cyberwatching.eu
The European watch on cybersecurity & privacy

Wi-fi: MARRIOT_CONFERENCE
EVENT06

cyberwatching.eu 2nd Concertation Meeting

#Concertation19

04 June 2019
Brussels, Belgium

www.cyberwatching.eu | www.twitter.com/cyberwatchingeu

cyberwatching.eu
The European watch on cybersecurity & privacy

2nd Concertation Meeting

#Concertation19

04 June 2019

Brussels, Belgium

www.cyberwatching.eu | www.twitter.com/cyberwatchingeu

Wi-fi: MARRIOT_CONFERENCE EVENT06

Break-out 3: Emerging Cybersecurity challenges from emerging technologies

Chair: Roberto Cascella, ECSO WG6 SRIA & Cyber Security Technologies

Participants
Break-out 3: Emerging Cybersecurity challenges from emerging technologies

Name, Project	
Sanja Budimir, COCOON	François Koeune, REASSURE
Mirko De Maldè, MH-MD	Paul Koster, SODA
Tom De Wasch, Privacy&Us	Adam Kozakiewicz, SISSDEN
JC ROBERT DelHaye	Evangelos Markatos, REACT
Gabi Dreo, CONCORDIA	Evangelos Markatos, PROTASIS
Konstantinos Giannoutakis, FORTIKA	Edmundo Monteiro, POSEIDON
Seda Goksu, FP7	Haris Mouratidis, DEFEND
Anna-Louise Grensing, KASTEL	Mary Pidgeon, PROTECTIVE
Kostas Kalaboukas, BPR4GDPR	

COCOON

https://cocoon-project.eu/

Dr. Sanja Budimir
Ghent University
Belgium

Emotion psychology meets cyber security in IoT smart homes

Emotion Appraisals and Action Tendencies*

Proactive	Destructive
Active solution search	Attack / Withdraw
Effective (protection, solution strategy)	Not effective (unknown target / stop using)
Problem focused	Emotion Focused
Short-term consequences (negative emotions)	Long-term consequences (anxiety, depression...)
Education	Tailored approach

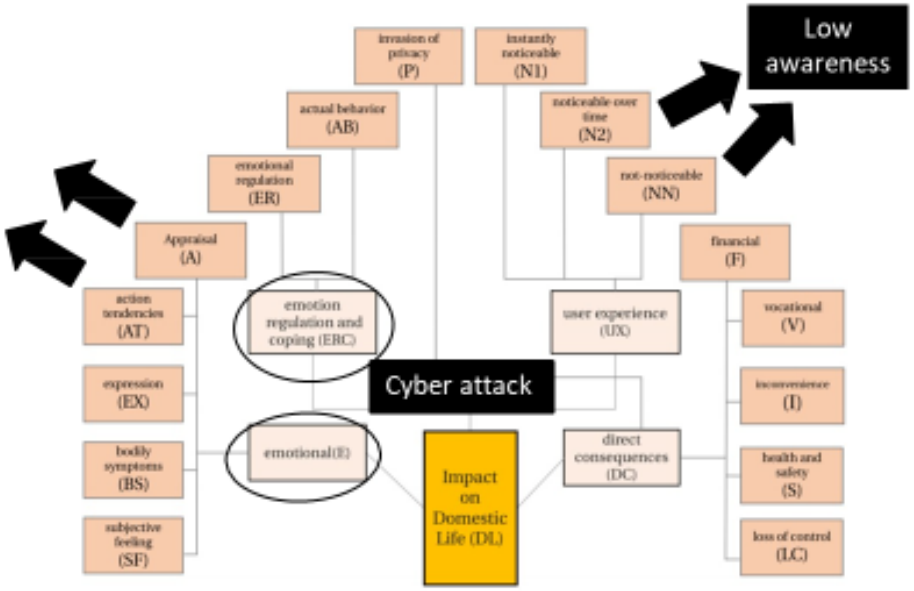


Figure 4: Impact on domestic life taxonomy criteria **

* Budimir, S., Fontaine, J.R.J., Roesch, E.B. (preparation for submission). Emotion psychology meets cyber-security: Victims' emotional experiences due to cybersecurity breach on their devices and accounts.

