Industrial Control Threat Intelligence

By Sergio Caltagirone
Director, Threat Intelligence, Dragos

Executive Summary

Modern network and asset defense require far greater visibility into the industrial control system threat landscape than in years past. The threat environment is highly dynamic, and adversaries who invest in the problem are outpacing defenders who do not. Threat intelligence is knowledge of adversaries and their malicious behaviors through which defenders gain better visibility. Threat Intelligence reduces harm by improving decision making before, during, and after cybersecurity incidents reducing operational mean time to recovery, reducing adversary dwell time, and enabling root cause analysis. It is a necessary component of any modern cybersecurity program that significantly improves the efficacy of all existing elements.

However, there is no "universal" threat intelligence product, so, organizations must match threat intelligence products to their threat profile. Generic threat intelligence developed around traditional information technology (IT) environments will not satisfy the unique requirements for industrial control. Therefore, industrial control system (ICS) owners and operators and IT groups that have ICS in their environment should seek out and obtain an ICS threat intelligence product, regardless of whether they are already receiving generic threat intelligence.

Threat intelligence must include both context and action and be delivered in a way to maximize its value to the consumer. Threat intelligence provides three critical elements: describe the threat, illustrate the impact, and recommend action. But, not all threat intelligence is equal, and consumers must be careful about consuming poor threat intelligence so as not to waste precious time and resources (e.g., indicator feeds without context). Good threat intelligence satisfies four primary properties: completeness, accuracy, relevance, and timeliness (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.

Contents

Executive Summary 1

Threat Intelligence 3

- Threat Intelligence Context 5
- Threat Intelligence Action 6
  - Indicators of Compromise (IOCs) 6
  - Behavioral Analytics 6
  - Conscious Non-Action (a.k.a. FUD-busting) 7
- Three Categories of Threat Intelligence 7
  - Tactical Threat Intelligence: Security Operations, Network Defenders, Incident Response 8
  - Operational Threat Intelligence: Threat Hunters and Security Leadership 9
  - Strategic Threat Intelligence: Security and Organizational Leadership 9

Using Threat Intelligence 9

The Difference Between ICS and IT Threat Intelligence 11

- Complementary Threat Intelligence Products 12
- Distinguishing Threat Intelligence Products 12
  - Data Sources and Visibility 13
  - Contextual Awareness 13
  - Action Relevance 13

The Threat Intelligence Role in IT-ICS Integration 14

Vulnerability Analysis 14

Measuring Threat Intelligence Quality 15

Measuring Threat Intelligence Impact 17

- Information Technology (IT) Threat Intelligence Measurement 17
- ICS Operations Threat Intelligence Measurement 17

Threat Intelligence

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

What is Threat Intelligence?

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

Threat intelligence 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 how weather forecasting allows organizations and individuals to shelter and prepare, threat intelligence details how adversaries compromise and disrupt systems so that defenders can better prepare to protect themselves before, during, and after an incident. Threat intelligence 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

Threat intelligence should answer three questions, known as the “3 Question Rule.”

Threat Intelligence "3 Question Rule"

All threat intelligence should answer three questions enabling the audience to quickly identify the relevance and impact their organization followed by immediate action if necessary.

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?

Threat intelligence answers these questions by defining the context – who should care about the threat and why; and by defining the action to be taken – how to protect and defend against it. Without context, threat intelligence lacks the necessary descriptive elements supporting decision making such as detection priority, or the relevance of the threat to an environment. Without action, threat intelligence lacks impact and tends to be useless to consumers already over-burdened with data.

Threat Intelligence: A composite of Two Elements

Threat intelligence is comprised of two elements: context and action. Without either intelligence is neither actionable nor understandable.

Context	Context describes the threat and proves or disproves the relevance and impact to the audience. "Context is king" is helping organizations properly prioritize
Action	What is the impact to an organization if the threat were realized?

Threat Intelligence Context

Threat intelligence context provides the necessary relevance around any threat. Not all threats are equal. Some threats only affect specific industries, verticals, or geographic regions. Some threats only affect particular technologies. Threats behave in different ways independent of their specific capabilities and infrastructure. Threat intelligence context addresses these and other factors, enabling defenders to identify whether they should care enough to take action quickly. Further, during threat detection, threat intelligence context enables quick prioritization and more effective incident response with reduced time to mitigation.

