Proactive Risk Management through Improved Situational Awareness

PROTECTIVE

PROACTIVE RISK MANAGEMENT

https://protective-h2020.eu/

PROTECTIVE is a H2020 funded Innovation Action to ***evolve cyber alert flow processing****, namely:*

- *correlation,*
- *prioritisation,*
- *analysis,*
- *visualisation,*
- *sharing,*

into effective solutions integrated into existing security toolsets for Computer Security Incident Response Teams (CSIRTs) .

PROTECTIVE
PROACTIVE RISK MANAGEMENT

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

Content

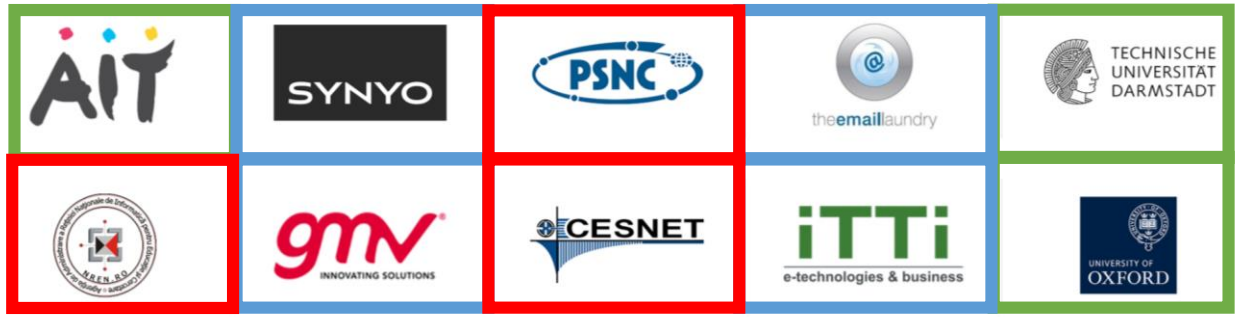
Project Details

PROTECTIVE
PROACTIVE RISK MANAGEMENT

Consortium

Innovation Action:

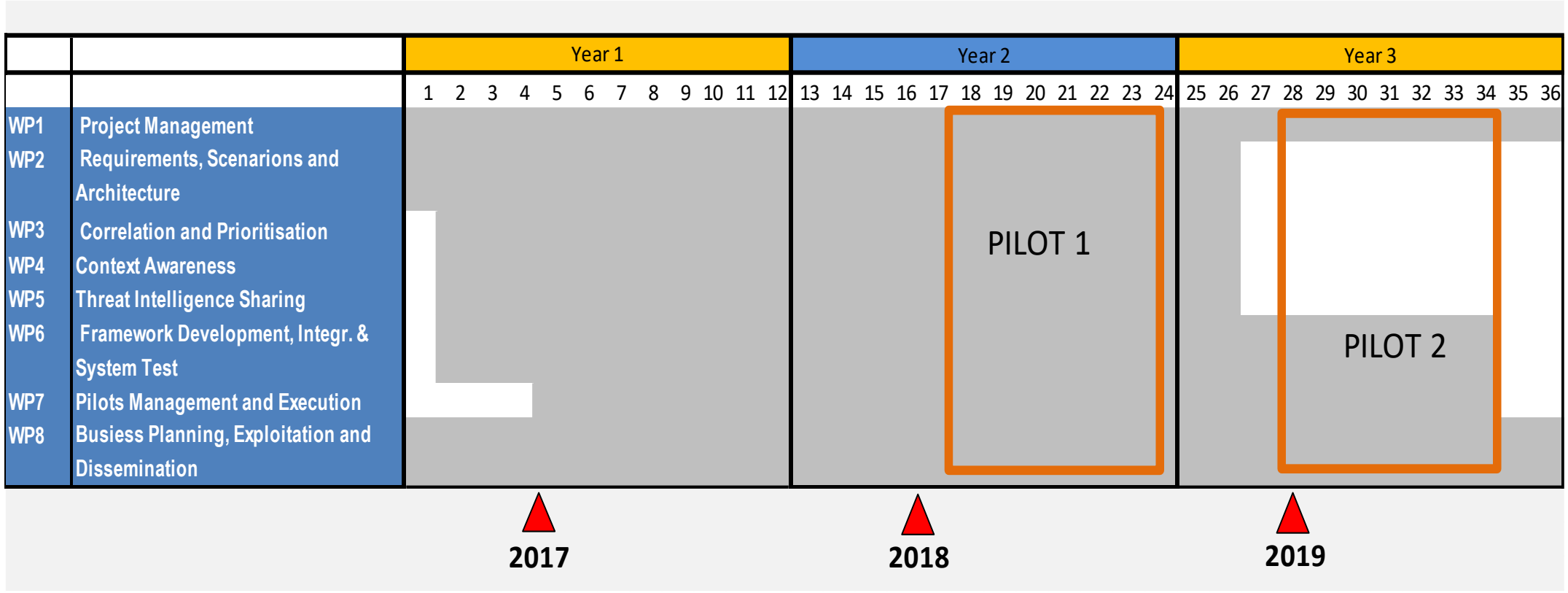
- 36 month duration
  - Sept 2016 – Aug 2019
- 10 partners:
  - 3 academic partners
  - 4 industry partners
  - 3 NREN (National Research & Educational Network) partners
- 8 countries: Ireland, UK, Poland, Austria, Germany, Spain, Czech Republic, Romania



