A WORD ABOUT TNO

➢ Dutch innovation and advisory body, founded by law in 1932 and currently comprising some 2800 professionals

➢ Active in many fields (a.o. healthcare, automotive, defence, energy and ICT), not-for-profit and independent of public & private interests

---

Cyber Security team (~45 FTE)

(focus areas)

- Monitoring & Detection
- Automated Security
- Transaction Security

key partners

- Dutch government
- NCSC
- MoD/ Defence industry (NL)
- Financials (NL)
- Telcos (Europe)
EVOLUTION OF RESILIENCE STRATEGIES

Traditional prevention: put up walls and hope for the best

Monitoring & response construct: detect (potential) attacks and limit damage

Threat intelligence capabilities: anticipate and take proactive precautions

Autonomous response & recovery: reduce dependency on human operation

often induced by (severe) incident

focus of this presentation
THE CTI PLAYING FIELD

CTI processes & solutions

operational
firewall mngmt,
patching, monitoring,
vulnerability mngmnt,
incident response, …

Public

SANS
PhishTank

FireEye

CERT/CSIRT

sys admin

process

Commercial

ALIENVault

strategic & tactical
policy development,
architecture design, staffing,
training, supplier mngmnt,…

Community

FIRST

CERT

CIRCL

ING

CTI insights
(TTP, IoC, …)

e.g. sightings

initiate CoA

situational
awareness

trends

policy
team

mngrs

security
architects

Towards a Mature CTI Practice – Borderless Cyber
AN AREA THAT NEEDS MATURING

- underdeveloped – strong emphasis on operational processing
- ad hoc workflows – relies on expertise of individuals
- limited resourcing – duties usually reside in CSIRT
- scattering of threat information – much resides in mailboxes
- little automation – e.g. exchange of threat information via e-mail

"pain" inflicted on cyber adversaries*

present efforts largely revolve around indicators
– but the real value lies in tactical intelligence!

focus of activities

* Pyramid of Pain published by David Bianco

Towards a Mature CTI Practice – Borderless Cyber
BUT WHAT CONSTITUTES “MATURE”?

CSIRT Handbook by CERT/CC

- Description of typical CSIRT services (2003), a.o. adopted by ENISA.
- **No clear definition** of CTI related services

MITRE’s SOC Capabilities

- **Intended as tangible and contemporary foundation** for maturing CTI provisions
- Developed in collaboration with major Dutch financials.

**Carson Zimmerman,** “Ten Strategies of a World-Class Cyber Security Operations Center”

- Modern perspective (2014), includes “intel & trending”
- Fairly **high level** and some (key) elements embedded in broader SOC capability
DEFINING CTI CAPABILITIES

CTI capabilities

STIX
CSV
OpenIOC

(threat information)

production of actionable CTI

elevate operational security & resilience

(outcome)
ELEVATE OPERATIONAL SECURITY

Towards a Mature CTI Practice – Borderless Cyber

threat indicators

- STIX
- OpenIOC

production of actionable CTI

monitor (SIEM, IDS)
block (firewall, ACL)
hunt (data lake)
(typical setup)

CTI-01:01 Ingestion of structured CTI
- establish indicator feeds
- pre-process for analysis (e.g. enrich with contextual data)

CTI-02:01 Triage & assignment
- select CoA
- automated
- playbook
- expert
(fast throughput)

CTI-02:02 Threat investigation
- assess threat & possible mitigations
- select action
- CoA
- monitor
- standardise for fast triage

CTI-02:03 CoA management
- prepare CoA (e.g. signature)
- initiate CoA
- API
- ticket
- monitor CoA establishment
COMPILING THE FRAMEWORK

CTI capabilities

CTI-01 CTI collection
CTI-01:01 Ingestion of structured CTI

CTI-02 Real-time CTI processing
CTI-02:01 Triage & assignment
CTI-02:02 Threat investigation
CTI-02:03 CoA management

elevate operational security & resilience
supply on-demand threat insights
outcome
production of actionable CTI

Towards a Mature CTI Practice – Borderless Cyber
**SUPPLY ON-DEMAND THREAT INSIGHTS**

**actors, TTP, campaigns….**

<table>
<thead>
<tr>
<th>CTI-01:01 Ingestion of structured CTI</th>
<th>CTI-01:02 Ingestion of unstructured CTI</th>
<th>CTI-02:02 Threat investigation</th>
<th>CTI-04:02 CTI dashboarding</th>
</tr>
</thead>
<tbody>
<tr>
<td>establish tactical feeds</td>
<td>acquire threat reports/ mailings</td>
<td>analyse &amp; correlate threat information</td>
<td>self-service portal</td>
</tr>
<tr>
<td>pre-process for analysis</td>
<td>abstract machine readable threat information</td>
<td></td>
<td>current threats</td>
</tr>
<tr>
<td>(typical scenario)</td>
<td>(align with needs of target audiences)</td>
<td>(align with needs of target audiences)</td>
<td>actor analysis</td>
</tr>
</tbody>
</table>

