Cyber Threat Intelligence (CTI)'s Coming of Age: Successes of Zero Budget CTI Programs

Authors
Sijmen Schenk, MSc (Royal Holloway, 2022)
Konstantinos Markantonakis, ISG, Royal Holloway

Abstract

Cyber Threat Intelligence (CTI) is an information security domain still in its infancy, with the early adopters now approaching their first ten years of operations. The purpose of this article is to present the best practices and lessons learned that were identified by interviewing eight organisations in the Netherlands that have set up their CTI teams in the last ten years. This research identified that despite the heavy commercialization of the CTI market, free open-source solutions have been playing a significant role for these CTI teams. This article introduces the field of CTI, describes the observed best practices, identified complications, and the feasibility of setting up CTI capabilities by leveraging the free open-source tools and datasets in popular use with the interview audiences. This article is written for a general audience and does not assume previous knowledge of this domain.[a]

[a] This article is based on an MSc dissertation written as part of the MSc in Information Security at the ISG, Royal Holloway, University of London. The full thesis is published on the ISG's website at `https://www.royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/research/explore-our-research/isg-technical-reports/`.

1 Introduction to Cyber Threat Intelligence (CTI)

This article will introduce the lessons learned from eight organisations that set up CTI (Cyber Threat Intelligence) teams within the Netherlands in the last ten years. We will start with a brief introduction to CTI and how it aims to support and enhance other information security domains. After this, we will delve into the observed successes, complications and best practices that could be identified in the development of these teams. We will start with a high-level definition of CTI.

Accurate intelligence allows stakeholders to prioritize rare investigative resources on the most significant threats. CTI has developed into a decisive factor in security operations and in successful cases, this led to effective investigation, attribution, prosecution, and conviction of malicious actors. Recent developments saw CTI's integration within the NIST framework[1] and its adoption as a control into the ISO 27002 standard[2] further enforcing its future significance. Being a novel field, a variety of interpretations for CTI can be found. This article does not aim to be authoritative or exhaustive, instead, it will present the perspectives of the interviewed organisations and how they leveraged CTI for their daily operations.

> "Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and action-oriented advice about an existing or emerging menace or hazard to assets. This intelligence can be used to inform decisions regarding the subject's response to that menace or hazard."
> Gartner

[1] `https://csrc.nist.gov/glossary/term/cyber_threat_intelligence`

[2] `https://www.iso.org/standard/75652.html`

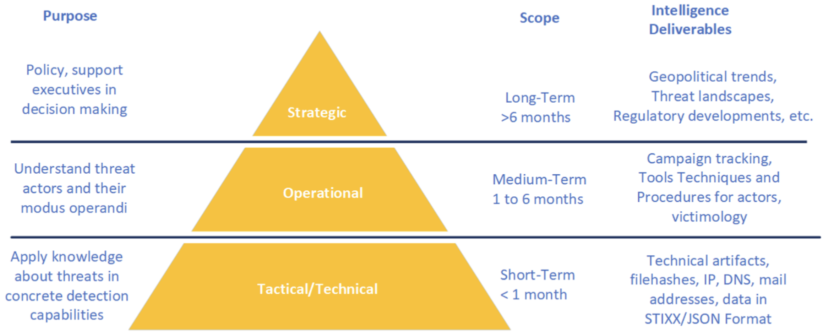

Purpose
Scope
Intelligence Deliverables
Policy, support executives in decision making
Strategic
Long-Term >6 months
Geopolitical trends, Threat landscapes, Regulatory developments, etc.
Understand threat actors and their modus operandi
Operational
Medium-Term 1 to 6 months
Campaign tracking, Tools Techniques and Procedures for actors, victimology
Apply knowledge about threats in concrete detection capabilities
Tactical/Technical
Short-Term < 1 month
Technical artifacts, filehashes, IP, DNS, mail addresses, data in STIXX/JSON Format

Figure 1: CTI Levels of Intelligence and their Purpose

2 Different Levels of CTI Consumption

The CTI literature has embraced three levels of intelligence. These can be viewed as different audiences that CTI products can be tailored to.

Strategic Intelligence can be considered the product of long-term trends and observations that can forecast future policy requirements; these products generally have a relevance longer than six months ahead and are aimed to advise stakeholders such as the CISO and board members.

Operational Intelligence can be actor profiling, attribution and (multiple) campaign tracking with the intent to identify or predict similar behaviour. This intelligence is often based on tactical-level observations which were identified as recurring between multiple intrusions. Examples for the audience can be the CTI teams themselves, or CTI collaborations with outside parties. As this level aims to identify malicious actors, it can also serve to support the involvement of law enforcement.

Tactical Intelligence directly deals with forensic observables such as file hashes, IP addresses, DNS and other infrastructure artefacts (identified as ‘indicators of compromise’) that were observed relating to a compromise. These intelligence products are primarily aimed at the SOC, CERT, and CTI teams as they can aid in detection and forensic investigation but frequently have a short-term relevance of less than a month. Once publicly identified as malicious, observables tend to be changed by the adversary and their operational relevance becomes reduced.

