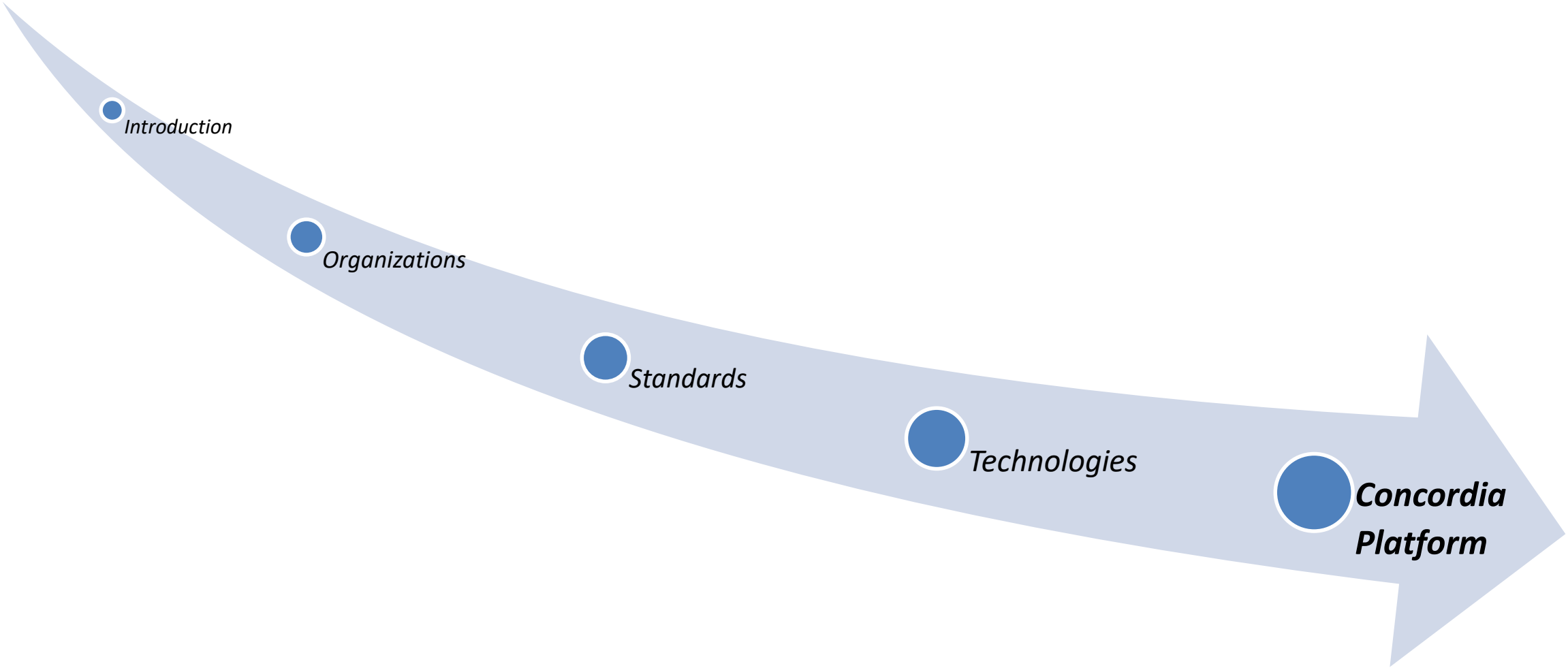
Threat Intelligence for Europe

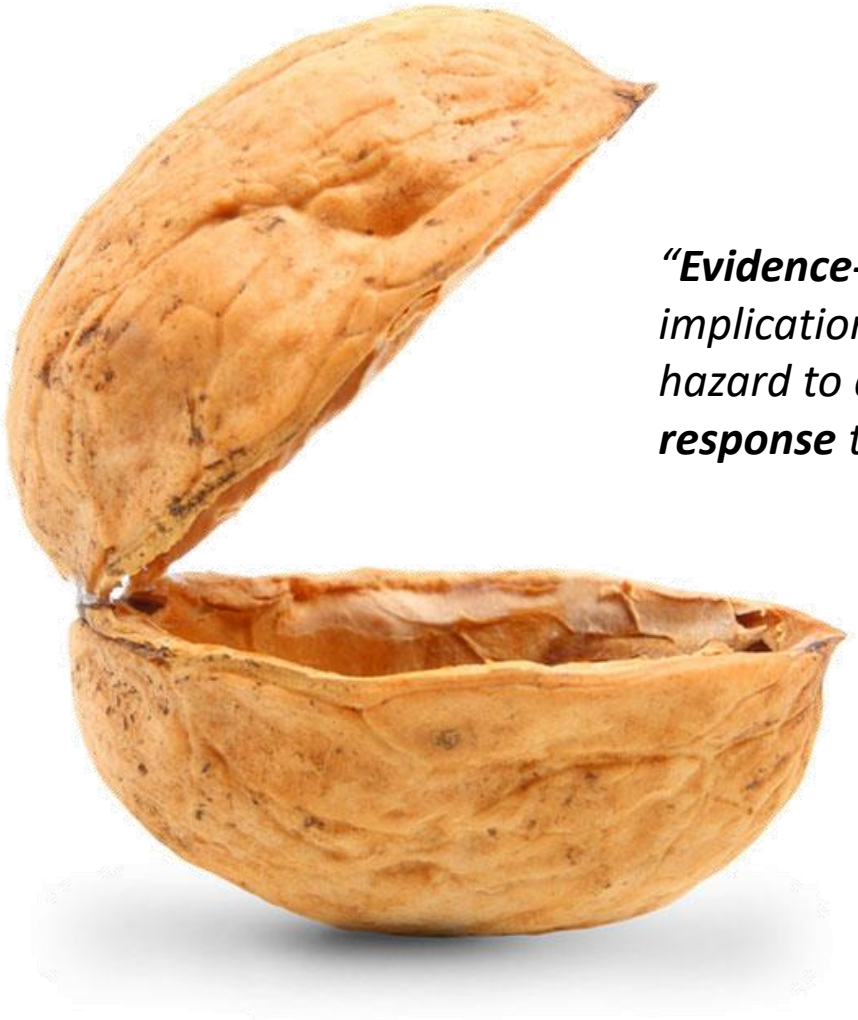
Dr. Marco Caselli, Siemens AG

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830927.

