Threat Intelligence Glossary

This document is designed to cover all acronyms used in the Threat Intelligence domain of the Blue Team Level 1 certification training course.

This document is TLP:White, and can be shared without breaching the Terms and Conditions of the BTL1 course.

Learn more about Blue Team Level 1 and purchase the certification here – https://securityblue.team/why-btl1/

TIP // Threat Intelligence Platform – A platform typically used to store indicators of compromise (IOCs) and intelligence reports which can be used to power defenses including firewalls, intrusion detection systems, and generate watchlists and provide event context in platforms such as endpoint detection and response (EDR) and security information and event management (SIEM) solutions.

TEC // Threat Exposure Check – The process of manually or autonomously checking an environment for the presence of malicious indicators, such as email subject lines, email sending addresses, malware hashes, and observed network activity connected to malicious IP addresses.

EDR // Endpoint Detection and Response – An EDR solution is typically an analysis platform with software agents that run on endpoints, continuously sending information to the EDR server for correlation, detecting anomalies and security events. EDRs can be configured to take automatic actions, such as stopping network connections and generate alerts for security analysts to investigate.

IDS/IPS/IDPS // **Intrusion Detection and Prevention System** – Typically systems will have either Intrusion Detection functionality, reporting on unusual or suspicious activity by generating alerts and logs, or Intrusion Prevention functionality, working to autonomously stop attempts without needing to wait for human intervention.

CTI // **Cyber Threat Intelligence** – The phrase given to security professionals and the industry surrounding the practice of threat intelligence in the cyber realm. The attribution of threat actors to cyber activity, and the sharing of intelligence to allow defenders to respond or prepare for cyber-attacks.

IOC // **Indicator of Compromise** – Intelligence gathered from malicious activity, intrusions, or incidents. An example would be a piece of malware that was observed in an attack against an organization. The file hashes and file name can be shared with other organizations so they can add it to blocklists or perform threat exposure checks.

TTP // **Tools, Techniques, and Procedures** – MITRE have defined over 240 unique tactics used by adversaries, known as TTPs. You can find them here, each with detailed descriptions, and the threat actors that have been known to use them.

MD5 // **Message Digest 5 Hashing Algorithm** - The MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities. It can still be used as a checksum to verify data integrity.

SHA1 // **Secure Hash Algorithm 1** - In cryptography, SHA-1 is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value known as a message digest – typically rendered as a hexadecimal number, 40 digits long.

SHA256 // **Secure Hash Algorithm 256** - SHA-256 is a one-way function that converts a text of any length into a string of 256 bits. This is known as a hashing function. In this case, it is a cryptographically secure hashing function, in that knowing the output tells you very little about the input. It is a modified version of SHA1

APT // **Advanced Persistent Threat** – A well-resourced and technically sophisticated threat actor, most likely linked to a country's government, typically focused on covert, long-term cyber operations, allowing them to complete their objectives without their targets detecting them.

OSINT // **Open-Source Intelligence** – Intelligence or information collected from publicly-available sources, such as social media, search engines, and websites that do not require registration or payment to access their content.

MISP // **Malware Information Sharing Platform** – An open-sourced threat intelligence platform that allows organizations to store threat intelligence information, and create information sharing and analysis centers by inviting other organizations to access the server.

DDoS // **Distributed Denial-of-Service** – An attack where hundreds or thousands of systems begin sending traffic to a target or targets, with the intention of using up the device's resources so that it can no longer process legitimate requests. This attack is typically conducted against web servers, preventing people from loading a website.

CVE // **Common Vulnerabilities and Exposures** – The naming convention given to vulnerabilities in software and hardware, allowing for easier sharing of information related to a specific weakness.

CVSS // **Common Vulnerability Severity Scoring** – The scoring system used to classify how severe vulnerabilities are based on a number of factors including technical sophistication, exploitation vector, and privileges needed for successful exploitation.

RDP // **Remote Desktop Protocol** – A Windows protocol that allows users to access other Windows systems using a graphical user interface as if they were on the system. Used by system administrators to access servers, or by IT support personnel to assist users. Can also be utilized by malicious actors to move around a network.

VPR // **Vulnerability Priority Rating** – A vulnerability scoring system created by Tenable that utilizes threat intelligence context to rate vulnerabilities based on the likelihood of them being exploited, and the impact successful exploitation would have.

SIGINT // **Signals Intelligence** - Signal intelligence involves the interception of radio signals and broadcast communications to gather intelligence.

COMINT // **Communications Intelligence** - Communications intelligence relating to communications between people and groups of people (messages and voice) and often synonymous with SIGINT.

ELINT // **Electronic Intelligence** - Electronic intelligence is collected from systems not used directly for communications, such as guidance communication for missile systems and radars.

UAV // **Unmanned Aerial Vehicle** – An aerial vehicle that is being flown autonomously or remotely, with no human pilot onboard, such as reconnaissance drones.

HUMINT // **Human Intelligence** - In the broadest sense, human intelligence (HUMINT) is gathered from other humans. This intelligence is often gathered through in-person meetings, debriefings personnel tasked with acquiring information through observation, and document gathering. Such information can be attained through espionage or open communications between diplomats.

GEOSINT // **Geospatial Intelligence** – The use of satellite imaging to monitor activities such as tracking individuals of interest, structural reconnaissance, military movement location and tracking, and monitoring natural disasters.

FIN // **Financially Motivated Threat Actor** – The name given to financially motivated threat actors by security and intelligence firm FireEye. These groups are typically associated with cybercrime activity and practices.

UNC // **Unclassified Threat Actor** - Groups that are currently undergoing analysis are referred to as “UNC” or Unclassified under the FireEye/Mandiant naming convention.

ISAC // **Information Sharing and Analysis Center** – A collective of organizations, typically operating in the same industries, that share actionable and strategic intelligence surrounding cyber attacks with the goal of improving each other’s defenses and ability to respond to security events and incidents.