A useful heuristic that can apply to these different levels of CTI is to consider the following when dealing with adversary activities:
Strategic Level applies to **the Who and Why** (actor and motivation),
Operational level applies to **the How and When** (campaign and methods), and
Tactical/Technical applies to **the What** (describing technical evidence).

The majority of CTI being consumed by the interview audience was tactical in nature, often as high-confidence data feeds of IOCs (Indicators of Compromise) which were matched to the organisation’s log sources.This matching process helped these teams identify sightings of malicious behaviour so that incident response could be performed.

3 Scope of the Dutch CTI Programs at Conception

The key stakeholder for each CTI team was asked how they had developed their CTI programs. We will first look at the objectives that these teams stated before they started their implementation.

All eight organisations focused their programs on tactical level intelligence whereby the CTI teams were primarily providing intelligence to the SOC/CERT capability of the organisations.

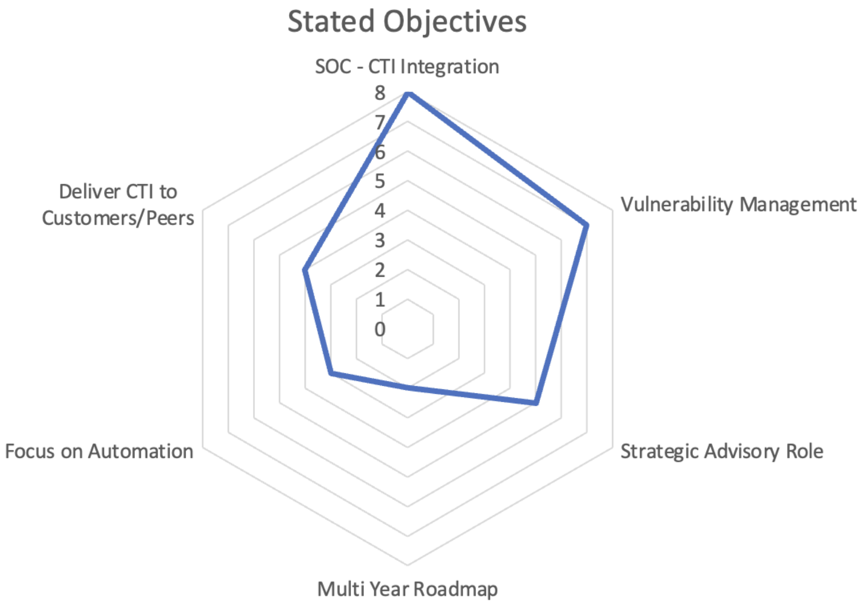


Figure 2: Stated Objectives for the CTI Initiative

All respondents had set predefined objectives before the CTI program started.

- For all eight respondents, the main objective of the CTI team was to integrate CTI capabilities with SOC/CERT processes.
- Seven respondents identified that their CTI program played a significant role in providing vulnerability assessments to their organisations (to assess the actual threat posed by emerging vulnerabilities in software products).
- Five respondents had also assigned their CTI teams a strategic advisory objective from the start, this meant that they also delivered intelligence to the strategic level.
- Four respondents had external customers or peers intended to be served with the intelligence generated by the CTI teams, for two parties this related to commercial customers, for two government parties these entities were government peers.
- Automation was deemed a priority objective for three respondents.
- One team had defined a specific multi-year roadmap from the start. The other team used shorter-scale planning horizons.

4 Usage of CTI Tools and the Significance of Open-source Resources

Interview respondents were asked to identify the CTI tools they leveraged in their programs and which tools they were aware of and that were being considered for future use.

- This identified the dominance of the MISP[3] (Malware Information Sharing Platform) being leveraged by all eight teams.

[3] https://www.misp-project.org/

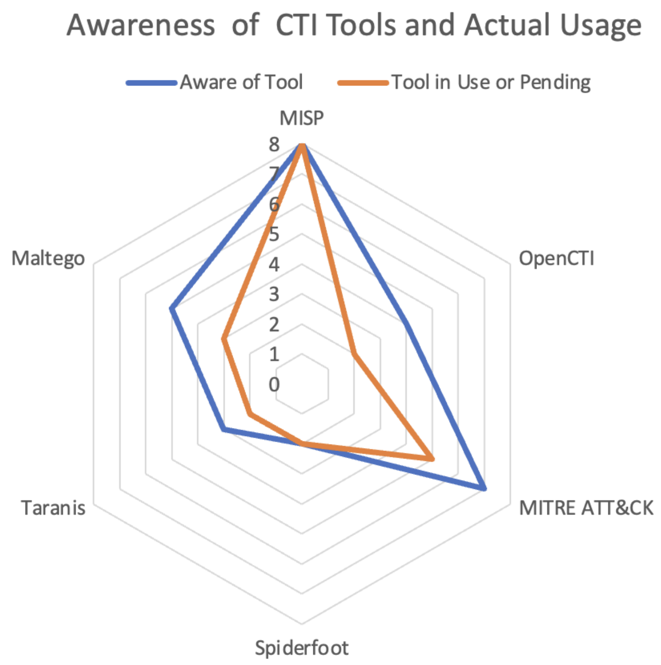


Figure 3: Usage of CTI Tools

- A second outlier was the prevalence of the MITRE ATT&CK[4] standard. This is a taxonomy for CTI capabilities that is provided with an extensive historic library of past compromises and actor attribution. This was well-known by seven teams and in daily use by five teams.