Overview


Introduction
Organizations
Standards
Technologies
Concordia Platform

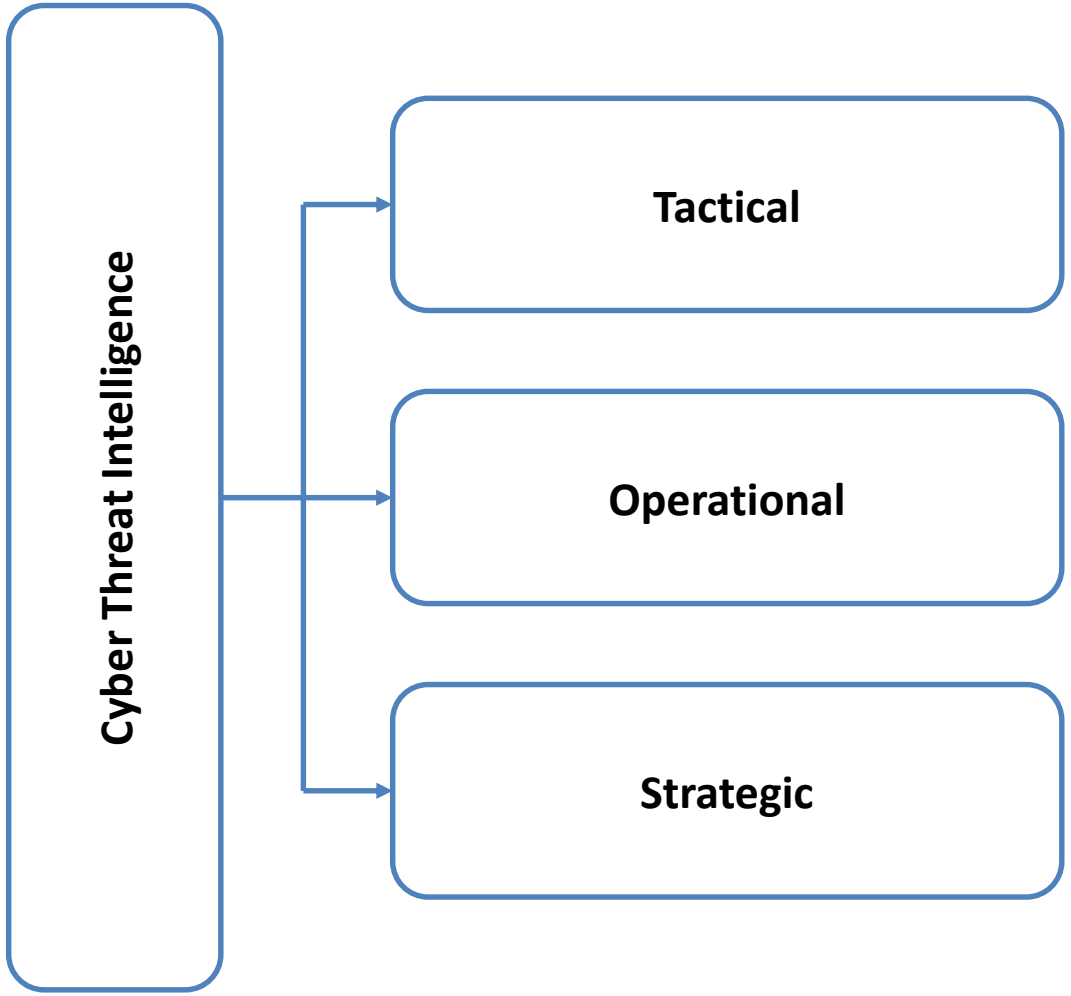
Cyber Threat Intelligence in a nutshell



*"**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."*

Gartner

Cyber Threat Intelligence classification



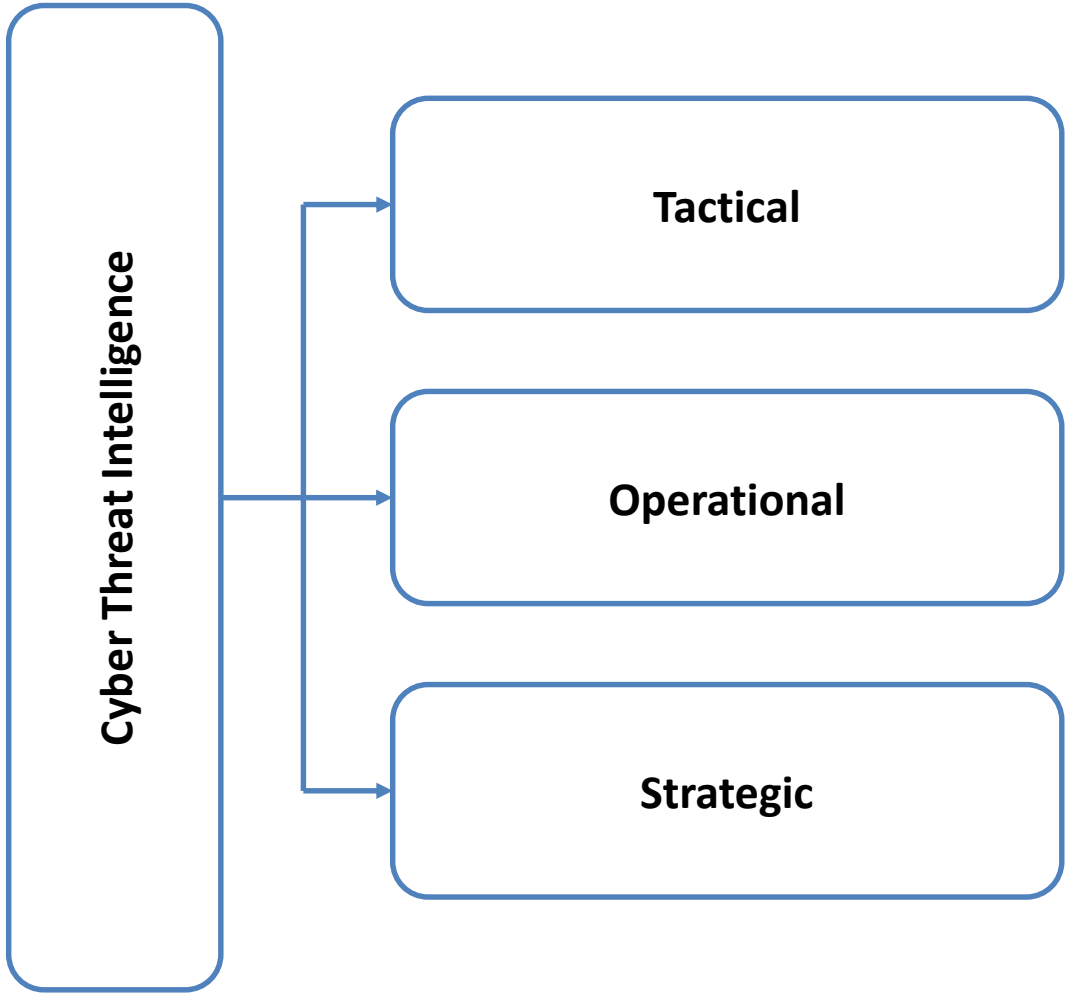
Tactical

Data from direct adversary action inside compromised systems

Examples