Threat intelligence context usually includes:

- A description of each Diamond Model feature
- A description of adversary behavior throughout the ICS Kill Chain
- Technical descriptions including network activity, malware analysis, and host and log activity
- Impact assessments, scenarios, and risk analysis to familiar industrial operating environments
- Important references for further research

EXAMPLE Threat Intelligence Context

Impact: **High**
Industries: **Electric Power Transmission**

Several public utilities involved in power transmission were compromised between 10 and 30 July 2017 using spear phishing emails. The emails contained a malicious Word document exploiting vulnerability MS08-067 successfully on unpatched workstations and then began worm-like activity spreading through the network via SMBv1 looking to cross network segments. The worm actively looks for historian applications and other evidence of operational networks involved in electric power transmission.

Once the worm discovered evidence of an operational network, the worm then contacted the command-and-control server at IP X.X.X.X via HTTPS registering the victim with the adversary. The adversary would then use the remote access capabilities of the worm to access the network and use local PowerShell resources to begin further internal reconnaissance and targeting. Dragos assesses with high confidence that the adversary is in the process of Stage 1 – information gathering prior to developing or deploying capabilities to disrupt electric power transmission.

Due to the very specific targeting of organizations involved in electric power transmission, this threat may not be relevant for organizations outside that industry. However, this threat does present general vulnerabilities and opportunities in all networks, and all owner/operators should examine their networks with regards to this threat behavior to prevent such attacks to their network in the future.

See also ….

Figure 1. Example Threat Intelligence Context

Threat Intelligence Action

Threat intelligence action provides technical and policy recommendations customized for the threat, its behavior, and impact. Threat intelligence action ranges from technical details enabling detection and hunting to the most strategic insight useful for company officer or board-level briefings.

Threat intelligence action recommendations usually 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

Indicators of Compromise (IOCs) are technical elements of information used to enable threat detection, and they're one component of threat intelligence action. Commonly, indicators of compromise (IOCs) include internet protocol (IP) addresses, domain names, file names, file hashes, etc. IOCs are designed to be compared with organizational logs to identify compromises. They're usually provided as "feeds" to ingest into SIEM platforms to generate alerts for a security operations center (SOC) much like anti-virus alerts. Contrary to the marketing messages of some providers, indicators of compromise are not threat intelligence, they are a component of threat intelligence but by themselves add little value. Instead, threat intelligence must contextualize IOCs for defenders as part of full-formed threat intelligence.

Threat Behavior Analytics identify system or user actions indicating suspicious or malicious activity. Like their name, they detect adversary tradecraft (i.e., behavior) rather than specific technical elements known to be bad. Threat behavior analytics have a long lifespan and are difficult for adversaries to modify, unlike IOCs which have a short lifespan and are easier for adversaries to modify. Threat behavior analytics can range from very simple to very complex correlating data across one or many sources. The best behavior analytics leverage contextual knowledge of the environment such as understanding the role of assets or users. For instance, the set of suspicious behaviors related to programmable logic controllers (PLCs) differ greatly from those surrounding an OPC or SQL server. Robust behavior analytics improve detection effectiveness by orders of magnitude beyond traditional detection mechanisms (such as anti-virus) because they're neither generic like anomaly-based approaches nor static like signature-based approaches. Behavior analytics also drive cost of ownership lower due to better false-positive and true-positive rates which are challenging for current machine-learning or anomaly-based approaches. Lastly, the context provided with each behavior analytic greatly improves response time as it enables teams to more rapidly move beyond detecting the threat and into scoping and responding to it.

EXAMPLE Threat Intelligence Action

Detect and mitigate any inbound or outbound network activity associated with IP address X.X.X.X between 10 July and 30 August 2017 due to its use as command-and-control for malicious activity – while HTTPS was leveraged in the known cases any communications should be suspect

Patch MS08-067 across the enterprise to prevent initial compromise

Prevent SMBv1 communication between IT and operational networks (e.g., OT, PCN) to prevent potential spread of the worm. Where SMBv1 is necessary for business operations, Dragos suggests operational networks restrict all SMBv1 activity/traffic except from necessary locations.

