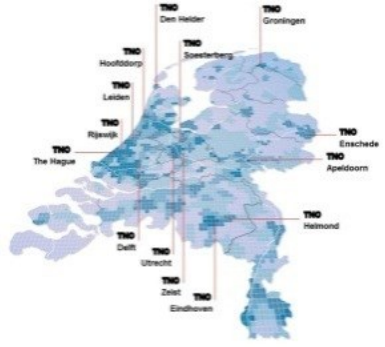
CTI CAPABILITY FRAMEWORK

ENISA CTI EVENT

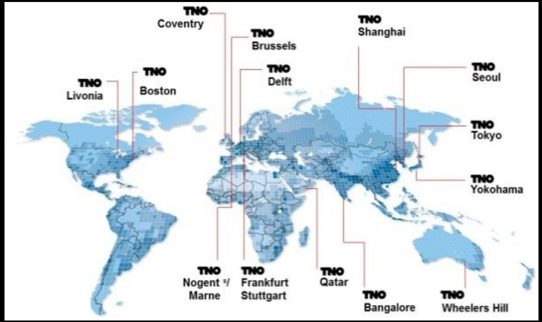
Richard Kerkdijk | October 31st 2017

TNO innovation for life

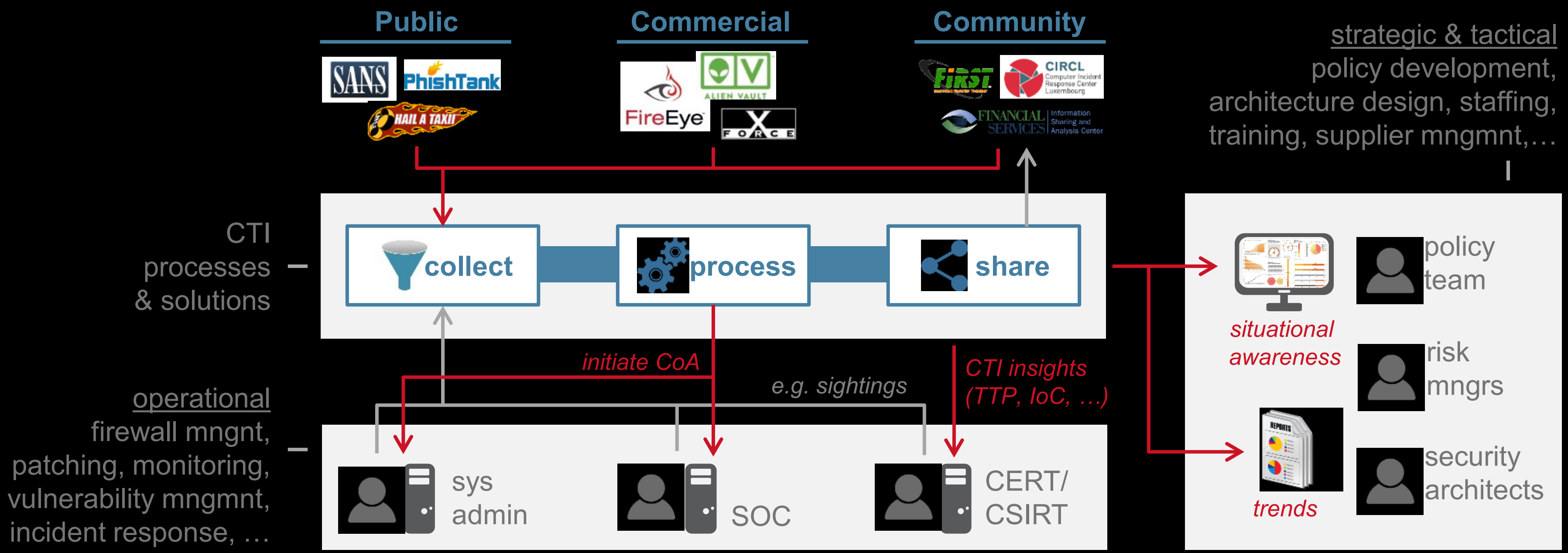
A WORD ABOUT TNO



- innovation and advisory
- independent
  - cyber security



THE CTI PLAYING FIELD



CTI processes & solutions

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

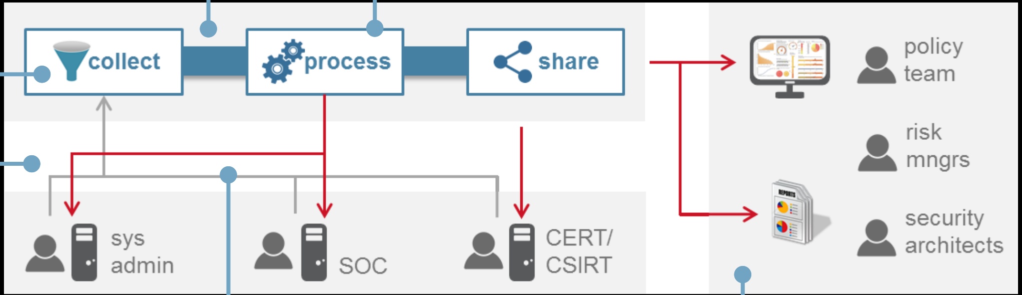
strategic & tactical
policy development, architecture design, staffing, training, supplier mngmnt,…

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

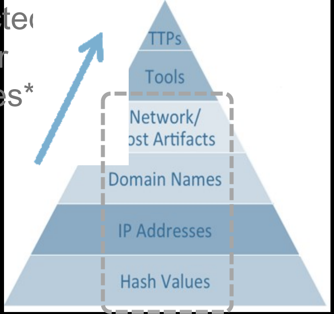


little **automation** – e.g. exchange of threat information via e-mail

limited use of **internal** threat information (e.g. “sightings”, honeypots)

relatively **underdeveloped** – typically limited to quarterly expert reports

“pain” inflicted on cyber adversaries*



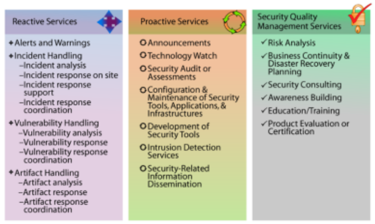
focus of activities

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



Reactive Services

- Alerts and Warnings
- Incident Handling
  - Incident analysis
  - Incident response on site
  - Incident response support
  - Incident response coordination
