“PROTECTIVE – Lessons Learnt to Date”

OASIS & FIRST Borderless Cyber Conference and Technical Symposium, Prague, 6-8th Dec 2017

Dr Jassim Happa, Research Fellow

Dept. of Computer Science, University of Oxford

jassim.happa@cs.ox.ac.uk

PROTECTIVE

PROACTIVE RISK MANAGEMENT

https://protective-h2020.eu/

European Commission

Overview

- Who?
- PROTECTIVE – Motivation, (High-Level) Approach and Goals
- Challenges
- Requirements Gathering and Findings
- High-Level Architecture
  - Data Enrichment
  - Prioritisation
  - Threat Intelligence Sharing
- Moving Forward
- Pilots

Purpose of presentation:

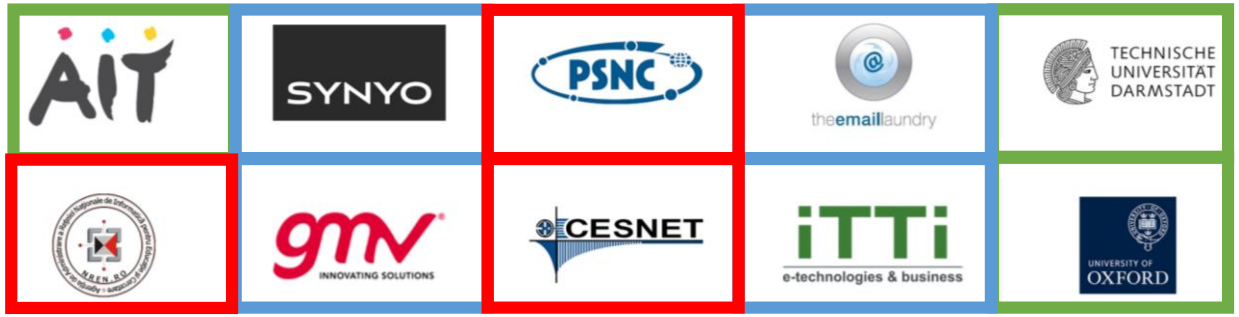
- Overview the project + lessons learnt to date
- Peer review of approach, feedback!
- Networking – let's talk!

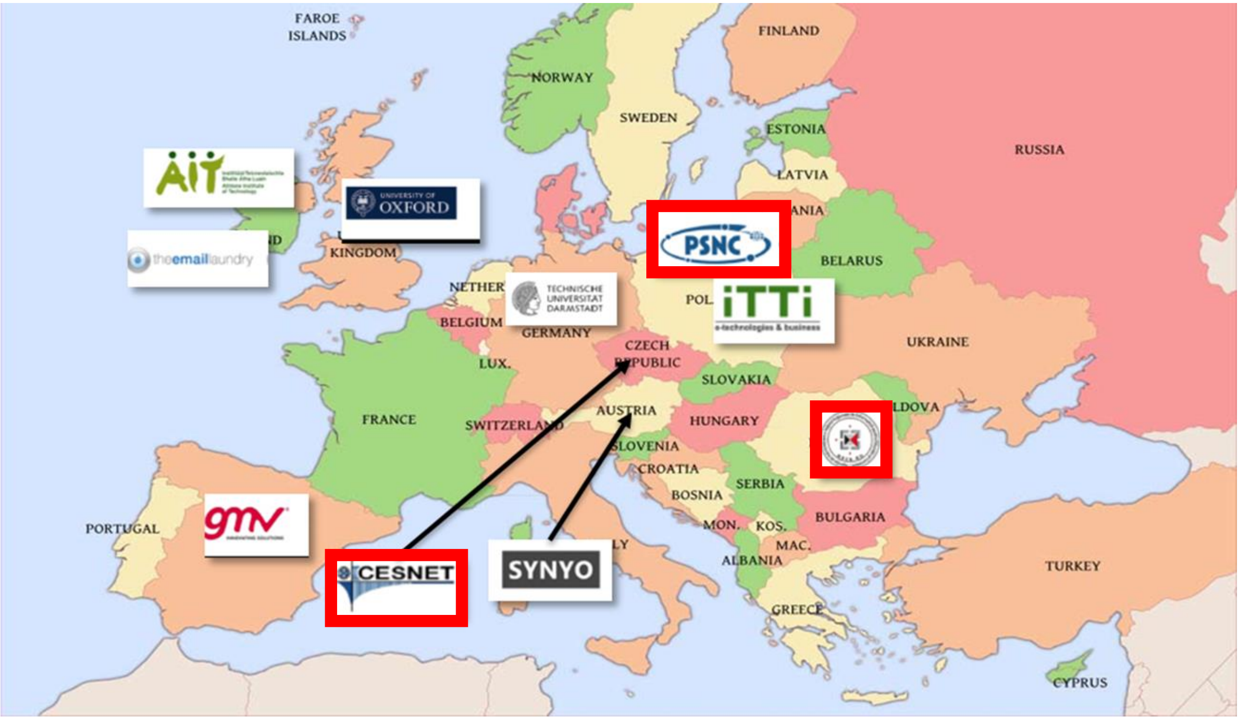
This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

Overview – Who?

EU Project:

- 36 month duration
    - Year 1 complete
- 10 partners:
    - 3 academic partners
    - 4 industry partners
    - 3 NREN (National Research & Educational Network) partners
- 8 countries: Ireland, UK, Poland, Austria, Germany, Spain, Czech Republic, Romania





This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

PROTECTIVE – Motivation

ENISA has identified a **set of recommendations** targeted to itself, the CERT community and other security actors aiming at:

- Promoting the continuity of incident feeds
- Making existing tools interoperable and promoting the use of standards for data exchange
- Enhancing capabilities in terms of:
  - **Interoperability**
  - **Correlation engines for incident analysis**
  - **Improved threat intelligence**
  - **Advanced analytics and visualisation**
  - **Automatic prioritisation**

Detect, SHARE, Protect

Solutions for Improving Threat Data Exchange among CERTs

October 2013

enisa

European Union Agency for Network and Information Security

www.enisa.europa.eu

ENISA (Detect, Share Protect, 2013)

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

(High-level) Approach – Key Ideas

Key idea: A platform for “*Proactive Risk Management through Improved Situational Awareness*”

- For **NREN** CSIRTs initially
  - Address NREN needs specifically. Starting point – existing tools well-tested in the NREN space
  - Eventually expand to public CSIRTs
  - Eventually share CTI with SMEs
- **Situational Awareness**: “*Within a volume of time and space, the perception of an enterprise’s security posture and its threat environment; the comprehension/meaning of both taken together (risk) and the projection of their status into the near future*” - US Committee on National Security Systems
- We need awareness capabilities w.r.t.:
  - **Threats** – internal and external alerts, incidents and intelligence
  - **Context** – “Mission” and “Constituency” (Asset management)
  - **Risk** – “Prioritisation” and “Correlation”

This project has received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

European Commission

Goals

- **Provide NRENs with improved security alert management capabilities (after ENISA)**
  - Starting with NRENs, then (hopefully) move to the public CSIRTs
- **Explore added value to SMEs** – warn SMEs early
- **Meta alerts:** summarising threats and incidents – what's the bigger picture? Fewer alerts!
- **Context awareness**: enable better prioritisation of internal events
- **Threat Intelligence Sharing** between NRENs
- **GDPR and NDA compliance**
- **Trust:** Confidentiality + Reputation scores + Quality of threat intelligence
- **Automation**, (automation, automation!)