The adversary leverages Windows PowerShell almost exclusively after initial access within a victim network – we recommend monitoring all PowerShell activity for behaviors associated with the activity described and disabling PowerShell on all hosts where it is unnecessary

Due to the high impact on operations caused by this threat including the loss of electric power transmission, it is recommended every organization involved in that activity prioritize this threat

Figure 2. Example Threat Intelligence Action

Conscious Non-Action (a.k.a. FUD-busting)

Consciously choosing not to take action is just as important as taking action. Taking action on all threat intelligence is a mistake. Consumers must evaluate threat intelligence for relevance and priority. That news story sensationalizing a recent attack may not be the most critical item of the day and applying focus may waste precious and expensive security resources. Effective threat intelligence provides supportive context, priority ranking, and an honest opinion of news likely to make your management ask questions so the team can stay focused on the right things. Threat intelligence should inform both action and non-action.

Consciously choosing not to take action is just as important as taking action; threat intelligence should inform both action and conscious non-action.

Three Categories of Threat Intelligence

Threat intelligence is generally categorized into three types: tactical, operational, and strategic. Many make the mistake of thinking the type of information determines the category – but that is incorrect. Intended audience, and their sphere of influence and action determine the threat intelligence category. Threat intelligence is most readily understood and properly applied when molded and delivered in packages designed for a specific audience.

For instance, we may present a CEO with strategic intelligence useful to manage business elements such as risk management, regulatory compliance, customer and employee safety, infrastructure investments, etc. While

alternatively, we present the tactical network defender technical opportunities which don't necessarily require understanding adversary intent and motivation.

Some threat intelligence providers will make a distinction between the categories and may even package them separately. Others will blend them into single reports or packages. What matters most is that the threat intelligence targets the various levels of the organization and informs them appropriately to maximize impact.

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.

Tactical Threat Intelligence: Security Operations, Network Defenders, Incident Response

Tactical threat intelligence targets network defenders and incident responders responsible for the most technical level of investigation and detection. This intelligence generally conveys technical indicators and behaviors to inform network-level action and remediation. Content generally included in tactical intelligence includes:

Tactical threat intelligence may include:

- Indicators such as IP addresses, domains, etc.
- Highly technical details such as malware reverse engineering analysis
- Network traffic and host behavior details

Operational Threat Intelligence: Threat Hunters and Security Leadership

Operational threat intelligence targets threat hunters and security leadership, providing intelligence on adversary behavior informing holistic remediation, hunting, incident response and behavioral detection. Additionally, operational intelligence should inform purchasing and data collection decisions to close strategic gaps in telemetry or defense.

Operational threat intelligence may include:

- Campaign history
- Behavioral descriptions
- End-to-end adversary operations

Strategic Threat Intelligence: Security and Organizational Leadership

Strategic threat intelligence targets security and organizational leadership, providing intelligence on business context and impact to inform risk management and organizational direction.

Strategic threat intelligence may include:

- Adversary background
- Assessed intent and motivation
- Business impact
- Victimology
- Forward-looking statements regarding likely adversary evolution, interests, and intent

Using Threat Intelligence

Threat intelligence alone cannot protect critical assets. Instead, threat intelligence complements every component of a cybersecurity practice: detection, response, and prevention. Threat intelligence, when appropriately used, will reduce harm to the organization because it increases the effectiveness of every component, ultimately decreasing mean time to recovery in operational networks and reducing adversary dwell time in traditional information technology environments. In optimal cases, threat intelligence may enable a defender to view “over the horizon” from their environment preventing a threat entirely.