- Vulnerability Handling
  - Vulnerability analysis
  - Vulnerability response
  - Vulnerability response coordination
- Artifact Handling
  - Artifact analysis
  - Artifact response
  - Artifact response coordination

Proactive Services

- Announcements
- Technology Watch
- Security Audit or Assessments
- Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

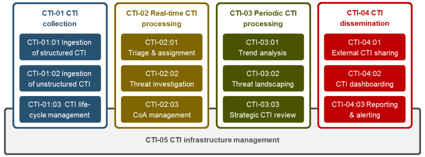
Security Quality Management Services

- ✓ Risk Analysis
- ✓ Business Continuity & Disaster Recovery Planning
- ✓ Security Consulting
- ✓ Awareness Building
- ✓ Education/Training
- ✓ Product Evaluation or Certification

revision?

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

CTI Capability Framework



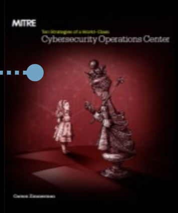
CTI-01 CTI collection	CTI-02 Real-time CTI processing	CTI-03 Periodic CTI processing	CTI-04 CTI dissemination
CTI-01:01 Ingestion of structured CTI	CTI-02:01 Triage & assignment	CTI-03:01 Trend analysis	CTI-04:01 External CTI sharing
CTI-01:02 Ingestion of unstructured CTI	CTI-02:02 Threat investigation	CTI-03:02 Threat landscaping	CTI-04:02 CTI dashboarding
CTI-01:03 CTI life-cycle management	CTI-02:03 CoA management	CTI-03:03 Strategic CTI review	CTI-04:03 Reporting & alerting

