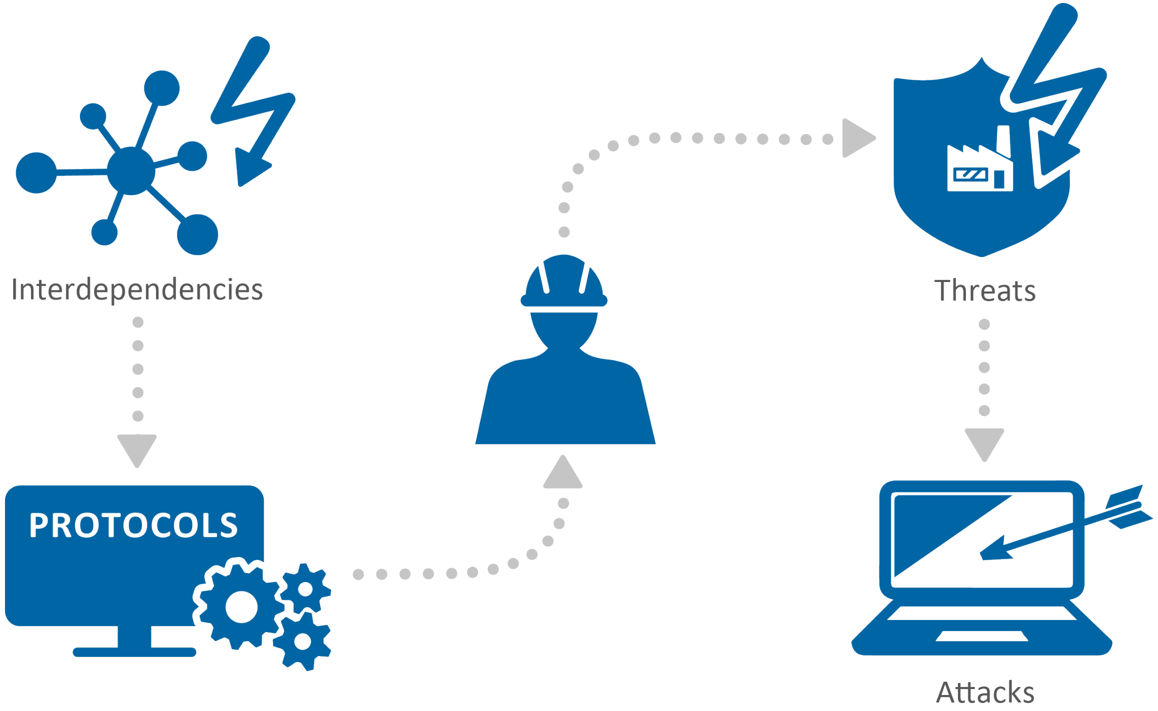
Securing Europe’s information society: bridging the gap between industry, security community and Member States

Rossella Mattioli, CSIRTs relations team

European Union Agency for Network and Information Security

ENISA 101



Securing Europe’s Information society

https://www.enisa.europa.eu/

Expertise

- Cloud and Big Data
- Critical Infrastructures and Services
- CSIRT Services
- CSIRTs and communities
- CSIRTs in Europe
- Cyber Crisis Management
- Cyber Exercises
- Cyber Security Education
- Data Protection
- Incident Reporting
- IoT and Smart Infrastructures
- National Cyber Security Strategies
- Standards and certification
- Threat and Risk Management
- Trainings for Cyber Security Specialists
- Trust Services

https://www.enisa.europa.eu/topics

Community

EUROPEAN CYBER SECURITY MONTH

https://cybersecuritymonth.eu/

EUROPEAN CYBER SECURITY CHALLENGE

Evil prevails when good humans do nothing!

https://www.europeancybersecuritychallenge.eu/

CYBER SECURITY TRAINING

enisa

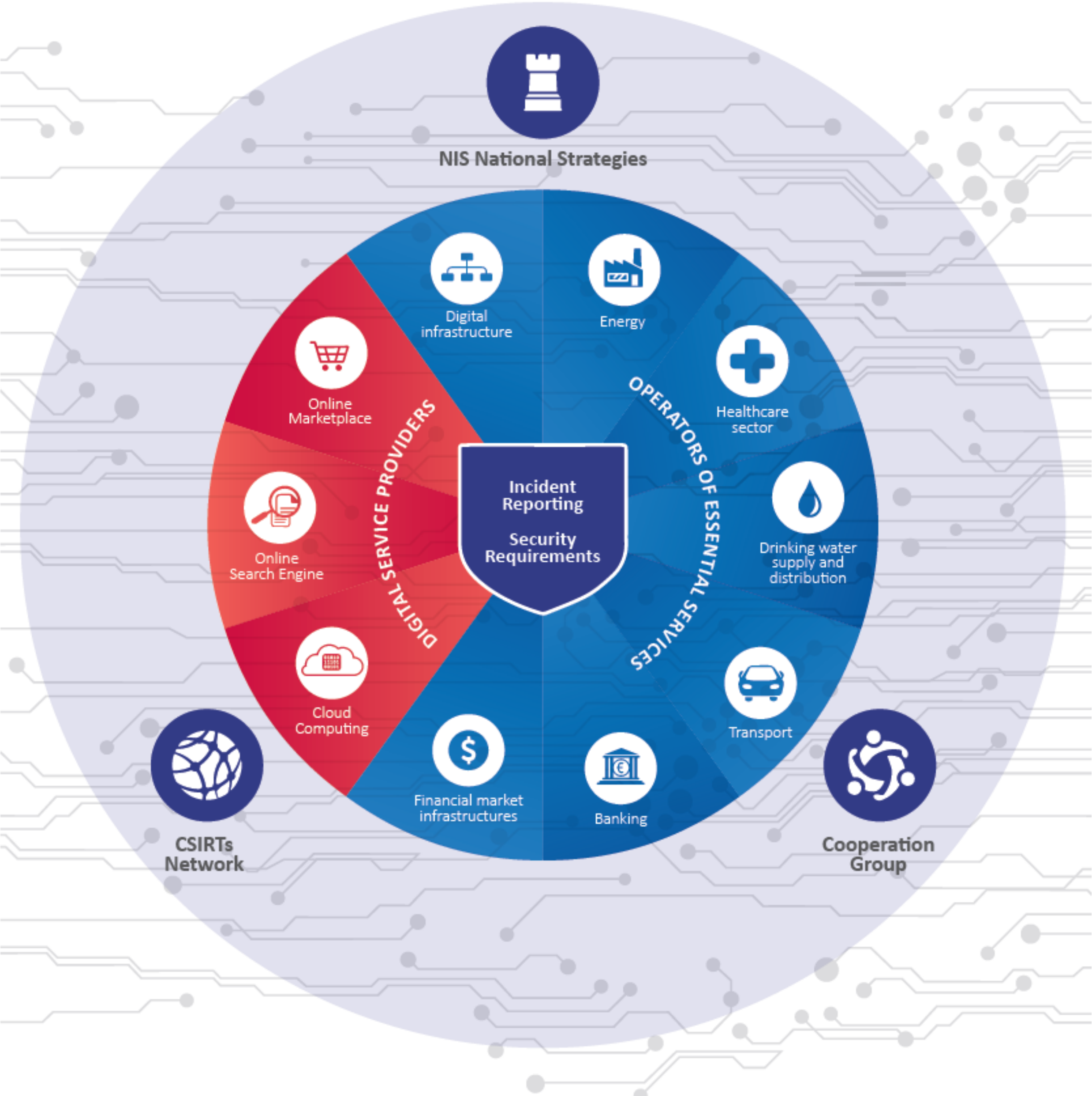
https://www.enisa.europa.eu/trainings

CYBER EUROPE 2018

enisa

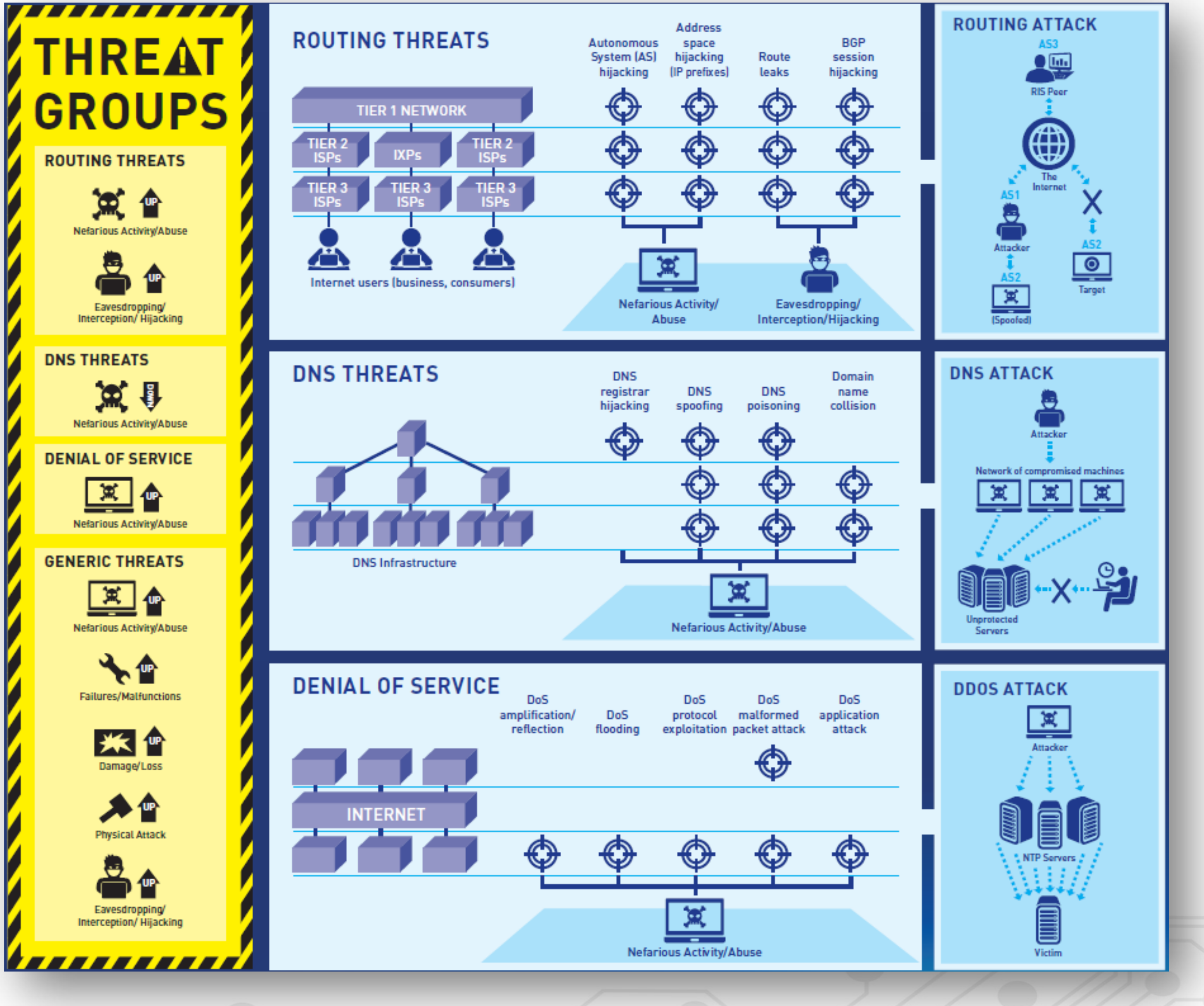
https://www.enisa.europa.eu/topics/cyber-exercises/