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

Challenges

- **Gathering both technical and human factor requirements** of NRENs
  - State of the art **literature survey** + **interviews of potential end-users** (analysts at NRENs)
- **Defining Cyber Threat Intelligence**
- **Defining Trust**: "Secure connection" vs "Quality of Event" vs "Reputation Scores" vs "Freshness" etc.
- **Understanding optimal use of Automation and Human** intelligence
  - Can we aggregate events in meaningful ways to generate intelligence -> fewer alerts!
  - Which aspects should be automated? What human factors prevent/enhance CTI sharing?
- **Understanding optimal data enrichment** – what insight is meaningful to add?
- **Understanding context** - generating and maintaining mission and constituency insight.
- **Understanding legal and ethical considerations** in the wake of the EU General Data Protection Regulation
  - Data handling concerns: At what point is threat intelligence personal data?
    - NIS directive helpful for exception handling here
  - Requirements analysis: Going from legal speak to tech speak is difficult.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

Desktop analysis – what is cyber threat intelligence?

- **CBEST 2016**: *"a particular kind of information. Intelligence and information are often used interchangeably as are information and data. To properly understand information (and therefore intelligence) it is necessary to put it in context and a useful model is the data information knowledge pyramid."*
- **Chismon & Ruks, 2015**: *"… information that can be acted upon to change outcomes. It's worth considering traditional intelligence before exploring threat intelligence, as in many ways the latter is simply traditional intelligence applied to cyber threats"*
- **Dalziel 2014**: Information about threats that is "*relevant, actionable and valuable*".
- **ENISA 2014** : Suggest four layers: "*low-level data", "detection indicators", "advisories"* and "*strategic reports"*
- **Friedman & Bouchard 2015**: "*knowledge about adversaries and their motivations, intentions, and methods that is collected, analysed, and disseminated in ways that help security and business staff at all levels protect the critical assets of the enterprise."*

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

Desktop analysis – what is cyber threat intelligence?

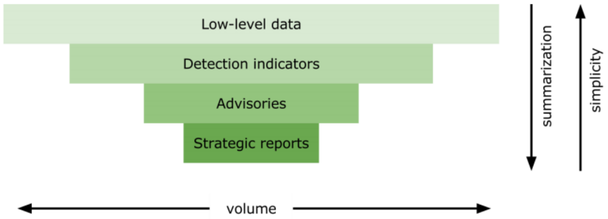
- **Gartner 2013** *“…evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.”*
- **NIST 2016**: *“Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision making processes”*
- **SANS 2016**: No definition(?), but describe Gartner, and elaborate: *“Part of defining TI is deciding what it is not. TI is not simply a list of atomic indicators that an attacker used at one point in time, without additional context into how the attack worked.”* Have a forum post outlining how each organisation can “*Defining Threat Intelligence Requirements*” for organisations.
- **STIX** – provides an in-depth discussion on domain objects and patterns, and a schema for CTI https://github.com/oasis-open/cti-stix2-json-schemas , but does not provide a definition.
- **VERIS** – focusses on Event Recording and Incident Sharing, and a schema for it - http://veriscommunity.net/schema-docs.html , does not discuss CTI specifically.

This project has received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

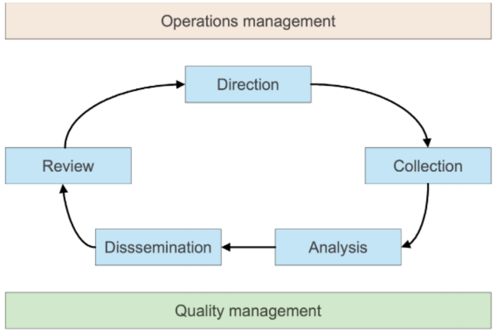
Desktop analysis – what is cyber threat intelligence?

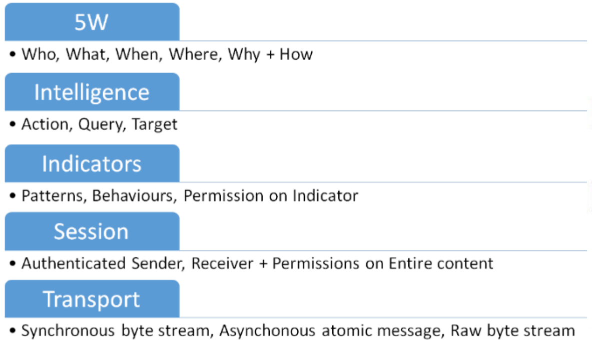
Key lessons learnt/key findings:

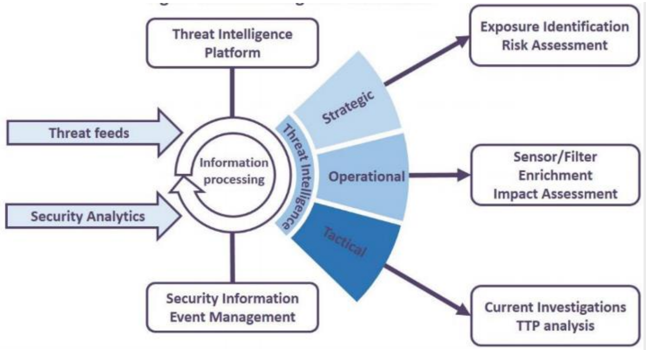
- Several organisations have adopted Gartner’s definition, incl. CERT-UK, Webroot, FireEye and Tripwire.
- Definitions have inconsistent uses of the words, *TI, CTI*, *data*, *information* and *knowledge*.
  - Imprecise definitions – e.g. CTI vs TI, difficult to translate
  - Definitions are (seemingly) ad hoc – not evidence based
- Taxonomies and figures often used instead of unambiguous, succinct definitions.

