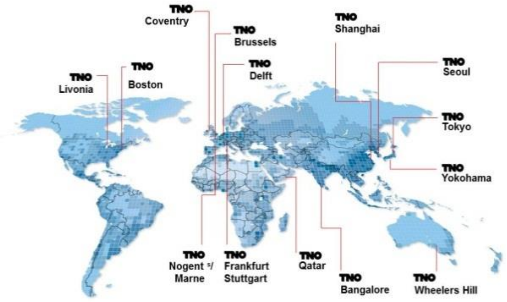
CYBER THREAT INTELLIGENCE

TOWARDS A MATURE CTI PRACTICE

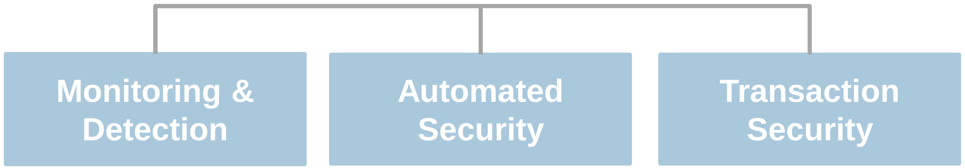
Richard Kerkdijk | December 7th 2017

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

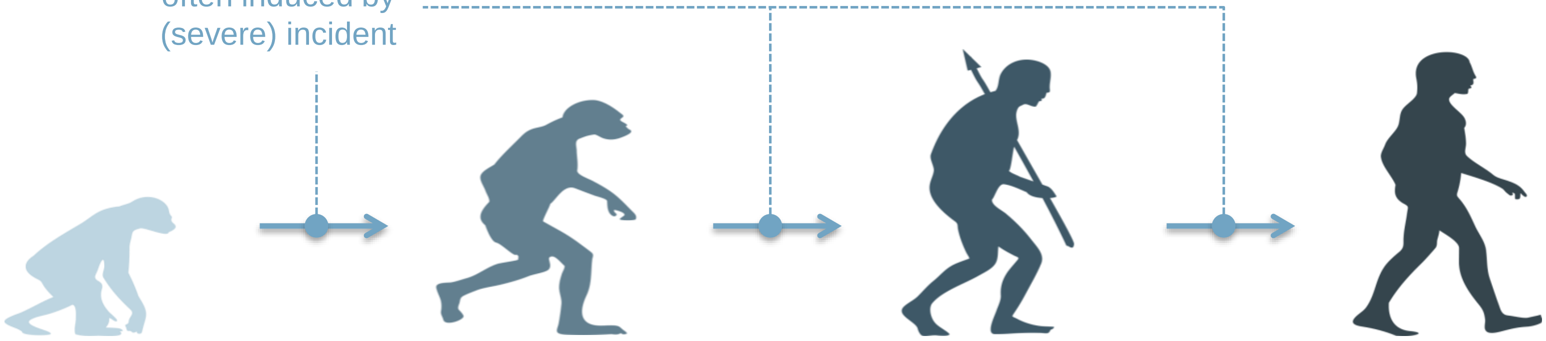
Automated Security

Transaction Security

key partners

- Dutch government
- NCSC
- MoD/ Defence industry (NL)
- Financials (NL)
- Telcos (Europe)

