21 January 2022

Webinar: The 4 Qualities of Good Cyber Threat Intelligence

Tom Winston, Ph.D. Director of Intelligence
Dragos, Inc.

OVERVIEW

In today's webinar:

- Overview
- Cyber Threat Intelligence
- Sourcing and Confidence in threat intelligence
- How to apply the diamond model.
- How threats differ across industries.

Overview

Overview

- What is Threat intelligence?
- Threat intelligence is the actionable knowledge and insight on adversaries and their malicious activities enabling defenders and their organizations to reduce harm through better security decision making

Overview

- Generic Threat Intelligence
  - Not good enough for industrial control systems
- Threat intelligence
  - Context
  - Action
    - Threat Assessment
    - Impact
    - Recommend action

Overview

- Not all threat intelligence is equal
- Good Threat intelligence follows CART
- An organization consuming high-quality threat intelligence will be able to leverage it across their cybersecurity program to improve detection, response, and prevention informing the most technical defenders and operators to the most strategic decision makers.
- High-quality threat intelligence applied diligently, can differentiate mediocre cybersecurity programs from great programs. For industrial control networks where the impact of a cybersecurity incident can mean millions in business losses, reputational damage, an environmental disaster, or loss of life, the diligent application of high-quality threat intelligence is now an absolute necessity.

Overview: With good CTI…

- Orgs can leverage:
  - Improved detection
  - Response
  - Prevention
  - Sharing critical information with technical defenders and strategic decision makers

Overview: Value of Good CTI

- It can differentiate mediocre. Vs. high quality cyber security programs
- ICS cyber security incidents can:
  - Halt Operations
  - Cost millions in damage
  - Damage reputation
  - Cause loss of life, or
  - Environmental disaster

Assessing Threat Intelligence

CTI must follow CART

- **Completeness**
- **Accuracy**
- **Relevance**
- **Timeliness**

Good CTI and CART

- Clear gradient, Not Binary Qualities
- Based on use case
  - Timeliness is a good example of this gradient
  - Some intelligence (likely more strategic) has a more fluid timeliness requirement
  - Tactical threat intelligence, however, has stricter requirements.

Cyber Threat Intelligence:

- Is knowledge – the outcome of an analytic process using hypothesis-led and evidence-based analysis from a variety of data sources.
- Produces insights on adversaries and their malicious activity.
- Enables defenders, and their organizations to improve their security decision making.
- Reduces harm when teams use the insight to improve their entire cybersecurity posture.

CTI

- When integrated into a security program:
  - Reduces both mean time to recovery during cybersecurity incidents, and adversary dwell time
  - Both metrics of high interest to ICS asset owner-operators and information technology operators
- Much like weather forecasting:
  - Allows organizations and individuals to shelter and prepare Details how adversaries compromise and disrupt systems
  - Enables defenders top better prepare to protect themselves before, during, and after an incident.

CTI

Delivers on this goal by using a variety of data to produce knowledge on adversaries such as:

- **Who** adversaries are, comprising the actors, sponsors, and employers
- **What** adversaries use, including their capabilities and infrastructure
- **Where** adversaries target, detailing industries, verticals and geographic regions
- **When** adversaries act, identifying timelines and patterns of life
- **Why** adversaries attack, including their motives and intent
- **How** adversaries operate, focused on their behaviors and patterns

CTI: 3 Question Rule

Threat	What is the threat? Addressing who, what, where, when, why and how.
Impact	What is the impact to an organization if the threat were realized?
Action	Which actions mitigate the threat in both the near- and mid-term?

CTI – Two Elements

Context	Context Describes the threat and proves or disproves the relevance and impact to the audience
Action	What is the impact to an organization if the threat were realized?