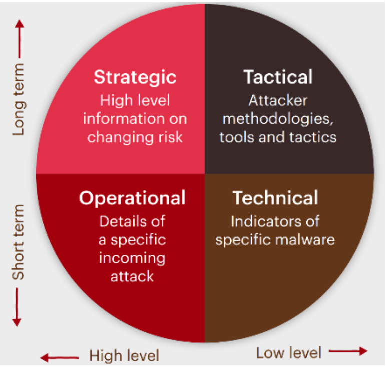


ENISA 2014




5W
• Who, What, When, Where, Why + How
Intelligence
• Action, Query, Target
Indicators
• Patterns, Behaviours, Permission on Indicator
Session
• Authenticated Sender, Receiver + Permissions on Entire content
Transport
• Synchronous byte stream, Asynchonous atomic message, Raw byte stream


Threat Intelligence Platform
Threat feeds
Security Analytics
Information processing
Threat Intelligence
Strategic
Operational
Tactical
Security Information Event Management
Exposure Identification Risk Assessment
Sensor/Filter Enrichment Impact Assessment
Current Investigations TTP analysis


Long term
Short term
Strategic
High level information on changing risk
Tactical
Attacker methodologies, tools and tactics
Operational
Details of a specific incoming attack
Technical
Indicators of specific malware
High level
Low level

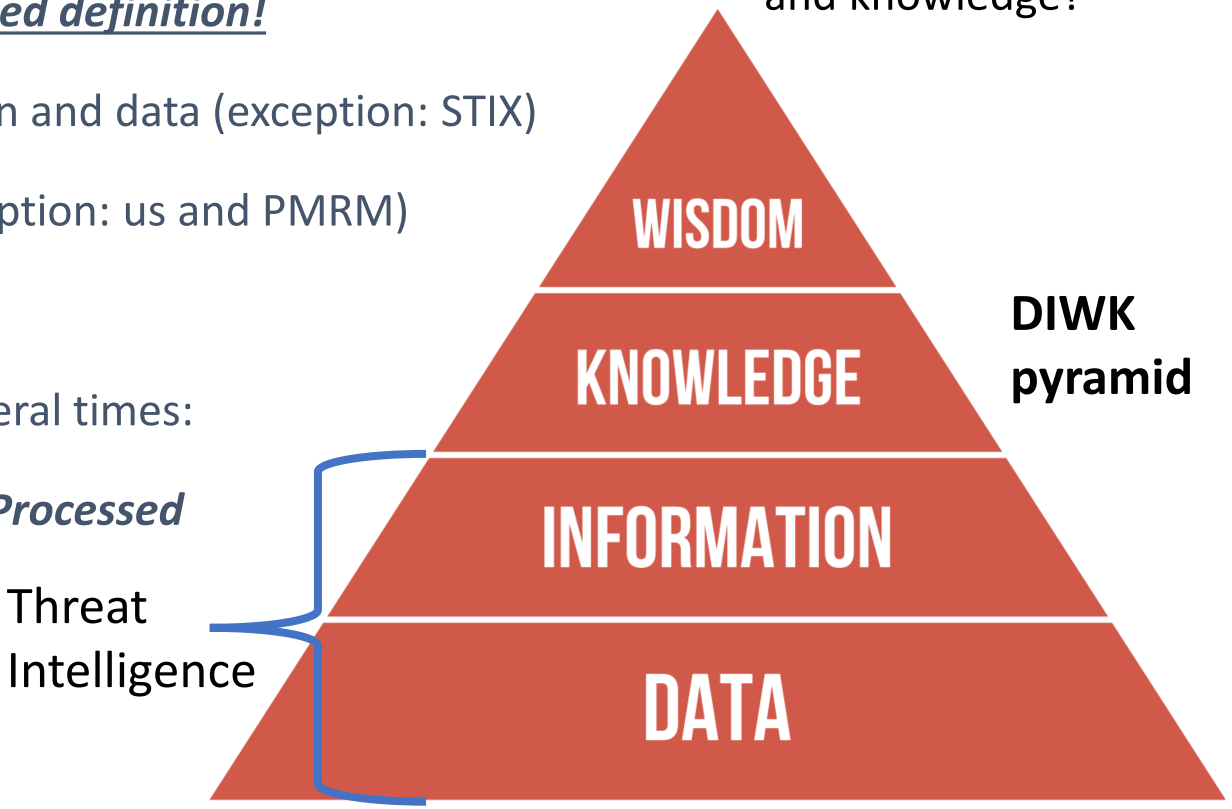
CBEST 2016 Burger et al. 2014 CERT-UK 2015 Chismon & Ruks 2015

This project has received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

Desktop analysis – what is cyber threat intelligence?

Key lessons learnt:

- Little focus on:
  - Definition: ***No universally-accepted definition!***
  - Relationship between information and data (exception: STIX)
  - GDPR and NDA compliance (exception: us and PMRM)
  - (Computational) Trust
- Literature refers to DIKW pyramid several times:
  - ***Actionable, Relevant, Valuable, Processed***
  - Processed:
    - Human
    - Machine (automated)



What about wisdom and knowledge?

DIWK pyramid

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

Sharing cyber threat intelligence

- **BIG question: “In a GDPR world (Europe) - what am I allowed to share?”**
- **Legal speak to tech speak is challenging** – A lot of efforts out there, some examples:
  - Fisk et al. “*Privacy Principles for Sharing Cyber Security Data*”. Principles of: **Least Disclosure, Qualitative Evaluation** and **Forward Progress**.
  - **PMRM** - https://www.oasis-open.org/committees/pmrm
  - **MITRE Privacy Engineering Framework** - https://www.mitre.org/publications/technical-papers/privacy-engineering-framework
  - **NIST IR 8062** - http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf
  - **EnCoRe** – “*Ensuring Consent and Revocation*” http://www.hpl.hp.com/breweb/encoreproject/
    - **Formal Methods (Hoare logic) to Detect and Resolve** Ambiguities in Privacy Requirements
    - **Run-time compliance monitors** for personal data handling violation checking (akin to IDSs)

This project has received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

Requirements Gathering and Findings

Capture – to understand human and tech needs

- **Desktop analysis** from state of the art review - literature
- Conducted and analysed **interviews and questionnaires**
  - 74 interviews and discussions
  - 69 main questions spread across 8 key areas:
    - **Practices, Technical, Legal/Policy, Trust, Human Aspects, Sharing, Risk Assessments**
  - Procedure:
    - Questionnaires, Semi-structured interview, Observations
    - Behavioural modelling (conceptual model) + requirements analysis

Analysis – for tool development and requirements generation

- Development of 42 key tool requirements

This project has received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

Interview findings – what is cyber threat intelligence?

Key findings:

- The concept of **Cyber Threat Intelligence is ill-defined**.
    - E.g. Some assumption that “data” is synonymous with “information”, “knowledge” and “intelligence”.
- Perception: Too many flavours of tools that achieve largely achieve the same thing, but slightly differently:
    - **Interoperability** – big concern
    - **Automation of higher level threat intelligence** – going from email ticket and sending of indicators to faster actions
    - **Preparation for GDPR** at NRENs, but **little preparation** in CTI standards
    - **Too much hyperbole, little evidence** to support bold CTI claims. Need more success stories/surveys published.
- STIX – **positively regarded**, but:
    - Perception: **“all (of STIX) or nothing”** –> cost/benefit of going in –> on the fence
    - Perception: E.g. **CVE – absolutely! Other standards, may not be as applicable**
    - Perception: Graph-like structure – too high level – **limits automation and interoperability**
    - Perception: Concerns about **maintenance and longevity**
        - First XML, now JSON – “how do we know it will be stable?”
- VERIS - **positively regarded**, but perception: not enough momentum, or well-known.

