsibilities of this type of professional are **Design and implement security measures, carry out software testing and evaluation, monitor networks and computer systems,** among many other tasks.

If you want to know more about this role, you can visit the following links:

- *https://resources.infosecinstitute.com/job-titles/security-engineer/*
- *https://www.careerexplorer.com/careers/security-engineer/*
- *https://www.simplilearn.com/tutorials/cyber-security-tutorial/how-to-become-cyber-security-engineer*

SECURITY CONSULTANT

Continuing with our list, we have the ***Security Consultants***. They are trained computer security professionals who use their expertise to provide advice and supervision on the security measures a company or computer system will use to preserve and protect its information and that of its customers.

Some of the functions that these professionals carry out are: **Evaluate threats, identify violations and bad security practices** and mainly, **create protocols, standards and contingency plans that can be used by the organization in its defensive scenario.**

If you want to know more about this role, you can visit the following links:

- *https://resources.infosecinstitute.com/job-titles/security-consultant/*
- *https://www.careerexplorer.com/careers/it-security-consultant/*
- *https://neuvoo.ca/neuvooPedia/en/security-consultant/*
- *https://www.cyberdegrees.org/jobs/security-consultant/*

SECURITY ARCHITECT

A vital position to aid with the deployment of defence-in-depth is a ***Security Architect***. Professionals in this position are responsible for designing, building and maintaining operational security structures that are deployed in an organization. These professionals must apply industry best practices, and must think like an adversary, anticipating their movements and creating action plans to prevent system compromises.

If you are interested in this position, you can get more information on these websites:

- *https://resources.infosecinstitute.com/job-titles/security-architect/*
- *https://www.cybersecurityeducation.org/careers/security-architect/*
- *https://www.careerexplorer.com/careers/security-architect/*
- *https://www.cyberdegrees.org/jobs/security-architect/*

FORENSIC ANALYST

And finally, we have one of the most technical roles in the defensive world. This is the ***Digital Forensics Analyst***. These are professionals who work on sensitive investigations, collecting and analyzing devices to identify digital evidence that can be used for either incident response, or legal prosecution purposes, depending on which organization they work for. Most large-scale organisations will have Forensic Analysts to assist with work such as incident response investigations, and insider threat monitoring. Analysts that work for law enforcement agencies will likely assist with criminal investigations to collect evidence that links to the suspect to any committed crimes.

If you want to know more about this role, you can visit the following links:

- *https://blog.eccouncil.org/what-does-a-digital-forensics-analyst-do-is-this-job-for-you/*
- *https://www.criminaljusticedegreeschools.com/criminal-justice-careers/computer-forensics-investigator/*
- *https://study.com/articles/Computer_Forensics_Analyst_Job_Description_Duties_and_Requirements.html*

CONCLUSION

In this section we covered some of the most well-known roles within the defensive security field, however if you think that we have missed something important, or want to contribute additional further reading resources, please leave you your comments in the BTL1 Feedback lesson!

Privacy & Cookies Policy
Privacy - Terms