CTI-05 CTI infrastructure management

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

MITRE’s SOC Capabilities

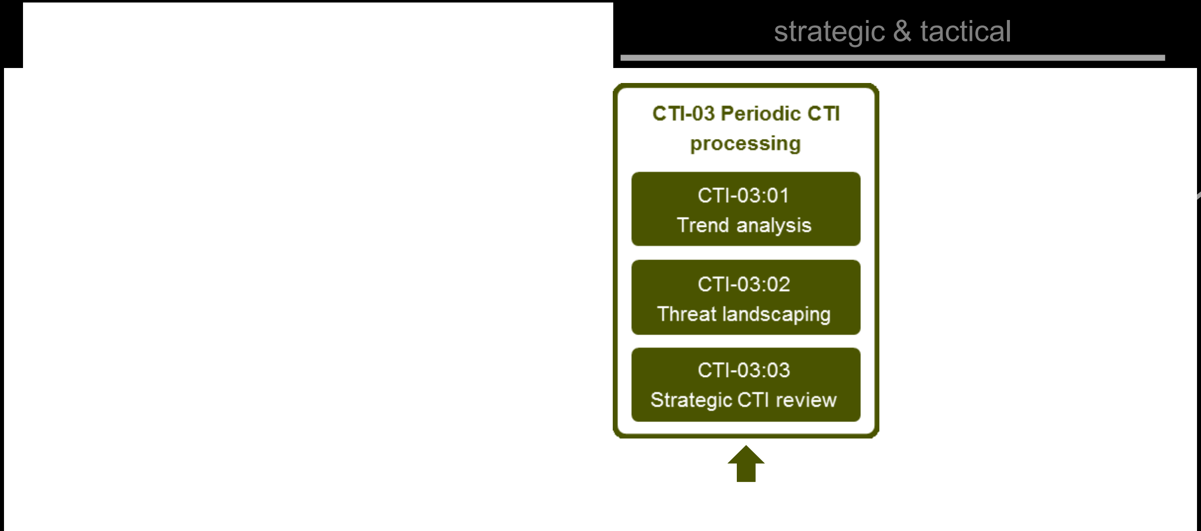
inspiration

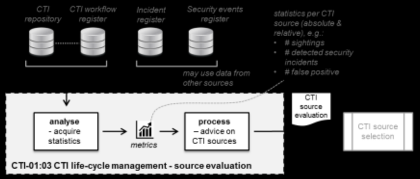

MITRE
Ten Strategies of a World-Class
Cybersecurity Operations Center

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

CTI CAPABILITY FRAMEWORK




CTI repository
CTI workflow register
Incident register
Security events register
may use data from other sources
statistics per CTI source (absolute & relative), e.g.:
• # sightings
• # detected security incidents
• # false positive
analyse - acquire statistics
metrics
process – advice on CTI sources
CTI source evaluation
CTI source selection
CTI-01:03 CTI life-cycle management - source evaluation

Sample workflow: CTI life-cycle management (source evaluation)