PROTECTIVE
PROACTIVE RISK MANAGEMENT

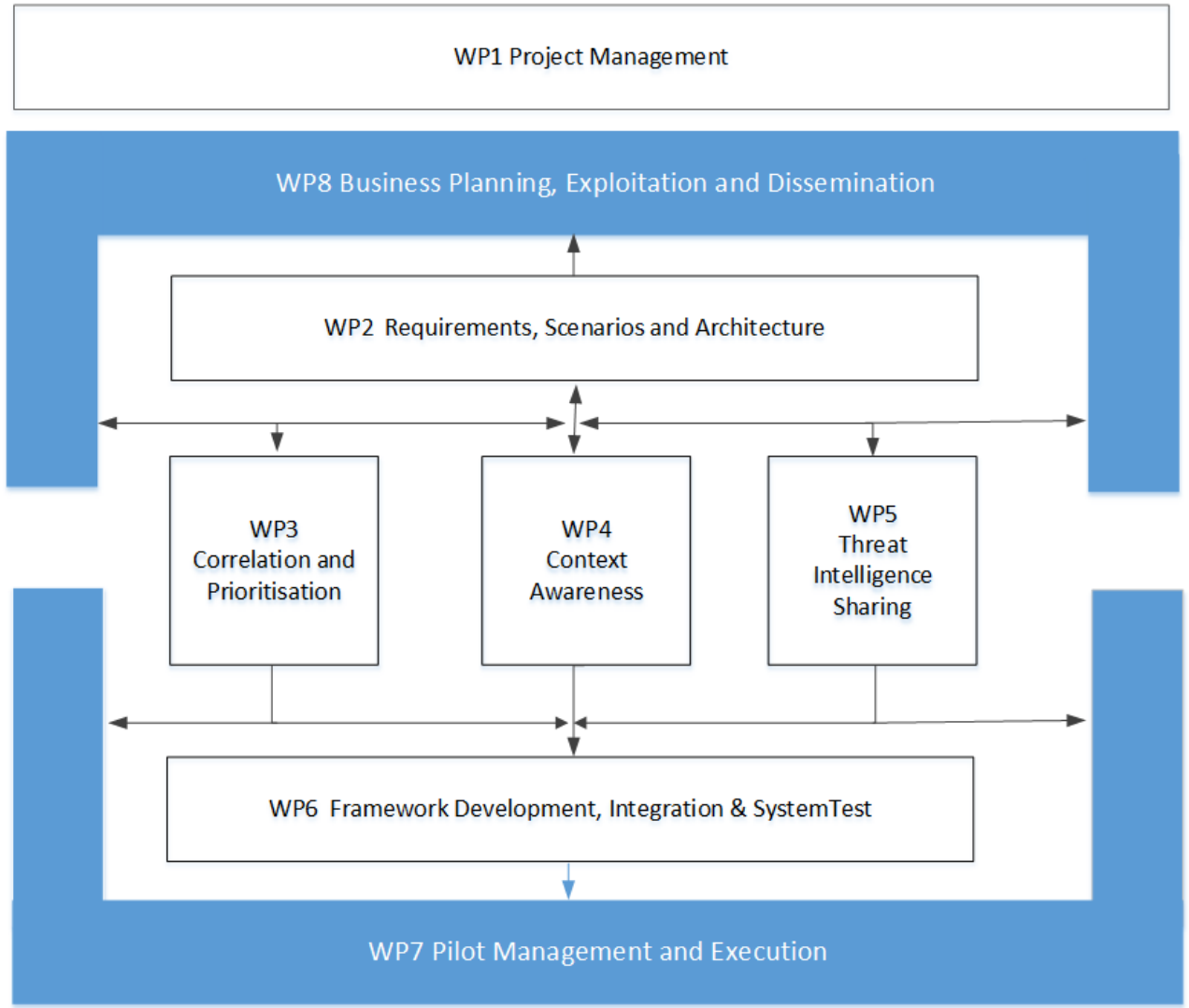
European Commission

Time-plan



PROTECTIVE
PROACTIVE RISK MANAGEMENT

Work plan



PROTECTIVE
PROACTIVE RISK MANAGEMENT

European Commission

Content

Motivation and Challenges

PROTECTIVE
PROACTIVE RISK MANAGEMENT

PROTECTIVE motivation> “Detect, SHARE, Protect”

- Make existing tools interoperable and promote the use of standards for data exchange
- Enhance the functionality of existing tools as regards:
  - Correlation engines for alert analysis
  - Automatic prioritisation of security alerts
  - Improved threat intelligence sharing
  - Advanced analytics and visualisation for massive numbers of alerts

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)

PROTECTIVE
PROACTIVE RISK MANAGEMENT

European Commission

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 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 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?
  - Requirements analysis: Going from legal speak to tech speak is difficult.

PROTECTIVE
PROACTIVE RISK MANAGEMENT

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

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 threat intelligence with SMEs
- Situational Awareness**:** 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"

PROTECTIVE
PROACTIVE RISK MANAGEMENT

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.

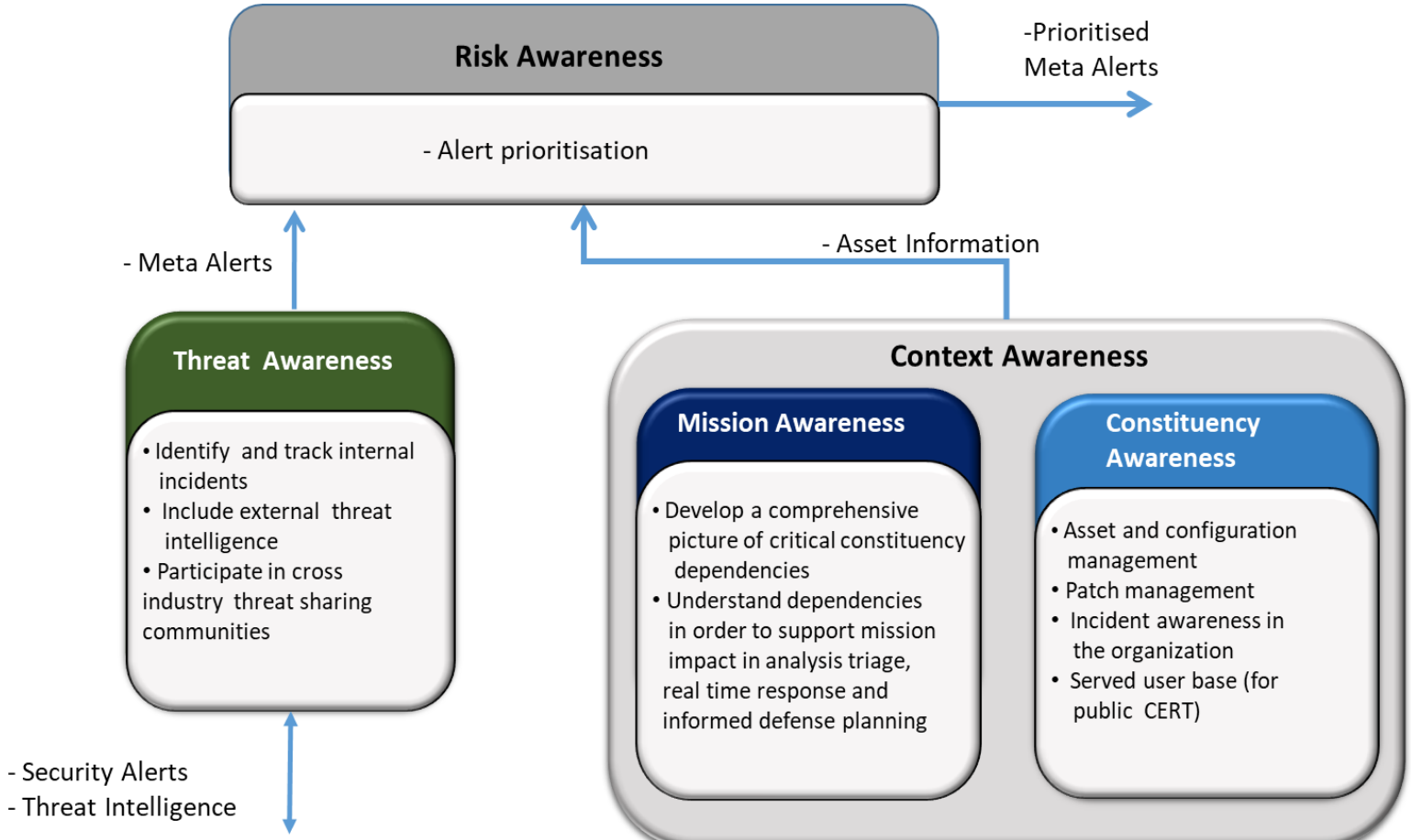
European Commission

PROTECTIVE approach-> situational awareness

Information Security Situational Awareness -
"Within a volume of time and space, the

- perception of an enterprise's threat environment and its security posture; the
- comprehension/meaning of both taken together (i.e. risk) and the
- projection of their status into the near future"

NIST IR 7298 Revision 2,
Glossary of Key Information Security Terms



(adapted from Mitre Corporation)