CTI

- Threat Intelligence Actions Include:
  - Detective guidance such as technical indicators or signatures of the activity to support identifying breaches in an environment
  - Policy guidance to protect the organization from a potential disruption hopefully leading to threat prevention
  - Detailed threat behavior to enable hunting for similar behavior
  - Data collection suggestions to support effective detection
  - Threat scope and impact details supporting risk-based strategic decision-making

CTI – 3 categories

Threat Intelligence Type	Audience	Description
Tactical	Security Operations Network Defenders Incident Response	Technical indicators and behaviors to inform network level action and remediation
Operational	Threat Hunters Incident Response Security Leadership	Intelligence on adversary behavior informing: holistic remediation, threat hunting, behavioral detection, purchasing decisions, and data collection.
Strategic	Security Leadership Organizational Leadership	Places threat into a business context and describes strategic impact informing risk management and organizational direction.

CTI - Using threat intelligence

- There is no one-stop shop for solving the complexities of protecting critical assets in any environment.

- CTI compliments:
  - Detection
  - Response
  - Prevention

CTI Uses

- There is no one-stop shop for solving the complexities of protecting critical assets in any environment.
  - Detect
  - Respond
  - Prevent

CTI: IT vs OT Threat Intelligence

- There is no “universal” threat intelligence. Threat intelligence products should be tailored for the use cases and security demands of specific classes of environments.
- ICS Threat Intelligence
  - Interested Adversary
  - Direct ICS Threat
  - Indirect ICS Threat

CTI: ICS Threat Intelligence

Interested Adversaries	Intelligence on activities of adversaries known to have an interest in control systems and operations networks. Example: DRAGONFLY compromises victim networks to gather information on the industrial control system and related operations but have not yet been identified disrupting or directly interfacing with industrial control systems
Direct ICS Impact	Intelligence on threats directly affecting the operation of industrial control systems Example: CRASHOVERRIDE is a malware framework designed and deployed to disrupt electric power transmission
Indirect ICS Impact	Intelligence on threats not associated with industrial control systems but have a high likelihood of disrupting their operation Example: WANNACRY ransomware does not target industrial control systems, but its capability has shown to be debilitating to organizations when it can access operational networks

CTI: Three Distinguishing Products

Data Sources and Visibility	A producer must have the data sources and visibility into the threats affecting the customer's environment. Without the proper data, there can be no relevant intelligence.
Contextual Awareness	A producer must have an understanding of the customer's business in order to make intelligence immediately relevant. Otherwise, the customer must translate all intelligence into their domain themselves.
Action, Relevance	A producer must understand the customer's operations so that they may recommend proper actions without causing any undue harm or simply stating generic best practices.

Intelligence Sources and Confidence

Intelligence Sources

- CTI Sources are typically:
  - Data sources (PCAP, other forensic artifacts such as logfiles, physical media)
  - Telemetry / Net flow data
  - Endpoint devices (third party)
  - Data Historians, or databases

Intelligence Sources

- Can have blind-spots
- Exhibit collection bias
- Require corroboration
- For ICS must have specific ICS honeypots to gain actionable insight:
  - Beyond port 502 (MODBUS), 20000 (DNP3)
  - Need asset visibility to understand context
  - Subject matter expertise on intricacies of ICS environments

Sources and Confidence

- All sources need confidence levels
- Good assessments use corroborated sources
- Sources should be described in terms of context
  - If data comes from a third-party tool, it must be attributed to that tool

Intelligence Sources and Confidence

- Assessments in CTI require confidence levels
- Sherman Kent (CIA Kent School of Analysis) defines confidence levels as Kent's words of Estimative Probability

Intelligence Sources and Confidence

Certain	100%
Almost Certain	93%
Probable	75%
Chances about even	50%
Probably not	30%
Almost Certainly not	7%
Impossible	0%

CTI – Low Confidence

- A hypothesis that is supported with available information.
- The information is likely single sourced and there are known collection/information gaps. However, this is a good assessment that is
- supported. It may not be finished intelligence though and may not be appropriate to be the only factor in making a decision.

