PVIB RONDETAFEL: MEETBAAR VEILIG MET SECURITY METRICS

HET MEETBAAR MAKEN VAN SECURITY

REINDER WOLTHUIS

INHOUD

MEETBAAR VEILIG MET SECURITY METRICS

Sorry voor de mix tussen Engels en Nederlandse slides

TNO innovation for life

INTRODUCTIE
WIE BEN IK

- Electrotechnical Engineering at University of Twente
- Previously KPN and ATOS. Joined **TNO** in 2006. PvIB member.
- >30 year working experience, of which about 25 in **innovation of information security/cybersecurity**
- Balancing between cyber security **project/program management and consultancy**
- Main current activities:
  - Initiator and program manager of the **Partnership for Cyber Security Innovation** (as of July 1st 2020) and its predecessor the Shared Research Program Cyber Security (2014-2020)
  - Coordinator of the **EU H2020 project SOCCRATES** (*SOC & CSIRT Response to Attacks & Threats based on attack defense graphs Evaluation Systems, 2019-2022*)
  - Conducting an annual **European telecom security benchmark** (around 25 participants a.o. Deutsche Telekom, British Telecom, Orange, Telefonica, KPN, Proximus)

INTRODUCTIE
OVER TNO

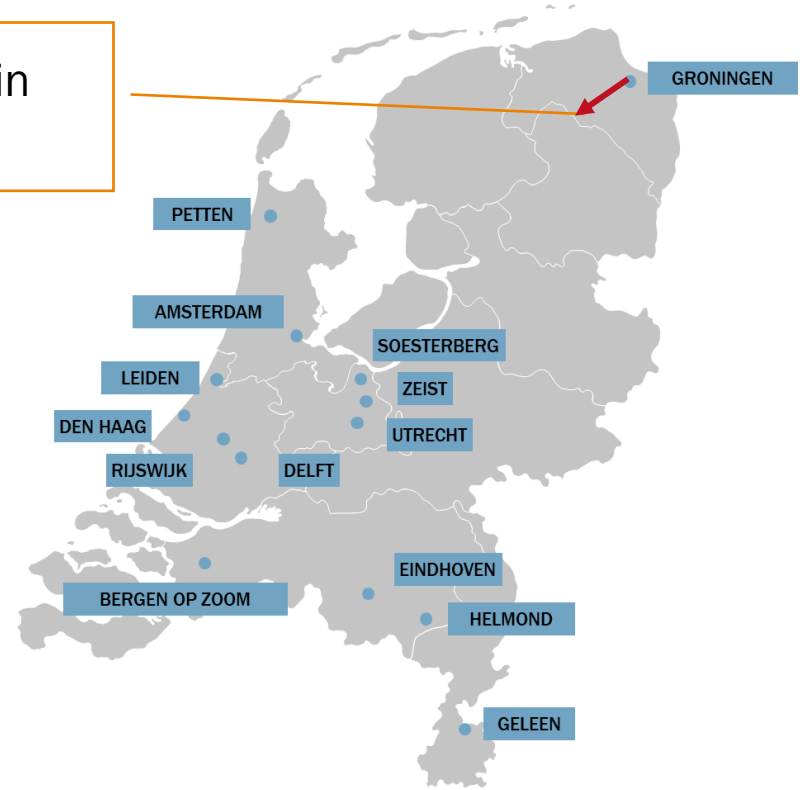
- TNO, the Netherlands Organisation for applied scientific research, was founded by law in 1932 to enable business and government to apply knowledge.
- As an organisation regulated by public law, we are **independent**: not part of any government, university or company. We are **not-for-profit**.
- Some numbers:
  - Around 3400 employees (2900 fte), 30+ nationalities
  - Annual turnover 482 million euro, of which 193 coming from Dutch government
  - 58 part-time professors

Applied research, bridging the gap between the scientific world and the business world

INTRODUCTIE
OVER TNO

- Multi disciplinary approach.
- Cyber security relevant expertise:
  - Technical (IT) security and Cryptology
  - Cooperation between organisations
  - Human Factor in security (usability, awareness, behaviour)
  - Data analytics, Machine learning, AI

TNO Office in Groningen



INTRODUCTIE
WAAR HEBBEN WE HET OVER

- Cyber security/cyber resilience metrics, niet (business) continuïteit
- Vanuit toegepast onderzoek perspectief, niet vanuit operationeel perspectief
- Doel is het delen van metrics-ervaringen vanuit verschillende invalshoeken en daarna over metrics discussiëren

- De presentatie is samengesteld uit slidesets van verschillende projecten. Dank aan mijn TNO collega's en vooral aan Richard Kerkdijk voor het beschikbaar stellen van de slides.

METRICS: THE HOLY GRAIL

HET DASHBOARD DAT OVERAL EEN ANTWOORD OP GEEFT

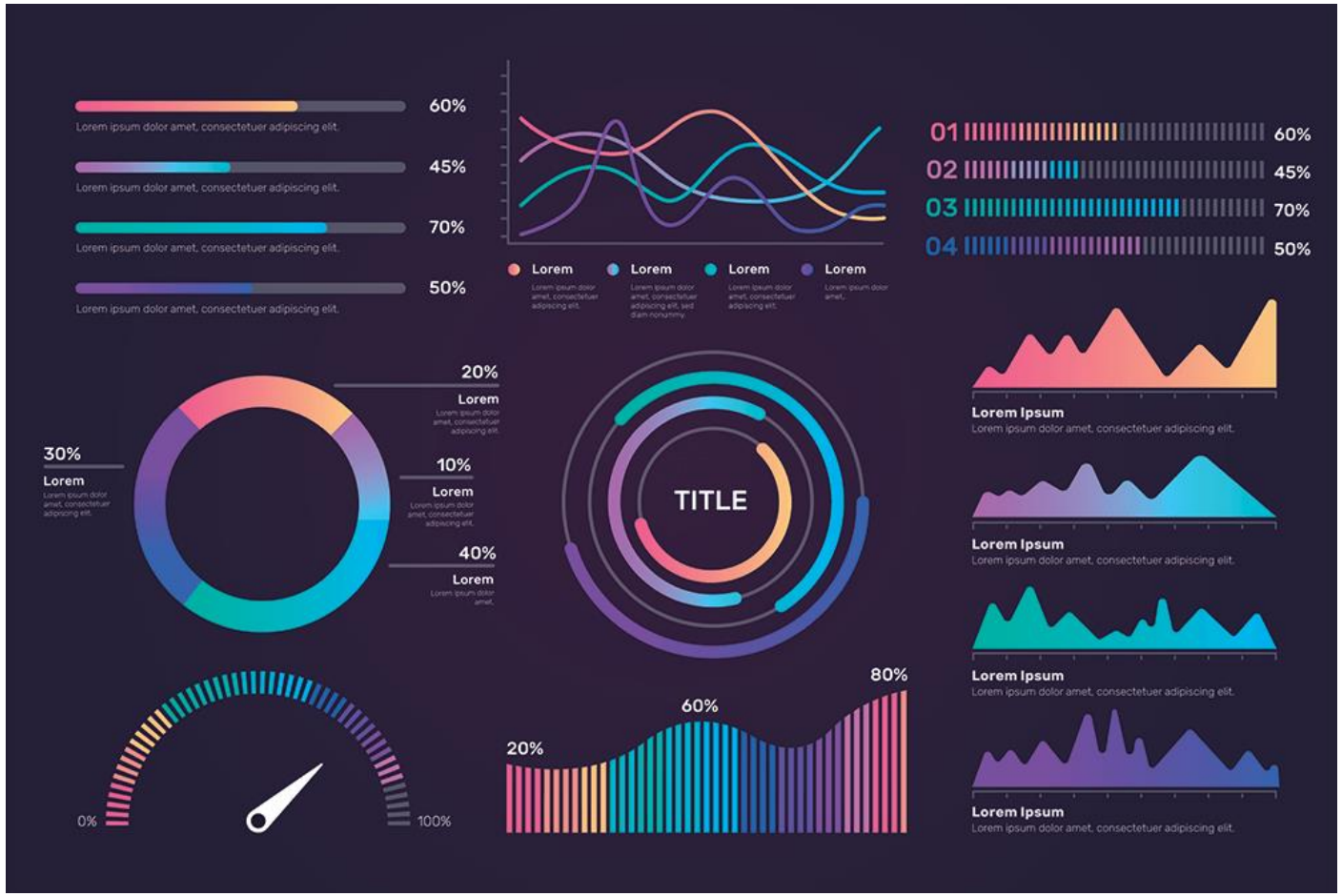
Hoe veilig ben ik?

Waar moet ik investeren?

Hoe veilig is de cloud?

Hoe veilig zijn de resultaten van mijn projecten?

Wat zijn mijn grootste risico's?



Hoe compliant ben ik aan mijn beleid?

Hoe security-Aware zijn mijn medewerkers?

Hoe doe ik het t.o.v. mijn concullega's?

Hoe veilig zijn de producten en diensten die ik inkoop?

Hoe veilig zijn mijn leveranciers?

HELAAS....
DE HOLY GRAIL BESTAAT (NOG) NIET

Zoveel doelen, zoveel verschillende metrics

METRICS

- If you cannot measure it, you cannot improve it.

  - *Lord Kelvin*

NIST:

- *measuring cybersecurity remains an under-developed topic – one in which there is not even a standard taxonomy for terms such as "measurements" and "metrics."*
- *…measuring the system's overall ability to* ***identify, protect, detect, respond, and recover*** *from cybersecurity risks and threats should be the real aim of a robust cybersecurity measurement program.*
- *NIST Special Publication (SP) 800-55 Revision 1 (rev2), Performance Measurement Guide for Information Security*

The IT Law wiki:

- **Security metrics** are metrics that indicate the degree to which security goals, such as data confidentiality, are being met.