Of the six tools identified, four tools are not commercial but open-source solutions which are available for free (MISP, MITRE ATT&CK, OpenCTI[5] and Taranis[6]). Because of this, these solutions are accessible capabilities for any team considering CTI adoption, as outside of configuration time and server resources no investment cost will be required to leverage them. These tools will now be described in more detail.

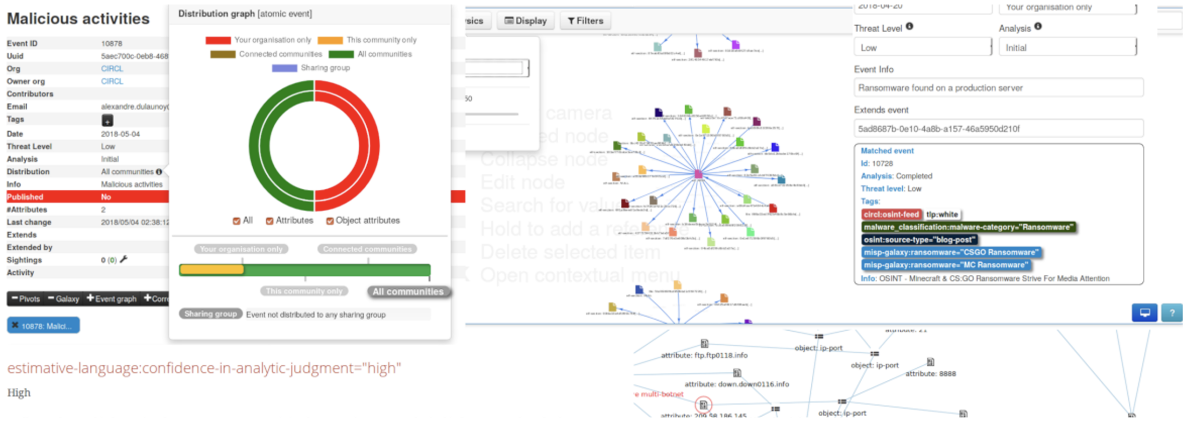
MISP, OpenCTI and the MITRE ATT&CK framework have complimentary features and they can be efficiently integrated with each other. This stack was in use with two respondents. In this implementation the OpenCTI platform was the front-end tool used by the intelligence stakeholder. OpenCTI was fed by tactical data originating from a self-hosted MISP instance and the data could be represented in the MITRE ATT&CK Framework and enriched with public MITRE ATT&CK resources.

5 Significant Open-Source CTI Resources

MISP (Malware Intelligence Sharing Platform by CIRCL.LU): Each of the CTI teams leveraged the MISP platform, with three teams defining it as the central CTI repository around which they shaped their CTI capabilities.

The Malware Information Sharing Platform (hereafter referred to as MISP) is an open-source (GNU Licensed) threat intelligence platform developed by the Luxembourg Cert, CIRCL.LU[7]. The program was set up to be open to other contributors, and notable contributors are the NATO cert NCIRC[8] and

[4] https://attack.mitre.org/
[5] https://www.ssi.gouv.fr/uploads/2019/10/anssi-doctrine_opencti-v1.0.pdf
[6] https://github.com/NCSC-NL/taranis3
[7] https://circl.lu/
[8] https://www.ncirc.nato.int/



Malicious activities

Event ID 10878
Uuid 5aec700c-0eb8-468
Org CIRCL
Owner org CIRCL
Contributors
Email alexandre.dulaunoy
Tags
Date 2018-05-04
Threat Level Low
Analysis Initial
Distribution All communities
Info Malicious activities
Published No
#Attributes 2
Last change 2018/05/04 02:38:12
Extends
Extended by
Sightings 0 (0)
Activity

Distribution graph [atomic event]

Sharing group Event not distributed to any sharing group

estimative-language:confidence-in-analytic-judgment="high"

High

Threat Level Low
Analysis Initial
Event Info Ransomware found on a production server
Extends event 5ad8687b-0e10-4a8b-a157-46a5950d210f

Matched event
Id: 10728
Analysis: Completed
Threat level: Low
Tags:
circl:osint-feed tlp:white
malware_classification:malware-category="Ransomware"
osint:source-type="blog-post"
misp-galaxy:ransomware="CSGO Ransomware"
misp-galaxy:ransomware="MC Ransomware"
Info: OSINT - Minecraft & CS:GO Ransomware Strive For Media Attention

Figure 4: MISP overview from `https://www.misp-project.org`

the European Union cert CERT-EU[9]. The MISP program is co-financed by the European Union.

