

Achieving & Measuring the Value of Cyber Threat Information Sharing

Lindsley Boiney, Clem Skorupka (presenting)

The MITRE Corporation

2018 International Information Sharing Conference

McLean, VA

Acknowledgements

This presentation is based on work conducted by the Homeland Security Systems Engineering & Development Institute.



The Homeland Security Systems Engineering & Development Institute (HSSEDI) is a federally funded research and development center (FFRDC) established by the Secretary of Homeland Security under Section 305 of the Homeland Security Act of 2002. The MITRE Corporation operates HSSEDI under the Department of Homeland Security (DHS) contract number HSHQDC-14-D-00006.

HSSEDI's mission is to assist the Secretary of Homeland Security, the Under Secretary for Science and Technology, and the DHS operating elements in addressing national homeland security system development issues where technical and systems engineering expertise is required. HSSEDI also consults with other government agencies, nongovernmental organizations, institutions of higher education, and nonprofit organizations. HSSEDI delivers independent and objective analyses and advice to support systems development, decision making, alternative approaches, and new insight into significant acquisition issues. HSSEDI's research is undertaken by mutual consent with DHS and is organized by tasks.

This report presents the results of concept exploration and analysis conducted under HSHQDC-17-J-00039: CS&C Front Office Advice and Analysis. The purpose of the task is to provide strategic advice and guidance regarding technically oriented challenges to senior decision-makers to assist in the growth and development of the homeland security enterprise.

The information presented in this report does not necessarily reflect official DHS opinion or policy.



The Cyber Operations Rapid Assessment (CORA) was developed under the MITRE Innovation Program Project No.: 25MSR615-BB Approved for Public Release; Distribution Unlimited. Case Number 15-2853



The authors would also like to thank Gabe Galvan and the Mid Atlantic Cyber Center for their support.

Outline

- **Abstract**
- **Background: CORA**
- **TVIS: Trust and Value in Information Sharing Framework**
- **Measurement**
- **Discussion and Feedback**

Abstract

- **Challenges:** Sharing cyber threat information (CTI) can meaningfully boost both individual and community defenses. However, threat sharing bodies (TSBs) often face challenges motivating initial and ongoing sharing between organizations due to the inherent sensitivities, risks, and costs involved.
- **Framework:** The *Trust and Value in Information Sharing (TVIS)* framework identifies the differentiated **value proposition** and degree of inter-organizational **trust** needed for sharing across a continuum of CTI sharing roles:
 - Passive Consumer, Active Consumer, Reporter, and Producer.
 - It provides **specific, actionable recommendations** for TSBs to build more robust, value-focused exchanges across diverse member organizations.
- **Measures:** The TVIS framework is further leveraged to develop a menu of candidate **performance measures** that TSBs can select from to capture the value of sharing from each role's perspective.
 - The candidate performance measures cover three aspects of the information sharing process essential for delivering value: quality CTI **content**, effective **exchange** of CTI, and **impact** on member security from leveraging CTI.

Background

- In recent years, the cybersecurity ecosystem has promoted the importance of sharing cyber threat information* to *boost individual and community defenses*
- Much of this *sharing is facilitated* through threat sharing bodies (TSBs) such as Information Sharing and Analysis Centers (*ISACs*) and Information Sharing and Analysis Organizations (*ISAOs*)
- But there are *challenges* in motivating initial and ongoing sharing between organizations due to the inherent sensitivities, risks, and costs involved

*we use the term **cyber threat information (CTI)** to refer to all types of information relevant to an organization's cyber defense. This encompasses indicators of attack and indicators of compromise, as well as broader information relevant to threat detection, mitigation, and analysis such as malware samples, best practices, mitigation strategies, etc.

CORA™ : Cyber Operations Rapid Assessment

https://www.mitre.org/sites/default/files/publications/pr_15-2853-cyber-operations-rapid-assessment-state-of-methodologies.pdf



■ Problem

- Many organizations are behind the curve in terms of threat intelligence, relying predominantly on static defensive measures and compliance-oriented processes. Transitioning to a “threat-oriented” posture is not easy, and change needs to occur across the triad of people, processes and technologies.

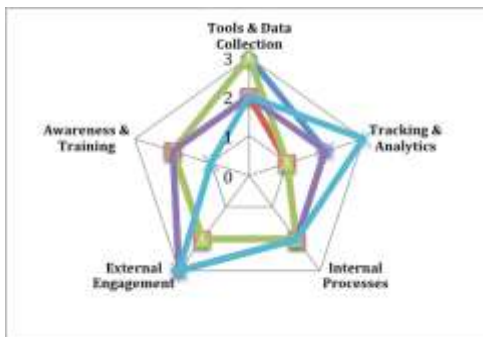
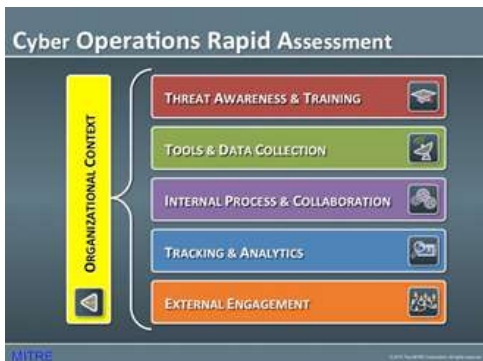
■ Idea

- MITRE has developed and piloted a Cyber Operations Rapid Assessment (CORA) methodology, to identify areas in cyber security defensive practices where improvements can be made in the collection, utilization, and sharing of threat intelligence.