This project has received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

Interview findings – NREN similarities and differences

Key findings:

- NREN work cultures are vastly different from each other:
  - **Hierarchical vs Flat organisational structures** – determines what goes and what doesn't.
  - **In-house tool development vs outsourcing** of network maintenance, hardware and software
  - **Varying in size** (from less than ten to several hundred)
    - Smaller NRENs are particularly strapped for resources
  - **Raison d'être** and **history** of CSIRT – fundamentally different from each other
    - Affects mission, priorities and strategic and run-time decision making
- **Impact of work cultures uncertain**, but we suspect they contribute to:
  - CTI requirements -> different missions, different environments, different priorities
  - "Ad hoc-ness" of selection and uses of tools
  - Ability to decide whether to integrate tools and standards into their environment
    - Hard choices: old and trustworthy vs new and fancy -> esp. when strapped for resources

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

(Preliminary) SME Requirements Gathering

Key findings:

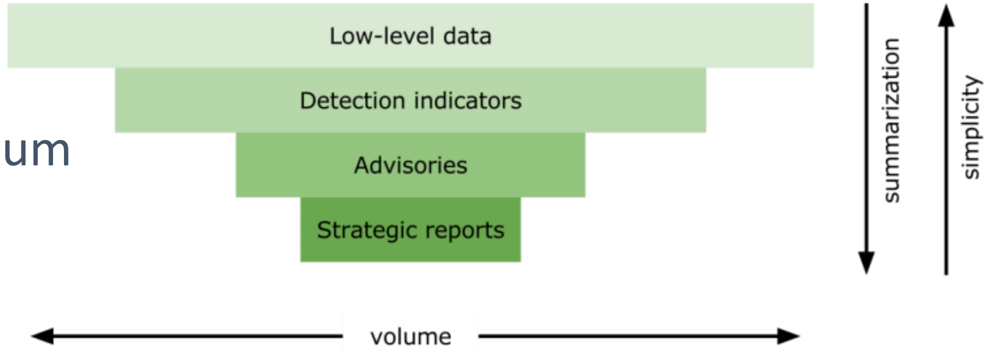
- SMEs do not have resources to deal with security
  - May outsource their security to Managed (Security) Service Providers
  - Event MSSPs may not have resources to keep up to date on CTI
    - How can we streamline this?
      - **Email advisories get ignored** - must avoid
      - **Linking CTI to customers** – “killer app” to existing services
      - **SMEs want this free/very cheap**
        - Akin to an RSS feed generated by the NRENs
- Challenges:
  - Filtering out relevant CTI to non-CSIRTs
  - Linking to customers (context)

Focus group and full questionnaires to follow…

This project has received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

PROTECTIVE CTI

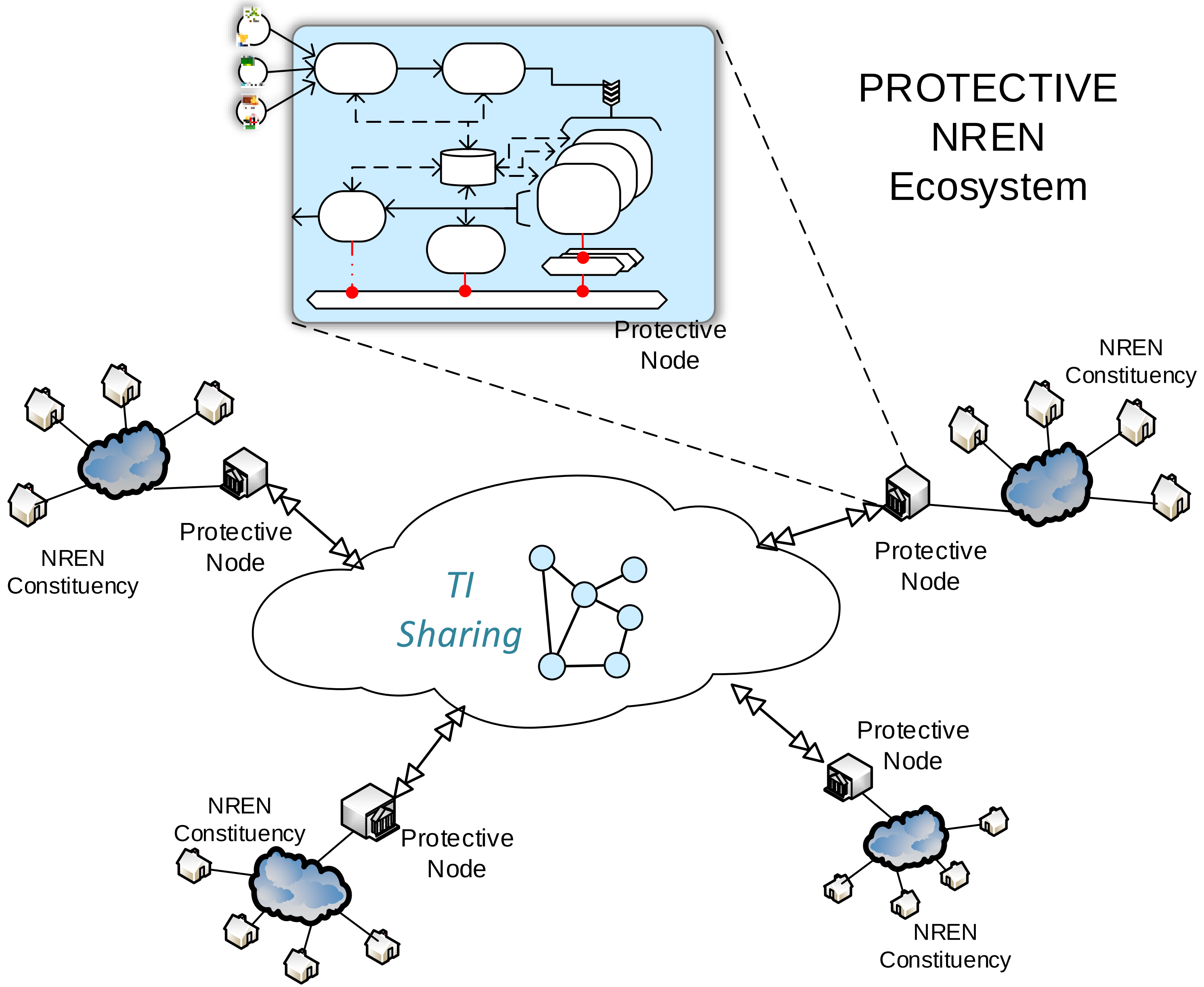
- PROTECTIVE adopts ENISA's definition of CTI and philosophy.
- PROTECTIVE uses IDEA (https://idea.cesnet.cz/) for the following reasons:
  - First step – work with what we know
    - Developers of IDEA are in the consortium
    - Works well for CESNET
  - Low-level data:
    - Flexibility and Simplicity
    - Easy to anonymise/pseudonymise/aggregate for GDPR
    - Append indicators, link to advisories and reports
    - Straightforward to create meta alerts