The MISP project was started in 2012 to provide an open and accessible sharing platform for both public and private entities.

Information in MISP is distributed by subscribing to threat intelligence feeds which contain IoCs (Indicators of Compromise) related to observed intrusions. Some feeds are open source and free to use, while others (more sensitive feeds) are restricted and require invitations and/or a commercial subscription.

The MISP platform has several graphing options that can aid in correlating event data. One of the powerful features of MISP is the ability to integrate the MISP data in a variety of tools, including the ability to directly match the MISP data against the organisation's network logging to identify malicious events that may have occurred on the network.

MISP can be easily deployed on an organisation's internal server or implemented as a Docker container. Several pre-configured MISP VMs are also made available[10] that can provide demonstration capabilities without requiring extensive configuration on the user's part.

OPENCTI: Two respondents had tested the OpenCTI platform and one respondent has OpenCTI in active use.

The OpenCTI project[11] was started in 2018 in collaboration with The French National Cert, ANSSI[12] and the EU Computer Emergency Response Team EU-CERT. Its objective was to help develop and facilitate the ANSSI's collaboration with its constituents and partners. To promote this technical collaboration, ANSSI (in collaboration with EU-CERT) developed a threat intelligence platform that operates as an open-source knowledge management database to create and share threat intelligence data.

OpenCTI provides a graphical web-based interface that presents the underlying data. The datasets can be provided by subscribing to community-shared threat intelligence feeds including feeds originating from MITRE or MISP. The platform also has a graphing engine to identify correlations of data points. There is a wide range of data feed integration supported, most notably MISP, MITRE ATT&CK, the CVE (vulnerability) database and several more.

[9] `https://cert.europa.eu/`
[10] `https://vm.misp-project.org/`
[11] `https://github.com/OpenCTI-Platform/opencti`
[12] `https://www.ssi.gouv.fr/en/`

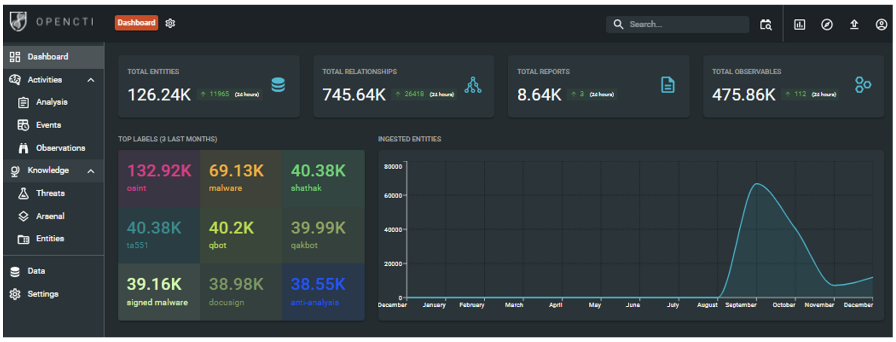
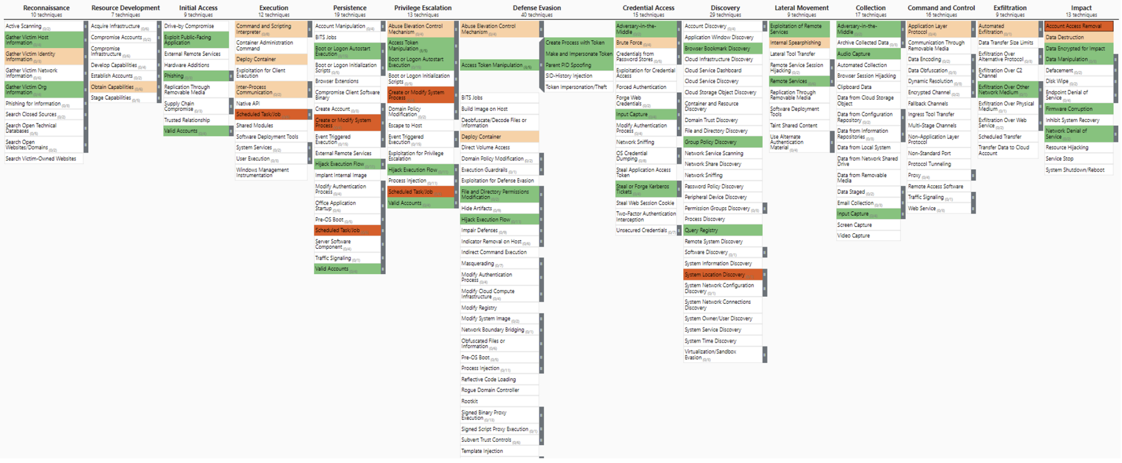


Figure 5: OpenCTI Graphical Dashboard


Reconnaissance
10 techniques
Active Scanning (0/2)
Gather Victim Host Information (0/4)
Gather Victim Identity Information (0/3)
Gather Victim Network Information (0/6)
Gather Victim Org Information (0/4)
Phishing for Information (0/3)
Search Closed Sources (0/2)
Search Open Technical Databases (0/5)
Search Open Websites/Domains (0/2)
Search Victim-Owned Websites