■ Findings

- CORA was found applicable to organizations across a broad range of sizes, industries, and capabilities. We are able to identify focus areas for improving threat intelligence utilization and exchange. Data ownership and accessibility, knowledge management, management and user threat awareness, and integration between IT and Cyber groups were examples of key discriminators for capabilities

https://www.mitre.org/sites/default/files/publications/pr_15-2853-cyber-operations-rapid-assessment-state-of-methodologies.pdf



Perspective of TSB Member Organizations

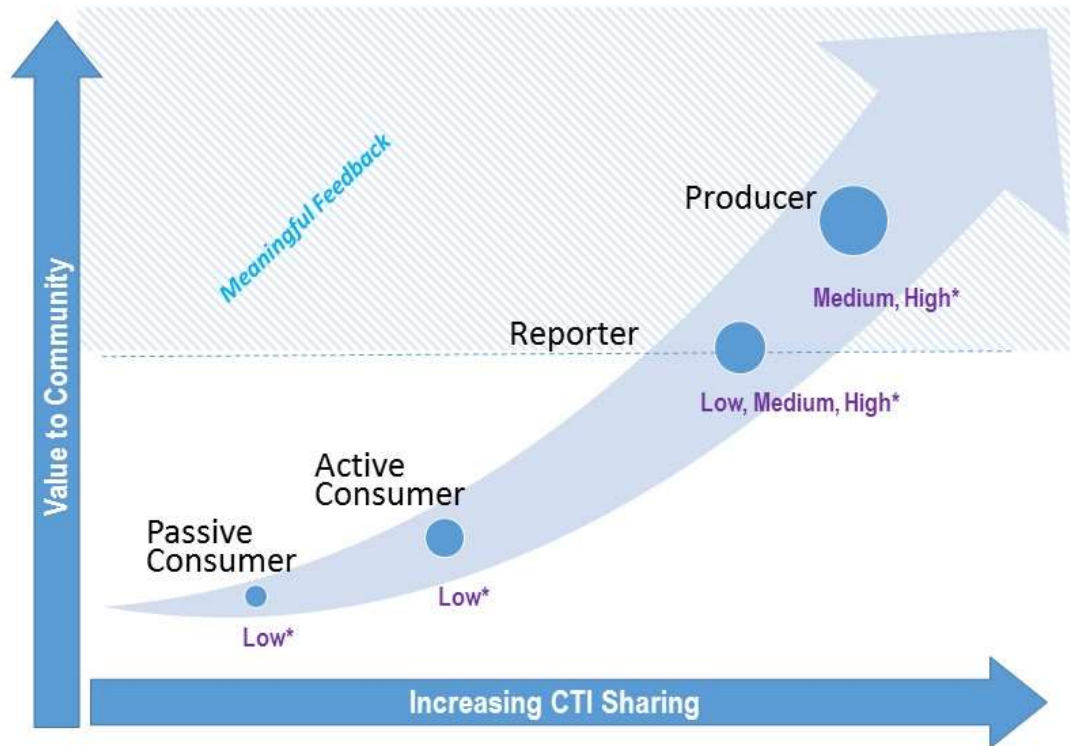
- MITRE has conducted over 30 Cyber Operations Rapid Assessment (CORA™) studies of organizations
 - Public and Private Entities
 - Range of Industries and Sectors
 - Range of size, capabilities, resources
 - Several in the context of ISAO/ISAC
- Diverse challenges affect willingness to share threat information:
 - Trust-based - *worth the risk?*
 - Ex: Unsure how information will be used
 - Value-Based - *worth the effort?*
 - Ex: Challenges filtering information
- Specific issues varied by organization's sharing role and goals

https://www.mitre.org/sites/default/files/publications/pr_15-2853-cyber-operations-rapid-assessment-state-of-methodologies.pdf

Trust and Value in Information Sharing (TVIS) framework

- Three fundamental principles:
 - A clear and relevant **value proposition** is essential to motivate an organization to expend the time, effort, and resources to participate in threat sharing activities
 - **Trust** in one's threat sharing partners and the supporting processes is also required for an organization to take the inherent risks in revealing potentially sensitive information, since either intentional or unintended disclosures could result in legal liability, reputation damage, competitive disadvantage, or even cyberattack
 - There is a **continuum of CTI sharing roles**: Passive Consumer, Active Consumer, Reporter, and Producer. Participants in different roles typically engage in different CTI sharing activities that have different values to the participants, and require different levels of trust.

TVIS Continuum: Increasing CTI Sharing Levels



*Level of Inter-organizational Trust Required for CTI Sharing

Passive Consumer - We receive reported threat information for our situational awareness

Active Consumer - We scan our networks for reported threats, but don't report back our findings

Reporter - We scan our networks for reported threats, and also report back our findings

Producer - We scan our networks for reported threats, report, and also identify and share additional threat information


Not a Maturity Model

Value Propositions (Examples)

- **Threat Awareness**
- **Relationships**
- **Unique information**
- **Best practices**
- **Better Threat-Informed C-Suite**
- **Shared Services**
- **Improved Defensive Posture**
- **Enhanced Reputation**
- **Advanced Threat Collaboration Activities**
- **Threat Intel Enrichment from others**
- **Supply Chain Security Improvements**

Passive Consumers – Value Proposition



<i>Value To Member Organization</i>	<i>Value To Threat Sharing Body</i>	<i>Recommendations For Threat Sharing Body</i>
<ul style="list-style-type: none"> • Relationships • Access to unique information • Access to best practices • Broader threat awareness • Motivate improved cyber resource allocation to C-Suite 	<ul style="list-style-type: none"> • Broader threat awareness • Membership fees 	<ul style="list-style-type: none"> • Provide CEO-level threat briefings for awareness and buy-in • Starter Package <ul style="list-style-type: none"> - Simple use cases and testimonials on value of threat sharing - Individual threat assessment - Individual capability assessment • Guidance for evolving a security program (incremental roadmap) • Provide outsourcing guidance, including service level agreements (SLAs) with managed security service providers (MSSPs) • Host forums for sharing best practices • Facilitate relationship building among organizations with common characteristics (e.g., threat profiles or supply chain partners)
<p>TRUST NEEDED: LOW</p> 	<p>CAVEAT: unless managed, a preponderance of Passive Consumers may be resented by more active members</p>	


