SPIN YOUR CTI PROCESS ROUND!

FIRST CTI Symposium 2023
8 November 2023
Andreas Sfakianakis
CTI Professional
CTI IS A JOURNEY!

#ctijourney
HOW CAN TEAMS EFFECTIVELY OPERATIONALIZE THEIR CTI PROCESS?

Problem Statement
WHO AM I

- CTI in Financial, Energy, and Technology sectors
- SANS, ENISA, FIRST.org, European Commission
- Twitter: @asfakian
  Mastodon: @asfakian@infosec.exchange
- Websites: www.threatintel.eu
DISCLAIMER

VIEWS ARE MY OWN, NOT MY EMPLOYER'S

MMMMKAY?
OUTLINE

Setting the scene  Workflow & Case Management  Basic Ingredients

References used within this presentation: https://bit.ly/firstcti23
WE HAVE GONE A LONG WAY

Growth in Organizations with Dedicated CTI Teams

<table>
<thead>
<tr>
<th>Year</th>
<th>2018</th>
<th>2019</th>
<th>2020</th>
<th>2021</th>
<th>2022</th>
<th>2023</th>
</tr>
</thead>
<tbody>
<tr>
<td>%</td>
<td>41.5</td>
<td>41.1</td>
<td>49.5</td>
<td>44.4</td>
<td>47.0</td>
<td>50.8</td>
</tr>
</tbody>
</table>

Are CTI requirements clearly defined in your organization?

- **Yes, we have documented intelligence requirements.**
  - 2023: 59.1%
  - 2022: 35.4%

- **No, our requirements are ad hoc.**
  - 2023: 24.1%
  - 2022: 33.5%

- **No, but we plan to define them.**
  - 2023: 14.0%
  - 2022: 20.1%

- **No, and we have no plans to formalize requirements.**
  - 2023: 2.8%
  - 2022: 11.0%
WE HAVE GONE A LONG WAY (2)

Collection Management Framework (CMF) Maturity Model

<table>
<thead>
<tr>
<th>Capabilities</th>
<th>Initial</th>
<th>Repeatable</th>
<th>Defined</th>
<th>Managed</th>
<th>Optimizing</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Source</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identification</td>
<td>Data sources are not well defined, and the organization lacks a comprehensive list of potential threat intelligence data sources</td>
<td>The organization has identified some key data sources, but not a fully comprehensive list</td>
<td>The organization has a well-defined list of critical data sources relevant to its industry and threats</td>
<td>The organization continuously monitors and updates its list of data sources as intelligence requirements mature</td>
<td>The organization actively participates in threat intelligence sharing communities and has real-time awareness of new data sources</td>
</tr>
<tr>
<td><strong>Data Collection</strong></td>
<td>Data is collected sporadically, without a systematic process, and there is no standardization in data format or protocols</td>
<td>Data collection is more consistent, but there is still no standardization</td>
<td>Data collection processes are standardized and automated</td>
<td>Data collection is not only automated but also optimized for efficiency and accuracy</td>
<td>Data collection is highly automated, dynamic, and adaptive to emerging threats</td>
</tr>
<tr>
<td><strong>Data Quality</strong></td>
<td>Data quality is unreliable, with no validation or verification processes in place.</td>
<td>Basic data quality controls are in place, but reliability can be inconsistent.</td>
<td>Data quality controls are well defined, and data is consistently reliable.</td>
<td>Data quality is measured and improved upon continually, with strict validation and verification processes.</td>
<td>The organization maintains a high standard of data quality, employing advanced analytics to enhance accuracy</td>
</tr>
<tr>
<td><strong>Data Integration</strong></td>
<td>Limited or no integration of data sources, resulting in siloed information</td>
<td>Some integration efforts have started, but data silos still exist.</td>
<td>Integration of data sources is actively managed, reducing data silos.</td>
<td>Data integration is holistic, with cross-source correlations and efficient data sharing mechanisms in place.</td>
<td>Data integration is seamless, and advanced analytics enable the organization to proactively identify and respond to threats.</td>
</tr>
</tbody>
</table>
WHAT'S OLD IS NEW AGAIN

In California, the 1918 Spanish flu killed up to 50 million people around the world and has been called "the mother of all pandemics.

Wear a Mask

Save a Life

In Seattle, Washington, policeman stand in a street wearing protective masks made by the Seattle Chapter of the Red Cross, during the influenza epidemic in 1918.
WHERE DO WE GO FROM HERE?
IMPORTANT THINGS ARE (SOMETIMES) BORING
CTI ANALYST SKILLSET

CYBER INTELLIGENCE
The products and processes across the intelligence cycle of assessing the capabilities, intentions, and activities – technical and otherwise – of potential adversaries and competitors in the cyber domain (with cyber counterintelligence as a sub-discipline).