EVOLUTION OF RESILIENCE STRATEGIES



often induced by (severe) incident

Traditional prevention
put up walls and hope for the best

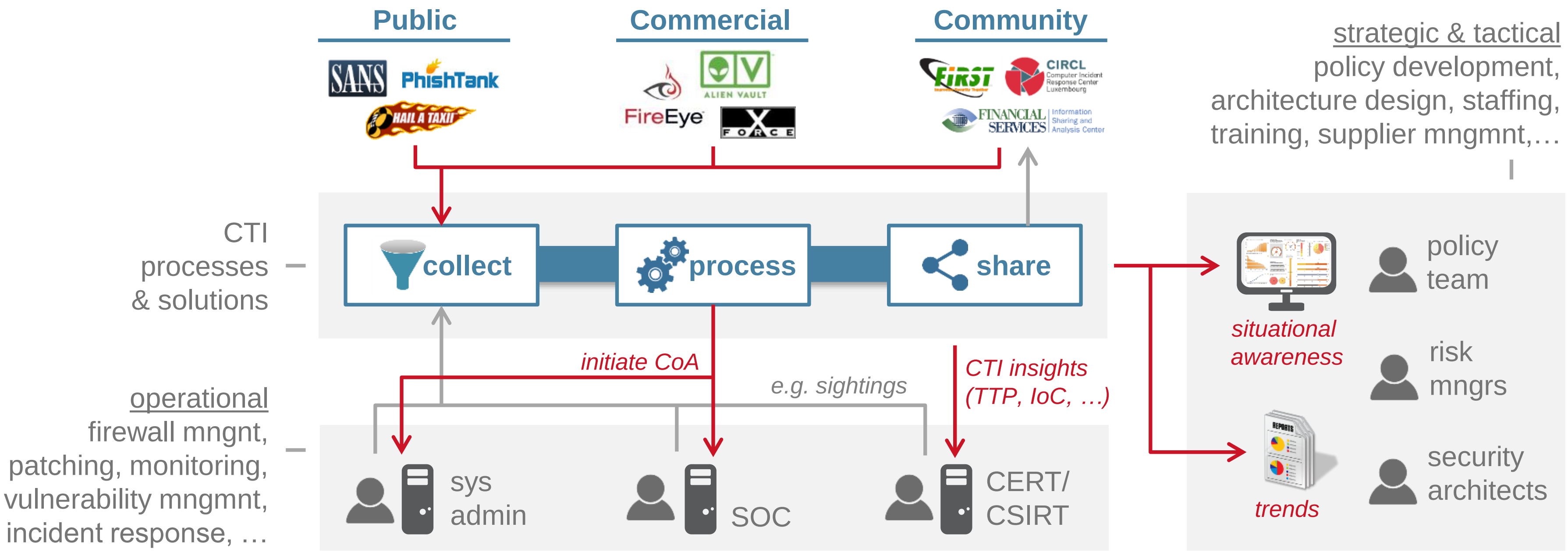
Monitoring & response construct
detect (potential) attacks and limit damage

Threat intelligence capabilities
anticipate and take proactive precautions

Autonomous response & recovery
reduce dependency on human operation

focus of this presentation

THE CTI PLAYING FIELD



Public

SANS PhishTank HAIL A TAXII

Commercial

FireEye ALIEN VAULT X-FORCE

Community

FIRST CIRCL Computer Incident Response Center Luxembourg FINANCIAL SERVICES Information Sharing and Analysis Center

CTI processes & solutions

collect

process

share

initiate CoA

e.g. sightings

CTI insights (TTP, IoC, …)

operational

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

sys admin

SOC

CERT/ CSIRT

strategic & tactical

policy development, architecture design, staffing, training, supplier mngmnt,…

situational awareness

trends

policy team

risk mngrs

security architects

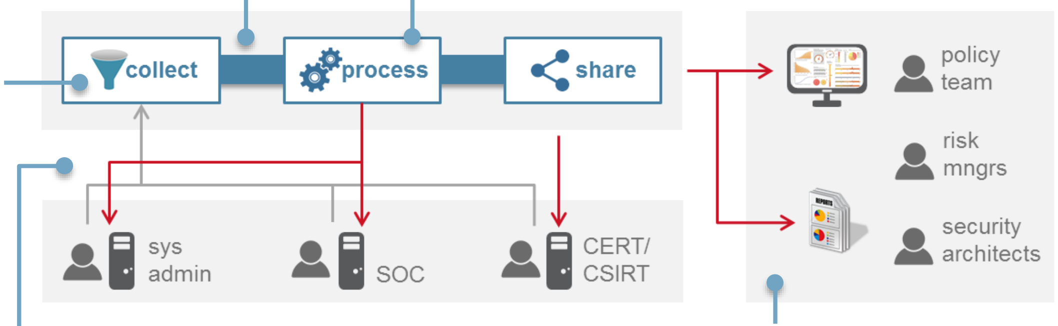
AN AREA THAT NEEDS MATURING

** Pyramid of Pain published by David Bianco*

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

ad hoc workflows – relies on expertise of individuals

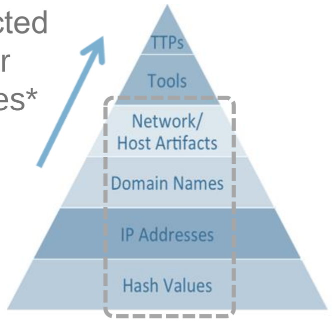
scattering of threat information – much resides in mailboxes