CTI Moderate Confidence Assessment

- A hypothesis that is supported with multiple pieces of available information and collection gaps are significantly reduced.
- The information may still be single sourced but there's multiple pieces of data or information supporting this hypothesis.
- We have accounted for the collection/information gaps even if we haven't been able to address all of them.

CTI High Confidence Assessment

- A hypothesis is supported by a predominant amount of the available data and information.
- it is supported through multiple sources, and the risk of collection gaps are all but eliminated. High confidence assessments are almost never single sourced.
- There will likely always be a collection gap even if we do not know what it is but we have accounted for everything possible and reduced the risk of that collection gap;
  - Even if we cannot get collection/information in a certain area it's all but certain to not change the outcome of the assessment.

Diamond Model

Diamond Model

- It's all about context
- Dragos defines 4 qualities of an activity group:
  - Infrastructure
  - Adversary
  - Capabilities
  - Victims

Dragos Activity Groups

The Diamond Model

ADVERSARY

- Associations with other groups/activities
- Home base
- Languages/cultural references
- Working hours
- Pattern of life

INFRASTRUCTURE

- C2 nodes
- Domains
- Hosting
- Obfuscation

CAPABILITIES

- Expertise
- Operational discipline
- Malware type: operational, open source, bespoke
- Exploit development
- Tools
- Espionage or disruption or both?

VICTIM

- Target description
- Apparent target objectives
- At Dragos, an AG is only named if the adversary aims for or purposefully affects ICS and/or OT of its target

Parasite

2017 - 2020

ICS IMPACT: Operations focus on ICS-related organizations, limited to IT network actions for initial access and information collection

ADVERSARY

- No links to tracked activity groups

INFRASTRUCTURE

- Adversary controlled domains & infrastructure for C2 & delivery
- Tor exit node to launch attacks

ACTIVITY GROUP

CAPABILITIES

- Exploiting known VPN vulnerabilities; SSH.NET, MASSCAN, dsniff, Impacket

VICTIM

- Oil & Gas, Aerospace, Utilities, Government, NGOs
- US, Middle East, Australia, Europe

Parasite

2020 - 2021

ICS IMPACT: Secondary disruption to OT networks and the risk of sensitive OT data leakage through ransomware deployment

ADVERSARY

- No links to tracked activity groups

INFRASTRUCTURE

- Adversary controlled domains & infrastructure utilizing self-signed SSL certificates

ACTIVITY GROUP

CAPABILITIES

- Deployment of Pay2Key ransomware

VICTIM

- Critical infrastructure and Oil & Gas entities
- Israel, Europe (unconfirmed)

Xenotime

SINCE 2014

ICS IMPACT: Demonstrated capability to execute disruptive ICS attacks, such as the 2017 TRISIS incident.

ADVERSARY

- Unique tool development

INFRASTRUCTURE

- Virtual Private Server and compromised legitimate infrastructure
- European web hosting providers
- Asian shipping company

ACTIVITY GROUP

CAPABILITIES

- TRISIS
- Custom credential harvesting
- Off-the-shelf tools

VICTIM

- Oil & Gas, Electric Utilities
- Middle East, Europe, North America, Australia

How Threats Differ across Industries

Every Industry is Different but…

- Different industry Verticals
  - ONG
  - Electric
  - Pharma
  - Chemical
- What differs?
  - Environments
  - Impacts

Industry Vertical

- Context is key (I said this before)
- Subject Matter Expertise
  - Each vertical has potentially unique environment
- What about OT?
  - OT is OT, but how it is implemented can differ
  - How it interfaces with IT…

OT Interfaces with IT

This will likely differ greatly across verticals

Q & A

Sources

- https://www.dragos.com/wp-content/uploads/Industrial-Control-Threat-Intelligence-Whitepaper.pdf
- http://www.activeresponse.org/the-4-qualities-of-good-threat-intelligence/
- *Sherman Kent and the Profession of Intelligence Analysis*, Center for the Study of Intelligence, Central Intelligence Agency, November 2002, p. 50
- http://www.robertmlee.org/blog/