Active Consumers – Value Proposition



<i>Value To Member Organization</i>	<i>Value To Threat Sharing Body</i>	<i>Recommendations For Threat Sharing Body</i>
<p>All from Passive Consumers plus:</p> <ul style="list-style-type: none"> • Opportunity for shared services or resources • Utilization of CTI to improve defensive cyber posture <p>TRUST NEEDED: LOW</p> 	<p>All from Passive Consumers plus:</p> <ul style="list-style-type: none"> • Improved security of ecosystem <p>CAVEAT: with no reporting, community cannot measure effectiveness</p>	<ul style="list-style-type: none"> • Provide tailored, readily filterable (tagged) threat feeds with unique content • Provide curation to ensure high quality CTI knowledge base • Establish “sharing broker” to oversee high level TSB activity and actively facilitate engagement across the membership • Provide use cases and testimonials on value of utilizing CTI • Provide tool-agnostic instructions on how to begin tracking indicators • Provide tool-agnostic guidance on how to check logs for different threat types • Provide “starter set” of relevant indicators tailored to the organization • Provide means/framework to support sharing with organization’s MSSP

Reporters – Value Proposition

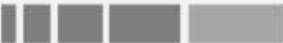


<i>Value to Member Organization</i>	<i>Value to Threat Sharing Body</i>	<i>Recommendations for Threat Sharing Body</i>
<p>All from Active Consumers plus:</p> <ul style="list-style-type: none"> • Knowledge that organization is adding value to the community • Enhanced reputation and “social credit” with peers; may lead to direct assistance from peers • Enhanced peer trust relationships may enable participation in more advanced threat discussions <p>TRUST NEEDED: LOW, MEDIUM, HIGH (varies by type of CTI)</p> 	<p>All from Active Consumers plus:</p> <ul style="list-style-type: none"> • Feedback on, and enrichment of TSB information • Reciprocity encourages Producers to contribute • Greater inter-organizational trust and support among peers <p>NOTE: Reporter role is key to feedback and measurement of performance</p>	<ul style="list-style-type: none"> • Provide guidance on what to report, emphasizing value of both null and positive sightings, and of feedback on what CTI is useful or not useful • Provide transparency in how data will be handled and shared or not shared <ul style="list-style-type: none"> - Consider a trusted third party for data management and support • Lower cost and effort to report via simple, integrated mechanisms • Acknowledge member reporting • Support both anonymous and attributed reporting • Leverage social media techniques to support collaboration <ul style="list-style-type: none"> - Track and display member reporting and feedback activity • Incentivize reporting on CTI, for instance: <ul style="list-style-type: none"> - Access to additional resources - Intangibles (e.g., recognition)

Can be difficult to motivate an organization to report


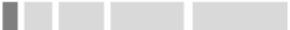






Producers – Value Proposition



<i>Value to Member Organization</i>	<i>Value to Threat Sharing Body</i>	<i>Recommendations for Threat Sharing Body</i>
<p>All from Reporters plus:</p> <ul style="list-style-type: none"> • Enrichment from other Producers • Ability to join Producer-only sharing subgroups • Potential for improved security of own supply chain <p>TRUST NEEDED: MEDIUM or HIGH</p> 	<p>All from Reporters plus:</p> <ul style="list-style-type: none"> • Unique observations and analysis • Potential for direct peer to peer assistance <p>Note: Producers have expectation of peer reciprocity, at least at Reporter level, to enhance situational awareness</p>	<ul style="list-style-type: none"> • Provide transparency in how data will be handled and shared • Provide tool suite to redact and cleanse different data types • Support membership subgroups based on: <ul style="list-style-type: none"> - Threat profile - Capabilities - Privacy requirements • Support subgroup needs for sensitive data handling <ul style="list-style-type: none"> - Vetting, requisite controls and capabilities • Host forums for sharing best practices against advanced threats • Incentivize production of CTI <ul style="list-style-type: none"> - Reduced membership fees, access to additional resources • Offer supply chain threat analysis • Provide big picture analytics (e.g., threat picture, emerging trends) for overall TSB or particular subgroups

Supporting Trust

- TSBs can support different needs for trust within subsets of their membership through practices such as
 - Allowing for both anonymous and attributed contributions
 - Supporting member subgroups with common needs for select activities
 - Employing social media-like applications to support subgroups and communities of interest
 - Deploying technical controls and protections such as encryption or authentication
 - Being transparent about how information is handled and shared internally and externally
 - Providing neutral third-party moderators and facilitators
 - Providing services such as secure portals and communication channels
 - Providing evaluation of member capabilities for protecting information
 - Providing independent review of controls

