CYBER THREAT INTELLIGENCE

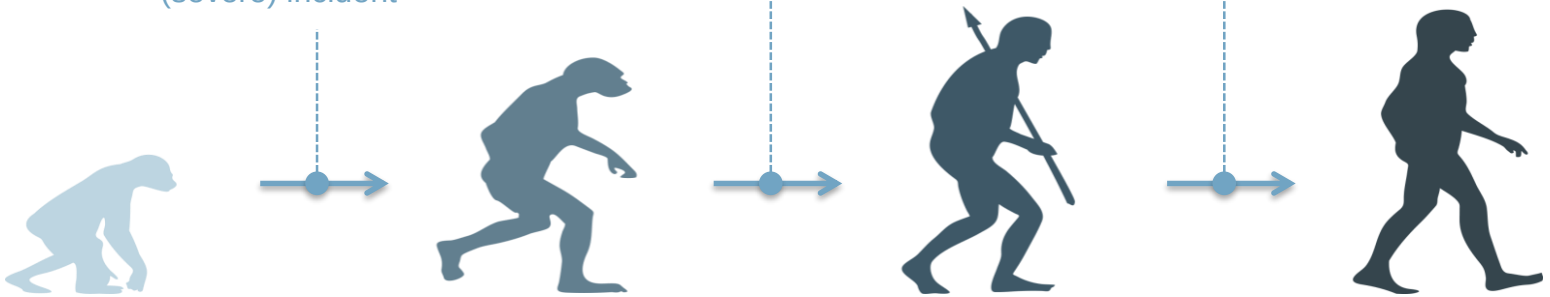
TOWARDS A MATURE CTI PRACTICE

Richard Kerkdijk | August 28th 2018

TNO innovation for life

EVOLUTION OF RESILIENCE STRATEGIES

often induced by
(severe) incident



Traditional prevention
put up walls and hope for the best

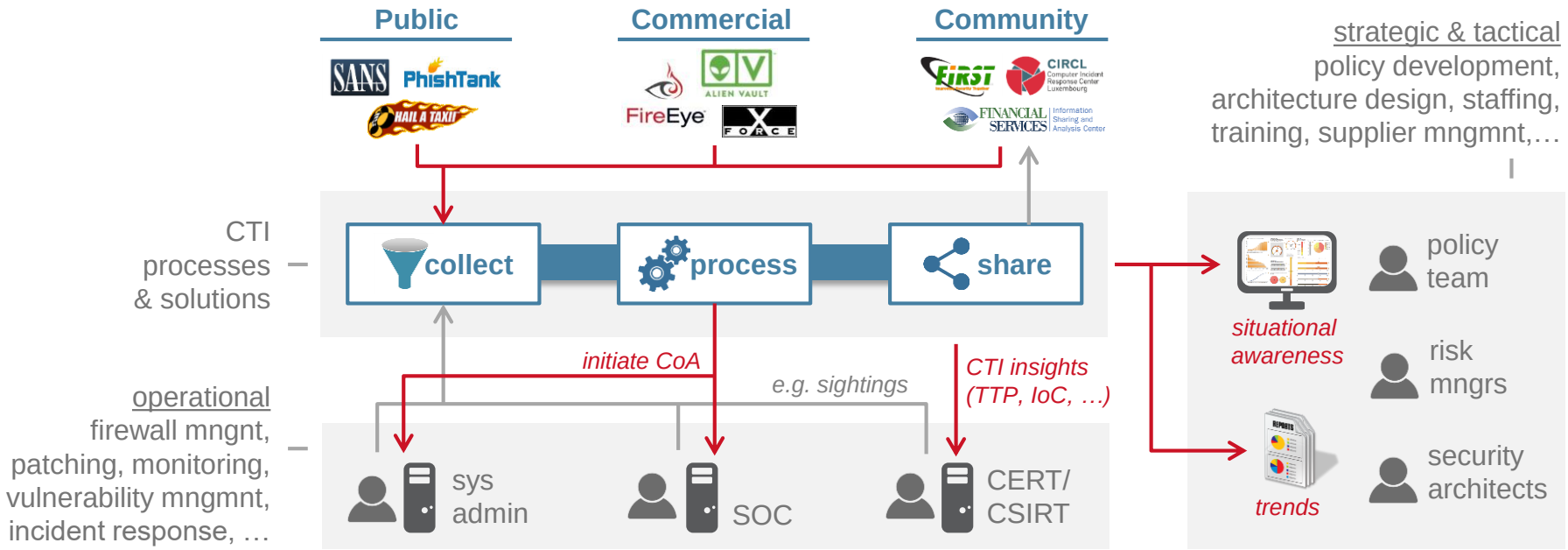
Monitoring & response construct
detect (potential) attacks and limit damage