Resource Development
7 techniques
Acquire Infrastructure (0/6)
Compromise Accounts (0/2)
Compromise Infrastructure (0/6)
Develop Capabilities (0/4)
Establish Accounts (0/2)
Obtain Capabilities (0/6)
Stage Capabilities (0/5)

Initial Access
9 techniques
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (0/3)
Replication Through Removable Media
Supply Chain Compromise (0/3)
Trusted Relationship
Valid Accounts (0/4)

Execution
12 techniques
Command and Scripting Interpreter (0/8)
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication (0/2)
Native API
Scheduled Task/Job (0/6)
Shared Modules
Software Deployment Tools
System Services (0/2)
User Execution (0/3)
Windows Management Instrumentation

Persistence
19 techniques
Account Manipulation (0/4)
BITS Jobs
Boot or Logon Autostart Execution (0/15)
Boot or Logon Initialization Scripts (0/5)
Browser Extensions
Compromise Client Software Binary
Create Account (0/3)
Create or Modify System Process (0/4)
Event Triggered Execution (0/15)
External Remote Services
Hijack Execution Flow (0/11)
Implant Internal Image
Modify Authentication Process (0/4)
Office Application Startup (0/6)
Pre-OS Boot (0/5)
Scheduled Task/Job (0/6)
Server Software Component (0/4)
Traffic Signaling (0/1)
Valid Accounts (0/4)

Privilege Escalation
13 techniques
Abuse Elevation Control Mechanism (0/4)
Access Token Manipulation (3/5)
Boot or Logon Autostart Execution (0/15)
Boot or Logon Initialization Scripts (0/5)
Create or Modify System Process (0/4)
Domain Policy Modification (0/2)
Escape to Host
Event Triggered Execution (0/15)
Exploitation for Privilege Escalation
Hijack Execution Flow (0/11)
Process Injection (0/11)
Scheduled Task/Job (0/6)
Valid Accounts (0/4)

Defense Evasion
40 techniques
Abuse Elevation Control Mechanism (0/4)
Access Token Manipulation (3/5)
Create Process with Token
Make and Impersonate Token
Parent PID Spoofing
SID-History Injection
Token Impersonation/Theft
BITS Jobs
Build Image on Host
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain Policy Modification (0/2)
Execution Guardrails (0/1)
Exploitation for Defense Evasion
File and Directory Permissions Modification (0/2)
Hide Artifacts (0/9)
Hijack Execution Flow (0/11)
Impair Defenses (0/9)
Indicator Removal on Host (0/6)
Indirect Command Execution
Masquerading (0/7)
Modify Authentication Process (0/4)
Modify Cloud Compute Infrastructure (0/4)
Modify Registry
Modify System Image (0/2)
Network Boundary Bridging (0/1)
Obfuscated Files or Information (0/6)
Pre-OS Boot (0/5)
Process Injection (0/11)
Reflective Code Loading
Rogue Domain Controller
Rootkit
Signed Binary Proxy Execution (0/13)
Signed Script Proxy Execution (0/1)
Subvert Trust Controls (0/6)
Template Injection

Credential Access
15 techniques
Adversary-in-the-Middle (0/2)
Brute Force (0/4)
Credentials from Password Stores (0/5)
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (0/2)
Input Capture (0/4)
Modify Authentication Process (0/4)
Network Sniffing
OS Credential Dumping (0/8)
Steal Application Access Token
Steal or Forge Kerberos Tickets (0/4)
Steal Web Session Cookie
Two-Factor Authentication Interception
Unsecured Credentials (0/7)

Discovery
29 techniques
Account Discovery (0/4)
Application Window Discovery
Browser Bookmark Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Network Service Scanning
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery (0/3)
Process Discovery
Query Registry
Remote System Discovery
Software Discovery (0/1)
System Information Discovery
System Location Discovery (0/1)
System Network Configuration Discovery (0/1)
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery
Virtualization/Sandbox Evasion (0/3)

Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (0/2)
Remote Services (0/6)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (0/4)

Collection
17 techniques
Adversary-in-the-Middle (0/2)
Archive Collected Data (0/3)
Audio Capture
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Cloud Storage Object
Data from Configuration Repository (0/2)
Data from Information Repositories (0/3)
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged (0/2)
Email Collection (0/3)
Input Capture (0/4)
Screen Capture
Video Capture

Command and Control
16 techniques
Application Layer Protocol (0/4)
Communication Through Removable Media
Data Encoding (0/2)
Data Obfuscation (0/3)
Dynamic Resolution (0/3)
Encrypted Channel (0/2)
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy (0/4)
Remote Access Software
Traffic Signaling (0/1)
Web Service (0/3)

Exfiltration
9 techniques
Automated Exfiltration (0/1)
Data Transfer Size Limits
Exfiltration Over Alternative Protocol (0/3)
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium (0/1)
Exfiltration Over Physical Medium (0/1)
Exfiltration Over Web Service (0/2)
Scheduled Transfer
Transfer Data to Cloud Account

Impact
13 techniques
Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation (0/3)
Defacement (0/2)
Disk Wipe (0/2)
Endpoint Denial of Service (0/4)
Firmware Corruption
Inhibit System Recovery
Network Denial of Service (0/2)
Resource Hijacking
Service Stop
System Shutdown/Reboot

Figure 6: Example of a MITRE ATT&CK Overlay in the Navigator Tool

MITRE ATT&CK library The MITRE ATT&CK Framework (Adversarial Tactics, Techniques, and Common Knowledge) was actively used by five respondents and two respondents intended to integrate it in the future.