METRICS
VERSCHILLENDE ASPECTEN

- Metrics = meten
  - Wat wil je meten (**doel**) = Bijv: Hoe compliant ben ik aan mijn security beleid?
  - Hoe meet je het (**meetmethode**)
  - Welke informatie is daarvoor nodig? (**data**)
  - Hoe ziet het meetresultaat er uit (**bijv. percentage van een norm**)
  - Voor wie is het meetresultaat? Bijvoorbeeld
    - **Beslissers**: RvB, budgethouders
    - **Gebruikers**: security professionals, operations, risk managers, compliancy afdelingen
    - **Projecten**: KPI's, zijn we secure by design
    - **Overheid**: regelgevers die willen weten of je aan wetgeving voldoet
    - ….

METRICS

VOORBEELDEN VAN METRICS IN VERSCHILLENDE SITUATIE

1. Benchmarking: hoe doe ik het t.o.v. van anderen
2. Compliance: hoe doe ik het tov (mijn eigen) normen
3. Cyber resilience metrics: Hoe goed ben ik resilient tegen cyber aanvallen
4. Supply chain: hoe veilig zijn de partijen waar ik van afhankelijk ben?
5. Dreiginglandschap: hoe weet ik welke dreigingen voor mij het meest relevant zijn
6. Innovatie-effectiviteit: hoe bepaal ik of security innovatie mij veiliger maakt

TOEPASSINGSVOORBEELDEN

BENCHMARKING: HOE DOE IK HET TOV VAN ANDEREN

- Project: Telco security bechmark, recurring consultancy project among European Telecom providers

TELCO SECURITY BENCHMARK

objective: compare security strategies and approaches among a representative group of European telcos, thereby enabling them to determine which specific aspects of security require attention within their respective organisations.

- Operated under the umbrella of ETIS – a European industry forum for telco collaboration
- Focused on telco industry with active peer interaction among the participants
- 23 participating telcos since 2009, many recurrent (e.g. bi-yearly) to monitor development over time.

FOCUS ON 6 DISTINCT THEMES

1. Corporate security function

2. Security Management

3. Commercial role of security

4. Security in development

5. Network & system security

6. Monitoring & response

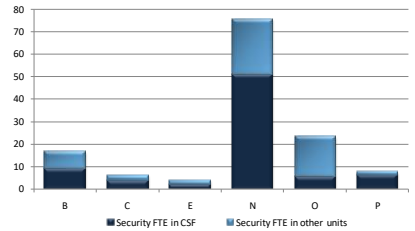
- Information gathered through
  - face to face interviews with specialists for respective themes (primary)
  - written survey among system administrators (secondary - complements theme 5 interview)
- All interviews conducted on-site at participant premises on one single day

OUTCOME AND DISSEMINATION

Performance qualification

- Telco performance rating for each security theme
  Weak-Basic-Mature-Excellent
- Provides explicit insight into present position
  Direct depiction of areas that require attention

Specific characteristics



- Comparison of actual strategies/ approaches
  Highlights selected topics
- Interesting aspects that cannot be reflected in performance score
  e.g. FTEs, specific practices

Successful practices

- Approaches proven successful at specific participants
  Might be adopted by others
- Well received in previous benchmarks – enhances value and usability

- Joint workshop to enrich results
- Outcome documented in anonymized report

- Interesting to see that this result is used for various reasons:
  - Show money was well invested
  - Ask for more budget
  - ….

TOEPASSINGSVOORBEELDEN

COMPLIANCE: HOE DOE IK HET TOV (MIJN EIGEN) NORMEN

(questions from ETIS security benchmark)

Compliance against security policy

- How do you monitor compliance with non-technical security procedures prescribed by your corporate security policy?
  - Self assessment reports
  - Audits
  - Data collected from processes or systems to assess compliance

- Learnings:
  - Remarkably few organisations actually collect data from processes and systems
  - Manual collecting information through reports and conducting audits is main way of working

TOEPASSINGSVOORBEELDEN

COMPLIANCE: HOE DOE IK HET TOV (MIJN EIGEN) NORMEN

(questions from ETIS security benchmark)

- How do you monitor compliance of your technical (IT and telco) infrastructure with the corporate security policy?
  - E.g. System hardening, Security patching, Accounts and privileges, User authentication
  - Coverage of technical compliance monitoring
  - Security testing with the purpose to assess policy compliance in your technical infrastructures

- Learnings:
  - Very few organisations use results from vulnerability scans to measure compliance
  - Most organisations do security testing, but results mostly not fed back into compliance monitoring

TOEPASSINGSVOORBEELDEN
CYBER RESILIENCE METRICS

- Project: Cyber resilience metrics, project in the Shared Research Program Cyber Security

POINT OF DEPARTURE

- Cyber resilience metrics should reflect readiness for sophisticated and targeted cyber attacks (APTs) above anything else
- The metrics should reveal effects achieved rather than the presence and implementation status of security controls
- The metrics should appeal to actual information needs of security coordinators (not solely on easy accessibility)
- Cyber resilience metrics do not have to be simple. A certain complexity is not objectionable (in fact seen as natural considering subject complexity)

Industry wide harmonisation of metrics and corresponding norms would be greatly welcomed but is positioned as a long term ambition

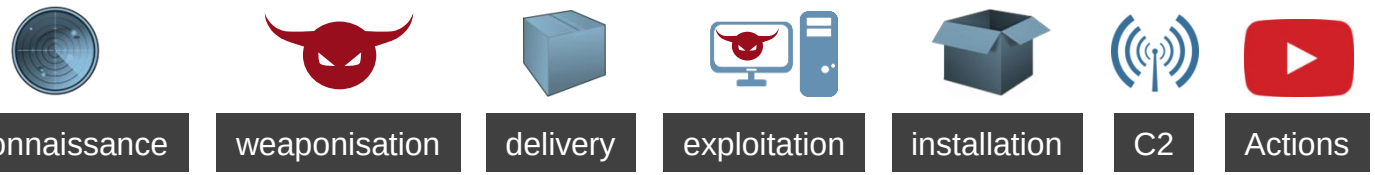
DEMARCATION OF “CYBER RESILIENCE”

- Since the concept of “cyber resilience” proved somewhat ambiguous (a.o. confusion with indicators for incident monitoring), a principal demarcation was agreed with the participants.

*Cyber resilience is the **ability** of an ecosystem (e.g. an organization, infrastructure, system) to*

- *…**prepare** for and **adapt** to changing conditions*
- *…**withstand deliberate attacks** on technical infrastructure that are (at least in part) conducted from cyberspace*
- *…rapidly **recover** from the negative effects of such attacks*
- *…**limit the damage** on business, people and society*

BUILDING A MEANINGFUL MODEL



Physical environment

Employee behaviour

Technical infrastructure

Customer behaviour

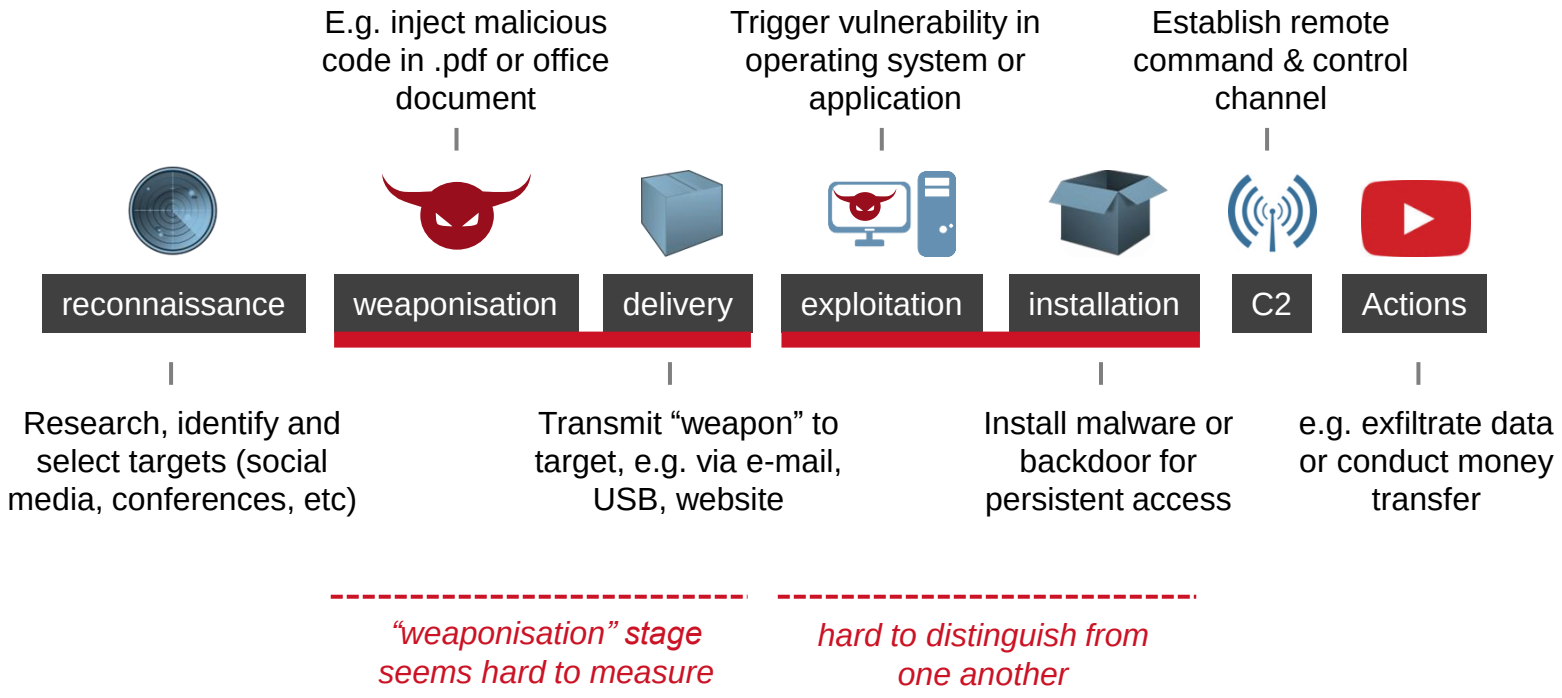
⋮

Resilience metrics will be most meaningful if they are differentiated by attack stages. Lockheed Martin's cyber kill chain is an acknowledged model to this end