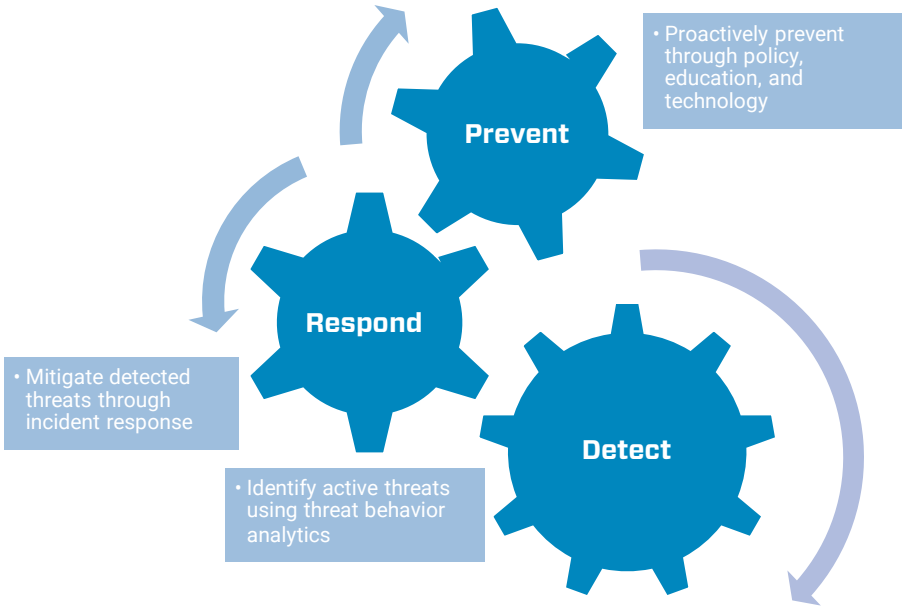

*Figure 3.**Detect**, **Respond**, and **Prevent**: the components of an effective defense that benefit from threat intelligence*

- **DETECT:** Threat intelligence detailing adversary operations enables detection through threat behavior analytics in addition to individual technical indicators which have a short life-span.
- **RESPOND:** Threat intelligence-informed incident response is directly correlated with a quicker and more complete threat remediation because responders begin with base knowledge rather than starting blindly. A speedier remediation means quicker time to recovery and reducing adversary dwell time where business can return to normal more quickly and with reduced impact.
- **PREVENT:** Properly used threat intelligence can prevent harm in many cases. The knowledge of the threat environment and adversary operational behaviors can broadly inform proactive protection and prevention activities.
    - Inform **architectural** decisions and technology procurement with a complete knowledge of the threat environment and potential gaps in coverage
    - Identify and address **data collection** gaps where adversary activity may hide that improves detection and response capabilities
    - Improve **assessment** (e.g., Red Team, Blue Team) by modeling actual threat behaviors to strengthen risk prioritization and measure performance against real adversaries
    - **Educate** users with actual threat stories to enhance their ability to protect the business by taking better action and noticing/reporting suspicious activity
    - Build accurate **threat models** using knowledge of adversary behavior instead of only hypothetical scenarios

The Difference Between ICS and IT Threat Intelligence

Threat intelligence is no "universal" threat intelligence. Threat intelligence tailors itself for the specific use case and security demands of a particular threat and customer environment. While operational networks share some cybersecurity approaches with traditional information technology (IT), they are not the same. IT and OT/ICS don't have the same threat landscape, they don't have the same consequences should incidents occur, and they don't have the same decision-making calculus. Therefore, they can't have the same threat intelligence.

ICS threat intelligence falls into three categories: **Interested Adversary, Direct ICS Threat,** and **Indirect ICS Threat.**

There is no "universal" threat intelligence. Threat intelligence products should be tailored for the use cases and security demands of specific classes of environments.

Any threat intelligence that does not conform to one of these categories is, at most, peripheral to the protection of industrial control systems.

ICS Threat Intelligence Categories

ICS threat intelligence falls into three categories – intelligence not conforming to these categories generally does not support industrial control security demands.

Interested Adversaries	Intelligence on activities of adversaries known to have an interest in control systems and operation 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

Complementary Threat Intelligence Products

In a large enterprise containing both traditional IT components and industrial control systems, a threat profile will be complex, and cross several threat domains. Therefore, for most organizations, no single threat intelligence product will satisfy the entire landscape. For instance, one provider may focus on email-borne threats while others on cloud-based threats, botnets, or ransomware. And then, very few, like Dragos, focus exclusively on industrial control system threats. These products complement each other to organizations with ICS threat profiles. For these organizations, having both traditional IT-focused threat intelligence AND ICS-focused threat intelligence products is essential to an effective defense.

Having both traditional IT-focused threat intelligence and ICS-focused threat intelligence products is essential to an effective defense.

Distinguishing Threat Intelligence Products

Three primary elements distinguish threat intelligence products: data sources and visibility, contextual awareness, and action relevance. It is essential when choosing threat intelligence products that an organization examine these carefully, or risk wasting money on an unsatisfactory choice.

Three elements clearly distinguish threat intelligence products. An evaluation of any threat intelligence product and producer should examine these elements which will help a customer select the best ones for their business.

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.

Data Sources and Visibility

Threat intelligence is entirely dependent on its source data and visibility into the threat landscape to generate useful insights. Threat intelligence providers cannot collect and see everything for every threat landscape. Therefore, each must curate their data sources and visibility to best address a subset of the threat landscape.

