What is Cyber Threat Intelligence?

gca.isa.org/blog/what-is-cyber-threat-intelligence

All Posts

- Tweet
-

This blog is the first in a three-part series defining Cyber Threat Intelligence (CTI). The second part features an in-depth explanation of practical uses for the Diamond Model in CTI analysis. The third part covered recent activity in Dragos Threat Groups.

Cyber Threat Intelligence blends traditional intelligence operations and analysis techniques with current issues in cybersecurity. Threat intelligence is knowledge—or the outcome of an analytic process using hypothesis-led and evidence-based analysis from a variety of data sources. Cybersecurity for this research will be defined as all that encompasses the technical, sociological, and psychological aspects of cyber threats today. Traditional intelligence operations and analysis is comprised of both theoretical and practical aspects. At its core, intelligence focuses on collecting information and synthesizing it into actionable data for policymakers or organizations.

Traditional Intelligence vs. Cyber Threat Intelligence as a Discipline

Traditional intelligence typically falls into two distinct categories: Strategic and Tactical. Both derive information for policymakers to assist in the complex international relations decision-making process. Strategic intelligence is the production of short and long publications, which policymakers use for such decision-making. Tactical (operational) intelligence is the collection of information from the field used to answer specific questions in what is commonly known as the intelligence community.

Cyber Threat Intelligence is categorized into three types: Tactical, Operational, and Strategic. CTI uses a third category, tactical, to describe the technical indicators and behaviors used to inform network level action and remediation. Operational intelligence is the work threat hunters and incident responders perform to catalogue adversary behavior, advise holistic remediation, and show examples of threat hunting processes. Finally, strategic threat intelligence places threats into a business context and describes the calculated impact, informing risk management and organizational direction.

All intelligence focuses on the collection of information to make informed decisions. Sometimes in CTI this is referred to as “telemetry.” Telemetry is key in CTI, as it provides the best picture of any given cyber event in real or near real-time. CTI collection is ever evolving, and many companies exist now that collect up-to-the-minute telemetry data.

Tradecraft used in cyberattacks or cyber breaches is key to mitigation. In this way, tradecraft used to construct zero-day threats or malware can, with the assistance of reverse engineering, provide clues to the most efficient mitigation techniques. While traditional intelligence focuses on securing nations, CTI focuses on securing organizations and critical infrastructure from breaches, attacks, and compromises.