ENISA 2014

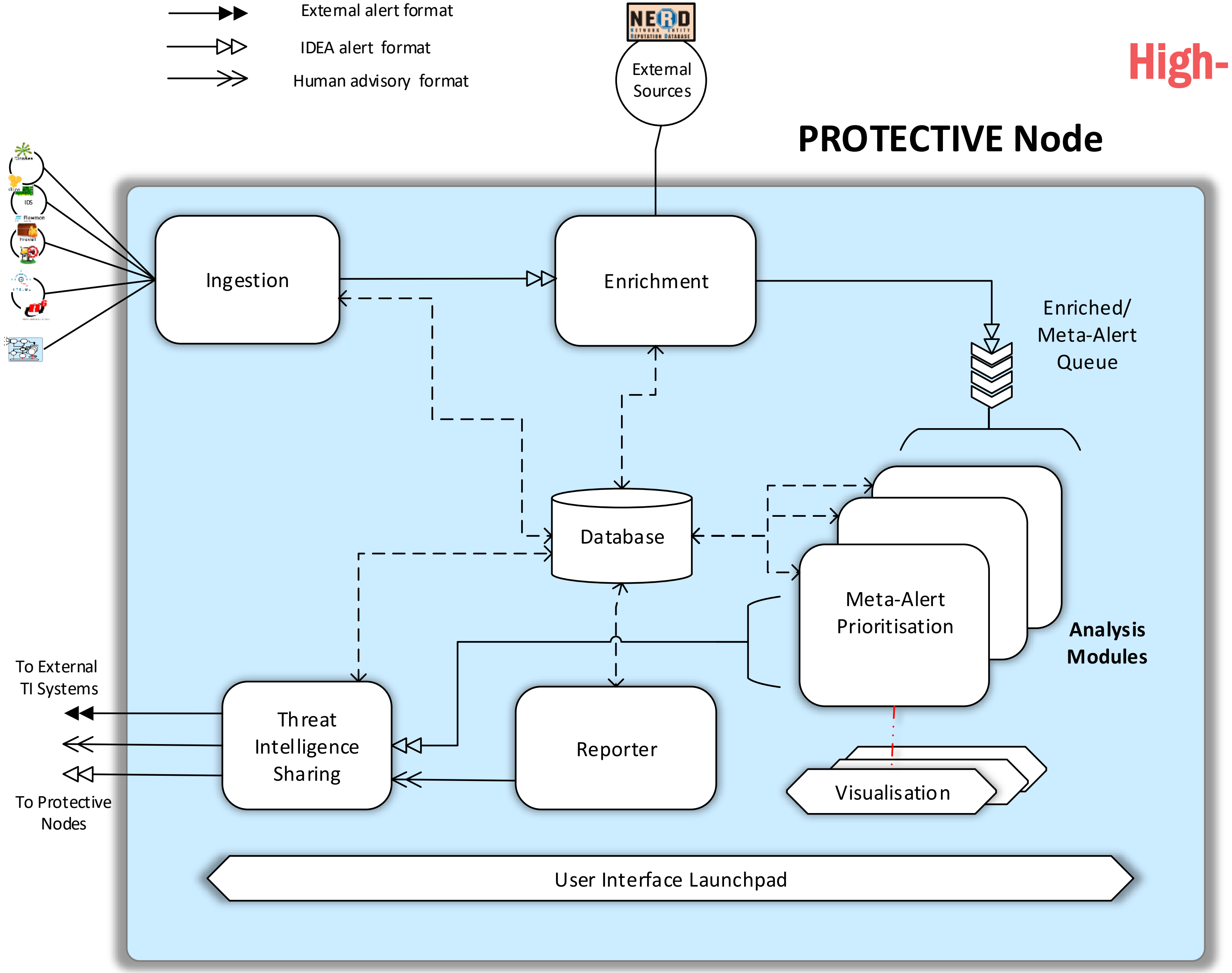
This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

High-Level Architecture



This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

High-Level Architecture

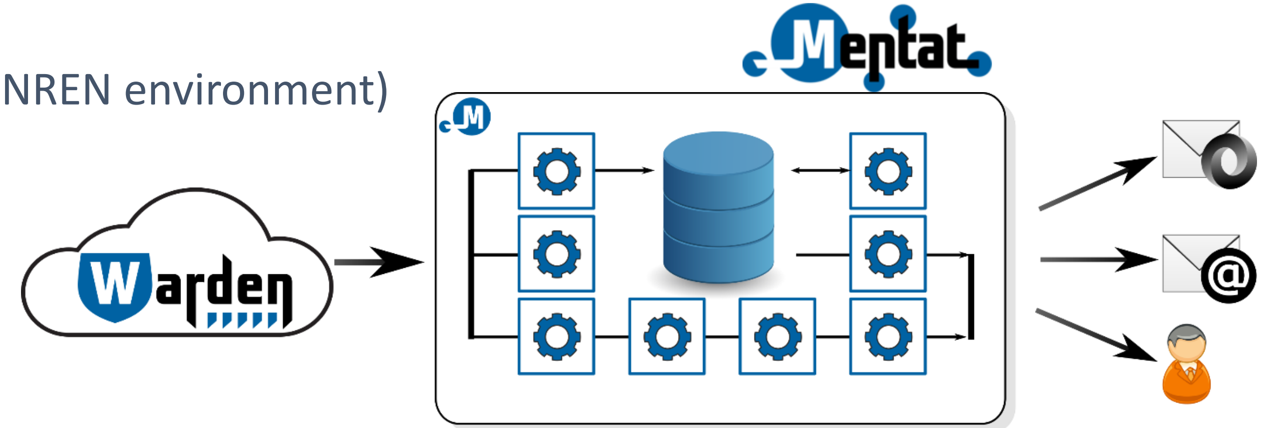


This project has received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

High-Level Architecture

Core:

- **Warden** (system for sharing information about detected events) - https://warden.cesnet.cz/
- **Mentat** (SIEM) - https://mentat.cesnet.cz/
    - **Inspector** (event checker)
- **NERD** (reputation database) - https://nerd.cesnet.cz/
- **IDEA** (event format) - https://idea.cesnet.cz/
- Well-tested in CESNET (used in a live NREN environment)
- Developers are in the consortium