Capacity

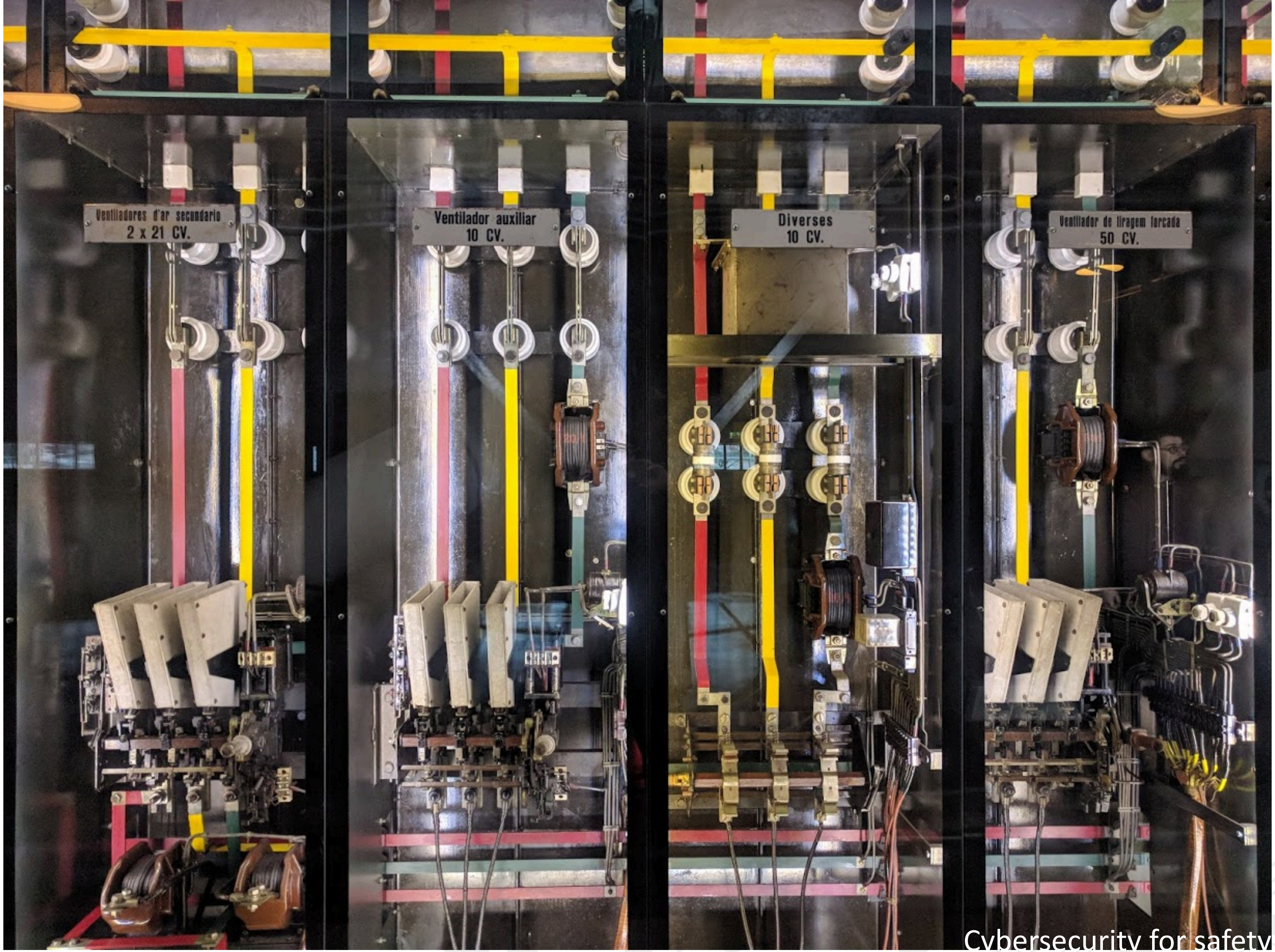

NIS National Strategies
Digital infrastructure
Energy
Healthcare sector
Drinking water supply and distribution
Transport
Banking
Financial market infrastructures
Cloud Computing
Online Search Engine
Online Marketplace
DIGITAL SERVICE PROVIDERS
OPERATORS OF ESSENTIAL SERVICES
Incident Reporting
Security Requirements
CSIRTs Network
Cooperation Group

Threat modelling and security measures

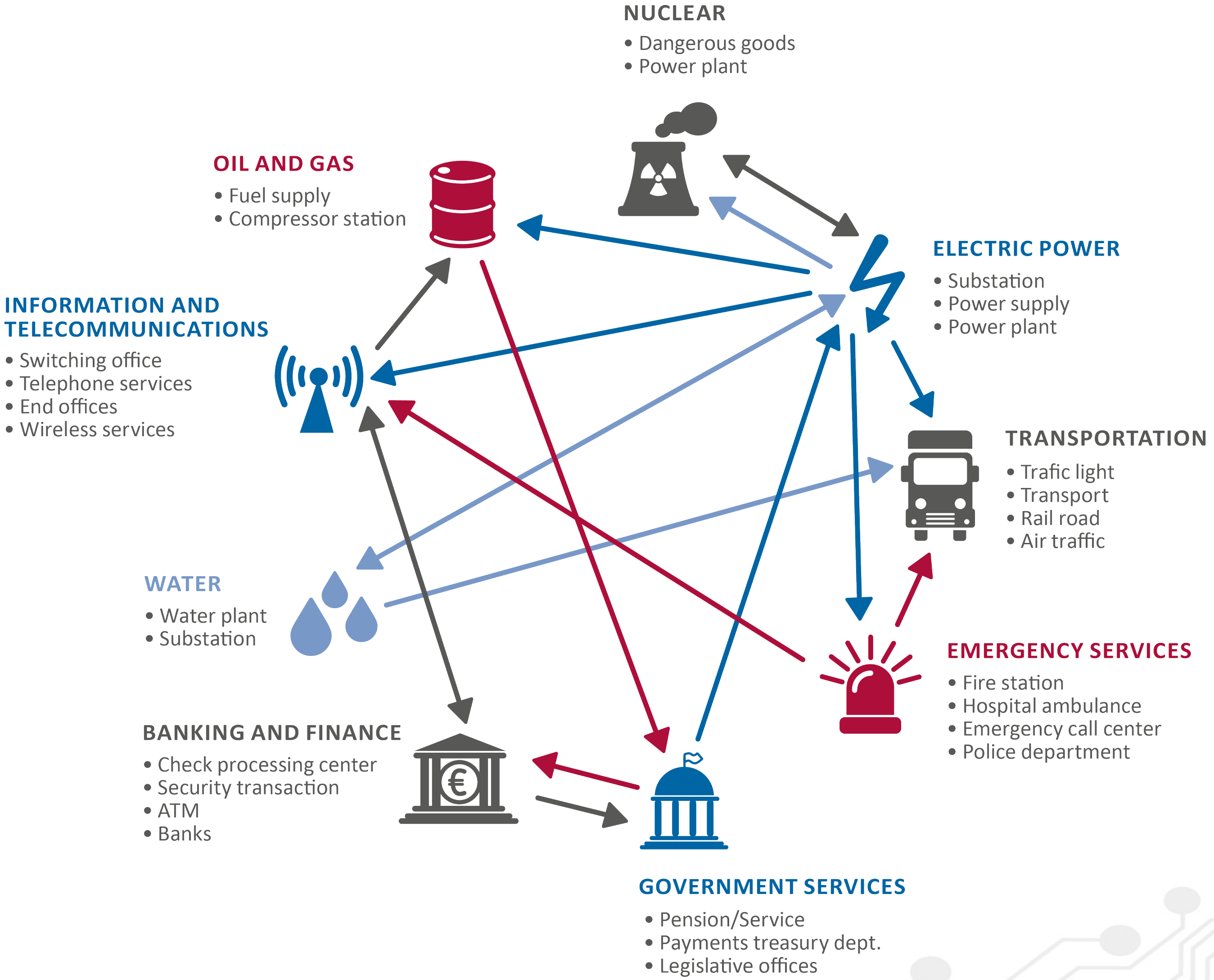
Internet infrastructure threats



../internetcii


Ventiladores d'ar secundario
2 x 21 CV.
Ventilador auxiliar
10 CV.
Diverses
10 CV.
Ventilador de tiragem forcada
50 CV.

