European Control System Security Incident Analysis Network

ECOSSIAN

Pan European detection and management of incidents and attacks on European Critical Infrastructures

Elancourt, April 26th 2017

ECOSSIAN FP7 PROJECT:

Pan European detection and management of incidents and attacks on European Critical Infrastructures

Daniel Meister
(Airbus Defence and Space GmbH)

Elancourt, April 26th 2017

European Control System Security Incident Analysis Network

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607577.

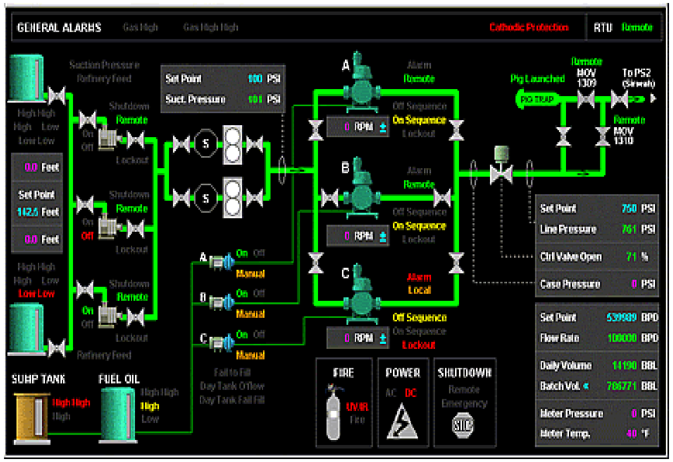
Background

- Modern Society strongly relies on reliable and continuous availability of critical infrastructures and their services

•A serious disruption of such services could lead to risk for safety of life and economic welfare

•Critical infrastructures are more and more in focus of attacks out of the cyber-space

- Terrorists
- Governments
- Competitor/industrial espionage
- Cyber criminals and …
- … growing convergence by "script kiddies"



Set Point 100 PSI
Suct. Pressure 101 PSI

0.0 Feet
Set Point 142.5 Feet
0.0 Feet

0 RPM
0 RPM
0 RPM

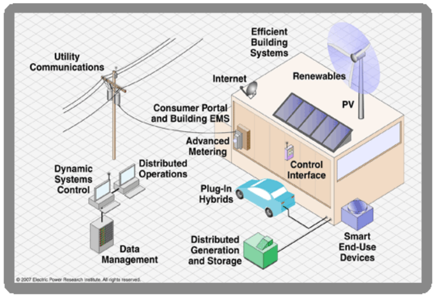
Set Point 750 PSI
Line Pressure 761 PSI
Ctrl Valve Open 71 %
Case Pressure 0 PSI

Set Point 539989 BPD
Flow Rate 100000 BPD
Daily Volume 14190 BBL
Batch Vol. 786771 BBL
Meter Pressure 0 PSI
Meter Temp. 40 °F

Motivation

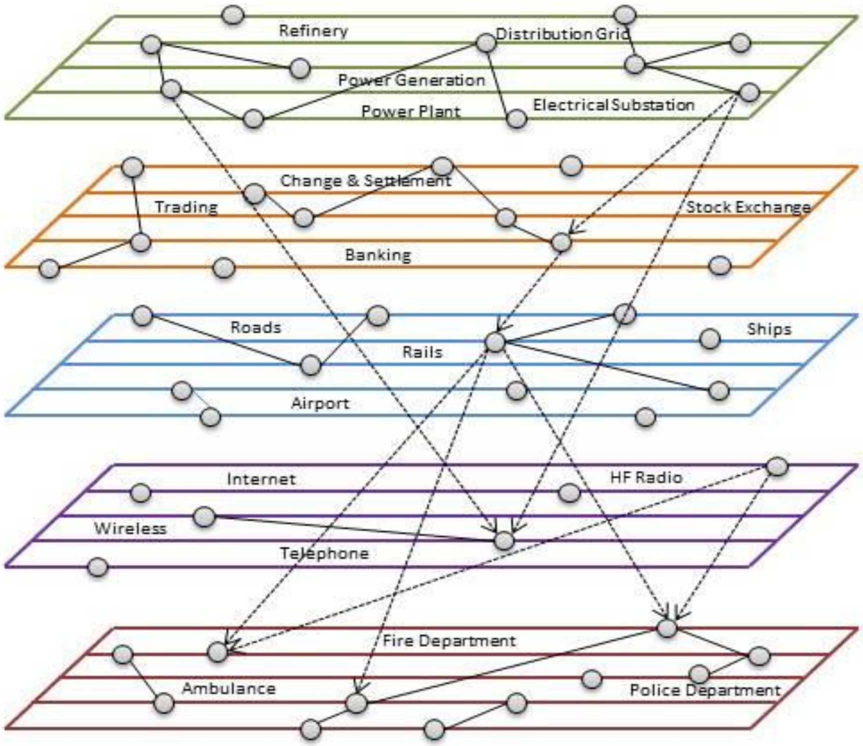
- Attack surface to critical infrastructures is continuously growing because:
  - Deployment of COTS-products
  - Change from proprietary protocols and products to common technologies coming from the pure IT world“
  - Losing the „Air-Gaps“ through convergence
  - More and more use of mobile devices and services
  - Very long Life-Cycle of plants (10-25 years)
  - Security capabilities of used technologies is 5 to 10 years behind enterprise IT
  - Common cyber-security approach is only very limited applicable in systems with these special needs e.g. real time response

© 2009 Electric Power Research Institute, Inc. All rights reserved.



Motivation

- Interdependencies between critical infrastructure (CI)



Energy, Oil & Gas

Finance

Transportation

Information & Telecom

Emergency Services

ECOSSIAN Key Figures

Timeframe

Start: 1st June, 2014

Duration: 3 years

Consortium

19 partners from 9 countries

Cost

Total: EUR 13.2 M

EC: EUR 9.2 M

AGI: EUR 1.1M

ECOSSIAN Mission

The mission of ECOSSIAN is to improve the **detection** and management of highly sophisticated cyber security incidents and attacks against critical infrastructures by implementing a pan-European **early warning** and **situational awareness** framework with command and control facilities.

Architecture (I)

Operator SOCs

Posteitaliane

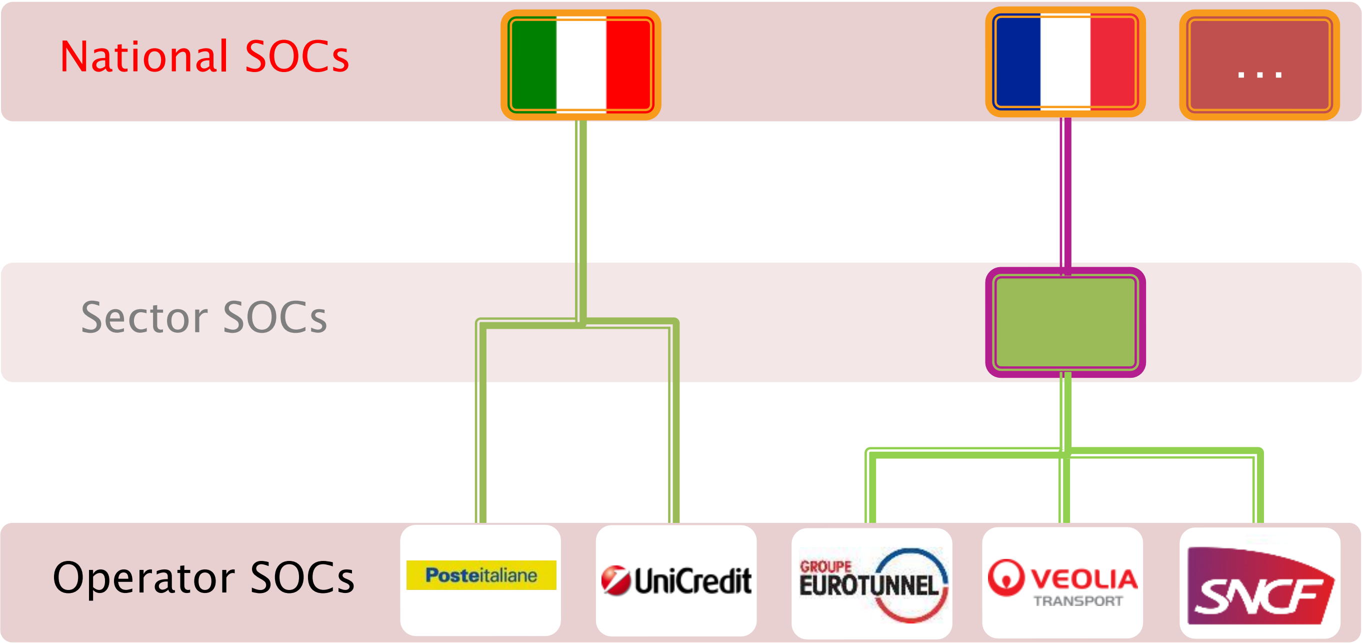
UniCredit

GROUPE EUROTUNNEL

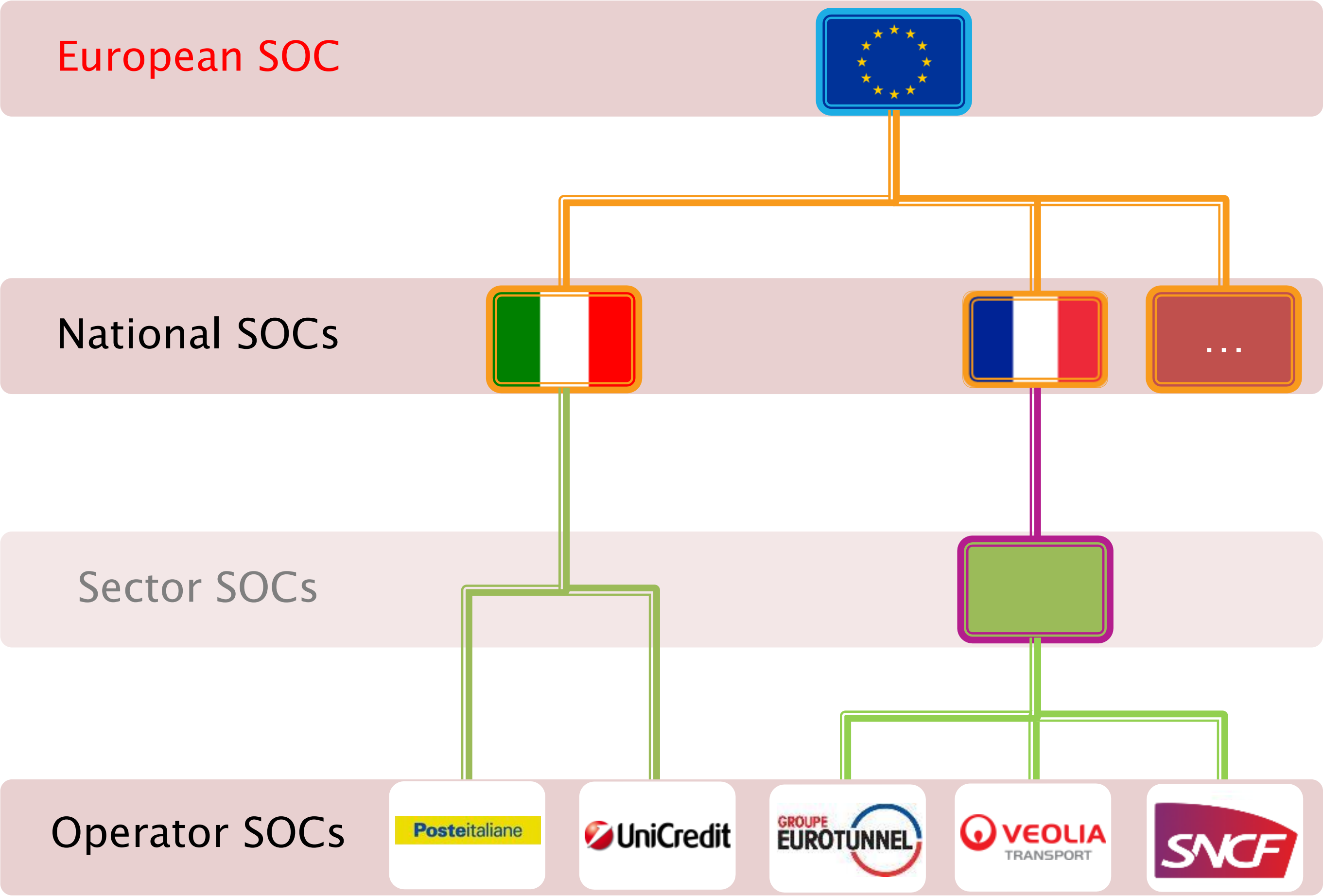
VEOLIA TRANSPORT

SNCF

Architecture (II)



Architecture (III)



ECOSSIAN Capabilities

Pan-European Situational Awareness Framework

Secure Incident Information Sharing Network

Advanced detection capabilities

Pan-European Early Warning entity

ECOSSIAN Demonstrations

Financial Sector	Energy Distribution Sector	Transportation Sector
Posteitaliane	Gas Networks Ireland	Infraestruturas de Portugal

Agenda

- **Welcome**
- **Introduction of the ECOSSIAN project**
  - Daniel Meister (Airbus Defence and Space GmbH)
- **ECOSSIAN national demonstrations (Summary and Feedback)**
  - **Italian Demonstration** - Early Warning System on Cyber-attacks targeting Critical Financial Infrastructures: Cécile Abdo (Airbus Cybersecurity)
  - **Irish Demonstration** - Detection of Attack on Gas Provider: Paul Gaynor (Gas Networks Ireland)
  - **Portuguese Demonstration** - Support for Forensic Analysis of Attack on Transportation Infrastructure: José Carlos Gonçalves (Serviços de Telecomunicações, S. A.)
- **Legal, Ethical and Social aspects**
  - Jessica Schroers (Katholieke Universiteit Leuven)
- **Break**
- **Operational demonstration**
- **Q&A and evaluation**
- **Cocktail & ECOSSIAN technology exhibition**

ECOSSIAN FP7 PROJECT:

National Demonstrations

Elancourt, April 26th 2017

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607577.

European Control System Security Incident Analysis Network

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607577.

