C

Cyber Threat Intelligence

Daniel Schlette
Chair of Information Systems, University of Regensburg, Regensburg, Germany

Synonyms

Threat intelligence

Definition

The security of information systems is a fragile state and under constant scrutiny of malicious actors. Therefore, security incidents, cyberattacks, and other forms of imminent threats are common and must be dealt with. Cyber Threat Intelligence (CTI) aims to provide meaningful and actionable knowledge about threats originating from and targeting the cyber domain (i.e., information systems) and manifesting in (successful) information security impairments. Additionally, threat intelligence is commonly defined by its focus on evidence (e.g., Indicators of Compromise) and its context which helps to inform decision makers about adequate response to threats (McMillan 2013).

CTI comprises different components and in essence refers to (1) the threat information itself, (2) structured data formats, (3) sharing platforms, and (4) incident response procedures. These components are further embraced by data quality and the CTI life cycle documenting a process from CTI generation to eventual revocation.

Background

Against the background of attackers sharing information about vulnerabilities, malware, or attack patterns, security analysts and defenders began to leverage security information. The aim to better protect information systems initially mandated the collection and aggregation of relevant knowledge. Thus, early work on threat information started by detailing the many aspects of information security incidents (Howard and Longstaff 1998). Threat information itself typically consists of various levels. Low-level cyber-observables express artifacts such as malicious files and their signatures but also extend to processes and network traffic. Higher-level threat information then provides insights on more complex Indicators of Compromise (IoC), vulnerabilities, and attacker behavior. Lastly, a third level of threat information deals with countermeasures relevant for incident response and attribution of attacks (Mavroeidis and Bromander 2017). When analyzed and put into context, all this information represents cyber threat intelligence. Accordingly, CTI is often seen to fulfill either operational, tactical, or strategic aims within an organization (Tounsi and Rais 2018). However, to make use of CTI for sharing, collaborative analysis, and

S. Jajodia et al. (eds.), *Encyclopedia of Cryptography, Security and Privacy*,
https://doi.org/10.1007/978-3-642-27739-9_1716-1

to overcome ambiguities, individual pieces of CTI must be structured. Consequently, an important element of CTI is structured data formats. These data formats often deal with a very specific aspect of CTI, but some also cover the full CTI spectrum. Over the course of the years, formats have been developed ranging from enumerations and scoring systems to frameworks and comprehensive CTI standards (Dandurand et al. 2014). As formats in the CTI ecosystem are manifold and diverse, there is a need for comparison. Emphasis on their dedicated functionalities specifies enumerations to identify vulnerabilities or assets. Scoring systems condense security information to a single indicative number. Frameworks typically support the understanding of attacker behavior. CTI standards then integrate these granular elements and provide a holistic view on security incidents and attacks (Menges and Pernul 2018). Built upon CTI formats, sharing and collaboration on threat information become possible. CTI-sharing platforms bring together different stakeholders using technologies for information storage and exchange. Besides, sharing of CTI has to deal with the legal environment, industry requirements, and incentives for participation (Skopik et al. 2016). At last, CTI goes beyond being purely informative and proves itself actionable by directly linking to incident response. To investigate, remediate, mitigate, and prevent security incidents, CTI not only contains information on root causes but can also show blueprints of adequate countermeasures. For all the above-mentioned components, data quality plays an important role as low-quality CTI implies ineffectiveness and can have severe consequence when applied to defensive information systems.

Theory and Applications

Whereas security information has been around for at least the last two decades, cyber threat intelligence is a much newer term and has significantly gained momentum in the last 7 years. Its theoretical foundations are strongly linked to practical application. For instance, defining CTI relates to organizational processes, and security information eventually becomes CTI. Analogous to the overall information security domain, people, processes, and technology are part of CTI and its applications. In CTI, security analysts with certain skills may perform threat hunting to identify and act upon CTI or derive incident response procedures. CTI personnel can thus be organized within the Security Operations Center (SOC) or form a standalone organizational unit with close contact to SOC, Computer Emergency and Response Team (CERT) and other IT-units (Brown and Lee 2019). Processes pertaining to CTI include consuming, using, and producing CTI. From a different perspective, the CTI life cycle describes transformation processes on threat information (Landauer et al. 2019). Technology supportive of CTI covers sharing platforms, most notably the MISP – Open Source Threat Intelligence Platform, TAXII – Trusted Automated Exchange of Indicator Information servers and proprietary solutions. The STIX – Structured Threat Information eXpression available in version 2.1 is currently a prevalent standard for CTI and follows a graph-based approach (Barnum 2014). Thereby, different types of CTI objects can be defined and connected. With MISP, VERIS – Vocabulary for Event Recording and Incident Sharing and IODEF – Incident Object Description Exchange Format, there exist other well-known and comprehensive CTI standards. Complementing CTI technology, sources of CTI include various security systems such as Security Information and Event Management (SIEM) systems, Intrusion Detection Systems (IDS), or firewalls (Lee 2020). As CTI fosters bidirectional transfer, these systems can serve as a sink too, which is particularly helpful to prevent security incidents in the future.