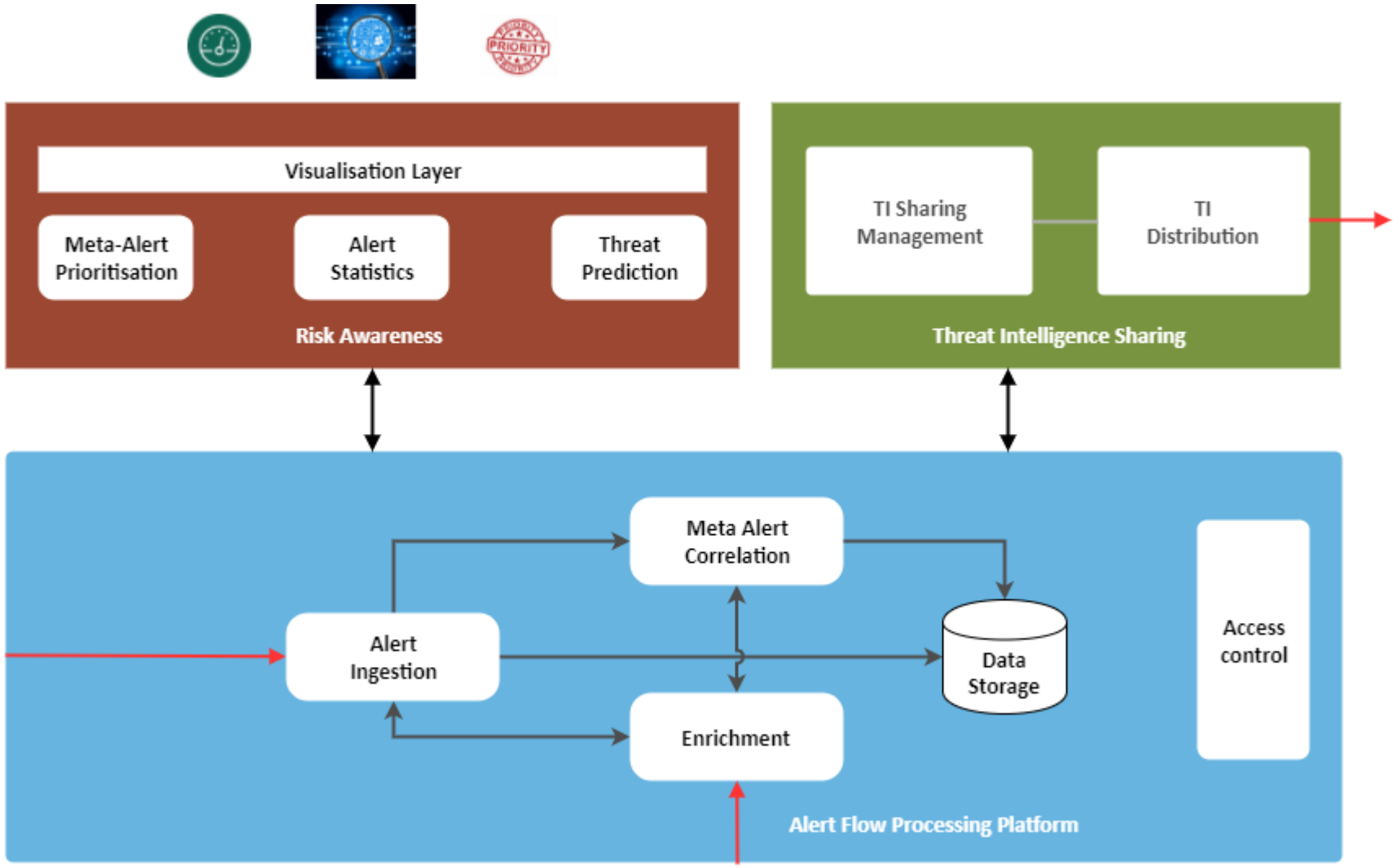
PROTECTIVE
PROACTIVE RISK MANAGEMENT

European Commission

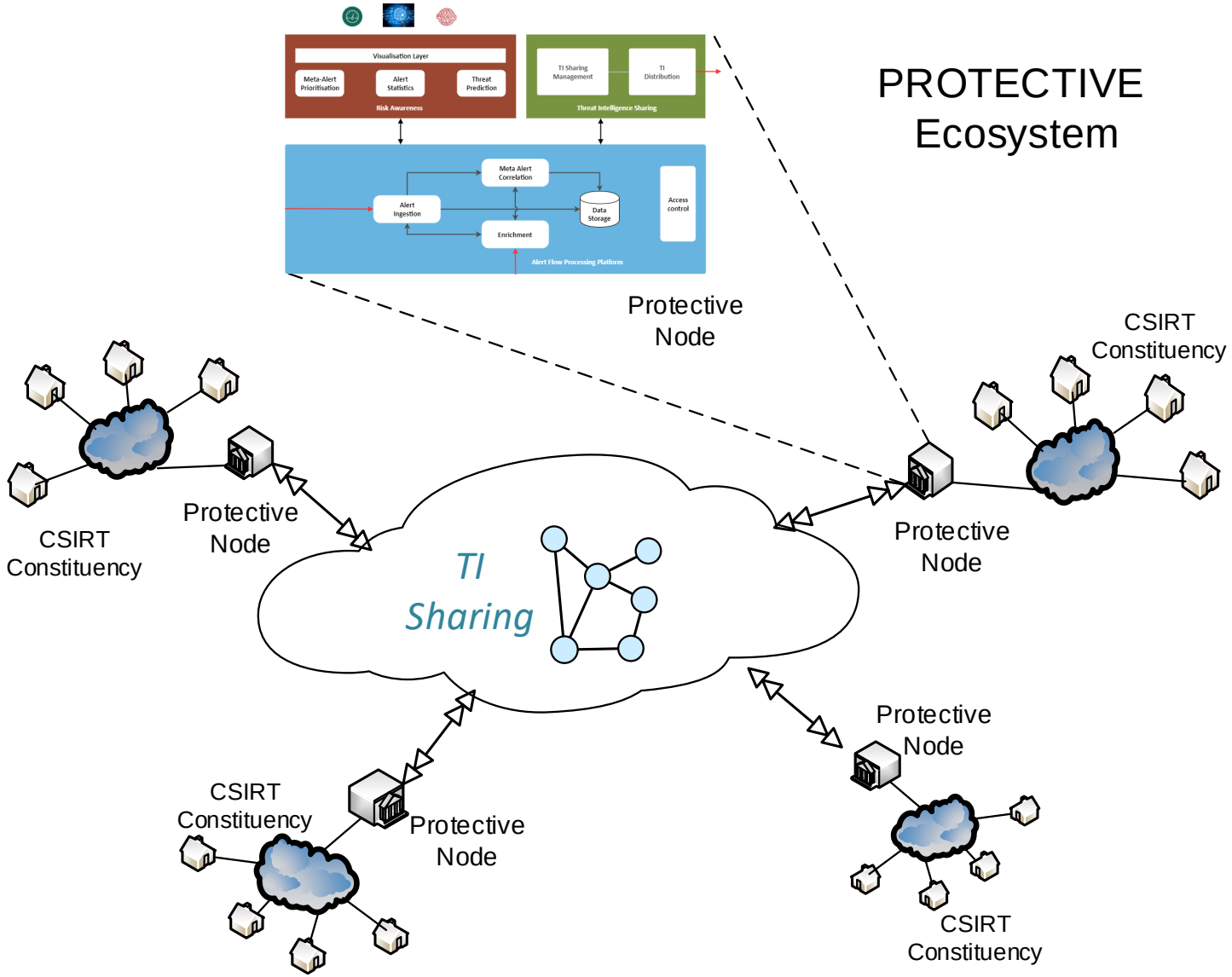
Goals

- 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!)