Everything is interconnected



NUCLEAR

- Dangerous goods
- Power plant

OIL AND GAS

- Fuel supply
- Compressor station

ELECTRIC POWER

- Substation
- Power supply
- Power plant

INFORMATION AND TELECOMMUNICATIONS

- Switching office
- Telephone services
- End offices
- Wireless services

TRANSPORTATION

- Trafic light
- Transport
- Rail road
- Air traffic

WATER

- Water plant
- Substation

EMERGENCY SERVICES

- Fire station
- Hospital ambulance
- Emergency call center
- Police department

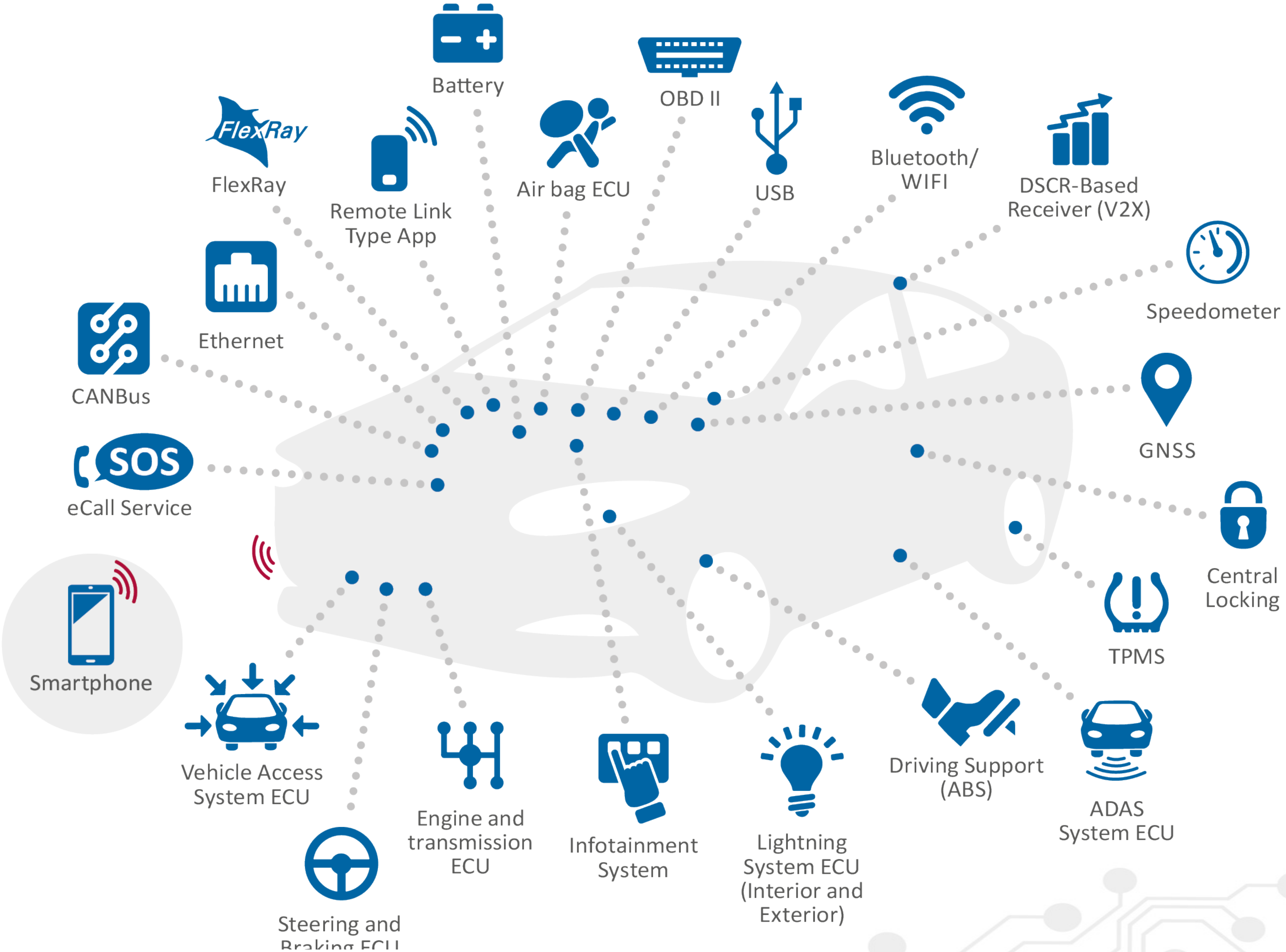
BANKING AND FINANCE

- Check processing center
- Security transaction
- ATM
- Banks

GOVERNMENT SERVICES

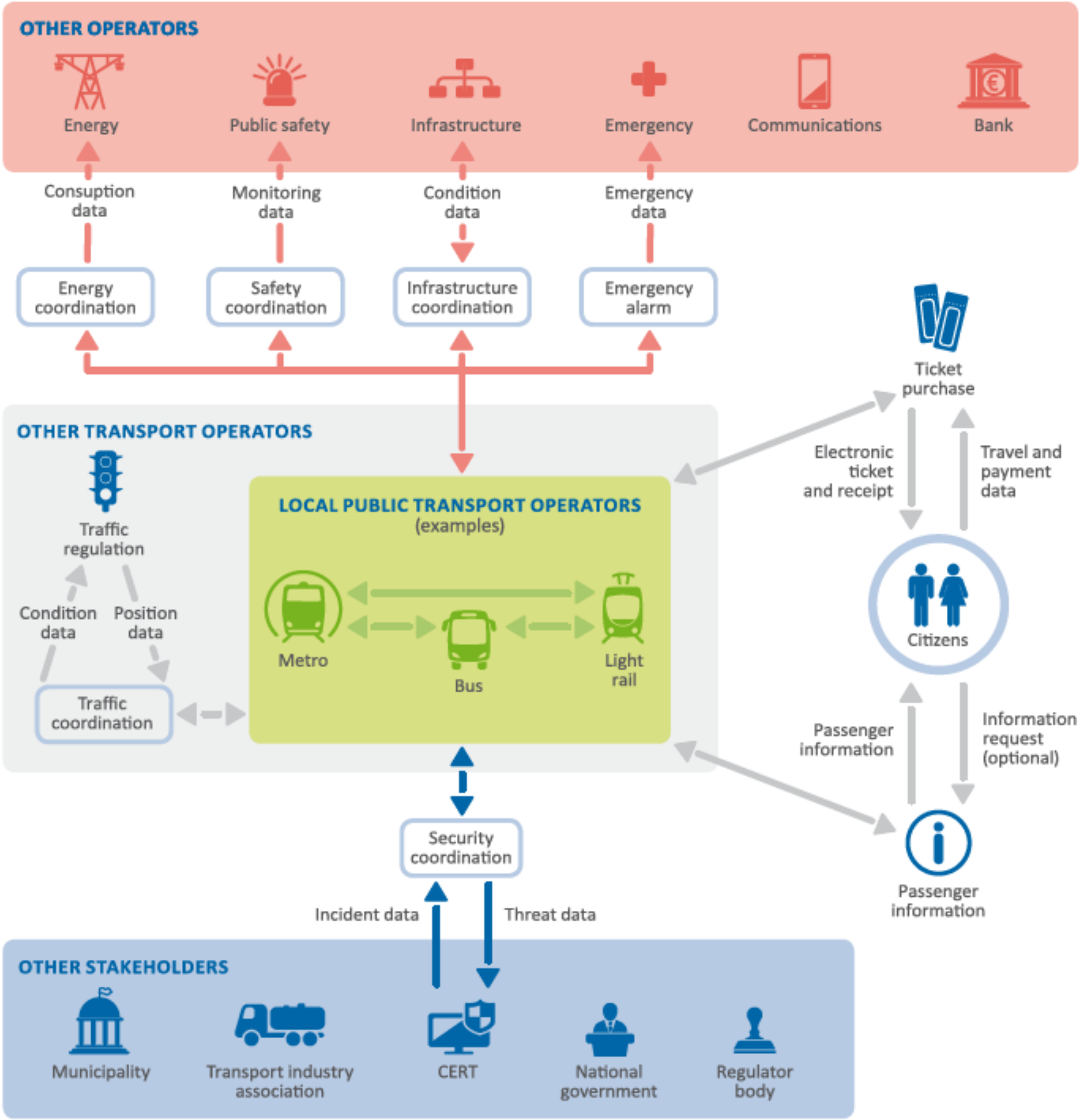
- Pension/Service
- Payments treasury dept.
- Legislative offices