ECOSSIAN FP7 PROJECT:

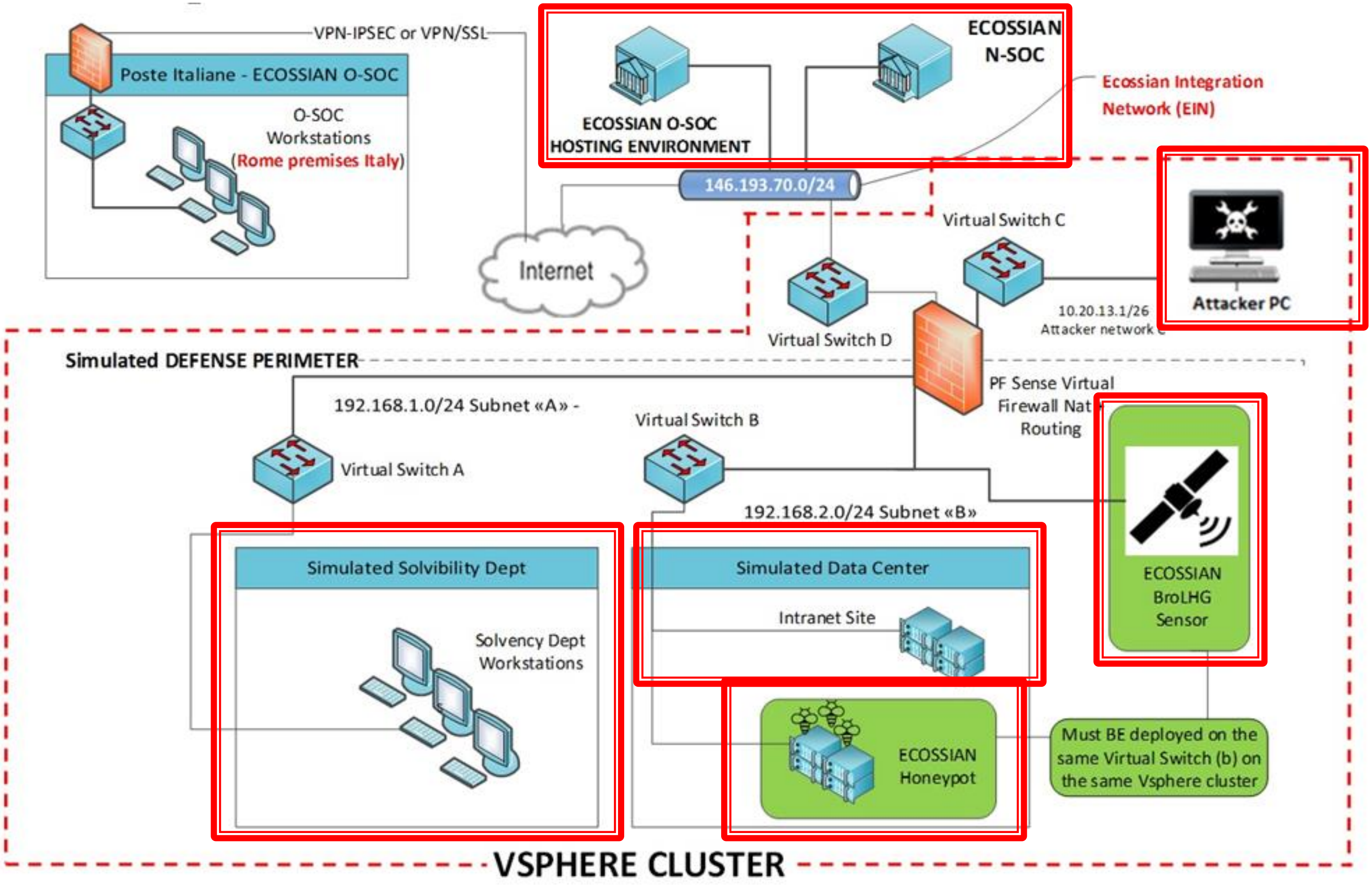
Italian demonstration: Early Warning System on Cyber-attacks targeting Critical Financial Infrastructures

Cécile Abdo
(Airbus Cybersecurity)

Elancourt, April 26th 2017

Italian demonstration

Demonstration infrastructure

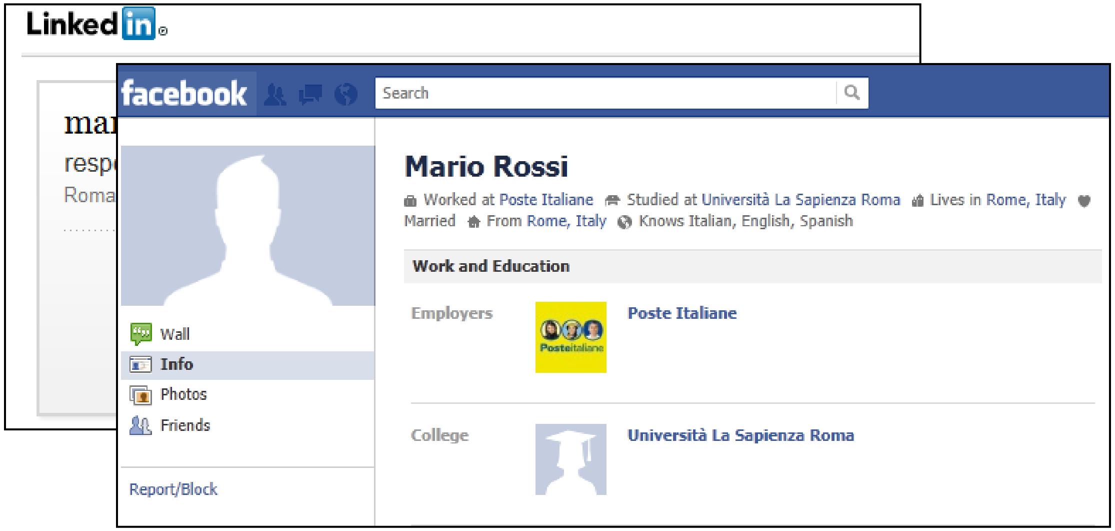

VPN-IPSEC or VPN/SSL
Poste Italiane - ECOSSIAN O-SOC
O-SOC Workstations (Rome premises Italy)
ECOSSIAN O-SOC HOSTING ENVIRONMENT
ECOSSIAN N-SOC
Ecossian Integration Network (EIN)
146.193.70.0/24
Internet
Virtual Switch C
Virtual Switch D
Attacker PC
10.20.13.1/26 Attacker network
Simulated DEFENSE PERIMETER
PF Sense Virtual Firewall Nat Routing
192.168.1.0/24 Subnet «A»
Virtual Switch A
Virtual Switch B
192.168.2.0/24 Subnet «B»
Simulated Solvibility Dept
Solvency Dept Workstations
Simulated Data Center
Intranet Site
ECOSSIAN Honeypot
ECOSSIAN BroLHG Sensor
Must BE deployed on the same Virtual Switch (b) on the same Vsphere cluster
VSPHERE CLUSTER

Scenario overview

- **Involved end-user**
  - Poste Italiane (PI) is a national and international benchmark in postal, courier, logistics, finance, insurance, and, most recently, the mobile phone market segments.
- **Incident management**
  - Attack detected by **ECOSSIAN sensors (Honeypot & BroLHG).** The SIEM generates a incident report.
  - Incident reported to the O-SOC through OSSIM and Cymerius
- **Incident sharing (Secure Gateway, ABE)**
- **Incident analysis by the N-SOC**
  - Correlation by CAESAIR
  - Situation awareness by Cymerius
  - Feedback to both PI's O-SOC and external stakeholders

Targeted attack: preliminary phase

Social Engineering & Spear Phishing Attack

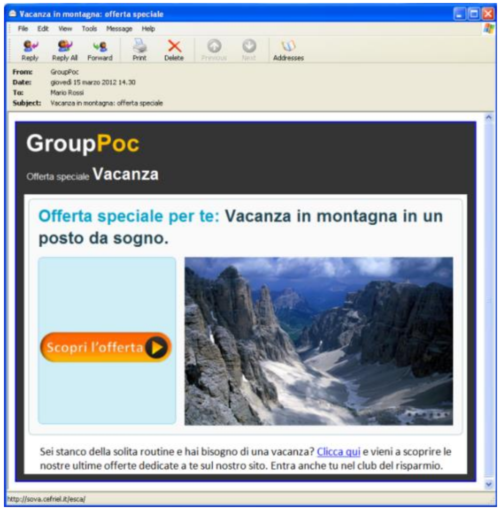


Mario Rossi

Worked at Poste Italiane · Studied at Università La Sapienza Roma · Lives in Rome, Italy · Married · From Rome, Italy · Knows Italian, English, Spanish

Work and Education

Employers	Poste Italiane
College	Università La Sapienza Roma



From: GroupPoc
Date: giovedì 15 marzo 2012 14.30
To: Mario Rossi
Subject: Vacanza in montagna: offerta speciale

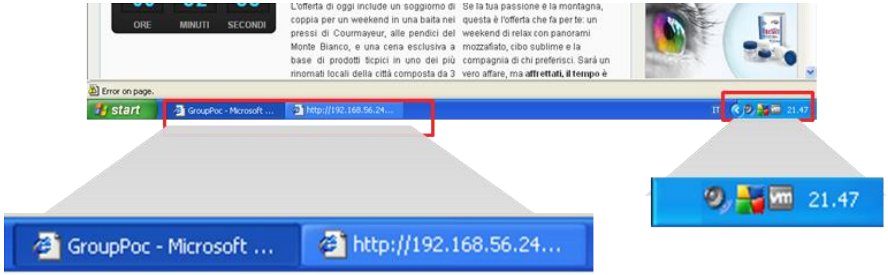
GroupPoc

Offerta speciale Vacanza

Offerta speciale per te: Vacanza in montagna in un posto da sogno.

Sei stanco della solita routine e hai bisogno di una vacanza? Clicca qui e vieni a scoprire le nostre ultime offerte dedicate a te sul nostro sito. Entra anche tu nel club del risparmio.

http://sova.cefriel.it/esca/



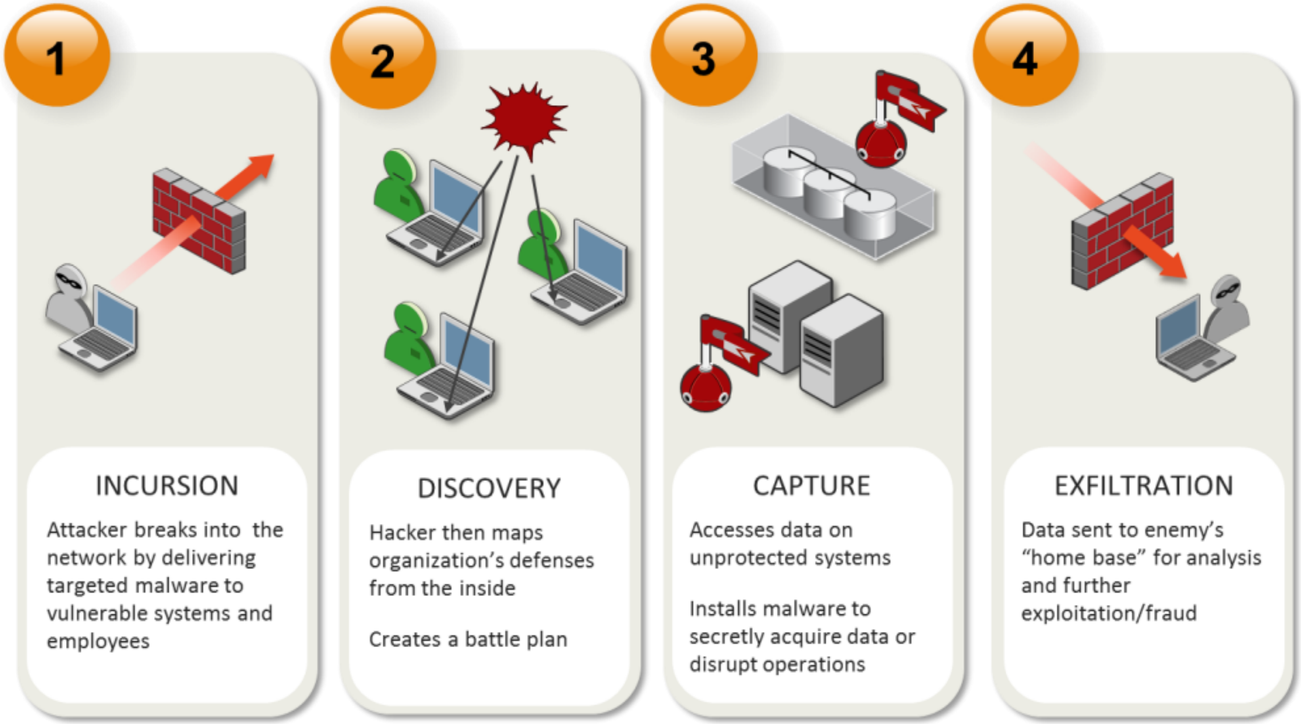
L'offerta di oggi include un soggiorno di coppia per un weekend in una baita nei pressi di Courmayeur, alle pendici del Monte Bianco, e una cena esclusiva a base di prodotti tipici in uno dei più rinomati locali della città composta da 3

Se la tua passione è la montagna, questa è l'offerta che fa per te: un weekend di relax con panorami mozzafiato, cibo sublime e la compagnia di chi preferisci. Sarà un vero affare, ma **affrettati, il tempo è**

Attack description

- **Advanced Persistent Threats (APT) attack**

- In four steps:
  - Incursion
  - Discovery
  - Capture
  - Exfiltration



INCURSION

Attacker breaks into the network by delivering targeted malware to vulnerable systems and employees

DISCOVERY

Hacker then maps organization's defenses from the inside

Creates a battle plan

CAPTURE

Accesses data on unprotected systems

Installs malware to secretly acquire data or disrupt operations

EXFILTRATION

Data sent to enemy's "home base" for analysis and further exploitation/fraud

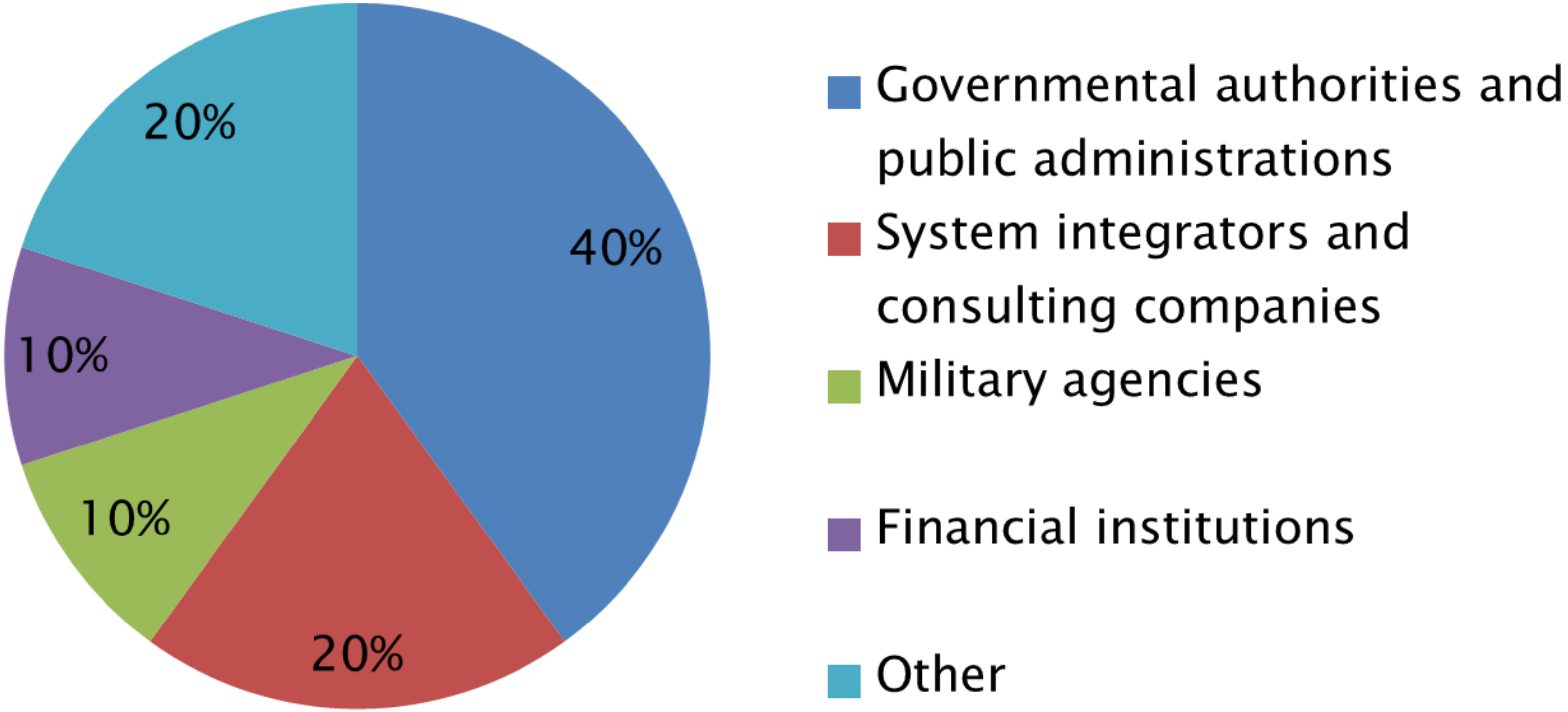
Source: Symantech

ECOSSIAN (O-SOC + N-SOC)

- Detection:
  - Honeypot
  - BroLHG
- Analysis & Correlation:
  - Cymerius
  - CAESAIR
  - Acquisition Module
- Information sharing:
  - Secure Gateway
  - Attribute Based Encryption

Italian demonstration

Attendees



55 % close to O-SOC business
45 % close to N-SOC business

Stakeholder feedback

- A questionnaire was filled by attendees on
  (i) the platform functional requirements
  (ii) the platform non-functional requirements
  (iii) legal, ethical and societal issues and
  (iv) other aspects contributing to depict a general assessment regarding the quality of the solution provided.