PROTECTIVE system



PROTECTIVE ecosystem



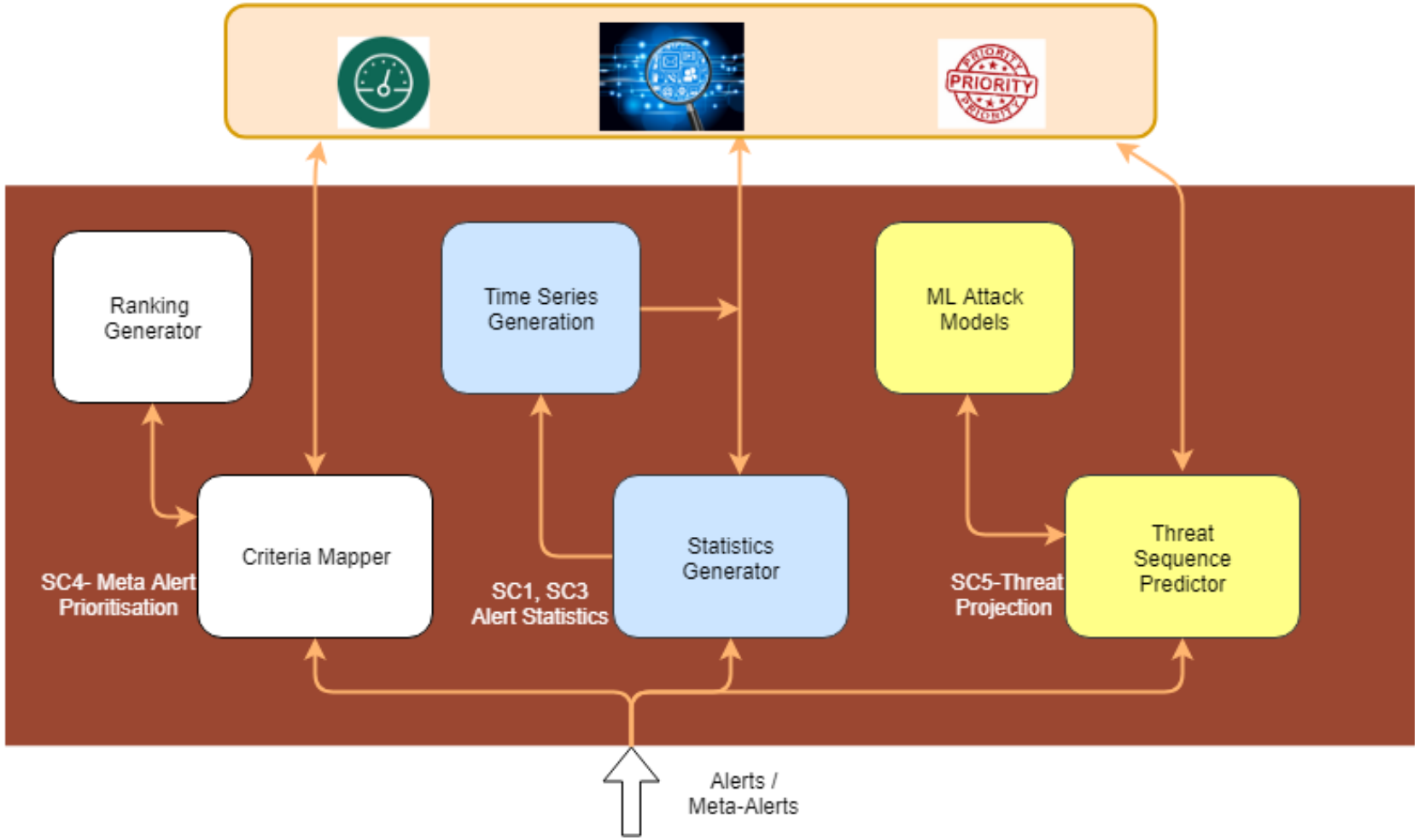
PROTECTIVE
PROACTIVE RISK MANAGEMENT

Content

Risk Awareness

PROTECTIVE
PROACTIVE RISK MANAGEMENT

Risk awareness



PROTECTIVE
PROACTIVE RISK MANAGEMENT

European Commission

Meta alert prioritisation

- Transformation (mapping) of meta-alerts' attributes into criteria by customizable templates supporting temporal (time-dependent) values
- Classification and ranking of meta-alerts based on learned preference model – two possible modes: assignment to preference-ordered classes or full ranking (meta-alerts also ranked inside classes)
- Multiple criteria considered at the same time – MCDA approach
- Learning based on data-sets provided by individual operators
  - Reference ranking / Assignment of criterial vectors (describing meta-alerts) to preference-ordered classes
- Dominance-based rough-set approach (DRSA) applied to deal with inconsistencies
- Interpretable preference model in form of DRSA decision rules

Alert statistics

- Predefined views to provide overview
- Fully-customizable dashboard by user to focus on particular dataset
  - Multiple relevant views on alerts and meta-alerts
  - Status of reporting nodes
  - Extendable with new views as new data (enriched) appear in database
- Timeseries to observe trends in data
- Simple anomaly detection in time series using EWMA and deviation
  - Parameters set by user

Threat projection

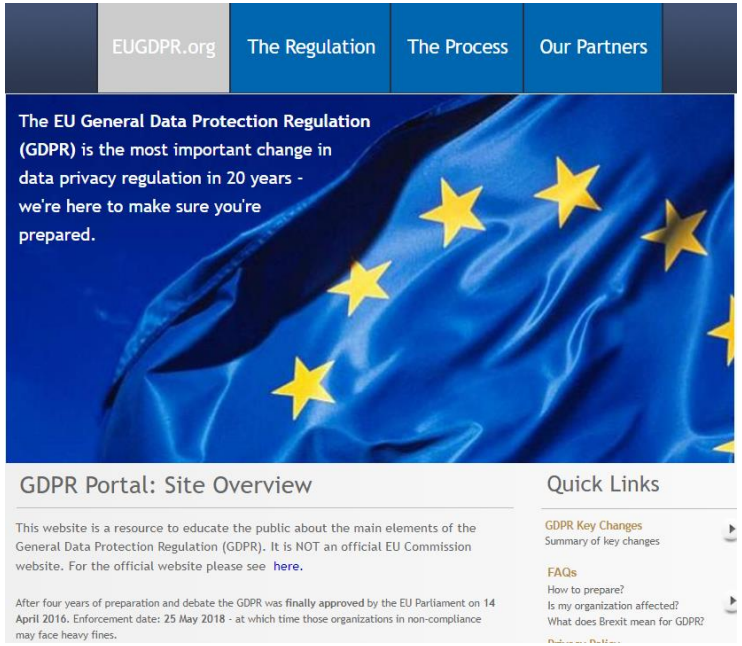
- Identify multi-stage attacks using sequential analysis
  - the sequential patterns are used to create models of attackers behaviour
  - can be used to predict future attacks if partial match found form current alerts
- Attack prediction using association rule mining
  - generates rule to predict next step
  - associates confidence level with rule
- Attack prediction using deep learning LSTM based approach
  - builds on language processing techniques

Content

Threat Intelligence Sharing

Emerging concerns in sharing threat intelligence

- GDPR/NDA - “What the baseline?”
  - GDPR not written with cyber threat intelligence in mind
- GDPR/NDA -“How do I know I meet legal specifications?”
  - 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.



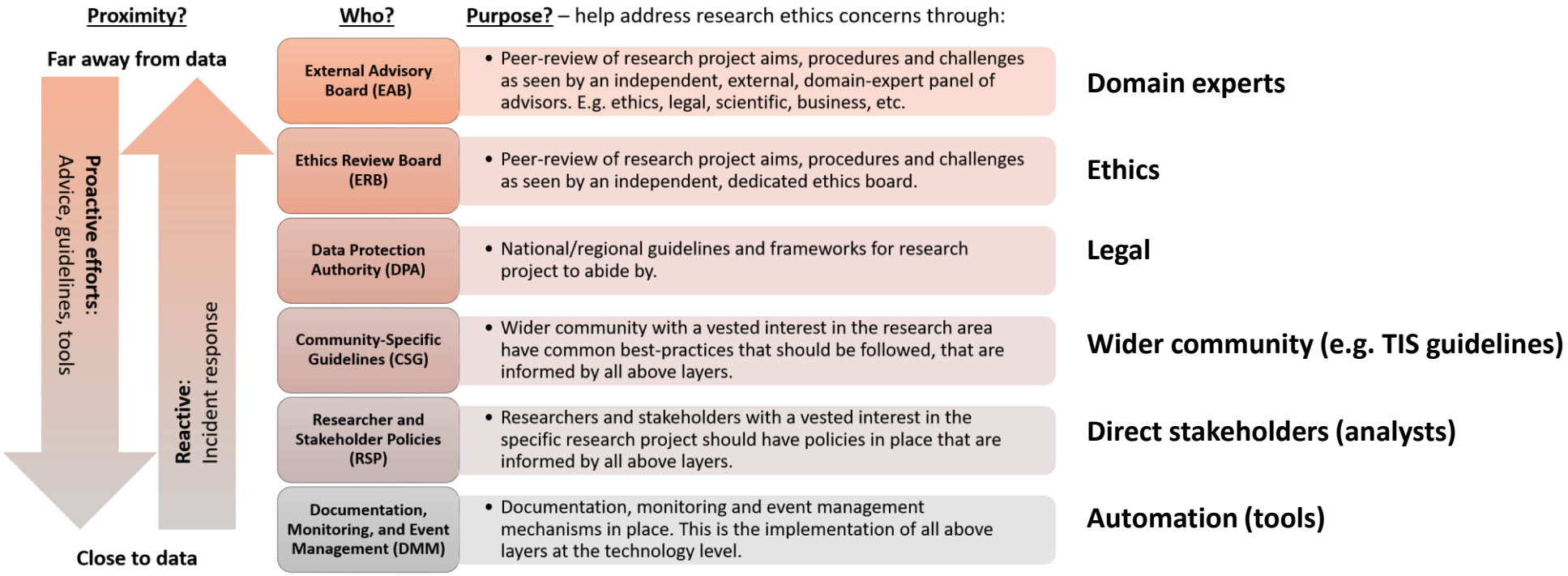
https://www.eugdpr.org/

PROTECTIVE
PROACTIVE RISK MANAGEMENT

European Commission

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!

