



**IDMEF V2 :
CYBER & PHYSICAL INCIDENT DETECTION FORMAT
THEORY & PRACTICE**

WEBINAR

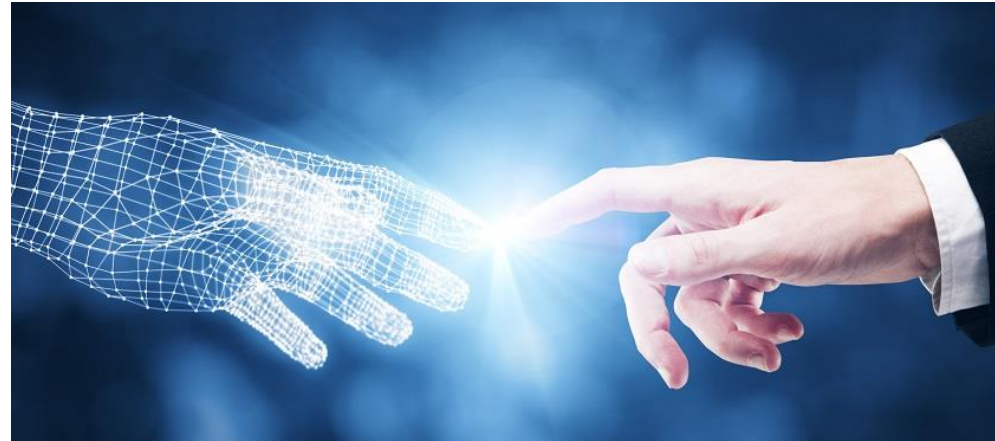
26 / 06 / 2025

Speakers

- Gilles Lehmann – IMT, France
 - Incident detection expert – IDMEFv2 Draft Author – System Architect
- Gabriele Giunta – ENGINEERING, Italia
 - Critical Infrastructure Protection Expert – Project Coordinator, Technical Manager
- Nicola Durante – ENGINEERING, Italia
 - Critical Infrastructure Protection Expert – IDMEFv2 implementation expert
- Cedric Gouy-Pailler
 - CEA, France, Head of the Artificial Intelligence and Machine Learning Laboratory



Introduction



Agenda

Introduction

IDMEFv2: Theory

IDMEFv2: Practice

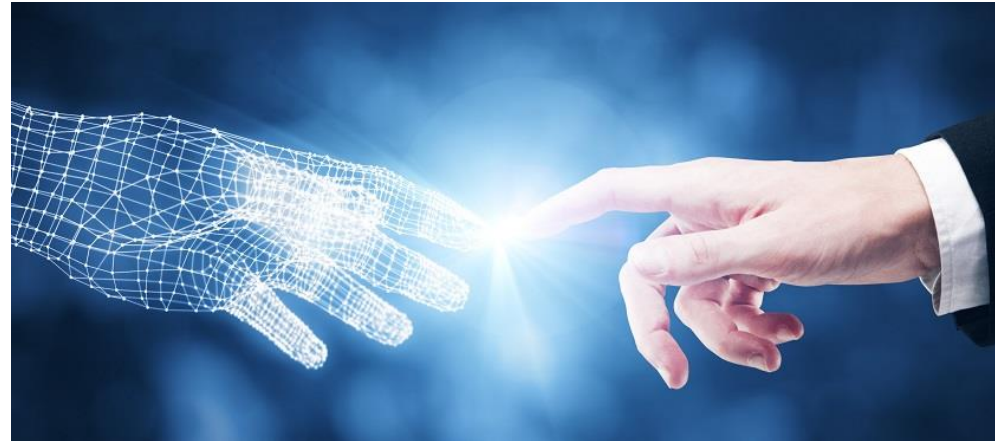
Conclusion / Q&A / Demonstration

Incident detection definition

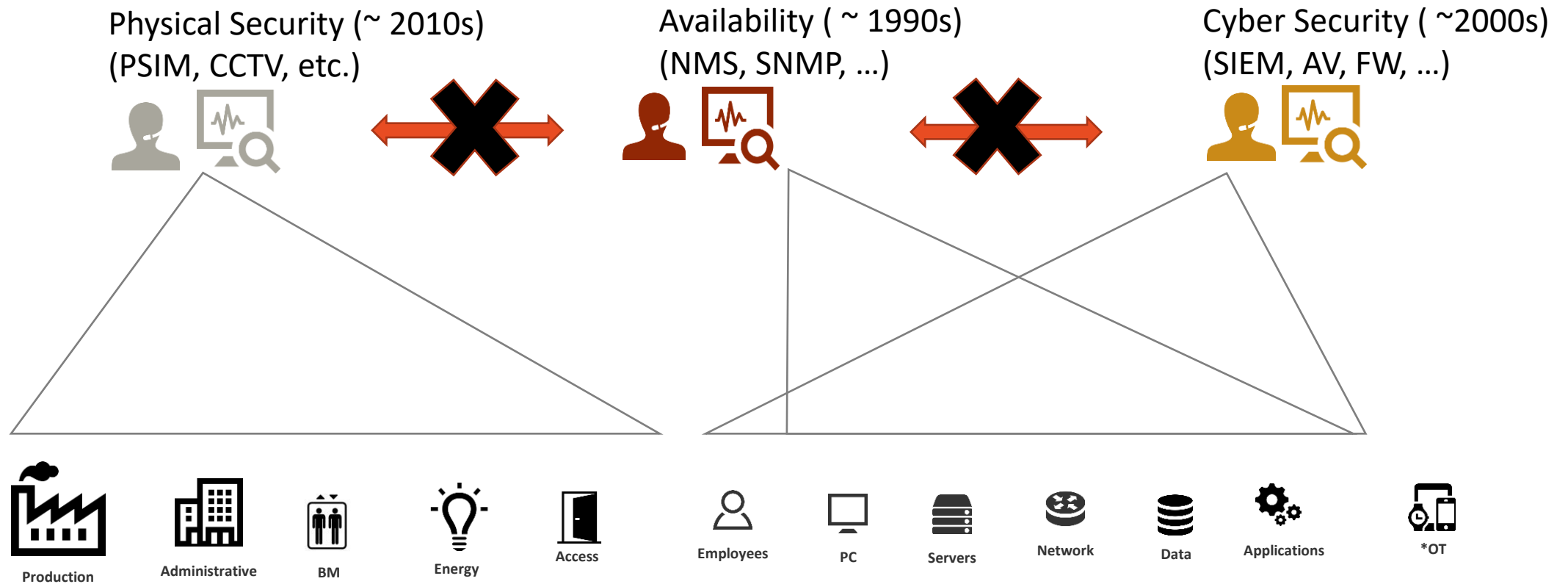
- Event
 - Anything that takes place or happens. An event is something that triggered a notice. Any incident starts off as an event or a combination of events, but not all events result in an incident. An event **need not be** an indication of wrongdoing
- Incident
 - An incident is an event that negatively affects an organization and requires immediate attention. An incident is an event that compromises or has a significant probability of compromising at least one of the organization's security criteria such as Confidentiality, Integrity or Availability.
- Incident detection is **the process of identifying threats by actively monitoring assets and finding anomalous activity**
- Incident examples:
 - Cyber intrusion in the finance server,
 - Physical intrusion in the data center,
 - An elevator breakdown,
 - A virus detected in a mail,
 - A heat wave announced for three days,
 -



IDMEFv2 : Theory



The problem : partitioned security monitoring



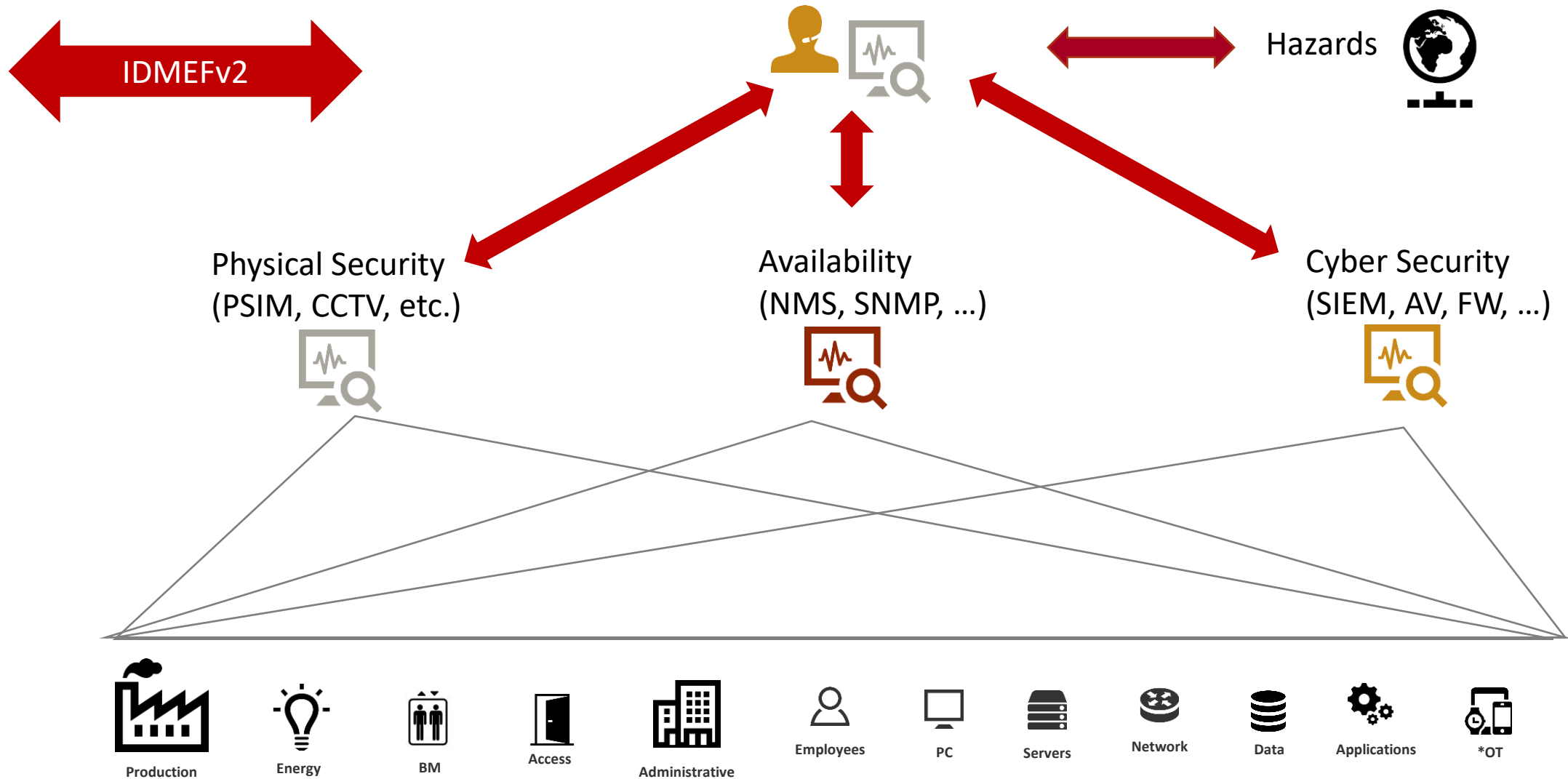
Partitioned security monitoring for a converging world

- 2020s: IoT/IIoT/everyT + smart [cities | transport | building | *younameit*]
 - => frontier between cyber and physical systems vanishing
- But security management systems are still compartmented (1990s legacy)
 - => Difficult to prevent/detect/respond to combined/complex incident or attacks.
 - Even CIA (Confidentiality-Integrity-Availability) monitoring is compartmented.
- Incidents are detected in separated tools/process:
 - No possible cross correlation or forensic
 - No team, resources and intelligence pooling
 - Complex and combined chained incidents or attacks can't be easily detected

Example : Why is my server not responding ?

- There are many reason why a server might not be responding :
 - cpu is 100 %, no more space on the disk, etc. (Availability)
 - the data is crypted by a cryptoware (Cyber)
 - there is an accidental (or intentional) fire in the server room (Physical)
 - the network card is damaged (Availability)
 - someone entered the server room and intentionally disconnected the server (Physical + Availability)
 - Someone entered the server (connected) and intentionally disconnected the server (cyber + cyber)
 - someone hacked the badger system, entered the server room and stole the server ... (Physical + Physical)
 - strong heat wave outside and the air conditioning in the datacenter is not working resulting on servers over heating and crashing down (Hazard + availability)
 - WCS: A Shahed drone destroyed the data center (physical)
 - etc.
- All those incidents should be reported/consolidated in the same monitoring platform.

The solution : unified security monitoring



IDMEFv2 : Incident Detection Message Exchange Format

- A universal JSON alert format for reporting « all » kind of incidents :
 - Cyber / IT : AV, FW, IDS, WAF, ... SIEM
 - Physical : CCTV, Movement detector, Badger, ... PSIM
 - Availability : performance management ... NMS
 - Hazards (Natural & Man Made) : storm, cold, pollution, fire, ...
- Security monitoring convergency objectives :
 - Improve prevention / detection / reaction
 - Reduce costs (human & material)

Less cost for more efficiency !

Incident detection formats : short state of art

- Cyber Security
 - Many proprietary format (essentially log format) but no universal standard
 - IDMEFv1 used in open-source but never really crossed the “commercial” line
 - Some log format standards initiatives (CEE (Dead), OCSF, ...)
- Physical Security
 - Newer domain , no identified standard
- Availability
 - SNMP for pooling and traps for incident notification
- Hazards
 - Destined to gain prominence due to climate change, few formats (CAP)

IDMEFv2 is the only format filling a need.
TINA!



CyberSecurity Formats

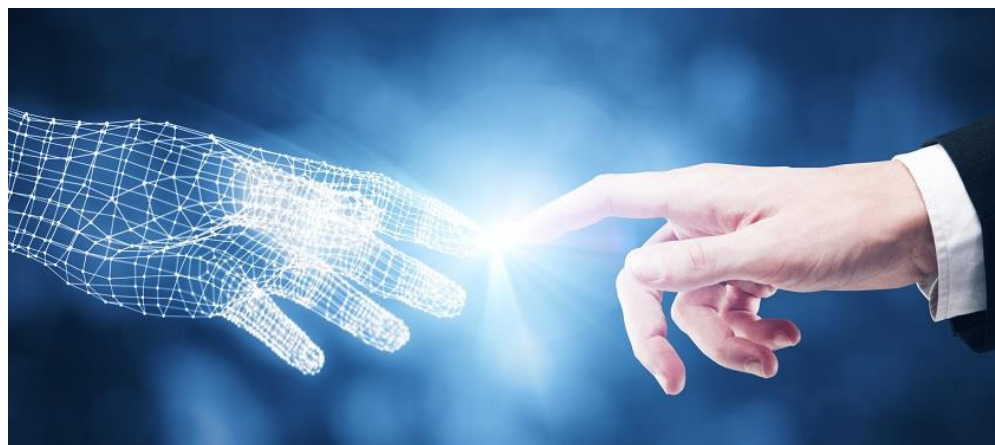
- **STIX** : Structured Threat Information Expression
 - CTI oriented
- **OCSF** : **Open Cybersecurity Schema Framework**
 - Very large and powerfull initiative (Splunk, AWS, IBM, etc.)
 - Cyber security Log/event oriented (Splunk ...)
 - No physical / hazards / availability/ etc ... yet)
 - No detection / correlation / agregation / Relation / enrichment
 - Choosed exhaustivity vs simplicity ...
 - *“In spirit, OCSF is like a next-generation, structured and standardized version of Syslog”*
- Those two formats are complementary to IDMEFv2 but not the same goal nor the same perimeter.



