CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

GEORGIOS PSYKAKOS, CERT-EU

ARTIFICIAL INTELLIGENCE CONFERENCE / 2019-06-03

TLP:GREEN

CERT-EU IN THE BLUEPRINT

AGENDA

- CERT-EU
- Blueprint
- Our Challenges
- A Good Plan
- Let’s Organise

WHAT IS CERT-EU?

- Cyber Defence Entity of all the EU Institutions, Bodies & Agencies;
- Started as a pilot scheme in 2011;
- Established in Dec 2017 as an independent, inter-institutional legal entity;
- Core mission: act as the cybersecurity information exchange and incident response coordination hub for its 65 constituents;
- 31 experts delivering various services to a heterogeneous constituency across diverse sectors;
- One of the key actors taking part in the Blueprint.

OUR SERVICES

CYBER THREAT INTELLIGENCE

THREAT MONITORING & DETECTION

DIGITAL FORENSICS & INCIDENT RESPONSE

VULNERABILITY ASSESSMENT & ADVISORIES

RED TEAM EXERCISES

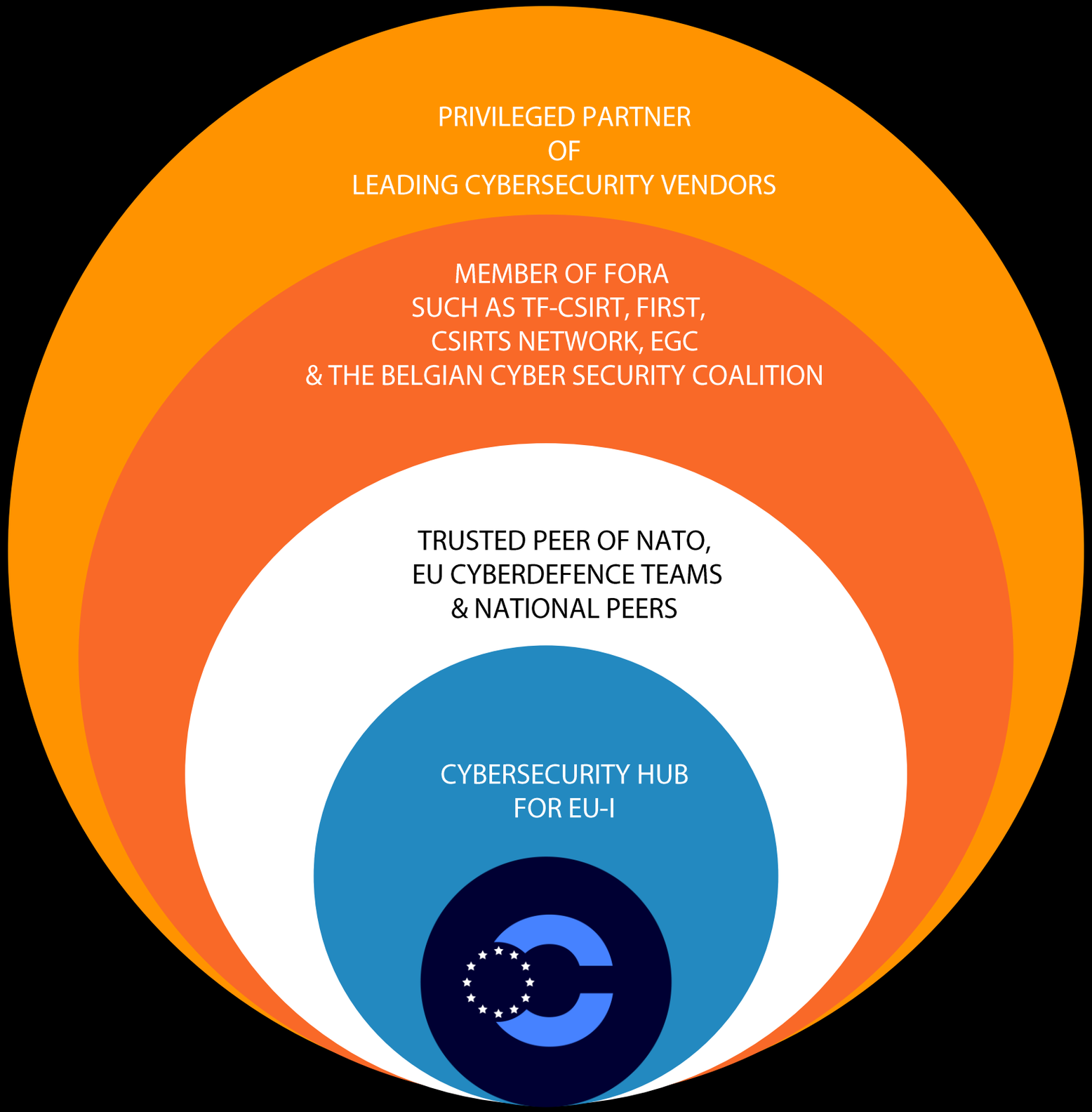
PENETRATION TESTING

PHISHING EXERCISES

THREAT HUNTING

ENHANCED MEDIA MONITOR

A WIDELY RESPECTED CERT



THREAT LANDSCAPE

- State or state-affiliated groups: they tend to possess advanced capabilities and significant resources as well as objectives aligned with the agenda of their sponsor;
- Organized crime: often engage in targeted attacks, driven by profits;
- Hacktivists: attackers with ideological motivations, seeking to raise awareness or benefit their cause through their cyber militancy;
- Opportunistic: largely amateur criminals or, sometimes, legitimate security researchers, looking to expose flaws and exploits.