TECHNICAL COMPETENCIES
The technical foundation for understanding the hardware and software of information and communications technology, especially as they relate to cybersecurity.

ANALYTIC COMPETENCIES
The human science basis for complex analysis of data and information from a variety of sources, including foundations of strategy, critical and systems thinking, reasoning and logic, problem solving, and decision making.

KNOWLEDGE MANAGEMENT (INFORMATICS) COMPETENCIES
The knowledge management and information science foundation for planning and organizing information collection (collection management), applying tools to gather and support complex data and information analysis and presentation.

COMMUNICATION AND ORGANIZATIONAL COMPETENCIES
These competencies emphasize clear expression of opinions and reasoning, along with effective communication of one's ideas, intentions, goals, presentation, and visual display, as well as project management skills.

CONTEXTUAL DOMAIN COMPETENCIES
The sector-specific, national/regional, and/or sociocultural foundations for analyzing complex problems; identifying key actors and roles; assessing perceptions, interests and intentions; sensemaking; drawing inferences from actions and behaviors; and discerning situational influences.

INSA
A BASIC STEP

WHAT IF I TOLD YOU

THAT WORKFLOW AND CASE MANAGEMENT WOULD HELP YOUR TEAM
WHY WORKFLOW AND CASE MANAGEMENT?

Workflow, Coordination, and Collaboration

Knowledge Management

Metrics
WORKFLOW, COORDINATION & COLLABORATION

- BACKLOG
  - IN PROGRESS
  - NEED REVISION
    - IN REVIEW
      - REVIEW COMPLETED
        - WAITING FOR FEEDBACK
          - DONE

SIMPLIFIED

WORKFLOW
KNOwLEDGE MANAGEMENT

- Tagging
- Custom fields
- Easy searching and filtering
- Source rating
- Access control
WHAT GETS MEASURED, GETS MANAGED

CANT WORRY ABOUT METRICS

IF YOU DONT MEASURE ANYTHING
MANAGEMENT METRICS

- Threats per criticality/impact level
- Time spent per PIR
- CTI assessments per threat type/threat actor
- CTI assessments (or time spent) supporting IR
- Quantitative feedback received per PIR
- Time spent on RFIs per stakeholder
- #hunts / #incidents from CTI assessments
TEAM METRICS

- Sources mostly used per PIR
- CTI deliverables per PIR
- CTI deliverables per stakeholder
- Average time spent per CTI deliverable
- CTI analysts’ workload
- Average time spent in each phase of the workflow
- Time spent on CTI projects
WORKFLOW AND CASE MANAGEMENT FOR CTI

SO HOT RIGHT NOW
BASIC INGREDIENTS
Remember

- Data into buckets
- Consistency is key
- Spend time to save time
WHAT'S YOUR CTI PROCESS?
TECHNOLOGY ENABLEMENT (1)

- Reporting and feedback
- PIRs, stakeholders, RFIs
- Dissemination of IOCs
- Easy-peasy collection!
- Workflows and threat playbooks
- IOC management
- Analysis capabilities
- Threat knowledge management

*SANS CTI Summit 2021*
TECHNOLOGY ENABLEMENT (2)

Recommendation is to live off the land (at least at the start of your CTI journey)
CTI ONE STOP SHOP

- Who you are / Contact Info
- Team’s Scope
- Intelligence Requirements
- CTI Report Library / CTI Blog
- Request For Information (RFI)

YOU'RE WELCOME TO USE OUR CTI PORTAL
REQUEST FOR INFORMATION (1)

SHOW ME THE RFI PORTAL!
REQUEST FOR INFORMATION (2)

CTI Team

Welcome! You can raise a Request For Information (RFI) for the Cyber Threat Intelligence team from the options provided.

What do you need help with?

Search

Threat Analysis

IOC-Sharing
Request Briefing
Subscribe to CTI
CTI Onboarding

Cyber Threat Advisory
Requests that are specific to a type of cyber threat or a cyber event. You can also submit requests that are related to technical analysis of Indicators of Compromise (IOCs), phishing, malware, etc.

Trend Report
Requests pertaining to a particular strategic threat(s) and/or threat actor over a period of time.
REQUEST FOR INFORMATION (3)
CTI CHEF APPROVES
FINAL REMARKS
FINAL REMARKS

- Operationalizing the CTI process is a common challenge

- The importance of workflow and case management

- The basic ingredients
REFERENCES

wander the abyss of uncited information

cite properly

SPIN IT ROUND!

Planning

Feedback

Collection

Your CTI Process

Dissemination

Processing

Analysis

YOU SPIN ME

RIGHT ROUND BABY RIGHT ROUND
THANK YOU!

Andreas Sfakianakis
@asfakian
threatintel.eu

TLP: CLEAR