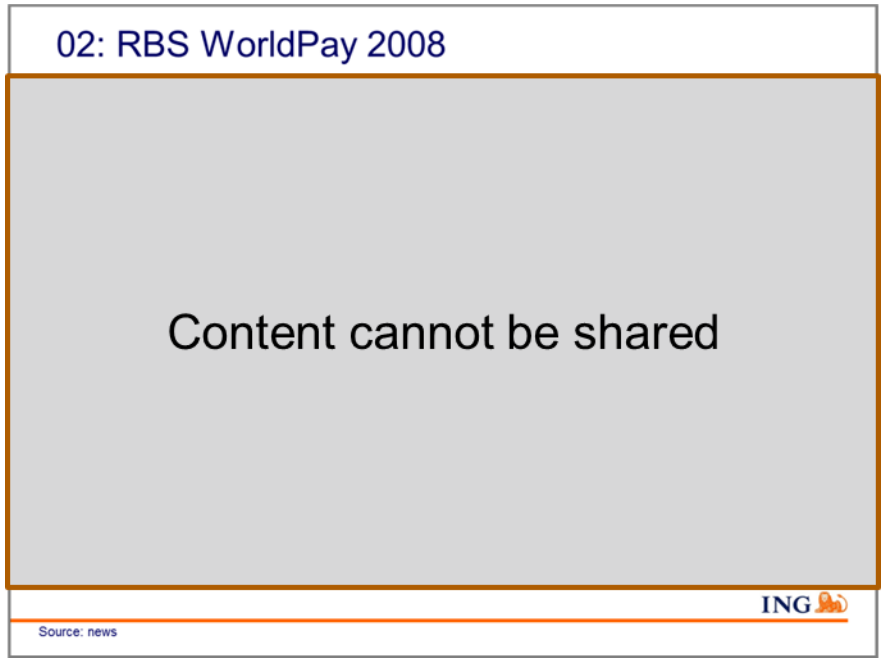
Further differentiation by attack surface enhances understanding of exact strengths and weaknesses

A CLOSER LOOK AT THE KILL CHAIN

- For the purpose that we are pursuing, it makes most sense to **merge specific stages** of the kill chain into one category of metrics

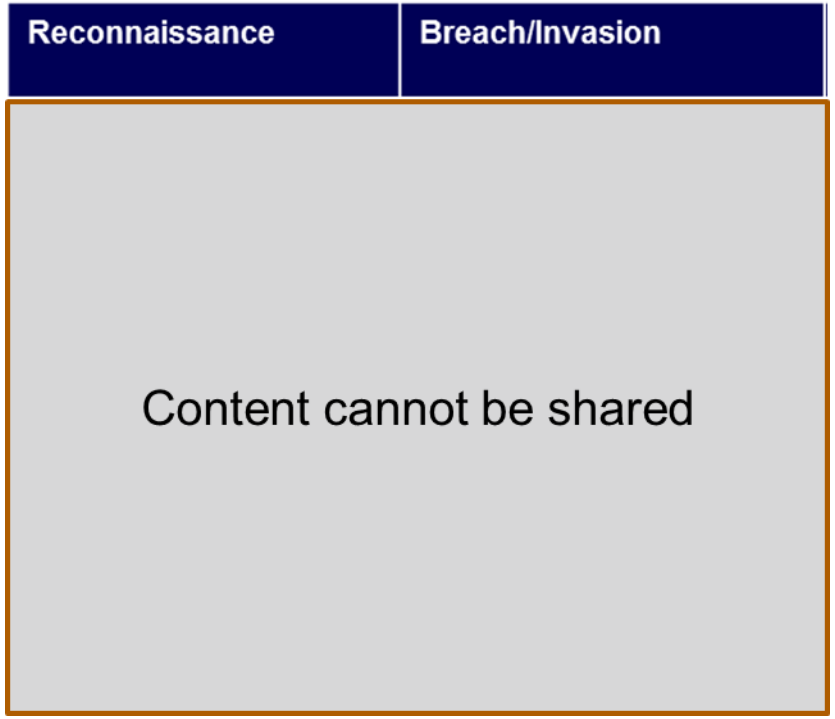


DEFINING THE ACTUAL METRICS



- Actual resilience metrics will be deduced from use cases with demonstrable relevance for the financial industry
- ING CSIRT kindly supplied 24 APT use cases that can be employed to this end (albeit with deviating attack stage distinction)

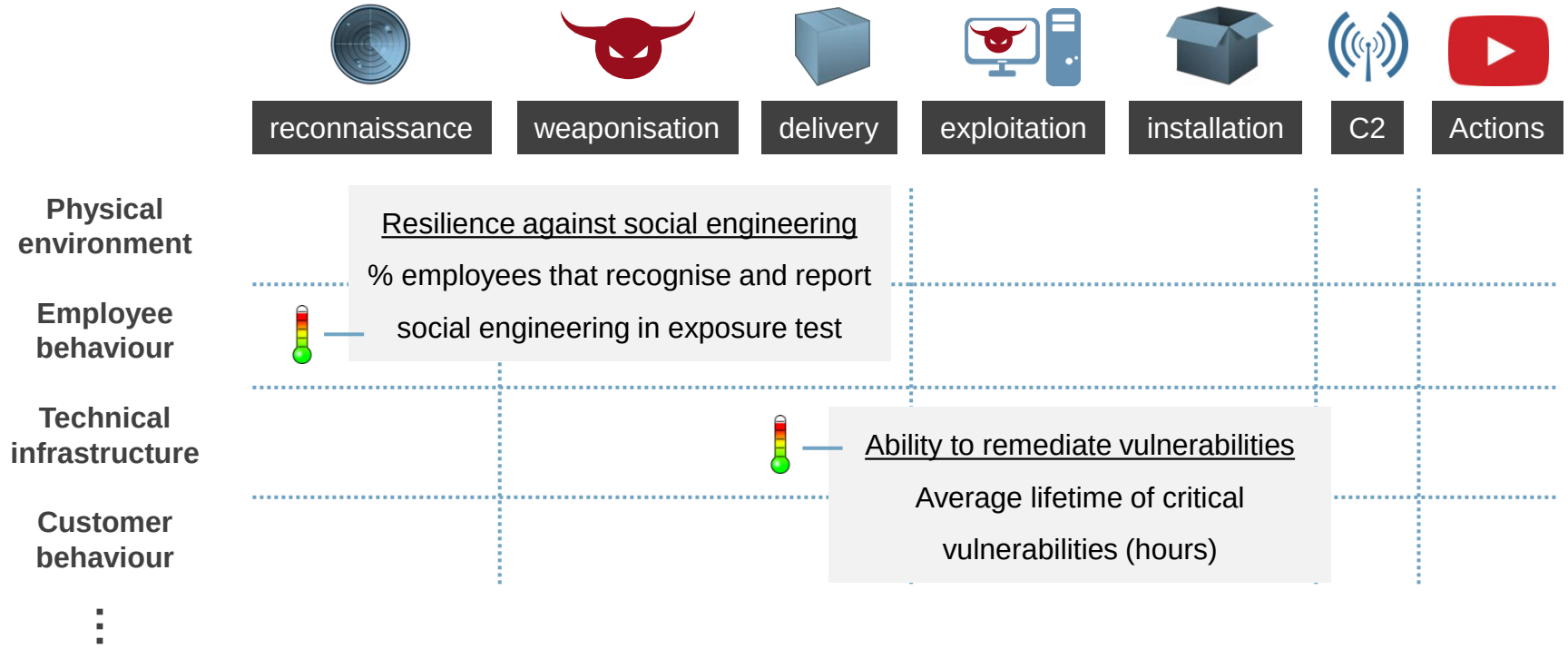
EXAMPLE OF UNFOLDING APT SCENARIO (1/4)



- Hard to make out what the attackers actually did in these stages…
- …but we can speculate that
  - social engineering was at least tried
  - a software vulnerability was exploited
  - credentials were stolen and abused *(e.g. of a call center operator)*

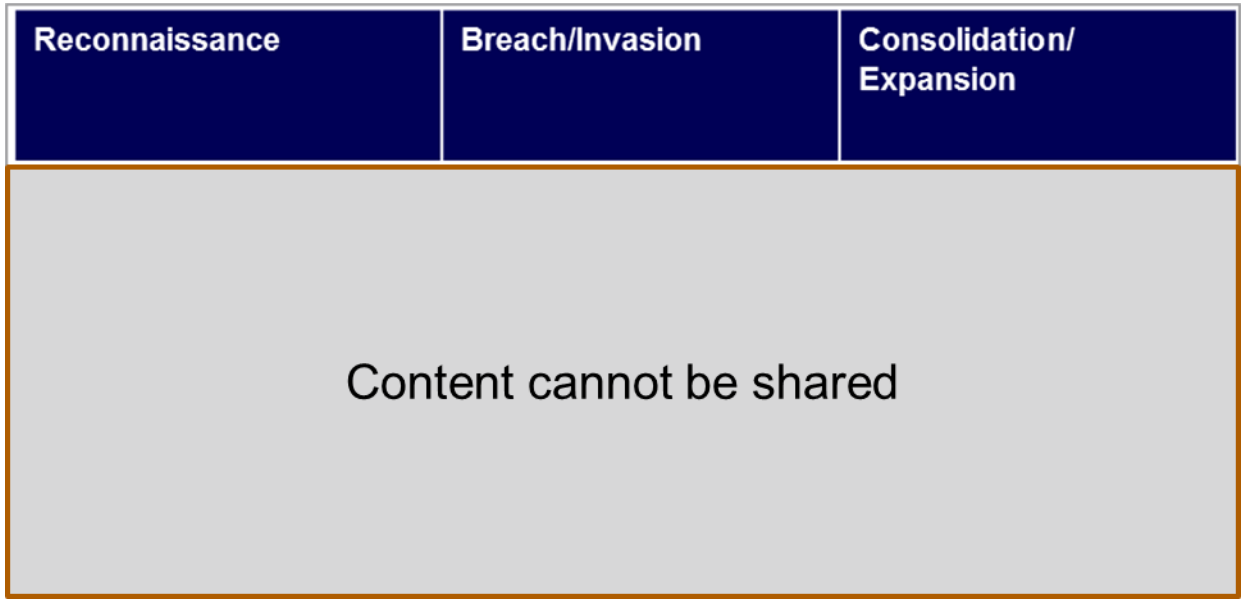
… thus it seems worthwhile to seek metrics that reveal resilience with respect to the above attack vectors

