

**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

☒ 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☐ T11) Introduction to Threat Intelligence

7 Topics

☐ Section Introduction, Threat Intelligence☐ Threat Intelligence Explained☐ Why Threat Intelligence can be Valuable☐ Types of Intelligence☐ The Future of Threat Intelligence☐ Further Reading, Threat Intelligence☐ Threat Intelligence Glossary☐ T12) Threat Actors & APTs

6 Topics 2 Quizzes

☐ T13) Operational Threat Intelligence

7 Topics 1 Quiz

☐ T14) Tactical Threat Intelligence

7 Topics 1 Quiz

☐ T15) Strategic Threat Intelligence

5 Topics 1 Quiz

Why Threat Intelligence can be Valuable

Blue Team Level 1 Certification (Standard) > T11) Introduction to Threat Intelligence > Why Thr...

IN PROGRESS

Threat Intelligence HOW IS INTELLIGENCE VALUABLE?



If used correctly, threat intelligence has the capability to provide a number of benefits for organizations of any size. Below are a number of examples of how this security practice can provide value to a business by providing in-depth context, prioritization, enrichment, and building a network with other organizations.

CYBER THREAT CONTEXT



While a risk analysis may take a very brief look at the threat actors out there and the chance that the organization will be attacked by them, having a dedicated threat intelligence function could allow the business to perform in-depth research on the threats that are out there, and use historic events and targeting to truly determine what the chances are of being in their crosshairs. Proactive defensive measures can be taken to further reduce the risk, such as giving a vulnerability management team context around the vulnerabilities that are identified during a scan, helping to prioritize patching, and reduce the attack surface.

INCIDENT PRIORITIZATION



Having two incidents occur simultaneously can be draining on resources, and it's crucial that the incident with the highest potential impact is given the right attention and resources so it can be dealt with before damage occurs. Threat intelligence context can potentially give incident responders the information they need to make informed decisions about which incident to prioritize based on the threat actors that have been known to target similar organizations, and by retrieving indicator of compromise enrichment to get as much information from every piece of data.

T16) 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

2 Quizzes

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

INVESTIGATION ENRICHMENT

Giving context to an investigation can make a huge difference. An IP on the internet scanning the organization's public IP range is very common, and normally these IPs are either blocked (if they are sending a high volume of requests) or left alone as the perimeter firewalls are actively blocking them. But, if threat intelligence context states that this IP has been utilized by an advanced persistent threat (APT), such as a foreign nation-state, then this definitely needs more investigation and analysis to see exactly what the IP in question is scanning for.

INFORMATION SHARING

Connecting with analysts in other organizations can really help to boost an organization's security posture, by simply seeing how other organizations manage their security and the tools they use. This insight can help the security team make informed decisions based on experience from intelligence sharing partners. It can also help the organization to better defend itself, by receiving early warning signs such as precursors and indicators of compromise, so proactive defensive measures can take place, stopping an attack before it has already begun. We will cover how information can be shared, and in what formats, in the lesson **T15) Strategic Threat Intelligence, IOC/TFP Distribution**.

PYRAMID OF PAIN

The Pyramid of Pain, which we will cover in more detail during the **T13) Operational Threat Intelligence** section, is an extremely important part of threat intelligence. Each level of the pyramid represents different types of attack indicators you might use to detect an adversary's activities and is broken up by how much pain it will cause them when you are able to deny those indicators to them. By denying indicators to malicious actors, we're making it harder for them to operate, potentially reducing their ability to launch successful cyberattacks against the organization.

| | |
|----------------------------|--------------|
| TTPs | •Tough! |
| Tools | •Challenging |
| Network/ Host Artifacts | •Annoying |
| Domain Names | •Simple |
| IP Addresses | •Easy |
| Hash Values | •Trivial |

Source: David J Bianco

[Previous Topic](#)

Mark Complete

✓

[Next Topic](#)

Back to Lesson