For industrial control threats, it requires curating threat data associated with industrial control environments. For instance, creating a network of honeypots and merely measuring network activity on TCP port 502 (MODBUS) is insufficient to gather any actionable intelligence on the ICS threat. Any network scanner doing a broad-based port scan will likely touch port 502 as a matter of course, unconnected to any threat. Effective industrial control-related intelligence gathering requires specific ICS honeypots to gain the actionable insight into adversaries targeting those systems. Be sure to ask potential threat intelligence providers about their visibility and data sources to ensure those align with the threats in your threat profile.

Contextual Awareness

Simple awareness of malicious activity is insufficient for effective decision making. Intelligence must be contextualized appropriately to ensure usefulness. Context provides the critical elements describing the threat, the impact, and risk measurement that support prioritization because there are too many threats for any organization to protect against or respond to all of them. However, to properly contextualize threats the threat intelligence producer must understand the customer's environment and operational requirements. Without the in-depth knowledge of industrial control system technology and operations, traditional IT threat analysts generally fail to adequately contextualize intelligence into ICS. Only analysts with such in-depth knowledge of ICS technology and operations can provide threat intelligence with context that advises effective decision making.

Action Relevance

Threat intelligence should lead to action. Threat intelligence that does not lead to action is a waste of time in most cases. Threat-intelligence driven action comes from a complete list of well-informed, threat specific recommendations to protect organizations. Generic recommendations provide no value (e.g., make sure patching is up-to-date), and highly speculative, ill-informed recommendations can lead to poor or disastrous results. Therefore, threat intelligence providers must understand customer environments and operational requirements to make useful recommendations. Just like contextual awareness for ICS, this requires analysts with a rich understanding of ICS technology and operations. Its absence can produce irrelevant, generic, or even harmful recommendations that erode, rather than enhance security.

The Threat Intelligence Role in IT-ICS Integration

Most ICS threats traverse the traditional IT (sometimes referred to as "business") networks whether they are within the same organization or pivot through a vendor or integrator's IT infrastructure. This behavior is typical because traditional IT networks are usually the only internet-connected portion of the enterprise. Adversaries take advantage of separate, uncoordinated organizational security structures, exploiting the seams and gaps to pass through undetected and unmitigated. Protecting the entire enterprise requires a holistic approach. Threat intelligence can bridge the IT-ICS divide.

Traditional IT network defenders should understand the threat landscape to the operational network because they'll likely be the front-door to most of the threats. Therefore, IT is usually in the best position to stop the threat before it reaches any operational environment. ICS threat intelligence should strive to help IT network defenders understand the threat impact and context to operations. ICS threat intelligence should also empower IT to take action to reduce the risk of threats utilizing their network to access any operational environments.

ICS network defenders should use ICS threat intelligence to collaborate with IT to identify weaknesses between the environments and reduce the exposure surface to minimize the opportunities for any adversaries. Of course, ICS threat intelligence should provide actionable recommendations for operators to protect their equipment and processes from disruption.

Together, with threat intelligence spanning both IT and ICS, an organization can take a holistic approach to secure itself against adversary tradecraft that exploits seams between organizations.

Vulnerability Analysis

Vulnerability analysis is the ability to uncover and understand the vulnerabilities inherent in every system that can be leveraged by adversaries to cause undesired effects. Vulnerabilities can result in adversaries gaining unauthorized access, executing unauthorized instructions/code, or disabling systems entirely. Vulnerability analysis is a critical component of good threat intelligence and when combined with adversary operations, completes the intelligence picture to make a potent tool for defenders.

Hundreds of vulnerabilities are detected and disclosed every month. This steady stream creates a major challenge for defenders who have to wade through all of these vulnerabilities to understand them in context of their environment and conduct a risk assessment – a difficult task.

The most useful threat intelligence supports defenders in their efforts to address these vulnerabilities. Threat intelligence-based vulnerability analysis provides four critical elements enabling quick assessments by defenders: description, threat awareness, impact, and mitigation. For example, a significant portion of ICS vulnerabilities released introduce little-to-no risk and many times the details of the vulnerability have been incorrect. Intelligence-based vulnerability assessment should clarify and add context to ensure asset owner-operators are better informed to prioritize and take the appropriate action.

Vulnerability Description Elements

Vulnerability analysis is necessary for complete threat intelligence. Threat intelligence producers must include our elements of information about a vulnerability to ensure good decision-making.