Inside and outside

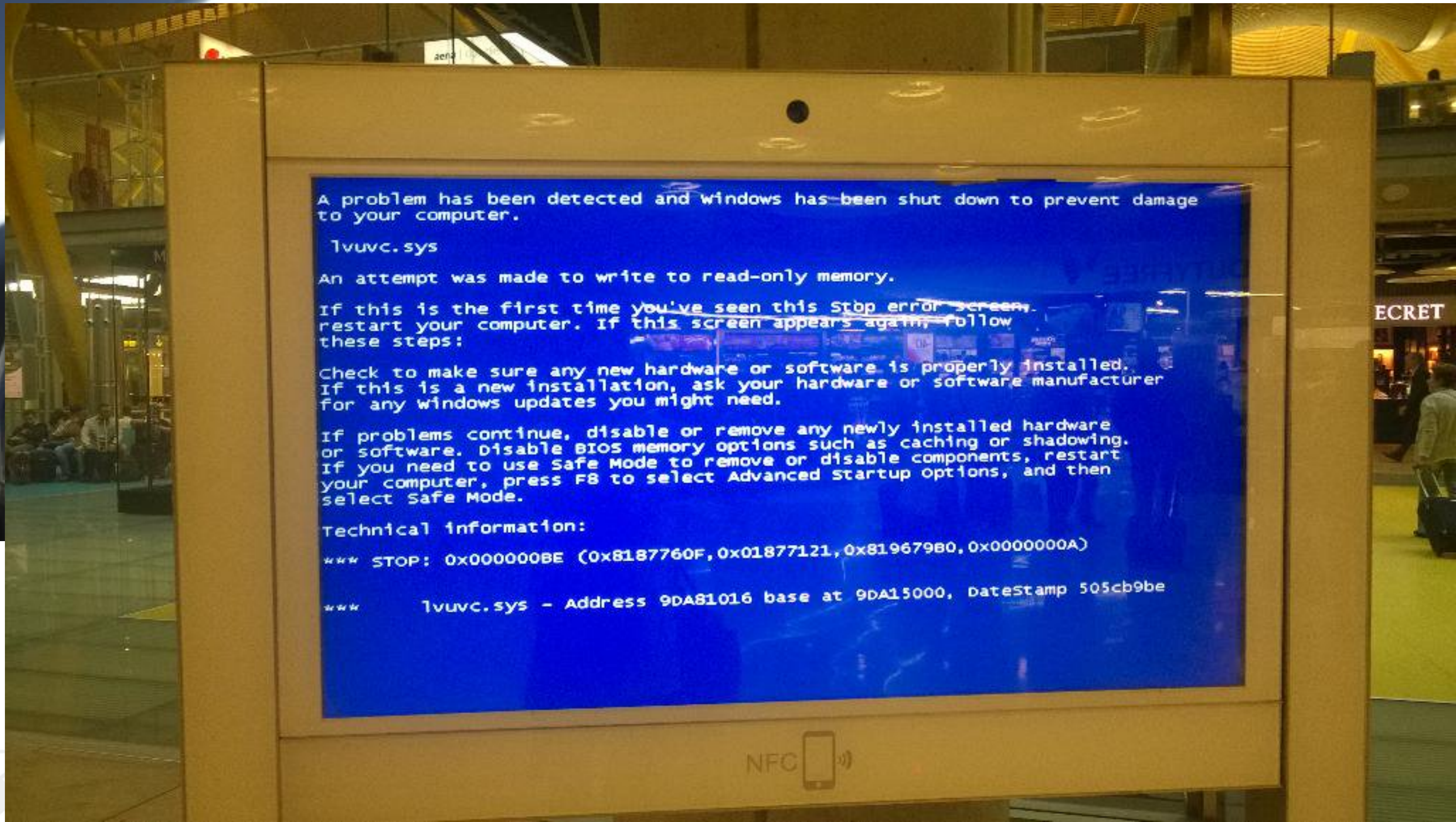


…/road

Think about your journey to #TR18

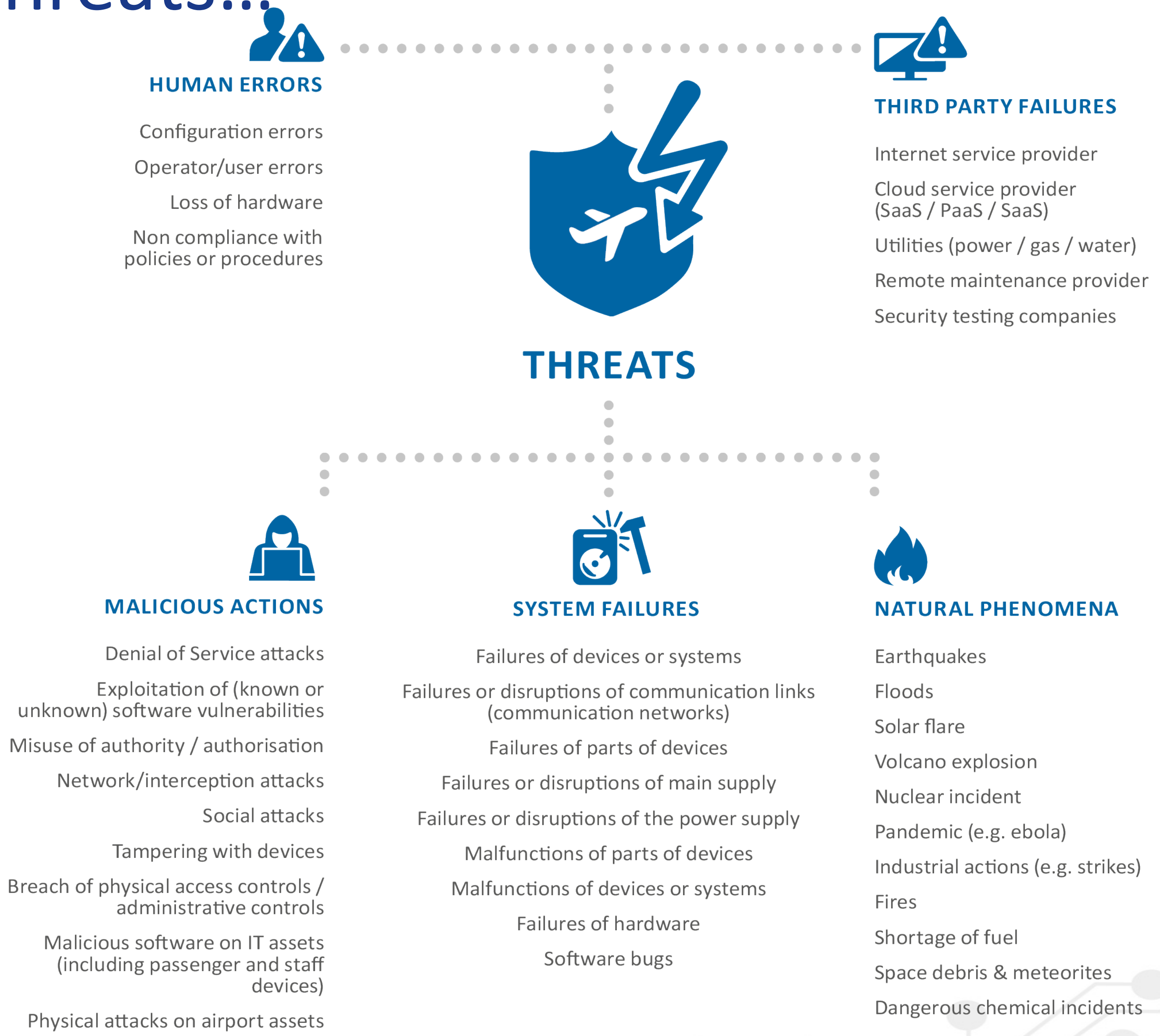


What could possibly go wrong?



```
A problem has been detected and Windows has been shut down to prevent damage
to your computer.

 lvuvc.sys

An attempt was made to write to read-only memory.

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x000000BE (0x8187760F,0x01877121,0x81967980,0x0000000A)


***      lvuvc.sys - Address 9DA81016 base at 9DA15000, DateStamp 505cb9be
```

Similar threats…



THREATS

HUMAN ERRORS

- Configuration errors
- Operator/user errors
- Loss of hardware
- Non compliance with policies or procedures

THIRD PARTY FAILURES

- Internet service provider
- Cloud service provider (SaaS / PaaS / SaaS)
- Utilities (power / gas / water)
- Remote maintenance provider
- Security testing companies

MALICIOUS ACTIONS

- Denial of Service attacks
- Exploitation of (known or unknown) software vulnerabilities
- Misuse of authority / authorisation
- Network/interception attacks
- Social attacks
- Tampering with devices
- Breach of physical access controls / administrative controls
- Malicious software on IT assets (including passenger and staff devices)
- Physical attacks on airport assets

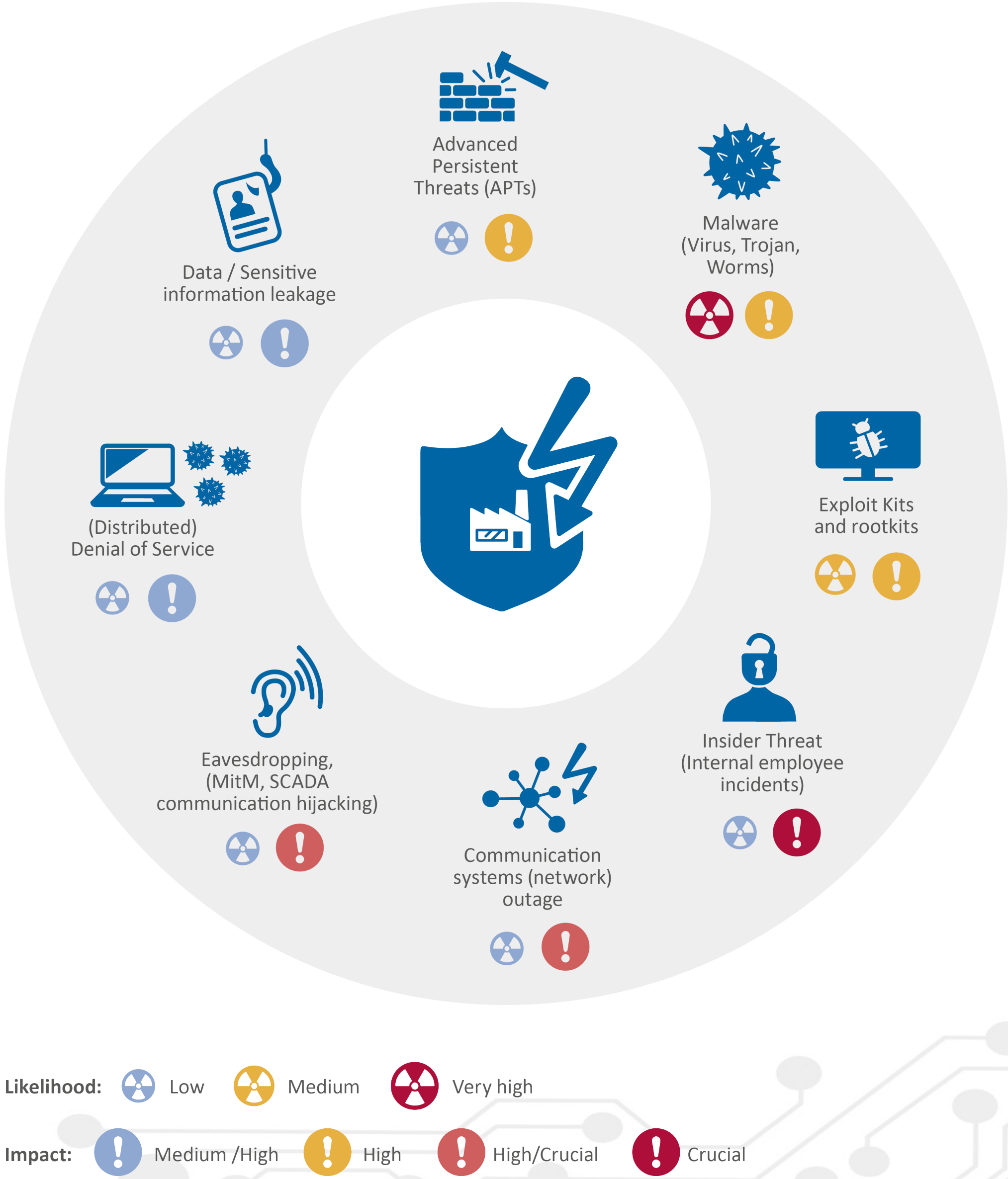
SYSTEM FAILURES

- Failures of devices or systems
- Failures or disruptions of communication links (communication networks)
- Failures of parts of devices
- Failures or disruptions of main supply
- Failures or disruptions of the power supply
- Malfunctions of parts of devices
- Malfunctions of devices or systems
- Failures of hardware
- Software bugs

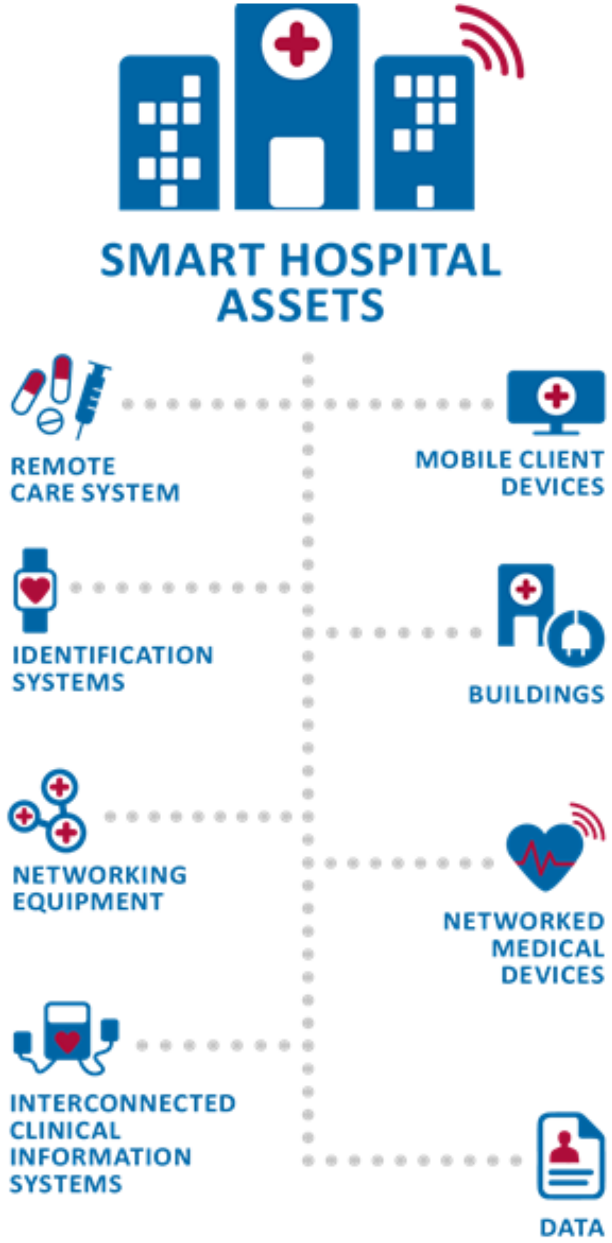
NATURAL PHENOMENA

- Earthquakes
- Floods
- Solar flare
- Volcano explosion
- Nuclear incident
- Pandemic (e.g. ebola)
- Industrial actions (e.g. strikes)
- Fires
- Shortage of fuel
- Space debris & meteorites
- Dangerous chemical incidents

…different infrastructures….