Threat intelligence capabilities
anticipate and take proactive precautions

Autonomous response & recovery
reduce dependency on human operation

focus of this presentation

THE CTI PLAYING FIELD

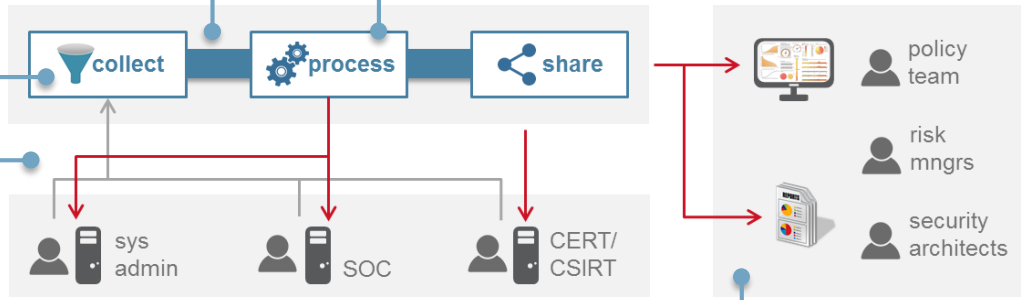


AN AREA THAT NEEDS MATURING

limited **resourcing** – duties usually reside in CSIRT

ad hoc workflows – relies on expertise of individuals

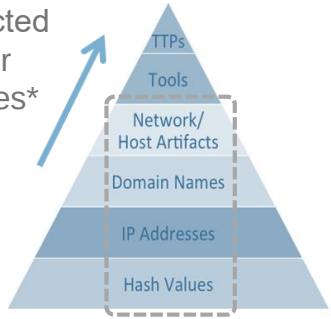
scattering of threat information – much resides in mailboxes



little **automation** – e.g. exchange of threat information via e-mail

underdeveloped – strong emphasis on operational processing

"pain" inflicted on cyber adversaries*



focus of activities

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

** Pyramid of Pain published by David Bianco*

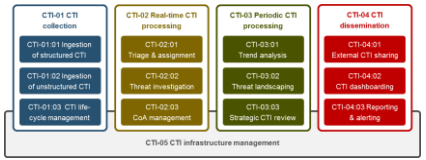
BUT WHAT CONSTITUTES “MATURE”?

CSIRT Handbook by CERT/CC

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

revision?