→ **mostly evaluated between 4/5 and 5/5**

Stakeholder feedback

Most positive feedback related to

- **Openness and transparence** of the ECOSSIAN framework in terms of how it handles security related information.
- **Compatibility of the ECOSSIAN framework** with legacy incident management processes and tools.
- The ability to **share information** in real time, considering that data could be anonymized and that attribute-based encryption (ABE) would guarantee only a selective access
- The **dashboard** (providing information on incidents, parameters, affected sites, causes etc.)
- The fit of the ECOSSIAN framework into related **national security strategies**.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607577.

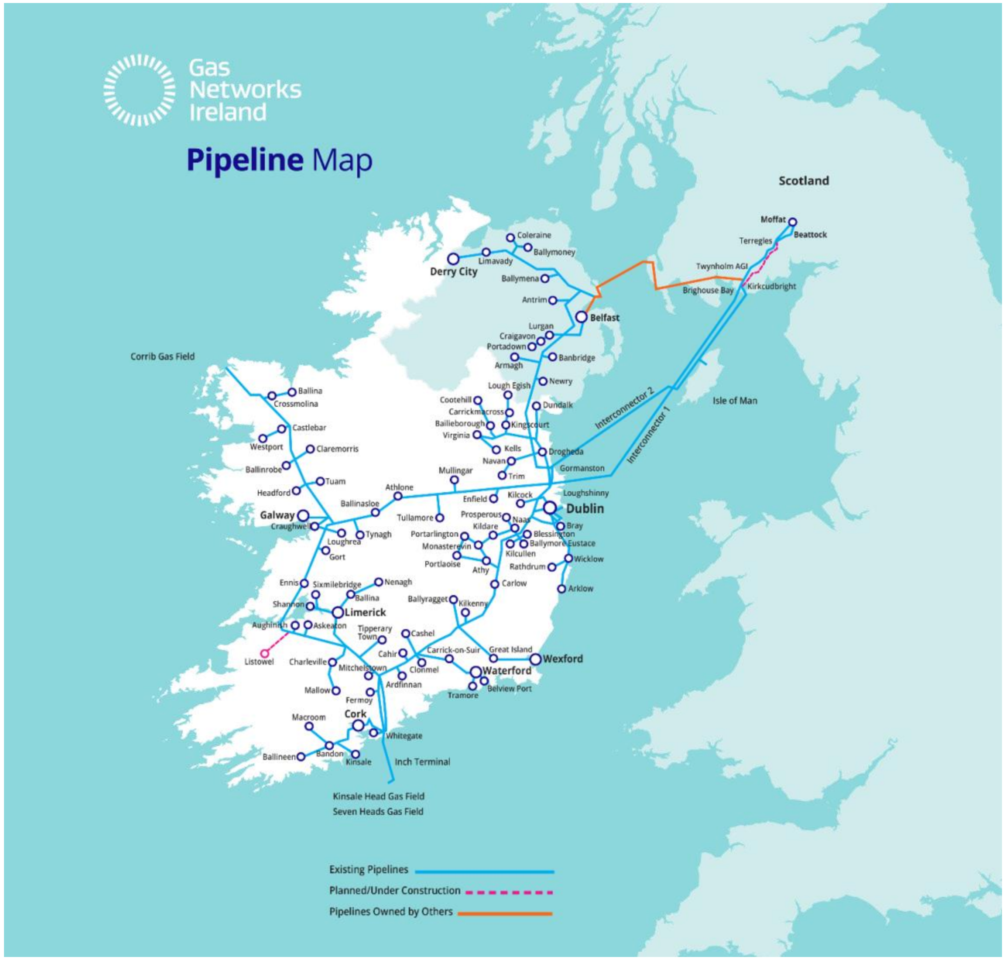
ECOSSIAN FP7 PROJECT:

Irish demonstration: Detection of Attack on Gas Provider

Paul Gaynor
(Gas Networks Ireland)

Elancourt, April 26th 2017

Gas Networks Ireland

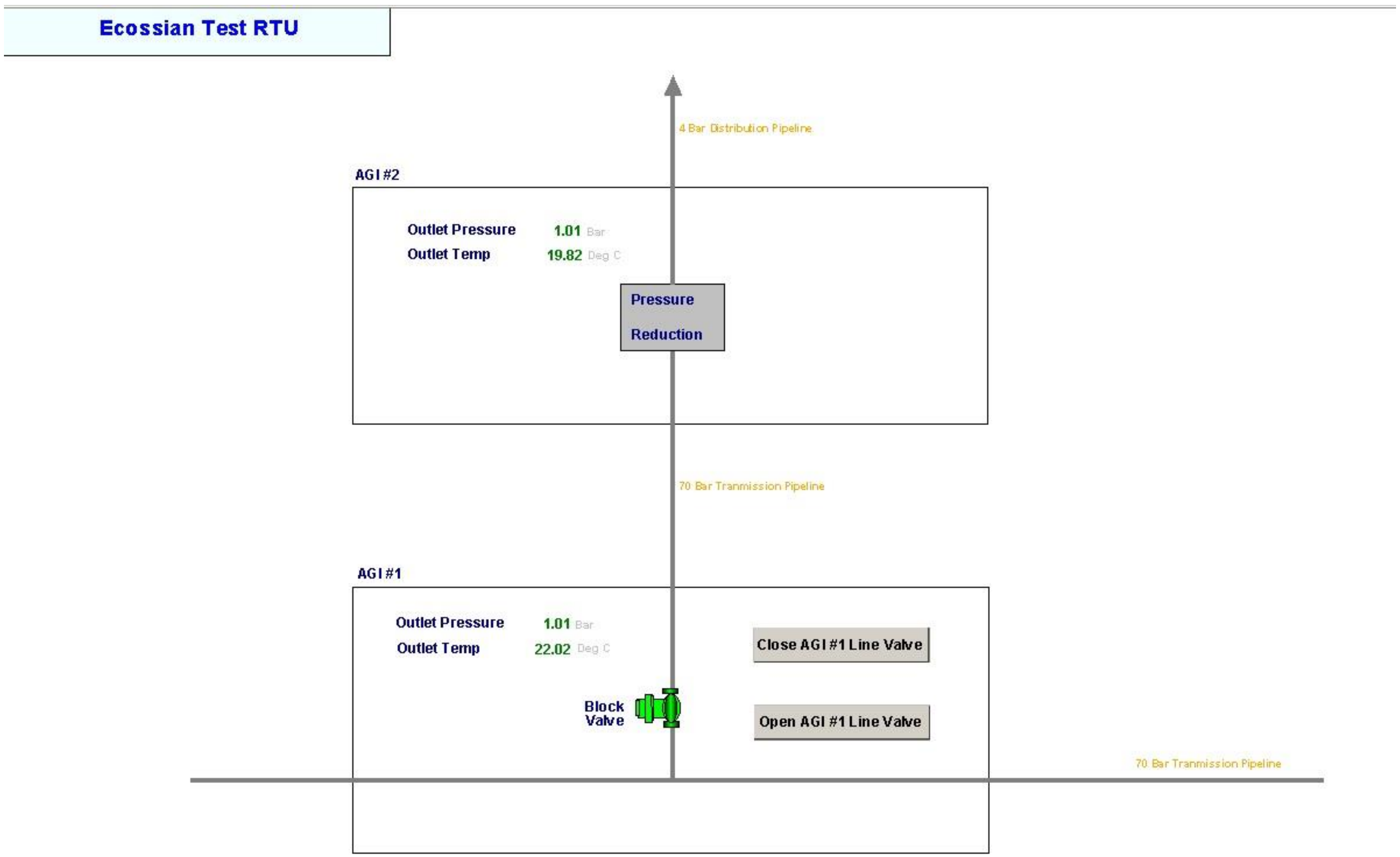


27%
National
Energy

680,000
Customers

13,954 KM
National
Pipeline

GNI Grid Control View of an AGI



Ecossian Test RTU

AGI #2

Outlet Pressure 1.01 Bar

Outlet Temp 19.82 Deg C

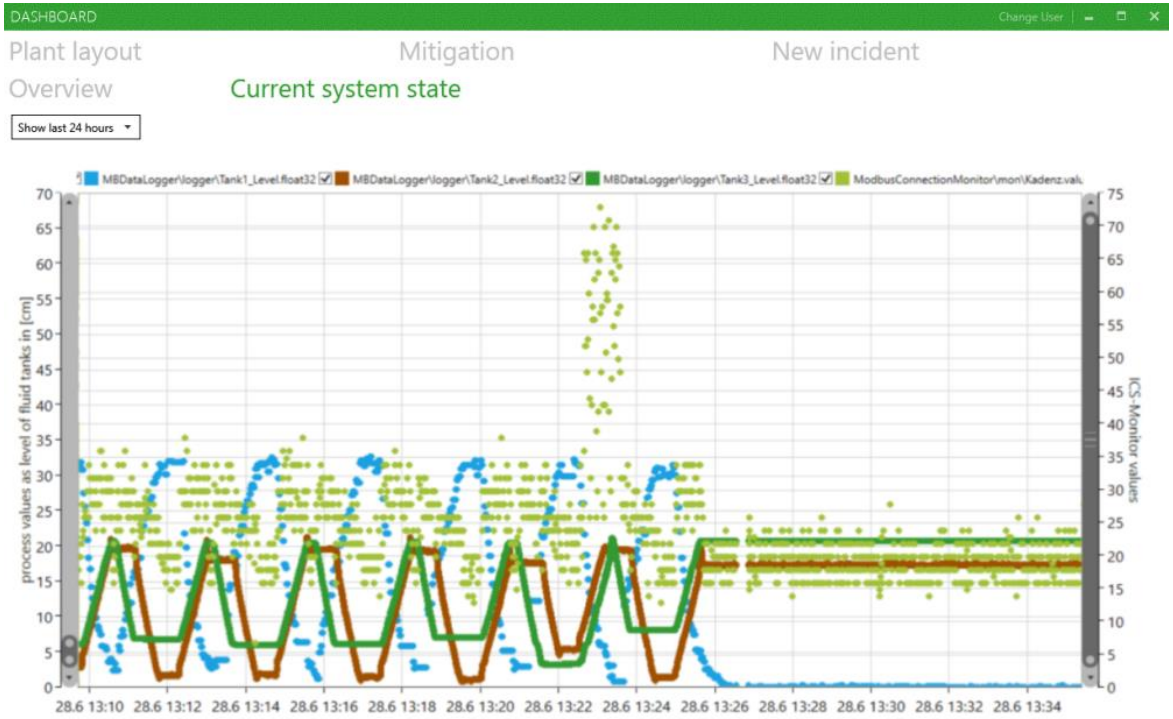
AGI #1

Outlet Pressure 1.01 Bar

Outlet Temp 22.02 Deg C

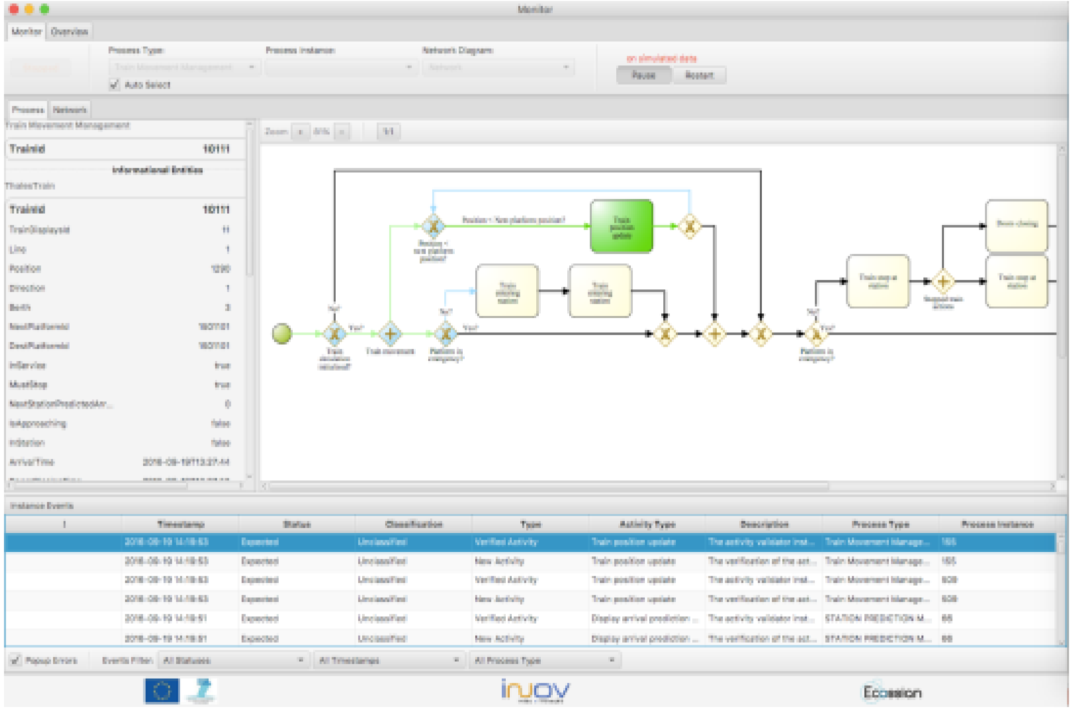
4 Bar Distribution Pipeline
Pressure Reduction
70 Bar Tranmission Pipeline
Block Valve
Close AGI #1 Line Valve
Open AGI #1 Line Valve
70 Bar Tranmission Pipeline

Sensor 1: ICS-Monitor



Distributed ICS Sensors and aggregation module detecting deviations from defined model.

Sensor 2: BP-IDS



Monitor

Process Type: Train Movement Management
Process Instance:
Network Diagram: Network
☑ Auto Select

on simulated data

Train Movement Management

TrainId	10111

Informational Entities

ThalesTrain

TrainId	10111
TrainDisplayId	11
Line	1
Position	1290
Direction	1
Berth	3
NextPlatformId	1801?01
DestPlatformId	1801?01
InService	true
MustStop	true
NextStationPredictedAr...	0
IsApproaching	false
InStation	false
ArrivalTime	2016-08-19T13:27:44

Instance Events

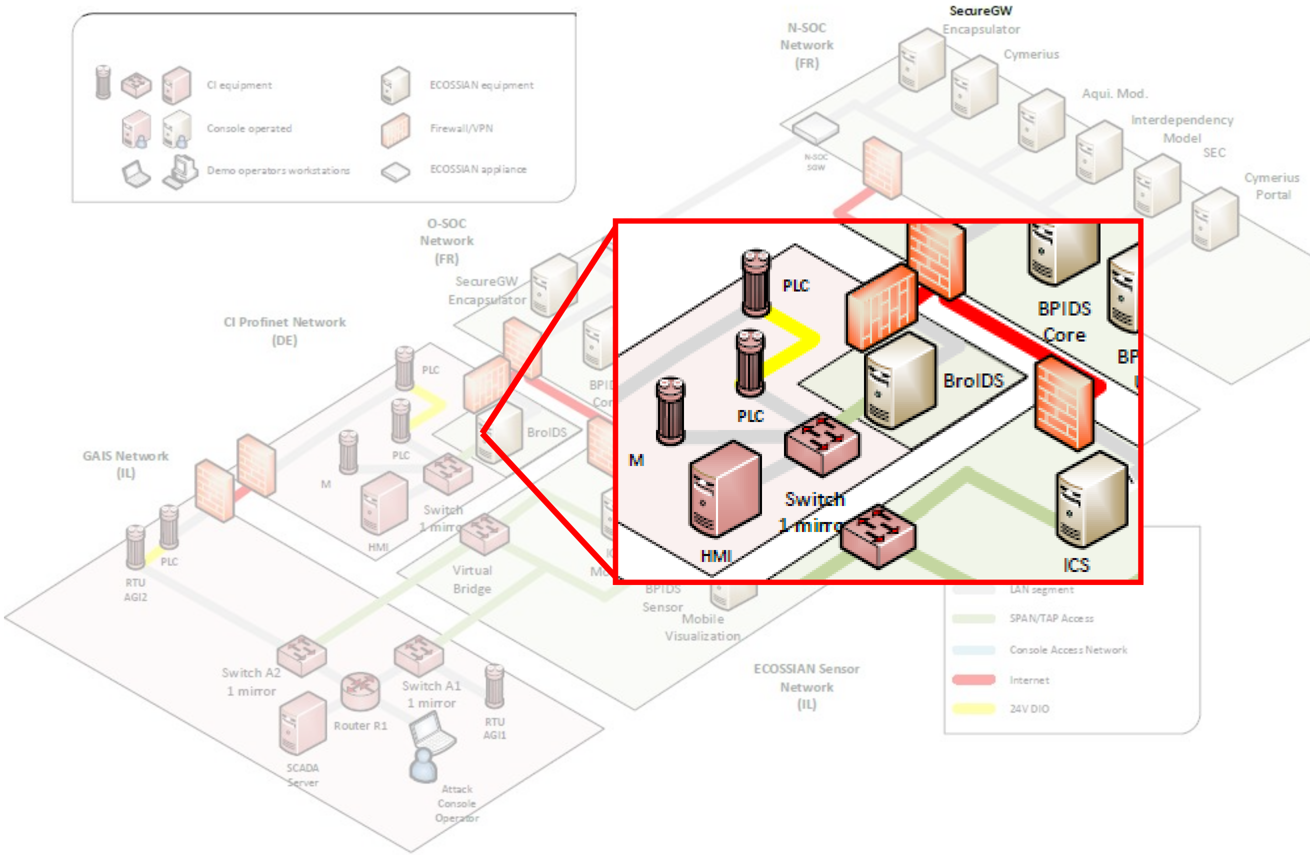
!	Timestamp	Status	Classification	Type	Activity Type	Description	Process Type	Process Instance
	2016-08-19 14:18:53	Expected	Unclassified	Verified Activity	Train position update	The activity validator inst...	Train Movement Manage...	155
	2016-08-19 14:18:53	Expected	Unclassified	New Activity	Train position update	The verification of the act...	Train Movement Manage...	155
	2016-08-19 14:18:53	Expected	Unclassified	Verified Activity	Train position update	The activity validator inst...	Train Movement Manage...	509
	2016-08-19 14:18:53	Expected	Unclassified	New Activity	Train position update	The verification of the act...	Train Movement Manage...	509
	2016-08-19 14:18:51	Expected	Unclassified	Verified Activity	Display arrival prediction ...	The activity validator inst...	STATION PREDICTION M...	88
	2016-08-19 14:18:51	Expected	Unclassified	New Activity	Display arrival prediction ...	The verification of the act...	STATION PREDICTION M...	88