IDMEFv2

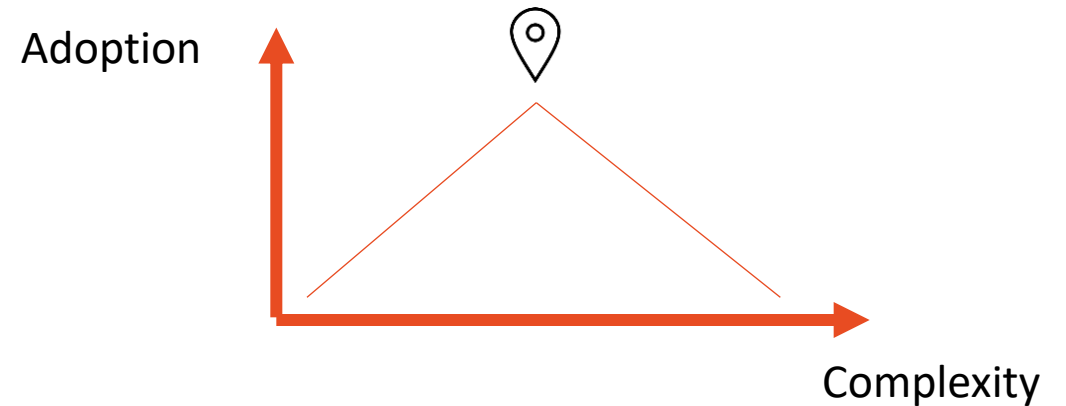
2.D.V05

Brief technical introduction



IDMEFv1 feedback

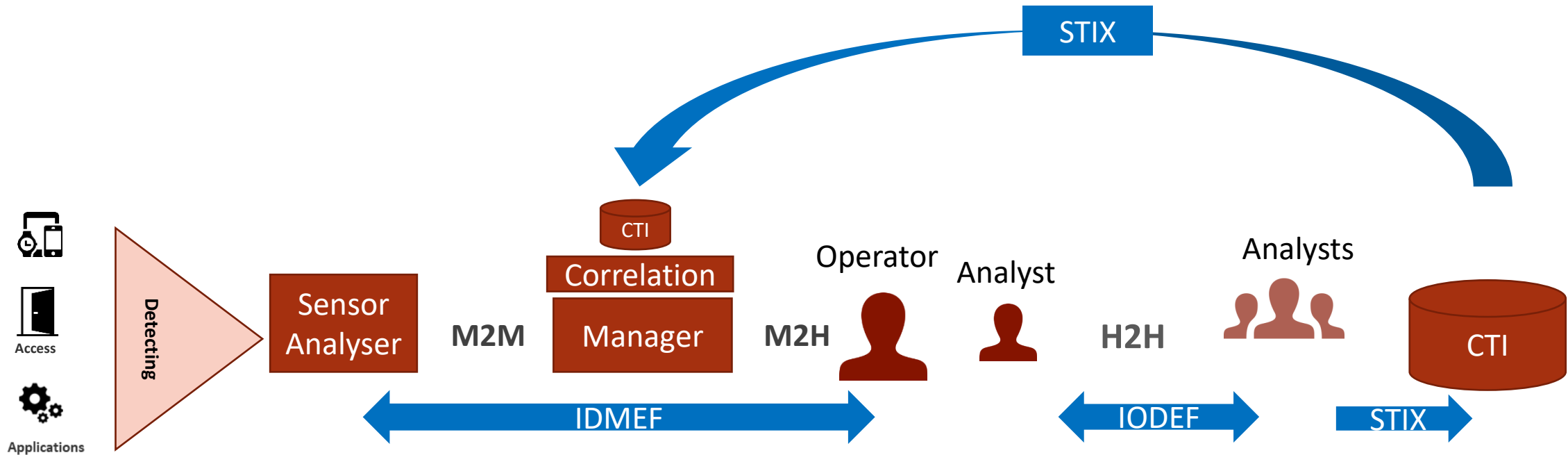
- LESS IS MORE / KISS
 - Exhaustivity leads to complexity
 - Deep Learning curve
 - Complex daily programming, operating, etc.
 - Not good for adoption !
- Incident detection focused
 - Not exhaustive logging nor analysis
- Cyber & Physical SECURITY (CIA...)
- Attribute enumeration everywhere possible
- End to end format



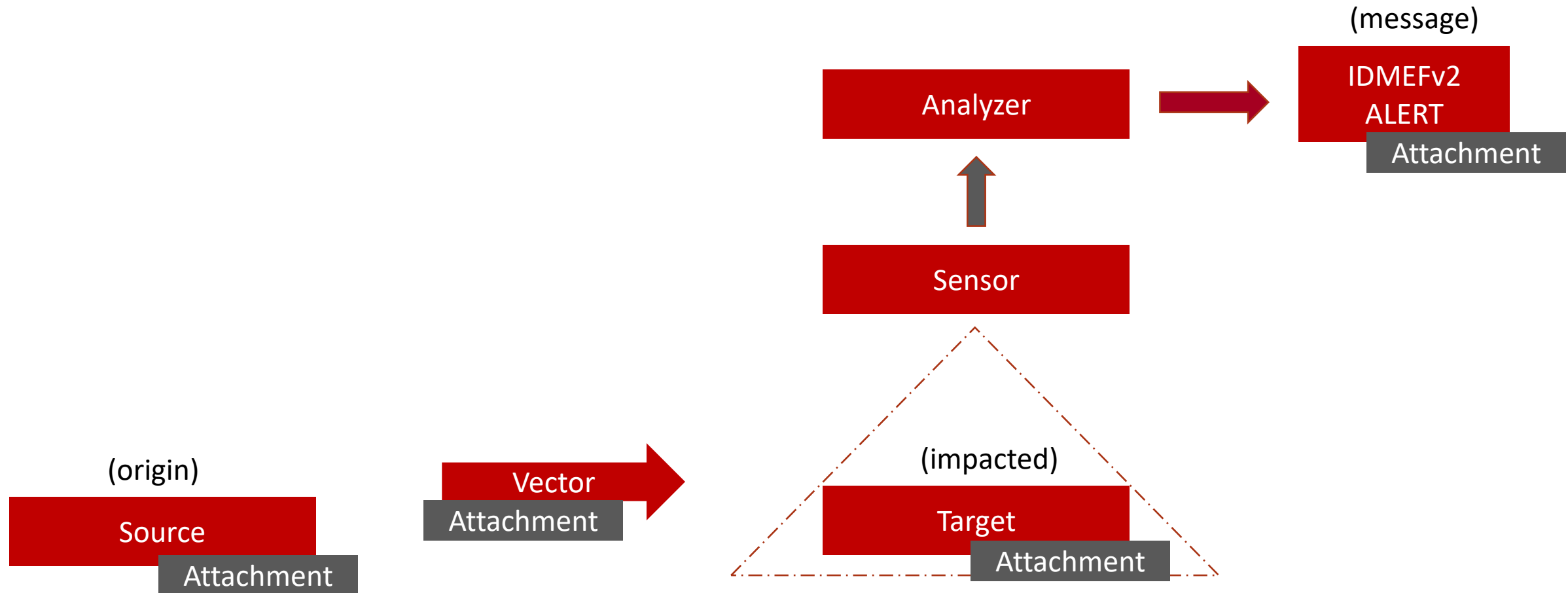
Source: <https://www.idmefv2.org/index.php/standardization-principles/>

IDMEF : End to end Detection only

- IDMEF : Incident **Detection** Message Exchange Format
- IODEF : Incident Object **Definition** Exchange Format
- STIX : Structured Threat Information Expression (OpenCTI)
- CTI : **Cyber threat intelligence** (CTI) is knowledge, skills and experience-based information concerning the occurrence and assessment of both cyber and physical threats and threat actors that is intended to help mitigate potential attacks and harmful events occurring in cyberspace (Wikipedia)



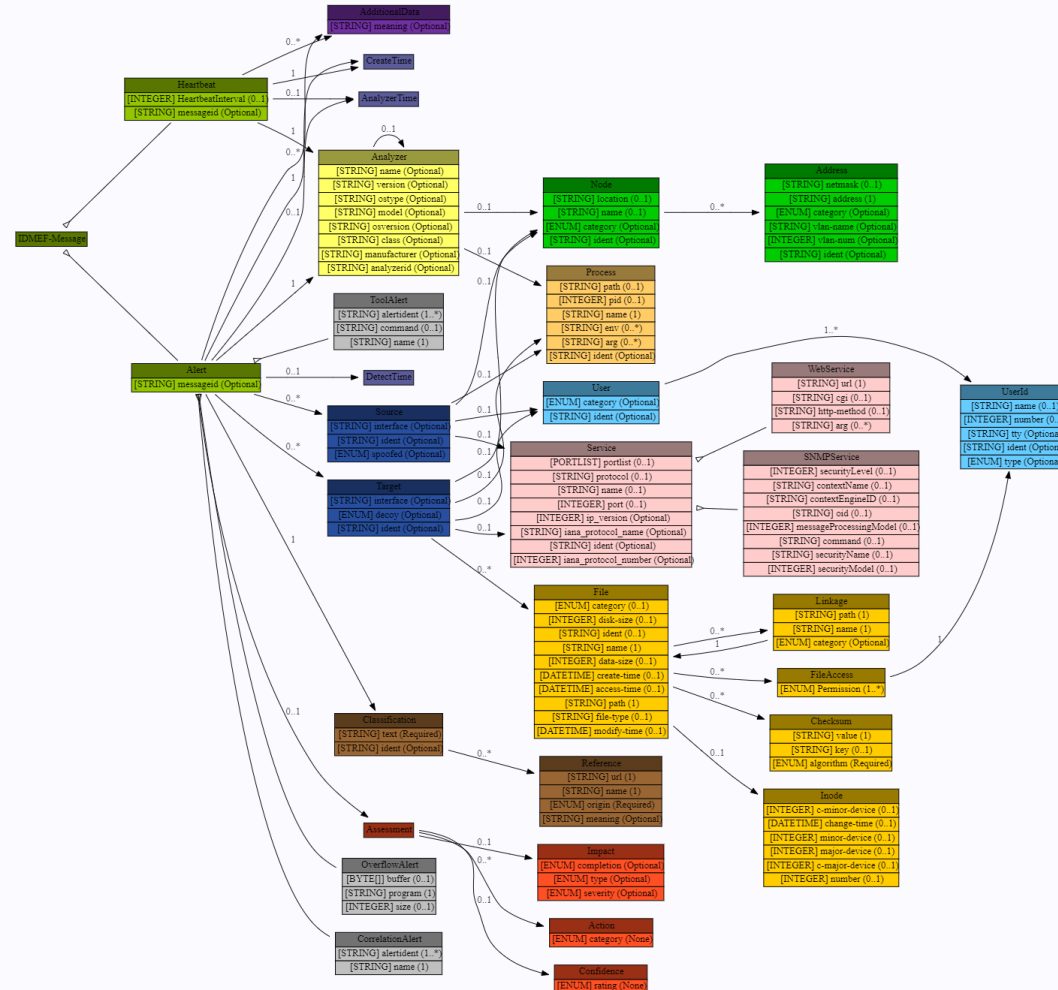
IDMEFv2 classes



IDMEFv1 classes ...

IDMEF-Message

All IDMEF messages are instances of the IDMEF-Message class; it is the top-level class of the IDMEF data model, as well as the IDMEF DTD. There are currently two types (subclasses) of IDMEF-Message: Alert and Heartbeat.



ALERT CLASS

•	STRING	Version	
•	UUID	ID	
•	STRING	OrganisationName / STRING	OrganisationId
•	STRING	EntityName / STRING	EntityId
•	ENUM[]	Category / STRING	ext-Category
•	ENUM	Cause	Intrusion.Burglary, Meteorological.Fog, Abusive.Spam
•	STRING	Description	Normal, Error, Malicious, Malfunction, Hazard, Unknow
•	ENUM	Status	Event / Incident
•	ENUM	Priority	Info, Low, Medium, High
•	FLOAT	Confidence	0 to 1
•	STRING	Note	
•	TIMESTAMP	CreateTime / TIMESTAMP	StartTime / TIMESTAMP
•	STRING[]	AltNames	EndTime
•	STRING[]	AltCategory	MISP, MITRE ATT@CK
•	URI[]	Ref	
•	UUID[]	CorrelID	Correlation
•	CONDITION[]	AggrCondition	Aggregation: List of IDMEFv2 attributes
•	UUID[]	PredID / UUID[]	RelID
			Previous / related alerts



Analyzer Class

- IP IP
- STRING Name
- STRING Hostname
- STRING Model Name, Brand, Version
- ENUM[] Type Cyber, Physical, Availability, Combined
- ENUM[] Category VAD, ADS, DDOS, HIDS, 3DLas, SIEM, NMS, ...
- STRING ext-Category
- ENUM[] Data Light, Temperature, Datagram, Log, SNMP, ...
- STRING ext-Data
- ENUM[] Method Biometric, Heuristic, Signature, ...
- STRING ext-Method
- GEOLOC GeoLocation +48.75726,+2.299528,+65.1
- UNLOCODE UnLocation GR ATH (<https://unece.org/trade/cefact/unlocode-code-list-country-and-territory>)
- STRING Location « Data Center », « Front Yard », « Room 306 », « Cafeteria », ...

Sensor Class

- IP IP
- STRING Name Front door camera
- STRING Hostname camera1.acme.com
- STRING Model
- GEOLOC GeoLocation
- UNLOCODE UnLocation
- STRING Location
- STRING CaptureZone

Source Class

- | | |
|--------------|-------------|
| • IP | IP |
| • STRING | Hostname |
| • STRING | Note |
| • STRING[] | TI |
| • STRING | User |
| • EMAIL | Email |
| • PROTOCOL[] | Protocol |
| • INT[] | Port |
| • GEOLOC | GeoLocation |
| • UNLOCODE | UnLocation |
| • STRING | Location |
| • ID[] | Attachment |

Threat Intelligence information

Target Class (Impacted asset)

- IP IP
- STRING Hostname
- STRING Note
- STRING Service
- STRING User
- EMAIL Email
- INT[] Port
- GEOLOC GeoLocation
- UNLOCODE UnLocation
- STRING Location
- ID[] Attachment

Vector Class

- | | | |
|------------|--------------|--------------------------------|
| • ENUM[] | Category | drone, human, email, file, ... |
| • STRING | ext-Category | |
| • STRING | Name | |
| • STRING | Note | |
| • STRING[] | TI | |
| • GEOLOC | GeoLocation | |
| • FLOAT | GeoRadius | |
| • UNLOCODE | UnLocation | |
| • STRING | Location | |
| • ID[] | Attachment | |



Attachment

- ID Name
- STRING FileName
- HASH[] Hash sha-256: 01ba4719c80b6fe911b091a7c05124b64eece964e09c058ef8f9805daca546b
- INT Size
- URI[] Ref
- URI[] ExternalURI
- STRING Note
- MEDIATYPE ContentType audio/x-wav, image/jpeg, ...
- STRING ContentEncoding JSON, Base64
- STRING Content

IDMEFv2 : simplified cyber example

```
{
  "Version": "2.0",
  "ID": "819df7bc-35ef-40d8-bbee-1901117370b2",
  "Description": "Authentication failed on root account",
  « Priority": "Medium",
  "CreateTime": "2021-05-10T16:55:29.196408+00:00",
  « StartTime": "2021-05-10T16:55:29.196408+00:00",
  "Category": [ "Attempt.Login"],
  "Analyzer": {
    "Name": « Acme SIEM",
    "IP ": "192.0.2.1",
    "Type": "Cyber",
    "Category": [ "SIEM", "LOG" ],
    "Source": [ {
      "IP": "192.0.2.17"} ]
    "Target": [ {
      "IP": "192.0.2.2",
      "User": "root" },
      "GeoLocation": "+48.75726,+2.299528,+65.1“,
      “Location”; “Data Center”
    ]
  }
}
```

- Failed authentication on a root account
- Someone connected on 192.0.2.17 failed to log in on 192.0.2.2 on the root account the 10/05/2021 at 16:55.
- The incident has been detected by a SIEM analysing logs.

IDMEFv2 : simplified physical example

```
{
  "Version": "2.0",
  "ID": "e5f9bbae-163e-42f9-a2f2-0daaf78febf1",
  "Status": "Incident",
  "Type": "Physical",
  "Entity": "Acme",
  "CreateTime": "2021-01-18T23:33:05.21Z",
  "StartTime": "2021-01-18T23:33:04.52Z",
  "Cause": "Malicious",
  "Category": [ "Intrusions.Burglary" ],
  « Priority": "Medium",
  "Confidence": 0.9,
  "Description": "Physical intrusion detected",
  "Analyzer": {
    "IP": "172.10.5.31",
    "Name": "Front door camera",
    "GeoLocation": "+48.75726,+2.299528,+65.1",
  },
  "Target": [ { "Location": "Front Garden" } ],
  "Vector": [ {
    "Category": [ "Human" ],
    "Attachment": [ "Picture" ]
  } ],
  "Attachment": [ {
    "Name": "Picture",
    "FileName": "img2021011823330521.jpg",
    "ExternalURI": [ https://data.acme.eu/img2021011823330521.jpg ],
    "ContentType": "image/jpeg"
  } ]
}
```

- A “human” has been detected in the front garden by « Human Activity Recognition » by “Front Door Camera” at 23:33 the 19/01/21.
- An URL pointing to a picture taken by the camera is attached to the message.

IDMEFv2 : simplified availability example

```
{
  "Version": "2.0.3",
  "ID": "e5f9bbae-163e-42f9-a2f2-0daaf78fefb1",
  "Status": "Incident",
  "Entity": "ACME",
  "CreateTime": "2021-01-18T23:33:05.21Z",
  "StartTime": "2021-01-18T23:33:04.52Z",
  "Category": [
    "Availability.Outage"
  ],
  "Confidence": 1.0,
  "Priority": "Critical",
  "Description": "CRITICAL - 172.10.5.31: rta nan, lost 100%",
  "Analyzer": {
    "IP": "172.10.1.1",
    "Name": "Local NMS",
    "Hostname": "nms.acme.com",
    "Type": "Availability",
    "Model": "Super NMS v5.2",
    "Category": [
      "NMS"
    ],
  },
  "Target": [
    {
      "IP": "172.10.5.31",
      "Hostname": "camera1.acme.com",
      "GeoLocation": "+48.75726,+2.299528,+65.1",
      "UnLocation": "GR ATH",
      "Location": "Front Door"
    }
  ]
}
```

- « camera1.example.com », 172.10.5.31, located on the front door of ACME building is not responding to ping request since 23:33 the 10/01/2021.

IDMEFv2 : simplified hazard example

```
{
  "Version": "2.0.3",
  "ID": "e5f9bbae-163e-42f9-a2f2-0daaf78fefb1",
  "Status": "Incident",
  "Entity": "ACME",
  "CreateTime": "2021-01-21T10:00:00.21Z",
  "StartTime": "2021-01-23T08:00:00.52Z",
  "EndTime": "2021-01-25T08:00:00.52Z",
  "Category": [
    "Meteorological.Storm"
  ],
  "Confidence": 0,5,
  "Priority": "Critical",
  "Description": "Heavy Storm on Athenes",
  "Analyzer": {
    "IP": "172.10.1.1",
    "Name": "Weather Analyzer",
    "Hostname": "https://wheather.acme.com/",
    "Type": "Hazards",
  },
  "Target": [
    {
      "GeoLocation": "+48.75726,+2.299528,+65.1",
      "UnLocation": "GR ATH",
      "Location": "ACME Office"
    }
  ]
}
```

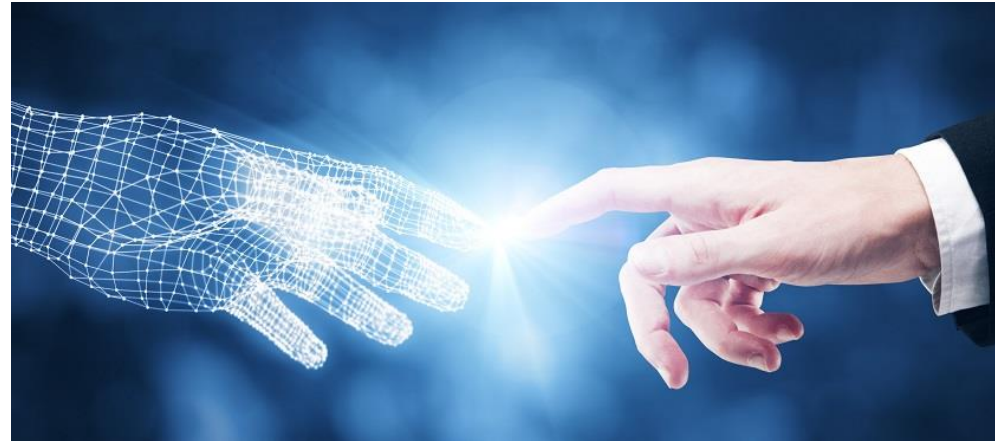
- Heavy storm is expected on Athenes starting next Wednesday at 10.00h for approximately 48 hours.