- Domains taken over by adversaries for spreading malicious code
- File signatures proving that a system has been infected

Cyber Threat Intelligence classification



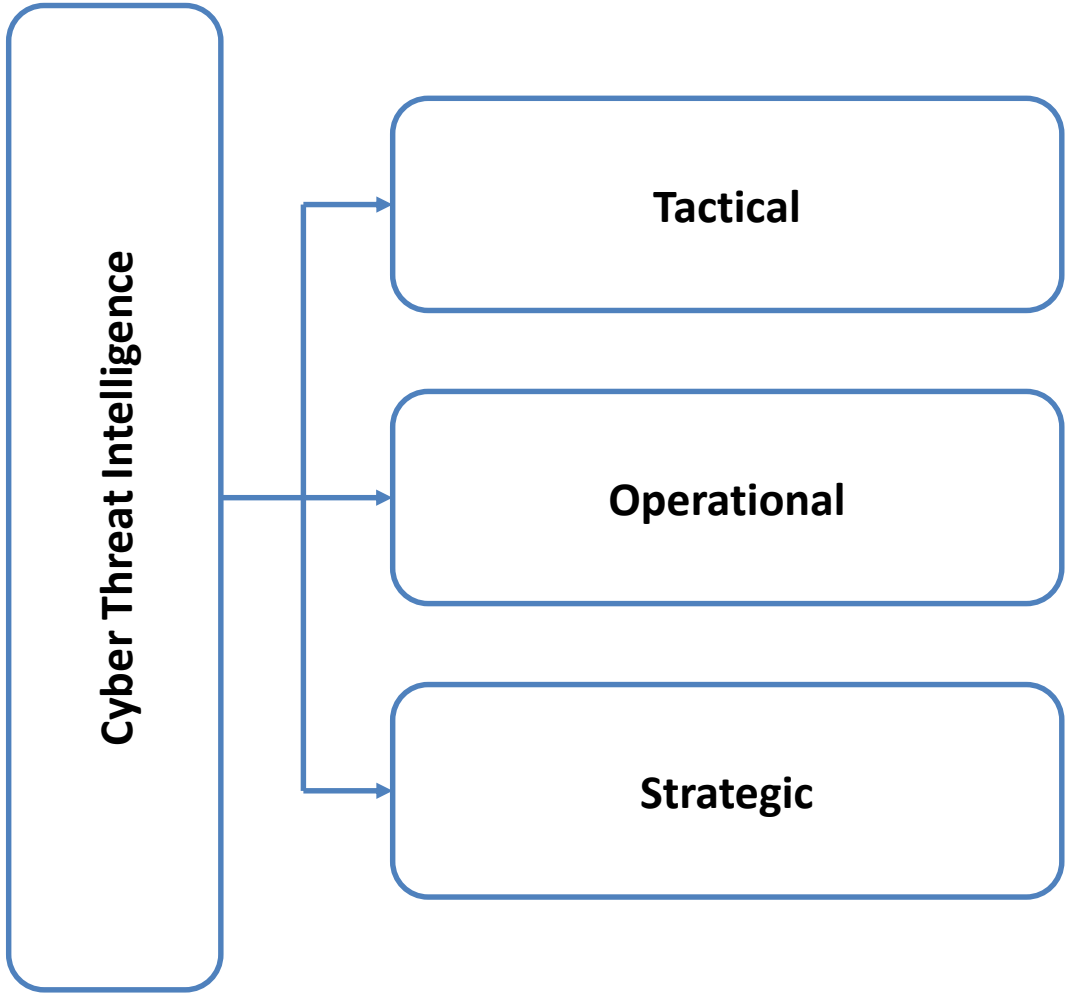
Operational

Information and reports useful for day-to-day decision-making

Examples

- Indicators that highlight current attack vectors being exploited
- Trend analysis determining the evolving capabilities of attackers