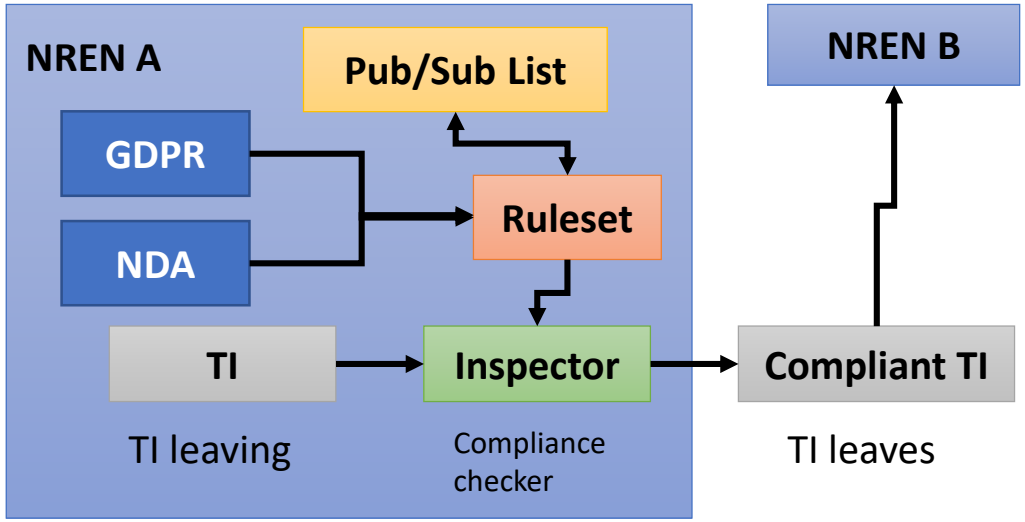


PROTECTIVE
PROACTIVE RISK MANAGEMENT

European Commission

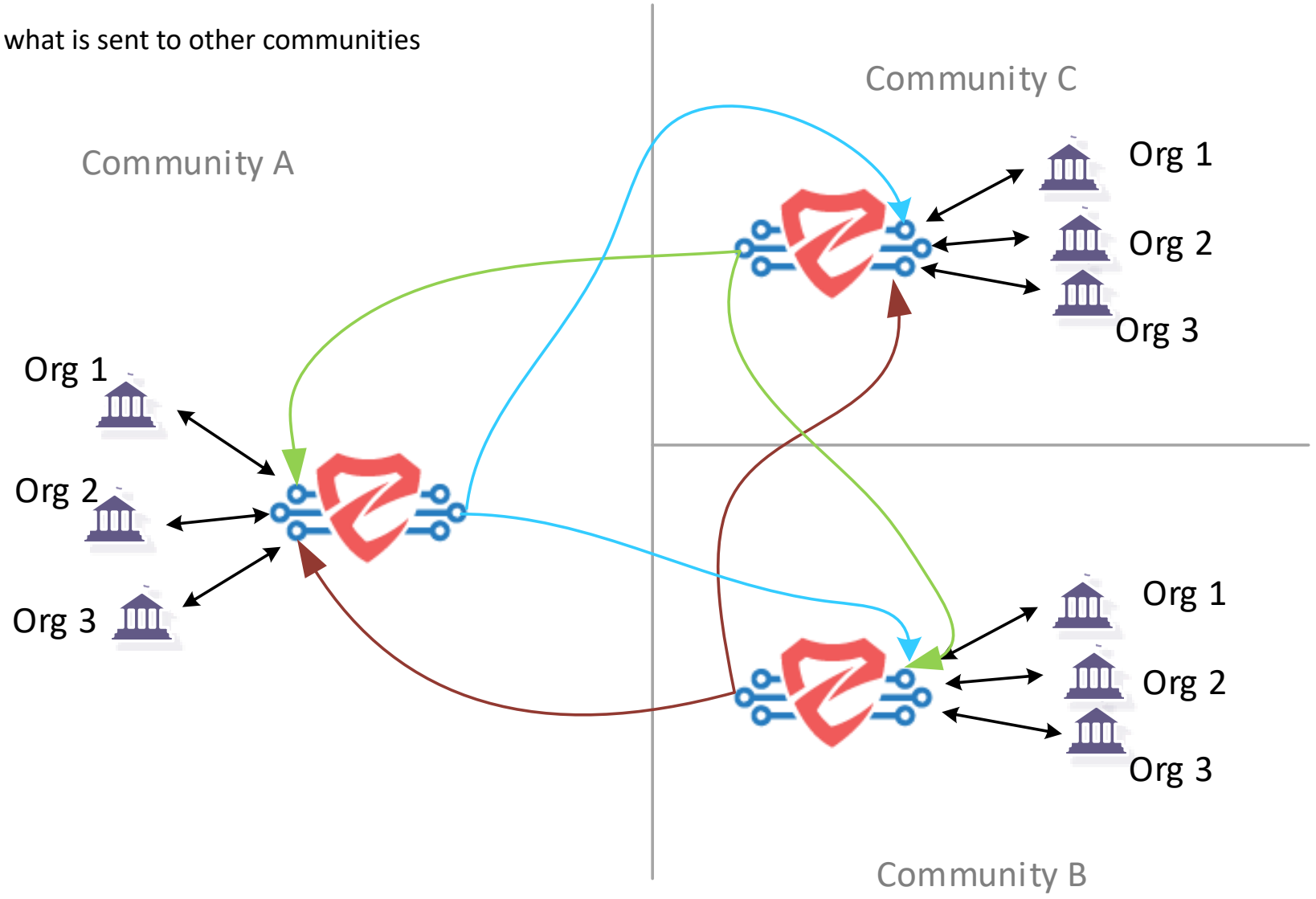
Sharing cyber threat intelligence

- CTI Sharing Compliance rules:
  - **Who am I <u>allowed to</u> share the TI with?** NOTE: separate from – “who can I share with?”
    - Filtering on top of a share (pub/sub-like) model
  - **What TI am I <u>allowed to</u> share?** NOTE: separate from – “what is available to share?”
    - Anonymisation/Pseudonymisation/Aggregation data