EXAMPLE OF UNFOLDING APT SCENARIO (2/4)

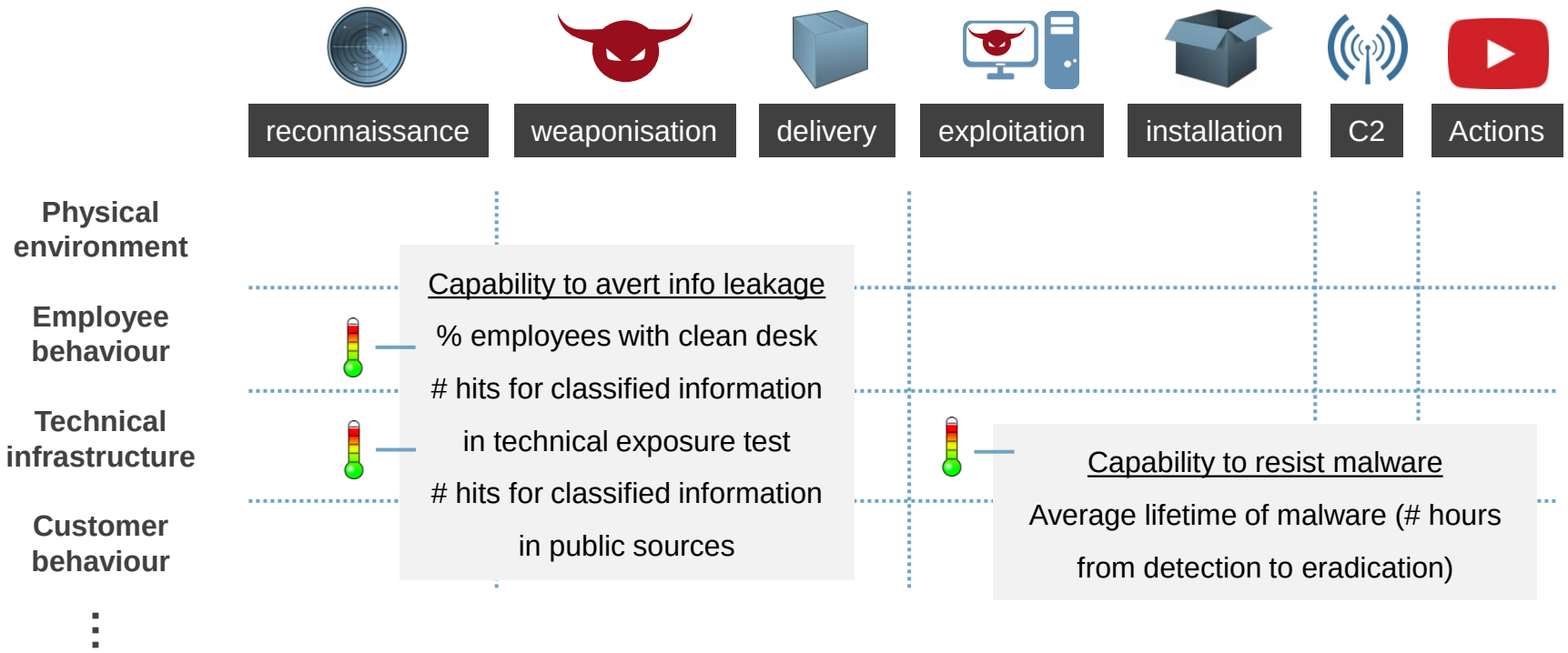


(samples – not exhaustive)

EXAMPLE OF UNFOLDING APT SCENARIO(3/4)

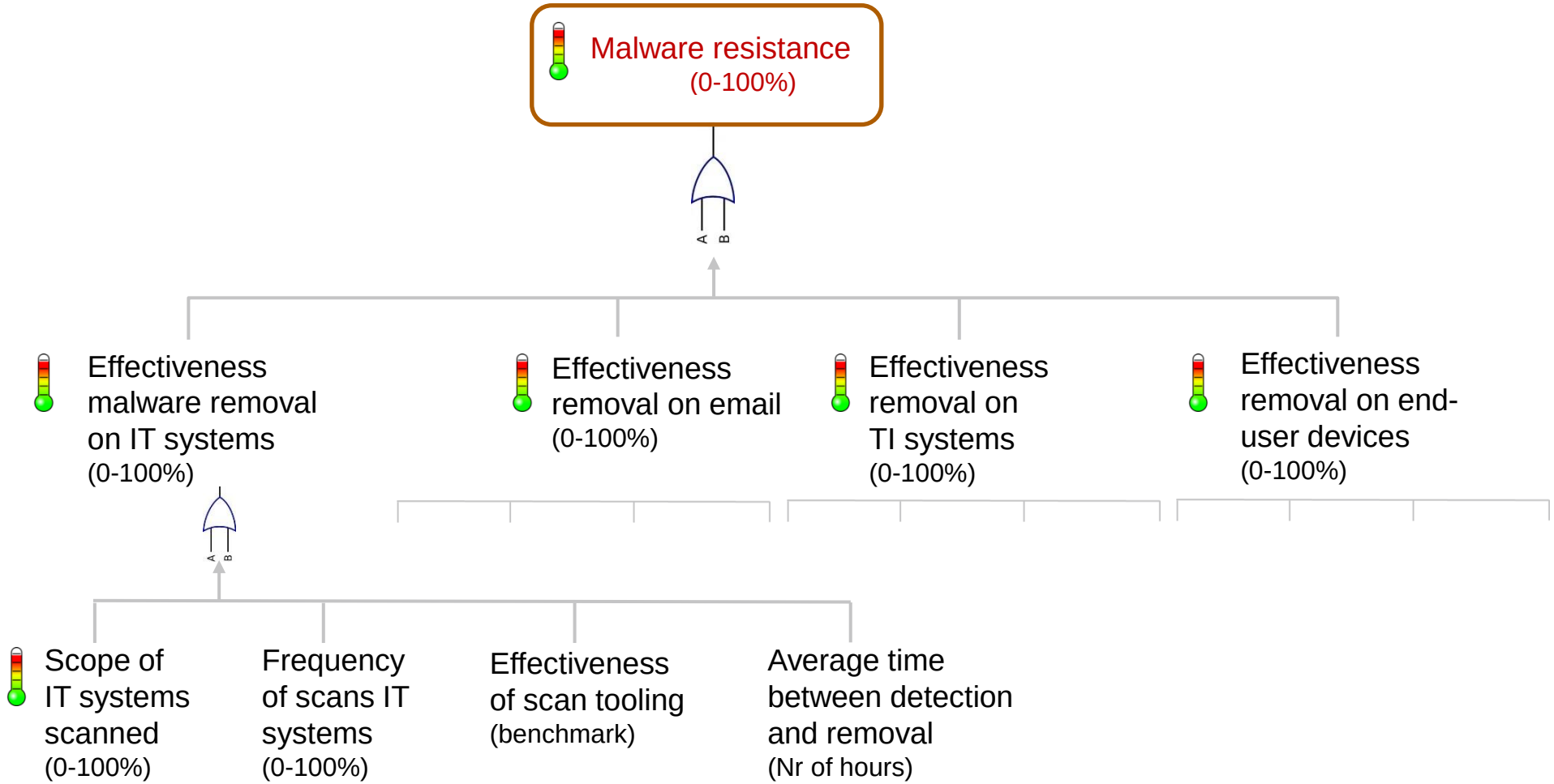


EXAMPLE OF UNFOLDING APT SCENARIO(4/4)



(samples – not exhaustive)

LAYERED STRUCTURE OF METRICS



RESULT

Library of cyber resilience metrics

- Harmonised categories of metrics (“ability to…”)
- Suggestions for metrics and measurement methods (“implementation guidance”)

Available at https://www.tno.nl/srpcybersecurity

CONCLUSION

- As expected, developing relevant cyber resilience metrics is not an easy task
- After some initial struggle we think we are heading in the right direction
  - Focus on APT
  - Apply kill chain model
  - Learn from APT use cases
- The project delivered a useful and innovative library of cyber resilience metrics

- Learnings:
  - We conducted a pilot at one of the program partners (a large bank)
  - Conclusion: the metrics were found to be very useful, but the data needed to actually use the metrics was not available / scattered all over the organisation / not in the right format / etc.

TOEPASSINGSVOORBEELDEN

SUPPLY CHAIN: HOE VEILIG ZIJN DE PARTIJEN WAAR IK VAN AFHANKELIJK BEN?