Open Problems and Future Directions

Research on CTI has led to a better understanding of its manifold facets. Nevertheless, challenges and open problems remain with regard to the use of threat information for active cyber

defense. Actionable CTI has yet to cope with its (semi-) automated use in incident response processes. Therefore, development of dedicated incident response data formats is a necessary step (Nespoli et al. 2017). Subsequently, integration into existing CTI formats (e.g., STIX2.1 and its Course of Action object) will support comprehensiveness as well as effectiveness of CTI. To this end, a second future direction is how to assure CTI quality. Whereas first approaches aim to analyze and propose quality metrics for CTI (Schlette et al. 2020), the subjective nature and the diversity of threat information demand further research. Based upon data analysis, a stronger data-centric focus must take the entire CTI life cycle and organizational dependencies into account. Here, a relevant challenge concerning CTI sharing is the involvement of CTI users beyond solely consuming CTI through sharing incentives or regulatory requirements.

Cross-References

- ▸ Cyber Threat Intelligence Sharing
- ▸ Security Operations Center
- ▸ Security Information and Event Management

References

Barnum S (2014) Standardizing cyber threat intelligence information with the structured threat information eXpression (STIX). Version 1.1, Revision 1. MITRE. http://stixproject.github.io/getting-started/whitepaper/

Brown R, Lee RM (2019) The evolution of cyber threat intelligence (CTI): 2019 SANS CTI survey. SANS

Dandurand L, Kaplan A, Kácha P, Kadobayashi Y, Kompanek A, Lima T et al (2014) Standards and tools for exchange and processing of actionable information. ENISA. https://www.enisa.europa.eu/publications/standards-and-tools-for-exchange-and-processing-of-actionable-information

Howard JD, Longstaff TA (1998) A common language for computer security incidents. Sandia National Labs

LandauerM, Skopik F, Wurzenberger M, Hotwagner W, Rauber A (2019) A framework for cyber threat intelligence extraction from raw log data. In: 2019 IEEE international conference on big data (Big Data). IEEE, pp 3200–3209. https://doi.org/10.1109/bigdata47090.2019.9006328

Lee RM (2020) 2020 SANS cyber threat intelligence (CTI) survey. SANS

Mavroeidis V, Bromander S (2017) Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within CTI. In: 2017 European intelligence and security informatics conference (EISIC). IEEE, pp 91–98

McMillan R (2013) Definition: threat intelligence. Gartner. https://www.gartner.com/en/documents/2487216/definition-threat-intelligence. Checked on 10 Jan 2020

Menges F, Pernul G (2018) A comparative analysis of incident reporting formats. Comput Secur 73:87–101. https://doi.org/10.1016/j.cose.2017.10.009

Nespoli P, Papamartzivanos D, Mármol FG, Kambourakis G (2017) Optimal countermeasures selection against cyber attacks: a comprehensive survey on reaction frameworks. IEEE Commun Surv Tutorials 20(2):1361–1396

Schlette D, Böhm F, Caselli M, Pernul G (2020) Measuring and visualizing cyber threat intelligence quality. Int J Inf Secur 1–18

Skopik F, Settanni G, Fiedler R (2016) A problem shared is a problem halved: a survey on the dimensions of collective cyber defense through security information sharing. Comput Secur 60:154–176. https://doi.org/10.1016/j.cose.2016.04.003

Tounsi W, Rais H (2018) A survey on technical threat intelligence in the age of sophisticated cyberattacks. Comput Secur 72:212–233