The non-profit research organization MITRE[13] is the custodian of the ATT&CK Framework. This cyber security taxonomy describes the phases and activities of a cyber compromise in specifically defined categories. The framework has several matrixes, with the Enterprise Matrix[14] being the most popular (and extensive). Other matrixes are specific to Mobile Device[15] threats and Industrial Control Systems[16].

A popular use case for ATT&CK is for defenders to identify their primary threat actors of concern and for each observed threat technique the respective box can be coloured to create a heatmap. This will create a graphical representation of the observed actor's tools, techniques, and capabilities to aid overall analysis and comparison. Organisations can even go as far as to colour the identified techniques to designate their organisation's ability to either detect or respond to these behaviours and identify gaps in their defensive perimeter concerning that specific threat actor.

MITRE created the ATT&CK Navigator tool[17] that allows users to generate these overlays and store them in several data formats to aid in its operation.

Additional tools: Other tools mentioned by the respondents include:

[13] https://www.mitre.org/
[14] https://attack.mitre.org/matrices/enterprise/
[15] https://attack.mitre.org/matrices/mobile/
[16] https://attack.mitre.org/matrices/enterprise/
[17] https://mitre-attack.github.io/attack-navigator/

- Maltego[18] was known by five respondents and used by three; it is a graphing analysis tool prepared with API connectors for popular CTI datasets. Maltego is a commercial tool but provides a free Community Edition[19] for non-commercial use with limited capabilities.
- Spiderfoot[20] is an OSINT/CTI footprinting tool that can identify internet infrastructure; two respondents were aware of this tool and had it in active use. Spiderfoot has a commercial tier, but a free open-source version is also made available.
- Taranis[21] is an open-source OSINT tool published by the Dutch NCSC. This tool was known by three respondents, and it is in use with two respondents. Taranis can help facilitate the process of monitoring and analysing news items for writing security advisories

6 Training Resources Leveraged to Develop Analyst Maturity

Respondents were asked about the training resources they leveraged to train their analysts.

- The SANS FOR 578 Cyber Threat Intelligence course[22] was the dominant training solution and each interviewed organisation leveraged this training to train their analysts.
- Three organisations leveraged the Treadstone 71 CTI tradecraft course[23].
- The threat Intelligence firm Fox-IT[24] had provided CTI training to two organisations.

Several organisations mentioned having assessed diverse OSINT training courses. No specifics were provided but the respondents mentioned that generic OSINT training did not satisfy their requirements for training CTI analysts as they were found not to be relevant for the tactical CTI domain specifically.

7 Complications Identified in the Programs

Respondents were asked whether they identified complications during the adoption of the CTI program. The responses were diverse. As a primary factor all but one of the programs exceeded their original time estimates. The cause behind the overall delay was diverse between organisations but the top three could be identified based on their stated impact.

1. Three organisations had issues staffing the CTI team. These teams identified a shortage of experienced CTI analysts on the job market as the primary concern.
2. The integration of the organisation's systems and network logging into CTI solutions (to automatically identify sightings of malicious origin) was deemed problematic by three organisations. In all cases, this had to do with the overall complexity of combining diverse data sources which led to subsequent delays.
3. The legal mandate to collect open-source intelligence was an issue for three organisations. GDPR requirements relating to the storage of indicators were initially problematic for three organisations. A specific mention was made about the legal complexity of the large-scale collection of technical artefacts such as e-mail addresses that were indicators used to distribute malware.

[18] https://www.maltego.com/

[19] https://www.maltego.com/ce-registration/

[20] https://www.spiderfoot.net/

[21] https://github.com/NCSC-NL/taranis3

[22] https://www.sans.org/cyber-security-courses/cyber-threat-intelligence/

[23] https://www.treadstone71.com/index.php/cyberintelligencetradecraft/certified-cyber-intelligence-analyst