☑ Popup Errors   Events Filter: All Statuses   All Timestamps   All Process Type

Business process specification-based intrusion detection system

BP-IDS process view

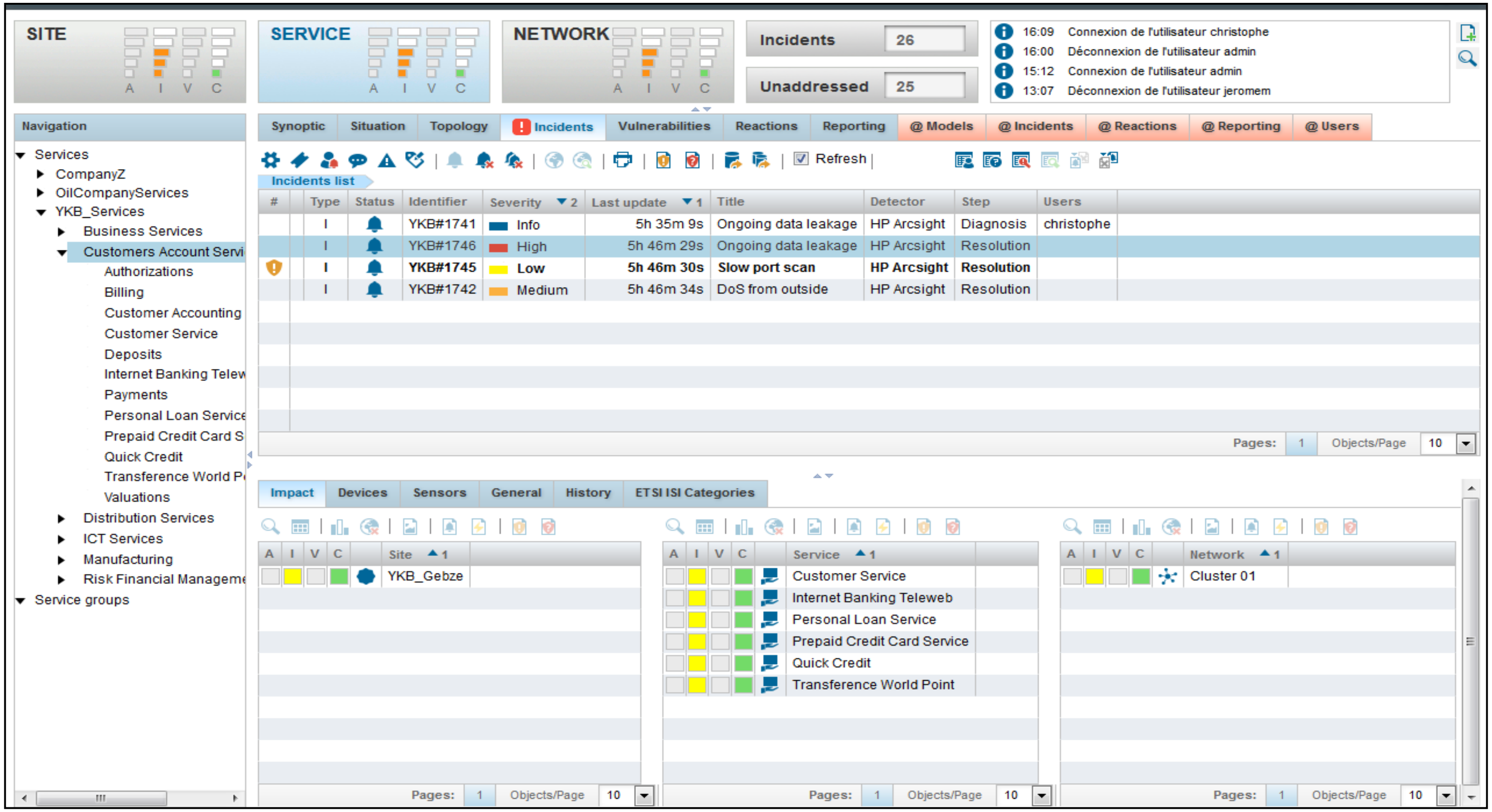
Sensor 3: BroIDS-ICS



The BroIDS-ICS sensor, analysing the PROFINET protocol, will detect changes in topology because of unexpected IP requests by using the PROFINET Discovery and basic Configuration Protocol (DCP).

The combination of BroICS-ICS and Cymerius helps to alert the O-SOC operator about a possible intrusion

Cymerius



Incidents 26

Unaddressed 25

16:09 Connexion de l'utilisateur christophe
16:00 Déconnexion de l'utilisateur admin
15:12 Connexion de l'utilisateur admin
13:07 Déconnexion de l'utilisateur jeromem

Navigation

- Services
  - CompanyZ
  - OilCompanyServices
  - YKB_Services
    - Business Services
    - Customers Account Servi
      - Authorizations
      - Billing
      - Customer Accounting
      - Customer Service
      - Deposits
      - Internet Banking Telew
      - Payments
      - Personal Loan Service
      - Prepaid Credit Card S
      - Quick Credit
      - Transference World P
      - Valuations
    - Distribution Services
    - ICT Services
    - Manufacturing
    - Risk Financial Manageme
- Service groups

#	Type	Status	Identifier	Severity ▼2	Last update ▼1	Title	Detector	Step	Users
	I		YKB#1741	Info	5h 35m 9s	Ongoing data leakage	HP Arcsight	Diagnosis	christophe
	I		YKB#1746	High	5h 46m 29s	Ongoing data leakage	HP Arcsight	Resolution	
	I		**YKB#1745**	**Low**	**5h 46m 30s**	**Slow port scan**	**HP Arcsight**	**Resolution**	
	I		YKB#1742	Medium	5h 46m 34s	DoS from outside	HP Arcsight	Resolution	

Pages: 1 Objects/Page 10

A	I	V	C		Site ▲1
	🟨		🟩		YKB_Gebze

Pages: 1 Objects/Page 10

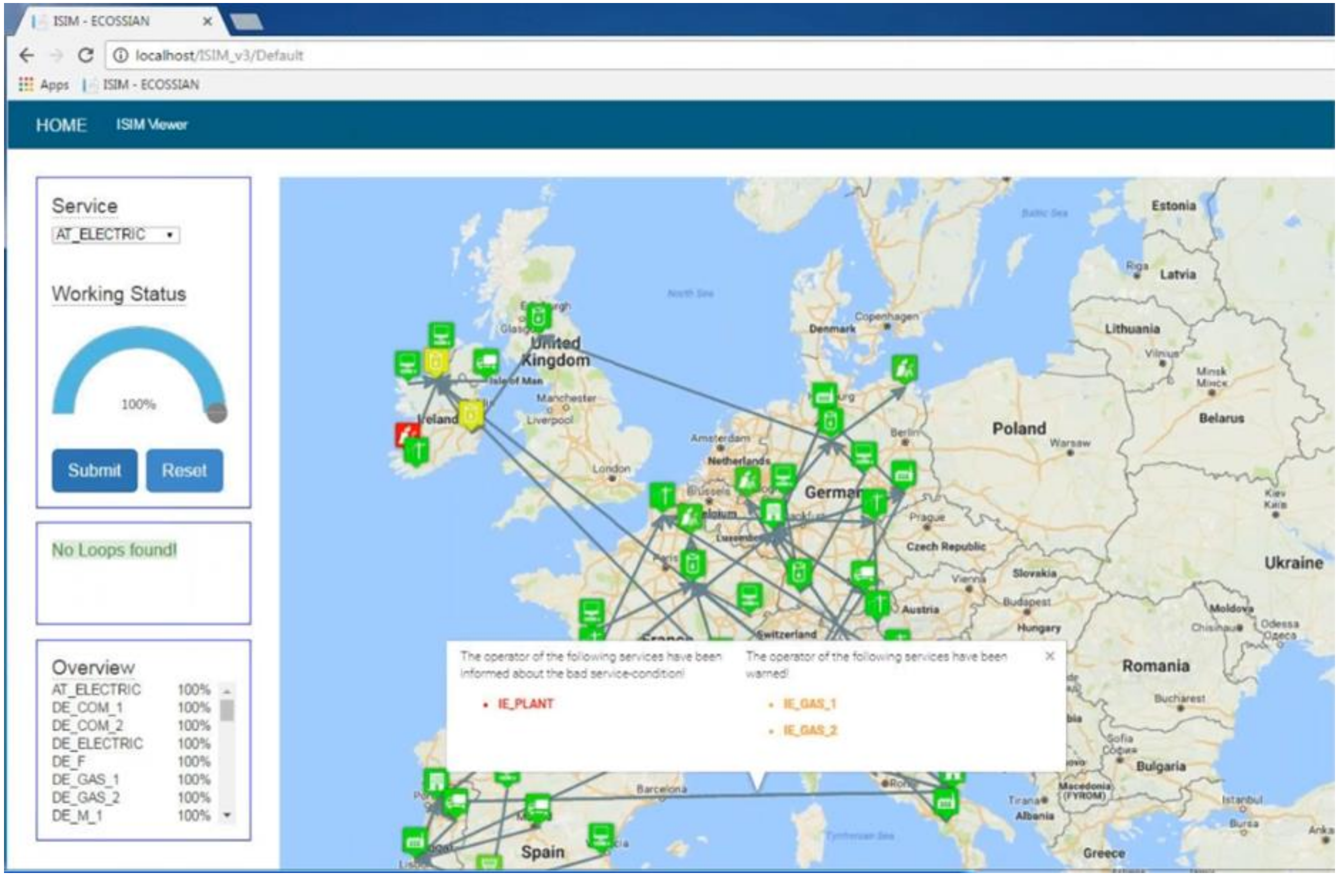
A	I	V	C		Service ▲1
	🟨		🟩		Customer Service
	🟨		🟩		Internet Banking Teleweb
	🟨		🟩		Personal Loan Service
	🟨		🟩		Prepaid Credit Card Service
	🟨		🟩		Quick Credit
	🟨		🟩		Transference World Point

Pages: 1 Objects/Page 10

A	I	V	C		Network ▲1
	🟨		🟩		Cluster 01

Pages: 1 Objects/Page 10

Interdependency Model



Service: AT_ELECTRIC

Working Status

100%

No Loops found!

Overview

AT_ELECTRIC	100%
DE_COM_1	100%
DE_COM_2	100%
DE_ELECTRIC	100%
DE_F	100%
DE_GAS_1	100%
DE_GAS_2	100%
DE_M_1	100%

The operator of the following services have been informed about the bad service-condition!

- IE_PLANT

The operator of the following services have been warned!

- IE_GAS_1
- IE_GAS_2

National Demonstration Feedback

Gas Networks Ireland HQ, Cork.

March 1st 2017

Energy providers, Utility providers, Government agencies, Academic researchers, Engineering consultants and Regulatory advisors

ECOSSIAN concept

Relevance of attack scenarios demonstrated

The ECOSSIAN hierarchical organisational proposal

Confidential exchange of files & information

Ecossian

This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607577.

ECOSSIAN FP7 PROJECT:

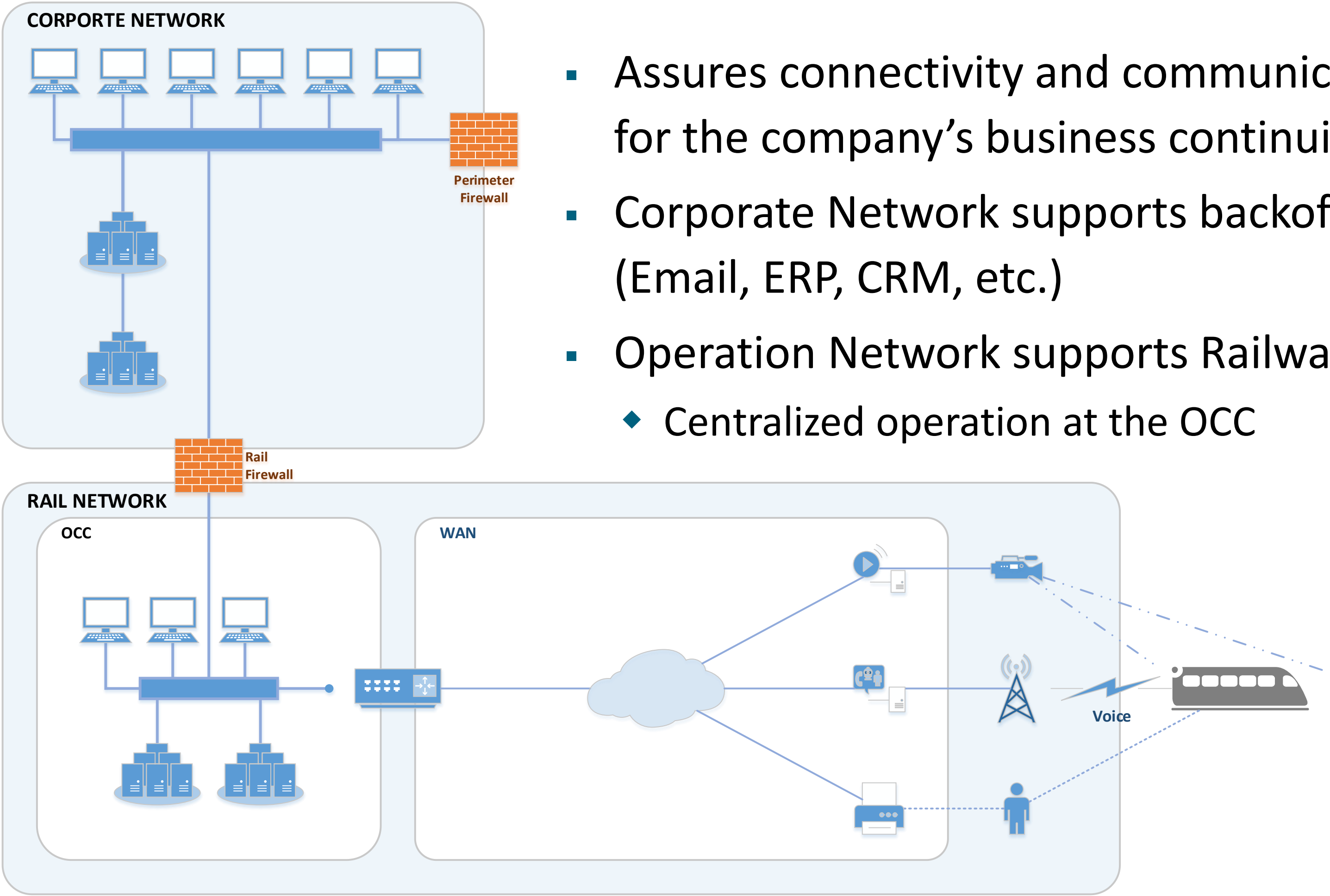
Portuguese demonstration: Support for Forensic Analysis of Attack on Transportation Infrastructure

José Carlos Gonçalves
(Serviços de Telecomunicações, S. A.)