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

underdeveloped – strong emphasis on operational processing

“pain” inflicted on cyber adversaries*

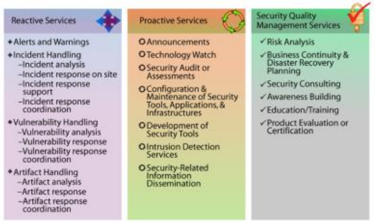


focus of activities

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

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

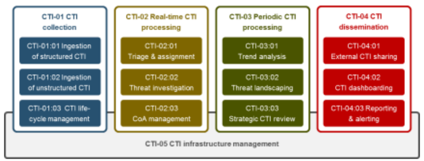
Security Quality Management Services

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

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

revision?

CTI Capability Framework



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-04:01 External CTI sharing
CTI-04:02 CTI dashboarding
CTI-04:03 Reporting & alerting
CTI-05 CTI infrastructure management

ABN·AMRO ING Rabobank TNO

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

inspiration

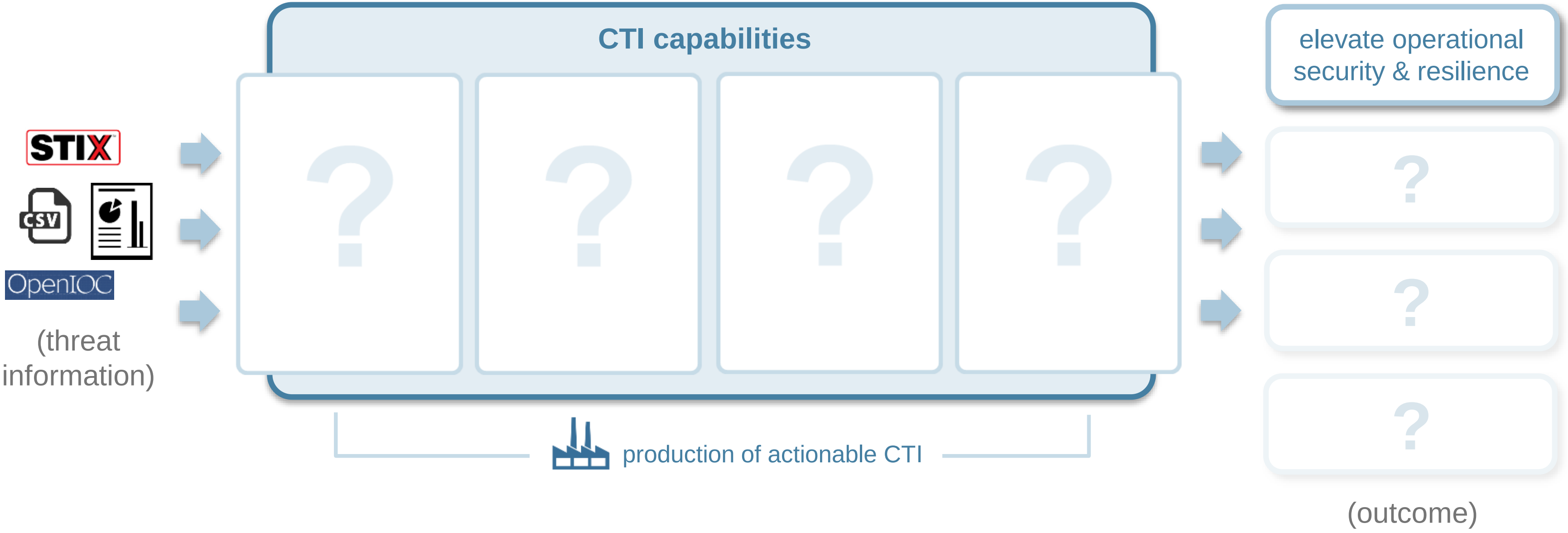
MITRE’s SOC Capabilities

MITRE
Ten Strategies of a World-Class
Cybersecurity Operations Center
Carson Zimmerman

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



(threat information)