IDMEFv2 four pillars

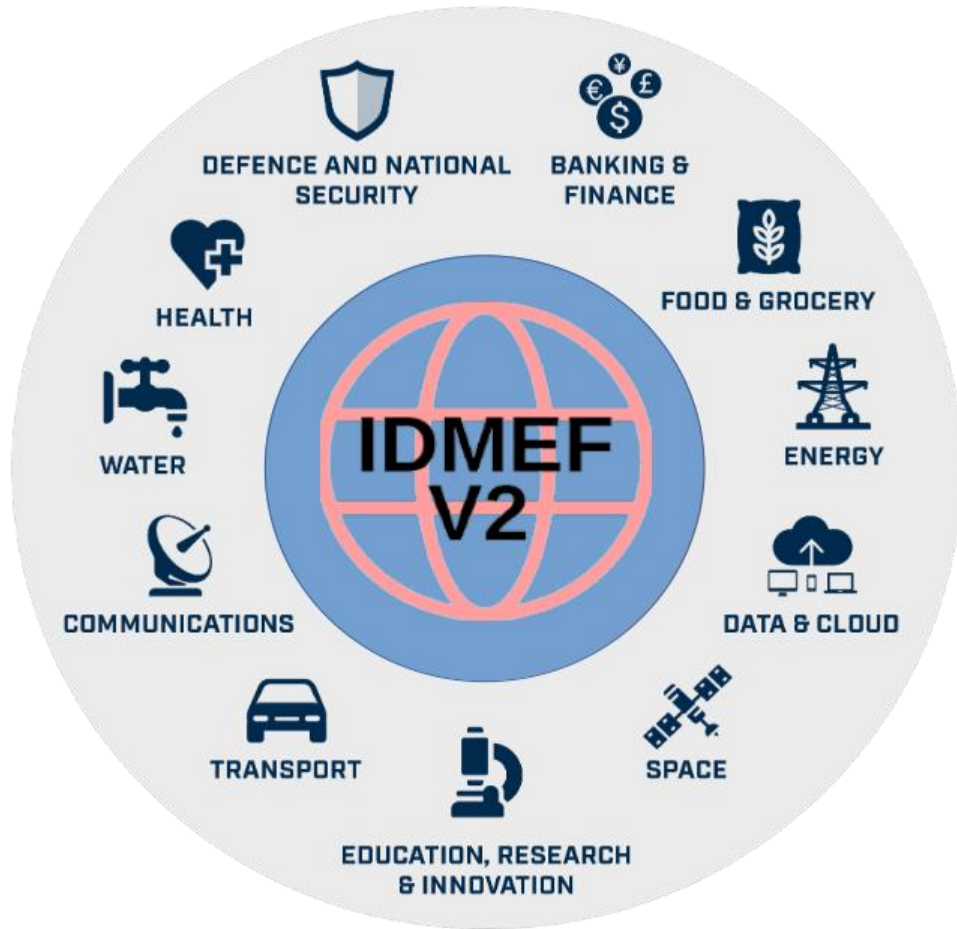
- Universal
 - Cyber & Physical / CIA / Hazards
 - Five dimensions : Space (x3), Time and « IP »
- Wide incident classification
 - Based on ENISA RIST (Reference Security Incident Taxonomy) work group
 - Centre for Research on the Epidemiology of Disasters (CRED): Disasters
- Simple and focused
 - Limited number of classes/attributes (and easy extension)
 - **Incident detection only**
 - JSON, HTTPs, Kafka
- End to end
 - From the Analyzer to the Operator



IDMEFv2 Use cases



IDMEFv2 & Critical Infrastructure



- IDMEFv2 has been designed for critical infrastructure security
- International collaboration with a H2020 project (7shield.eu)
- 7SHIELD : Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of **physical and cyber threats**

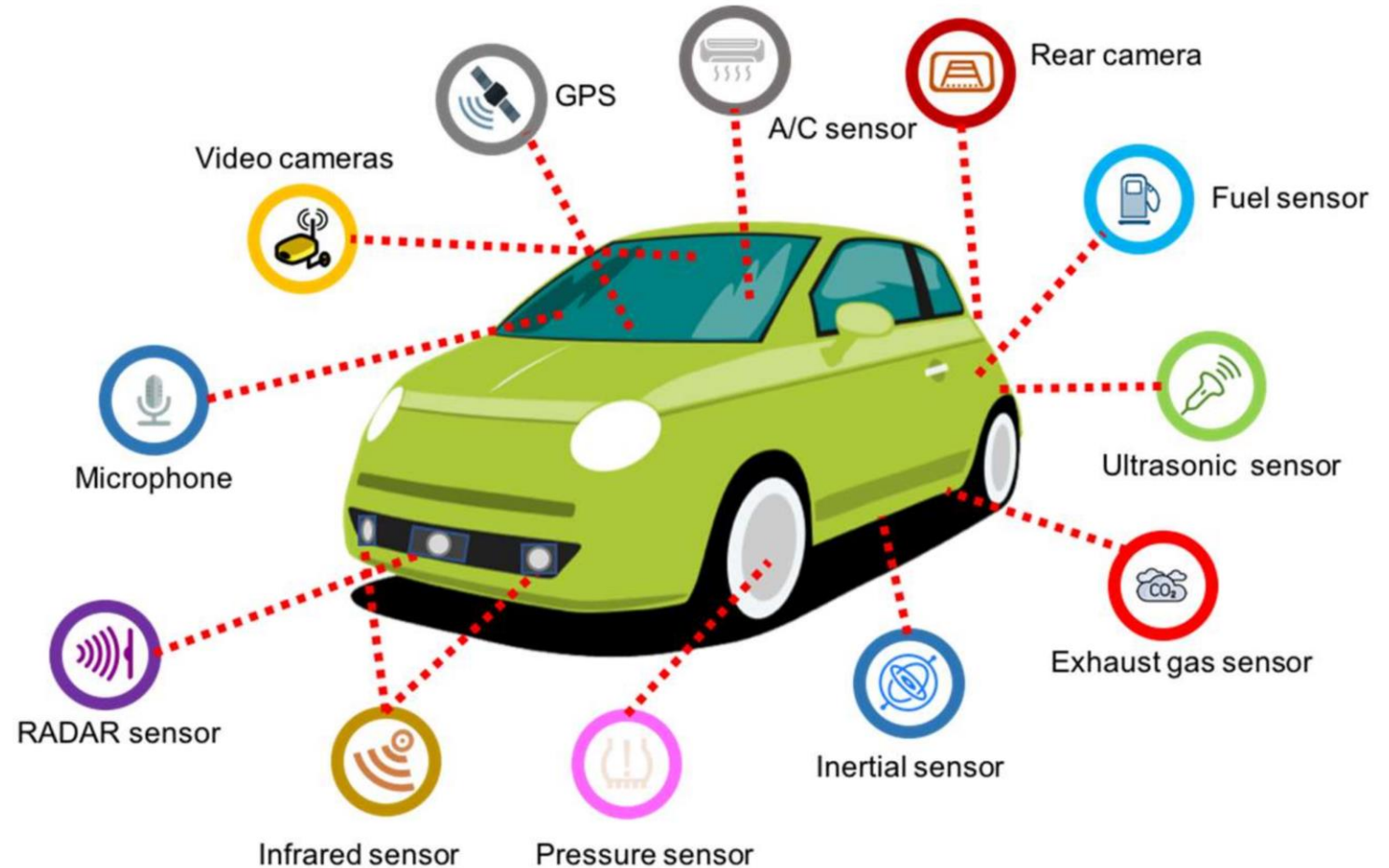
IDMEFv2: smart systems



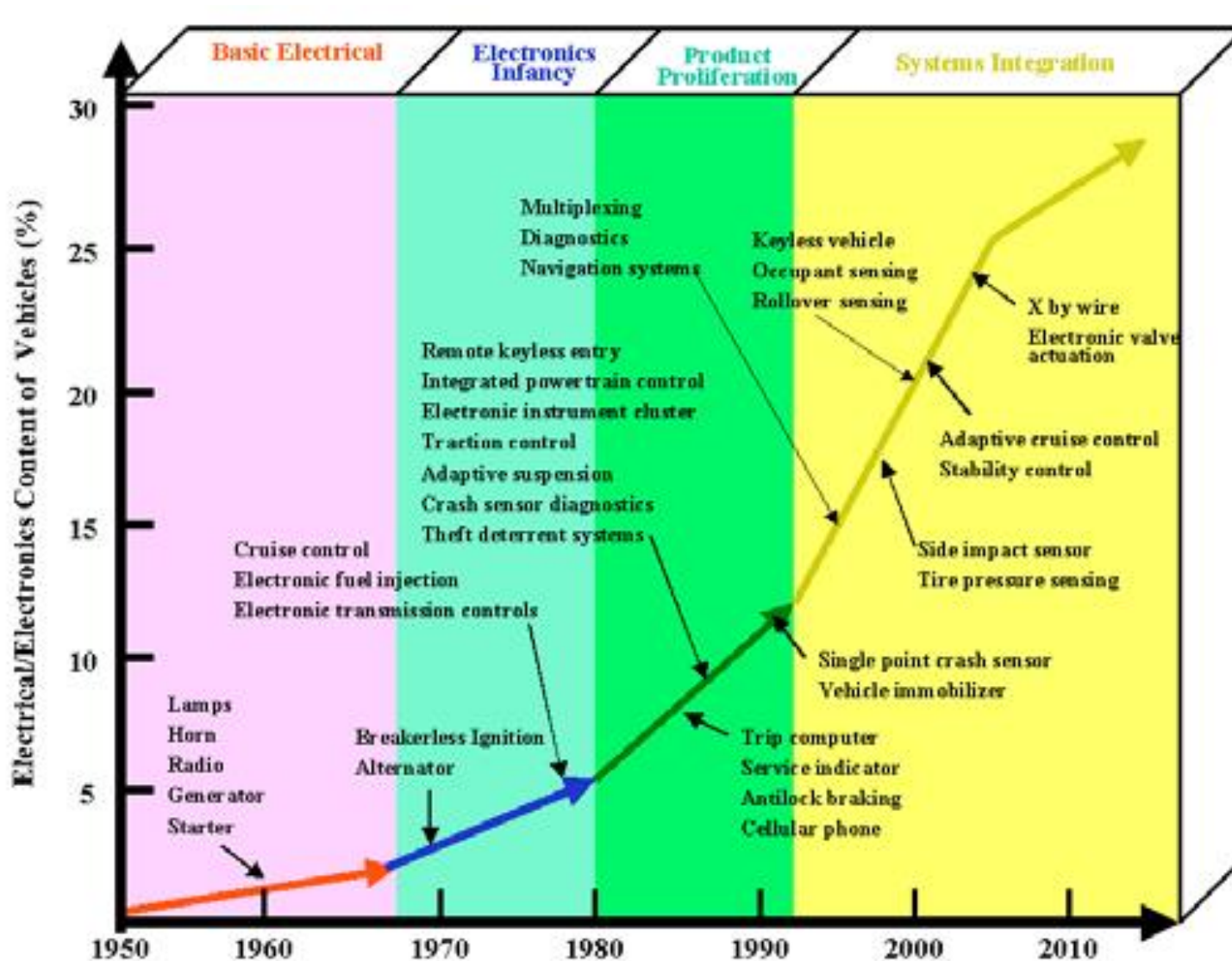
- **Smart systems** incorporate functions of **sensing**, actuation, and control in order to describe and **analyze** a situation and make decisions.

Example : connected vehicle

- Sensors can detect (physical) incidents but can also be potential (cyber)targets for taking car control
- Car is also more vulnerable to external hazards : snow, rain, ice, wind, heat, storm, etc.
- Sensors can also detect breakdown (Avail)

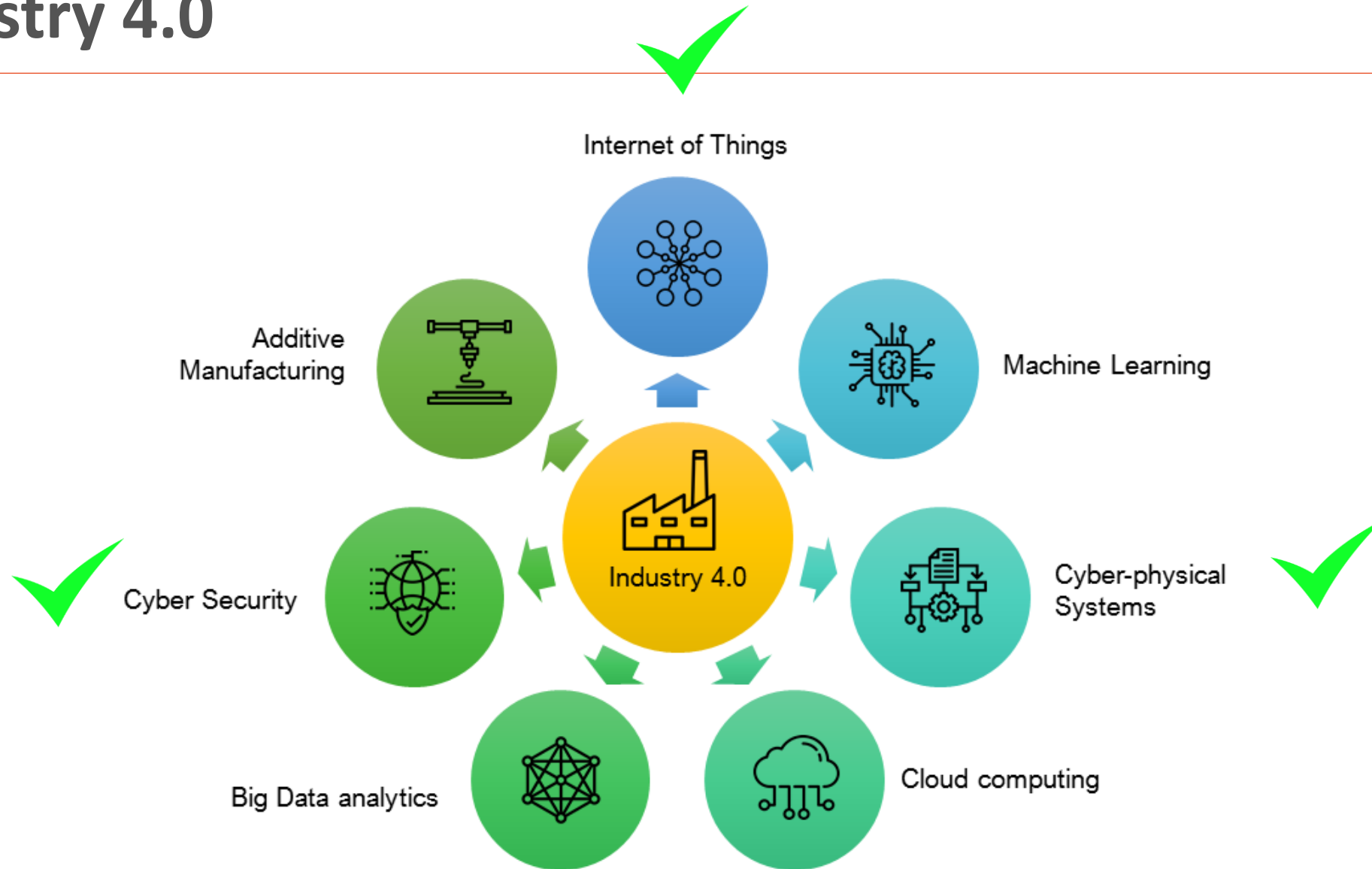


History of Automotive Electronics



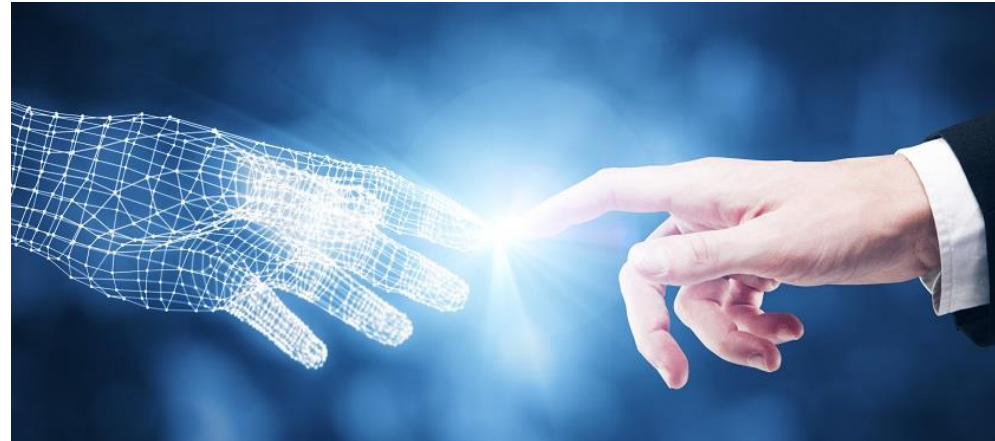
- Cars were mechanics vehicles with four wheels, inside human doing most of the “computing” (driving, turning, braking, etc.)
- Cars are becoming computers with four wheels (eventually carrying humans.)

