A CTI doctrine for CTI production
ABOUT US.

Fabien Gainier
Head of Commons studio

David Bizeul
Chief Scientific Officer,
CAMPUS CYBER PROJECT
GOALS

DEVELOPMENT OF SOVEREIGN CYBER SOLUTIONS

REINFORCE THE SYNERGIES BETWEEN THE CYBER ACTORS

INCREASE ATTRACTIVITY
IN FEW WORDS

39% public / 61% private

A 26 000m² facility

187 Members - 46 Partners - 134 Residents
COMMONS STUDIO.

+ **EXPLORE**

  Explore complex issues
  Identify and anticipate future developments in the cyber market.
  Explore by reducing investment risks through pooling.

  Raise innovation by pooled assets
  Deliver proof of concept, prototype, guideline, doctrine.

+ **PRODUCE**

  Lever ecosystem impact with common spread
  Spread European ecosystem points of view.
  Foster development of European standard.
  Increase the interoperability of European solutions.

+ **SHARE**
COMMONS STUDIO IN FIGURES.

+ **24 Commons**
  Produce or in production

+ **14 Workgroups**
  12 still on going from 10 to 20 members

+ **650 People involved**
  From 20 to 80 specialists by community

+ **200 Organisations**
  Involved in the studio
COMMUNITY OF INTEREST.

+ IA AND CYBERSECURITY
+ CRYPTO-ASSETS SECURITY
+ CYBER4TOMORROW
+ TRAINING AND CRISIS CYBER
+ CTI
+ POST QUANTUM CRYPTOGRAPHY
+ SECURITY AND DETECTION IN CLOUD
+ FINANCIAL AND INSURANCE
+ MONITORING AND DETECTION IN MOBILITY
+ DRONES ET ROBOTS SECURITY
+ AGILE SECURITY
+ VULNERABILITY MANAGEMENT
+ TRAINING

CAMPUS CYBER © - First
WWW.CAMPUSCYBER.FR
Wiki of the cyber commons studio for the dissemination of knowledge (wiki.campuscyber.fr)
AGENDA.

01. GOAL.
02. USE CASES.
03. DOCTRINE.
04. PLATFORM.
05. TAKE AWAYS.
• Information overload everywhere
  • Even in cybersecurity
  • Even on cyber threat intelligence

• But lack of structure
  • Source and context is a value driver
  • Plaintext files often come from somewhere else
  • No TTP, IOCs in JPG format….

• People who know do not share (so much…)
  • Intelligence as a weapon
  • Intelligence as a business mode
  • Intelligence as a key advantage
CTI AS A GROUP 101

• Federate people
  • Willing to share
  • Understanding the benefit of mutualization

• Agree on guidelines
  • Orientation (what to focus on)
  • Structure and format
  • Toolset that is relevant

• Run a proof of concept
  • Explain before starting
  • Provide attractive deliverables to start
  • Extend the network to maintain
01. **GOALS (why?).**

+ OPTIMIZE analyst time

+ STORE in a central repository

+ ENHANCE sharing of expert best practices

+ IMPROVE CTI quality for actionability
02. USE CASES (what?).

5 ACHIEVABLE use cases:

• Cyber Threat Intelligence in OSINT world
  • Blog posts consolidation as structured data
• Hot topics and CTI Focus
  • Exploited vulnerability
  • Geopolitical event and collateral damage
• Collaborative report
  • Shared analysis and write a joint paper as an industry position
• Incident sharing
  • Detailed information from a victim in order to protect its peers
• Sightings and measures
  • What is being observed, when and where
02. USE CASES (OSINT example)

Scope

Resources

Distributed repositories

Mixed objects

Result

Company staff

Expertise waste

OSINT

Resources

Distributed repositories

Mixed objects

Result

Company staff

Expertise waste
02. **USE CASES (OSINT example)**

- **Scope**
  - Company staff
  - Company staff
  - Company staff
  - Company staff

- **Resources**
  - Company staff

- **Distributed repositories**
  - Central repository

- **Mixed objects**
  - Graph-based CTI

- **Result**
  - Expertise waste
  - Expertise optimization
DOCTRINE (how?)

- Pack of 60 rules to do great things
- Available in PDF for everyone
- We did that because we did not find one...
- Organized in scoping rules
  - Global rules
  - Specific rules for use cases focus
Example #0 – Naming convention

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCOPE – FIELD - ID</td>
<td>Summary of the rule with a MUST/SHOULD criteria</td>
</tr>
</tbody>
</table>
**Example #1 – Creation and Sharing**

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GLOBAL-CONTENT-1</td>
<td>Threat Intelligence MUST be normalized under the STIX standard.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GLOBAL-SHARING-7</td>
<td>Export must be possible using STIX format, MISP format, CSV file and text file.</td>
</tr>
</tbody>
</table>
### Example #2 - Metadata

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GLOBAL-SHARING-3</td>
<td>The use of TLP MUST be enforced</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GLOBAL-SENSITIVITY-2</td>
<td>The use of PAP MUST be enforced</td>
</tr>
</tbody>
</table>

If not explicitly mentioned in the document, applicable PAP by default will be of similar TLP color-codes.
### Example #3 – Use cases focused rules

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSINT-SOURCE-1</td>
<td>Information MUST come from an OSINT source or at least from a source accommodating of broad data sharing (TLP:CLEAR, TLP:GREEN) and will be marked accordingly</td>
</tr>
<tr>
<td>INCIDENT-TIME-1</td>
<td>Each artefact associated with the incident MUST be timestamped precisely to establish an attack timeline</td>
</tr>
</tbody>
</table>
• **Criteria**
  • Mapping of technical features vs doctrine
  • Members experience and appetite
  • Hosting environment

• **Choice**
  • OpenCTI w/ Filigran support
Introduction

On 28 August 2023, cybersecurity researcher Randy Blyth published an analysis of a new malicious JavaScript framework deployed on compromised websites to deliver further malware using the drive-by-download technique. This newly discovered malware is called ClearFake due to the clear text JavaScript injected into the compromised website, which was not obfuscated in the early version as is usually the case for Javascript malware.

ClearFake is another "Fake updates" threat leveraging social engineering to trick the user into running a fake web browser update, as for SyncThief and Fake3D malware. By linking the "Fake updates" links to the watering hole technique, ClearFake operators target a wide range of users and conduct effective, scalable malware distribution campaigns.
04. PLATFORM (Use case #1/OSINT).
Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft

**Description:** Mandiant has observed wide exploitation of a zero-day vulnerability in the MOVEit Transfer secure managed file transfer software for subsequent data theft. This vulnerability was announced by Progress Software Corporation on May 31, 2023, and has been assigned CVE-2023-34362. Based on initial analysis from Mandiant incident response engagements, the earliest evidence of exploitation occurred on...
04. **PLATFORM (Use case #2/CTI Focus).**
05. **TAKE AWAYS**

1. **Obvious steps but long-term project**
   - 2 years
   - Tons of discussions to promote sharing (who accept to share what and how?)

2. **Doctrine can probably be better**
   - Adapt it to your environment
   - Bring new ideas

3. **Governance aspects not 100% ready**
   - Licence content
   - Validation mechanisms
THANK YOU!

Doctrine file
https://wiki.campuscyber.fr/images/1/10/221206_GT_CTI_doctrine.pdf

fabien@campuscyber.fr
david.bizeul@sekoia.io