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
- TI1) 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
- 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

Threat Intelligence Explained

In its simplest form, ***"threat intelligence is information that an organization uses to understand the threats that are currently targeting them, or could target them in the future".*** This knowledge can help security teams to develop better defenses, mitigate cyber risk, and aid with monitoring their networks for any signs of compromise, so teams can remove malicious actors as quickly as possible.

Threat intelligence aims to provide information on more sophisticated threats, such as Advanced Persistent Threats (APTs), zero-day vulnerabilities, and global malware campaigns. It will help the organization to understand who is (or could be) attacking them, why they're doing it, and the tactics they use so they can be replicated in penetration tests and red team engagements, or defensive measures put in place to stop or slow down attackers.

Typically actual intelligence is shared in the form of indicators of compromise (IOCs) which are artifacts that have been observed in relation to malicious activity. These can be email addresses that have been sending malicious emails, IP addresses that are hosting websites trying to steal user's account details, or file-based artifacts such as a malware file name, file size, or its' MD5 hash value.

We will cover all of the above in future lessons, so you can get an idea of what threat intelligence actually involves.

THREAT INTELLIGENCE LIFECYCLE

Threat intelligence is all about gathering raw data, and transforming it into intelligence that has value and can actually be used. To achieve this, we can follow what's known as the "Threat Intelligence Lifecycle". This can vary depending on which organization you're looking at – so we'll be combining the best bits of the lifecycles presented by Recorded Future and CrowdStrike.

1) Planning & Direction

This is the most crucial part, as it determines what the scope is for this specific threat intelligence project. Goals need to be set, and the stakeholders need to be clearly defined. This helps the project to stay on track, and not waste time or resources working on intelligence that is not important.

For example, if an organization received intelligence from another company that a foreign hacking group posted on a dark web forum boasting they are about to conduct a prolonged cyber attack against the company, an intelligence program could plan to do the following activities:

- **Research and learn more about the hacking group, including who is involved, and how skilled/sophisticated they are.**
- **Check for public exposure in order to understand the attack surface of the organization** (the total number of ways hackers could break into a network. If a company had all of their systems fully patched, they would have a small attack surface, however, if patches were not applied there are more security flaws attackers can take advantage of).
- **Discover the most appropriate actions that can be taken to defend against this threat.**

2) Collection

This is the stage where the team will go out and collect all of the data they need to achieve their end goal of creating actionable intelligence. In our example, this would include scraping as many posts from the underground forum as they can get access to, any information associated with forum user accounts, performing OSINT searches to try to

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 | 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

find information on the group, and anything else they agree is in scope as defined in phase 1. Mature threat intelligence teams typically use a centralized threat intelligence platform (such as MISP, which we will discuss later in this domain) to store indicators and indicators of compromise from a range of public and private threat feeders, which are lists of actionable intelligence shared between organizations.

3) Processing

Now that the team has a vast amount of data, they need to transform it into a clear and readable format so that it can be analyzed, typically by human threat intelligence analysts. Following our example again, it was mentioned that the source of the hacking group's claim to conduct an attack came from a "dark web forum" and that the actors were foreign. If the posts were not written in English, they would need to be expertly translated to ensure that the exact information was maintained. This is an example of processing collected data to make it easier to analyze.

4) Analysis

This stage involves a human process where processed information (from the previous step) is turned into actionable intelligence that can be used. Depending on the circumstances, the decisions might involve whether to investigate a potential threat, what actions to take immediately to block an attack, how to strengthen security controls, or how much investment in additional security resources is justified.

This information needs to be presented in an appropriate manner based on the audience. If a technical threat intelligence piece was being passed to security analysts then it can remain technical and use security jargon, however, if it is a more strategic piece being presented to a typically non-technical audience such as members of the executive board, then it needs to be simpler and not use jargon, with a focus on how this intelligence affects the business considering factors such as money and reputation.

5) Dissemination

Dissemination involves getting the finished intelligence output to the places it needs to go. This can be SOC or Security Analyst, fellow Threat Intelligence Analysts, and even the executive board (for high-level strategic intelligence, that can be used to inform security budgets and decision making).

For each of these audiences, you need to ask:

- What threat intelligence do they need, and how can external information support their activities?
- How should the intelligence be presented to make it easily understandable and actionable for that audience?
- How often should we provide updates and other information?
- Through what media should the intelligence be disseminated?
- How should we follow up if they have questions?