** Heartfield, R., Loukas, G., Budimir, S., Bezemskij, A., Fontaine, J. R., Filippoupolitis, A., & Roesch, E. (2018). A taxonomy of cyber-physical threats and impact in the smart home. Computers & Security.

Cocoon is an international research Consortium, funded by the EU FP7 CHIST-ERA funding scheme.

University of Reading | University of Greenwich | ETH zürich | Ghent University | TU/e Eindhoven University of Technology

Privacy&Us – Privacy & Usability – https://privacyus.eu

Train creative, entrepreneural and innovative ESRs able to face current and future challenges in the area of privacy and usability

ESRs will be supported by an international, multidisciplinary, intersectoral consortium that combines academic and non-academic perspectives

- Computer Science:
- Engineering:
- Information Systems:
- Psychology:
- Design & Media:
- Social Sciences:
- Economy:
- Law

FORTIKA

Cyber Security Accelerator for trusted SMEs IT Ecosystems

16 participants from
9 EU countries

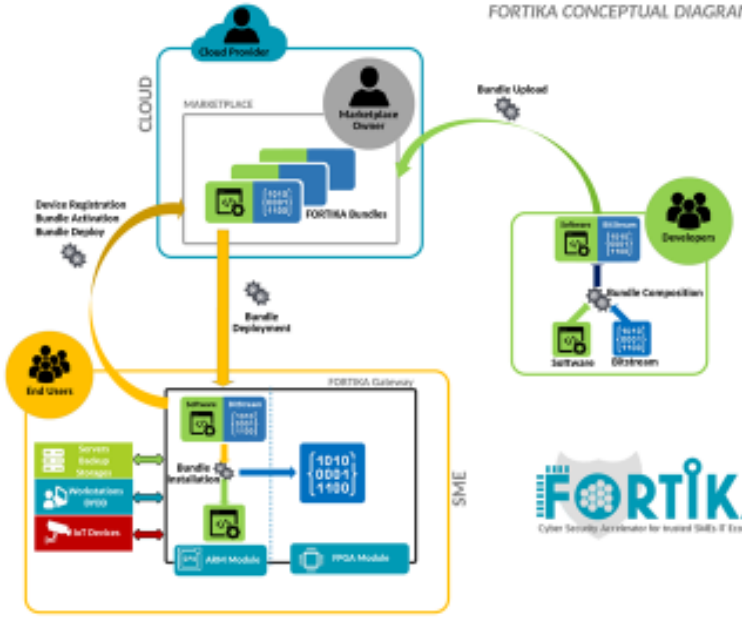
*...adopts a **security-by-design** hybrid approach that integrates **HW & SW** with **business needs** & **behavioural patterns** at individual and organisational level*

...aims at:

- **minimizing the exposure** of SMEs to cyber security risks & threats
- **helping them respond to cyber security incidents**
- **relieving** them from all **unnecessary costs** for security solutions

- ...introduces a **HW enabled middleware security layer** as add-on to existing network gateways
- ...introduces of a SW defined **smart ecosystem**, i.e. the "FORTIKA Marketplace", with virtualized security
- ...orients to trusted cyber-security services packaged to tailored solutions for enterprises
- ...deploys a **resilient overall cybersecurity solution** that:
  - ✓ accommodates **security intelligence**
  - ✓ encourages security-friendly **behavioural & organisational changes**
  - ✓ can be **easily tailored** and **adjusted** to the versatile & dynamically changing needs of SMEs
  - ✓ re-uses the **existing service & product portfolio** of security solution providers across Europe

FORTIKA CONCEPTUAL DIAGRAM



Pilot 1: **A mobile marketing firm** (MOTIVIAN - BG)

Pilot 2: **A electrical vehicle manufacturer** (ALKE - IT)