CTI Capability Framework



ABN·AMRO ING Rabobank TNO

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

inspiration

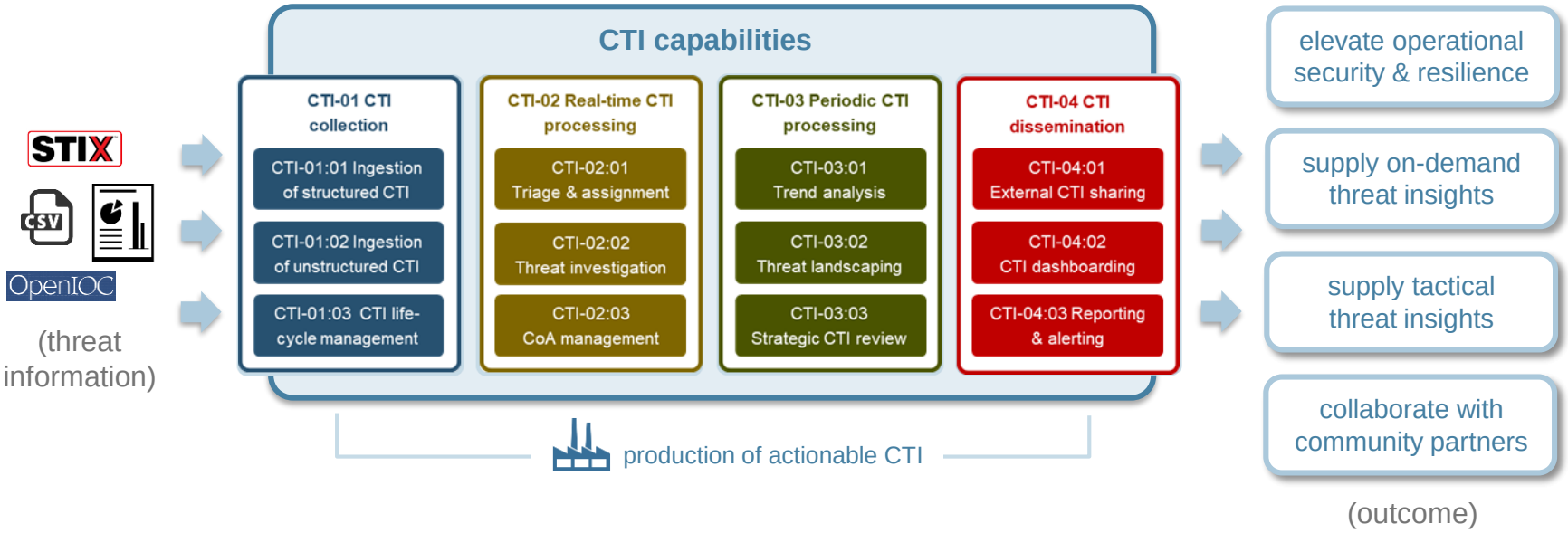
MITRE’s SOC Capabilities

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

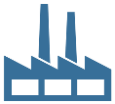
DEFINING CTI CAPABILITIES

Note: framework to be published as ENISA guidebook later this year



ELEVATE OPERATIONAL SECURITY

threat indicators



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

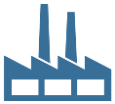
- ❑ assess threat & possible mitigations
- ❑ select action
  - CoA
  - monitor
- ❑ standardise for fast triage

CTI-02:03 CoA management

- ❑ prepare CoA *(e.g. signature)*
- ❑ initiate CoA
  - API
  - ticket
- ❑ monitor CoA establishment

SUPPLY ON-DEMAND THREAT INSIGHTS

actors, TTP, campaigns….



production of actionable CTI

Q specific threat insights

CERT/CSIRT

(typical scenario)

CTI-01:01 Ingestion of structured CTI

- ❑ establish tactical feeds
- ❑ pre-process for analysis

CTI-01:02 Ingestion of unstructured CTI

- ❑ acquire threat reports/ mailings
- ❑ abstract machine readable threat information

CTI-02:02 Threat investigation

- ❑ analyse & correlate threat information

archive in structured repository

CTI-04:02 CTI dashboarding

- ❑ self-service portal
  - current threats
  - actor analysis
  - …

(align with needs of target audiences)

SUPPLY TACTICAL THREAT INSIGHTS

threat information

STIX CSV OpenIOC

production of actionable CTI

trends

Top Threats 2016	Assessed Trends 2016	Change in ranking
1. Malware		→
2. Web based attacks		→
3. Web application attacks		→
4. Denial of service		↑
5. Botnets		↓
6. Phishing		↑

(example)

from: ENISA Threat Landscape Report 2016

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

- ❑ ID stakeholders & their needs
- ❑ develop reporting products/ formats
- ❑ create and distribute reports

TAKE AWAYS

- We see a need for a **CTI capability framework** that can serve as a foundation for establishing a mature CTI practice.
- Practices for collecting and processing CTI might offer an interesting direction for **standardisation**. One could even imagine a certification scheme.
- Not every organization will need (or be able) to develop all capabilities encompassed in the proposed framework – a **balanced selection** can also be appropriate

THANK YOU & FURTHER READING

TNO innovation for life

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

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