- Project: Metrics2Trust, project in the Partnership for Cyber Security Innovation

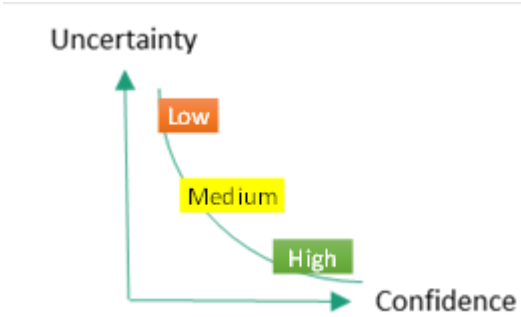
Metrics2Trust

Trend 9: Growing dependency on third parties

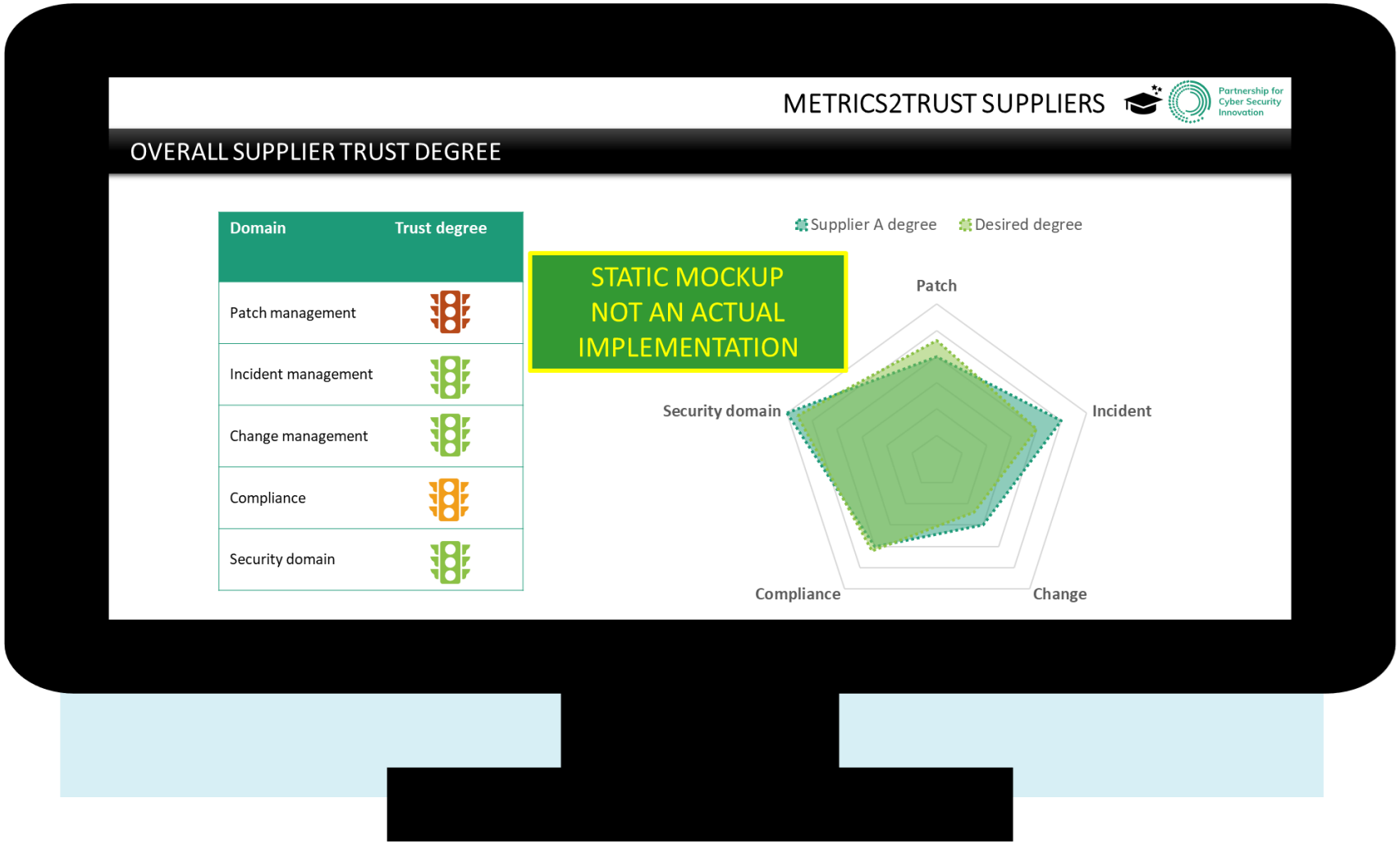
Organizations are working together with and utilize products from software vendors and equipment vendors. We also see an increase in outsourcing of IT to, e.g., cloud-based services. This causes an increase in dependency on third parties. Vendor lock-in is one of the possible consequences. Furthermore the overall security of an organization becomes dependent on the quality of security in the products and services of third parties.

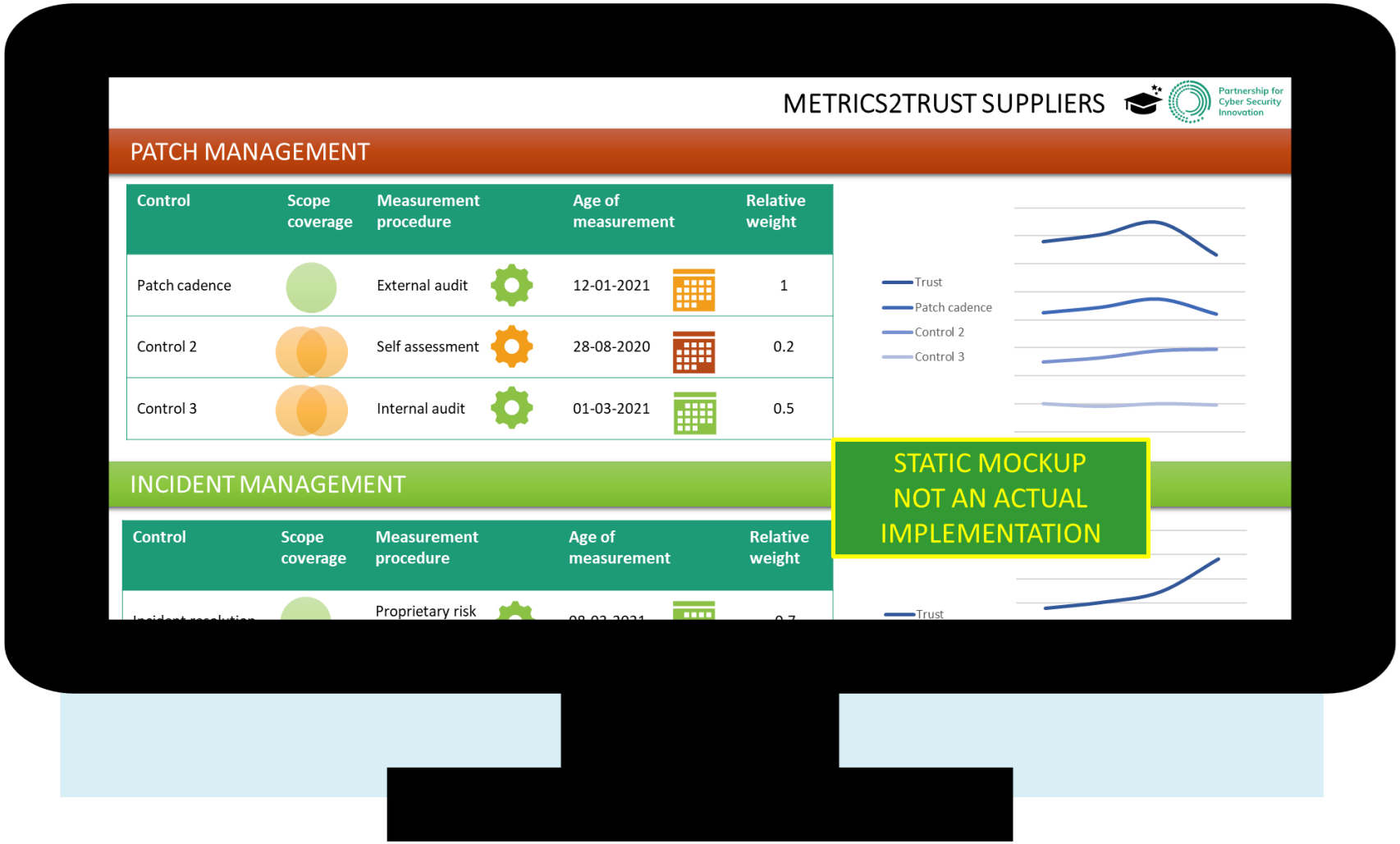
The starting point

- Organisations more and more rely on suppliers and third parties for products and services
- Growing complexity of third-party chain ecosystems
- Need for continuous supplier security trust
- Many metrics available for supplier risk profiles



Need to reuse available metrics to create generic and user-specific modules to identify changes of confidence in trust to do transposition of risk by building a trust model in an interactive dashboard


METRICS2TRUST SUPPLIERS
Partnership for Cyber Security Innovation
OVERALL SUPPLIER TRUST DEGREE
Domain
Trust degree
Patch management
Incident management
Change management
Compliance
Security domain
STATIC MOCKUP
NOT AN ACTUAL
IMPLEMENTATION
Supplier A degree
Desired degree
Patch
Incident
Change
Compliance
Security domain


METRICS2TRUST SUPPLIERS
Partnership for Cyber Security Innovation
PATCH MANAGEMENT
Control
Scope coverage
Measurement procedure
Age of measurement
Relative weight
Patch cadence
External audit
12-01-2021
1
Control 2
Self assessment
28-08-2020
0.2
Control 3
Internal audit
01-03-2021
0.5
Trust
Patch cadence
Control 2
Control 3
INCIDENT MANAGEMENT
Control
Scope coverage
Measurement procedure
Age of measurement
Relative weight
Proprietary risk
Trust
STATIC MOCKUP
NOT AN ACTUAL
IMPLEMENTATION

Data

- Many different sources
  - Differences in maturity level, depth of detail, structure, standard, …