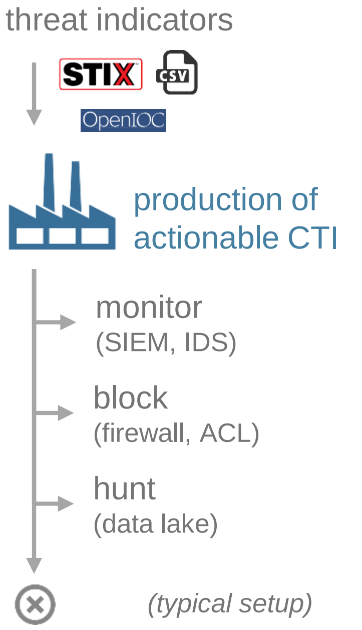
CTI capabilities

production of actionable CTI

elevate operational security & resilience

(outcome)

ELEVATE OPERATIONAL SECURITY



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)

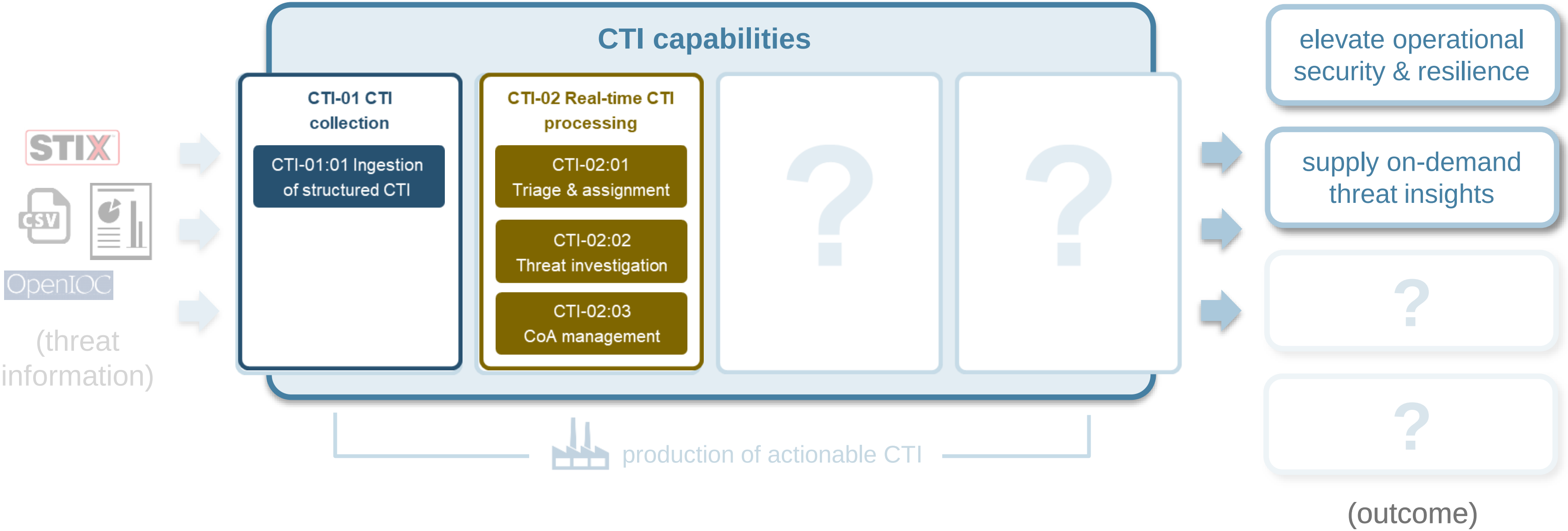
CTI-02:02 Threat investigation

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

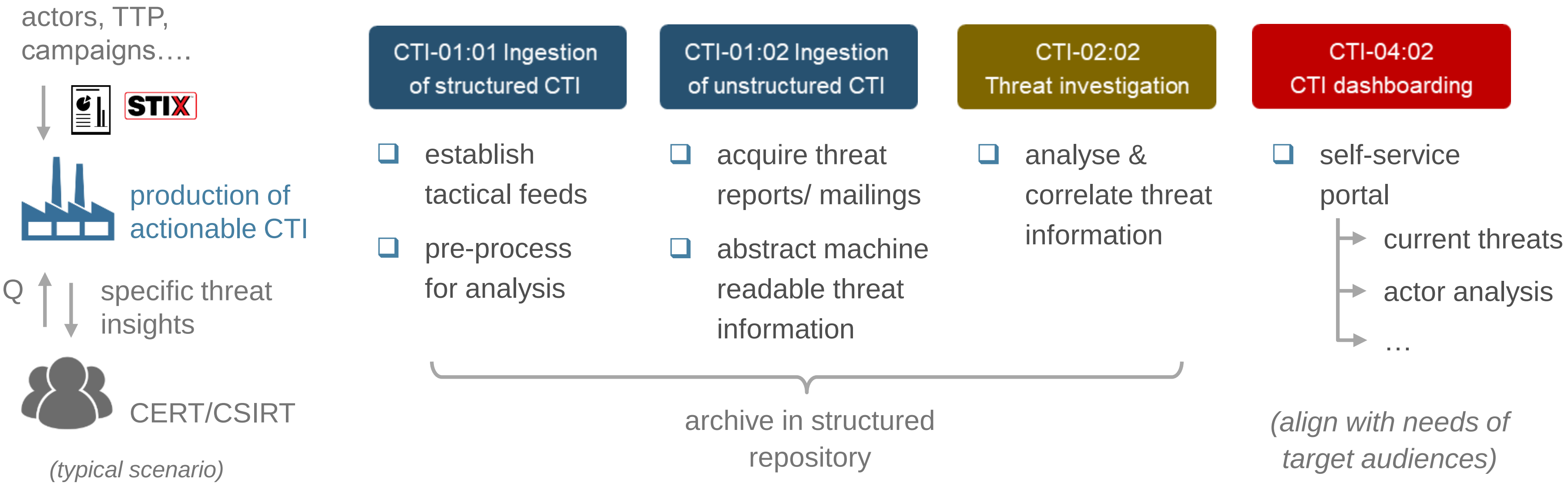
CTI-02:03 CoA management

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

COMPILING THE FRAMEWORK


STIX
CSV
OpenIOC