Industry 4.0





IDMEFv2: Practice

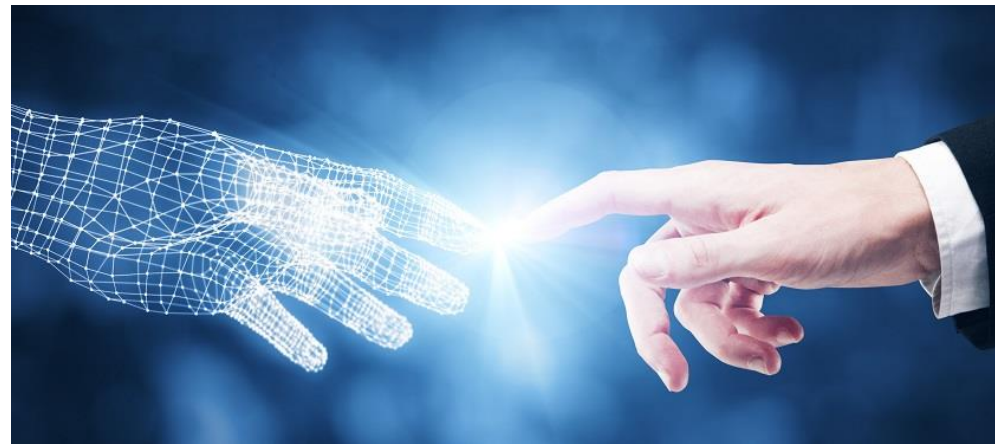


Practice Agenda

- 7SHIELD – <https://www.7shield.eu>
 - Cyber and physical threats against Ground Segment
- PRECINCT – <https://www.precinct.info>
 - Preparedness and Resilience Enforcement for Critical Infrastructure Cascading Cyberphysical Threats
- CyberSEAS – <https://cyberseas.eu>
 - Cybersecurity in the Electrical Power and Energy System
- ATLANTIS – www.atlantis-horizon.eu
 - Enhancing resilience and Cyber-Physical-Human (CPH) security of the key EU Critical Infrastructures
- TESTUDO – <https://testudo-project.eu>
 - Surveillance and protection of the European Critical Infrastructure
- ENDURANCE – <https://endurance-horizon.eu>
 - Enhanced Disruption Resilience and Cooperation in Europe
- KINAITICS – <https://kinaitics.eu/>
 - Cyber-kinetic attacks using Artificial Intelligence
- SAFE4SOC – <https://safe4soc.eu/>
 - Standard Alert Format Exchange for SOC – Cross border SOC collaboration



Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats

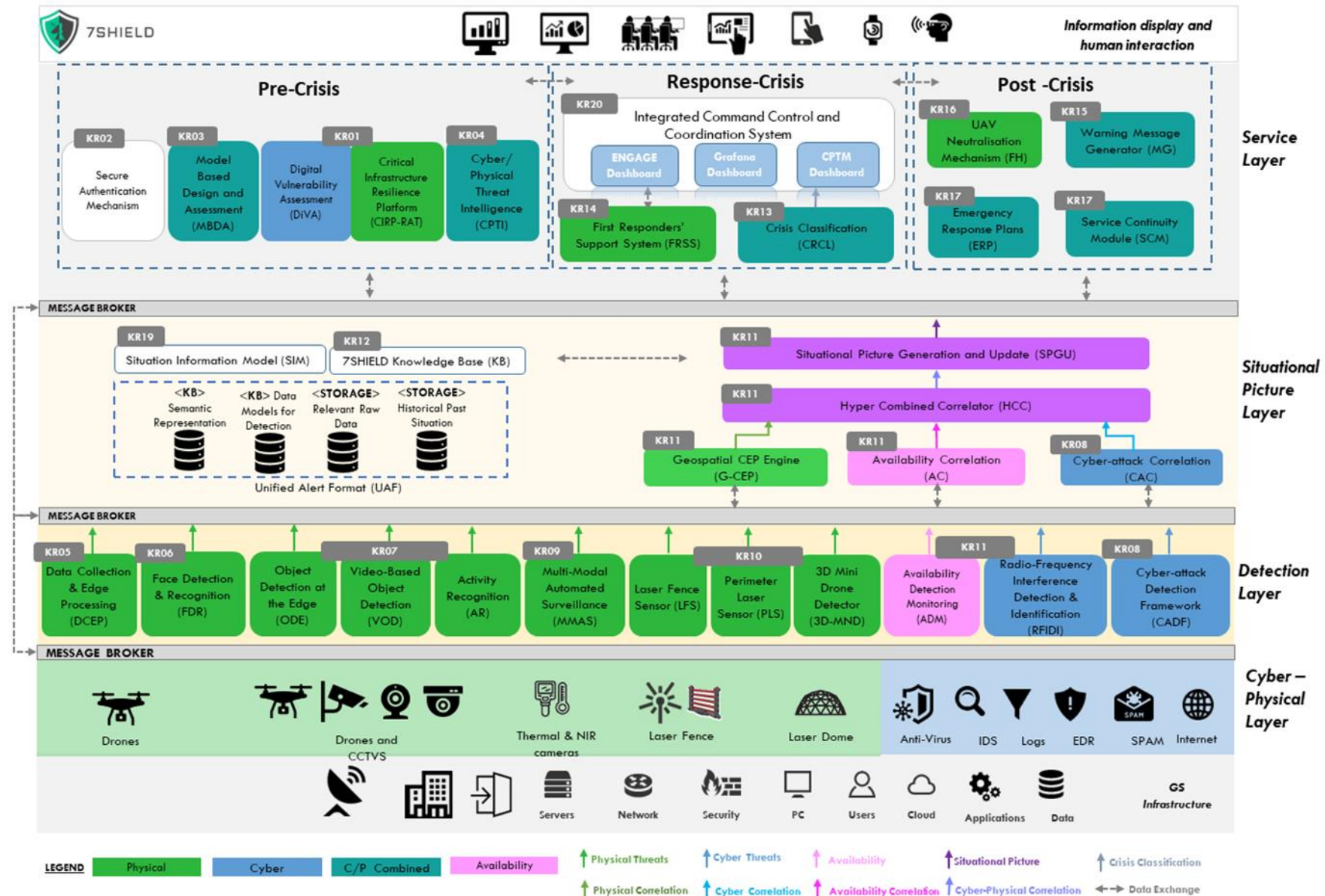


7SHIELD Objective

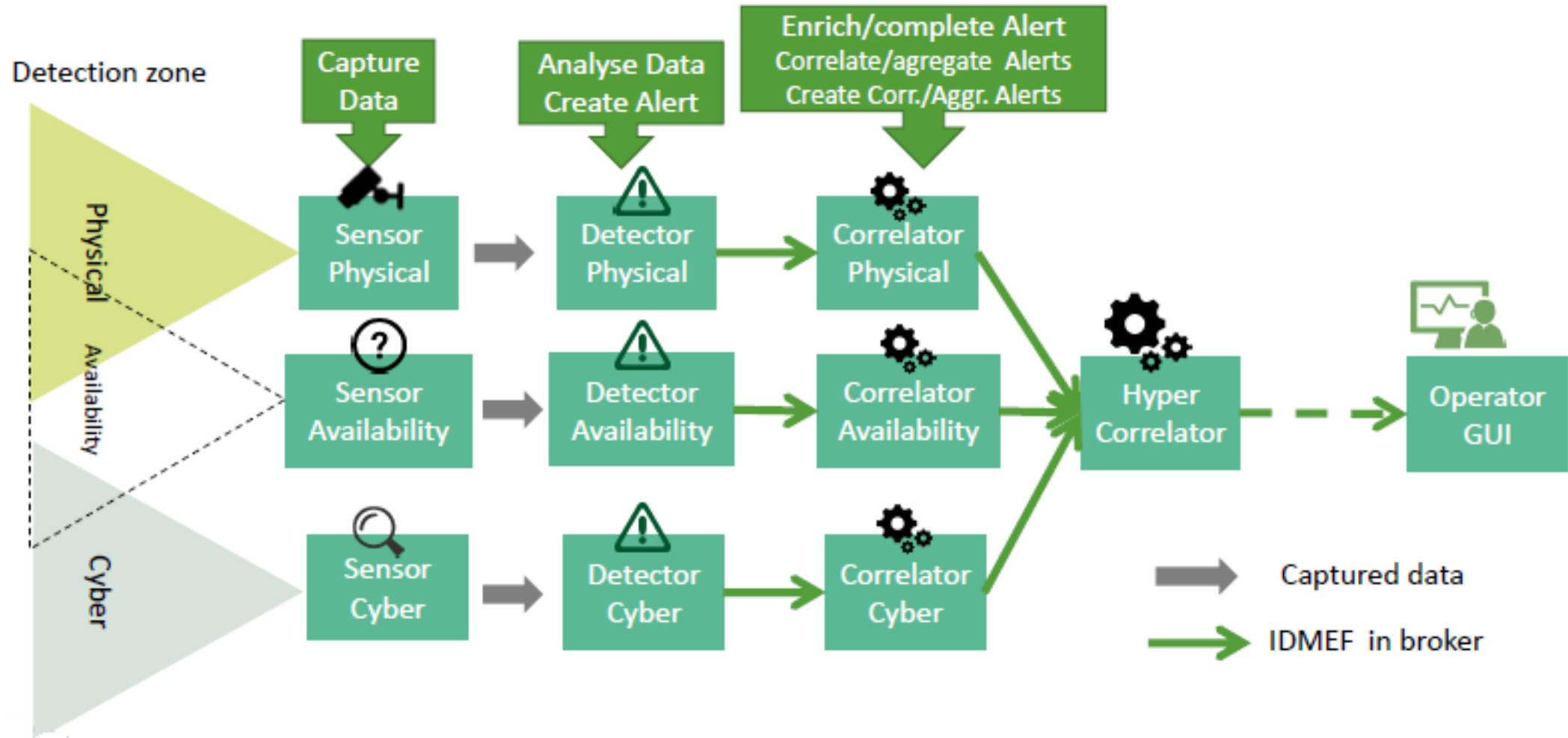
- 7SHIELD: Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats
 - H2020 – (2020 / 2023)
- IDMEF team was working on a cyber oriented IDMEFv1 update in the SECEF (SECurity Exchange Format) project when joining 7Shield.
- Three “ideas” emerged for a “one for all” incident format:
 - Adding availability detection was confirmed
 - Adding physical detection is a need and should be tried
 - Natural hazards were also threats that should be considered
 - Pilot Artic Space Center in Finland with significant snowfall
 - Noa Ground Segment in Greece is surrounded by forest and wildfire threats

7Shield / IDMEFv2 Architecture

- 20 IDMEFv2 modules connected to kafka broker
- CCTV, Laser, AV, IDS, SIEM, NMS, PSIM, etc.

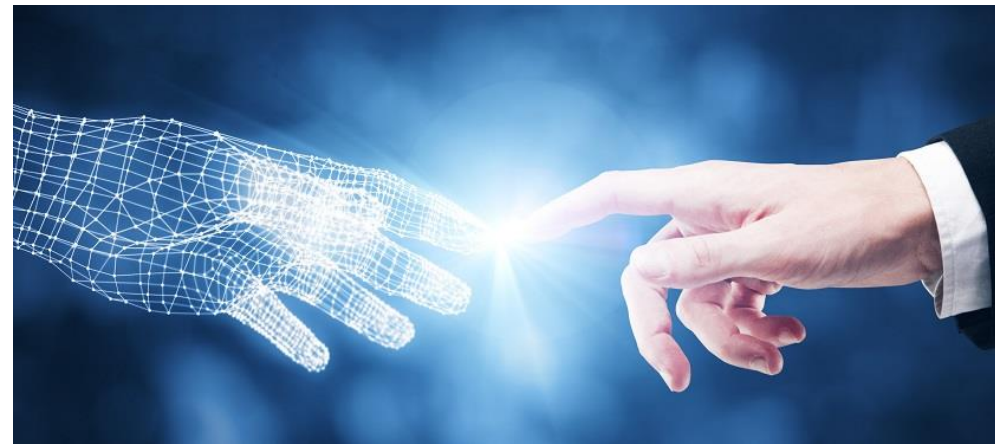


7Shield : Correlation Architecture



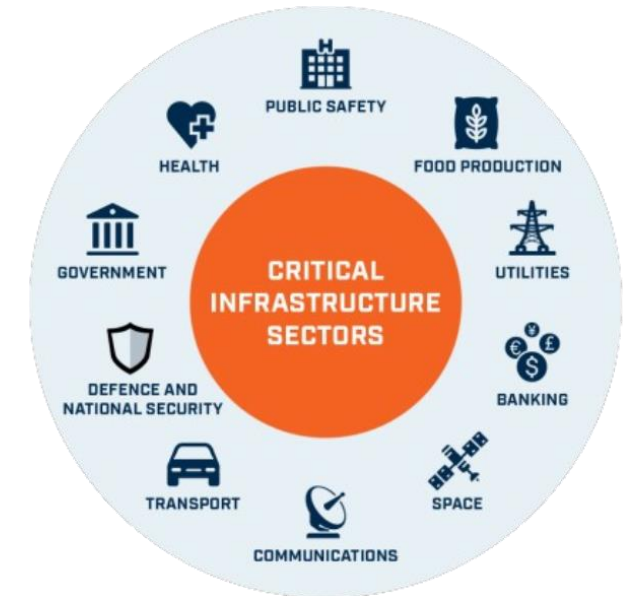
IDMEFv2 Feedback

- Convergency between cyber and physical world is on its way
- **It's possible to define a universal format** to deal with all kind of incidents: cyber, physical, natural, availability, etc.
- **It's possible in theory AND in practice**
 - Obvious now but very ambitious before ...
- IDMEFv2 is the only format which allows communication between all security elements
- Such a format needs tuning and promotion.



CER Directive on Critical Entities

- A **Critical Entity** is considered of particular European significance if it provides an essential service to six or more EU countries.
- **List of (11) essential services**
 - Transport, Energy, Banking, Financial
 - Health, Drinking Water, Waste Water,
 - Digital Infra, Public Administration, Space
 - Production, Processing and Distribution of Food
- **Directive (EU) 2022/2557** of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC



INFRA Projects :: Basic Info

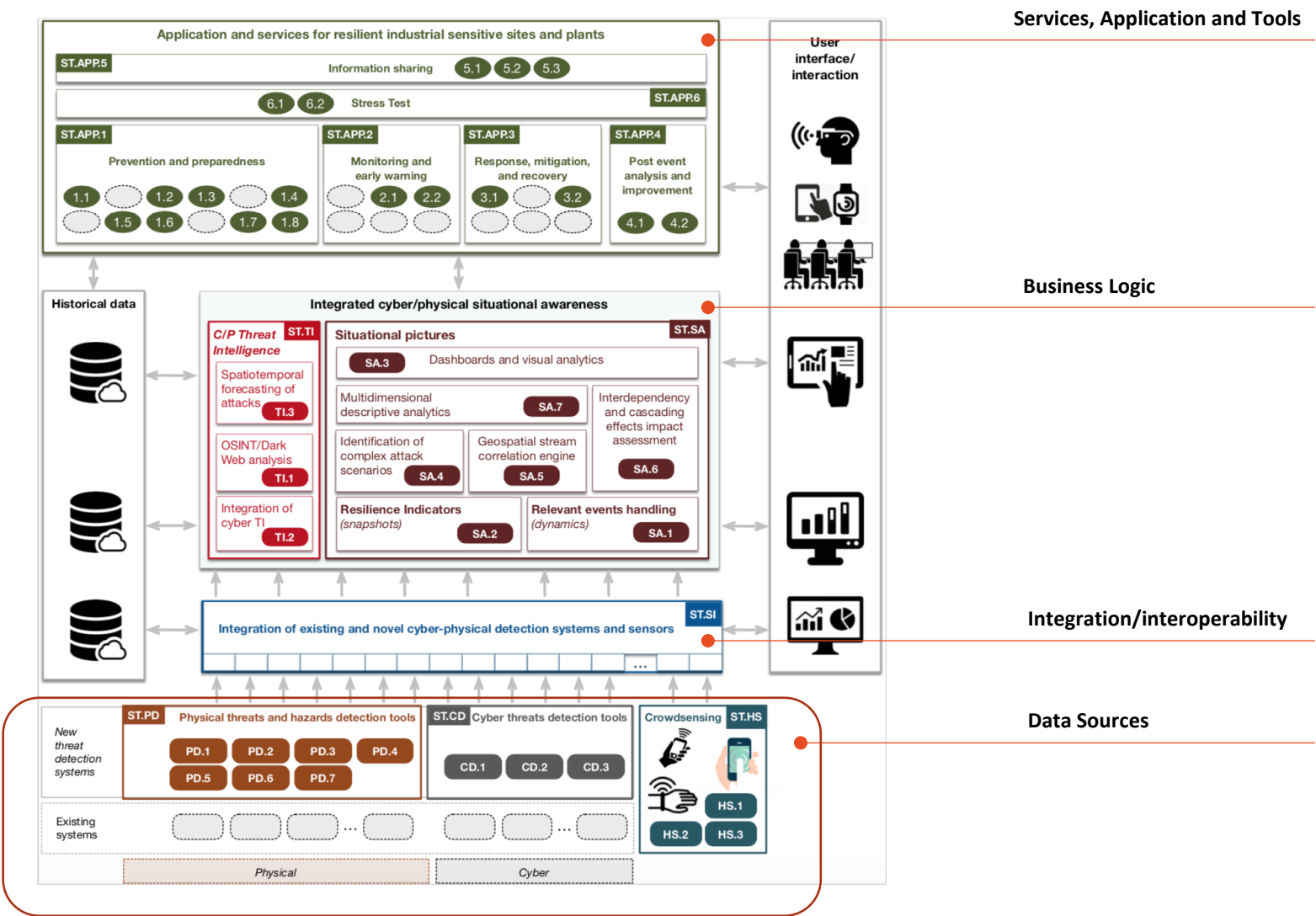
- **PRECINCT [2021]: Preparedness and Resilience Enforcement for Critical INfrastructure Cascading Cyberphysical Threats and effects with focus on district or regional protection**
 - WEBSITE: <https://www.precinct.info/en/>
 - CORDIS: <https://cordis.europa.eu/project/id/101021668>
- **CyberSEAS [2021]: Cyber Securing Energy dAta Services**
 - WEBSITE: <https://cyberseas.eu/>
 - CORDIS: <https://cordis.europa.eu/project/id/101020560>
- **ATLANTIS [2022]: Improved resilience of Critical Infratsructures Against Large scale transNational and sysTemic rISks**
 - WEBSITE: <https://www.atlantis-horizon.eu/>
 - CORDIS: <https://cordis.europa.eu/project/id/101073909>
- **TESTUDO [2023]: Autonomous Swarm of Heterogeneous resource in infrastructure protection via threat prediction and prevention**
 - WEBSITE: <https://testudo-project.eu/>
 - CORDIS: <https://cordis.europa.eu/project/id/101121258>
- **ENDURANCE [2024]: Strategies and Services for Enhanced Disruption Resilience and Cooperation in Europe**
 - WEBSITE: <https://endurance-horizon.eu/>
 - CORDIS: <https://cordis.europa.eu/project/id/101168007>