System and Organization Controls (SOC) 2 Report

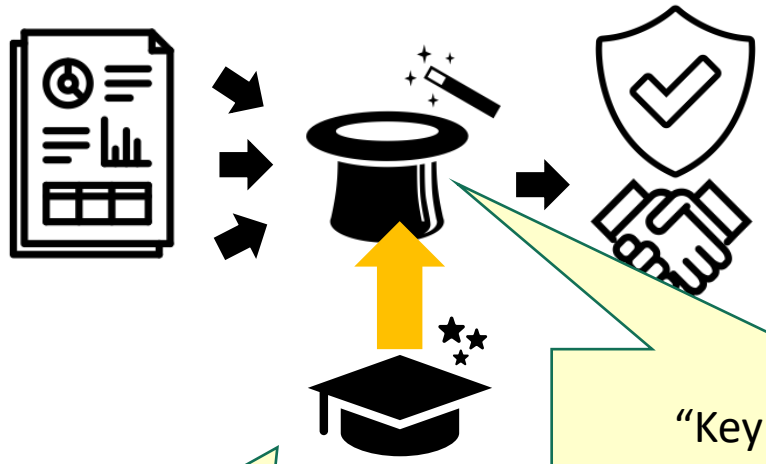
BITSIGHT® The Standard in SECURITY RATINGS

Service Level Report

Key finding, result and outcome

- Open Source Intelligence (OSINT)
- Security ratings
- Internal security solutions
- Information sharing mechanisms
- Supplier security self-assessments
- Security certifications
- On-site security assessments/audits

"Key finding: There are numerous metrics based on an abundance of features. Both from inside and outside sources"



"Key result: model "*demystifies*" the measuring and processing of metrics, increasing re-usability enabling automation" by an interactive dashboard that combines existing measures

"Key outcome: added value of model into day to day activities"

Key learnings

- Maturity of data sources
  - Require substantial manual labour to abstract useful data from available sources
  - Combining insight from different documents is mainly a manual process
  - Missing level of detail to obtain useful insights
  - Limited access to ‘dynamic’ data sources, large portion is ‘static’

- Proof of Concept Assessment:
  - Concept is still valid, turning it into a usable tool is very hard
  - Requires substantial manual preprocessing in order to construct a dashboard
  - Assumption that “Data is available and can be shared” ≠ reality
  - Value lies in structurization and standardization

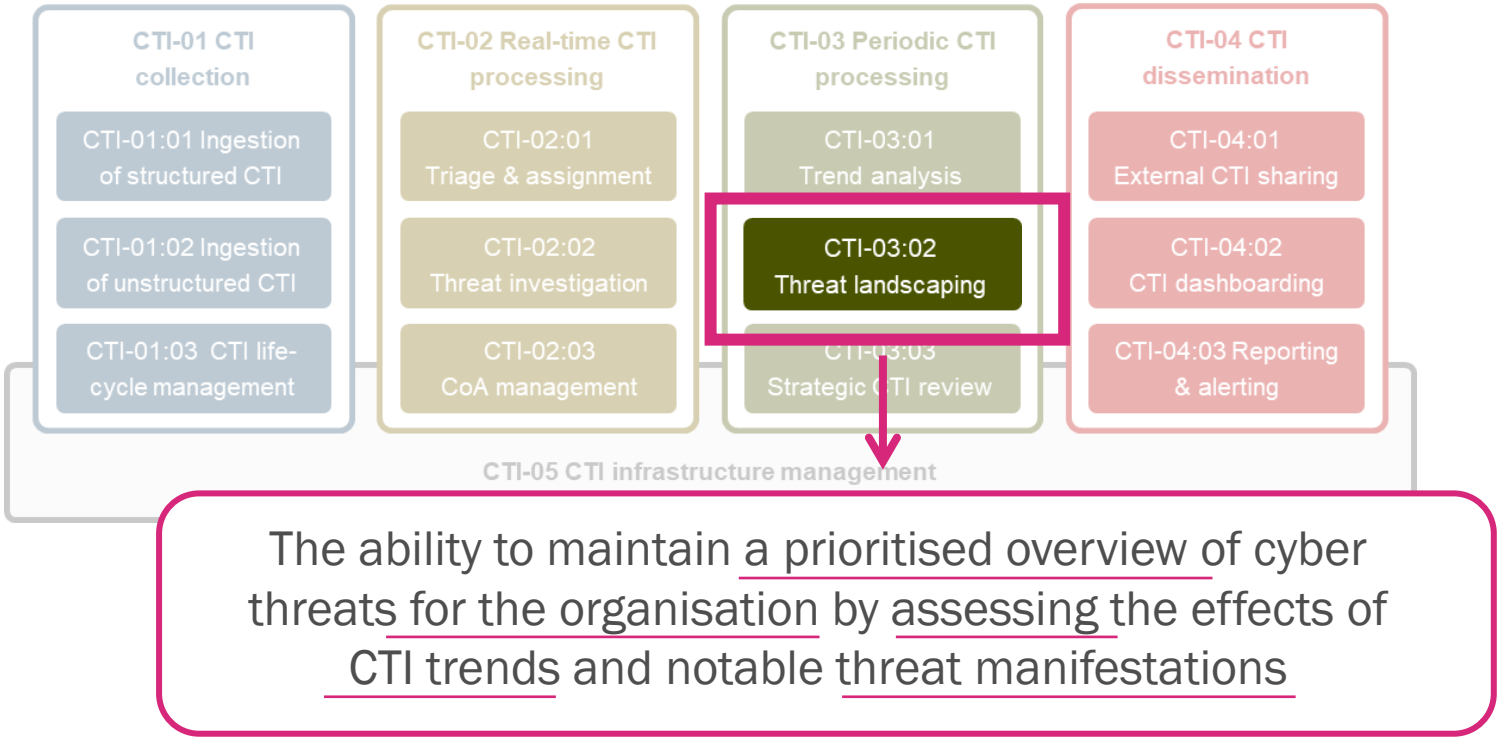
TOEPASSINGSVOORBEELDEN

DREIGINGLANDSCHAP: HOE WEET IK WELKE HET MEEST RELEVANT ZIJN

- Project: Threat Landscaping, project in the Shared Research Program Cyber Security

SO WHAT IS THREAT LANDSCAPING?

[CTI capability framework developed by TNO & Dutch financials]



The ability to maintain a prioritised overview of cyber threats for the organisation by assessing the effects of CTI trends and notable threat manifestations

CISOs, security architects, product owners, risk managers, fraud teams...

Purpose of a TL

- Inform stakeholders about current and emerging threats
- Facilitate intelligence led priorities and decisions

INDIVIDUAL VS SECTORAL PERSPECTIVE

align & cross-reference – consistency, completeness

TL of individual organisation

- Great variety of business profiles

revenue portfolio regionality IT infra controls (...)

- Should evoke equally great variety in appreciation of threats and their respective priorities

Sectoral TL

- Show threats that affect (or have a strong presence across) the sector as a whole
- Reveal need/ potential for inter-bank collaborations on threat assessment or remediation.
- Feed smaller FIs that don't have capability to make their own

A LOOK AT EXISTING THREAT LANDSCAPES

[not exhaustive - illustrative examples]

ENISA TL

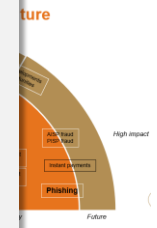
Top Threats 2017	Assessed Trends 2017	Top
1. Malware		1. Malware
2. Web Based Attacks		2. Web Base
3. Web Application Attacks		3. Web Appl
4. Phishing		4. Phishing
5. Spam		5. Denial of

- Includes indic
  ranking and t
- Inconsistent r
  motives, meth
- High level – n
  for individual organisation

TL for Industrial Automation

priority ranking

Financial threat landscape



v on threats
happening vs

ation on
s /impact, limited
scope

general picture

- Great variety in focus, nature and granularity
- Often too generalised to offer action perspective for individual organisation

TLs for finance sector

- Multiple TLs, each with specific perspective
  – technical, fraud, cyber, threat actors…
- Different interpretations of same threat

driven by opinions of experts rather than by measurable data

DESIRE: UNIFORM AND STAKEHOLDER CENTRIC

The TL needs a uniform and consistent format that feeds stakeholders with actionable threat insights and accommodates both individual and sectoral landscaping initiatives

- Design choice: populate top level TL with campaigns

`[campaign(s)] by [actor (type)]`

example: manipulation of financial assets *by* Carbanak group

example: IPR theft *by* Chinese APTx groups

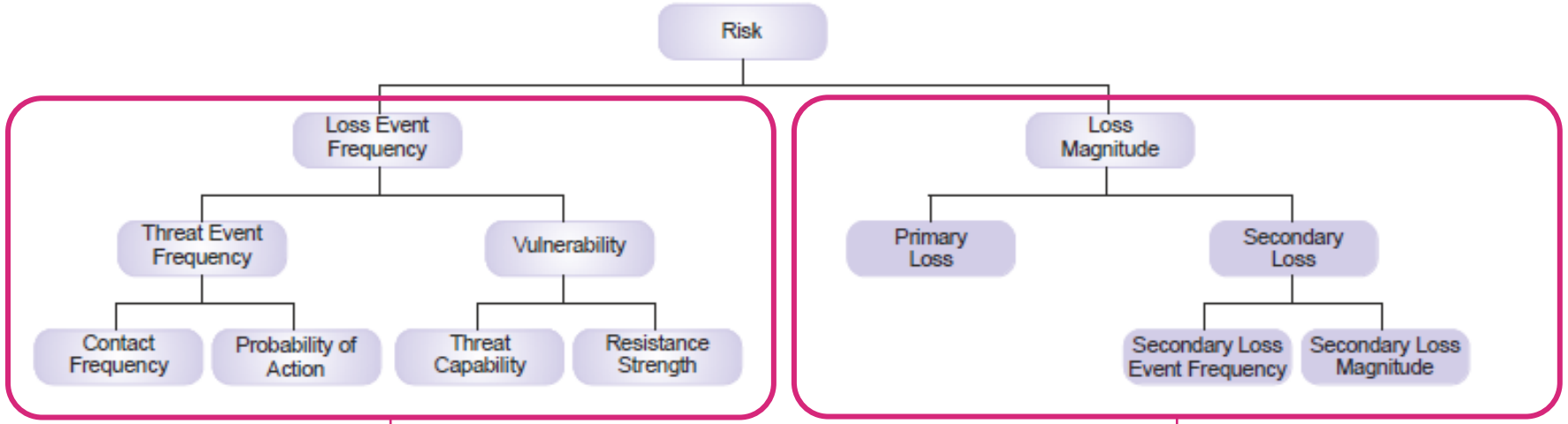
- Focus on attacker end game – underlying characteristics in separate views + used to determine relative severity