Sharing Role	Value to Individual Member Organization	Value to Threat Sharing Body	Recommendations for Threat Sharing Body
<p>Passive Consumer We receive reported threat information for the situational awareness.</p> 	<ul style="list-style-type: none"> Relationships Access to unique information Access to best practices Broader threat awareness Motivate improved cyber resource allocation to C-Suite <p>TRUST NEEDED: LOW</p> 	<ul style="list-style-type: none"> Broader threat awareness Membership fees <p>CAVEAT: unless managed, a preponderance of passive consumers may be resented by more active members</p>	<ul style="list-style-type: none"> Provide CEO-level threat briefings for awareness and buy-in Starter Package <ul style="list-style-type: none"> Simple use cases and testimonials on value of threat sharing Individual threat assessment Individual capability assessment Guidance for evolving a security program (incremental roadmap) Provide outsourcing guidance, including service level agreements (SLAs) with managed security service providers (MSSPs) Host forums for sharing best practices Facilitate relationship building among organizations with common characteristics (e.g., threat profiles or supply chain partners)
<p>Active Consumer We scan our networks for reported threats, but don't report back our findings.</p> 	<p>All from Passive Consumers plus:</p> <ul style="list-style-type: none"> Opportunity for shared services or resources Utilization of CTI to improve defensive cyber posture <p>TRUST NEEDED: LOW</p> 	<p>All from Passive Consumers plus:</p> <ul style="list-style-type: none"> Improved security of ecosystem <p>CAVEAT: with no reporting, community cannot measure effectiveness</p>	<ul style="list-style-type: none"> Provide tailored, readily filterable (tagged) threat feeds with unique content Provide curation to ensure high quality CTI knowledge base Establish "sharing broker" to oversee high level TSB activity and actively facilitate engagement across the membership Provide use cases and testimonials on value of utilizing CTI Provide tool-agnostic instructions on how to begin tracking indicators Provide tool-agnostic guidance on how to check logs for different threat types Provide "starter set" of relevant indicators tailored to the organization Provide means/framework to support sharing with organization's MSSP
<p>Reporter We scan our networks for reported threats, and also report back our findings.</p> 	<p>All from Active Consumers plus:</p> <ul style="list-style-type: none"> Knowledge that organization is adding value to the community Enhanced reputation and "social credit" with peers; may lead to direct assistance from peers Enhanced peer trust relationships may enable participation in more advanced threat discussions <p>TRUST NEEDED: LOW, MEDIUM, HIGH (varies by type of CTI)</p> 	<p>All from Active Consumers plus:</p> <ul style="list-style-type: none"> Feedback on, and enrichment of TSB information Reciprocity encourages Producers to contribute Greater inter-organizational trust and support among peers <p>NOTE: Reporter role is key to feedback and measurement of performance</p>	<ul style="list-style-type: none"> Provide guidance on what to report, emphasizing value of both null and positive sightings, and of feedback on what CTI is useful or not useful Provide transparency in how data will be handled and shared or not shared <ul style="list-style-type: none"> Consider a trusted third party for data management and support Lower cost and effort to report via simple, integrated mechanisms Acknowledge member reporting Support both anonymous and attributed reporting Leverage social media techniques to support collaboration Track and display member reporting and feedback activity Incentivize reporting on CTI, for instance: <ul style="list-style-type: none"> Access to additional resources Intangibles (e.g., recognition)
<p>Producer We scan our networks for reported threats, and also identify and share additional threat information.</p> 	<p>All from Reporters plus:</p> <ul style="list-style-type: none"> Enrichment from other Producers Ability to join Producer-only sharing subgroups Potential for improved security of own supply chain <p>TRUST NEEDED: MEDIUM or HIGH</p> 	<p>All from Reporters plus:</p> <ul style="list-style-type: none"> Unique observations and analysis Potential for direct peer to peer assistance <p>NOTE: Producers have expectation of peer reciprocity, at least at Reporter level, to enhance situational awareness</p>	<ul style="list-style-type: none"> Provide transparency in how data will be handled and shared Provide tool suite to redact and cleanse different data types Support membership subgroups based on: <ul style="list-style-type: none"> Threat profile Capabilities Privacy requirements Support subgroup needs for sensitive data handling <ul style="list-style-type: none"> Vetting, requisite controls and capabilities Host forums for sharing best practices against advanced threats Incentivize production of CTI <ul style="list-style-type: none"> Reduced membership fees, access to additional resources Offer supply chain threat analysis Provide big picture analytics (e.g., threat picture, emerging trends) for overall TSB or particular subgroups

Measurement and the CTI Sharing Process





■ Why?

- Information sharing performance measures enable TSBs to identify performance gaps and adapt services as threats evolve
- Measures can motivate broader organizational participation in sharing efforts as they help justify expenditure of time and resources

■ How?

- Measurement need not be onerous: can start small and build
- Paper presents a menu of options (not exhaustive) for TSBs
- TSBs can select and tailor measures as needed
- Some measures based on TSB data (e.g., downloads, subscriptions, attendance)
- Some measures based on *data from members* (customer satisfaction type): that's a good thing!

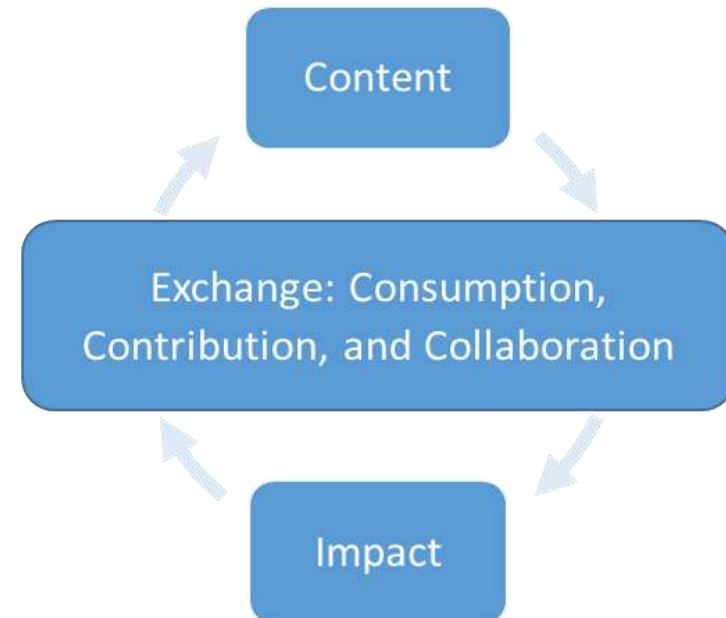
Measurement Should Capture Differentiated Value of TSB Activities