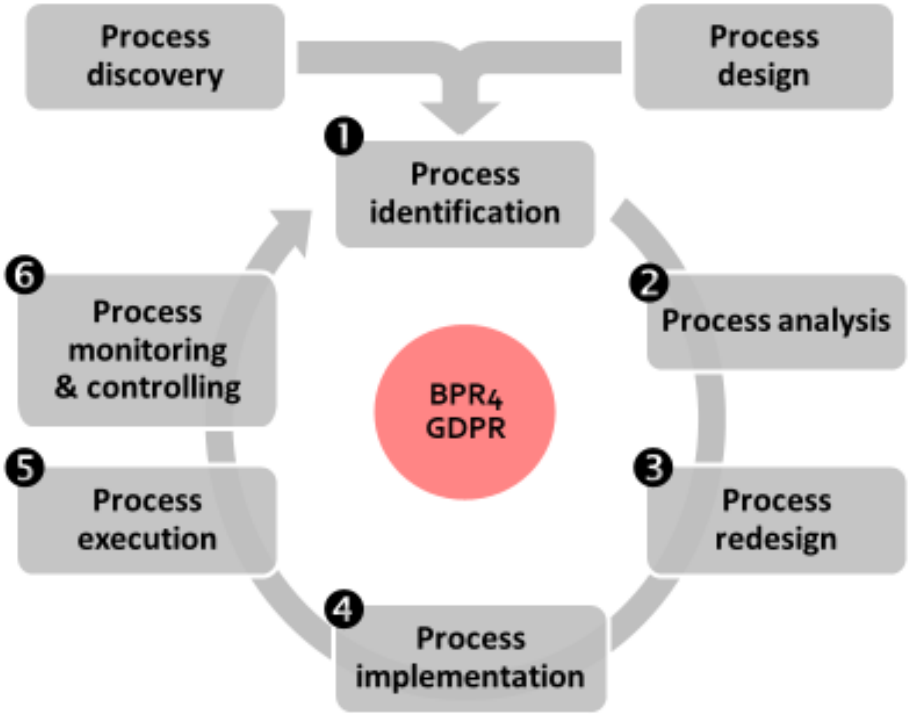
Pilot 3: **A software house** (NEMETSCHEK - BG)

Pilot 4: **An SME specialized in security** (Obrela Security Industries Ltd.- UK)

Pilot 5: **An energy management SME** (Wattics Ltd. -IE)

BPR4GDPR: Business Process Re-engineering and functional toolkit for GDPR compliance

- ✓ Automatic process re-engineering to become compliant by design
- ✓ Tools covering the full lifecycle of process identification, analysis, execution and control
- ✓ Policy-based framework governance conceived on the basis of GDPR
- ✓ Mechanisms for offering Compliance-as-a-Service



H2020 project 731591
http://www.reassure.eu/

REASSURE

- Topic: side-channel attacks (physical attacks against embedded systems)
- Goal: Improve side-channel assessment & resistance
  - Efficient & reliable processes and tools for specialized labs
  - « Starter kits » for non-experts (IoT…)
  - Standardized methods (ISO, JHAS, ENISA…)
- Main achievements
  - Tutorial « understanding leakage detection » (material available online)
  - Various online tools: leakage simulator, reference traces, protected implementations, online tutorials…
  - Input to standardization bodies
- Visit https://reassure.eu/

SODA Scalable Oblivious Data Analytics

Enable practical privacy-preserving analytics on big data with MPC

technology + legal + users + validation

Despite

- Significant advances in MPC performance and MPC-based machine learning
- Legal analysis: MPC-encrypted data considered de-identified for GDPR
- MPC frameworks & proof of concepts

MPC has challenges to overcome for broad adoption

NASK

SISSDEN – Secure Information Sharing Sensor Delivery Event Network

SISSDEN

~1000 IP addresses
255 nodes

119 ASNs , 58 countries
~2 billion events/year

- CiscoASA,
- Cowrie,
- Conpot,
- Dionaea,
- Elasticpot,
- Glastopf,
- Heralding,
- Honeypy,
- MICROS,
- Spampot,
- Struts,
- Weblogic, ...