TI Sharing – p2p sharing architecture

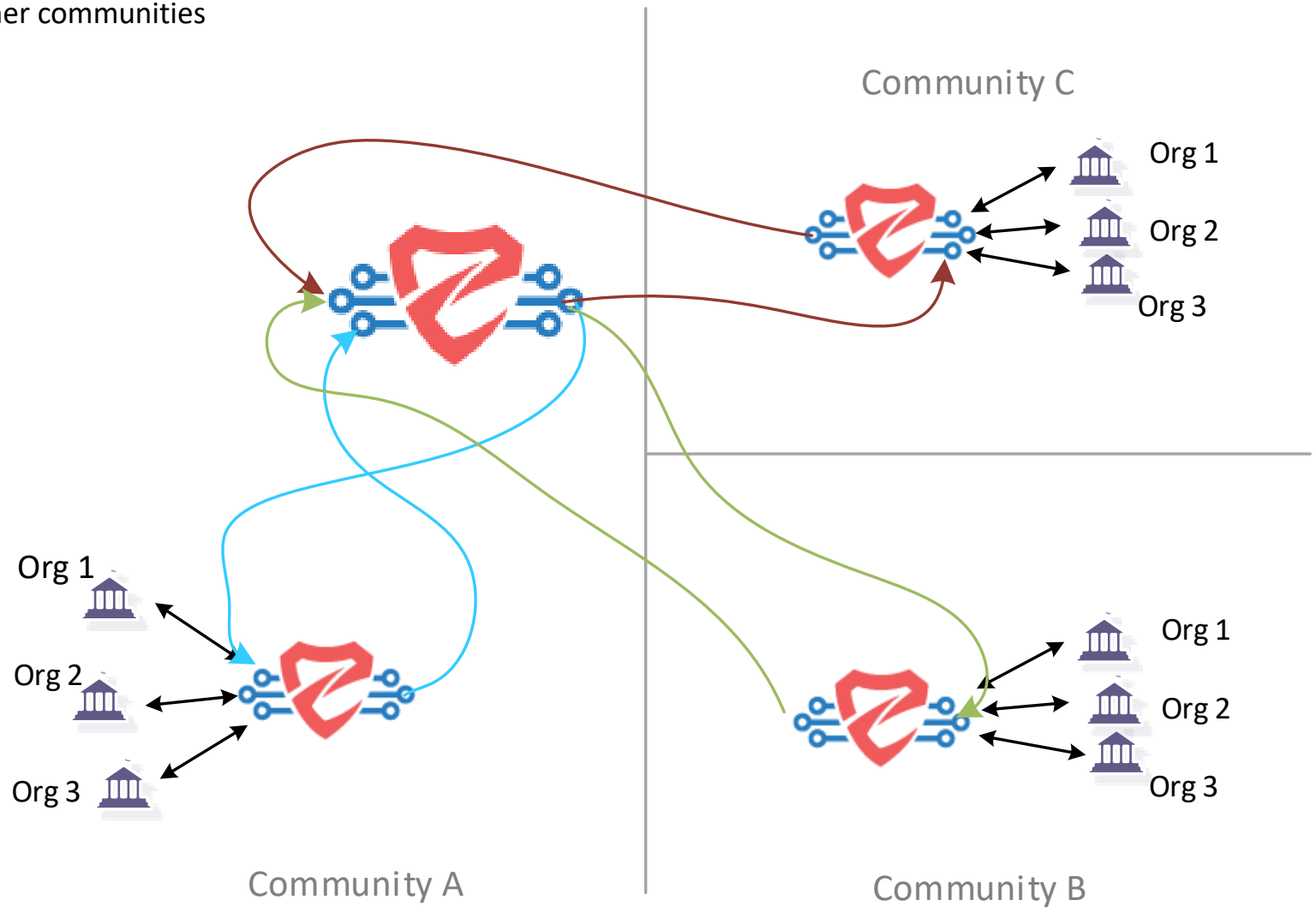
Community controls what is sent to other communities



PROTECTIVE
PROACTIVE RISK MANAGEMENT

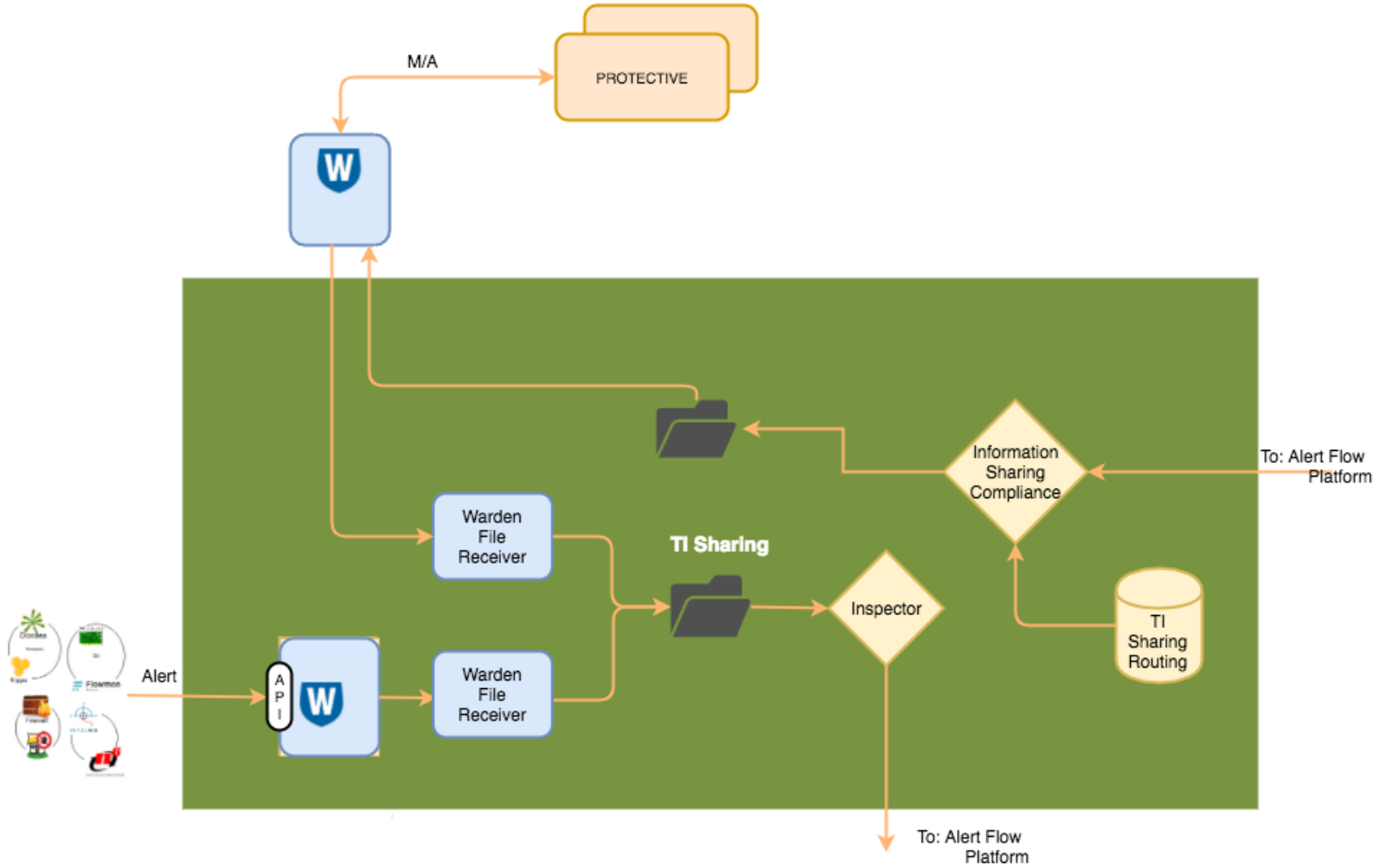
TI Sharing – centralised sharing architecture

Community controls what is sent central server but not what is sent to other communities



