STIX in Practice for Incident Response

Freddy Dezeure
Head of CERT-EU
http://cert.europa.eu/
About Us

- EU Institutions’ own CERT
- Supports 60+ entities
- Operational defense against cyber threats
Other EU Cyber Bodies

ENISA
- Europe-wide mandate in cyber security
- Supporting best practices, capacity building and awareness raising

EUROPOL EC3
- Europe-wide mandate in fight against cyber-crime
- Operational cooperation between police computer crime units
Services

Constituents

Prevention → Detection → Incident Handling → Response

CERT-EU

Advisories
White Papers

Alerts

Specialised support
Peers & Partners
Law enforcement

Malware analysis
Security Tools

Threat Intelligence

Threat assessment

Feeds
IOCs
Rules
Context
Agenda

- Introduction
- Architecture
- Use case 1: Detection
- Use case 2: Scoping
- Use case 3: Strategic insight
- Apply
STIX Model+

- Associated Campaigns
- Historical Campaigns
- Attribution
- Associated Actors
- Related TTP
- Exploit Target
- Exploit Target
- Related Threat Actors
- Related Incidents
- Related Indicators
- Related TTP
- Leveraged TTP
- COA Taken
- COA Requested
- Suggested COA
- Victims
- Sources
- Clients
- Observables
- SubObservables
CTI Architecture

**Sources**
- Internal Intelligence
  - CERT-EU
  - Constituents
- External Intelligence
  - Peers
  - Partners
  - Other sources

**Data**
- Unstructured
- Structured
- STIX/Cybox
- MISP

**CTI Repository**
- Collector
- Import Control
- CTI-db
  - Actors
  - TTPs
  - Campaigns
  - Courses of Action
  - Targets
  - Incidents
  - Organisations
  - Indicators
  - Observables
- Export Control
- Producer

**Products**
- Threat Landscape
- Specific Threats
- MISP
- STIX/Cybox

**Recipients**
- Constituents
- Peers
- Partners

**CTI Architecture**
CTI Architecture

- **Sources**
  - Constituents
  - Peers
  - Partners
  - Others

- **Consumers**
  - Constituents
  - Peers
  - Partners

- **CERT-EU**
  - CTI Repository
  - Correlation

- **Feedback**
  - Positives
  - False Positives

**Processes**
- **Collected** Threat data
- **Shared** Threat data
- **Formatting**
- **Contextualisation**
- **Standard Format**
- **Routing**
- **Course of Action**
- **Partners**
- **Peers**
- **Consumers**
- **Constituents**

**Partners**
- **Others**
- **Peers**
- **Constituents**
Threat Data Collection

- Large diversity of information sources
- Too much irrelevant information
- Accuracy not guaranteed
- Unclear timing
- Unclear sighting or targeting
- Difficult prioritisation
Contextualisation

Industry best practice?
### Poor Context

<table>
<thead>
<tr>
<th>Timing</th>
<th>Detect_date</th>
<th>Start_date</th>
<th>End_date</th>
<th>KillChain</th>
<th>Targeting</th>
<th>Geoloc</th>
<th>Sector</th>
</tr>
</thead>
</table>

- **Block traffic to the following domains:**
  - arabooks.ch
  - artas.org
  - tsoftonline.com
  - [www.eamtm.com](http://www.eamtm.com)
  - news.grouptumbler.com

- **Block traffic to the following IPs:**
  - 200.63.46.23
  - 194.38.160.153
  - 95.128.72.24
  - 72.34.47.186
  - 188.40.99.143
  - 85.95.236.114
### Better Context

<table>
<thead>
<tr>
<th>Exploit files</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>First seen</strong></td>
<td><strong>Filename</strong></td>
</tr>
<tr>
<td>2013-11-04</td>
<td>-</td>
</tr>
<tr>
<td>2014-03-20</td>
<td>nota.pdf</td>
</tr>
<tr>
<td>2014-03-14</td>
<td>dip.mail march.pdf</td>
</tr>
<tr>
<td>2014-03-11</td>
<td>Bulletin-PSIM-No.31-(625)-March-10-2014.pdf</td>
</tr>
<tr>
<td>2014-03-05</td>
<td>March.pdf</td>
</tr>
<tr>
<td>2013-07-01</td>
<td>paper_format.pdf</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Droppers</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>First seen</strong></td>
<td><strong>Filename</strong></td>
</tr>
<tr>
<td>2014-04-27</td>
<td>rcs.DSC.1232222233.jpg</td>
</tr>
<tr>
<td>2014-03-18</td>
<td>rcs.18.jpg</td>
</tr>
<tr>
<td>2013-11-11</td>
<td>rcs.3ana3.doc</td>
</tr>
</tbody>
</table>