Packet capture of incoming traffic
Intrusion detection
Darknet (network telescope)
Partner systems (spamtrap, AmpPot, ...)
Third-party data sources for correlation
Operational botnet tracking
Multiple analytics on the collected data
Long- and short-term sandboxes
Curated reference data set

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700176.
Call H2020-DS-2015-1: „Digital Security: Cybersecurity, Privacy and Trust"
Topic DS-04-2015: „Information driven Cyber Security Management"

CyberDefcon

UNIVERSITÄT DES SAARLANDES

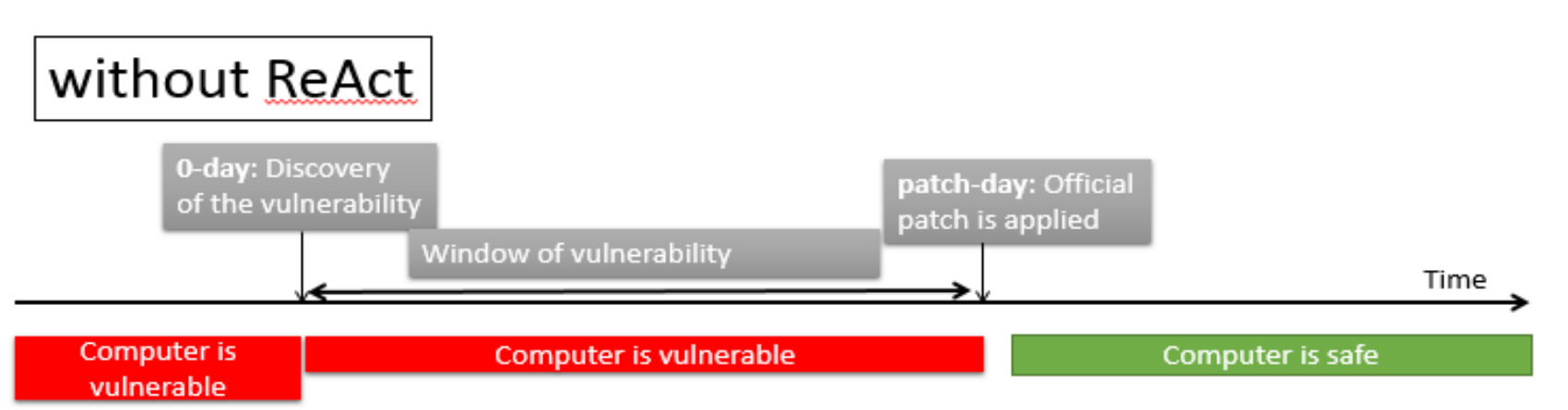
ECLEXYS

Posteitaliane

montimage

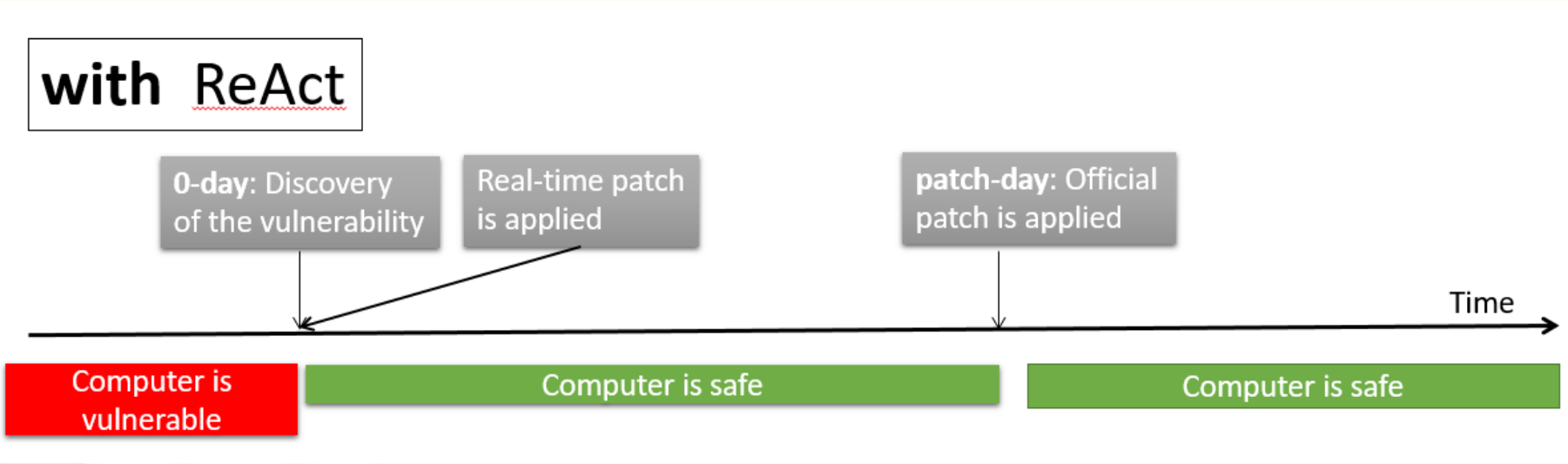
ReAct: What is it about?