**production of actionable CTI**

**specific threat insights**

**CERT/CSIRT**

**archive in structured repository**
EXPANDING THE FRAMEWORK

Towards a Mature CTI Practice – Borderless Cyber

CTI capabilities

CTI-01 CTI collection
- CTI-01:01 Ingestion of structured CTI
- CTI-01:02 Ingestion of unstructured CTI

CTI-02 Real-time CTI processing
- CTI-02:01 Triage & assignment
- CTI-02:02 Threat investigation
- CTI-02:03 CoA management

CTI-04 CTI dissemination
- CTI-04:02 CTI dashboarding

elevate operational security & resilience

supply on-demand threat insights

supply tactical threat insights

production of actionable CTI

(outcome)

(threat information)
SUPPLY TACTICAL THREAT INSIGHTS

- Assess effects of CTI trends and events
- Create prioritized list of cyber threats
- ID threats/trends for which organisation is not prepared
- Assess causes/shortcomings
- Raise with security leaders
- ID stakeholders & their needs
- Develop reporting products/ formats
- Create and distribute reports

CTI-03:01 Trend analysis
- Analyse threat info collected over time
- ID structural changes, e.g. in attacker MO
  (often fed by trigger)

CTI-03:02 Threat landscaping
- Assess effects of CTI trends and events
- Create prioritized list of cyber threats

CTI-03:03 Strategic CTI review
- ID threats/trends for which organisation is not prepared
- Assess causes/shortcomings
- Raise with security leaders

CTI-04:03 Reporting & alerting

Threat information production of actionable CTI

From: ENISA Threat Landscape Report 2016
EXPANDING SOME MORE

CTI capabilities

CTI-01 CTI collection
- CTI-01:01 Ingestion of structured CTI
- CTI-01:02 Ingestion of unstructured CTI

CTI-02 Real-time CTI processing
- CTI-02:01 Triage & assignment
- CTI-02:02 Threat investigation
- CTI-02:03 CoA management

CTI-03 Periodic CTI processing
- CTI-03:01 Trend analysis
- CTI-03:02 Threat landscaping
- CTI-03:03 Strategic CTI review

CTI-04 CTI dissemination
- CTI-04:02 CTI dashboarding
- CTI-04:03 Reporting & alerting

production of actionable CTI

elevate operational security & resilience
supply on-demand threat insights
supply tactical threat insights

(outcome)
EVALUATE & IMPROVE THE SETUP

threat indicators
- monitor (SIEM, IDS)
- block (firewall, ACL)
- hunt (data lake)

note: also includes
- CTI source selection
- CTI data maintenance
  (not covered today)

production of actionable CTI

measure effects
(sightings, incidents, false positives …)

evaluate sources
(relevance, quality)

measure value
(unicity, richness…)

CTI-01:03 CTI life-cycle management

- acquire source performance data
- evaluate threat information sources

discontinue/replace?
ALMOST THERE

CTI capabilities

- **CTI-01 CTI collection**
  - CTI-01:01 Ingestion of structured CTI
  - CTI-01:02 Ingestion of unstructured CTI
  - CTI-01:03 CTI life-cycle management

- **CTI-02 Real-time CTI processing**
  - CTI-02:01 Triage & assignment
  - CTI-02:02 Threat investigation
  - CTI-02:03 CoA management

- **CTI-03 Periodic CTI processing**
  - CTI-03:01 Trend analysis
  - CTI-03:02 Threat landscaping
  - CTI-03:03 Strategic CTI review

- **CTI-04 CTI dissemination**
  - CTI-04:02 CTI dashboarding
  - CTI-04:03 Reporting & alerting

**Production of actionable CTI**

- **Elevate operational security & resilience**
- **Supply on-demand threat insights**
- **Supply tactical threat insights**
- **Collaborate with community partners**

*threat information*
COLLABORATE WITH COMMUNITY PARTNERS

- prepare threat info for community partners
  - unique
  - vetted
  - cleared
- distribute via designated channels

communities may differ in terms of
- focus of threat info exchange
- formats, practices and rules of play

this may affect capabilities required for appropriate contribution
CTI CAPABILITY FRAMEWORK

Towards a Mature CTI Practice – Borderless Cyber

For each, model addresses:

a. definition & purpose
b. core operations/ workflow
c. automation potential

e. Explicitly detached from security team demarcations (SOC, CERT…)

Exploring possibilities to transform into ENISA guideline
TAKE AWAYS

- We see a need for a **CTI capability framework** that can serve as a foundation for establishing a mature CTI practice.

- Not every organization will need (or be able) to develop all capabilities encompassed in the framework – a **balanced selection** can also be appropriate.

- As you develop these CTI capabilities, you may discover **automation needs** you had not anticipated before. This might for instance result in new requirements for your CTI platform.
THANK YOU & FURTHER READING

Richard Kerkdijk
+31 6 2290 64 64
richard.kerkdijk@tno.nl

https://www.tno.nl/media/9419/
innovating-in-cyber-security.pdf