INFRA Projects :: Mission and Scope

- Provide a set of **intelligent (often autonomous) software solutions** able
- to enhance the
 - **situation awareness,**
 - **risk and resilience assessment,**
 - **cyber-physical security** of Critical Infrastructure
- improvement of **protection capabilities.**
 - to enable faster and more effective **prevention, response, recovery** and **mitigation** actions to threats and risks,
 - looking at **interdependencies** (cross-border and cross-domain dimension)
 - by exploiting, integrating and processing a high rate of input data from **distributed and heterogeneous information sources.**
- to enable stakeholders to take **fast and well-informed decisions** inside and cross-companies.
 - Information with the **right quality and reliability content** is made available to concerned actors and shared between them even in case of critical events with irregular communication.

CIP/INFRA Reference Architecture



PRECINCT Use Case Example



• DATA SOURCE LAYER

- physical real-time data
- cyber real-time data
- existing CIP real-time data
- historical data
- open data
- data models
- other sources

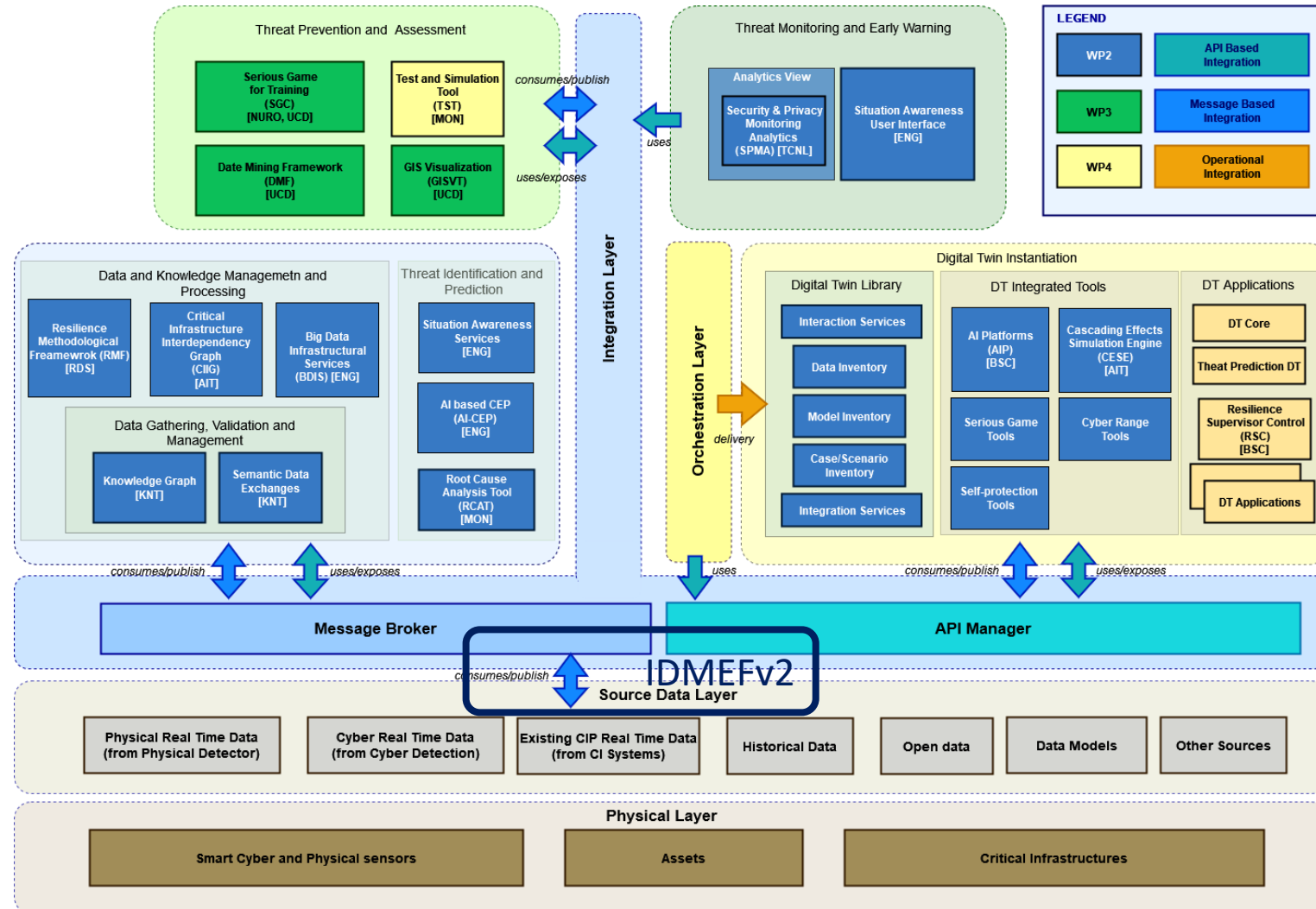
- Data from heterogeneous sources are then normalized in IDMEFv2.0

• INTEGRATION LAYER

- Message Broker
- API Manager

• DATA and KNOWLEDGE MANAGEMENT and PROCESSING

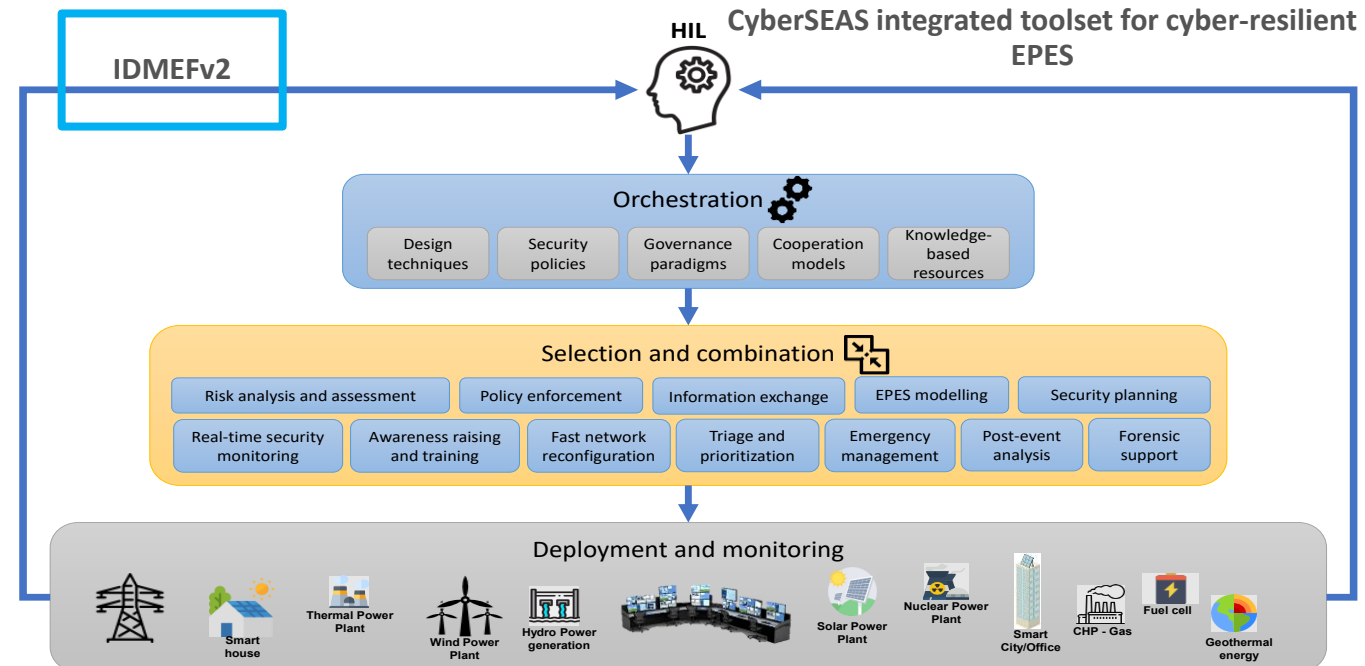
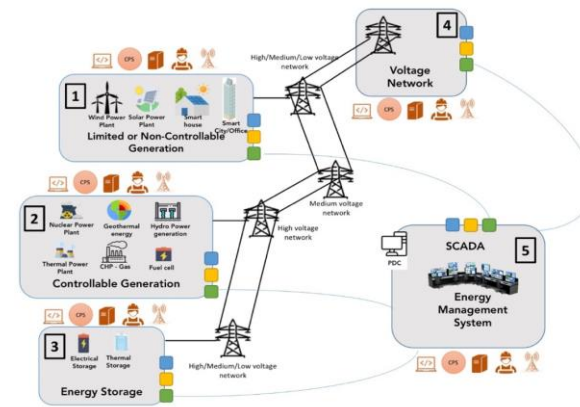
• DIGITAL TWIN INSTANTIATION



CyberSEAS Use Case Example

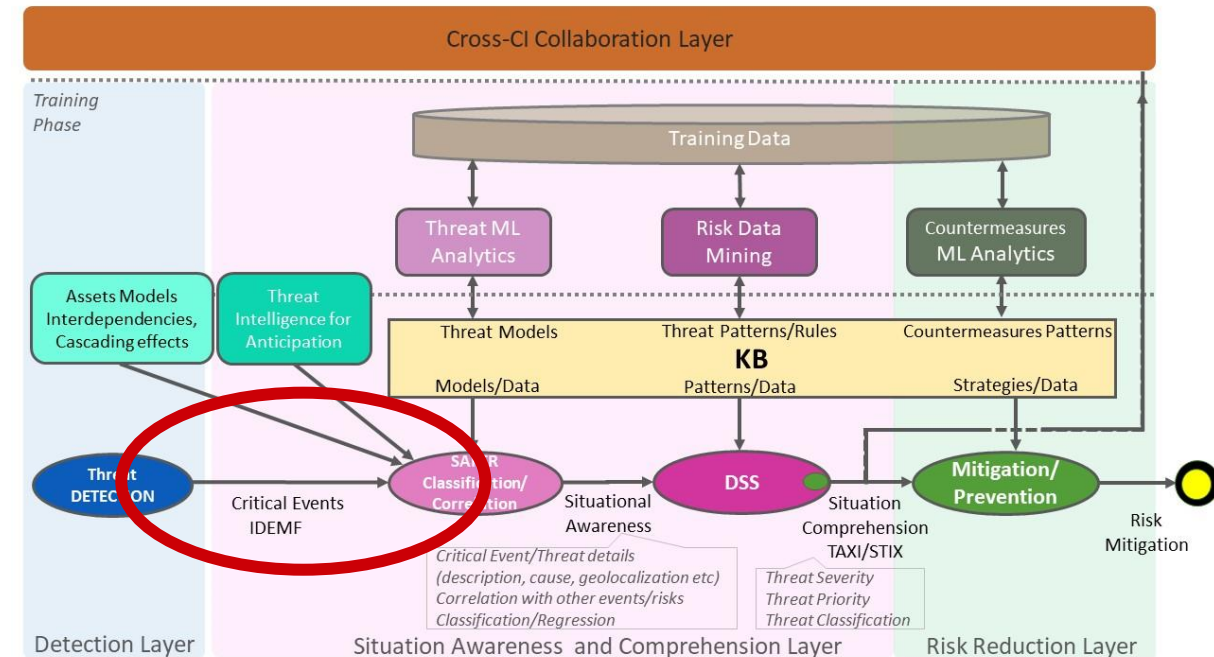
Electrical Power and Energy System (EPES)

1. **Limited or non-controllable generation:** Includes all generation systems characterized by a limited and/or a non-controllable generation power, typically because based on natural phenomena that are uncontrollable or that can be controlled to a limited extent
2. **Controllable generation:** Includes generation systems characterized by a controllable generation power, such as nuclear, hydro, and gas
3. **Energy storage:** Groups the set of all systems dedicated to the storage of energy that is in excess and/or that cannot be used at generation time
4. **Voltage network:** Includes the devices and machinery of the transmission network used to “move” the energy across the EPES infrastructure. It is characterized by a voltage (low, medium, or high) and by a multitude of hardware devices providing connectivity features
5. **Energy Management System:** The centralized part of the EPES, responsible for monitoring and for managing the EPES infrastructure. It includes systems like SCADA devices, Phasor Data Concentrators, Historical data archives, Human Machine Interfaces, etc.



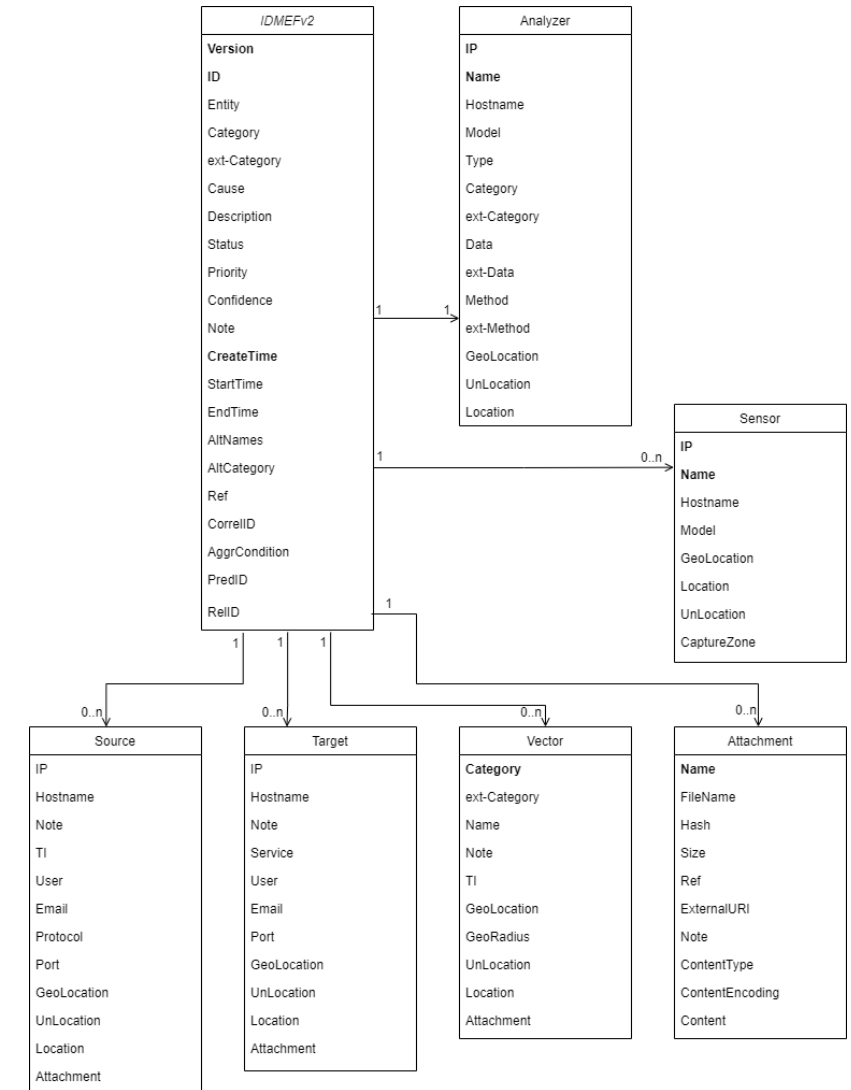
ATLANTIS Use Case Example

- The detected events are provided to the SAFER component in the **standardized IDMEF format** through a UAF message.
- CYBER DETECTORS:
 - **Disinformation Campaign:** Tool to identify and issue alerts in case of disinformation campaigns (**TRULY MEDIA**)
 - **Disinformation Campaign:** Deepfake analysis + Image Tagging + Image Similarity
 - **THINT:** Analysis and grouping of cyber threat intelligence data provided by **TRULY MEDIA**
 - **EBRA** - Network analysis tool (FROM Fortigate logs)
 - **SIGMO:** Intrusion Detection System for CYBER scenarios.
- PHYSICAL AND HUMAN DETECTORS:
 - **SNIFFER** as environmental sensor (air quality) for CYBER-PHYSICAL scenarios
 - **Human-in-Vicinity (HIVIC)** technology to involve "human sensors" in CYBER-PHYSICAL scenarios