(threat information)
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
?
?
production of actionable CTI
elevate operational security & resilience
supply on-demand threat insights
?
?
(outcome)

SUPPLY ON-DEMAND THREAT INSIGHTS



actors, TTP, campaigns….

STIX

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

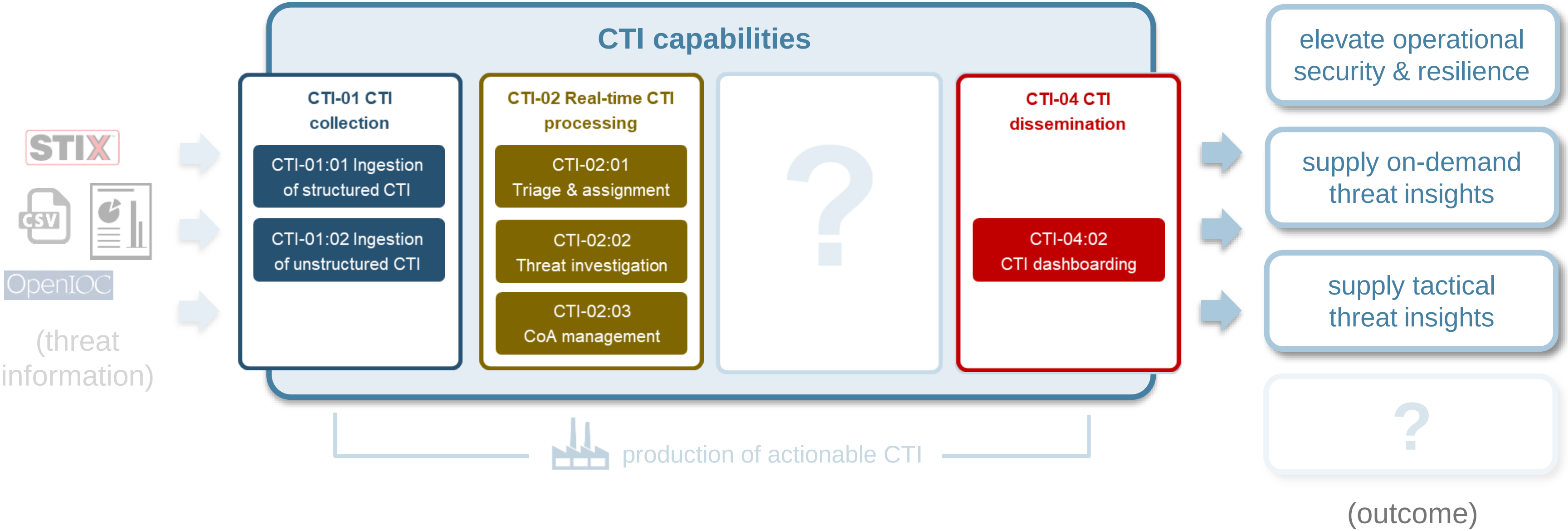
archive in structured repository

CTI-04:02 CTI dashboarding

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

(align with needs of target audiences)