PROTECTIVE
PROACTIVE RISK MANAGEMENT

TI sharing –PROTECTIVE system



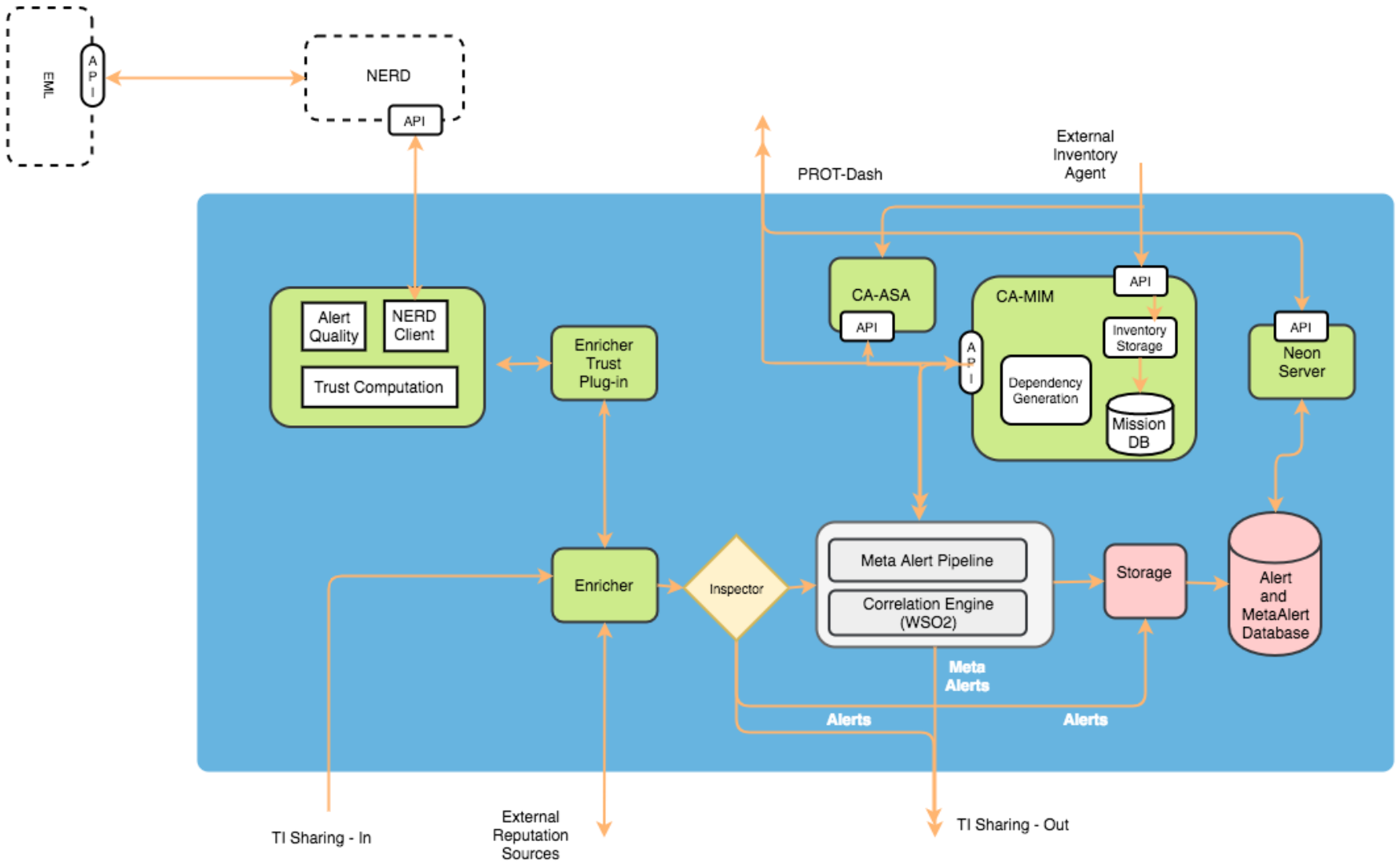
Text

Content

Alert Processing

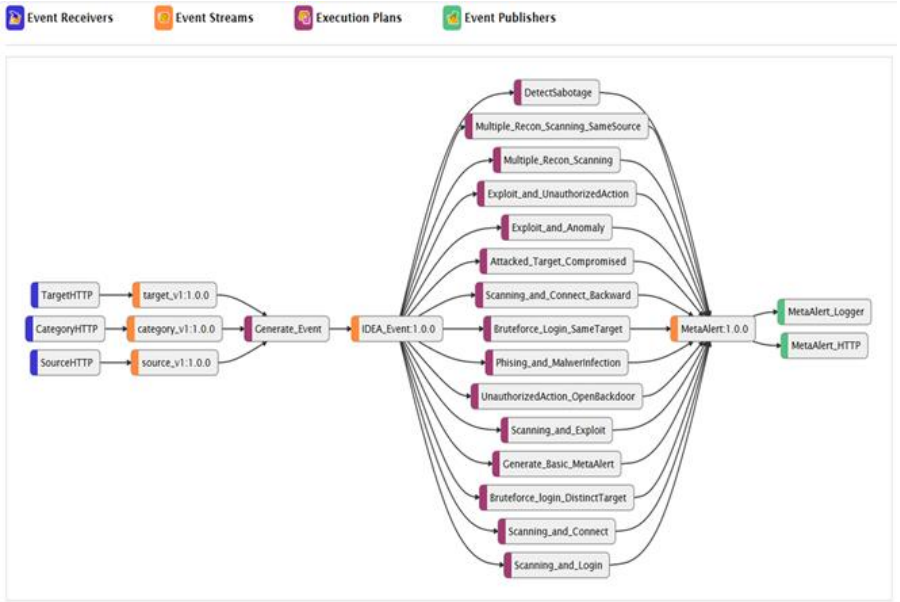
PROTECTIVE
PROACTIVE RISK MANAGEMENT

Alert processing



Meta-alert correlation

- Correlated based on source and target IP address
- Alerts correlation based on time window.
- Rule-based correlation strategy to detect known attack scenarios.
- Generate Meta-alerts from existing Meta-alerts, based on time window.

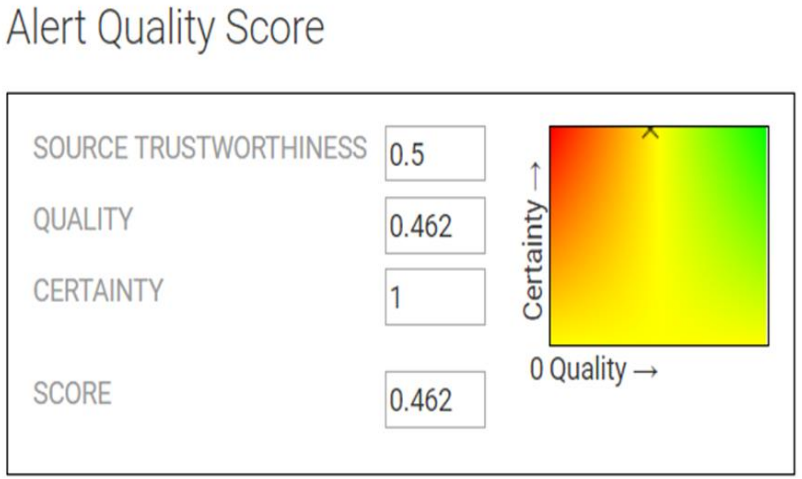


This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 700071. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained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

Alert trust

The Alert Trust module takes the following into account for calculating a **quality** score:

- **IP Recurrence (IPR):** how often have we seen the IP address of the attacker?
- **Source Relevance (SR):** how reliable is the detector? how likely is that the detector produced a false positive
- **Attack Freshness (AF):** how fresh (i.e., new) is the alert?
- **Completeness (C):** Are any important fields (e.g., the port number or the protocol) missing?



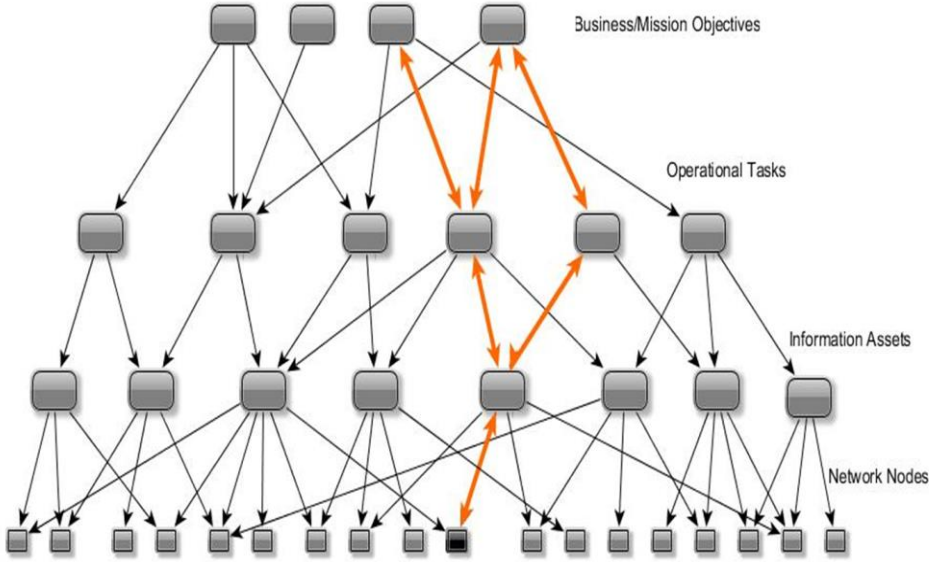
PROTECTIVE
PROACTIVE RISK MANAGEMENT

Context Awareness

- Develop a comprehensive picture of critical constituency dependencies and asset configurations.