Cyber Threat Intelligence classification



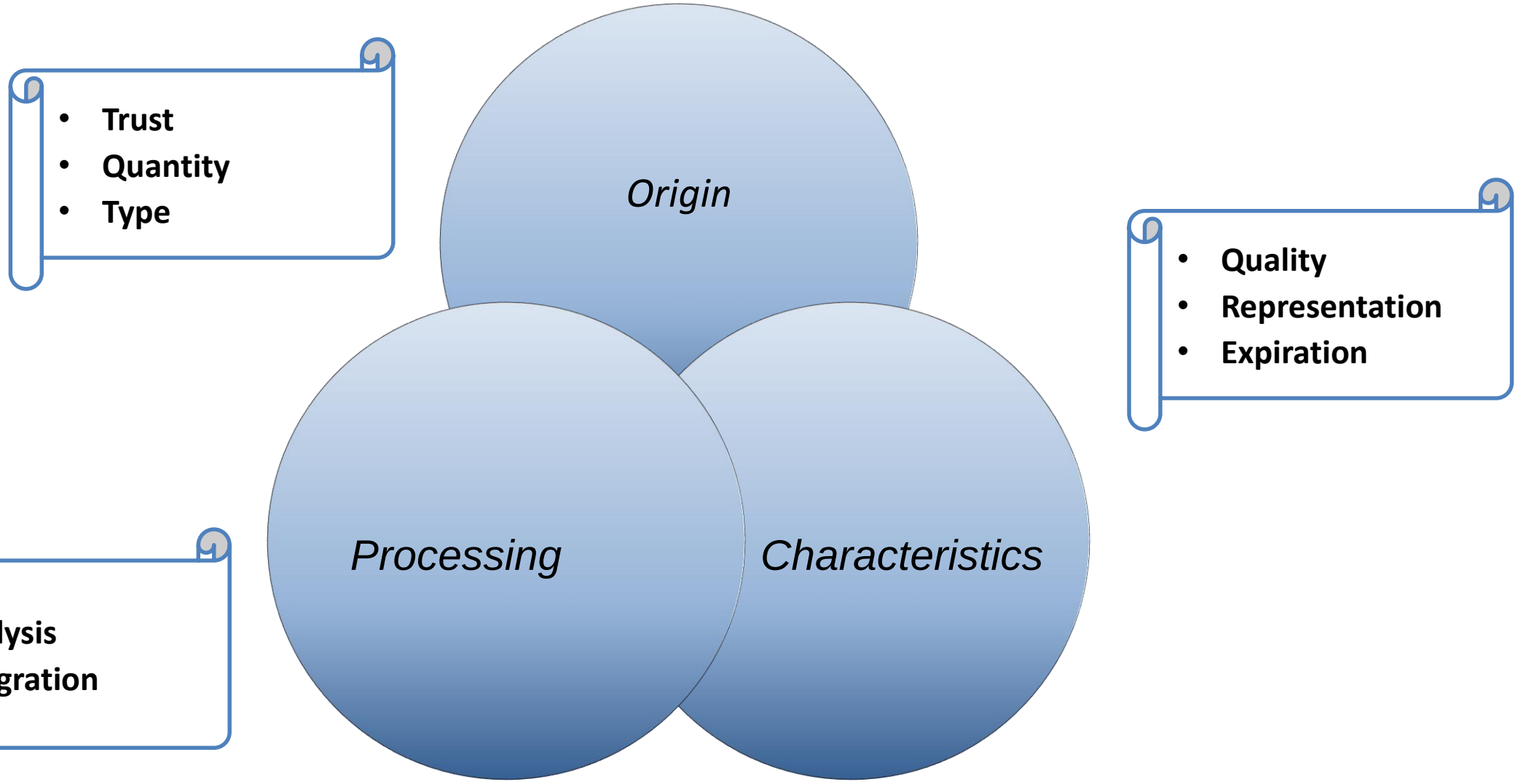
Strategic

Knowledge about threat actors' capabilities and motivations

Examples

- Information about emerging threats and possible mitigation
- Future threat scenarios and assessments on their impacts on businesses

Cyber Threat Intelligence sharing – Challenges and limitations



Organizations

FIRST

FIRST is the global Forum of Incident Response and Security Teams

Foundation: 1990

Mission statement:

"cooperatively handle computer security incidents and promote incident prevention programs"

- FIRST encourages cooperation between different teams through a mutual exchange of information, joint research activities and the implementation of common defense strategies in the event of large-scale attacks.
- FIRST members develop and share technical information, tools, methodologies, processes and best practices
- FIRST promotes the development of quality security products, policies and best practices
- FIRST promotes the creation and expansion of Incident Response teams and membership from organizations from around the world

TF-CSIRT

TF-CSIRT is the European Situational Awareness & Best Practice Sharing Community

Foundation: 2000

Mission statement:

"facilitate and improve the collaboration between the European CSIRT community"

TF-CSIRT

- Task force within GEANT for exchanging experiences and knowledge among European security teams within a trusted environment
- The Trusted Introducer Service forms the trusted backbone of infrastructure services and serves as clearinghouse for all security and incident response teams
- Liaison with ENISA, FIRST, APNIC
- TRANSITS provides affordable, high-quality training to both new and experienced Computer Security and Incident Response Team (CSIRT) personnel, as well as individuals with a bona-fide interest in establishing a CSIRT

EE-ISAC

EE-ISAC is the Information Sharing & Analysis Centre for the European Energy community

Foundation: 2015

Mission statement:

"helps utilities to improve the cyber security and resilience of their grid"

EE-ISAC

- Industry-driven, information sharing network of trust with the participation of public institutions (e.g., academia, governmental, non-profit foundations)
- Sharing on:
  - real-time security data & analysis
  - reports on security incidents and cyber breaches as well as future challenges
  - technical & operational experiences with applied security solutions
- Enabler for:
  - set up long lasting trust relationships with partners across the entire value chain
  - learn from their peer's experiences
  - compare & evaluate security solutions both from a technical and operational viewpoint

Standards

STIX – Structured Threat Information eXpression

Open-source language and serialization format used to exchange cyber threat intelligence

Current release: 2.0 (2.1 is currently under public review)

STIX™

Key aspects:

- It is comprehensive, flexible, extendable

Conveys information observed on a system or network (e.g., an IP address).

Contains a pattern that can be used to detect suspicious or malicious cyber activity.