Elancourt, April 26th 2017

European Control System Security Incident Analysis Network

IP Network Architecture



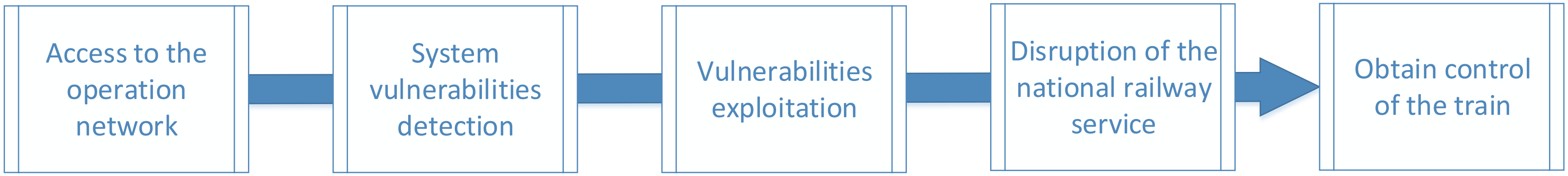
- Assures connectivity and communication security for the company’s business continuity;
- Corporate Network supports backoffice applications (Email, ERP, CRM, etc.)
- Operation Network supports Railway applications
  - Centralized operation at the OCC

Demo Targeted Systems

- Speed Limit System, supports the infrastructure manager to coordinate the enforcement of speed limits on specific segments of the track;
- SCADA System, which performs the Infrastructure Supervision and Train Energy Control;
- Obstacle Detection System, on dangerous cliffs, help detecting falling rocks on the track;
- Train-to-Ground System, used to communicate directly between the OCC and the train driver;
- Video surveillance System, supports the achievement of infrastructure security and people safety;
- Communication Network infrastructure, supports the communication and security of the railway applications.

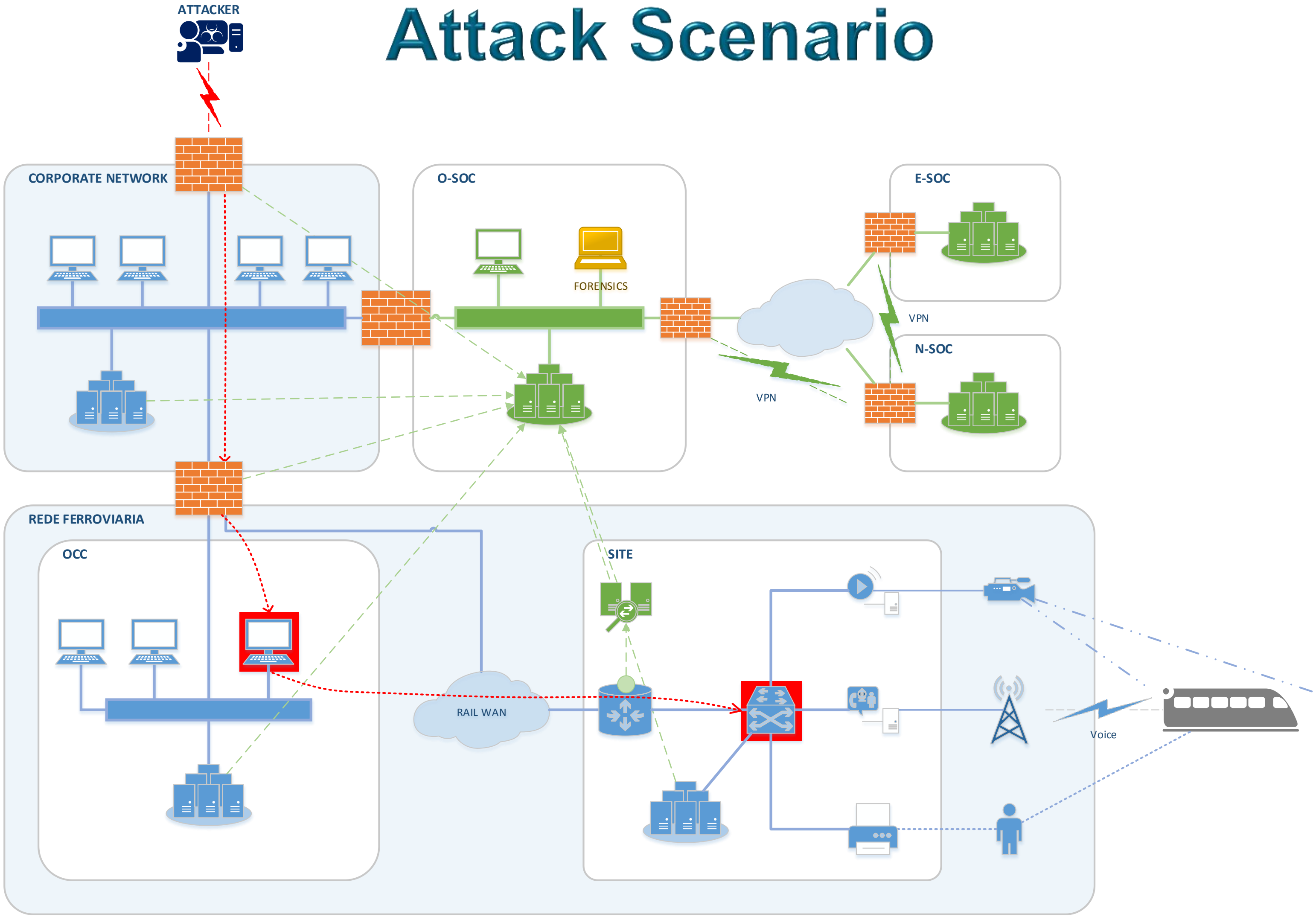
Attack Methodology

- Gain access to the railway operation network;
- Gather system information and detect vulnerabilities;
- Exploit system vulnerabilities and cause service disruption;
- Achieve attacker’s goal by obtaining control the train.


Access to the operation network
System vulnerabilities detection
Vulnerabilities exploitation
Disruption of the national railway service
Obtain control of the train

Portuguese use-case

Attack Scenario

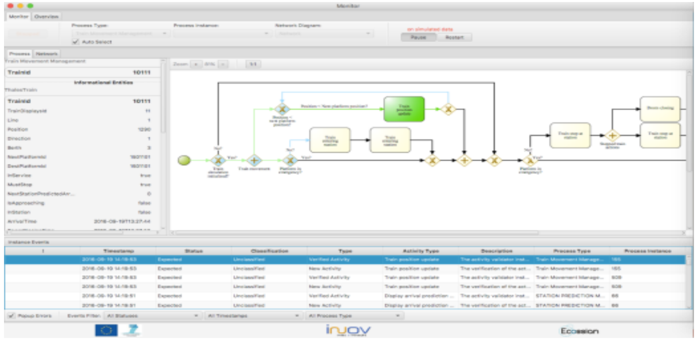


Attack & Detection

System	Attack	ECOSSIAN Sensor – Detection
Speed Limit System	Forged speed limitation orders	BPIDS – Process verification through logs
SCADA System	Execution of SCADA commands at the PLC	BPIDS – Process verification through logs
Obstacle Detection System	Injection of a false detection	BPIDS – Process verification through logs
Train-to-Ground System	DoS	N/A
Video surveillance System	DoS	N/A
Communication Network infrastructure	VPN access with stolen credentials	AECID – Statistical deviation from historical trends based on the VPN and firewall logs
	Network scanning	BroLHG – Detects abnormal traffic
	Remote connection	BroLHG – Detects abnormal traffic

BP-IDS

Business Process based Intrusion Detection System (BP-IDS) which collects traces of business process execution through a set of passive sensors installed on the organisation’s ICT infrastructure, and compares it in real-time with a BP specification.

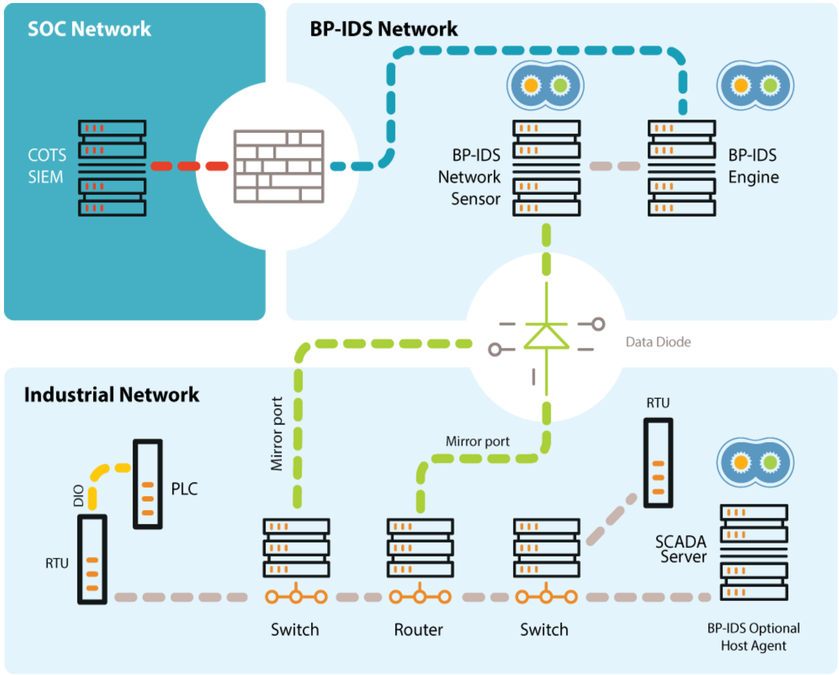


Train Movement Management

TrainId	10111
Informational Entities	
ThalesTrain	
TrainId	10111
TrainDisplayId	11
Line	1
Position	1290
Direction	1
Berth	3
NextPlatformId	1601101
DestPlatformId	1601101
InService	true
MustStop	true
NextStationPredictedAr...	0
IsApproaching	false
InStation	false
ArrivalTime	2016-09-19T13:27:44

!	Timestamp	Status	Classification	Type	Activity Type	Description	Process Type	Process Instance
	2016-09-19 14:18:53	Expected	Unclassified	Verified Activity	Train position update	The activity validator inst...	Train Movement Manage...	165
	2016-09-19 14:18:53	Expected	Unclassified	New Activity	Train position update	The verification of the act...	Train Movement Manage...	165
	2016-09-19 14:18:53	Expected	Unclassified	Verified Activity	Train position update	The activity validator inst...	Train Movement Manage...	608
	2016-09-19 14:18:53	Expected	Unclassified	New Activity	Train position update	The verification of the act...	Train Movement Manage...	608
	2016-09-19 14:18:51	Expected	Unclassified	Verified Activity	Display arrival prediction ...	The activity validator inst...	STATION PREDICTION M...	66
	2016-09-19 14:18:51	Expected	Unclassified	New Activity	Display arrival prediction ...	The verification of the act...	STATION PREDICTION M...	66

BP-IDS process view

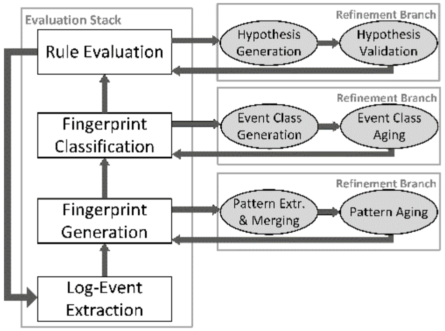


BP–IDS typical deployment scenario

ÆCID

ÆCID (Automatic Event Correlation for Incident Detection) is a partially self-learning, whitelisting-based anomaly detection system operating on log file collections in computer networks – scalable from small industrial control systems to large-scale enterprise infrastructures.

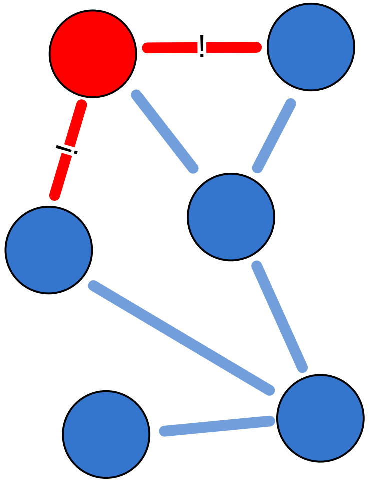
ÆCID digests log output from the network layer (e. g., firewalls, switches, routers) and application layer (e. g., Web servers, DNS, application servers etc.). It detects anomalies of various kinds, including unusual single events, anomalous event parameters, deviating event frequencies, and – most important – suspicious violations of trained event correlations. It can notify operators via numerous channels about discovered anomalies.



BroLHG

Many CI systems reside in closed networks, where changes are less common. In such networks the detection of a change in behaviour in fact can detect the first symptoms of an attack within the network, even before any real benefit can be gained by the attacker.

Link History Graph (LHG) looks at the TCP/IP traffic behaviours of systems to determine their normal behaviour. It catalogues services visible in the traffic stream (tcpdump) on each system it is monitoring, and sees with whom systems are communicating within the local area network (LAN).



Portuguese use-case

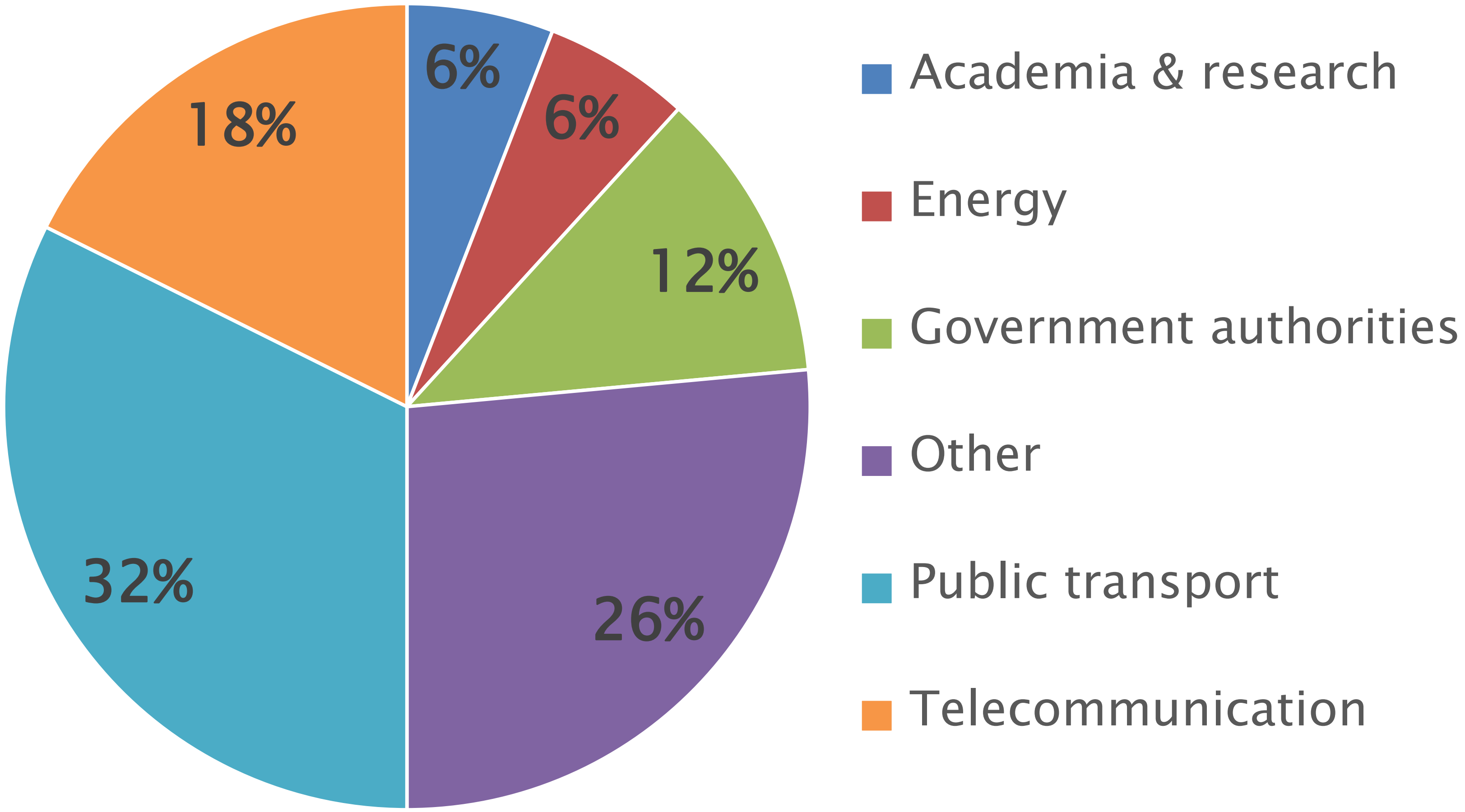
Demonstration

Results & Notes

- Held at IP Headquarters, where 71 guests were present from academia, critical infrastructures (CI) operators, military, regulators, law enforcement agencies and others;
- 46% of the attendees reply to the questionnaire, with a quite positive feedback;
- Suggestion: Potential re-use of ECOSSIAN results as reference within future calls of Horizon 2020 could substantially leverage ECOSSIAN's sustainability.