-
  a.
  b.
  c.
- **detached**

TREND ANALYSIS

typically results from data science

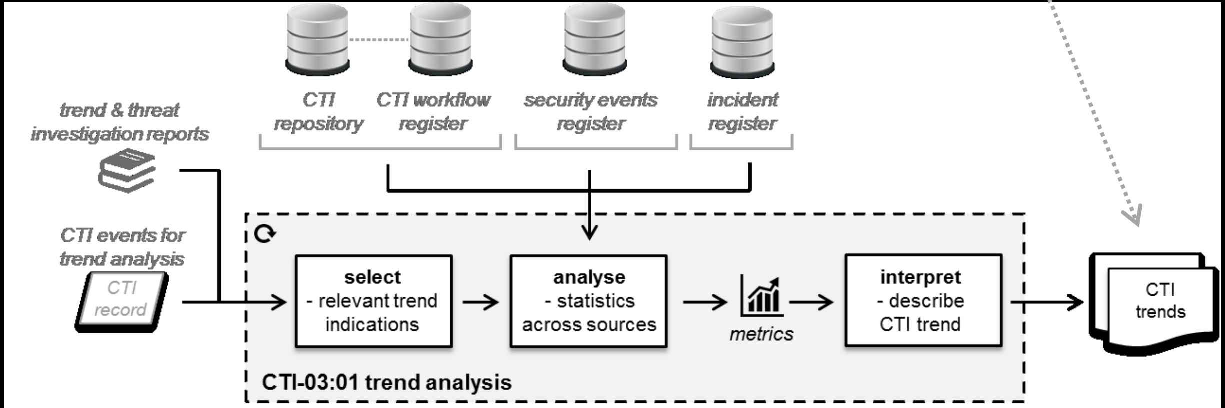
metrics/ statistics

(example)

trigger	trend indications	relevant	CTI	CoA	event	incident	trend
major incident at peer organisation	router malware (TTP)	Y	⬆	⬆	N	N	Y
	nation state espionage (actor)	Y	⬆	N	N	N	Y

DEFINITION

deduce tactical insights concerning nature, severity and relevance of cyber threats from aggregated CTI collected over time



CTI repository

CTI workflow register

security events register

incident register

trend & threat investigation reports

CTI events for trend analysis

CTI record

select
- relevant trend indications

analyse
- statistics across sources

metrics

interpret
- describe CTI trend

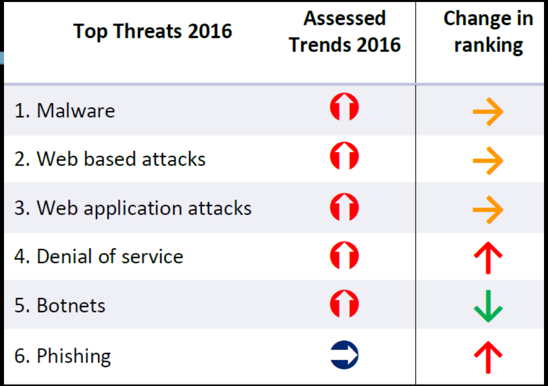
CTI trends

CTI-03:01 trend analysis

THREAT LANDSCAPING

new
entry

sightings, incidents, alerts…
- present and expected
- relative to other threats



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	➡	↑

source: ENISA Threat Landscape Report 2016
Published: Feb 2017

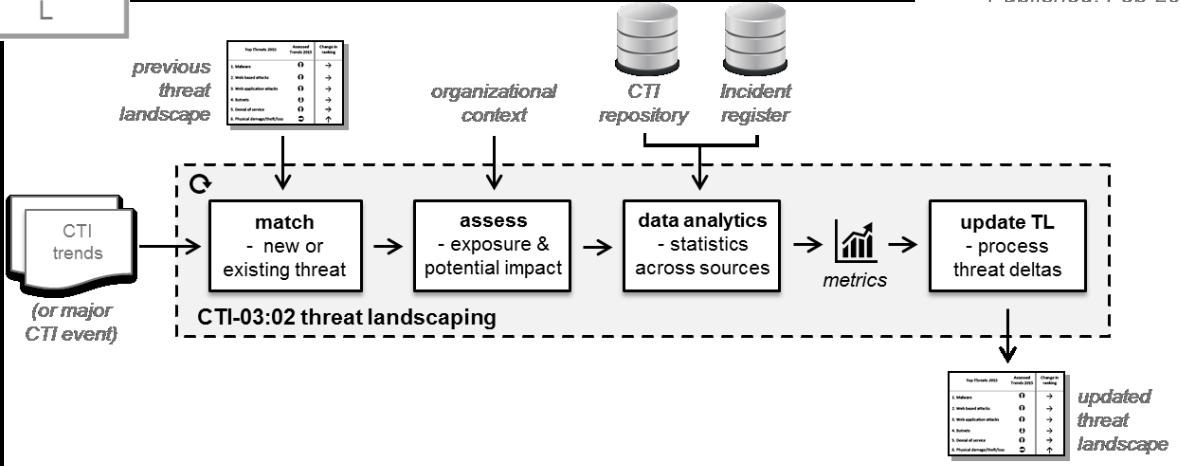
organisational context

	match	impact	resilience
router malware (TTP)	*new*	H	L

(example)