A type of Tactics, Techniques, and Procedures (TTP) that describes ways threat actors attempt to compromise targets.

An action taken to either prevent an attack or respond to an attack.

A type of TTP, also known as malicious code and malicious software, used to compromise the confidentiality, integrity, or availability of a victim's data or system.

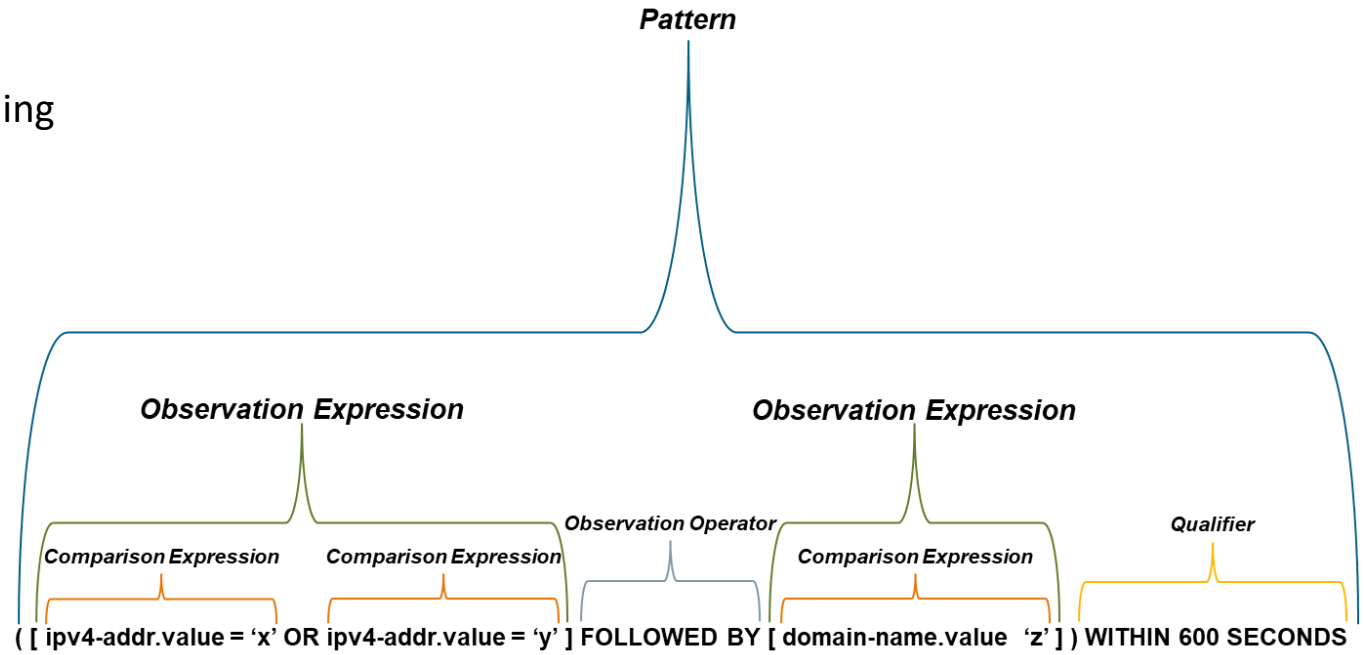
STIX – Structured Threat Information eXpression

Open-source language and serialization format used to exchange cyber threat intelligence

Current release: 2.0 (2.1 is currently under public review)

Key aspects:

- It is comprehensive, flexible, extendable
- It includes a query language: the STIX Patterning



STIX – Structured Threat Information eXpression

Open-source language and serialization format used to exchange cyber threat intelligence

Current release: 2.0 (2.1 is currently under public review)

Key aspects:

- It is comprehensive, flexible, extendable
- It includes a query language: the STIX Patterning
- It is part of an ecosystem of frameworks and tools

ATT&CK™
Adversarial Tactics, Techniques & Common Knowledge

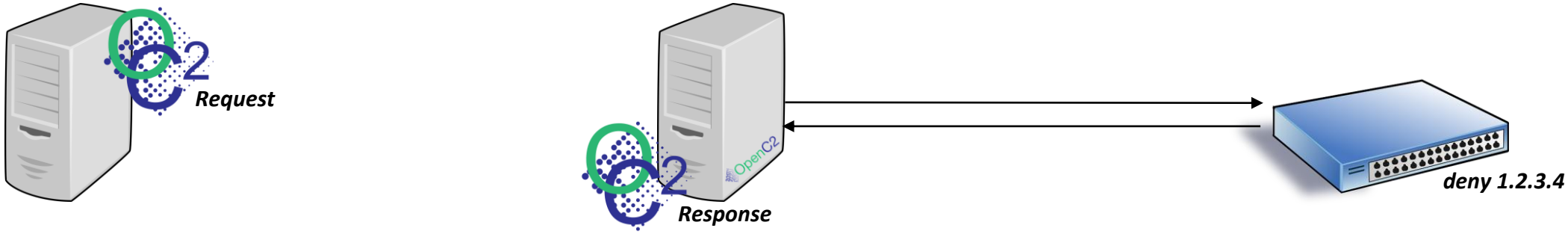
OpenC2 – Open Command and Control

Open-source language to enable the command and control of cyber defense components

Current release: 1.0

Key aspects:

- Focus on a comprehensive set of well-defined atomic actions to defend against a cyber attack or response to cyber incident
- OpenC2 works through the concept of “profiles”, defining the set of possible actions and responses for each component implementing that profile
- OpenC2 defines its operational model on top of HTTPS communications among the involved components



CACAO – Collaborative Automated Course of Action Operations

Open-source format encoding the steps for mitigating and responding to cyber attacks

Current release: 0.1

Key aspects:

- Focus on exchanging “playbooks”, such as descriptions of actions that operators (e.g., incident handlers) need to take to defend against security threats
- CACAO has formally started September 2019 and momentarily provides early concepts and collections of requirements
- As for the ideas discussed so far, CACAO would place itself on top of standards such as OpenC2 defining relationships among atomic “response” actions as well as describing the rules with which those actions can be updated and rearranged