Portuguese use-case

Attendees



ECOSSIAN FP7 PROJECT:

Legal, Ethical and Societal Aspects

Jessica Schroers
(Katholieke Universiteit Leuven)

Elancourt, April 26th 2017

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607577.

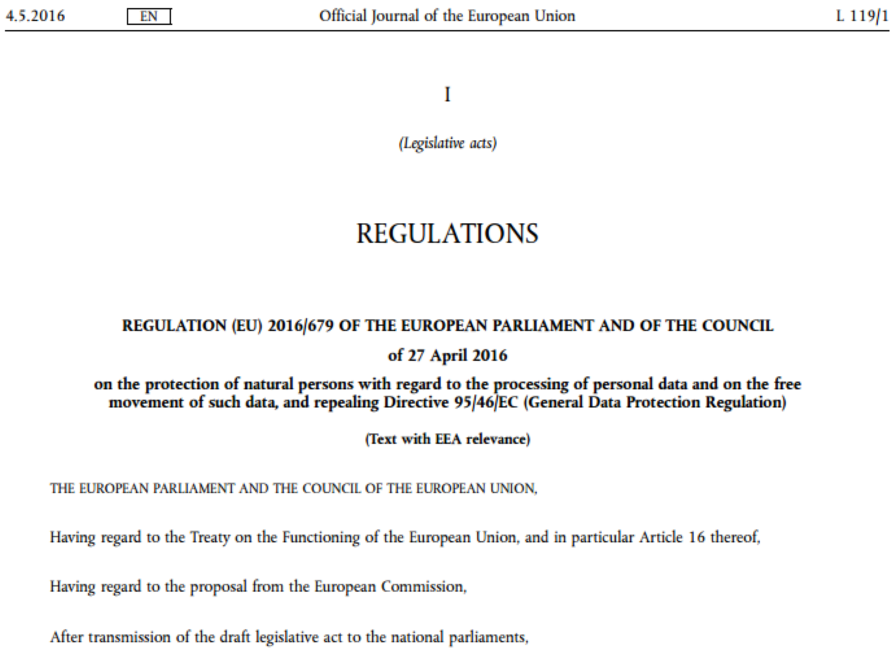
European Control System Security Incident Analysis Network

Legal, Ethical and Societal aspects in ECOSSIAN

- Legal:
  - General Data Protection Regulation
  - NIS Directive
- Ethical & Societal
  - EELPS evaluation
  - Public Private Partnerships

General Data Protection Regulation

- Applies from 25.5.2018
- Personal data



4.5.2016 EN Official Journal of the European Union L 119/1

I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

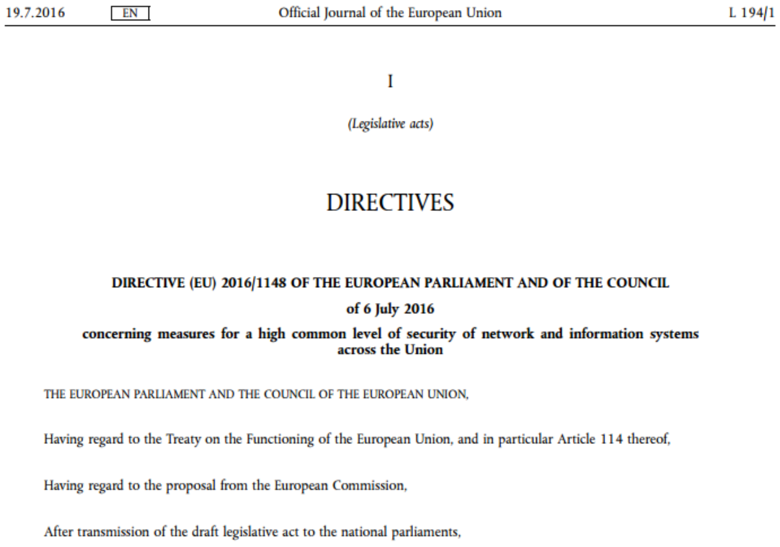
Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

NIS Directive

- Directive → need to be implemented by Member States till 9 May 2018

- Obligations for:
  - Member States
  - Operators of essential services
  - Digital service provider



19.7.2016 EN Official Journal of the European Union L 194/1

I

(Legislative acts)

DIRECTIVES

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 6 July 2016

concerning measures for a high common level of security of network and information systems across the Union

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

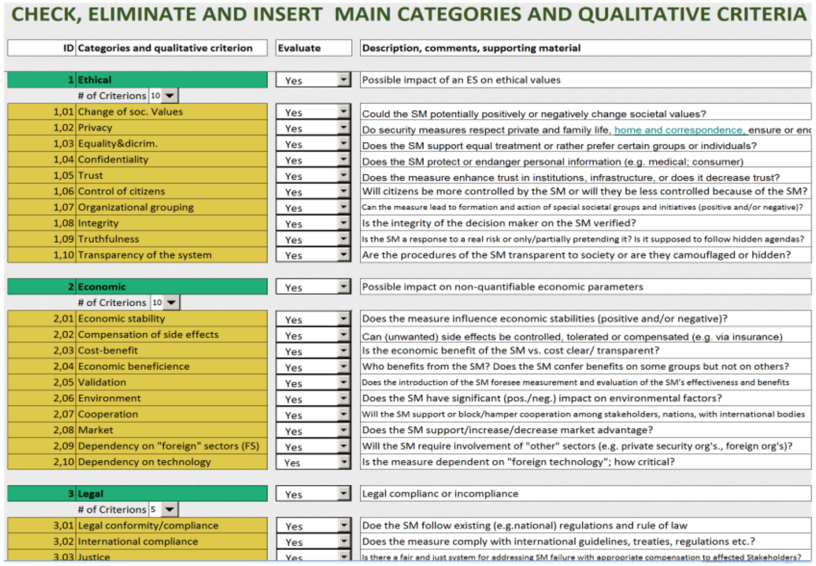
ECOSSIAN and the NIS Directive

- appropriate and proportional technical measures: Threat Detection Modules (ICS Monitor, BPIDS, BroLHG, BroProfinet, AECID, Honeypot) focusing ICS →Detect Incidents & Monitor operations
- Cymerius & Secure Gateway: Analysis, Reporting and Secure Information Sharing and Notification to:
  - Competent Authorities
  - National/Sectorial CSIRT’s (N/S-SOCs)
  - Other MS Operators or CSIRTs (O/N/S SOCs)

EELPS evaluation: Qualitative Factors

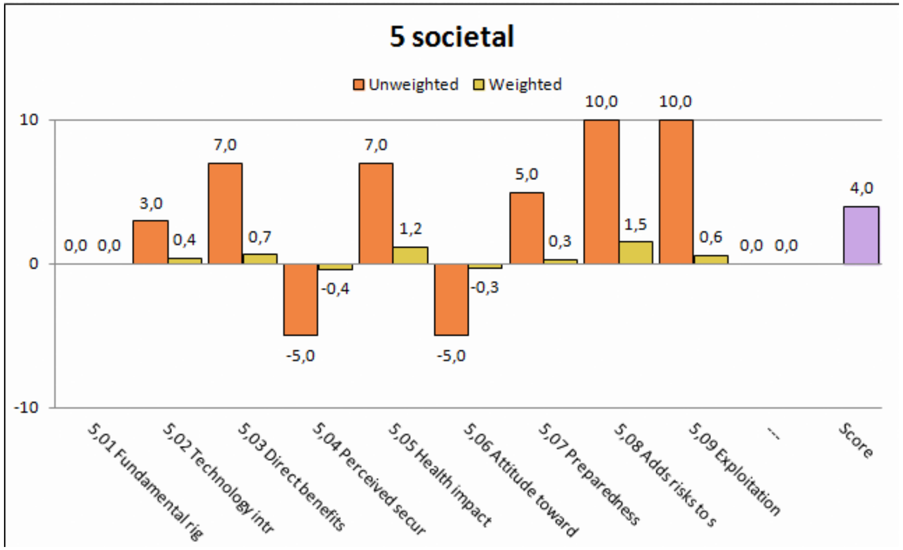
A large number of *Qualitative Criteria* identified, categorized and evaluated (*EELPS*)

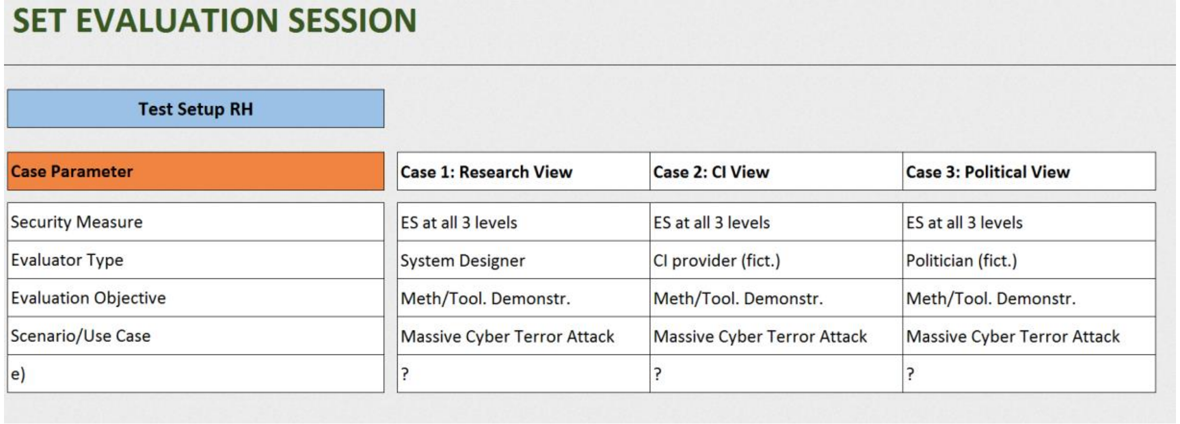
- ***E****thical values:* Privacy, personal freedom, protection of personal data
- ***E****conomic* “Intang.”: Reputation; competition; collaboration; …
- ***L****egal & regulatory:* restrictions from/to fundamental & other rights; compliance with (inter)national rules of law, …
- ***P****olitical factors:* influence on political reputation; strong dependence on neighboring states; compliance with national and EU security strategies, …
- ***S****ocietal values:* human rights, cohesion, fairness & equality, environment



CHECK, ELIMINATE AND INSERT MAIN CATEGORIES AND QUALITATIVE CRITERIA

ID	Categories and qualitative criterion	Evaluate	Description, comments, supporting material
1	**Ethical**	Yes	Possible impact of an ES on ethical values
	# of Criterions 10		
1,01	Change of soc. Values	Yes	Could the SM potentially positively or negatively change societal values?
1,02	Privacy	Yes	Do security measures respect private and family life, home and correspondence, ensure or enc
1,03	Equality&dicrim.	Yes	Does the SM support equal treatment or rather prefer certain groups or individuals?
1,04	Confidentiality	Yes	Does the SM protect or endanger personal information (e.g. medical; consumer)
1,05	Trust	Yes	Does the measure enhance trust in institutions, infrastructure, or does it decrease trust?
1,06	Control of citizens	Yes	Will citizens be more controlled by the SM or will they be less controlled because of the SM?
1,07	Organizational grouping	Yes	Can the measure lead to formation and action of special societal groups and initiatives (positive and/or negative)?
1,08	Integrity	Yes	Is the integrity of the decision maker on the SM verified?
1,09	Truthfulness	Yes	Is the SM a response to a real risk or only/partially pretending it? Is it supposed to follow hidden agendas?
1,10	Transparency of the system	Yes	Are the procedures of the SM transparent to society or are they camouflaged or hidden?
2	**Economic**	Yes	Possible impact on non-quantifiable economic parameters
	# of Criterions 10		
2,01	Economic stability	Yes	Does the measure influence economic stabilities (positive and/or negative)?
2,02	Compensation of side effects	Yes	Can (unwanted) side effects be controlled, tolerated or compensated (e.g. via insurance)
2,03	Cost-benefit	Yes	Is the economic benefit of the SM vs. cost clear/ transparent?
2,04	Economic beneficience	Yes	Who benefits from the SM? Does the SM confer benefits on some groups but not on others?
2,05	Validation	Yes	Does the introduction of the SM foresee measurement and evaluation of the SM's effectiveness and benefits
2,06	Environment	Yes	Does the SM have significant (pos./neg.) impact on environmental factors?
2,07	Cooperation	Yes	Will the SM support or block/hamper cooperation among stakeholders, nations, with international bodies
2,08	Market	Yes	Does the SM support/increase/decrease market advantage?
2,09	Dependency on "foreign" sectors (FS)	Yes	Will the SM require involvement of "other" sectors (e.g. private security org's., foreign org's)?
2,10	Dependency on technology	Yes	Is the measure dependent on "foreign technology"; how critical?
3	**Legal**	Yes	Legal complianc or incompliance
	# of Criterions 5		
3,01	Legal conformity/compliance	Yes	Doe the SM follow existing (e.g.national) regulations and rule of law
3,02	International compliance	Yes	Does the measure comply with international guidelines, treaties, regulations etc.?
3,03	Justice	Yes	Is there a fair and just system for addressing SM failure with appropriate compensation to affected Stakeholders?





SET EVALUATION SESSION

Test Setup RH

Case Parameter	**Case 1: Research View**	**Case 2: CI View**	**Case 3: Political View**
Security Measure	ES at all 3 levels	ES at all 3 levels	ES at all 3 levels
Evaluator Type	System Designer	CI provider (fict.)	Politician (fict.)
Evaluation Objective	Meth/Tool. Demonstr.	Meth/Tool. Demonstr.	Meth/Tool. Demonstr.
Scenario/Use Case	Massive Cyber Terror Attack	Massive Cyber Terror Attack	Massive Cyber Terror Attack
e)	?	?	?

PPP Main challenges and Opportunities

- Overall, the success of future ECOSSIAN implementations **should not be taken for granted**. D7.9 / D7.10 have identified significant capability and capacity gaps.
- Furthermore, the **European political, security, and defence** context has changed in fundamental ways, since the inception of the ECOSSIAN Project.
- **United Kingdom**: a new context for communication, cooperation, and coordination.
- Much work needs to be done regarding culture, ethics, behaviour, principles, and policies. **Solidarity** is key (EU Principle).
- However, the **value and urgency** of ECOSSIAN-like systems has increased:
    - **Hybrid threats** are on the rise;
    - **EU-NATO Joint Declaration** opens new possibilities for enhancing and integrating situational awareness and early warning capabilities

PPP main guidelines

- Public-Private Partnerships (PPPs) **<u>are essential features and enablers</u>** for future successful ECOSSIAN system implementations.
- The proposed PPP models and recommendations take a **<u>holistic</u>** approach, covering 7 points-of-view:
  - Principles, Policies, and Frameworks
  - Processes
  - Organizational Structures
  - Culture, Ethics, and Behaviour
  - Information
  - Services, Infrastructure, and Applications
  - People, Skills, and Competencies
- The recommendations are based on widely accepted **<u>standards and industry best practice</u>**, to promote interoperability and widespread adoption.