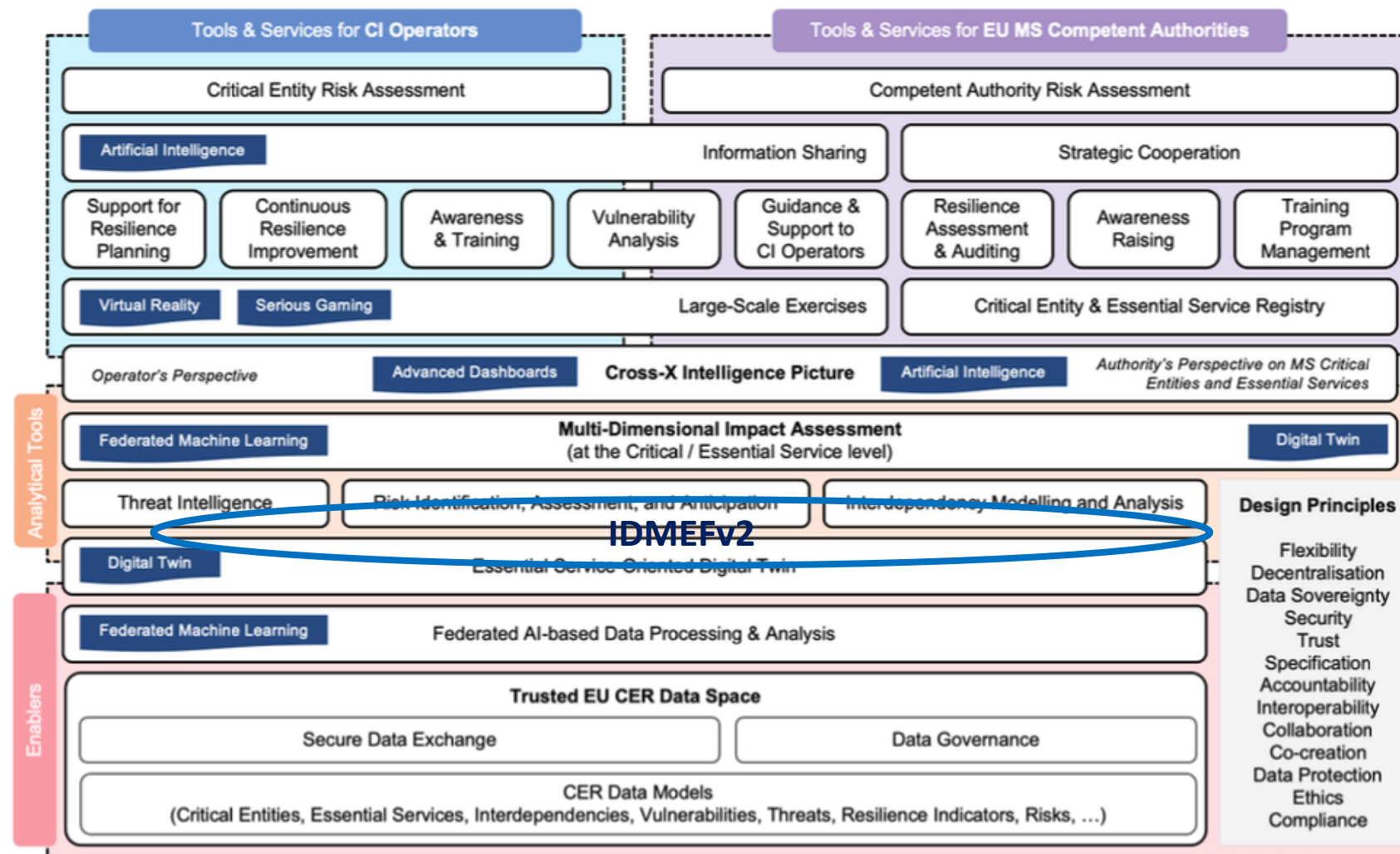
TESTUDO Data Model

- It is crucial to provide **reliable, asynchronous** interaction and **data exchange** between different detection systems and services.
- Leveraging on an **event-driven architecture**, the Incident Detection Message Exchange Format version 2 (IDMEFv2) it is intended to be a standard data format that incident detection systems can use to report alerts about events that they deem noticeable.
- Key features: (1) **Structured Data Representation**; (2) **Extensibility**; (3) **Interoperability**; (4) **Enhanced Information**.



ENDURANCE FUTURE ADOPTION

- Interoperability among ENABLERS and Analytical Tools could rely on IDMEF v2.



Critical Infrastructure Projects 1/2

- **Importance of normalization format**
 - Enables interoperability across heterogeneous systems
 - Facilitates automated processing, correlation, and incident response
 - Serves as a foundation for scalable and modular security architectures
- **Types of data represented in IDMEF format:**
 - Cyber detection from CIs networks
 - Physical detection of:
 - People movement anomalies and abnormal behaviours
 - Quantity of people in an area
 - Fire, smoke, chemical agents
 - Air quality anomalies
- **Promoting the format**
 - In TESTUDO the IDMEF format is explicitly mentioned in the GA
 - In PRECINCT, CyberSeas and ATLANTIS it is widely adopted
 - In ENDURANCE it is promoted extensively

Critical Infrastructure Projects 2/2

- **Lesson learned**

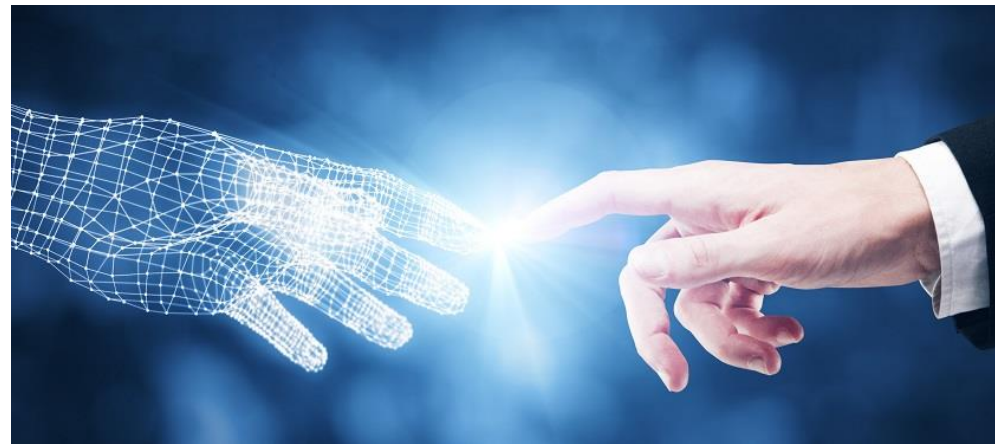
- **Easy acceptance** of the format
- The latest drafts (v3, v4) are **mature enough** for unsupervised implementation
- An **adaptation layer** is always needed to transform data in IDMEFv2 format
- **Guidelines and examples** on the best practices to represent specific data are very useful

- **Technological usage and feedback**

- Adapting to IDMEF is **not time-consuming** when properly abstracted
- The **attachment** field offers flexibility for custom or domain-specific content
- **User feedback** confirmed that early prototyping and documentation reduced integration errors
- Usage of the same format allows for better correlation of the alerts



Cyber-kinetic attacks using Artificial Intelligence



Impact of artificial intelligence on products and services

Artificial intelligence (AI) is profoundly modifying **products** and **systems** in various sectors. On the one hand, its adoption creates new risks for systems and on the other hand, it has an impact on cyber-physical security practices, both on the attack and defense sides.

Convergence of physical and cyber security in presence of artificial intelligence

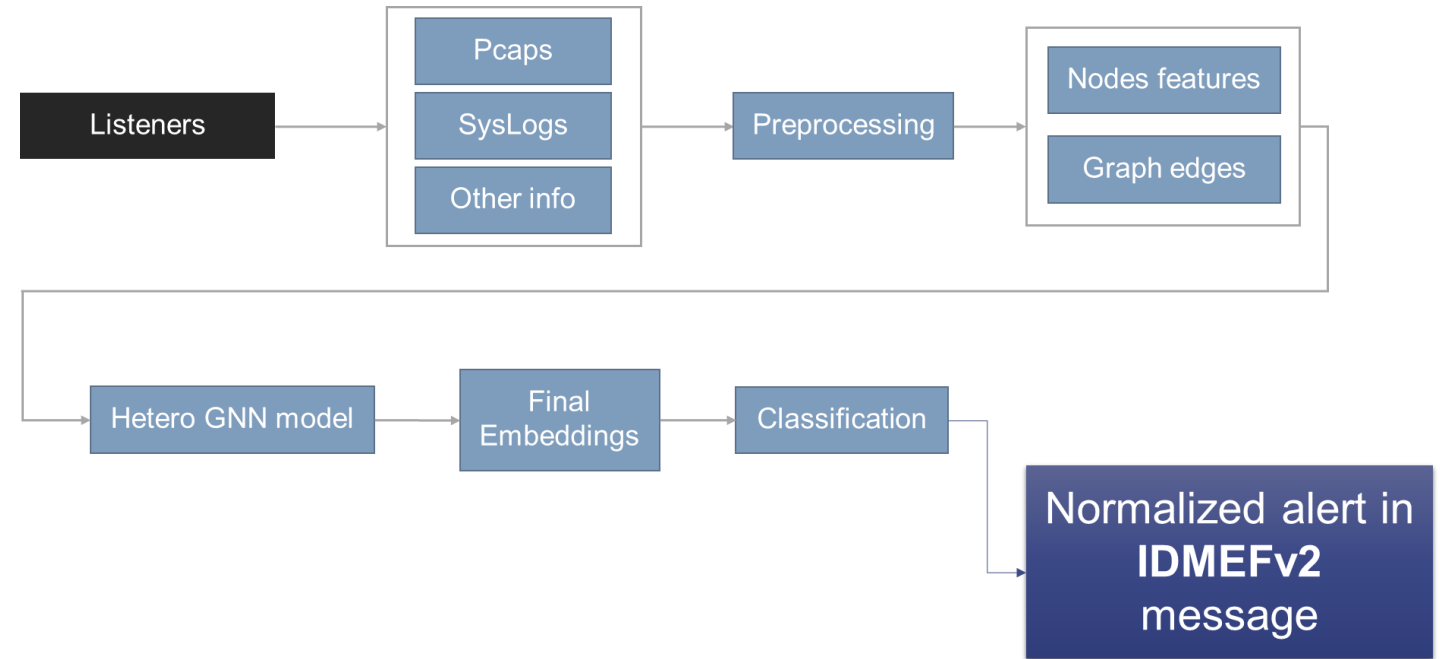
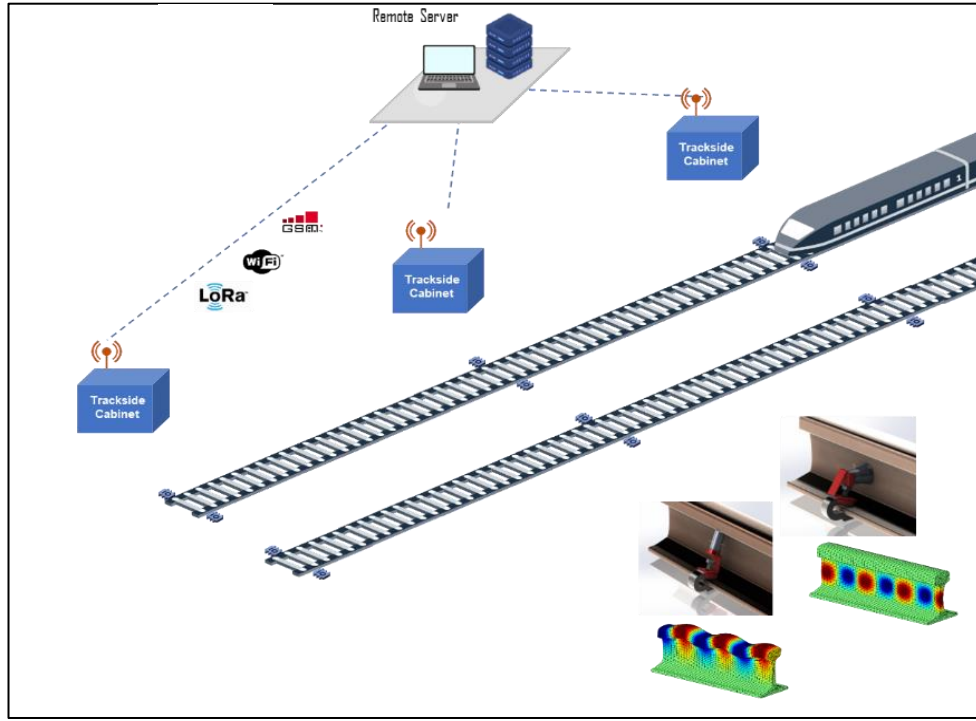
It is well-known that attacks or malfunctions in the cyber world can **have critical impacts on the physical world**, especially in critical infrastructures. Conversely, intentional perturbations of physical systems, through e.g., attacks on sensor measurements, can have disastrous consequences on digital control mechanisms, and consequently on physical processes.

Protecting systems when artificial intelligence and humans are involved

Protection of systems must take into account:

- Physical attack surface
- Cyber attack surface
- Artificial intelligence flaws
- Humans flaws and humans interactions with systems

KINAITICS Use Case Example



Data

Log server
NetFlow data
Log system



AI model
Heterogeneous graph
GNN – Graph Neural Networks



Alerts shared in
IDMEFv2 messages

Output

- What we needed:
 - Cyber – physical – availability events to be shared
 - Artificial Intelligence used to produce alerts
 - Sharing information on detection events
 - Model
 - Parameters
 - Some features
- What we found in IDMEFv2:
 - Simple format compared to competitors
 - Quick setup of the event sharing mechanisms
 - Tunable format
 - Ready for artificial intelligence (AI producing events)
 - Opportunity to gather events in a single format coming from various sources (events correlation)

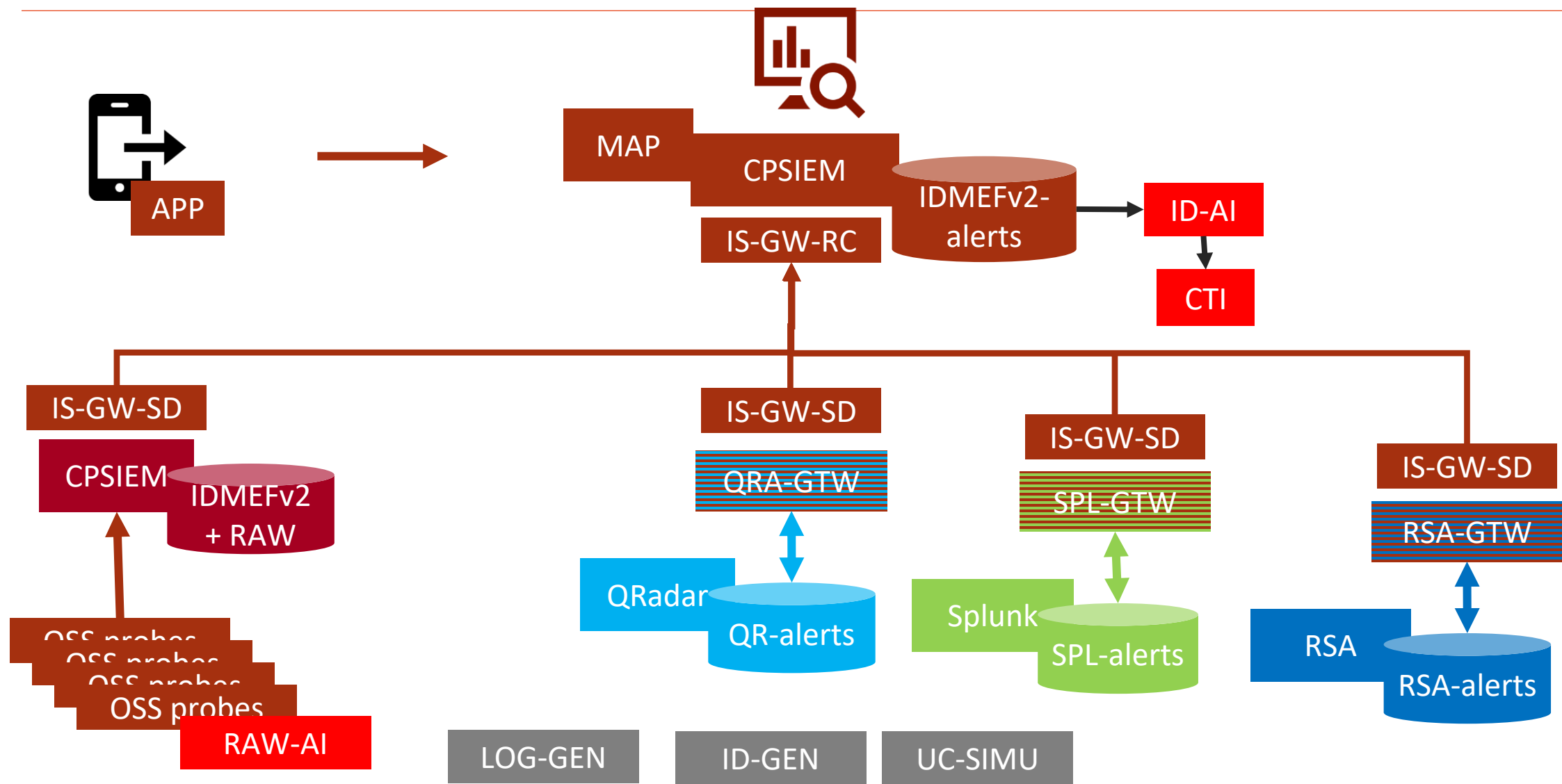
```
{
  "Version": "2.D.V03",
  "ID": "49f39cac-ec67-34c2-83ec-dc780a11a871",
  "CreateTime": "2025-02-19T09:48:35.740120",
  "Confidence": 1.0,
  "Category": ["ext-value"],
  "ext-Category": "Network.Intrusion",
  "Analyzer": {
    "IP": "132.167.224.6",
    "Name": "CEA_ANALYZER",
    "Hostname": "www.cea.fr",
    "Type": ["Cyber"],
    "Category": ["NIDS"],
    "Data": ["Network"],
    "Method": ["Statistical"],
    "Model": "697a989c451f462eb7bc730fa65a1c12"
  },
  "Source": [
    {
      "IP": "91.189.88.152",
      "Port": [80]
    }
  ],
  "Target": [
    {
      "IP": "192.168.226.71",
```