ARE WE READY?

BACKGROUND & CHALLENGES

BLUEPRINT

Exchange of Information
Education & Training
Strategic & Technical Cooperation

enisa
EUROPOL
EUROPEAN DEFENCE AGENCY

European External Action Service

EU Intelligence Analysis Center
EU Military Staff Intelligence Directorate
Rapid Alert System

Technical Information
Incident Coordination

CSIRTs NETWORK

European Commission

ARGUS I&II

Exchange of Information
Training

NATO
OTAN

Council of the European Union

Cyber Diplomacy Toolbox
Integrated Political Crisis Response
Cyber Defence Policy Framework

CHALLENGES

- Culture: vast majority of existing EU-Institutions departments focus on policy; only a “handful” with experience on cyber operations;
- Entropy: policy complexity increases exponentially; the threat landscape adapts quickly; Information & Communication Technology evolves rapidly introducing new challenges;
- Diversity: in the missions of our constituency; variety of ICT infrastructures.

“IN THE MIDST OF CHAOS, THERE IS ALSO OPPORTUNITY” – SUN TZU

A GOOD PLAN

- Policy: define clear objectives; include precise procedures; be simple; unify processes; keep it steady;
- People: most important asset; emphasize on cyber security mentality; expand technical knowledge; engage senior management;
- Tools: team – develop capability; community – foster cooperation; automate and invest in R&D;
- Alliance: information sharing; learn from others; maintain awareness; multiply available resources;
- Plan: continuous improvement; “winter is coming”.