- Time line: before and after **ZERO-day**
  - Before the vulnerability is found (i.e. before ZERO-day)
    - Computer is vulnerable
  - Before the patch is applied
    - Computer is vulnerable
- After the patch is applied
  - Computer is safe



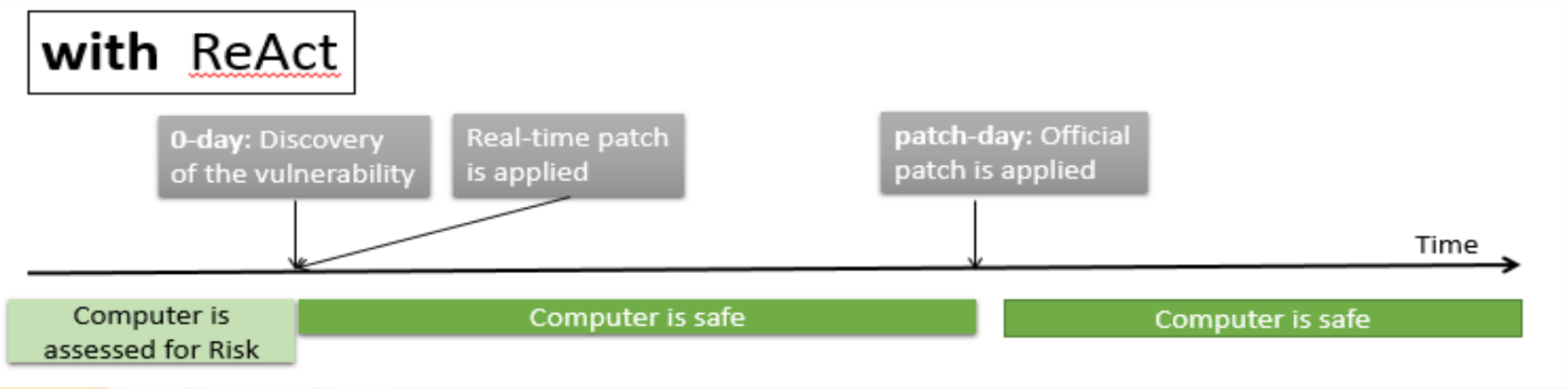
ReAct

- Can we improve the situation?
- Can we do something before the patch is applied?
  - YES!
  - Real-time patch!! (Selective Fortification)
    - Instrumentation, binary re-writing, memory protection, etc. to isolate the bug
    - Note: it does not *remove* the bug – it isolates the bug



ReAct

- Can we do any better?
- *Can we do something before the bug is found???*
  - ???
  - YES!
  - Prediction
  - Predict which computers are more vulnerable to attacks
  - Patch them, monitor them, fortify them, etc.