EXPANDING THE FRAMEWORK



STIX
CSV
OpenIOC
(threat information)
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
production of actionable CTI
elevate operational security & resilience
supply on-demand threat insights
supply tactical threat insights
?
(outcome)

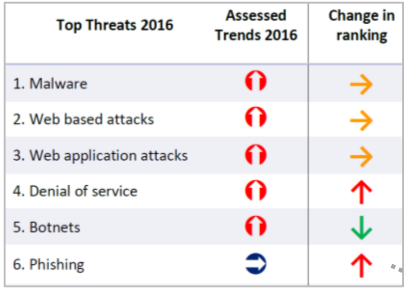
SUPPLY TACTICAL THREAT INSIGHTS

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

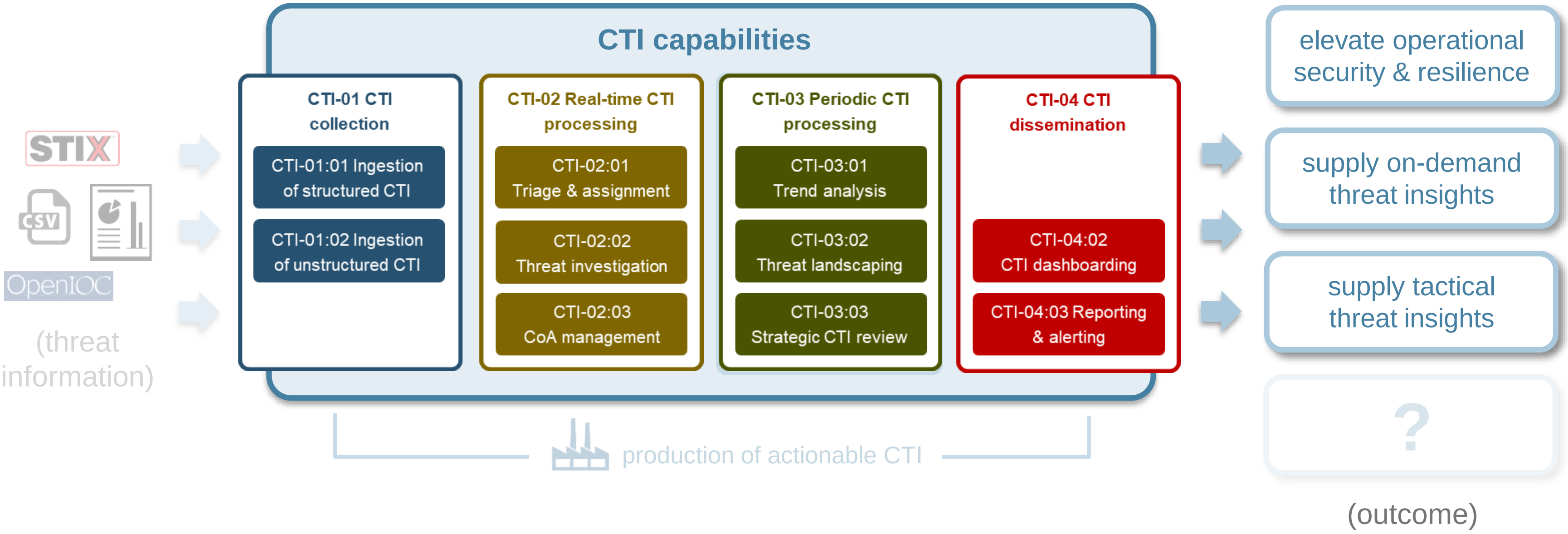
CTI-03:03 Strategic CTI review

- ❑ 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

EXPANDING SOME MORE



STIX

CSV

OpenIOC

(threat information)