Standard Alert Format Exchange For SOCs



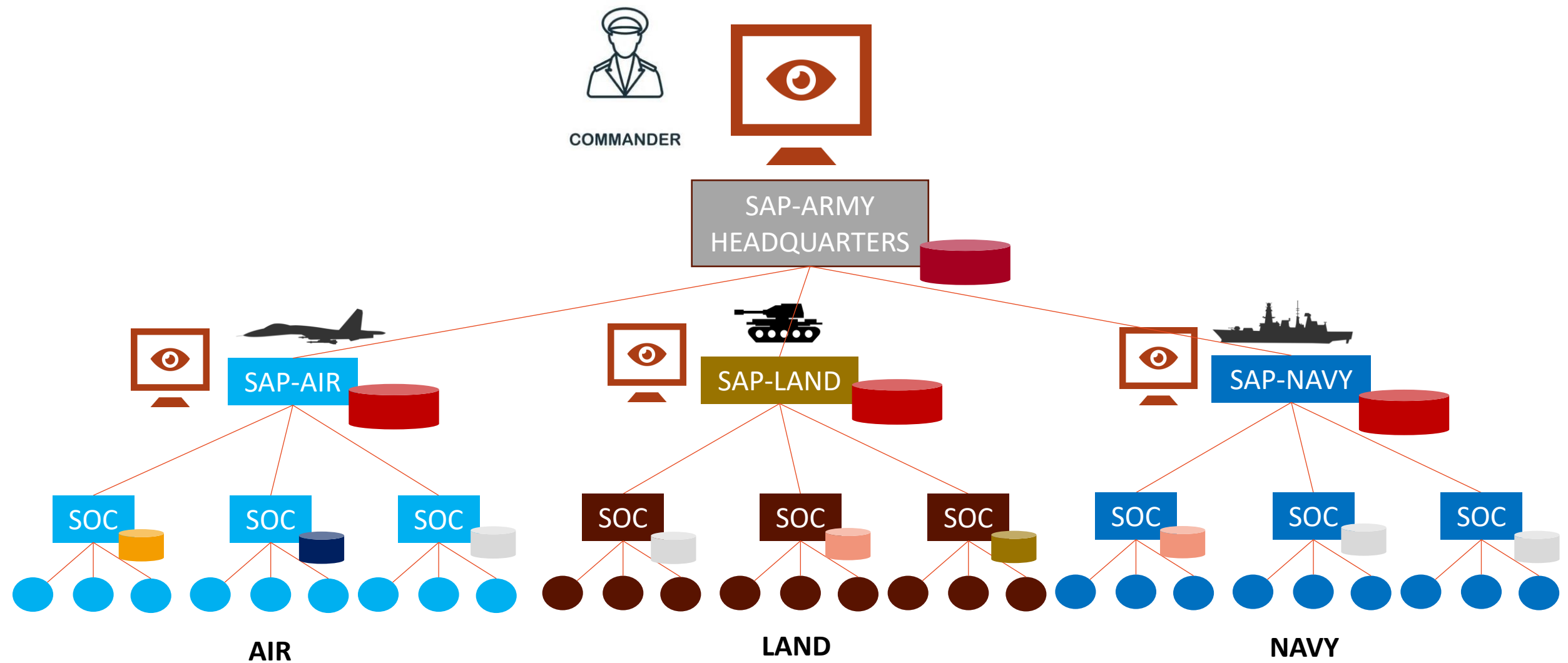
- SAFE4SOC: Standard Alert Format Exchange for SOC
- Safe4Soc is part of the « Cross Border SOC's » calls which aim to encourage collaboration between European socs
- Three major concepts
 - IDMEFv2 gateways for commercial SIEMs (Splunk, Qradar and RSA)
 - “Information Sharing Gateway” (and its Information Sharing Agreement)
 - AI centralized detection for CTI creation



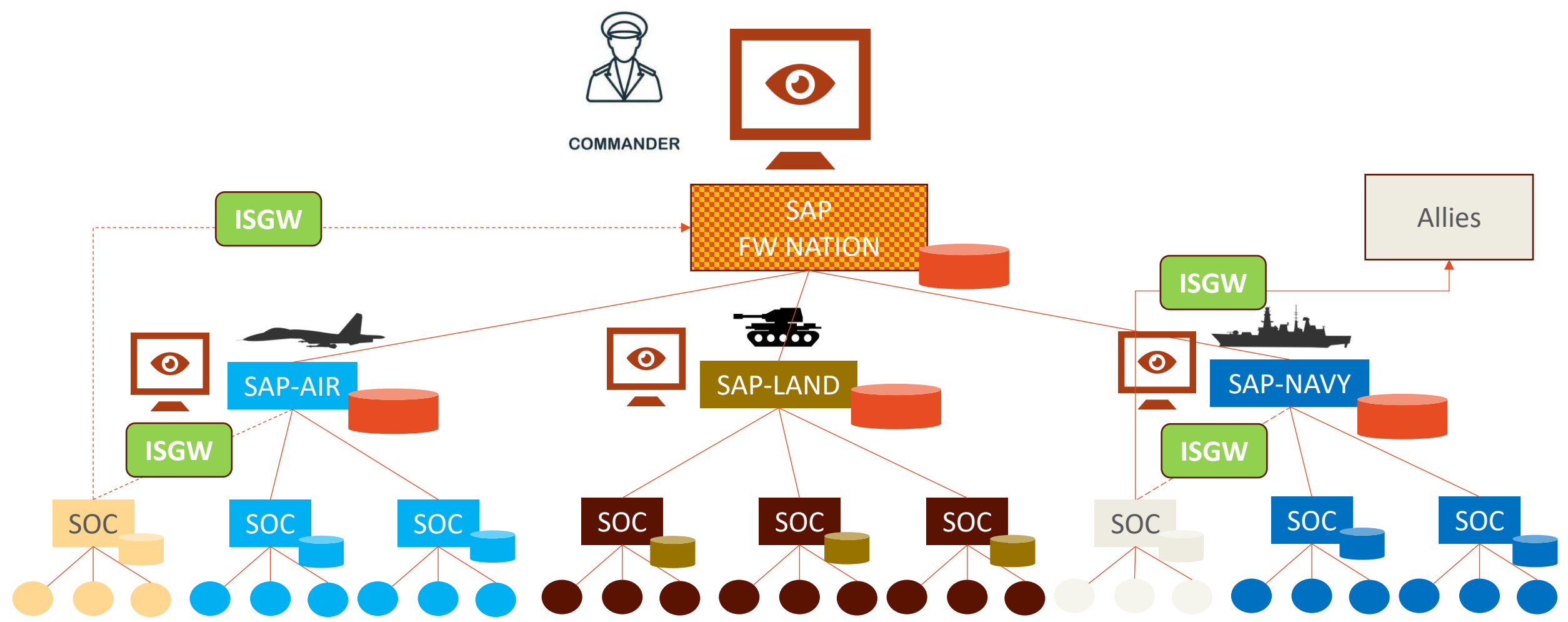
SAFE4SOC IDMEFv2 « running code »

- S4S code is on the IDMEFv2 Github : <https://github.com/IDMEFv2>
- Python and Java librairies
- IDMEFv2 Online JSON Validator
- IDMEFv2 Gateways
 - Splunk, Suricata, Wazuh, Zabbix
 - Coming: Qradar, RSA Envision, Graylog, ElastAlert, CAP, OSCF (?), etc.
- Concerto SIEM
 - The first IDMEFv2 SIEM (Prelude OSS fork)
- IDMEFv2 Android Alerter

Army architecture use case



Framework Nation Concept (NATO)



- SIEMS format are very different (confirmation)
 - Not the same concepts: offences, alerts, incidents, events, ...
 - Not the same naming for the same concepts:
 - source.ip, src_ip, src, src[0].ip[0], etc.
 - Not the same « look and feel »
 - No place for physical security ... **In 2025, SIEMS ARE NOT SIEMS anymore (only « CSIEM »)**
 - Etc.
- « *What happens in the SOC stays in the SOC* »
 - Information sharing gateway and agreement is a very important concept to ease SOC's collaboration.
- SIEMS, SOCS, PSIM, etc ... interoperability should be nations & industry priority
 - It's not a gadget it's a necessity, specially in times of (hybrid) wars
- Official standardisation path is another real challenge

Technical feedback for security product coders

- Before, coders were using syslog for « all » information
 - System logs and incident detection
- Some are moving to JSON for incidents (ex: ClamAV)
- Two major difficulties
 - Coders don't document their log format => difficult to analyze
 - Coders don't know what to put in their « Alert » => so they put everything
- Choosing a pre-documented and alert oriented format will ease everything (even the work of tool coders)



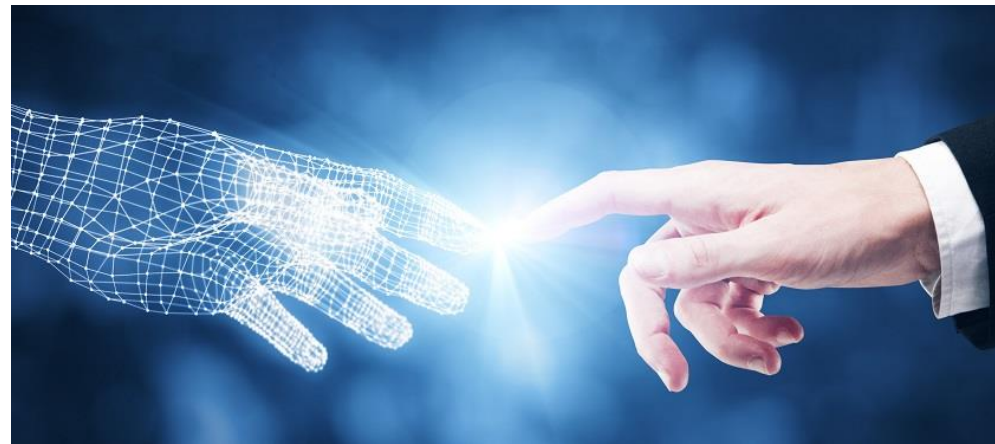
Conclusion





IDMEFv2 IETF Standardization

When you do something, know that you will have against you those who would like to do the same thing, those who wanted the opposite, and the vast majority of those who wanted to do nothing.



IDMEFv2 , the genesis

« Detection » Team



- 2008 : Vigilo NMS (SNMP)
- 2012 : Prelude SIEM (IDMEFv1)
- 2014 : Unity 360
 - Availability + CyberSecurity monitoring convergency
- 2015 : R&D SECEF1 (Security Exchange Format)
 - IDMEFv1 promotion
- 2019 : R&D SECEF2
 - IDMEFv1 (cyber) update and standardisation
- 2020 : R&D 7Shield Cyber + Physical Ground Segment
 - Cyber + Physical + Availability
 - Snow, Fire, etc.
- 2022 : IDMEFv2 IETF draft
- 2023 : R&D Safe4Soc Digital project
 - (Cross Border SOCs collaboration)
- 2025 : Webinar with ENG

ENGINEERING



- 2020: 7Shield project manager (G. Guinta)
- Other IDMEFv2 projects after:
 - Precinct
 - CyberSeas
 - Atlantis
 - Kynaitics
 - Testudo
 - Endurance
- 2025: Webinar with Gilles



IDMEF / IETF : Brief history

2007 : IDMEFv1 (RFC 4765) (H. Debar – Research Director TSP)

- Cyber **Intrusion** Detection format (XML, IDXP)
- <https://www.rfc-editor.org/rfc/rfc4765.html>
- Mostly used in cyber open-source software : Prelude OSS, Suricata, Snort, Ossec, Samhain, etc. and research

2020 – 2022 : IDMEFv2 : Design & Test


- Cyber & Physical **Incident** Detection Format (JSON, HTTPs)
- Designed and tested on large scale research project www.7shield.eu
- Deployed on 5 Ground Segment pilots around Europe

2022 : IDMEFv2 : Starting IETF Standardization process

- Draft V00 published in October 2022 (G. Lehmann) – (2025 – V005)
 - <https://datatracker.ietf.org/doc/draft-lehmann-idmefv2/>
 - <https://datatracker.ietf.org/doc/draft-lehmann-idmefv2-https-transport/>

« It does not matter how slowly you go as long as you do not stop. »

IETF : Two DRAFTS submitted

 Datatracker

Groups Documents Meetings Other User

Report a bug

Sign in

Document search

Transport of Incident Detection Message Exchange Format version 2 (IDMEFv2) Messages over HTTPS draft-lehmann-idmefv2-https-transport-04

StatusEmail expansionsHistory

Versions:
0001020304

This document is an Internet-Draft (I-D). Anyone may submit an I-D to the IETF. This I-D is **not endorsed**

draft-poirotte-idmefv2-https-transport

draft-lehmann-idmefv2-https-transport

00

00


01

Oct 2022

Apr 2023

Oct 2023

Document	Type	Active Internet-Draft (individual)
	Author	Gilles Lehmann
	Last updated	2025-04-01
	Replaces	draft-poirotte-idmefv2-https-transport
	RFC stream	(None)
	Intended RFC status	(None)

 Datatracker

Groups Documents Meetings Other User

Report a bug

Sign in

Document search

The Incident Detection Message Exchange Format version 2 (IDMEFv2) draft-lehmann-idmefv2-05

StatusEmail expansionsHistory

Versions:
000102030405

This document is an Internet-Draft (I-D). Anyone may submit an I-D to the IETF. This I-D is **not endorsed by the IETF** and has **no formal standing** in the [IETF standards process](#).

draft-lehmann-idmefv2

00

01

02

03

04

05

Oct 2022

Apr 2023

Oct 2023

Apr 2024

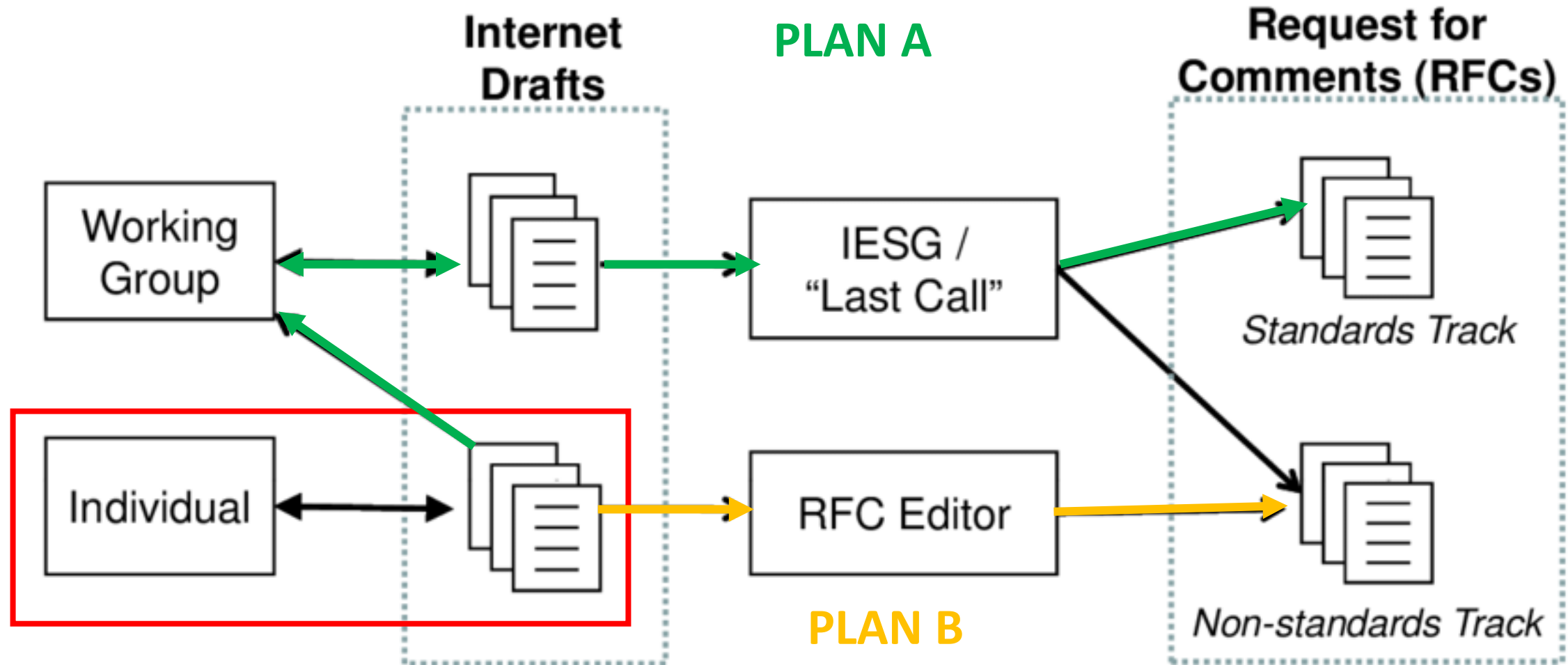
Oct 2024

Apr 2025

Document	Type	Active Internet-Draft (individual)
	Author	Gilles Lehmann
	Last updated	2025-04-01
	RFC stream	(None)
	Intended RFC status	(None)
	Formats	txt html xml htmlized bibtex bibxml
Stream	Stream state	(No stream defined)



IETF Standardization process



Standardization chances: Pros & cons

- Cons :
 - IETF is more “protocol” than “format” oriented
 - Standardization process is a long and uncertain challenge (and we running out of time)
 - Cyber and Physical detection convergence is still a new and disruptive concept
 - Communities and tools are still confined
 - Very very very few cross competencies
 - IDMEFv2 is a “proposed” standard (vs industry “imposed” standards)
- Pros :
 - Many difficulties since we started but till now stars kept (more or less) aligned
 - Huge work has already been done :
 - The V00 drafts are written and published (~ years of work)
 - Implementations are coded : two libraries + one full prototype + safe4soc (~ years of coding)
 - IDMEFv2 has been tested on many projects
 - IDMEFv1 and OSS legacy : should help at IETF and adoption (?)
 - **The need for IDMEFv2 is more and more obvious and the place is empty**

Next steps

- Draft tuning
 - Small typos : alerts/incidents
 - Complete new incident categories
 - UID in all classes
 - Target category
 - ...
- Hopefully a BCP (Best common Practice) draft
- Grow community and visibility (you can help!)
- Back to IETF for an official Area Director sponsored RFC (Probably experimental)
- Maybe try OASIS standardisation (STIX, etc.) in parallel

**DEAD LINE
S1 2027**

How to participate

- Keep informed and spread the word
 - News letter, LinkedIn, IDMEFv2 mailing list
- Test and use IDMEFv2 tools
- Implement your own IDMEFv2 gateways
- Read the drafts and visit the IDMEFv2 website
- Any ideas are welcome ...