This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

High-Level Architecture – Data Enrichment

New capabilities – added in the project:

- Meta alert **generation** – based on IDEA format
  - Hierarchies/Trees of IDEA events – summarises many events
- Meta alert **correlation –** based on broad alert information scope
- Meta alert **prioritisation -** broad set of prioritisation approaches
- Computational **Trust**

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

High-Level Architecture – Data Enrichment

New capabilities – added in the project:

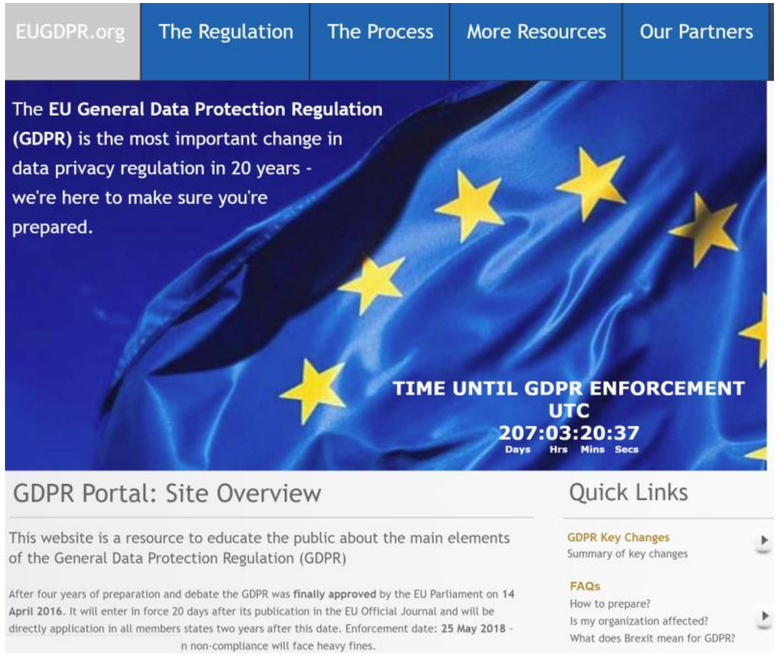
- Context awareness
  - **Mission Asset Information Repository**
  - **Mission Impact Modelling**
  - **External Inventory Interface defined**
- Challenges:
  - Updating list - frequency?
  - Level of detail.

This project has received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

European Commission

Emerging concerns in sharing CTI

- **GDPR/NDA - “What the <u>baseline?</u>”**
  - GDPR not written with cyber threat intelligence in mind
- **GDPR/NDA -“How do I know I meet <u>legal specifications</u>?”**
  - Experimenting with run-time information sharing compliance monitors for NDAs and GDPR
    - **Use-case based** - multiple domain expert review
      - e.g. legal, ethical, technical reviews
    - **Rule-based** – akin to an IDS, based on Inspector
    - **Iterative refinement** – improve over two pilots
  - **From the ground up –** interviews and desktop analysis.



The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years - we're here to make sure you're prepared.

TIME UNTIL GDPR ENFORCEMENT UTC
207:03:20:37
Days Hrs Mins Secs

GDPR Portal: Site Overview

This website is a resource to educate the public about the main elements of the General Data Protection Regulation (GDPR)

After four years of preparation and debate the GDPR was **finally approved** by the EU Parliament on **14 April 2016.** It will enter in force 20 days after its publication in the EU Official Journal and will be directly application in all members states two years after this date. Enforcement date: **25 May 2018** - n non-compliance will face heavy fines.

Quick Links

GDPR Key Changes
Summary of key changes

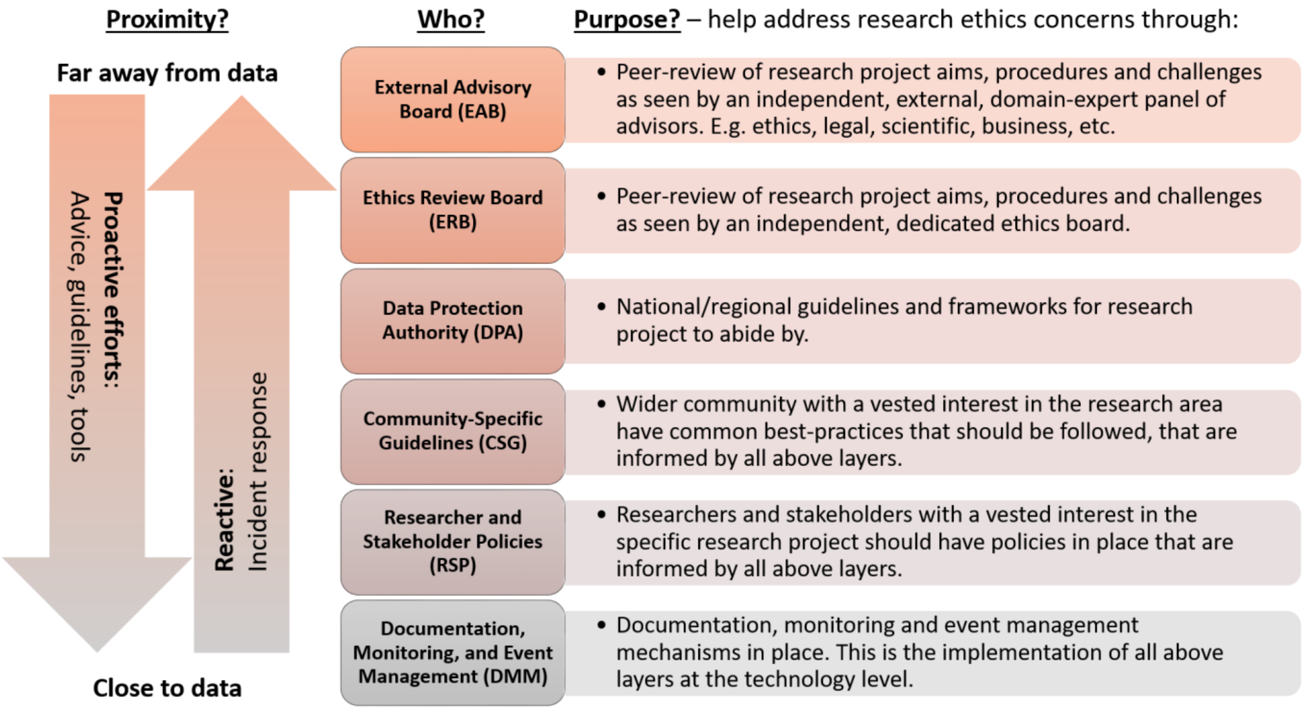
FAQs
How to prepare?
Is my organization affected?
What does Brexit mean for GDPR?

https://www.eugdpr.org/

This project has received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

Challenging Use Cases

- New capabilities: How do we deal with ethical and legal concerns?
- How do we come up with rules in the first place? Illegal or Sensitive (Personal, Classified, NDA, etc.)
  - During: **Research**, **Development**, in **Use** – look at the problems from different lenses!