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

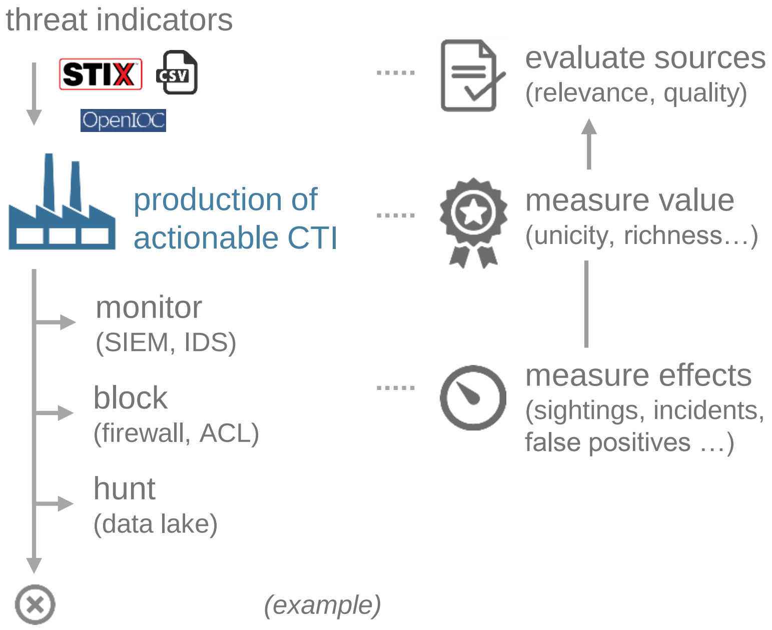
supply on-demand threat insights

supply tactical threat insights

?

(outcome)

EVALUATE & IMPROVE THE SETUP



threat indicators

production of actionable CTI

monitor
(SIEM, IDS)

block
(firewall, ACL)

hunt
(data lake)

(example)

evaluate sources
(relevance, quality)

measure value
(unicity, richness…)

measure effects
(sightings, incidents, false positives …)

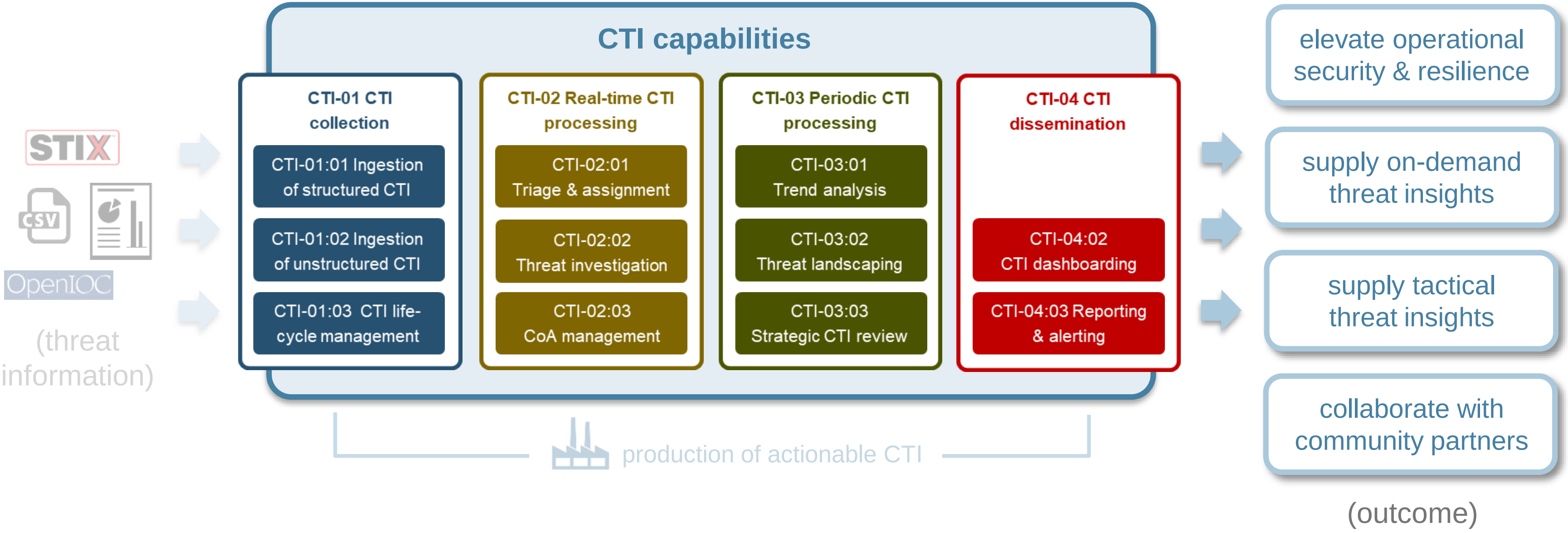
CTI-01:03 CTI life-cycle management

- ❑ acquire source performance data
- ❑ evaluate threat information sources

discontinue/replace?