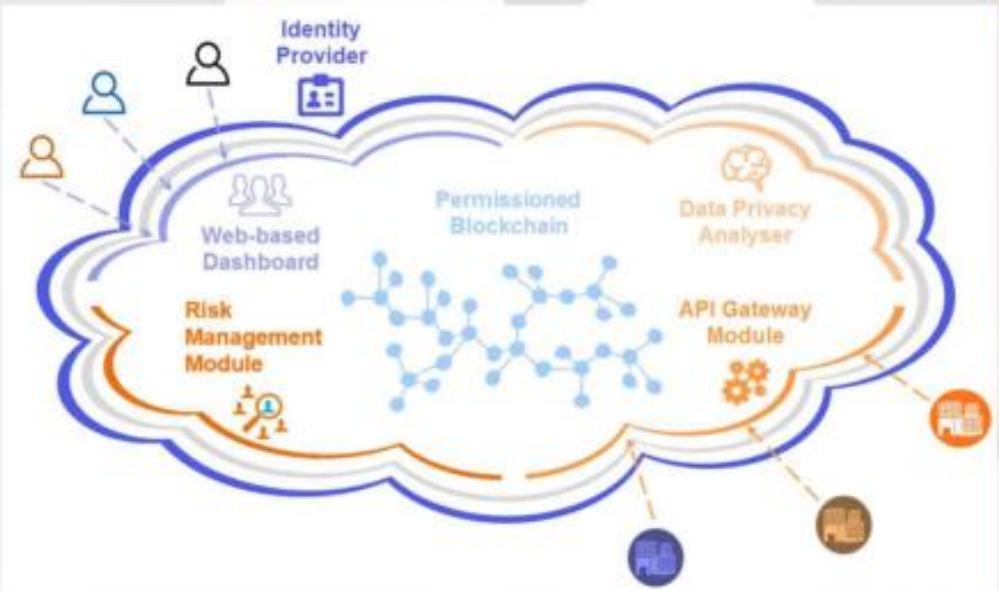


The ReAct project: 2018-2021

- Funded by the European Commission
- Collaboration with
  - Symantec (Leyla Bilge, Petros Efstathopoulos)
  - Ruhr Bochum (Thorsten Holtz)
  - Vrije Universiteit (Herbert Bos)
  - UCY (Elias Athanasopoulos)
  - Eurecom (Davide Balzaroti)

POSEIDON

Funded by Horizon 2020
Framework Programme of the European Union



PoSeID-on aims to deliver an innovative and **scalable platform**, as an integrated and comprehensive solution **aimed to safeguard the rights of data subjects,** exploiting the cutting-edge technologies of **Smart Contracts** and **Blockchain**, as well as support organizations in data management and processing while ensuring **GDPR** compliance.

https://www.poseidon-h2020.eu

Edmundo Monteiro, University of Coimbra
edmundo@dei.uc.pt

Cyberwatching.eu Concertation Meeting
June 4th, 2019, Brussels

DEFeND

DATA GOVERNANCE FOR SUPPORTING GDPR

Deliver an innovative data privacy governance platform, which will facilitate scoping and processing of data and data breach management and will support organisations towards continuous GDPR compliance.

1. Design and development of a successful, **MARKET-ORIENTED, PLATFORM** to support organizations towards GDPR compliance
2. Develop a **MODULAR SOLUTION** that covers different aspects of the GDPR
3. **AUTOMATED** methods and techniques to elicit, map and **ANALYZE DATA** that organizations hold for individuals
4. Advanced modelling languages and methodologies for privacy-by-design and **DATA PROTECTION** management
5. Specification, management and enforcement of **PERSONAL DATA CONSENT**
6. Integrated **ENCRYPTION AND ANONYMIZATION** solutions for GDPR
7. **DEPLOYMENT** and **VALIDATION** of the DEFeND platform in real operational environments

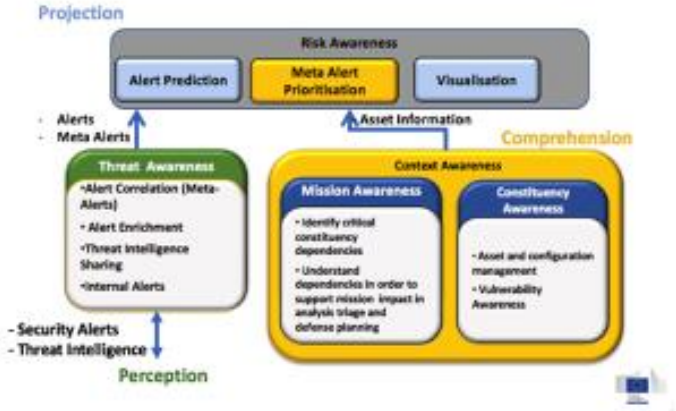
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 787068.

PROTECTIVE
PROACTIVE RISK MANAGEMENT

cyberwatching.eu
The European watch on cybersecurity & privacy

- TI Situational Awareness

Sensors, TI
Sharing
Perception
Comprehension
Projection



- **Join** NRENs, MSSP Community or **Build** your own SME Sectors, Enterprise, CI
- M34: Open-source: Extendable: Alert formats IDEA, MISP, STIX
- https://protective-h2020.eu/pilot/ @ProtectiveH2020 Mary Pidgeon

PROTECTIVE

Cyberwatching.eu Concertation Meeting – 4th June 2019