  Link

  - business objectives/missions to:
  - business processes/services to:
  - computing infrastructure
- Understand dependencies in order to support
  - alert analysis triage,
  - real time response
  - informed defense planning



PROTECTIVE
PROACTIVE RISK MANAGEMENT

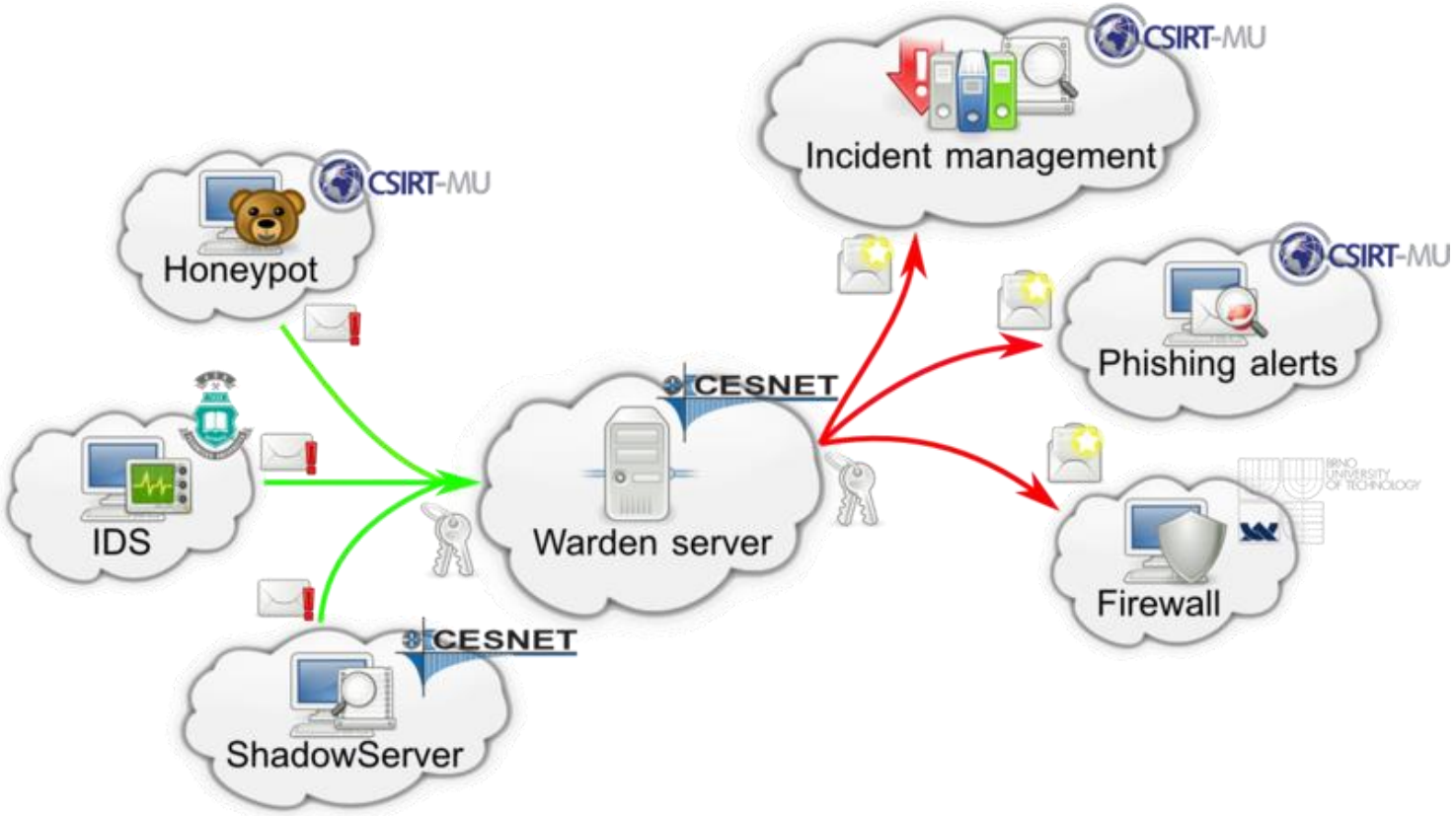
European Commission

Content

Existing Tools

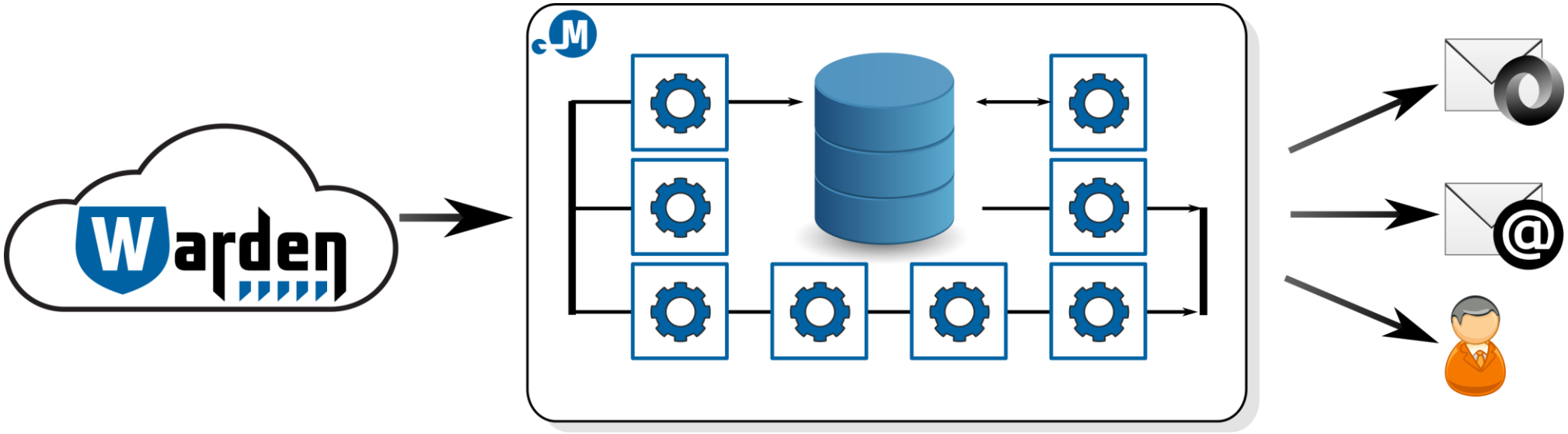
PROTECTIVE
PROACTIVE RISK MANAGEMENT

Warden



https://warden.cesnet.cz/en/architecture

Mentat



https://mentat.cesnet.cz/en/index

Content

Pilots

PROTECTIVE
PROACTIVE RISK MANAGEMENT

Pilots

- **Pilot 1: Internal focus with consortium developers**
  - Jan 2018 - August 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)

Content

Conclusions

PROTECTIVE
PROACTIVE RISK MANAGEMENT

Conclusions

- PROTECTIVE is an EU international collaborative research project
- PROTECTIVE will contribute to cyber crime prevention by developing
  - a correlation engine for cyber incident analysis
  - platform for improved threat intelligence sharing
  - advanced analytics and visualisation for massive numbers of incidents
  - constituency context awareness system to enable..
  - automated security alert prioritisation based on operator preferences
- PROTECTIVE will validate the projects outputs through a multi-partner threat intelligence sharing pilot involving NRENs and SME
- PROTECTIVE will provide an open source cyber threat management platform for further exploitation by the cyber-defense community.

PROTECTIVE
PROACTIVE RISK MANAGEMENT

European Commission

Questions?

www.protective-h2020.eu

- Contact us:

  info@protective-h2020.eu

  @ProtectiveH2020

PROTECTIVE
PROACTIVE RISK MANAGEMENT

European Commission

PROTECTIVE

PROACTIVE RISK MANAGEMENT

https://protective-h2020.eu/