Technologies

MISP – Malware Information Sharing Platform

MISP is the open-source threat sharing platform of choice for CONCORDIA

Project started: 2011 **Stakeholders:** CIRCL, NATO

Why: state of the art for threat intelligence sharing in Europe

Features

- Database to store technical and non-technical threat intelligence information
- Built-in sharing functionality to ease data exchange using different distributions modes
- Automatic correlation of the stored events
- Import/Export of data in multiple formats (e.g., direct creation of intrusion detection rules)
- Comprehensive set of APIs for integrating MISP to businesses' technology stacks
- Flexible data model and adjustable taxonomies

OTX – Open Threat Exchange

OTX is an open threat intelligence community enabling collaborative defense

Project started: 2012

Stakeholders: AT&T Cybersecurity (previously AlienVault)

Features

- OTX is the world's largest crowd-sourced computer-security platform (80,000+ participants in 140 countries who share more than 19 million potential threats daily)
- Cloud-hosted service
- Threat intelligence information sharing and checking (while protecting personal information)
- Information and statistics of cyber threats around the world
- Natural language processing and machine learning to facilitate the collection and correlation of data from many sources

CONCORDIA Platform

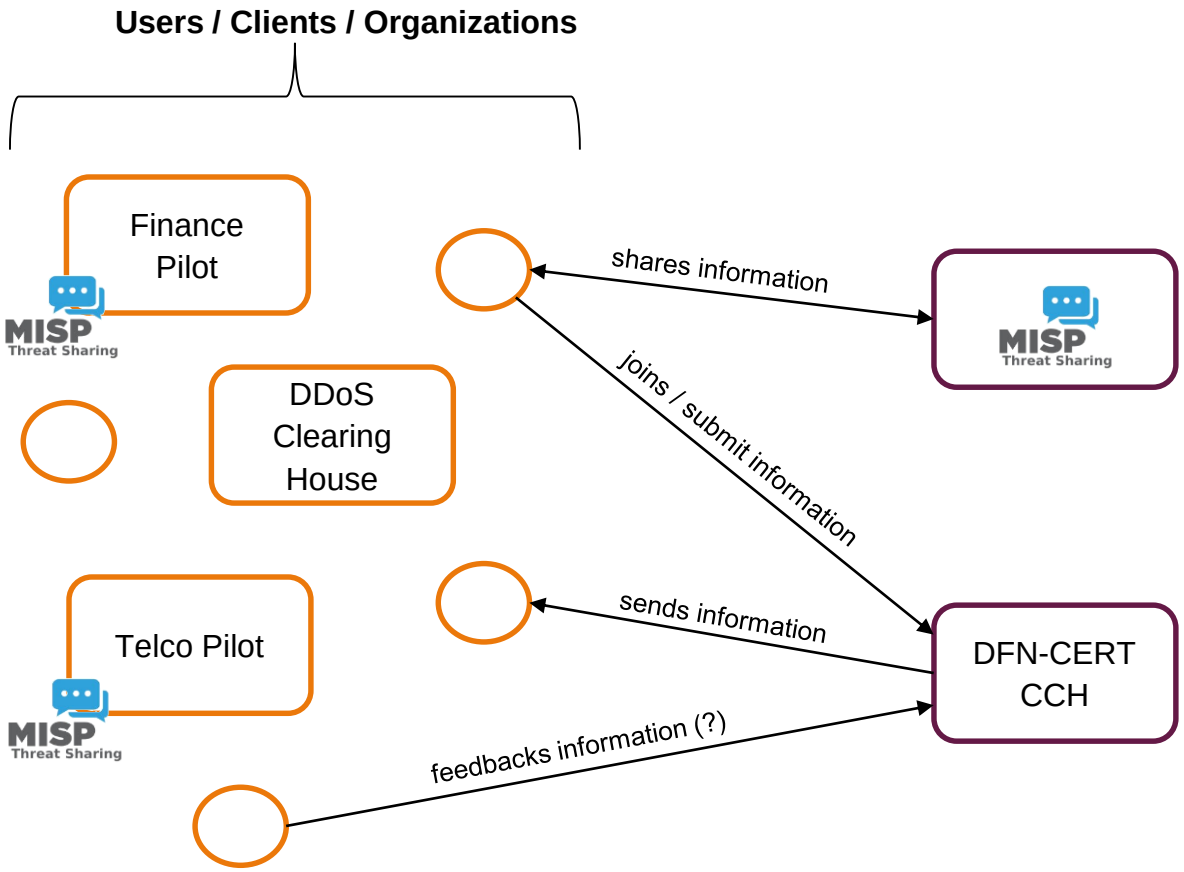
CONCORDIA Threat Intelligence Platform Outlines

"In addition to community building for the European stakeholders, CONCORDIA mission is to develop community data sharing solutions such Threat Intelligence for Europe…"

"Build an open-source Threat Intelligence platform for Europe for sharing Cybersecurity information across academic, industrial and other organizations, involving especially the European CERT community."