Advanced Persistent Threats (APTs)
Malware (Virus, Trojan, Worms)
Exploit Kits and rootkits
Insider Threat (Internal employee incidents)
Communication systems (network) outage
Eavesdropping, (MitM, SCADA communication hijacking)
(Distributed) Denial of Service
Data / Sensitive information leakage
Likelihood:
Low
Medium
Very high
Impact:
Medium /High
High
High/Crucial
Crucial

../scada

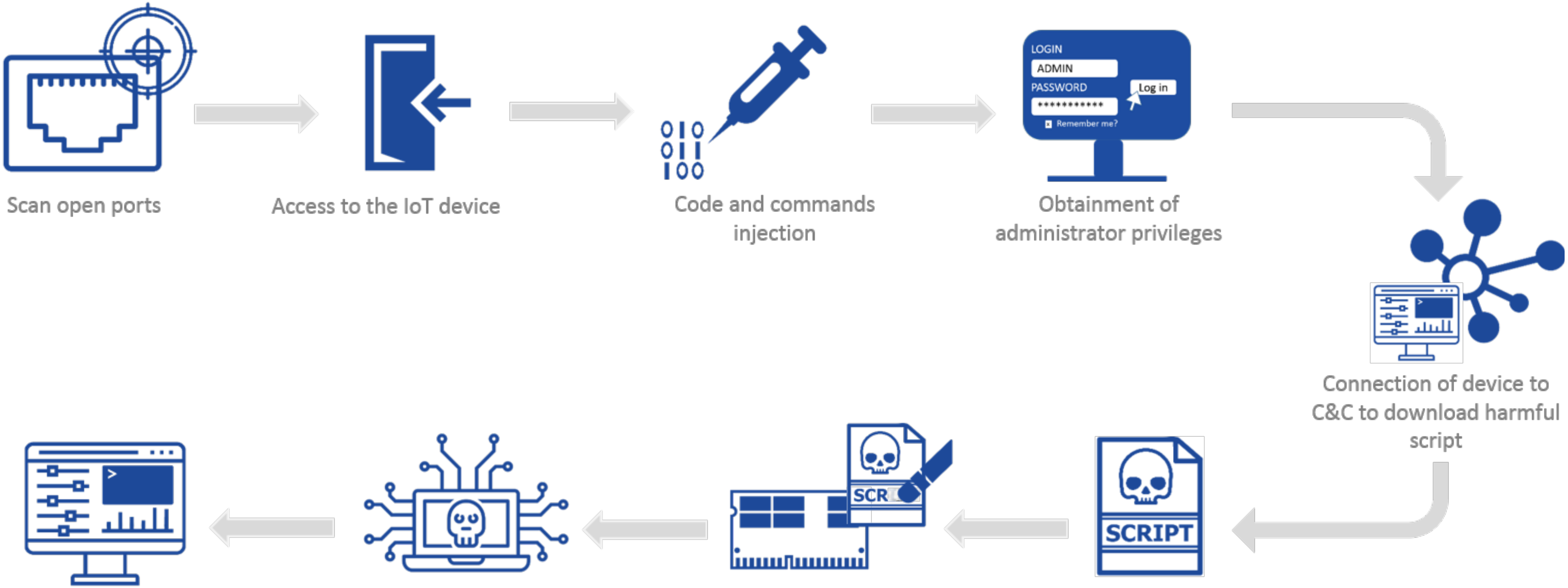


SMART HOSPITAL ASSETS

- REMOTE CARE SYSTEM
- MOBILE CLIENT DEVICES
- IDENTIFICATION SYSTEMS
- BUILDINGS
- NETWORKING EQUIPMENT
- NETWORKED MEDICAL DEVICES
- INTERCONNECTED CLINICAL INFORMATION SYSTEMS
- DATA

../ehealth

Developing most feared attack scenarios



Scan open ports

Access to the IoT device

Code and commands injection

Obtainment of administrator privileges

Connection of device to C&C to download harmful script

Execution of the malicious script

The script deletes itself and runs in-memory

Spread and attack other vulnerable devices

Attacker controls the botnet from a C&C centre

Attack 3 – IoT Botnet / Commands injection

POLICY AND STANDARDS

- GP-PS-01 – Adherence to regulation
- GP-PS-02 – Liability

GOOD PRACTICES

ORGANISATIONAL MEASURES

GENERAL

- GP-OM-01 – Designate a dedicated security team
- GP-OM-02 – Define a dedicated ISMS

SECURE DEVELOPMENT

- GP-OM-03 – Assess the threat model and use cases
- GP-OM-04 – Provide security and privacy by design
- GP-OM-05 – Implement and test the security functions

SECURITY UNTIL THE END-OF-LIFE

- GP-OM-06 – Assess the security controls and patch vulnerabilities
- GP-OM-07 – Define a security update policy
- GP-OM-08 – Perform a vulnerability survey
- GP-OM-09 – Check the security assumptions regularly during life-time
- GP-OM-10 – Protect the software update mechanism
- GP-OM-11 – Raise user awareness

TECHNICAL

COMMUNICATION PROTECTION

- GP-SF-03 – Provide end-to-end protection in confidentiality and integrity
- GP-SF-04 – Mitigate vulnerabilities or limitations of standard security library
- GP-SF-05 – Consider denial of service as a usual threat to communication infrastructures
- GP-SF-06 – Protect remote monitoring and administration interfaces

IDENTIFICATION, AUTHENTICATION, AUTHORIZATION

- GP-SF-16 – Use mutual authentication for remote communication
- GP-SF-17 – Use multi-factor authentication for use authentication
- GP-SF-18 – Implement access control measures to separate the privileges of different users as well as the privileges of different applications
- GP-SF-19 – Allow and encourage the use of strong passwords
- GP-SF-20 – Enforce session management policies to avoid session hijacking
- GP-SF-21 – Provide the user with mechanisms to securely erase their private data

SECURITY AUDIT

- GP-SF-01 - Security events must be securely logged
- GP-SF-02 – Users must be informed of security events

SELF-PROTECTION

- GP-SF-22 – Define a consistent policy for self-protection
- GP-SF-23 – Implement Hardware self-protection
- GP-SF-24 – Implement Software self-protection
- GP-SF-25 – Protect Non-user data
- GP-SF-26 – Perform Hardening
- GP-SF-27 – Isolate components

CRYPTOGRAPHY

- GP-SF-07 – Do not create proprietary cryptographic schemes, but use state-of-the-art standards instead
- GP-SF-08 – Rely on an expert in cryptography
- GP-SF-09 – Consider using dedicated and independently audited, hardware security modules
- GP-SF-10 – Cryptographic keys should be securely managed

USER DATA PROTECTION

- GP-SF-11 – Identify personal data
- GP-SF-12 – Implement transparency measures
- GP-SF-13 – Design the product/service with legitimate purpose and proportionality in mind
- GP-SF-14 – Define access control, anonymity and unlinkability measures to enforce the protection of private data
- GP-SF-15 – Define measures to ensure secure deletion of user data in case of a change of ownership

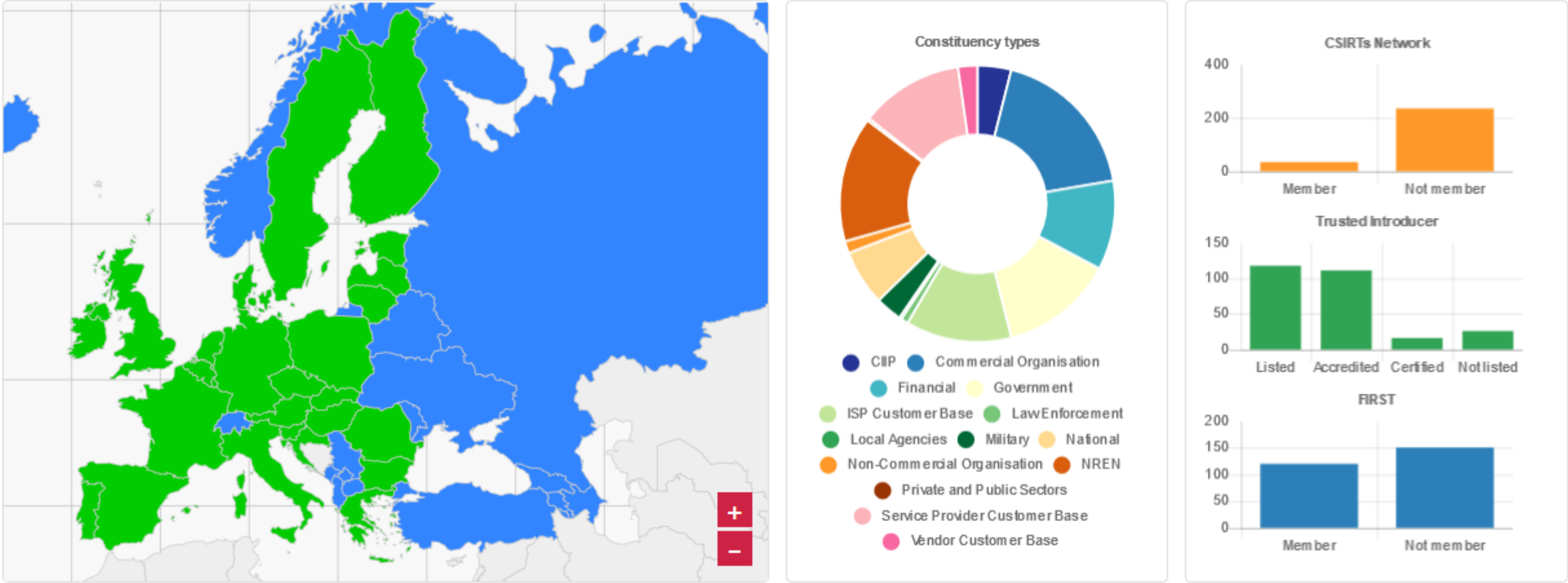
…/road

ENISA TRANSSEC Expert Group

https://resilience.enisa.europa.eu/

Facilitate information exchange, collaboration and incident response

CSIRTs in Europe



../csirts-map

272 CSIRTs teams in EU

- Everybody is talking about incidents:
  - Incident handling
  - Incident reporting
  - Cross border incidents
  - Statistics
  - Performance and internal KPI
  - Comparison with other entities
  - Trends
  - Global / annual overview
  - Explanation of external report
  - Media outreach
  - Policy discussion