[24] https://www.fox-it.com/nl-en/academy/

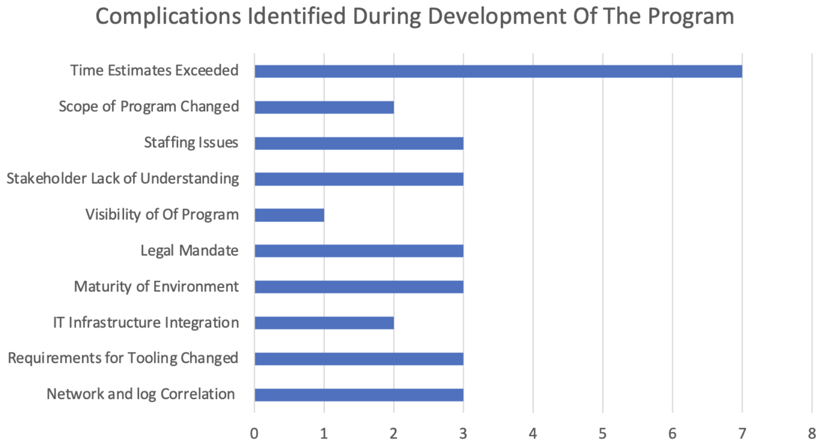


Figure 7: Complications Identified During Implementation of Program

8 Future Outlook

Shortage of Cybersecurity Staff Affecting the CTI Field Likely to Remain for Several Years

Three teams identified staffing as one of their main impediments in developing their CTI programs to full maturity. Though European educational programs are being developed to help fill the gap of cyber security skilled workers, this shortage will likely remain in the upcoming years. This shortage can be expected to affect new CTI teams. It may be recommended to consider staffing an early priority for organisations with ambitions to set up CTI teams. Two teams mitigated this shortage by cross-training their SOC/CERT analysts in the CTI discipline.

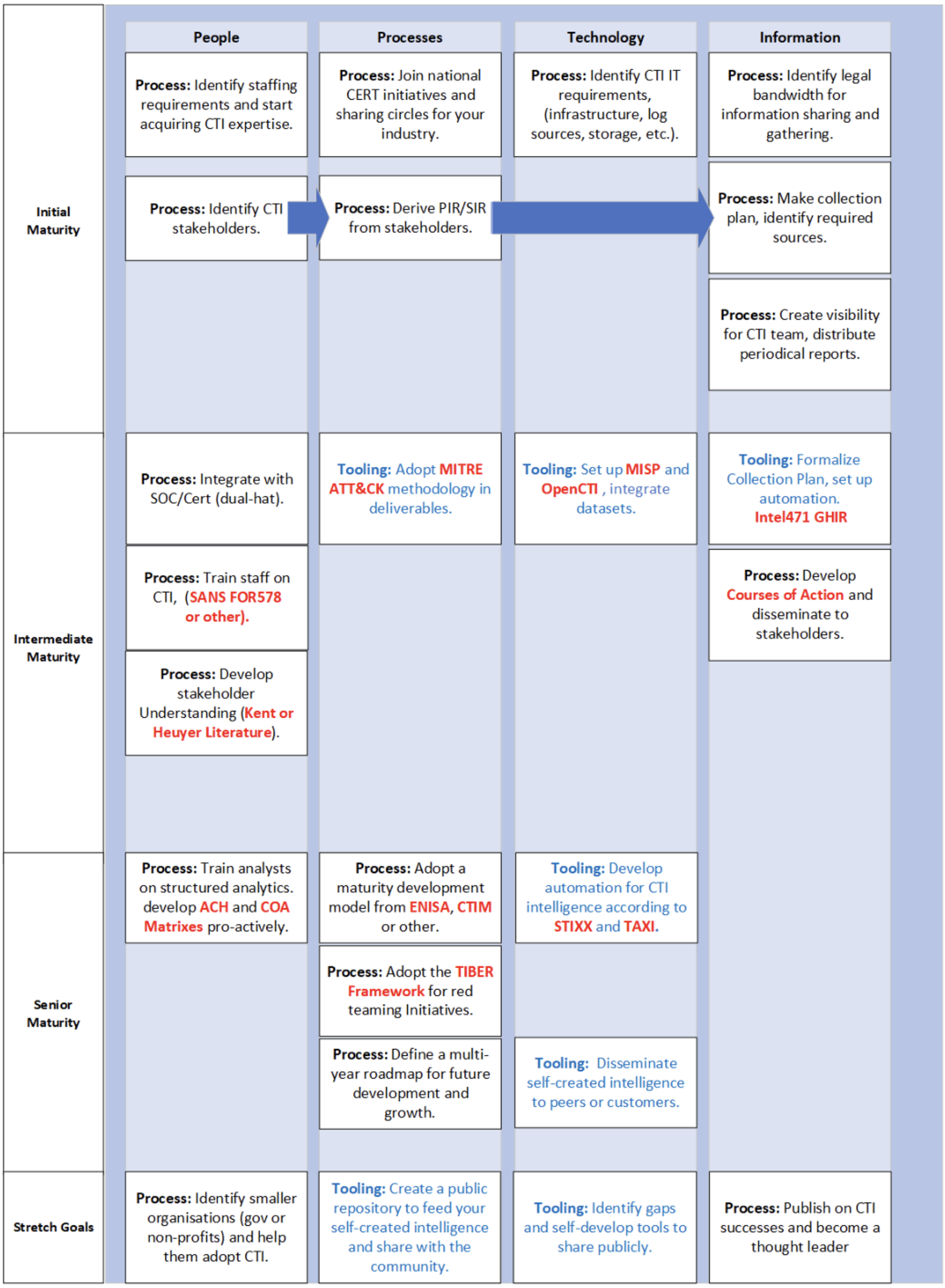
Future Automation of CTI – Integration in Orchestration Processes (SOAR)

One respondent identified that their future development plan would rely on adopting security orchestration processes and the automated integration of CTI processes. This concept is known as Security Orchestration and Automated Response (SOAR). As some of the technical implementations of CTI are based on retrieving external information and applying it to internal logging, further process integration can likely be achieved and this could be considered in future implementations. An aggregated overview of the lessons learned is provided as a graphic in Fig 8.