### Timing
- **Detect date**: ✓
- **Start date**: ✓
- **End date**: N/A

### KillChain
- ✓

### Targeting
- ✗

### GeoLoc

### Sector
13
EU-I - Targeting one or more constituents

EU-Centric – Targeting EU Member States

EU Nearby - Targeting close partners (e.g. NATO, USA)

World-Class - EU-I might be ‘opportunity’ or ‘collateral’ victims of major world-wide threats

Threat Scope

Threat Level

High
Very sophisticated APT

Medium
APT

Low
Non-targeted mass attacks / malware

Threat Scope

World-Wide EU-nearby EU-centric EU-I

Threat level

High priority threat
Medium priority threat
Low priority threat
Out of scope = 'noise'

Threat Scope
Constituent Perspective

- Limited resources
- Specific IT security tools
- Specific policies
- Prioritisation
- Automation / Routing
- Minimise false-positives
- Actionable context when needed
Threat Data Sharing

Raw + Context

Selection Routing

Prioritise
Decide
Act

IDS
Firewall
Mail server
Log analyser
Host Scanner
Intelligence Awareness

SIEM
Use Case 1: Detection

- Products
  - SNORT
  - YARA
  - CSV
  - MISP
  - STIX / Cybox

- Recipients
  - Constituents
  - Peers
  - Partners

- Detection
  - SOURCEFIRE
  - SURICATA
  - Q-RADAR
  - ARCSIGHT
  - SPLUNK
  - THOR
  - nCASE
  - Proxy

CTI-db
- Actors
- TTPs
- Campaigns
- Courses of Action
- Targets
- Incidents
- Organisations

Export Control
- Indicators
- Observables

Producer

CTI-db
- Indicators
- Observables
Use Case 2: Scoping

- Malware reversing
- Internal process
  - Scanning for IOCs in logs and hosts
  - Scanning for anomalous traffic
  - Hits on the proxy/IDS
- External process
  - Has anybody else seen this?
    - No? -> You’re on your own
    - Yes? -> Multiply knowledge on IOCs
    - What’s the timeline
  - Sinkholing
Pivoting via Actor / Campaign

Incident 1

Incident 2

Incident 3

Unique TTPs
Yara
Snort
# Use Case 3: Strategic Insight

## Technical
- Immediate reaction to threats: Detection, Prevention, Reaction (eradication, recovery), Report
- Dynamic feeding cyber-defense tools: IDS, IPS, SIEM, Security Scanners, Mailguard, Firewalls, etc

## Tactical
- Understanding cyber-attacks tactical context: threat type and level, timing of events, techniques/malware used.
- Planning structured course of actions for permanent protection

## Strategic
- Understanding the broader context.
- Strategic context: profile, motives, new techniques/tactics, sector and location of victims, business risk.
- Planning high level actions for non-technical treatment of the threat.

## Threat Landscape
- Periodic Bulletin
- Security Brief

## CITAR
- For every new significant campaign

## CIMBL Feeds
- IOC Rules
  - (Near real-time -> Towards full automation)
Current Content

**Threat Actors**
- 200+
- Espionage/Strategic
- Hacktivists
- Cyber-criminals

**Campaigns**
- 300+
- Espionage (political, industrial, etc)
- Hacktivism
- CyberCrime

**Incidents & Indicators**
- 3000+ per year
- Scope: Constituency / EU-centric / EU-nearby/ World-class

**Victims**
- 500+
- Continent/country
- Sector (Diplomacy, Defense, Energy, Transport, etc)
- Type (Private, Public)

**Observables**
- 800,000 targeted IOCs
- Malicious Domains = 65%
- Malicious Files = 10%
- Malicious email addresses = 8%
- Malicious IP = 5%
- Malicious URL = 4%
- Other (Regkey, snort, etc) = 8%

**Techniques, Tactics, Procedures**
- 500+
- "Identity card" of malware, botnets, C&C infrastructures, tools, exploit-kits
- Killchain analysis
- Focus on sophisticated & targeted TTP
Some Open Issues

- How to manage lifetime of the data
- How to remove data downstream
- How to control sharing groups downstream
- Implement Course of Action
- How to maintain the treasure trove of TTPs
Apply Slide

- Insist with your suppliers to deliver context with their feeds
- Identify “your” definitions to filter inputs/outputs
  - Threat scope and level
  - Sharing groups
  - Course of Action
  - ...
- Start implementing your own internal STIX repository
- Embed it in your processes
Thank You!

http://cert.europa.eu/