European Control System Security Incident Analysis Network

ECOSSIAN

Operational demonstration

Elancourt, April 26th 2017

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607577.

Overall scenario presentation:

Pan European detection and management of incidents and attacks on European Critical Infrastructures

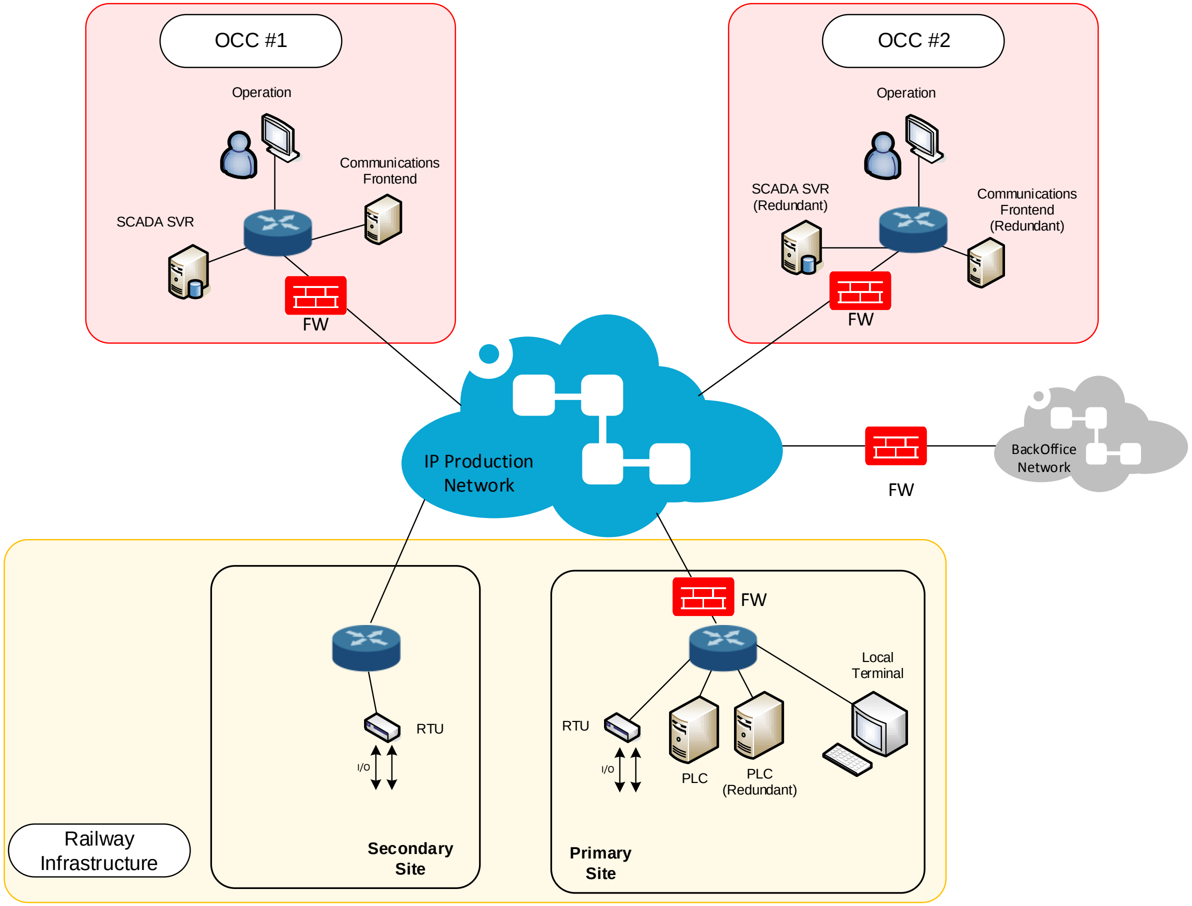
Elancourt, April 26th 2017

European Control System Security Incident Analysis Network

Background – SCADA System

- The SCADA system allows supervision and control of several railway systems in real-time and in a centralized manner:
    - One system will be demo;
    - The operation of the Electric Grid, power lines and sub-station, which powers the train traction.
- Based on a distributed architecture with three different levels:
    - Remote Terminal Unit (RTU);
    - Programmable Logic Controller (PLC)
    - Application (SCADA Servers).

Background – SCADA System



Objectives and demonstration flow

- **Objective:**
  - **Detection of a cyber-attack on the Portuguese railway system.**
- Demonstration flow:
  - Phase 1: Attack on the Critical Infrastructure of the Railway sector
  - Phase 2: Detection of the attack
  - Phase 3: Incident response and mitigation at O-SOC level
  - Phase 4: Incident response and mitigation at Portuguese N-SOC level
  - Phase 5: Situation awareness and alerting capabilities at E-SOC level
- Relevance
  - Address incidents and events that match current threats that pose a real danger to industrial networks

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607577.

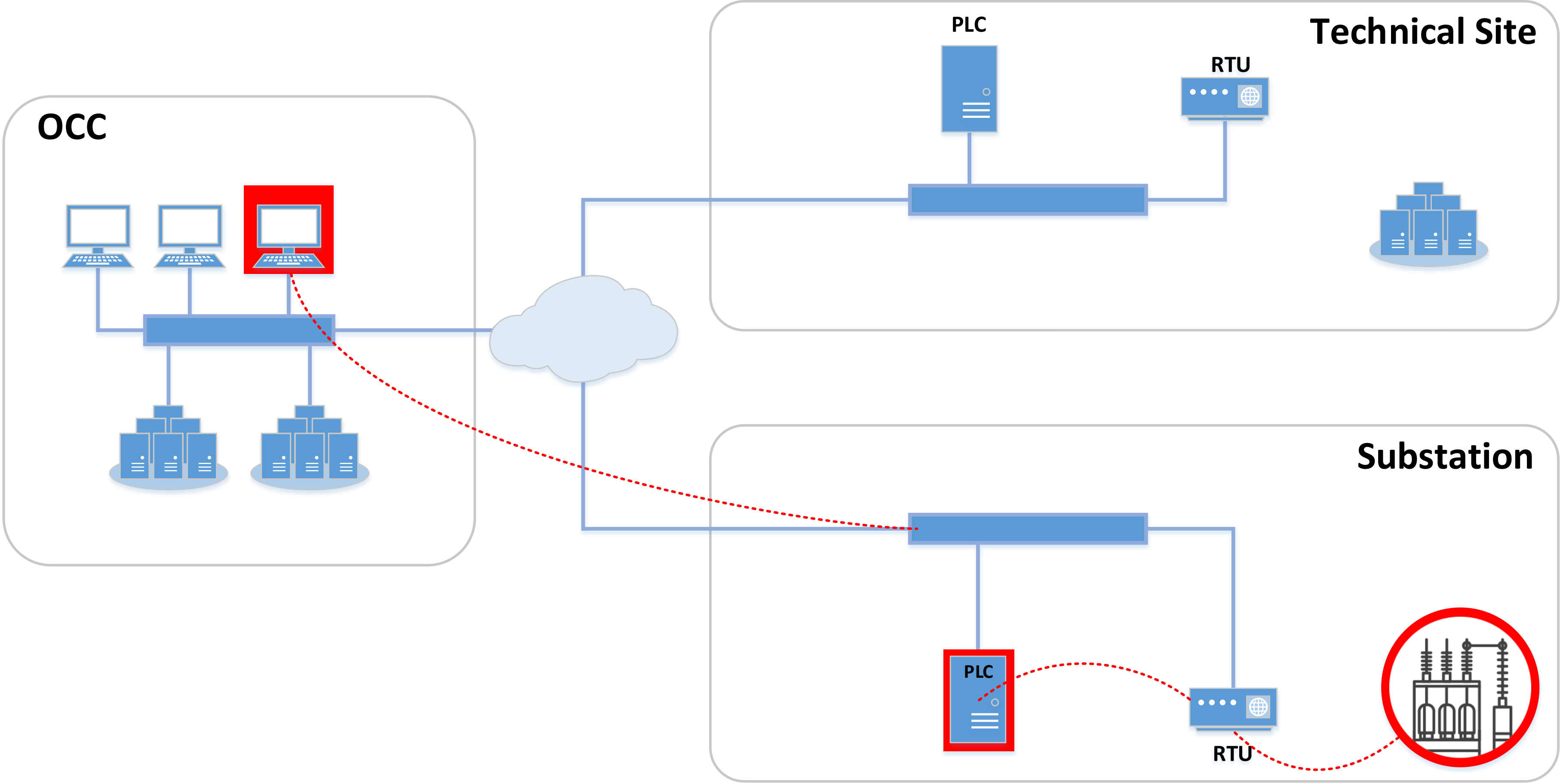
Operational demonstration

Phase 1: Attack

Introduction

- **Goal: Execution of SCADA commands at the local level without being perceived by the OCC**
- **Target: Railway SCADA Systems - Train Energy Control**
- **Methodology:**
  - **Compromise of the SCADA host (PLC), not shown in the demo;**
  - **Execution of commands (Opening of circuit breakers);**
  - **Discard of Logs sent to OCC.**
- **Detection:**
  - **Process verification of the execution of SCADA commands (BPIDS)**

Attack Scenario



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607577.

Operational demonstration

Phase 2: Detection

Introduction

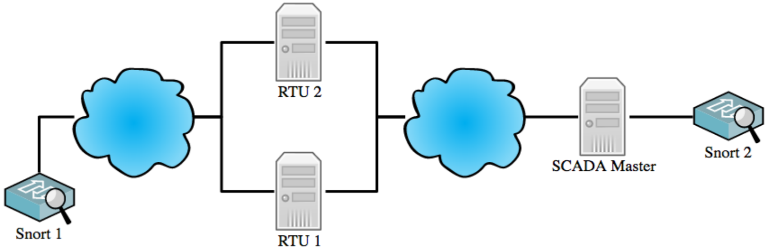
- **Detection of the attack by the BPIDS sensor.**
  - The network is monitored by ECOSSIAN sensors that **detect isolated and uncorrelated “evidences”** related to the running attack.
  - These evidences **reveal traces left behind by sophisticated techniques** adopted by the attacker.

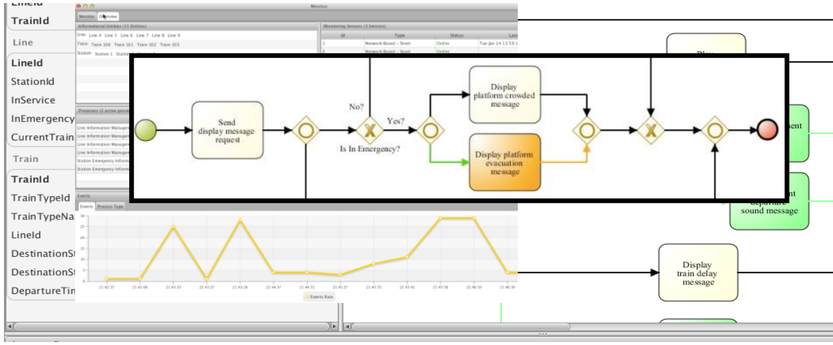
- O-SOC Operator
  - **Supervision** of the security issues of the company’s IT.
  - **Real-time view** on the cyber security state of the controlled network and processes.

BPIDS

Business process specification-based intrusion detection system :

- Detects deviations from specification of monitored critical processes:
  - Input: Real time raw data captured directly from passive network sensors or logs. The events are mapped into process activities.
  - Output: Detected deviations providing:
    - Contextual information regarding the business process where the deviation was detected (Systems involved, previous process history, expected process activities, etc.)




TrainId
Line
LineId
StationId
InService
InEmergency
CurrentTrain
Train
TrainId
TrainTypeId
TrainTypeNa
LineId
DestinationSt
DestinationSt
DepartureTin
Monitor
Overview
Informational Entities (13 Entities)
Monitoring Sensors (3 Sensors)
Processes (2 active processes)
Events
Process Type
Events Rate
Send display message request
No?
Yes?
Is In Emergency?
Display platform crowded message
Display platform evacuation message
Display train delay message
sound message

Operational demonstration

Phase 3: Incident response and mitigation at O-SOC level

This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607577.

European Control System Security Incident Analysis Network

O-SOC level: supervision

SIEM (OSSIM or others)

- Open source Security Information and Event Management System
- **Aggregation** and **Correlation** of **Sensor Events**

O-SOC Cymerius

- **Situational awareness** solution used within a SOC
- Incident view linked with a **business impact evaluation**
- Situation overview along with **mitigation actions** specifically adapted to cyber incidents

ECOSSIAN capabilities

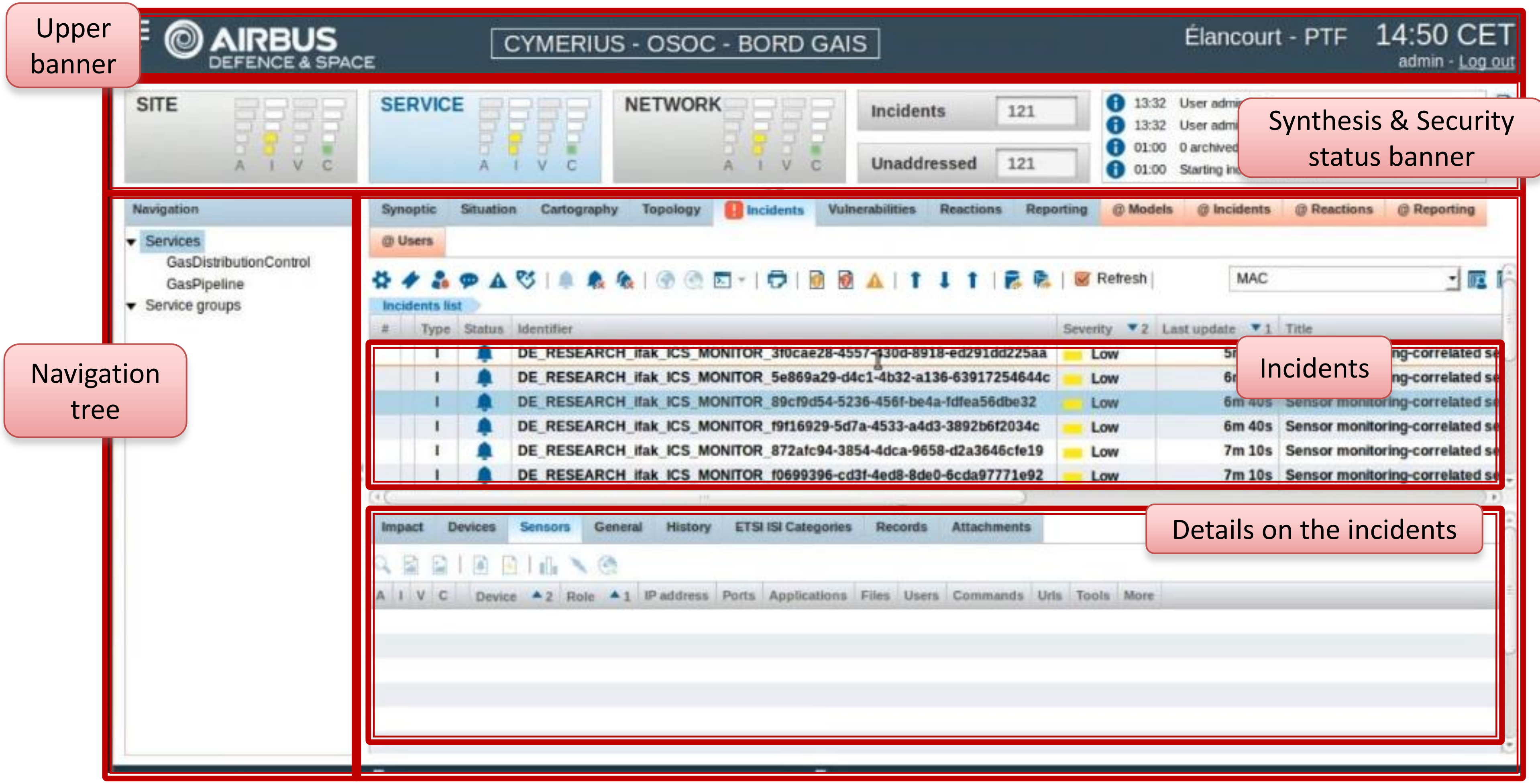
- **Supervision** of the cyber-security state of the **monitored infrastructure**.
- Capacity to supervise incidents in a centralized and user-friendly way.
- **Inter-operability with many different SIEM** solutions (like OSSIM in this case).