<i>Member Sharing Role</i>	<i>Value to Member Organization</i>
<p>Passive Consumer </p> <p>We receive reported threat information for our situational awareness.</p>	<ul style="list-style-type: none"> • Relationships • Access to unique information • Access to best practices • Broader threat awareness • Motivate improved cyber resource allocation
<p>Active Consumer </p> <p>We scan our networks for reported threats, but don't report back our findings.</p>	<p>All from Passive Consumers plus:</p> <ul style="list-style-type: none"> • Opportunity for shared services or resources • Utilization of CTI to improve defensive cyber posture
<p>Reporter </p> <p>We scan our networks for reported threats, and also report back our findings.</p>	<p>All from Active Consumers plus:</p> <ul style="list-style-type: none"> • Enhanced reputation and “social credit” with peers; may lead to direct assistance from peers • Enhanced peer trust relationships may enable participation in more advanced threat discussions
<p>Producer </p> <p>We scan our networks for reported threats, report, and also identify and share additional threat information.</p>	<p>All from Reporters plus:</p> <ul style="list-style-type: none"> • Enrichment from other Producers • Ability to join Producer-only sharing subgroups • Potential for improved security of own supply chain

Information Sharing is a Process

Measures should cover CTI Content, Exchange, and Impact

- Content being shared
 - Paper discusses 8 attributes of CTI quality
- Exchange of CTI within TSB
 - Consumption of CTI (*utilization*)
 - Contribution to CTI (*feedback, enrichment*)
 - Collaboration on CTI (*community*)
- Impact on Members' Security
 - Enhanced Threat Awareness
 - Improved Defensive Capabilities



Cyber Threat Information Sharing Process

Potential Benefits and Utilization of CTI Types

<i>CTI Type</i>	<i>Description / Examples</i>	<i>Potential Benefits</i>	<i>Utilization by Member Sharing Role</i>
Threat landscape briefings	Describe threats and activities of threat actors relevant to community, region, or sector.	Improve threat awareness, inform risk management, help direct allocation of resources for maximum improvement of defenses.	All Roles
Best Practices	Guidance, how-to's, lessons learned on various cyber security capabilities and technologies.	Improve cyber defensive capabilities (either technologies or processes): staffing, tracking tools, analytic tools, CONOPs, incident response, security awareness training, mitigation strategies.	All Roles
Adversary Profiles	Actor- or campaign-centric descriptions of motivations, targeting, and tactics, techniques and procedures (TTPs).	Guide response, inform development of operational capabilities, inform understanding of threat and risk.	Active Consumers, Reporters, and Producers
Indicators and Signatures	IP addresses, malicious domains or URLs, hashes of known malware files.	Tactical defense, identifying / blocking malicious activity.	Active Consumers, Reporters, and Producers
Courses of Action	Specific recommendations on how to prevent or mitigate a threat, such as malware removal instructions, patching or configuration guidance.	Improved, more complete, more timely prevention and response to mitigate risk from a given threat.	Active Consumers, Reporters, and Producers
Analytics	Network-based, host-based, or other techniques for identifying or analyzing attacks.	Tactical defense, analyzing attacks and malware, identifying new attacks.	Active Consumers, Reporters, and Producers



CONTENT: Something worth sharing?

8 Attributes of CTI Quality

- Uniqueness
- Accuracy
- Completeness
- Timeliness
- Relevance
- Consumability
- Filterability
- Richness of Context

Different member organization sharing roles have different needs and perspectives for these attributes



Attributes of CTI Quality (1 of 3)

Completeness

- Completeness captures how well the information covers the full range of relevant threats, rather than a select subset of them. More complete information reduces gaps in understanding and awareness of pertinent threats. Degree of completeness is never absolute, but can be considered relative to the TSB's stated scope, such as its associated industry sector or geographical region.

Relevance

- CTI should be relevant to the members' threat profiles. Relevance can include such factors as the type of actor (APT, cyber-criminal, hacktivist), the industry or sector being targeted (financial, healthcare, retail, defense), or the adversary tactics, techniques and procedures (TTPs) and attack vectors used (phishing, distributed denial of service (DDOS), web application attacks, ransomware).

Uniqueness

- Unique CTI is novel content not already provided elsewhere. A TSB may provide unique content via feeds that members cannot acquire elsewhere, or from member-supplied feedback (sightings, analysis, reports of false positives, new indicators) that result in uniquely enriched CTI. Not all CTI need be unique. For example, the TSB could provide summaries or retransmissions of open source, government, or commercially available information as part of its services offerings.



Attributes of CTI Quality (2 of 3)

Accuracy

- Operational consumers need some estimate of CTI accuracy in order to select and prioritize their use of indicators and other data. Measures can help address questions such as: Has the CTI been vetted by analysts against other sources? Have any false positives been reported? Over time, has the source been found to correctly identify threats?

Timeliness

- CTI should be timely enough for consumers to decide and act while the information is still relevant. The appropriate timescale could vary between seconds for a tactical decision on blocking web traffic, to hours for an operational decision to push an emergency patch, to weeks or months for a strategic decision to reallocate resources. A TSB may wish to measure the timeliness of their CTI against that of open sources, government sources, another TSB, or to their own prior performance.

Richness of Context

- Context, such as the role of an indicator in an attack, the likely intent or target of the attacker, or the associated malware, is important to make CTI actionable. A TSB may employ an attack life cycle model to capture and measure aspects of context in its CTI collection.