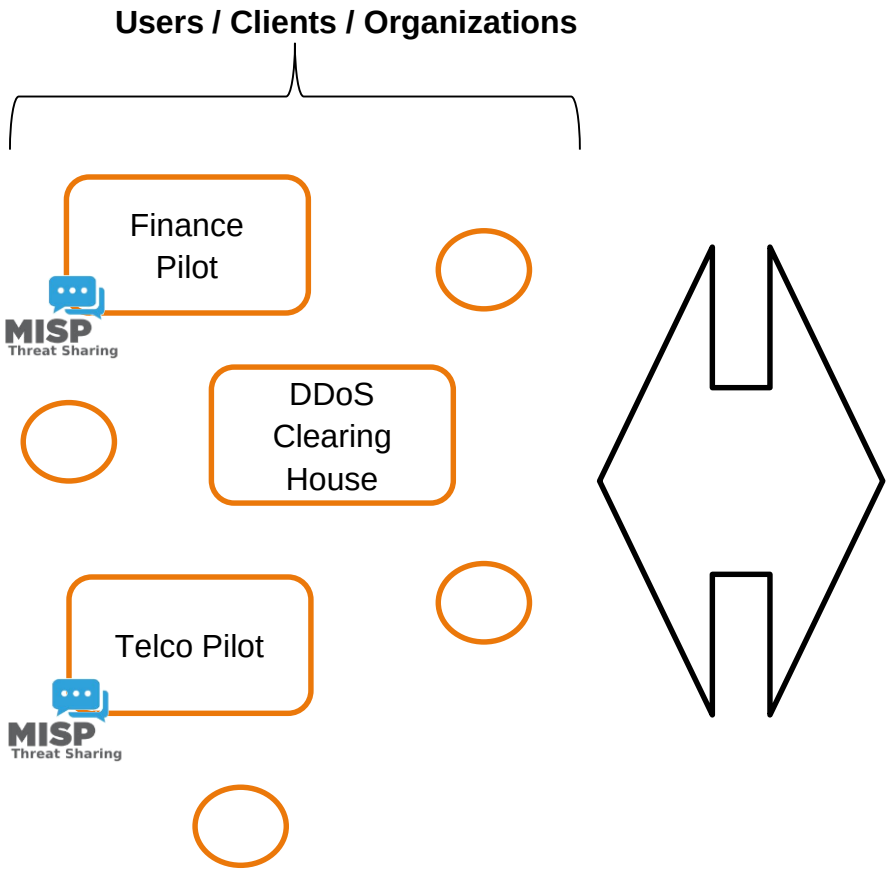
"Build a central threat intelligence platform for the exchange of actionable information related to security attacks or incidents to be used within the CONCORDIA consortium"

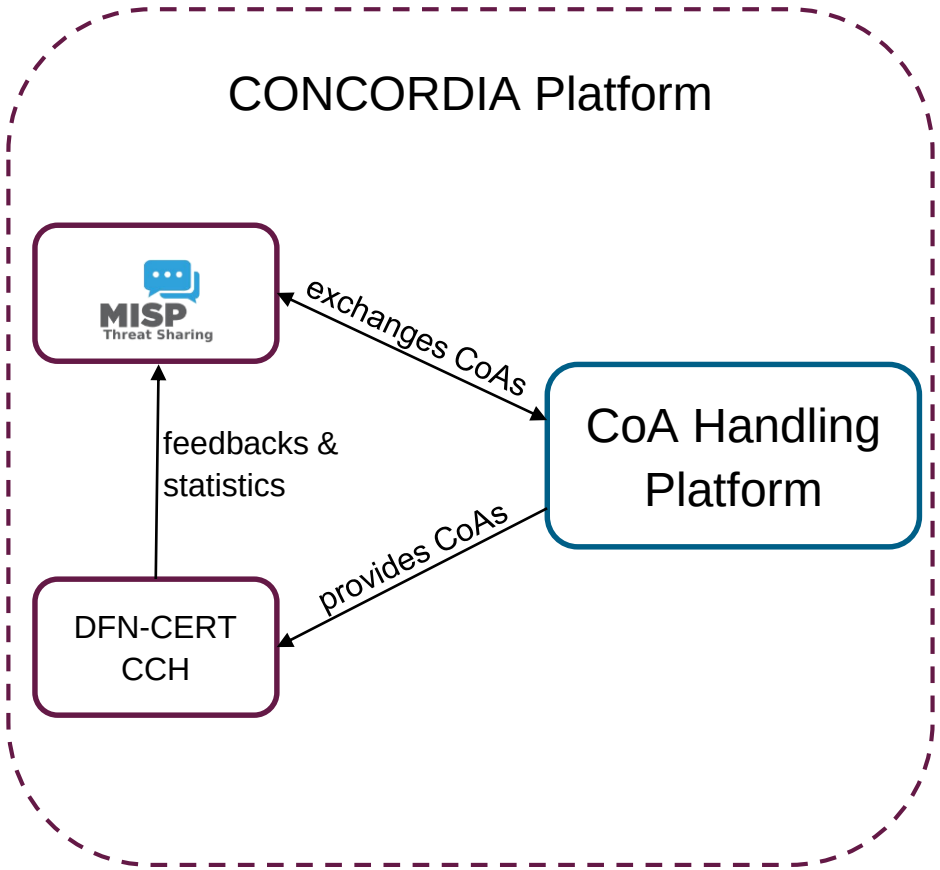
CONCORDIA Threat Intelligence Platform Overview



