Advanced Cyber Threat Intelligence Glossary

Created By: Apurv Tiwari, Junior Teaching Assistant

Instructor: Alyssa Berriche

1. **OSINT - Open Source Intelligence**; refers to any information that can legally be gathered from free, public sources about an individual or organization.
2. **Cyber Kill Chain -** Framework consisting of seven steps that enhances visibility into an attack and enriches an analyst's understanding of an adversary's tactics, techniques and procedures.
3. **Diamond Model -** a formal method applying scientific principles of measurement, testability, and repeatability to intrusion analysis, providing a comprehensive method of activity documentation, synthesis, and correlation.
4. **Maltego -** An interactive, visual data mining and link analysis tool used to conduct online investigations/threat research through a library of plugins called "transforms".
5. **CTI - Cyber Threat Intelligence** encompasses every detail about a threat, including where it originated, who coded it, who has modified it since, how it's delivered, the kind of damage it does, and numerous other traits and signifiers. In addition to indicators of specific malware, threat intelligence also covers the tools and tactics cyber-attackers use, details on specific types of attacks, and dynamic information about potential risks and new risk sources.
6. **TIP - Threat Intelligence Platforms** provides features that aid with analysis of potential threats and corresponding mitigation including features like explore threats, provide investigation workflows, understand the broader context and implications of threats and share information.
7. **Heatmap -** a graphical representation of data that uses a system of color-coding to represent different values.
8. **MITRE ATT&CK -** a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.

9. **Cognitive Bias -** a systematic error in thinking that affects the decisions and judgments that people make.
10. **Intelligence Cycle -** process of developing raw information into finished intelligence for policymakers to use in decision making and action.
11. **IPS - Intrusion Preventions System -** a form of network security that works to detect and prevent identified threats. Intrusion prevention systems continuously monitor your network, looking for possible malicious incidents and capturing information about them.
12. **IOC - Indicators of Compromise** - pieces of forensic data, such as data found in system log entries or files, that identify potentially malicious activity on a system or network.
13. **SIEM - Security Information and Event Management** - a software solution that aggregates and analyzes activity from many different resources across your entire IT infrastructure.
14. **Dark Web -** The dark web refers to encrypted online content that is not indexed by conventional search engines.
15. **Endpoint -** An endpoint device is an Internet-capable computer hardware device on a TCP/IP network.
16. **Metadata -** a set of data that describes and gives information about other data.
17. **IDS - Intrusion Detection System -** a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered.
18. **EDR - Endpoint Detection and Response -** the tools primarily focused on detecting and investigating suspicious activities (and traces of such) other problems on hosts/endpoints.
19. **Proxy -** a server that acts as an intermediary for requests from clients seeking resources from other servers.
20. **YARA -** YARA rules are a way of identifying malware (or other files) by creating rules that look for certain characteristics, mainly used in malware research and detection.
21. **STIX -** Structured Threat Information Expression (STIX™) is a language and serialization format used to exchange cyber threat intelligence (CTI).
22. **Threat landscape -** A threat landscape (also called a threat environment) is. a collection of threats in a particular domain or context, with information on identified vulnerable assets, threats, risks, threat actors and observed trends.
23. **TTP - Tactics, Techniques and Procedures -** TTPs are the patterns of activities or methods associated with a specific threat actor or group of threat actors.

CYBRARY

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

24. **Sandbox -** a testing environment that isolates code and experimentation from the production environment or repository.
25. **ISAC - Information Sharing and Analysis Centers**
26. **ISAO - Information Sharing and Analysis Organizations**
27. **Threat Actor -** any individual or group of individuals that attempts to or successfully conducts malicious activities against enterprises, whether intentionally or unintentionally.
28. **Attack Surface -** The Attack Surface describes all of the different points where an attacker could get into a system, and where they could get data out.
29. **Dork -** A Google dork query, sometimes just referred to as a dork, is a search string that uses advanced search operators to find information that is not readily available on a website.
30. **Regular expression -** A regular expression is a special text string for describing a search pattern.
31. **CVSS - Common Vulnerability Scoring System -** It provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity.
32. **TLP - Traffic Light Protocol -** TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience.
33. **TAXII - Trusted Automated eXchange of Indicator Information -** It is a free and open transport mechanism that standardizes the automated exchange of cyber threat information.
34. **Threat Feed Aggregator -** Collects, organises and displays threat based data from various sources.
35. **SOC- Security Operation Center -** a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.
36. **OTX - Open Threat Exchange -** a free to use, crowd-sourced computer-security platform
37. **MISP - Malware Information Sharing Platform -** is an open source threat intelligence platform. The project develops utilities and documentation for more effective threat intelligence, by sharing indicators of compromise.
38. **CRITS - Collaborative Research Into Threats -** is an open source malware and threat repository that leverages other open source software to create a unified tool for analysts and security experts engaged in threat defense.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

39. **WHOIS -** a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource.
40. **ACH - Analysis of Competing Hypothesis** requires an analyst to explicitly identify all the reasonable alternatives and have them compete against each other for the analyst's favor, rather than evaluating their plausibility one at a time.

References

1. **What is OSINT, SentinelOne,** https://www.sentinelone.com/blog/what-is-osint-how-is-it-used/
2. **Cyber Kill Chain, LockheedMartin,** https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
3. **Diamond model, Paper,** https://apps.dtic.mil/docs/citations/ADA586960
4. **ATT&CK, MITRE,** https://attack.mitre.org/
5. **Cyber Threat Intelligence, OASIS,** https://oasis-open.github.io/cti-documentation/
6. **CRITS, Github,** https://crits.github.io/

CYBRARY