WE NEED YOU!



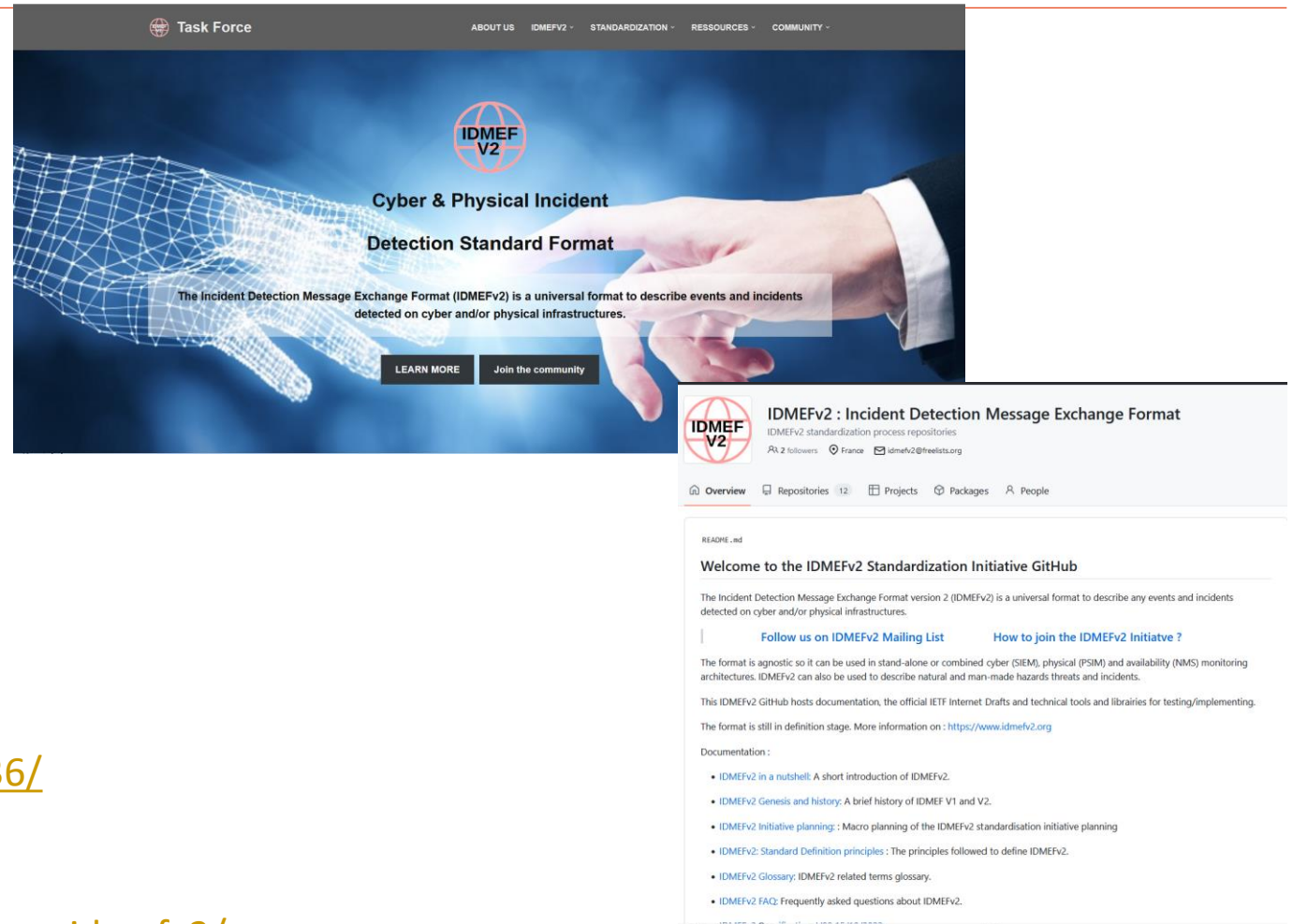


IDMEFv2 Task Force



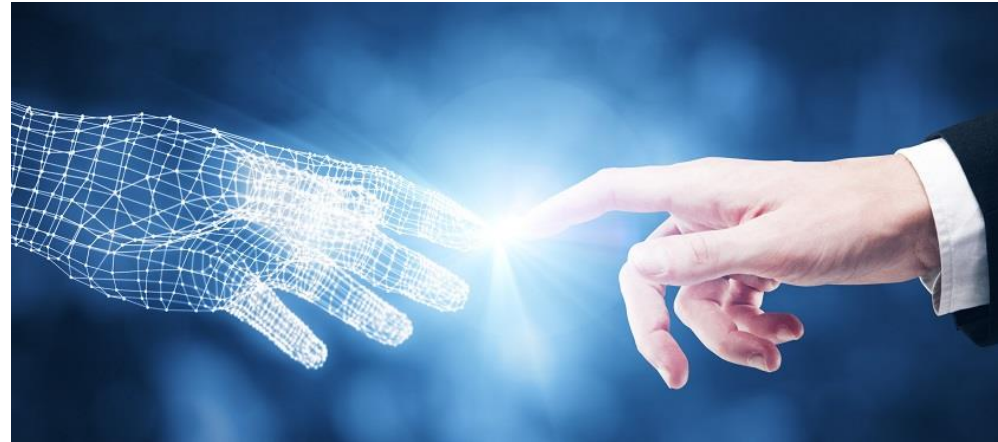
Links

- IDMEFv2 Website
 - <https://www.idmefv2.org>
- IDMEFv2 GitHub
 - <https://github.com/IDMEFv2>
- IDMEFv2 Mailing List
 - <https://list.idmefv2.org>
- IDMEFv2 Task Force Members
 - <https://idmefv2.ovh/index.php/members/>
- LinkedIn
 - <https://www.linkedin.com/groups/13006336/>
- Official drafts at IETF :
 - <https://datatracker.ietf.org/doc/draft-lehmann-idmefv2/>
 - <https://datatracker.ietf.org/doc/draft-lehmann-idmefv2-https-transport/>





Q&A

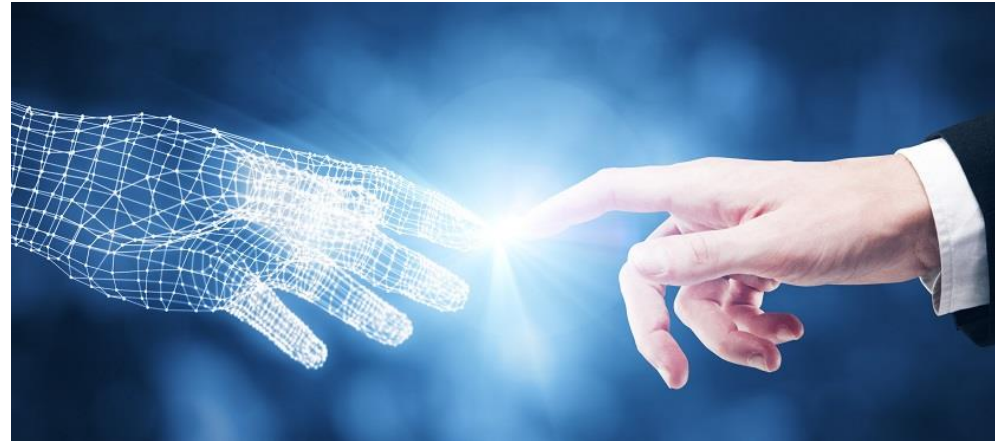


QUESTIONS ?

“The man who asks a question is a fool for a minute, the man who does not ask is a fool for life.”



Demonstration



Demonstration

- IDMEFv2 Validator
- IDMEFv2 SIEM AKA « Concerto SIEM »
- IDMEFv2 Alerter

Validator

- Validate
- Discover
- Learn
- Test
- Etc.

IDMEFv2 - JSON Validator Latest Schema - 2.D.V05

Delete Copy Export Import Example </> Exercise Validate intrusion-detection-1.json Validation results

```
1 {
2   "Version": "2.0.3",
3   "ID": "e5f9bbae-163e-42f9-a2f2-0daaf78fefb2",
4   "CreateTime": "2021-01-18T23:34:05.21Z",
5   "StartTime": "2021-01-18T23:34:04.52Z",
6   "Cause": "Malicious",
7   "Category": [
8     "Intrusion.Burglary"
9   ],
10  "Severity": "medium",
11  "Confidence": 0.9,
12  "Description": "Physical intrusion detected",
13  "Analyzer": {
14    "IP": "1.1.1.1",
15    "Name": "Motion detector"
16  },
17  "Sensor": [
18    {
19      "IP": "1.1.1.2",
20      "Name": "Infrared camera 42"
21    }
22  ],
23  "Vector": [
24    {
```

Path: **Root.Severity**, Error: should NOT have additional properties
Path: **Root.Observable**, Error: should NOT have additional properties
Path: **Version**, Error: should be equal to one of the allowed values
Path: **Vector[0].AttachHandle**, Error: should NOT have additional properties
Path: **Vector[0].ObservableHandle**, Error: should NOT have additional properties
Path: **Vector[0].Category[0]**, Error: should be equal to one of the allowed values
Path: **Attachment[0].Handle**, Error: should NOT have additional properties
Path: **Attachment[0]**, Error: should have required property 'Name'
Path: **Attachment[0].ExternalURI**, Error: should be array

Autocompletion and error highlighting: **enabled** Schema version 2.D.V05

Concerto SIEM: First IDMEFv2 SIEM

ALERTANALYSEARCHIVEADMIN?

Sys

Archive18.1KAlerts051323172

AlertsAggregated alertsMacrovisualization

No filterInactive1 month23/05/25 14:2423/06/25 14:24

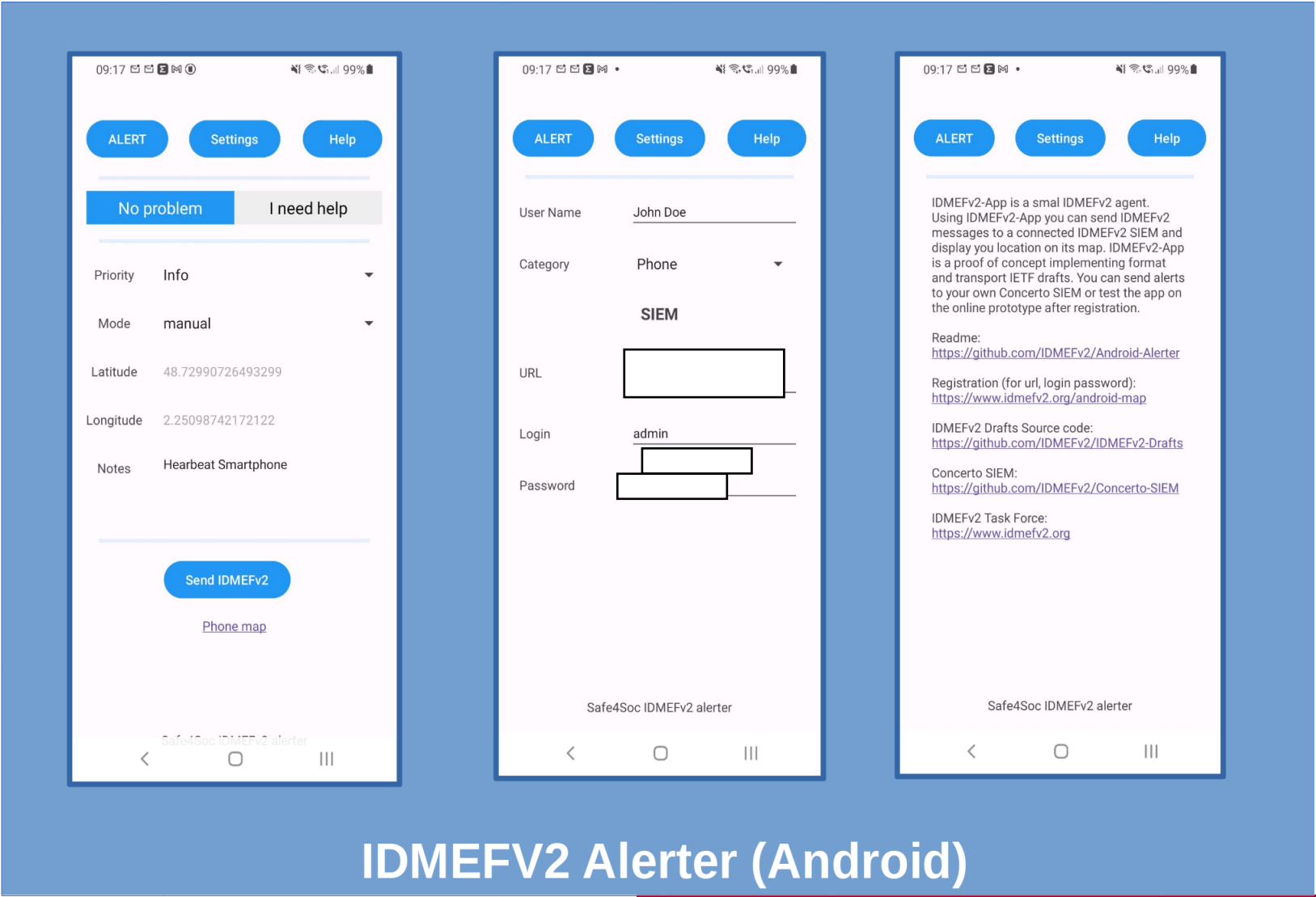
CriterionSearchGroup bySelect your field

+ Timeline

	Priority	Create time	Category	Description	Target	Target location
+	Medium	23 Jun 2025, 14:18:24	Attempt.Login	Someone tried to log in as 'root' from 80.9	10.244.0.1	Data Center
+	Low	23 Jun 2025, 13:55:37	Attempt.Login	Someone tried to log in as 'jay' from 144.4	10.244.0.1	Data Center
+	Medium	23 Jun 2025, 13:55:35	Attempt.Login	Someone tried to log in with an invalid use	10.244.0.1	Data Center
+	Low	23 Jun 2025, 13:47:35	Attempt.Login	Someone tried to log in as 'ubuntu' from 1	10.244.0.1	Data Center
+	Medium	23 Jun 2025, 13:47:32	Attempt.Login	Someone tried to log in with an invalid use	10.244.0.1	Data Center
+	Low	23 Jun 2025, 13:45:56	Attempt.Login	Someone tried to log in as 'postgres' from	10.244.0.1	Data Center
+	Medium	23 Jun 2025, 13:45:54	Attempt.Login	Someone tried to log in with an invalid use	10.244.0.1	Data Center
+	Medium	23 Jun 2025, 13:42:19	Attempt.Login	Someone tried to log in as 'root' from 34.1	10.244.0.1	Data Center
+	Medium	23 Jun 2025, 13:41:46	Attempt.Login	Someone tried to log in with an invalid use	10.244.0.1	Data Center
+	Low	23 Jun 2025, 13:41:07	Attempt.Login	Someone tried to log in as 'admin' from 37	10.244.0.1	Data Center
+	Medium	23 Jun 2025, 13:41:05	Attempt.Login	Someone tried to log in with an invalid use	10.244.0.1	Data Center
+	Medium	23 Jun 2025, 13:40:01	Attempt.Login	Someone tried to log in as 'root' from 188.	10.244.0.1	Data Center
+	Medium	23 Jun 2025, 13:35:13	Attempt.Login	Someone tried to log in as 'root' from 188.	10.244.0.1	Data Center
+	Medium	23 Jun 2025, 13:29:29	Attempt.Login	Someone tried to log in as 'root' from 80.9	10.244.0.1	Data Center
+	Medium	23 Jun 2025, 13:25:36	Attempt.Login	Someone tried to log in as 'root' from 117.	10.244.0.1	Data Center



IDMEFv2 Alerter (Android App)



IDMEFV2 Alerter (Android)



Incident Detection Task Force

www.idmefv2.org