Description	A short and easily-understood description of the vulnerability accessible to most security professionals
Threat Awareness	Understanding the vulnerability in the threat environment, including active exploitation and the scope and scale of such use
Impact	The potential impact of the vulnerability when leveraged by an adversary
Mitigation	The actions available to defenders to prevent or reduce the risk of the vulnerability impacting operations

Measuring Threat Intelligence Quality

Poor threat intelligence is worse than no threat intelligence at all. Poor threat intelligence leads to bad decisions that waste precious resources and yield potentially harmful consequences to business and operations. Therefore, it is imperative that organizations carefully evaluate their threat intelligence providers and choose those who demonstrate a commitment to only high quality. But, how do you assess threat intelligence?

Threat intelligence quality should be measured across four primary dimensions: **Completeness, Accuracy, Relevance,** and **Timeliness** (CART). Threat intelligence lacking any of these qualities will likely not satisfy your requirements and may just waste valuable time and resources, or worse yet, cause a detrimental impact.

Dimension	Description	Three Critical Evolution Questions
C Completeness	Threat intelligence must provide sufficient detail to enable a proper response	1. Does the threat intelligence cover all of the critical digital forensics domains? Host forensics, malware analysis, network traffic analysis, and log analysis? 2. Does the threat intelligence incorporate vulnerability analysis? 3. Does the threat intelligence correlate across the entire threat spectrum and incorporate non-cyber intelligence and events to produce a complete threat profile?
A Accuracy	Inaccurate threat intelligence is worse than no threat intelligence and any quality threat intelligence must be accurate	1. What data sources corroborate threat intelligence to ensure accuracy? 2. Is the threat intelligence updated when new information is learned or knowledge changes? 3. Is the threat intelligence time-bound to ensure that customers understand the limited nature of the information?
R Relevance	Threat intelligence must address only relevant threats to the organization and be delivered in a method that allows for effective action	1. What data sources and visibility are used and do they identify threats to my organization? 2. Do the analysts have experience with my business and operations to ensure proper context and actionable recommendations? 3. How do customers submit requirements and provide feedback to support more relevant intelligence?
T Timeliness	Threat intelligence must be produced and delivered quickly so that it can be and used fast enough to make a difference	1. How is the threat intelligence delivered to ensure quick consumption? 2. How long between the discovery of a threat and customer notification? 3. Is threat intelligence released as it is learned or is it held back for more data before informing customers?

Measuring Threat Intelligence Impact

Measuring threat intelligence impact and return-on-investment (ROI) is challenging, as it is with many aspects of a security program. However, there are two simple metrics generally effective at measuring threat intelligence ROI: adversary dwell time and time to recovery. Effective integration of threat intelligence with security programs should reduce both.

Information Technology (IT) Threat Intelligence Measurement

In an information technology environment, the best metric to assess threat intelligence value is a reduction in Mean Adversary Dwell Time. **Adversary Dwell Time** is the time measured between when an adversary first gained unauthorized access to a network/system and when incident response successfully severed adversary access and control. Calculating the mean adversary dwell time requires an organization to maintain records of the dwell time between incidents and then choose a timeframe (generally yearly) on which to calculate the average dwell time of all incidents. Security programs integrated with threat intelligence show marked improvement in prevention, detection, and response meaning dwell time should fall year-over-year.

ICS Operations Threat Intelligence Measurement

Industrial control networks operate differently than information technology networks. Therefore, the metric to determine threat intelligence effectiveness is different. In industrial control, the critical metric is Mean Time to Recovery. **Time to Recovery** measures the time when an adversary first causes an operational disruption to when operations return to normal. Calculating mean time to recovery requires an organization to maintain a record of all cyber activities creating operational impact and the period from the beginning of disruption until the resumption of normal operations. The mean time is then the average impact of all operational incidents (generally yearly). ICS/OT security programs integrated with threat intelligence should be able to improve prevention, detection, and response to a cyber-event recovering operations from any impact on visibility, control, or safety more quickly meaning time to recovery should fall year-over-year.

Dragos WorldView ICS Threat Intelligence - Trial Subscription

Dragos WorldView is the Industrial Cybersecurity industry's only product *exclusively* focused on ICS/OT Threat Intelligence. Please Visit **https://dragos.com/worldview/** for more information and to request a trial Dragos WorldView subscription.