DEFINITION

create prioritized list of most relevant cyber threats by assessing effects of (major) CTI trends and events



STRATEGIC CTI REVIEW

access control, integrity protection, monitoring…

(example of outcome)

router malware (TTP)
1. router security policy
2. router reinforcement program
3. router forensics training

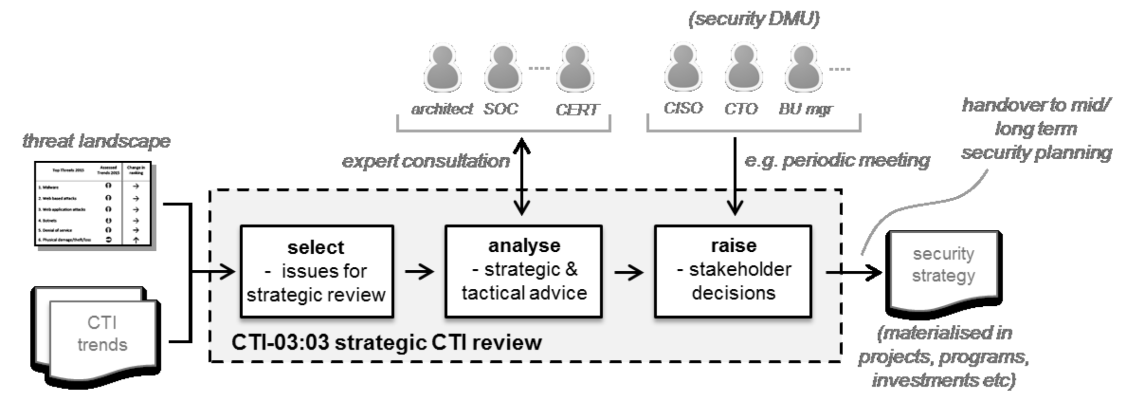
nation state espionage (actor)
4. expert recruitment

require planning and budgeting

(not on-the-fly actions…)

DEFINITION

identify and raise CTI developments for strategic decision making and mid-long term security planning

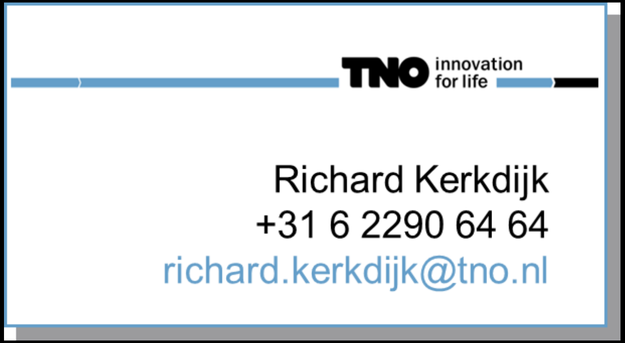


(security DMU)
architect
SOC
CERT
CISO
CTO
BU mgr
threat landscape
CTI trends
expert consultation
e.g. periodic meeting
handover to mid/ long term security planning
select - issues for strategic review
analyse - strategic & tactical advice
raise - stakeholder decisions
CTI-03:03 strategic CTI review
security strategy
(materialised in projects, programs, investments etc)

TAKE AWAYS

- **CTI capability framework** *(even better: common framework that also covers monitoring, VM and incident response)*
- **strategic and tactical CTI processing**
- **situational awareness** **risk management**

THANK YOU & FURTHER READING



TNO innovation for life

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

Innovating in Cyber Security
Shared research 2017