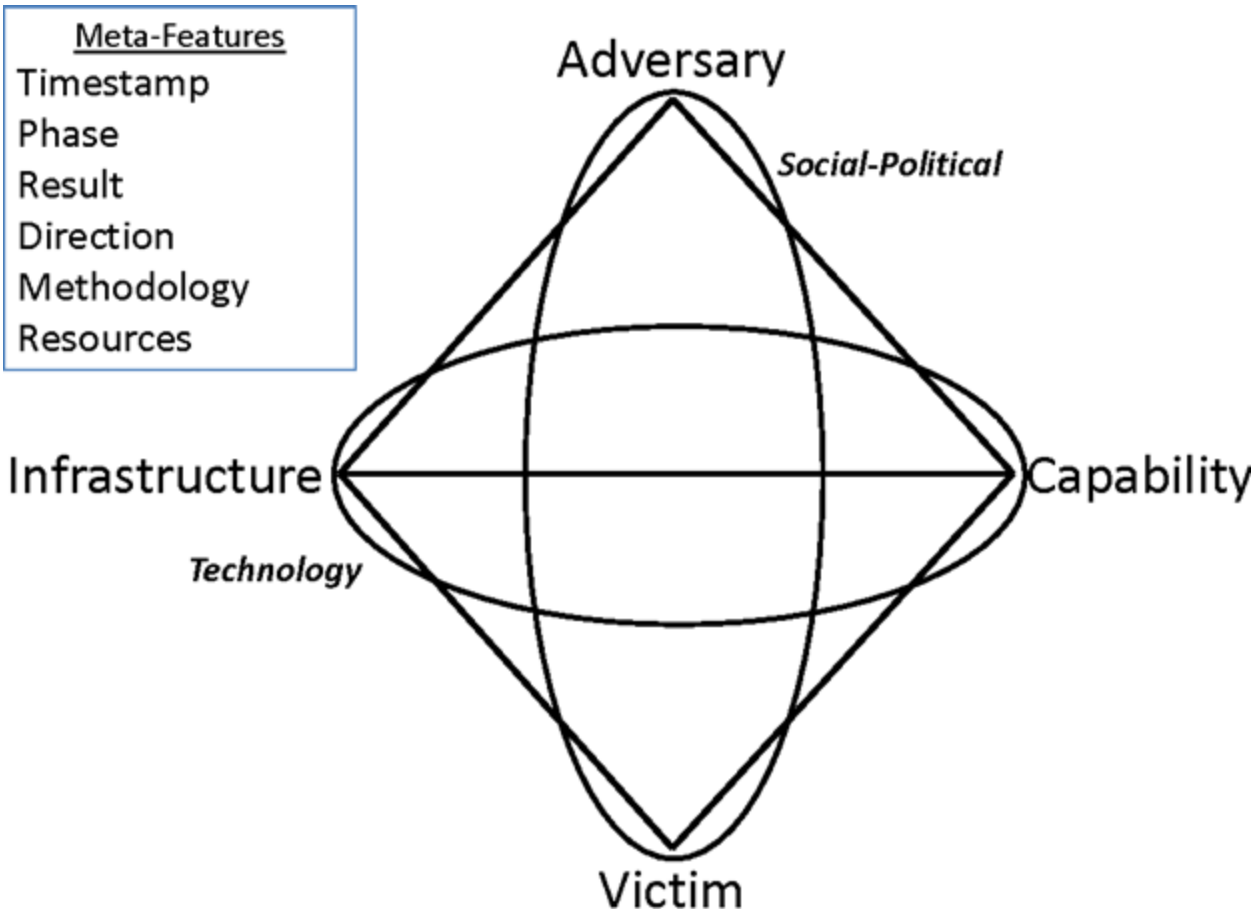
It may seem like the two disciplines or paradigms are sufficiently different to exist on their own. However, traditional intelligence is the foundation of CTI, and as such, CTI benefits much from the classical definitions of traditional intelligence and the associated collection processes.

Elements of Cyber Threat Intelligence

According to Caltagirone, the four elements of good (cyber) threat intelligence are: Completeness, Accuracy, Relevance, and Timeliness. Completeness means the analyst must mine, research, and otherwise provide all relevant information to detect the threat in an effort to ultimately prevent it. Accuracy means success always outweighs errors and mistakes. Relevance means that the threat must be pertinent to the organization. Timeliness means that corrective actions must be broadcast quickly and to large audiences to prevent further intrusions or compromises.

The Diamond Model

Further research by Caltagirone shows that the Diamond Model provides an atomic event of any intrusion activity. The Diamond model is composed of four core features: Adversary, Infrastructure, Capability, and Victim. Strictly speaking, if an analyst can find three of the four axes, the analyst should report it. But in practice, many CTI analysts report with only one or two axes defined. The model establishes a formal method applying scientific principles to intrusion analysis—those of measurement, testability, and repeatability—providing a comprehensive method of activity documentation, synthesis, and correlation.



Dr. Tom Winston

Dr. Tom Winston is a director of intelligence content for Dragos. Tom has over 25 years of professional experience in many areas to include cybersecurity, ICS/SCADA systems, Critical Infrastructure protection, academics as well as systems and network engineering. He joined Dragos after serving for several years as a professor of cybersecurity engineering at George Mason University. Prior to that Tom served in a 15 year-long career at the CIA as an operations, digital forensics, and ICS/SCADA expert. His experience focused on threats to critical infrastructure (ICS/SCADA) systems, as well as foreign cyber intelligence and threat analysis. Tom has extensive experience in mobile device, removable/fixed media digital forensics, as well and has visited over 30 countries worldwide, and speaks over a dozen foreign languages.