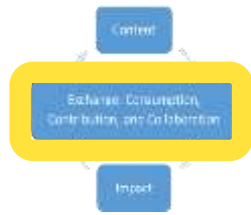
Attributes of CTI Quality (3 of 3)

Filterability

- The ability to filter CTI is important to prevent information overload. Member organizations want the right CTI for their particular threat profile, attack surface, or capabilities. Greater value can be derived from CTI when it can be filtered or prioritized according to the organization's needs and cybersecurity profile.
- Ex: member organizations may wish to filter CTI content by characteristics such as: industry sector or region; threat vector (spear phish, DDoS, etc.); threat intent (cybercrime, espionage, etc.); source (open source, government, TSB); type of CTI (IP, URL, file hash, etc.); or confidence level.

Consumability

- CTI must be consumable to have value. Members can be frustrated when they cannot effectively consume CTI because it is in a format that requires mature capabilities and resources they do not possess, because the format is not sufficiently structured to leverage their advanced capabilities, or because there is more information than they can parse usefully within their operational cycle.
- Ex: detailed, free-text threat reports may have little value to consumers without the analytic staff and resources to process them. Automated machine-readable feeds may have little value to consumers without the capabilities to automatically parse and apply relevant signatures from those feeds.



EXCHANGE: Is Someone Using It?

■ Consumption of CTI

- The TSB may be producing and sending quality information, but there is only value to members if they can consume and utilize it
- Look beyond counting outputs to actual member consumption activities

■ Contribution to CTI

- Ensures the TSB does not devolve into a one-way distribution channel
- Are members contributing something back to the TSB so it is learning and enriching its CTI while improving member security?
- Different sharing roles can contribute, give feedback, in different ways

■ Collaboration on CTI

- Collaboration within the TSB community in some form is vital for building trust relationships and enabling the pooling of resources
- Different sharing roles can collaborate in different ways



IMPACT: Effect on Member Security

- **Long Term Outcomes – infrequently observed**
 - Prevention of attack
 - Quicker detection of attack

- **Intermediate Outcomes – observable, measurable, reflect value**
 - **Enhanced Threat Awareness**
 - Greater management buy-in
 - Improved resource allocation
 - **Improved Defensive Capabilities**
 - New trusted peer relationships that can be leveraged in event of attack
 - New staff functions such as cyber threat intel or malware analysis
 - Checking networks for more types of indicators



Passive Consumers - Measures

Measures of CTI Content Quality

Outcome: Quality CTI

- *Are the types of CTI provided by this TSB (best practices, threat landscapes) relevant to your organization? (Relevance)*
- *Does the CTI provided cover the range of threats of interest to your organization? (Completeness)*
- *Has the TSB provided your organization with unique CTI not obtained elsewhere? (Uniqueness)*

Measures of Effective CTI Exchange

Outcome: CTI Consumption

- % member organizations attending (meetings, telecons, etc.)
- % member organizations attending by topic area
- % member organizations viewing best practices and threat landscape briefings
- % member organizations submitting Request for Information

Outcome: CTI Contributions

- % member organizations providing satisfaction ratings on TSB activities (meetings, etc.)

Outcome: CTI Collaboration

- *Have TSB activities and CTI helped your organization build trusted relationships with other organizations?*
- *Have TSB activities and CTI improved your organization's engagement with a security service provider?*

Measures of Effective CTI IMPACT

Outcome: Threat Awareness

- *Have TSB activities and CTI improved your organization's strategic awareness and understanding of relevant cyber threats?*

Outcome: Defensive Capabilities

- *Have TSB activities and CTI improved your organization's allocation of cyber resources?*
- *Have TSB activities and CTI improved your organization's cyber defensive capabilities (either processes or technology controls)?*



Active Consumers - Measures

Measures of CTI Content Quality

Any from Passive Consumers plus:

Outcome: Quality CTI

- Are the types of CTI provided by this TSB (indicators, analytics, etc.) readily consumable by your organization? (**Consumability**)
- Is CTI from this TSB easy to filter or prioritize according to your organization's needs? (**Filterability**)
- Is CTI from this TSB sufficiently timely for your organization's needs? (**Timeliness**)
- Average time from TSB receipt of CTI to publishing to members (**Timeliness**)
- Has the CTI provided by the TSB been accurate? (**Accuracy**)
- Does CTI provided by the TSB have enough context to be readily actionable? (**Sufficient Context**)
- % indicators linked to threat reports (**Sufficient Context**)

Measures of Effective CTI Exchange

Any from Passive Consumers plus:

Outcome: CTI Consumption

- % member organizations querying repository
- % member organizations viewing operational CTI (indicators, signatures, analytics, COAs, adversary profiles, etc.)
- % member organizations subscribing to feeds
- Have TSB activities and CTI improved your organization's ability to ingest indicators?

Outcome: CTI Contributions

- % member organizations providing satisfaction ratings on TSB operational/tactical CTI
- Have TSB activities and CTI improved your organization's willingness to report on indicators? (sightings, false positives, additional context, etc.)

Outcome: CTI Collaboration

- Have TSB activities led to any sharing of resources with TSB peers?
- Have TSB activities led to any collaborative product evaluations with any of your TSB peers?

Measures of Effective CTI IMPACT

Any from Passive Consumers plus:

Outcome: Threat Awareness

- Have TSB activities and CTI improved your organization's tactical or operational awareness of relevant cyber threats?
- Have TSB member sightings improved your organization's tactical or operational awareness of relevant cyber threats?

Outcome: Defensive Capabilities

- Have TSB activities and CTI improved your organization's ability to track threat indicators or incidents?
- Have TSB activities and CTI improved your organization's ability to scan networks or hosts for potential threats?
- Have TSB activities and CTI led to your organization's detection or prevention of any threat activity?