9 Conclusion

By its nature intelligence serves to answer the questions of a specific stakeholder. In doing so, a successful CTI program will not be generic but tailored to the respective organisation. While some programs may choose to collaborate with commercial partners to integrate CTI capabilities, systems and staff, the direction chosen by the interview audience had a strong preference to consider non-commercial open-source solutions instead. In doing so, each organisation had created a CTI capability that they deemed to be successful in meeting their stakeholders' requirements. The growing prevalence of open-source community-driven projects is a driving force within CTI. **I assert, that at this stage a successful CTI capability can be started without a specific tooling budget by leveraging these free and public resources.**

A small-scale SOC capability may already be enhanced with zero budget CTI by setting up a local MISP instance and leveraging this to contextualize observed events. This can be done by the SOC itself without requiring additional staff, as the value of additional context may at times help identify false positives and save time in the long run.



	People	Processes	Technology	Information
Initial Maturity	**Process:** Identify staffing requirements and start acquiring CTI expertise. **Process:** Identify CTI stakeholders.	**Process:** Join national CERT initiatives and sharing circles for your industry. **Process:** Derive PIR/SIR from stakeholders.	**Process:** Identify CTI IT requirements, (infrastructure, log sources, storage, etc.).	**Process:** Identify legal bandwidth for information sharing and gathering. **Process:** Make collection plan, identify required sources. **Process:** Create visibility for CTI team, distribute periodical reports.
Intermediate Maturity	**Process:** Integrate with SOC/Cert (dual-hat). **Process:** Train staff on CTI, (**SANS FOR578 or other).** **Process:** Develop stakeholder Understanding (**Kent or Heuyer Literature**).	**Tooling:** Adopt **MITRE ATT&CK** methodology in deliverables.	**Tooling:** Set up **MISP** and **OpenCTI** , integrate datasets.	**Tooling:** Formalize Collection Plan, set up automation. **Intel471 GHIR** **Process:** Develop **Courses of Action** and disseminate to stakeholders.
Senior Maturity	**Process:** Train analysts on structured analytics. develop **ACH** and **COA Matrixes** pro-actively.	**Process:** Adopt a maturity development model from **ENISA**, **CTIM** or other. **Process:** Adopt the **TIBER Framework** for red teaming Initiatives. **Process:** Define a multi-year roadmap for future development and growth.	**Tooling:** Develop automation for CTI intelligence according to **STIXX** and **TAXI**. **Tooling:** Disseminate self-created intelligence to peers or customers.	
Stretch Goals	**Process:** Identify smaller organisations (gov or non-profits) and help them adopt CTI.	**Tooling:** Create a public repository to feed your self-created intelligence and share with the community.	**Tooling:** Identify gaps and self-develop tools to share publicly.	**Process:** Publish on CTI successes and become a thought leader

Figure 8: Aggregation of Best Practices per Maturity Phase

Acknowledgement. The Dutch National CERT NCSC was a primary influence on the interviewed audience. In their role as National Cert, they are a primary driver for information security in the Netherlands. Other (European) National CERTs are also significant resources for CTI knowledge and capabilities. It would be wise for any security-minded organisation, regardless of size or budget to start a conversation with their respective National CERT and assess the tools and resources provided to them.

Biographies

Sijmen Schenk graduated MSc in Information Security with Distinction at the University of London in 2022. He is a military intelligence veteran with a specialization in information security. He works as a consultant to help organisations mature their SOC, CERT and CTI capabilities to perform complex investigations. His research interests are cyber threat intelligence, computer forensics, incident response and the analysis of malware and malware-related infrastructure.

Konstantinos Markantonakis is a Professor at the Information Security Group at Royal Holloway University of London and the Director of the Information Security Group Smart Card and IoT Security Centre (SCC) with research, teaching, and managerial responsibilities. He is also the Director of the Transformative Digital Technologies, Security and Society Catalyst responsible for coordinating multidisciplinary and impactful research. His main research interests involve smart card security and applications, IoTs/CPS, embedded system security and trusted execution environments, secure payment systems, cloud computing and transparent and explainable AI. He has published more than 210 papers, articles and book chapters in international conferences/journals. He continues to act as a consultant on a variety of information security topics.

Series editor: Dr Maryam Mehrnezhad, ISG, Royal Holloway