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

ALMOST THERE



STIX

CSV

OpenIOC

(threat information)

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

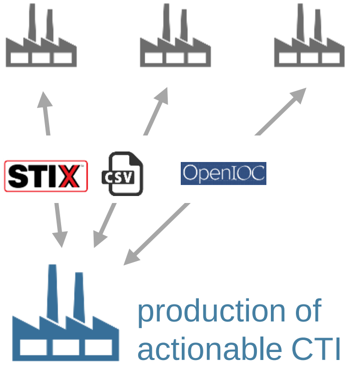
supply on-demand threat insights

supply tactical threat insights

collaborate with community partners

(outcome)

COLLABORATE WITH COMMUNITY PARTNERS



production of actionable CTI

CTI-04:01
External CTI sharing

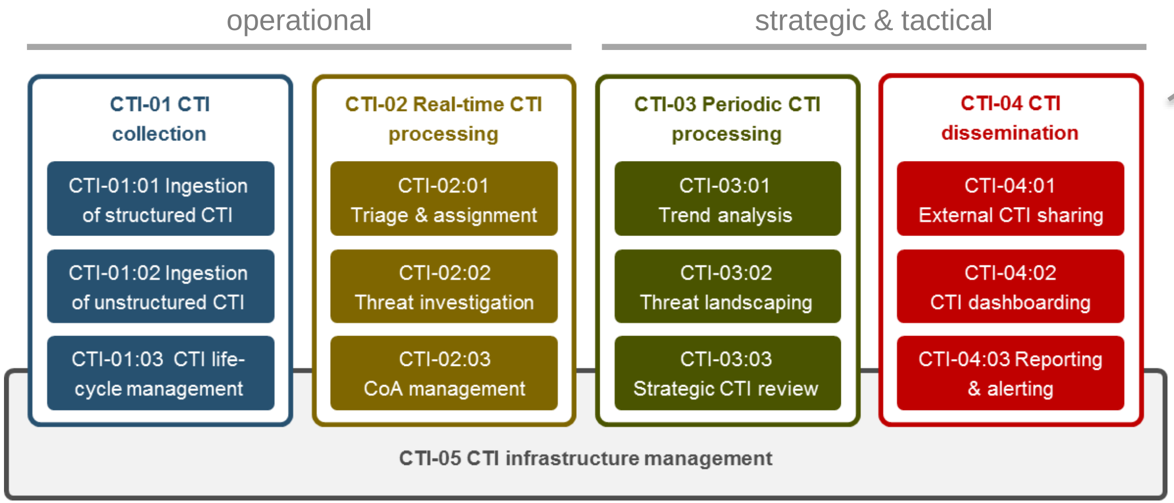
- ❑ prepare threat info for community partners
  - unique
  - vetted
  - cleared
- ❑ distribute via designated channels

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



operational

strategic & tactical

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

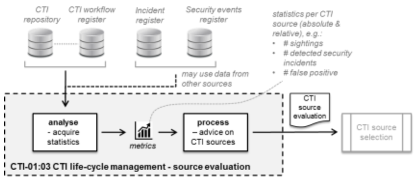
CTI-03 Periodic CTI processing

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

CTI-04 CTI dissemination

- CTI-04:01 External CTI sharing
- CTI-04:02 CTI dashboarding
- CTI-04:03 Reporting & alerting

CTI-05 CTI infrastructure management



CTI repository
CTI workflow register
Incident register
Security events register
statistics per CTI source (absolute & relative), e.g.:
• # sightings
• # detected security incidents
• # false positive
may use data from other sources
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)

- For each, model addresses
  a. definition & purpose
  b. core operations/ workflow
  c. automation potential
- 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

Innovating in Cyber Security

Shared research 2017

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