Reporters - Measures

Measures of CTI Content Quality

Any from Active Consumers plus:

Outcome: Quality CTI

- % indicators reported as false positives (Accuracy)

Measures of Effective CTI Exchange

Any from Active Consumers plus:

Outcome: CTI Consumption

Same as above

Outcome: CTI Contributions

- % member organizations reporting sightings
- % member organizations responding to Request for Information
- % indicators on which members have reported
- *Do TSB mechanisms make it easy for your organization to report on indicators (sightings, false positives, additional context, etc.)?*

Outcome: CTI Collaboration

- *Have TSB activities led to direct assistance from any of your TSB peers regarding a threat or incident?*
- *Have TSB activities led to collaborative response to threats with other members?)*

Measures of Effective CTI IMPACT

Any from Active Consumers plus:

Outcome: Threat Awareness

- *Have TSB activities given your organization access to unique cyber threat information about advanced threats not available elsewhere?*
- *Has your organization's reporting led to access to CTI not available to the broader TSB community (e.g., restricted, special topic sharing groups)?*

Outcome: Defensive Capabilities

- *Has your organization participated in any restricted, special topic sharing groups that led to deployment of unique detection and prevention capabilities not available to the broader TSB community?*



Producers - Measures

Measures of CTI Content Quality

Measures of Effective CTI Exchange

Measures of Effective CTI IMPACT

All from Reporters plus:

Value to Individual Member Organization

- Enrichment from other Producers
- Ability to join Producer-only sharing subgroups
- Potential for improved security of own supply chain

Value to Threat Sharing Body

- Unique observations and analysis
- Potential for direct, high-skill peer to peer assistance

Any from Reporters plus:

Outcome: Quality CTI

Same as above

Any from Reporters plus:

Outcome: CTI Consumption

Same as above

Outcome: CTI Contributions

- # new indicators, signatures, threat reports, etc. contributed by members
- % member organizations contributing new CTI

Outcome: CTI Collaboration

- *Have TSB activities led to collaborative analysis of threats with other members?*
- *Have TSB activities and CTI improved your organization's interactions with its supply chain?*
- *Is there sufficient reciprocity in CTI sharing among TSB members?*

Any from Reporters plus:



Outcome: Threat Awareness

Same as above



Outcome: Defensive Capabilities

Same as above

Measures of CTI Quality, Exchange, and Impact by Role (1 of 2)

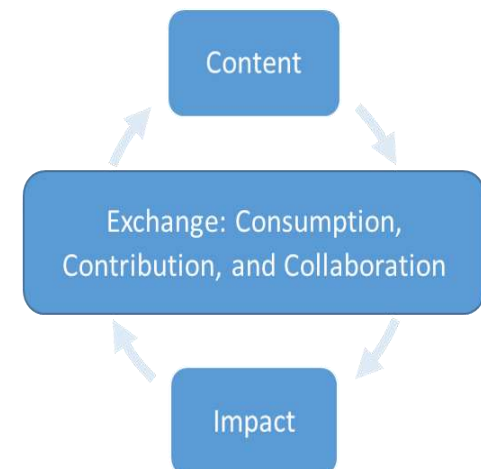
<i>Sharing Role</i>	<i>Value of Sharing</i>	<i>Measures of CTI Content Quality</i>	<i>Measures of Effective CTI Exchange</i>	<i>Measures of Effective CTI IMPACT</i>
<p>Passive Consumer We receive reported threat information for the situational awareness.</p> 	<p>Value to Individual Member Organization</p> <ul style="list-style-type: none"> Relationships Access to unique information Access to best practices Broader threat awareness Motivate improved cyber resource allocation to C-Suite Utilization of CTI to improve defensive cyber posture <p>Value to Threat Sharing Body</p> <ul style="list-style-type: none"> Broader threat awareness Membership fees 	<p>Outcome: Quality CTI</p> <ul style="list-style-type: none"> Are the types of CTI provided by this TSB (best practices, threat landscapes) relevant to your organization? (<i>Relevance</i>) Does the CTI provided cover the range of threats of interest to your organization? (<i>Completeness</i>) Has the TSB provided your organization with unique CTI not obtained elsewhere? (<i>Uniqueness</i>) 	<p>Outcome: CTI Consumption</p> <ul style="list-style-type: none"> % member organizations attending (meetings, telecons, etc.) % member organizations attending by topic area % member organizations viewing best practices and threat landscape briefings % member organizations submitting Request for Information <p>Outcome: CTI Contributions</p> <ul style="list-style-type: none"> % member organizations providing satisfaction ratings on TSB activities (meetings, etc.) <p>Outcome: CTI Collaboration</p> <ul style="list-style-type: none"> Have TSB activities and CTI helped your organization build trusted relationships with other organizations? Have TSB activities and CTI improved your organization's engagement with a security service provider? 	<p>Outcome: Threat Awareness</p> <ul style="list-style-type: none"> Have TSB activities and CTI improved your organization's strategic awareness and understanding of relevant cyber threats? <p>Outcome: Defensive Capabilities</p> <ul style="list-style-type: none"> Have TSB activities and CTI improved your organization's allocation of cyber resources? Have TSB activities and CTI improved your organization's cyber defensive capabilities (either processes or technology controls)?
<p>Active Consumer We scan our networks for reported threats, but don't report back our findings.</p> 	<p>All from Passive Consumers plus:</p> <p>Value to Individual Member Organization</p> <ul style="list-style-type: none"> Shared TSB services or resources <p>Value to Threat Sharing Body</p> <ul style="list-style-type: none"> Improved security of ecosystem 	<p>Any from Passive Consumers plus:</p> <p>Outcome: Quality CTI</p> <ul style="list-style-type: none"> Are the types of CTI provided by this TSB (indicators, analytics, etc.) readily consumable by your organization? (<i>Consumability</i>) Is CTI from this TSB easy to filter or prioritize according to your organization's needs? (<i>Filterability</i>) Is CTI from this TSB sufficiently timely for your organization's needs? (<i>Timeliness</i>) Average time from TSB receipt of CTI to publishing to members (<i>Timeliness</i>) Has the CTI provided by the TSB been accurate? (<i>Accuracy</i>) Does CTI provided by the TSB have enough context to be readily actionable? (<i>Sufficient Context</i>) % indicators linked to threat reports (<i>Sufficient Context</i>) 	<p>Any from Passive Consumers plus:</p> <p>Outcome: CTI Consumption</p> <ul style="list-style-type: none"> % member organizations querying repository % member organizations viewing operational CTI (indicators, signatures, analytics, COAs, adversary profiles, etc.) % member organizations subscribing to feeds Have TSB activities and CTI improved your organization's ability to ingest indicators? <p>Outcome: CTI Contributions</p> <ul style="list-style-type: none"> % member organizations providing satisfaction ratings on TSB operational/tactical CTI Have TSB activities and CTI improved your organization's willingness to report on indicators? (sightings, false positives, additional context, etc.) <p>Outcome: CTI Collaboration</p> <ul style="list-style-type: none"> Have TSB activities led to any sharing of resources with TSB peers? Have TSB activities led to any collaborative product evaluations with any of your TSB peers? 	<p>Any from Passive Consumers plus:</p> <p>Outcome: Threat Awareness</p> <ul style="list-style-type: none"> Have TSB activities and CTI improved your organization's tactical or operational awareness of relevant cyber threats? Have TSB <u>member sightings</u> improved your organization's tactical or operational awareness of relevant cyber threats? <p>Outcome: Defensive Capabilities</p> <ul style="list-style-type: none"> Have TSB activities and CTI improved your organization's ability to <u>track</u> threat indicators or incidents? Have TSB activities and CTI improved your organization's ability to <u>scan</u> networks or hosts for potential threats? Have TSB activities and CTI led to your organization's <u>detection</u> or <u>prevention</u> of any threat activity?