BE AN EXAMPLE

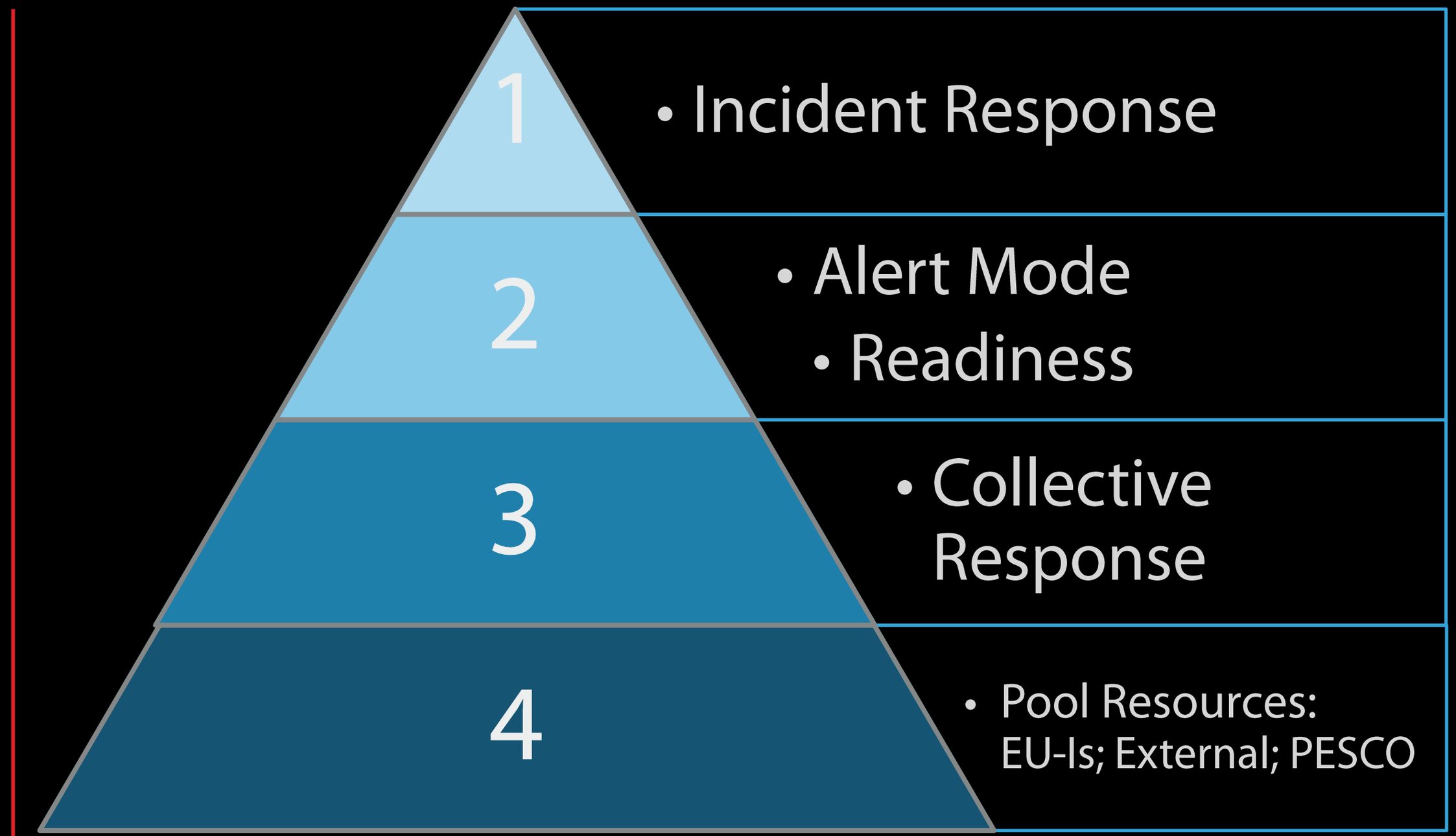
- EU-pace/NATO locked shields: greatest so far operational challenge; shaped an inter-institutional incident response team; engaged all teams; introduced senior management of CERT-EU as training audience;
- EU elections: launched tailored services for the European Parliament; went on operational Readiness status;
- Major attacks paper: an ongoing effort for EU-Institutions on collective response against significant attacks.

MAJOR ATTACKS PAPER

KEYS

- Standard Operating Procedures: derived from CERT-EU's experience; best practices; tailored tools;
- Situational Awareness: by a sensor network; by threat feeds; by using advanced threat detection;
- Operational Alert System to complement EEAS RAS;
- Contribution: capacity and willingness to engage.

STAGES


1
• Incident Response
2
• Alert Mode
• Readiness
3
• Collective Response
4
• Pool Resources:
EU-Is; External; PESCO
DE-ESCALATION
Lines to Take

BENEFITS

- Streamlines with existing structures' mandate; does not introduce new bodies;
- Cost effective; utilises constituents' existing capabilities and available resources for the benefit of all;
- Simple SOPs that have been tested and ensure response in timely manner;
- Full Crisis Management lifecycle: prevention, preparedness, response, recovery.

THINK CONSTITUENT

CERT-EU

FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

CREATE VALUE