Current situation

CONCORDIA Threat Intelligence Platform Overview

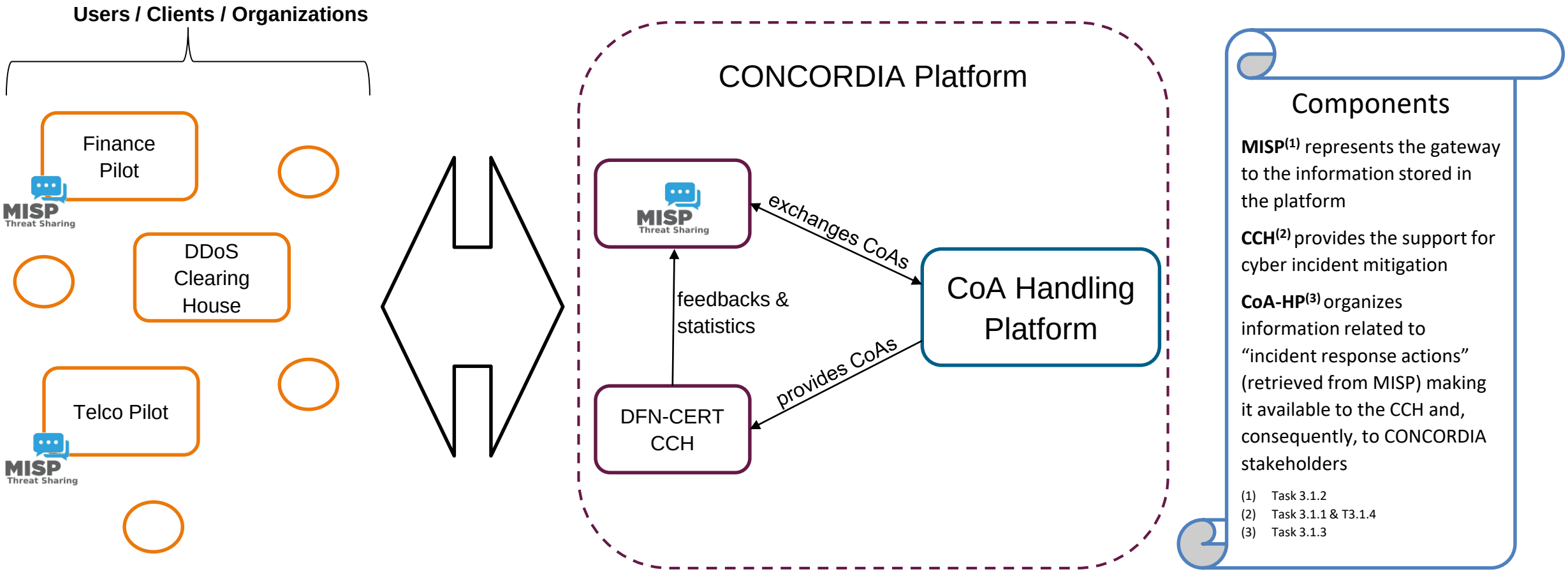




Proposal

The **CONCORDIA Platform** is a central virtual platform that supports threat intelligence sharing and cyber incident mitigation for CONCORDIA stakeholders.

CONCORDIA Threat Intelligence Platform Overview



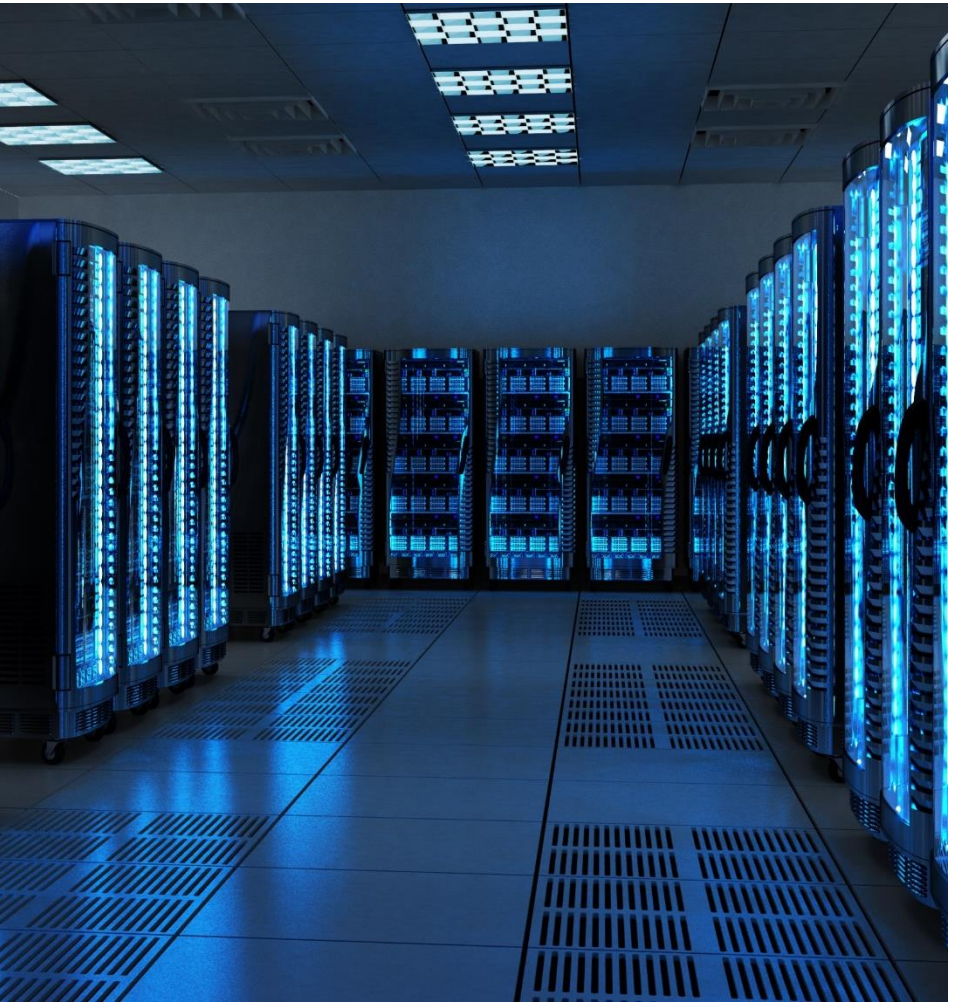
Components

MISP[1] represents the gateway to the information stored in the platform

CCH[2] provides the support for cyber incident mitigation

CoA-HP[3] organizes information related to "incident response actions" (retrieved from MISP) making it available to the CCH and, consequently, to CONCORDIA stakeholders

(1) Task 3.1.2
(2) Task 3.1.1 & T3.1.4
(3) Task 3.1.3



Thank you

Dr. Marco Caselli
Senior Key Expert
Siemens AG
Corporate Technology
E-mail: marco.caselli@siemens.com

Contact

Research Institute CODE
Carl-Wery-Straße 22
81739 Munich
Germany

contact@concordia-h2020.eu

Follow us

www.concordia-h2020.eu

www.twitter.com/concordiah2020

www.facebook.com/concordia.eu

www.linkedin.com/in/concordia-h2020

www.instagram.com/concordiah2020.eu