Reference Taxonomy Task Force

ALEF-CSIRT

BSI/CERT-Bund

CaixaBank

CCN-CERT

CERT-HR

CERT.AT

CERT.be

CERT.LV/TF-CSIRT

CERT-BDF

CERT-LT

CERT-PT

CERT-SE

CERT-XLM

CESNET-CERTS

CIRCL

DFN-CERT

Eurocontrol / EATM-CERT

EC3

EGI-CSIRT

ENISA

FIRST

Gemalto

GOVCERT –AT

GOVCERT.LU

INCIBE

IRIS-CERT

KBC Group CERT

LITNET CERT

NTF CIRT

Open Systems

SCOMM-TECH

S-CURE

SI-CERT

Siemens

SOCA

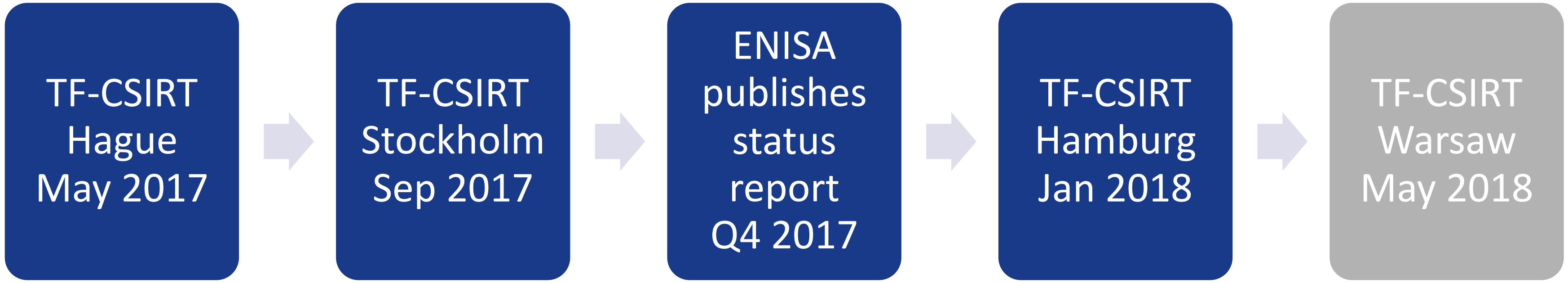
SWITCH CERT

Tallinn University

Telia CERT

UK MOD / University of Warwick

Timeline



TF-CSIRT Hague May 2017

TF-CSIRT Stockholm Sep 2017

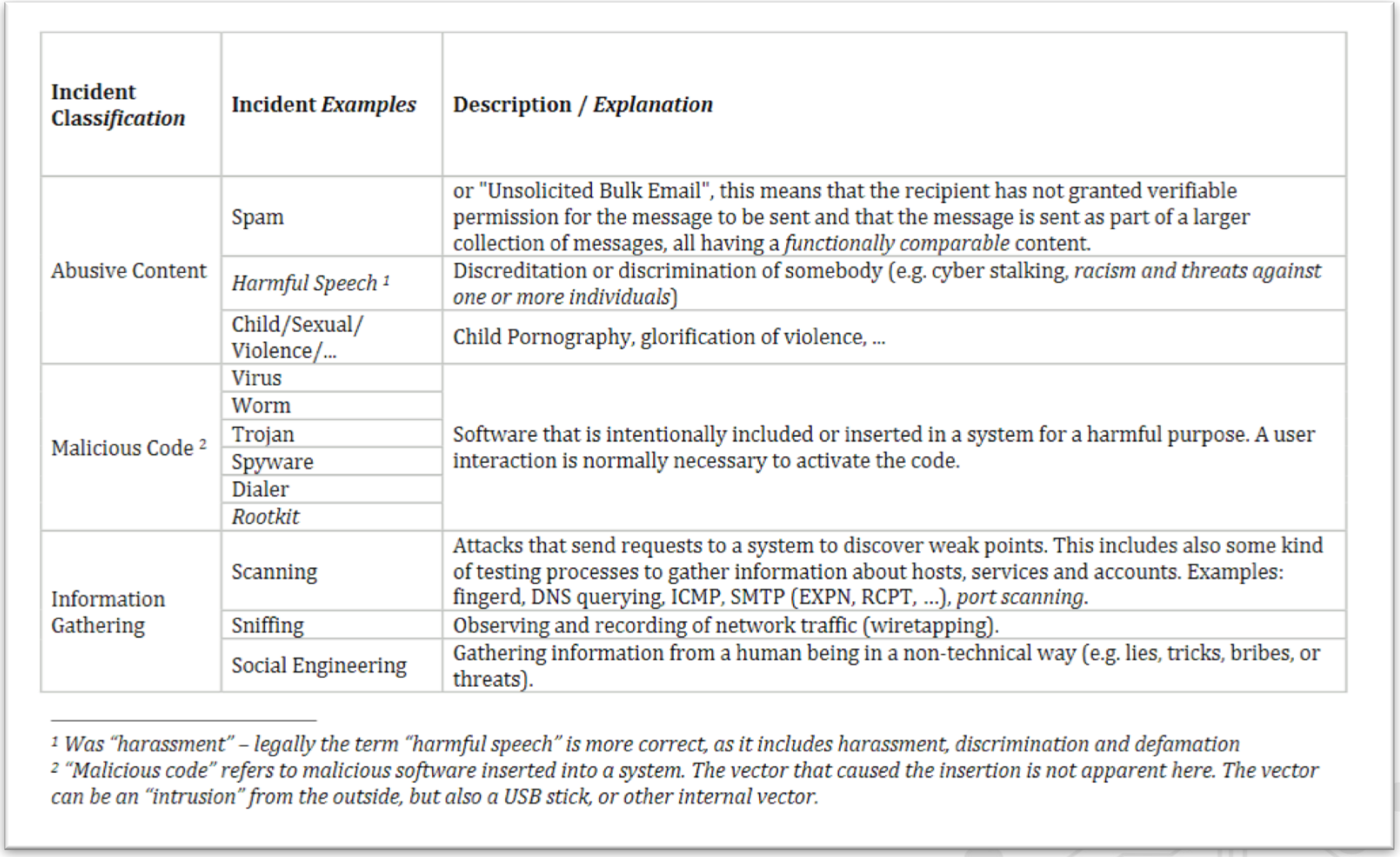
ENISA publishes status report Q4 2017

TF-CSIRT Hamburg Jan 2018

TF-CSIRT Warsaw May 2018

https://tf-csirt.org/groups/

eCSIRT.net mkVI (starting point)



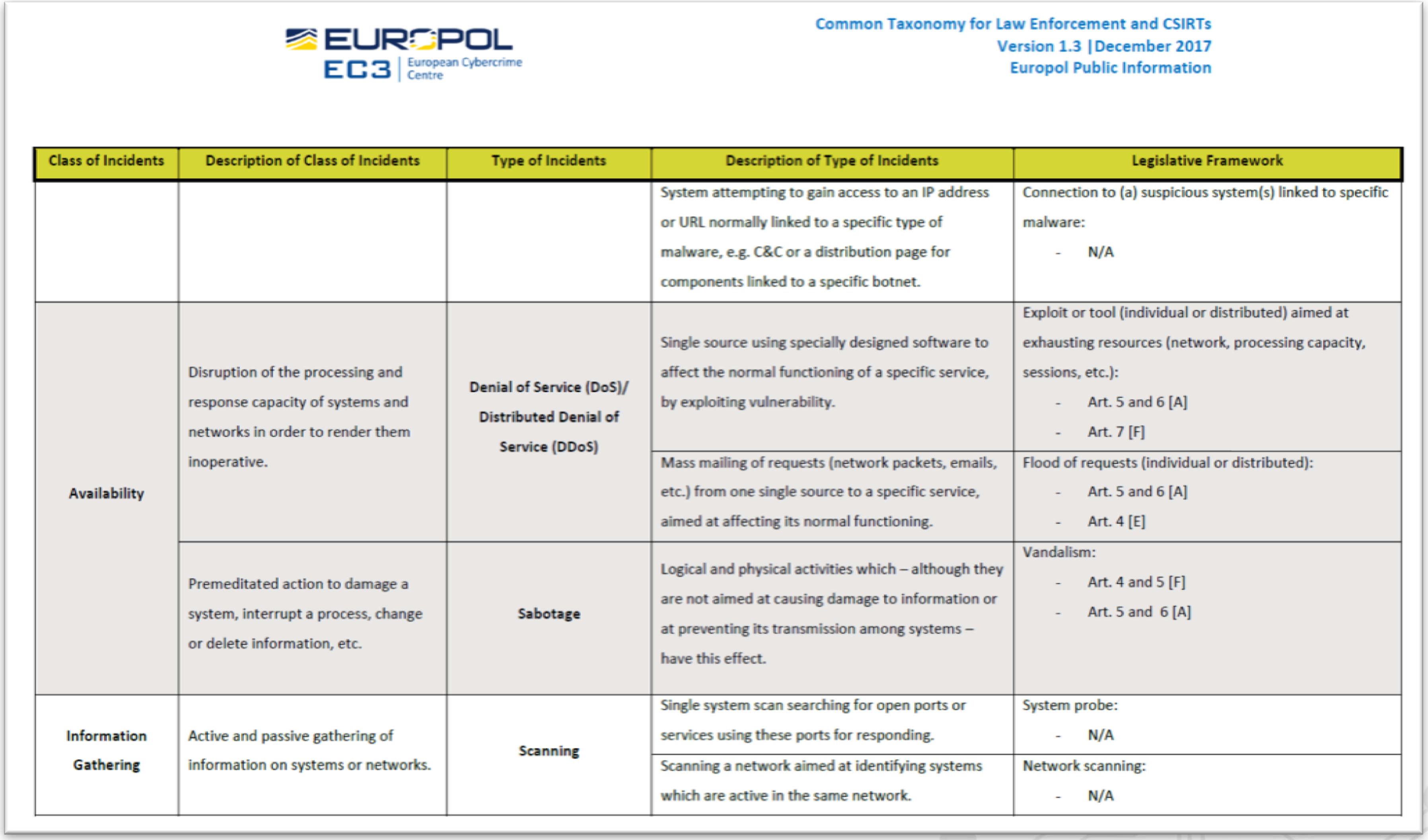
Incident *Classification*	**Incident *Examples***	**Description / *Explanation***
Abusive Content	Spam	or "Unsolicited Bulk Email", this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having a *functionally comparable* content.
	Harmful Speech [1]	Discreditation or discrimination of somebody (e.g. cyber stalking, *racism and threats against one or more individuals*)
	Child/Sexual/ Violence/...	Child Pornography, glorification of violence, ...
Malicious Code [2]	Virus	Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.
	Worm	
	Trojan	
	Spyware	
	Dialer	
	Rootkit	
Information Gathering	Scanning	Attacks that send requests to a system to discover weak points. This includes also some kind of testing processes to gather information about hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, ...), *port scanning*.
	Sniffing	Observing and recording of network traffic (wiretapping).
	Social Engineering	Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats).