Proximity?

Far away from data

Proactive efforts: Advice, guidelines, tools

Reactive: Incident response

Close to data

Who?	**Purpose?** – help address research ethics concerns through:	
External Advisory Board (EAB)	Peer-review of research project aims, procedures and challenges as seen by an independent, external, domain-expert panel of advisors. E.g. ethics, legal, scientific, business, etc.	**Domain experts**
Ethics Review Board (ERB)	Peer-review of research project aims, procedures and challenges as seen by an independent, dedicated ethics board.	**Ethics**
Data Protection Authority (DPA)	National/regional guidelines and frameworks for research project to abide by.	**Legal**
Community-Specific Guidelines (CSG)	Wider community with a vested interest in the research area have common best-practices that should be followed, that are informed by all above layers.	**Wider community (e.g. TIS guidelines)**
Researcher and Stakeholder Policies (RSP)	Researchers and stakeholders with a vested interest in the specific research project should have policies in place that are informed by all above layers.	**Direct stakeholders (analysts)**
Documentation, Monitoring, and Event Management (DMM)	Documentation, monitoring and event management mechanisms in place. This is the implementation of all above layers at the technology level.	**Automation (tools)**

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

Moving Forward – PROTECTIVE and the CTI community

- **Can we come up with a definition?**
- **More empirical evidence, more studies! –** let's make sure this is what end-users want, but also what they need
  - Refine requirements with other NRENs and public CSIRTs
- **Moving towards v1.0** – with novel capabilities being:
  - Meta-alerts (in the context of CTI)
  - Computational Trust
  - Towards *Information Sharing Compliance* (GDPR, NDAs)
  - **We are still experimenting**, still learning, still trying out new and exciting things
- **STIX support:** conversion or native support – interoperability
- **Pilots – trialling the system in NREN environments**
  - Towards *Multinational Alliance for Collaborative Cyber Situational Awareness Information Sharing Framework*
- **We want to engage more and get more evidence**
  - Keen to get feedback/comments/suggestions/collaboration!

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

Pilots

- **Pilot 1: Internal focus with consortium developers**
  - Jan 2018 - July 2018
  - Functional, system and usability testing in three live NREN environments.
  - Constituency focus, then Community focus. Configuration: P2P
- **Pilot 2: External focus**
  - Dec/Jan 2018/2019 – July 2019
  - Aim: minimise disruption, maximise benefit, get outsider feedback
  - In conversations with other NRENs + SMEs
    - (SMEs as subscribers only – akin to an RSS feed)

This project has received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

Questions?

Jassim Happa. Research Fellow,

University of Oxford,

jassim.happa@cs.ox.ac.uk

Brian Lee. Project coordinator,

Athlone Institute of Technology

blee@AIT.IE

This project has received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

Bibliography

- Ahrend, J. M., Jirotka, M., & Jones, K. (2016). On the collaborative practices of cyber threat intelligence analysts to develop and utilize tacit Threat and Defence Knowledge. Cyber Situational Awareness, Data Analytics And Assessment (CyberSA).
- Bromiley, M. (2016). Threat Intelligence: What It Is, and How to Use It Effectively SANS. SANS.
- Burger, E. W., Goodman, M. D., Kampanakis, P., & Zhu, K. A. (2014). Taxonomy model for cyber threat intelligence information exchange technologies. ACM Workshop on Information Sharing & Collaborative Security.
- CBEST, 2016. Intelligence-Led Testing Understanding Cyber Threat Intelligence Operations. Bank of England.
- CERT-UK. (2015). Integrating Threat Intelligence Defining an Intelligence Driven Cyber Security Strategy. CERT-UK, CPNI.
- Chismon, D., & Ruks, M. (2015). Threat Intelligence: Collecting, Analysing, Evaluating. MWR InfoSecurity.
- CNSS. (2015). Committee on National Security Systems (CNSS) Glossary. Retrieved from https://www.cnss.gov/CNSS/openDoc.cfm?0SK1qPsaRpQtdsXBZsIxLQ==
- Dalziel, H. (2014). How to define and build an effective cyber threat intelligence capability. Syngress.
- Dandurand, L., & Serrano, O. S. (2013). Towards improved cyber security information sharing. International Conference on Cyber Conflict (CyCon).
- Danyliw, R., Meijer, J., & Demchenko, Y. (2007). The incident object description exchange format. Retrieved 2017, from https://tools.ietf.org/html/rfc5070
- Debar, H., Curry, D., & Feinstein, B. (2007). Intrusion Detection Message Exchange Format (IDMEF). Retrieved 2017, from https://www.ietf.org/rfc/rfc4765.txt
- EnCoRe – "Ensuring Consent and Revocation" http://www.hpl.hp.com/breweb/encoreproject/
- ENISA. (2013, March). Detect, SHARE, Protect. https://www.enisa.europa.eu/publications/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs/at_download/fullReport
- ENISA. (2014). Standards and tools for exchange and processing of actionable information. https://www.enisa.europa.eu/publications/standards-and-tools-for-exchange-and-processing-of-actionable-information/
- ENISAa. (2014). Actionable Information for Security Incident Response. Retrieved from https://www.enisa.europa.eu/publications/actionable-information-for-security/
- ENISAa. (2016). ENISA Threat Taxonomy. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information
- ENISAb. (2016). NCSS Good Practice Guide Designing and Implementing National Cyber Security Strategies. Retrieved 2017, from https://www.enisa.europa.eu/publications/ncss-good-practice-guide