Measures of CTI Quality, Exchange, and Impact by Role (2 of 2)

<i>Sharing Role</i>	<i>Value of Sharing</i>	<i>Measures of CTI Content Quality</i>	<i>Measures of Effective CTI Exchange</i>	<i>Measures of Effective CTI IMPACT</i>
<p>Reporter</p> <p>We scan our networks for reported threats, and also report back our findings.</p> 	<p>All from Active Consumers plus:</p> <p>Value to Individual Member Organization</p> <ul style="list-style-type: none"> Enhanced reputation and "social credit" with peers; may lead to direct assistance from peers Enhanced peer trust relationships may enable participation in more advanced threat discussions <p>Value to Threat Sharing Body</p> <ul style="list-style-type: none"> Feedback on, and enrichment of TSB information Greater inter-organizational trust and support among peers Reciprocity encourages more parties to contribute 	<p>Any from Active Consumers plus:</p> <p>Outcome: Quality CTI</p> <ul style="list-style-type: none"> % indicators reported as false positives (Accuracy) 	<p>Any from Active Consumers plus:</p> <p>Outcome: CTI Consumption Same as above</p> <p>Outcome: CTI Contributions</p> <ul style="list-style-type: none"> % member organizations reporting sightings % member organizations responding to Request for Information % indicators on which members have reported Do TSB mechanisms make it easy for your organization to report on indicators (sightings, false positives, additional context, etc.)? <p>Outcome: CTI Collaboration</p> <ul style="list-style-type: none"> Have TSB activities led to direct assistance from any of your TSB peers regarding a threat or incident? Have TSB activities led to collaborative response to threats with other members? 	<p>Any from Active Consumers plus:</p> <p>Outcome: Threat Awareness</p> <ul style="list-style-type: none"> Have TSB activities given your organization access to unique cyber threat information about advanced threats not available elsewhere? Has your organization's reporting led to access to CTI not available to the broader TSB community (e.g., restricted, special topic sharing groups)? <p>Outcome: Defensive Capabilities</p> <ul style="list-style-type: none"> Has your organization participated in any restricted, special topic sharing groups that led to deployment of unique detection and prevention capabilities not available to the broader TSB community?
<p>Producer</p> <p>We scan our networks for reported threats, and also identify and share additional threat information.</p> 	<p>All from Reporters plus:</p> <p>Value to Individual Member Organization</p> <ul style="list-style-type: none"> Enrichment from other Producers Ability to join Producer-only sharing subgroups Potential for improved security of own supply chain <p>Value to Threat Sharing Body</p> <ul style="list-style-type: none"> Unique observations and analysis Potential for direct, high-skill peer to peer assistance 	<p>Any from Reporters plus:</p> <p>Outcome: Quality CTI Same as above</p>	<p>Any from Reporters plus:</p> <p>Outcome: CTI Consumption Same as above</p> <p>Outcome: CTI Contributions</p> <ul style="list-style-type: none"> # new indicators, signatures, threat reports, etc. contributed by members % member organizations contributing new CTI <p>Outcome: CTI Collaboration</p> <ul style="list-style-type: none"> Have TSB activities led to collaborative analysis of threats with other members? Have TSB activities and CTI improved your organization's interactions with its supply chain? Is there sufficient reciprocity in CTI sharing among TSB members? 	<p>Any from Reporters plus:</p> <p>Outcome: Threat Awareness Same as above</p> <p>Outcome: Defensive Capabilities Same as above</p>

Summary

- Members of TSBs can be diverse, needing different levels of trust and different value from sharing activities
- Helpful to think in terms of 4 Sharing Roles, ranging from Passive Consumers to Producers
- Measurement is essential for TSBs to identify gaps and adapt
- Measurement is important for motivating broader organizational participation
- Help TSBs think beyond how many indicators they produce
- Help TSBs think systematically across the information sharing life cycle



Discussion and Feedback