[1] *Was "harassment" – legally the term "harmful speech" is more correct, as it includes harassment, discrimination and defamation*

[2] *"Malicious code" refers to malicious software inserted into a system. The vector that caused the insertion is not apparent here. The vector can be an "intrusion" from the outside, but also a USB stick, or other internal vector.*

https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf

Common Taxonomy CSIRT-LEA



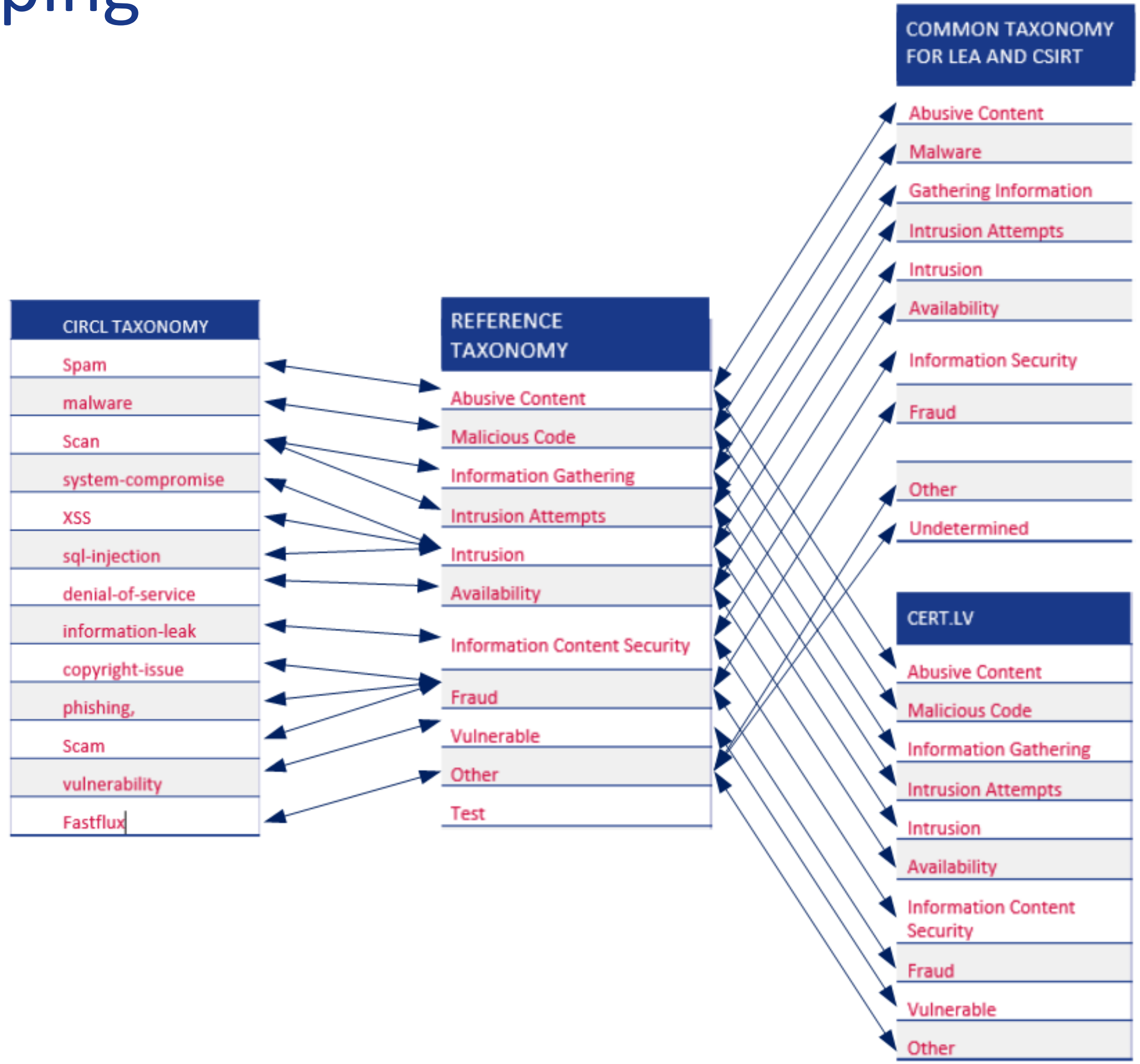
EUROPOL
EC3 European Cybercrime Centre

Common Taxonomy for Law Enforcement and CSIRTs
Version 1.3 | December 2017
Europol Public Information

Class of Incidents	Description of Class of Incidents	Type of Incidents	Description of Type of Incidents	Legislative Framework
			System attempting to gain access to an IP address or URL normally linked to a specific type of malware, e.g. C&C or a distribution page for components linked to a specific botnet.	Connection to (a) suspicious system(s) linked to specific malware: - N/A
Availability	Disruption of the processing and response capacity of systems and networks in order to render them inoperative.	**Denial of Service (DoS)/ Distributed Denial of Service (DDoS)**	Single source using specially designed software to affect the normal functioning of a specific service, by exploiting vulnerability.	Exploit or tool (individual or distributed) aimed at exhausting resources (network, processing capacity, sessions, etc.): - Art. 5 and 6 [A] - Art. 7 [F]
			Mass mailing of requests (network packets, emails, etc.) from one single source to a specific service, aimed at affecting its normal functioning.	Flood of requests (individual or distributed): - Art. 5 and 6 [A] - Art. 4 [E]
	Premeditated action to damage a system, interrupt a process, change or delete information, etc.	**Sabotage**	Logical and physical activities which – although they are not aimed at causing damage to information or at preventing its transmission among systems – have this effect.	Vandalism: - Art. 4 and 5 [F] - Art. 5 and 6 [A]
Information Gathering	Active and passive gathering of information on systems or networks.	**Scanning**	Single system scan searching for open ports or services using these ports for responding.	System probe: - N/A
			Scanning a network aimed at identifying systems which are active in the same network.	Network scanning: - N/A

https://www.europol.europa.eu/publications-documents/common-taxonomy-for-law-enforcement-and-csirts

Pivot Mapping



CIRCL TAXONOMY

Spam
malware
Scan
system-compromise
XSS
sql-injection
denial-of-service
information-leak
copyright-issue
phishing,
Scam
vulnerability
Fastflux

REFERENCE TAXONOMY

Abusive Content
Malicious Code
Information Gathering
Intrusion Attempts
Intrusion
Availability
Information Content Security
Fraud
Vulnerable
Other
Test

COMMON TAXONOMY FOR LEA AND CSIRT

Abusive Content
Malware
Gathering Information
Intrusion Attempts
Intrusion
Availability
Information Security
Fraud
Other
Undetermined

CERT.LV

Abusive Content
Malicious Code
Information Gathering
Intrusion Attempts
Intrusion
Availability
Information Content Security
Fraud
Vulnerable
Other

Tools

INTELMQ

http://intelmq.readthedocs.io/en/latest/

MISP
Threat Sharing

https://github.com/MISP/misp-taxonomies

TheHive

https://thehive-project.org/

../trainings

Examples of online trainings available

Mobile threats incident handling

Digital forensics

Large scale incident handling

Network forensics

Triage & basic incident handling

Vulnerability handling

Artifact analysis fundamentals

Advanced artifact handling

Writing security advisories

Developing countermeasures

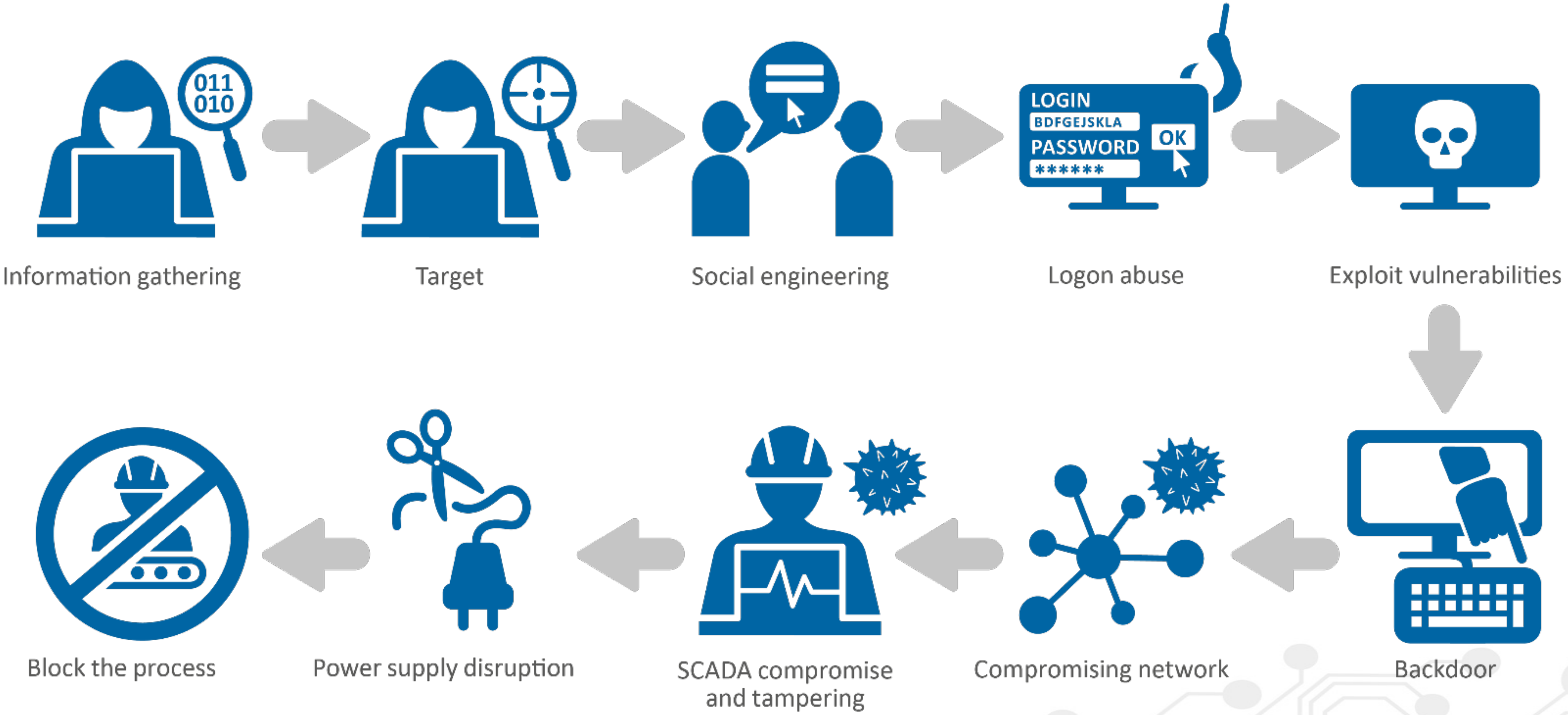
Identification and handling of electronic evidence