1-FTL-NL: complement with alternate formats where appropriate

e.g. emerging threats where actor is unknown or “non-cyber” threats such as “duty of care shift”

DESIRE: EVIDENCE BASED

The TL needs to be populated and prioritised on the basis of actual observations (evidence) rather than human opinions



FAIR risk taxonomy
https://www.fairinstitute.org/

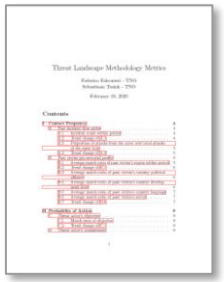
threat quantification – strength of threat + strength of controls

translate to context of TL

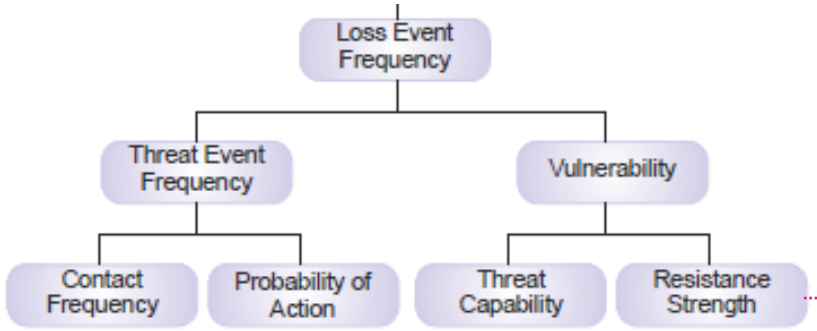
impact quantification – per specific campaign in the TL

follow existing scheme of organisation

COMPILING THREAT METRICS



31 metrics across 8 categories – explicitly verified against practical experiences of involved FIs



A. Past incident timing

B. Past victim profiles

B1 - match with past victim's region of operation

B4 – match with past victim's country development level

C. Threat actor objective

D. Actor commitment

D3 – average amount of days between attacker attempts

E. Threat actor skills

E3 – ATT&CK technique coverage

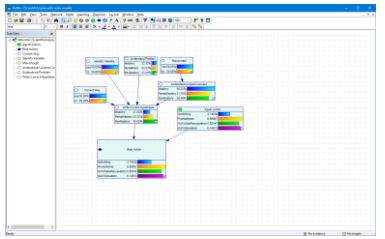
E5 – % past attacks that was successful

F. Detection capabilities

G. Exploitation surface

H. Response capabilities

F4 – DETT&CT campaign coverage

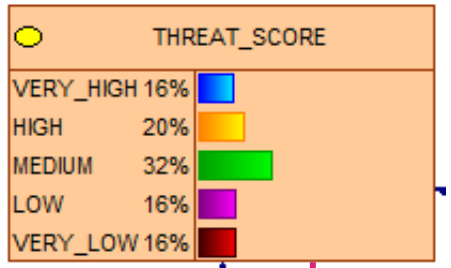


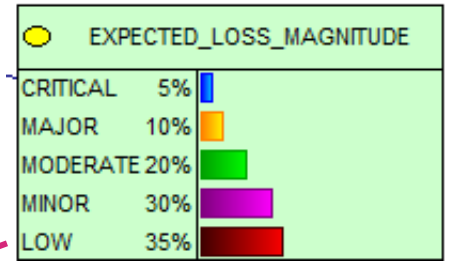
GENIE modeler
https://www.bayesfusion.com/genie/

DESIRE: DATA DRIVEN THREAT SCORE

The TL should reflect evidence driven priorities that are specific to an individual organisation

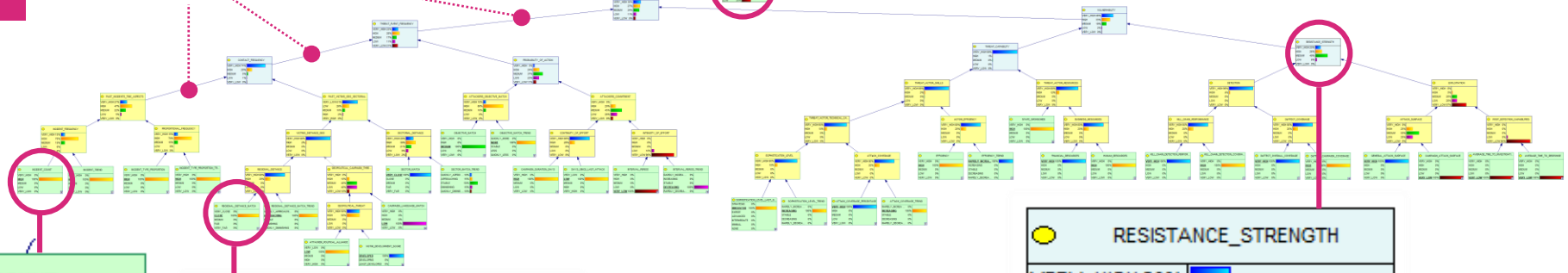
transform to quantitative score

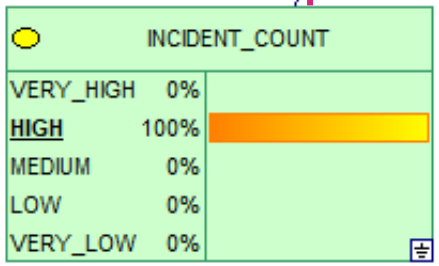


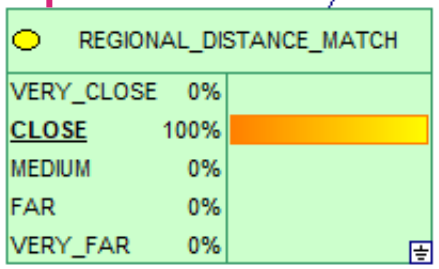


organisation native impact rating (reflects risk appetite)

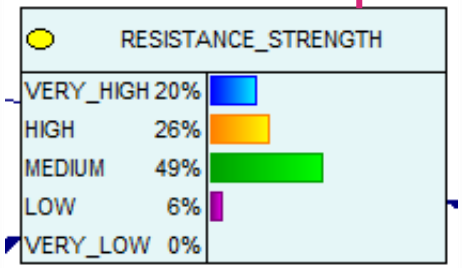
tailored weighting







customised metric ranges



presence and strength of security controls (inherently specific)

PRO FORMA VALIDATION

Source: https://www.symantec.com/blogs/threat-intelligence/targeted-ransomware-threat

Pro forma calculations for two actual campaigns
- GoGalocker (targeted ransomware) and Emotet (distribution of third party malicious payloads)

- All source information required to quantify the metrics seems realistically attainable
- Threat scores and relative priority really do vary and outcome corresponds to expectations
- Scores are relatively close - model supplies ranking where human experts might have difficulty

manual effort for now – outlook is extensive automation

KEY TAKE AWAYS

- Metrics driven threat prioritization creates transparency and minimizes influence of expert judgement
- Maintaining a joint, sectoral threat landscape adds great value to communities such as the FI-ISAC but also requires a degree of trust among the participating FIs
- Evidence based threat prioritisation requires some maturity, e.g. a reasonably developed intelligence practice
- Automation is key for employing realistic (and thus elaborate) threat metrics models in actual practice