6) Feedback

It is critically important to understand your overall intelligence priorities and the requirements of the security teams that will be consuming the threat intelligence. Their needs guide all phases of the intelligence lifecycle and tell you:

- What types of data to collect
- How to process and enrich the data to turn it into useful information
- How to analyze the information and present it as actionable intelligence
- To whom each type of intelligence must be disseminated (as mentioned in the dissemination stage), how quickly it needs to be disseminated, and how fast to respond to questions

You need regular feedback to make sure you understand the requirements of each group, and to make adjustments as their requirements and priorities change.

THREAT INTELLIGENCE ANALYSTS

Cyber threat intelligence analysts have skills that are not seen in other areas. Analysts spend a long time performing in-depth analysis work, so they are highly aware of bias, they will question everything, hunt for evidence, and think outside the box. These roles involve a lot of technical analysis, research, and problem-solving, working to identify malicious actors, track them, and keep on top of their techniques and tactics, allowing organizations to prepare for attacks and respond to them effectively. Tactics will be mapped to frameworks such as the Cyber Kill Chain by Lockheed Martin, or the MITRE ATT&CK Framework, while malicious indicators are compared against the Pyramid of Pain. We will cover all three of these in future lessons. Analysts come from a diverse range of backgrounds, quite often being from police forces or military personnel due to the skills they possess.

TYPES OF THREAT INTELLIGENCE

Strategic Threat Intelligence

This type of intelligence provides high-level, typically non-technical information that can be understood by anyone. It is used when presenting to executives and other decision-makers within an organization to aid with decisions such as budget spending and policy review or creation. Below are some examples of strategic intelligence pieces:

- A presentation that covers global events and links them with cyber activity (such as the Coronavirus pandemic resulting in an increase of tailored phishing attacks claiming to be from health authorities such as the World Health Organization).
- A report on patterns of cyber attacks that the organization is facing over a period of time (such as recognizing that the organization is receiving more distributed denial of service (DDoS) attacks on Monday, and suggesting plans to mitigate this).
- Keeping the internal security team informed about activity related to threat actors that target organizations operating in the same industries (such as the threat intelligence team in a bank monitoring for attacks against other banks, and updating their internal team so they are aware and can prepare for attacks).

Strategic intelligence specialists can be very geographically-focused, understanding the political situation and motives of a country. They will then provide closer tracking of threat actors which have been linked to regions or countries that may pose a threat to the organization based on the industries it operates in. Any geopolitical tension between the country or countries the organization operates in and foreign nations. They will also focus on activity happening within the industry that the business operates in. So strategic analysts at a bank or financial institution would keep track of any cyber attacks that occur within the financial industry.

Operational Threat Intelligence

Operational intelligence is all about studying threat actors that might target the organization, in order to gain information about who they are, their motivations, and tactics, techniques, and procedures (TTPs) used to conduct campaigns or prolonged cyber operations. This can help to build more effective defenses by actively monitoring techniques that are used by adversaries, and understanding the actor(s) at a deeper level. This work, which is typically technical, is not easily automated and requires human analysts to track and research malicious groups.

Tactical Threat Intelligence

Tactical intelligence is technical in nature, and is of immediate value to an organization. It is typically shared in the form of indicators of compromise (IOCs), which are known malicious artifacts such as URLs, domains, email addresses, file hashes, IP addresses, and more. These can either be used by human analysts to check for exposure or can be ingested by security tools via APIs or threat feeds. Below are some examples of tactical intelligence pieces:

- A list of email addresses (IOCs) that are being used to send phishing emails containing the Emotet malware are given to an analyst, and they manually check the email gateway security tool to identify any incoming emails from these addresses.
- A threat feed that can be subscribed to, which includes a constantly updated list of malicious IPs, primarily intended to feed into network intrusion prevention systems, so they can autonomously block bad IPs.
- A public report from a threat intelligence company that includes a number of IOCs gathered by monitoring exploitation activity targeting a new zero-day vulnerability.

Each of these different areas of threat intelligence and their associated roles and activities will be covered within the Threat Intelligence domain, so you can gain an insight into all of the above.

Privacy & Cookies Policy
Privacy - Terms