Automation in incident handling

../trainings

ENISA training on aviation cybersecurity co-organized with EASA

ATTACK SCENARIO: SCADA SYSTEM COMPROMISE



Information gathering

Target

Social engineering

Logon abuse

Exploit vulnerabilities

Backdoor

Compromising network

SCADA compromise and tampering

Power supply disruption

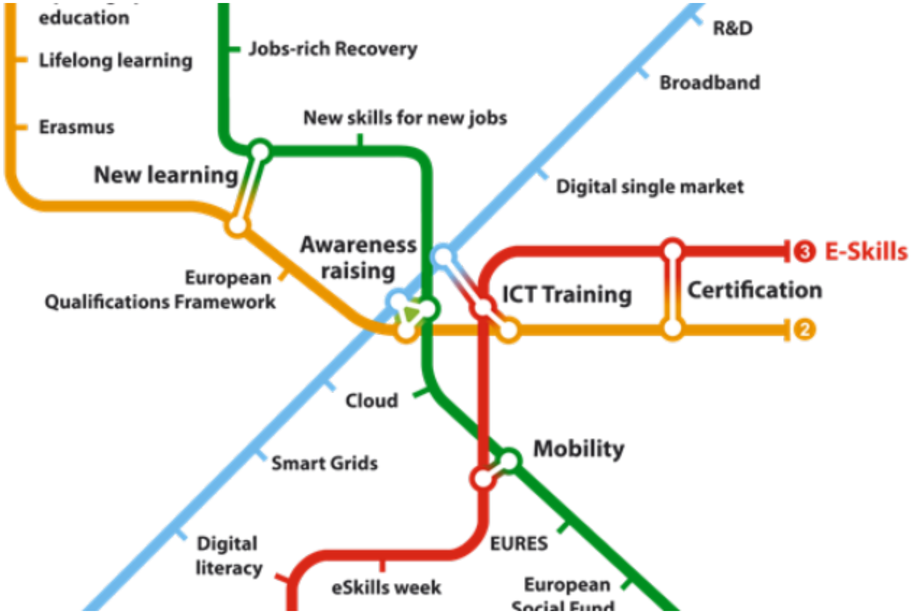
Block the process

../trainings

https://www.youtube.com/watch?v=hCDOp7_hsjY

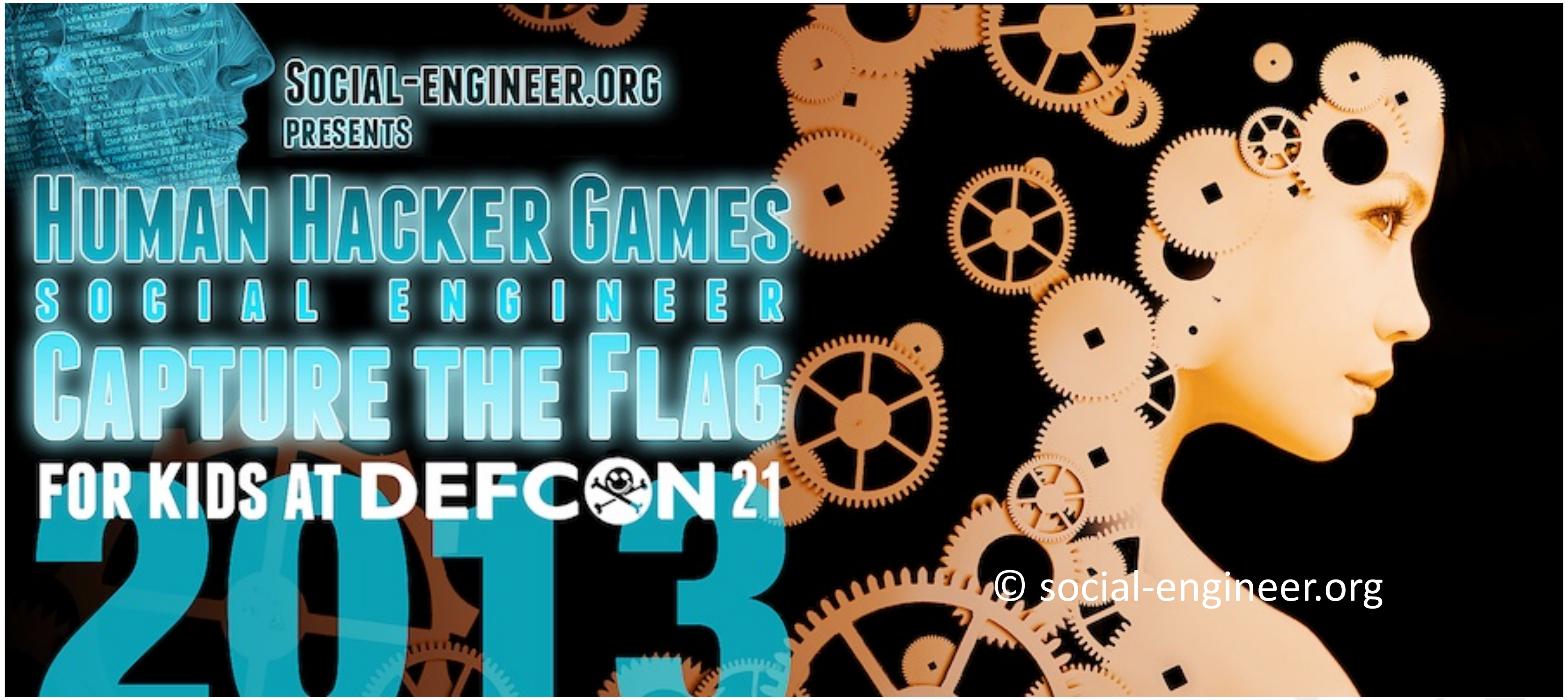
Foster the growth of the next generation security talents

Lets go back to April 29, 2014



CTF - Capture The Future

How CTFs can foster the engagement of future cyber security professionals.



© social-engineer.org

CTF - Capture The Future

We need to engage future cyber security professionals

We need more people

We need specialized experts:

- Pen-testers
- Risk assessment experts
- Quality assurance experts
- Reverse engineers
- Critical Information Infrastructure experts
- Etc

Millennials

- were born with the Internet
- have a multitasking and tech oriented way of learning

Capture the Flag

Where

- Hacking cons
- Academia
- Onsite
- Online

Sponsored by

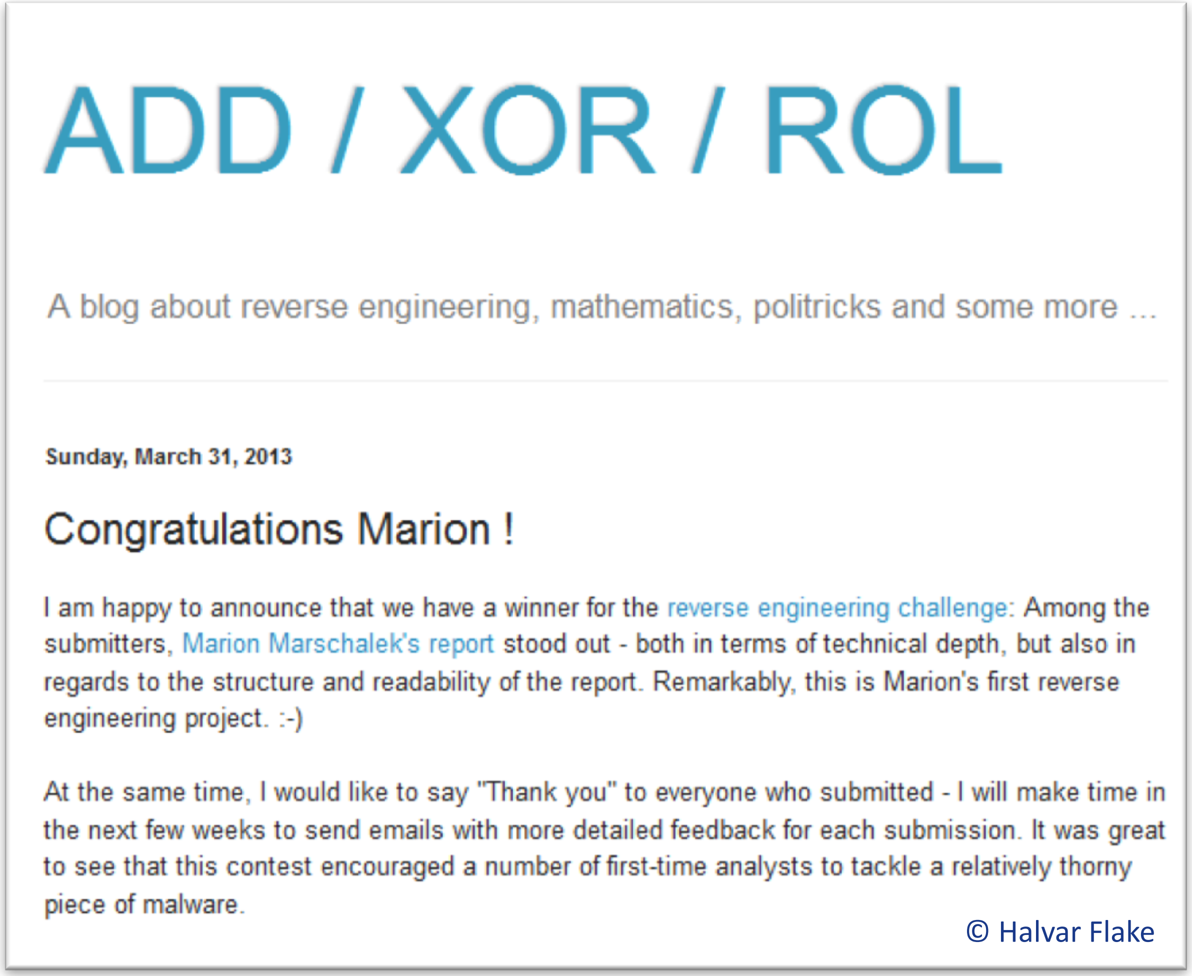
- Private companies
- Governmental orgs

Scope:

- Train students
- Use pro as mentors
- Recruit talents
- Engage kids

© UCSB security lab

Reverse engineering challenges



ADD / XOR / ROL

A blog about reverse engineering, mathematics, politricks and some more ...

Sunday, March 31, 2013

Congratulations Marion !

I am happy to announce that we have a winner for the reverse engineering challenge: Among the submitters, Marion Marschalek's report stood out - both in terms of technical depth, but also in regards to the structure and readability of the report. Remarkably, this is Marion's first reverse engineering project. :-)

At the same time, I would like to say "Thank you" to everyone who submitted - I will make time in the next few weeks to send emails with more detailed feedback for each submission. It was great to see that this contest encouraged a number of first-time analysts to tackle a relatively thorny piece of malware.

© Halvar Flake

Where

- Hacking cons
- Online
- Academia

Sponsored by

- Private companies
- Hacking cons
- Security experts

Scope:

- Engage new people
- Train students
- Recruit talents

Fast forward

https://www.blackhoodie.re/

https://www.europeancybersecuritychallenge.eu/

Securing Europe’s information society: bridging the gap between industry, security community and Member States

Robert M Lee - Keynote: Exploring the Unknown ICS Threat Landscape
74.8
Jens Zerbst - Defence-in-Depth in a time of Advanced Persistent Threats
46.3
Erwin Kooi - How grid operator can use the presented research to improve the securing and resilience of the (smart) energy grid
Maik Brüggeman - PLC-Blaster - A Worm Living in Your PLC
Marie Moe & Eireann Leverett - Embodied Vulnerabilities - How to find, fix and think about them
John Matherly - The Rise of the Machines
78.2
Lucas Lundgren - Lightweight protocol! Serious equipment! Critical implications!

Raise the level of awareness on cyber security in Europe

Facilitate information exchange, collaboration and incident response

Foster the growth of the next generation security talents

Enable higher level of security for European citizens

Wanna help?

Apply for ENISA experts groups - https://resilience.enisa.europa.eu/

Register your CSIRT - https://www.enisa.europa.eu/csirts-map

Participate to https://www.enisa.europa.eu/topics/cyber-exercises/

Prepare a team for https://www.europeancybersecuritychallenge.eu/

Organize an event for https://cybersecuritymonth.eu/

Check out our events https://www.enisa.europa.eu/events

Share your knowledge, mentor others
and make the world a safer place!

> “…We have a lot of potential here," primarily in that we all like each other and that we're all interested in similar things. And my goal all my life has just been to make a difference, so somehow have some positive impact. That's where the motto for the L0pht of make a dent in the universe came from. And the first thing of doing that is to find like-minded folks and get that movement going. It's really difficult to do it on your own.”

Mudge

https://duo.com/decipher/tag/l0pht

Thank you

🌐 https://www.enisa.europa.eu/

✉ CSIRT-Relations@enisa.europa.eu