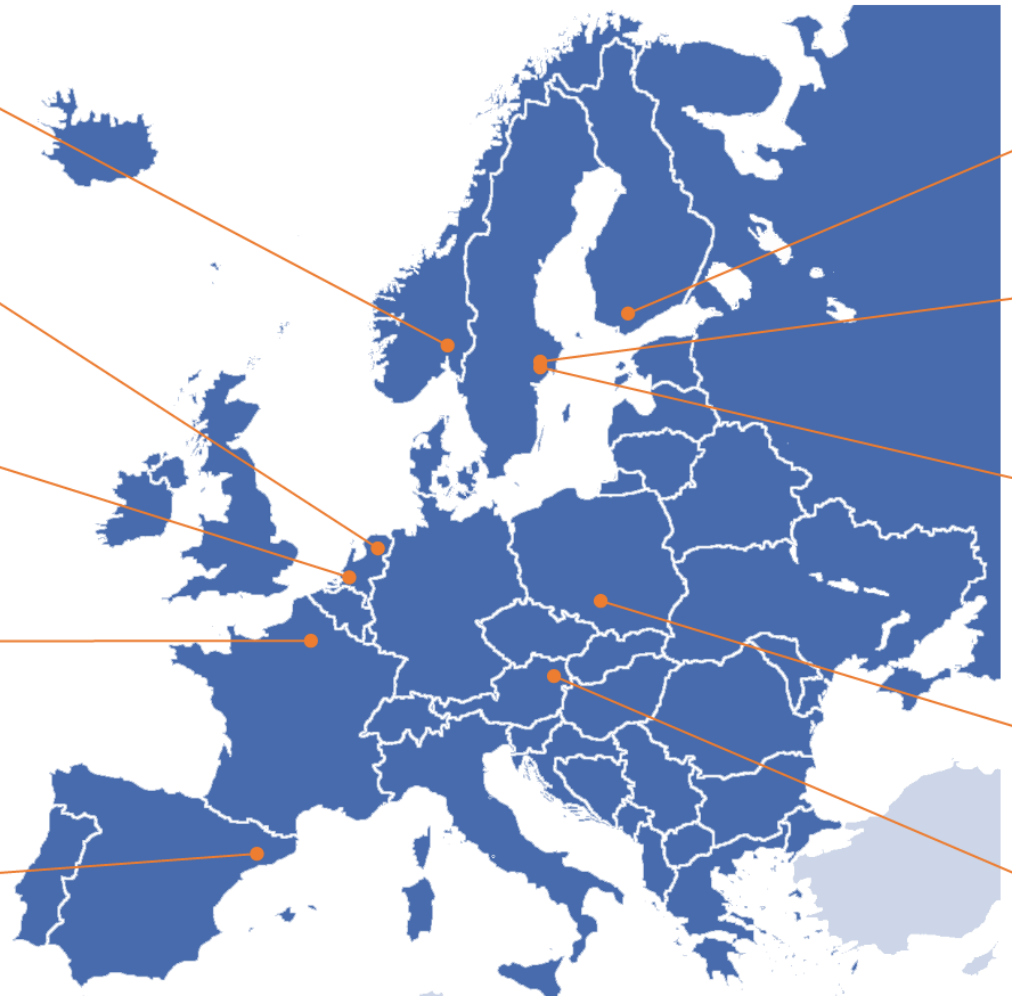
TOEPASSINGSVOORBEELDEN

INNOVATIE: HOE BEPAAL IK OF INNOVATIE MIJ VEILIGER MAAKT

- Project: SOCCRATES (SOC and CSIRT Response to Attacks and Threats based on Attack Defense Graphs Evaluation Systems), EU funded project led by TNO

SOCCRATES CONSORTIUM

SOCCRATES



mnemonic
Securing your business.

TNO innovation for life

SHADOWSERVER

Institut Mines-Télécom

TELECOM SudParis
Une école de l'IMT

Atos

F-Secure

KTH VETENSKAP OCH KONST

foreseeti

VATTENFALL

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Challenge & Objectives

SOCCRATES

Project challenge:

How can SOC and CSIRT operations effectively improve their capability in detecting and managing response to complex cyber-attacks and emerging threats, in complex and continuously evolving ICT infrastructures while there is a shortage of qualified cybersecurity talent?

Main objective:

Develop and implement a security automation and decision support platform that enhances the effectiveness of SOC and CSIRT operations.

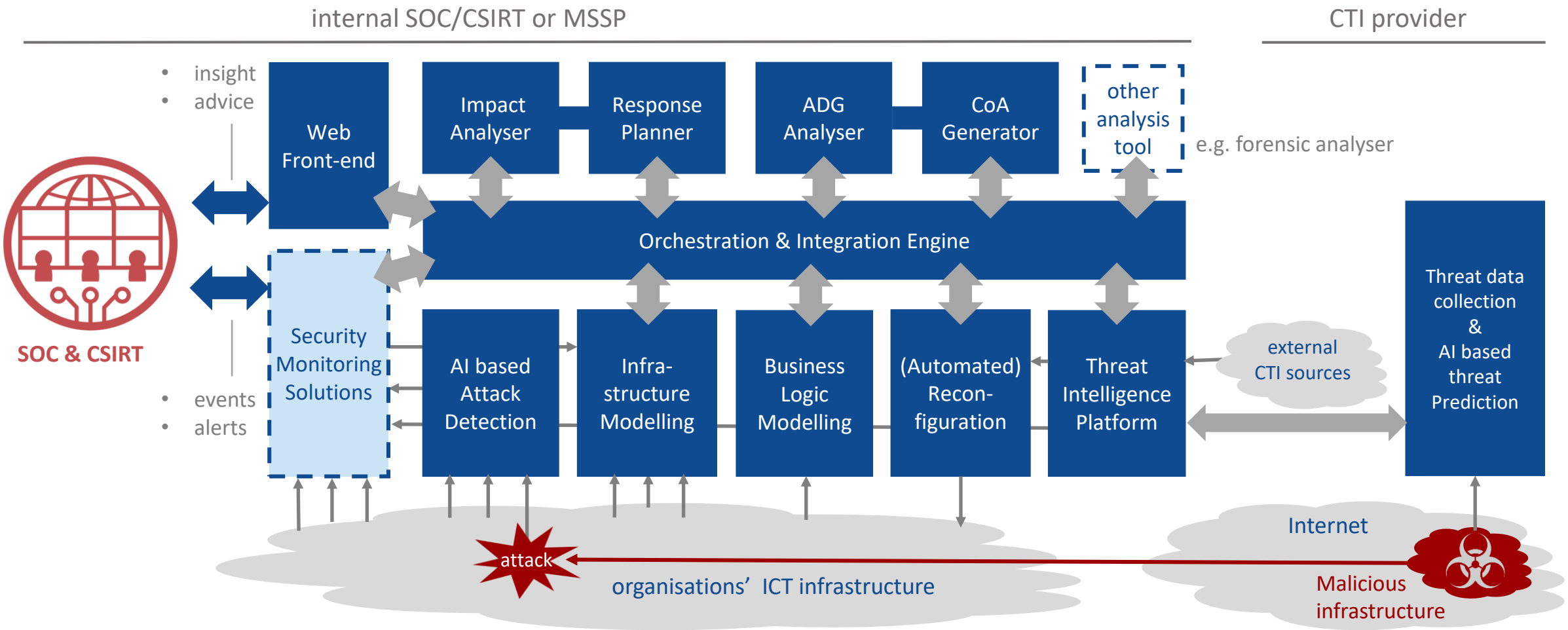
VISION

SOCCRATES

Security automation & decision support for SOC/CSIRT operations

www.soccrates.eu

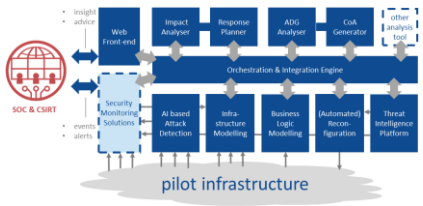
SOCCRATES Component Architecture



SOCCRATES PILOT

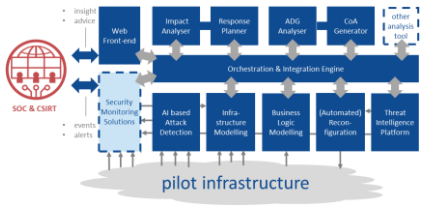
On-site validation

mnemonic



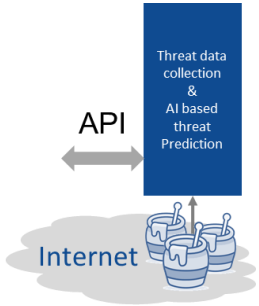
MSSP SOC/CSIRT

VATTENFALL

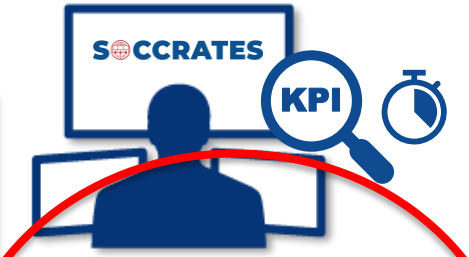


Corporate IT SOC

SHADOWSERVER



Provide DGA & Threat Data



Validate the KPI improvements in the use cases UC1 to UC5

PLATFORM AND PILOT METRICS

Goal: Validate the improvements that the SOCCRATES platform generates

- Formal KPI's

  Example: Prototype successfully improves detection capability (incl. detecting attacks in encrypted traffic)

- A more operational perspective, the plan is to monitor two sets of metrics:

1. Platform activity and performance. What went on in the SOCCRATES platform during the pilot and capture that in numbers and (trend) graphs. Required data will be collected directly from the platform, preferably in an automated fashion.

   Example: # times that a worksflow completed successfully in the past week

2. Analyst experience and perception. The extent to which analysts involved in the pilot actually used the platform's functions and the value that they were able to take from this. Analysts will be asked to fill in a weekly questionnaire and take part in a number of evaluation sessions to supply further context.

   Example: How many times did the platform provide significant added value in your work as a security analyst

CONCLUSIE EN DISUSSIE

MIJN LEERPUNTEN

METRICS
MIJN LEERPUNTEN (1)

- Waarvoor gebruik je metrics?
  - Het is belangrijk om goede uitgangspunten te formuleren metrics goed te ontwerpen, om teleurstellingen achteraf te voorkomen

- Bedenk goed waar je metrics voor wilt gebruiken, definieer doel, doelgroep. En blijf daar ook bij.
- Bepaal daarna de meetmethode en eventueel een norm.
- Inventariseer welke data nodig is en of die ook beschikbaar is

METRICS
MIJN LEERPUNTEN (2)

- Wat zeggen metrics nu eigenlijk?
- Voorbeeld:
  - De metrics zeggen dat 99,9 van al je systemen goed zijn gepatched volgens het laatste patch level, conform de norm in je beleid
  - Goed bezig!
- Maar wat als een paar belangrijke systemen in die 0,1 procent niet goed zijn gepatched en kritieke vulnerabilities bevatten waardoor aan aanvaller kan binnenkomen?

- Gebruik metrics met verstand
- Gebruik metrics met verschillende invalshoeken ter verificatie
- Vertrouw niet blindelings op de cijfers

METRICS
MIJN LEERPUNTEN (3)

- Metrics worden doorgaans beter van meer en kwalitatief betere data
- Data is in overvloed aanwezig, maar niet altijd (tijdig) beschikbaar en niet altijd in het juiste formaat en niet altijd van de juiste kwaliteit

- Kijk bij de data beschikbaarheid niet alleen naar je eigen organisatie, maar ook naar professionale dataleveranciers (zoals Bitsight)
- Voor actuele metrics is automatisering noodzakelijk zodat snel actuele data in de metrics kunnen worden ingevoerd.

DISCUSSIE

BEDANKT VOOR
UW AANDACHT

TNO innovation for life