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

Bibliography 2

- FIPS. (2006). PUB 200. Retrieved from Minimum Security Requirements for Federal Information and Information Systems: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf
- FireEye. (2017). FireEye Threat Intelligence Webpage https://www.fireeye.com/products/cyber-threat-intelligence.html FireEye.
- Fisk et al. “Privacy Principles for Sharing Cyber Security Data”. Principles of: Least Disclosure, Qualitative Evaluation and Forward Progress.
- Fransen, F., Smulders, A., & Kerkdijk, R. (2015). Cyber security information exchange to gain insight into the effects of cyber threats and incidents. Elektrotechnik und Informationstechnik.
- Frické, M. (2009). The knowledge pyramid: a critique of the DIKW hierarchy. Journal of information science, 131-142.
- Friedman, J., & Bouchard, M. (2015). Definitive guide to cyber threat intelligence. CyberEdge Press.
- Garrido-Pelaz, R., González-Manzano, L., & Pastrana, S. (2016). Shall we collaborate?: A model to analyse the benefits of information sharing. ACM Workshop on Information Sharing and Collaborative Security.
- Goodwin, C., Nicholas, J. P., Bryant, J., Ciglic, K., Kleiner, A., Kutterer, C., & Storch, T. (2015). A framework for cybersecurity information sharing and risk reduction. Microsoft.
- Haass, J., Ahn, G.-J., & Grimmelmann, F. (2015). ACTRA-A Case Study for Threat Information Sharing. ACM Workshop on information sharing and collaborative security.
- Habib, S. M., Ries, S., Hauke, S., & Mühlhäuser, M. (2012). Fusion of Opinions under Uncertainty and Conflict -- Application to Trust Assessment for Cloud Marketplaces. IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 109-118.
- Harkins, M. (2016). Managing risk and information security. Apress.
- IntelMQ. (2017). IntelMQ. Retrieved 04 25, 2017, from https://github.com/certtools/intelmq
- Jang, J.-w., Kang, H., Woo, J., Mohaisen, A., & Kim, H. K. (2015). Andro-AutoPsy: Anti-malware system based on similarity matching of malware and malware creator-centric information. Digital Investigation, 14, 17-35.
- Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). Guide to Cyber Threat Information Sharing. National Institute of Standards and Technology (NIST).
- Kacha, P. (2013). IDEA: Designing the Data Model for Security Event Exchange. Computers: Recent Advances in Computer Science.
- Kacha, P., M. Kostenec, M., & Kropacova, A. (2016). Warden 3: Internet Threat Sharing Platform. International Journal of Computers.
- Kaijankoski, E. A. (2015). Cybersecurity Information Sharing Between Public-Private Sector Agencies. Calhoun.
- Kijewski, P., & Pawliński, P. (2014). Proactive Detection and Automated Exchange of Network Security Incidents. Abgerufen am.
- Lewis, R., Louviens, P., Abbott, P., Clewley, N., & Jones, K. (2014). Cybersecurity Information Sharing: A Framework for Sustainable Information Security Management in UK SME Supply Chains. European Conference on Information Systems (ECIS).

This project has received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

European Commission

Bibliography 3

- Liu, Y., Muller, S., & Xu, K. (2007). A static compliance-checking framework for business process models. IBM Systems Journal, 46, 335-361.
- MACCSA. (2013). Information Sharing Framework. https://www.terena.org/mail-archives/refeds/pdfjJz1CRtYC4.pdf
- Mauro, F., & Stella, D. (2016). Brief Overview of the Legal Instruments and Restrictions for Sharing Data While Complying with the EU Data Protection Law. International Conference on Web Engineering.
- McMillan, R. (2013). Definition: Threat Intelligence. https://www.gartner.com/doc/2487216
- MITRE Privacy Engineering Framework - https://www.mitre.org/publications/technical-papers/privacy-engineering-framework
- MITRE. (2015). An Overview of MITRE Cyber Situational Awareness Solutions. Retrieved 2017, from https://www.mitre.org/sites/default/files/publications/pr-15-2592-overview-of-mitre-cyber-situational-awareness-solutions.pdf
- Mohaisen, A., Al-Ibrahim, O., Kamhoua, C., Kwiat, K., & Njilla, L. (2017). Rethinking information sharing for actionable threat intelligence. Cornell University Library.
- Moriarty, K. (2012). Real-time inter-network defense.
- Movius, L., & Krup, N. (2009). US and EU privacy policy: comparison of regulatory approaches. International Journal of Communication.
- NCIAgency. (2017). Malware Information Sharing Platform. https://www.ncia.nato.int/Documents/Agency%20publications/Malware%20Information%20Sharing%20Platform%20(MISP).pdf
- NIST 2016: "Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision making processes"
- NIST IR 8062 - http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf
- NIST. (2013). Glossary of Key Information Security Terms. National Institute of Standards and Technology.
- NIST. (2016). SP 800-150. Retrieved from Guide to Cyber Threat Information Sharing: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf
- OASIS PMRM - https://www.oasis-open.org/committees/pmrm
- Ries, S., Habib, S. M., Mühlhäuser, M., & Varadharajan, V. (2011). CertainLogic: A Logic for Modeling Trust and Uncertainty (Short paper). 4th International Conference on Trust and Trustworthy Computing, pp. 254-261.
- Rowley, J. (2007). The wisdom hierarchy: representations of the DIKW hierarchy. Journal of Information and Communication Science, 163–180.
- Sauerwein, C., Sillaber, C., Mussmann, A., & Breu, R. (2017). Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives. Wirtschaftsinformatik.
- Sedenberg, E. M., & Mulligan, D. K. (2015). Public Health as a Model for Cybersecurity Information Sharing. Berkeley .
- Serrano, O., Dandurand, L., & Brown, S. (2014). On the design of a cyber security data sharing system. ACM Workshop on Information Sharing & Collaborative Security.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

Bibliography 4

- Sillaber, C., Sauerwein, C., Mussmann, A., & Breu, R. (2016). Data Quality Challenges and Future Research Directions in Threat Intelligence Sharing Practice. ACM Workshop on Information Sharing and Collaborative Security.
- Soto-Mendoza, V., Serrano-Alvarado, P., Desmontils, E., & Garcia-Macias, J. (2015). Policies composition based on data usage context. International Workshop on Consuming Linked Data (COLD2015) at ISWC.
- STIX – https://github.com/oasis-open/cti-stix2-json-schemas
- TeleManagement Forum. (2013). Sharing Threat Intelligence to Mitigate Cyber Attacks. Retrieved 2017, from https://www.edge-technologies.com/system/files/documents/SharingThreatIntelligence_ArchitectureV0.8final.pdf
- Tripwire. (2014). Tripwire Webpage https://www.tripwire.com/state-of-security/security-data-protection/cyber-threat-intelligence/
- Vasek, M., Weeden, M., & Moore, T. (2016). Measuring the Impact of Sharing Abuse Data with Web Hosting Providers. ACM Workshop on Information Sharing and Collaborative Security.
- VERIS - http://veriscommunity.net/schema-docs.html
- Wagner, C., Dulaunoy, A., Wagener, G., & Iklody, A. (2016). MISP-The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform. WISCS.
- Webroot. (2014). Threat Intelligence: What is it, and how can it protect you from today's advanced cyber-attacks? Webroot.
- Willis, B. (2012). Sharing Cyber-Threat Information: An Outcomes-based Approach. Intel Corporation.
- Zeleny, M. (2005). Human Systems Management: Integrating Knowledge, Management and Systems. World Scientific, 15–16.
- Zhao, W., & White, G. (2012). A collaborative information sharing framework for community cyber security. Technologies for Homeland Security (HST).
- Zins, C. (2007). Conceptual Approaches for Defining Data, Information, and Knowledge. Journal of the American Society for Information Science and Technology, 58(4), 479–493.

This project has received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

Dr Jassim Happa, Research Fellow

Dept. of Computer Science, University of Oxford

jassim.happa@cs.ox.ac.uk

PROTECTIVE

PROACTIVE RISK MANAGEMENT

https://protective-h2020.eu/