Actions

- **Investigation, incident response and mitigation:**
  1. Incident supervision and analysis (O-SOC level)
  2. Reaction plan for network and SCADA teams
  3. Information sharing towards N-SOC

- O-SOC operator

Cymerius – Incident supervision



Upper banner

Synthesis & Security status banner

Navigation tree

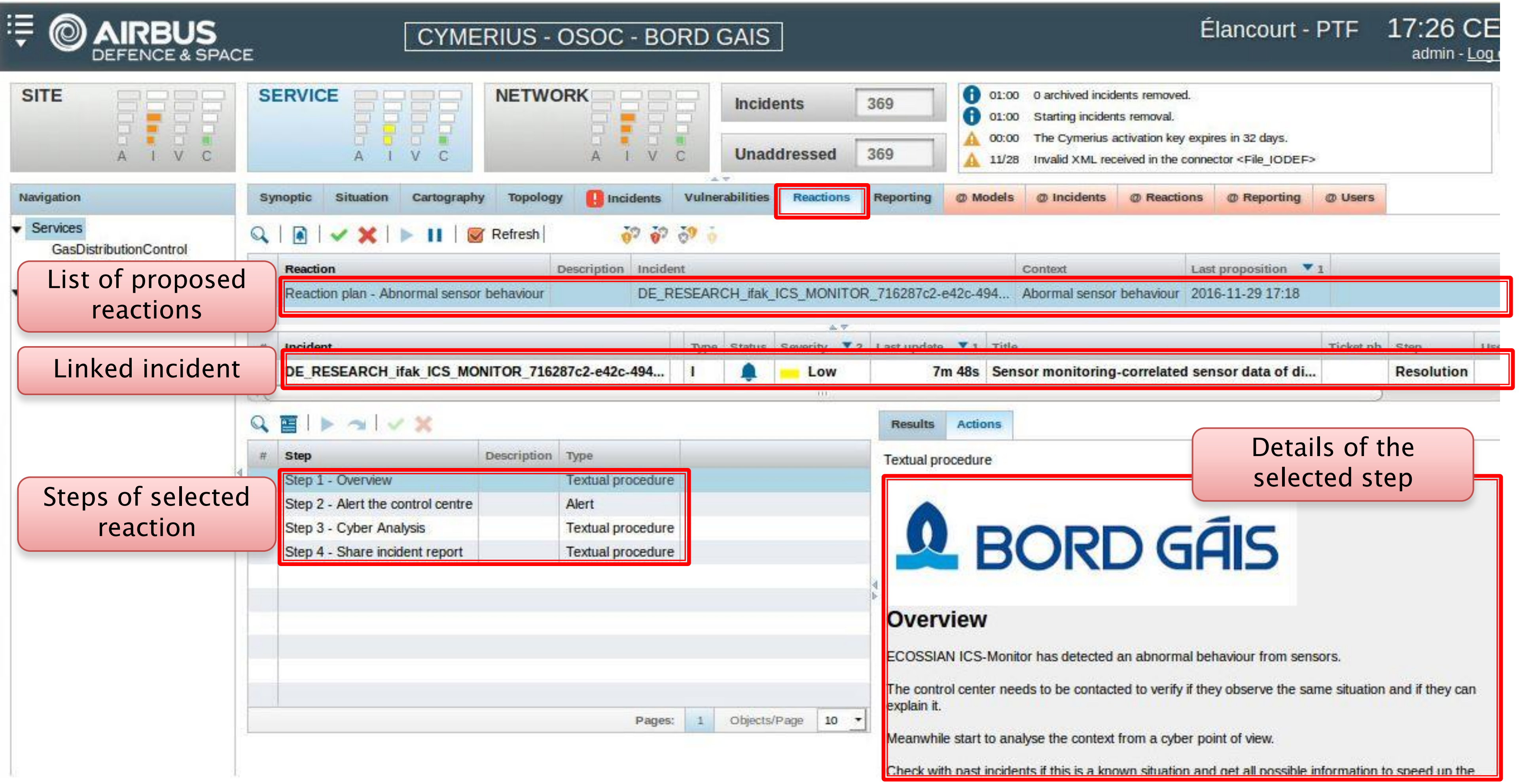
Incidents

Details on the incidents

13:32 User admi
13:32 User admi
01:00 0 archived
01:00 Starting in

#	Type	Status	Identifier	Severity ▼2	Last update ▼1	Title
	I	🔔	DE_RESEARCH_ifak_ICS_MONITOR_3f0cae28-4557-430d-8918-ed291dd225aa	Low	5r	ng-correlated se
	I	🔔	DE_RESEARCH_ifak_ICS_MONITOR_5e869a29-d4c1-4b32-a136-63917254644c	Low	6r	ng-correlated se
	I	🔔	DE_RESEARCH_ifak_ICS_MONITOR_89cf9d54-5236-456f-be4a-fdfea56dbe32	Low	6m 40s	Sensor monitoring-correlated se
	I	🔔	DE_RESEARCH_ifak_ICS_MONITOR_f9f16929-5d7a-4533-a4d3-3892b6f2034c	Low	6m 40s	Sensor monitoring-correlated se
	I	🔔	DE_RESEARCH_ifak_ICS_MONITOR_872afc94-3854-4dca-9658-d2a3646cfe19	Low	7m 10s	Sensor monitoring-correlated se
	I	🔔	DE_RESEARCH_ifak_ICS_MONITOR_f0699396-cd3f-4ed8-8de0-6cda97771e92	Low	7m 10s	Sensor monitoring-correlated se

Cymerius – Reaction plan



Incidents	369
Unaddressed	369

ℹ	01:00	0 archived incidents removed.
ℹ	01:00	Starting incidents removal.
⚠	00:00	The Cymerius activation key expires in 32 days.
⚠	11/28	Invalid XML received in the connector <File_IODEF>

Reaction	Description	Incident	Context	Last proposition ▼ 1
Reaction plan - Abnormal sensor behaviour		DE_RESEARCH_ifak_ICS_MONITOR_716287c2-e42c-494...	Abormal sensor behaviour	2016-11-29 17:18

Incident	Type	Status	Severity ▼ 2	Last update ▼ 1	Title	Ticket nb	Step
DE_RESEARCH_ifak_ICS_MONITOR_716287c2-e42c-494...	I	🔔	Low	7m 48s	Sensor monitoring-correlated sensor data of di...		Resolution

#	Step	Description	Type
	Step 1 - Overview		Textual procedure
	Step 2 - Alert the control centre		Alert
	Step 3 - Cyber Analysis		Textual procedure
	Step 4 - Share incident report		Textual procedure

Textual procedure

BORD GÁIS

Overview

ECOSSIAN ICS-Monitor has detected an abnormal behaviour from sensors.

The control center needs to be contacted to verify if they observe the same situation and if they can explain it.

Meanwhile start to analyse the context from a cyber point of view.

Check with past incidents if this is a known situation and get all possible information to speed up the

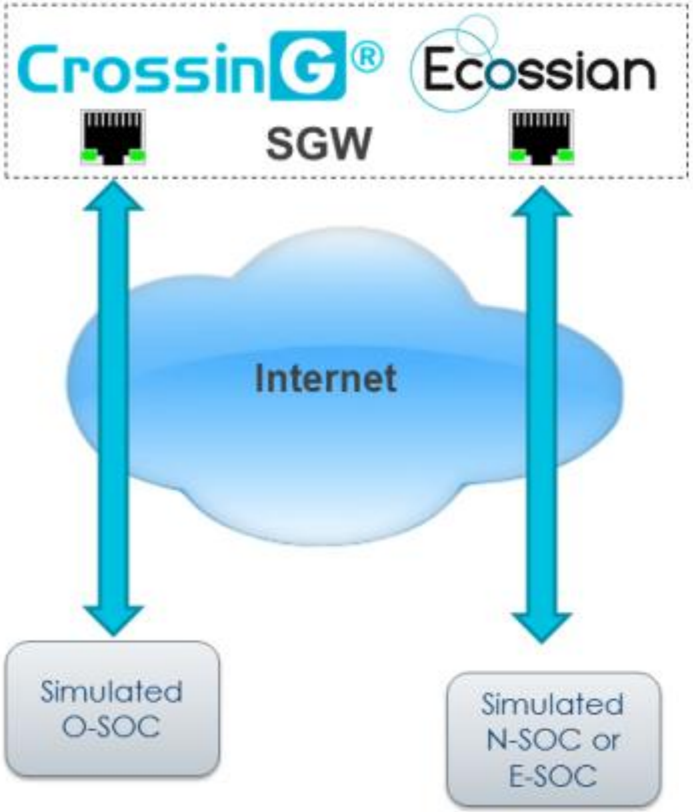
List of proposed reactions

Linked incident

Steps of selected reaction

Details of the selected step

O-SOC to N-SOC: incident forwarding



Secure Gateway

- Encapsulator interface
- Unidirectional information channel
- Virus and malware verification
- Security label verification
- Security event logging
- Anonymization by the Encapsulator module
- Every message going out of the SOC shall be **approved by a SOC Manager**.

Information sharing

- **Cryptographic Access Control**: design of mechanisms for providing **confidentiality** of shared information

Attribute-Based-Encryption

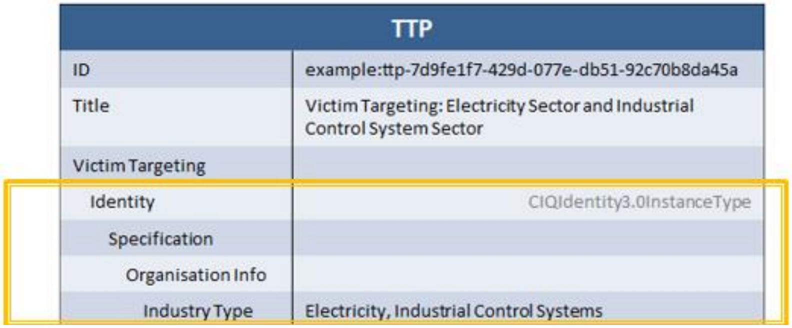
Attributes Definition

Attribute Type	Possible Values
SOC–Level	OSOC, NSOC, ESOC
Country	AT, DE, ES, FR, GB, IE, NL, PT, …
SOC Sector	Chemical, Dams, Defense, Emergency_Services, Financial_Services, Government_Facilities, Healthcare_and_Public Health, Information_Technology, Nuclear, Transportation_Systems, Water_and_Wastewater_Systems, etc.
TLP	TLP–Red, TLP–Amber, TLP–Green

Access Policies Formulation

Policy: ((“OSOC” AND “GB” AND “Health”) OR (“TLP-Red”))

Partial Message Encryption



TTP	
ID	example:ttp-7d9fe1f7-429d-077e-db51-92c70b8da45a
Title	Victim Targeting: Electricity Sector and Industrial Control System Sector
Victim Targeting	
Identity	CIQIdentity3.0InstanceType
Specification	
Organisation Info	
Industry Type	Electricity, Industrial Control Systems

Policy: E-SOC, Electricity, ICS

Operational demonstration

Phase 4: Incident response and mitigation at N-SOC level

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607577.

Introduction

- **Investigation, incident response and mitigation:**
  1. Forensics analysis
  2. National collaboration and support for solving the incident
  3. National situation awareness (warnings)
  4. National preparedness (detection and mitigation feedback sharing)

- O-SOC operator
- N-SOC Operator
  - High-level information from O-SOCs
  - **Situational awareness** and view on the **nation’s critical infrastructures**
  - **Nation-wide forensics analysis**

N-SOC level: National support & analysis

Acquisition Module

- Data collection from the O-SOCs and public external sources

N-SOC Cymerius

- Update incident with CAESAIR Analysis and recommendations (from N-SOC operator)

CAESAIR

- **Correlation/analysis engine** for situational awareness and incident response
- Designed for the **deeper investigation of incident reports**
- Automated **import of external security sources** (CVE, TI) to build up a **body of knowledge**
- Automatically **discovers related resources** and supports **human's in validating findings**

ECOSSIAN capabilities

- **National support :** Collaboration and support at national level to help the SOC at Operator level solving the incidents they are facing.
- **Analysis tools:** CAESAIR

Acquisition Module

Collects data reported by the O-SOCs, and acquired from public external sources, temporarily stores it, and makes it available to the analysis components.

Compliant with the most widely adopted data formats and protocols for cyber incident and threat information description and exchange.

SECLISTS.ORG

CVE COMPATIBLE cve.mitre.org

STIX™

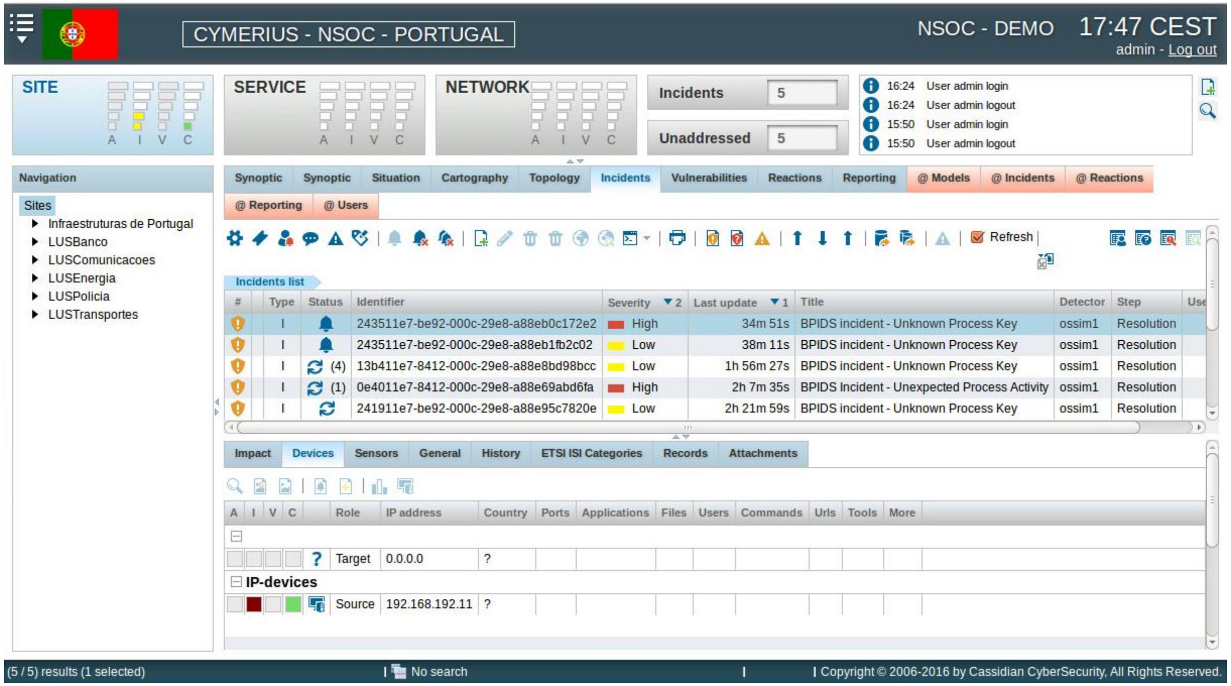
IODEF RFC 5070 INCIDENT OBJECT DEFINITION EXCHANGE FORMAT

TAXII™

{JSON}

CPE™ common platform enumeration

N-SOC Cymerius



CYMERIUS - NSOC - PORTUGAL

NSOC - DEMO 17:47 CEST

admin - Log out

Incidents 5

Unaddressed 5

16:24 User admin login
16:24 User admin logout
15:50 User admin login
15:50 User admin logout

#		Type	Status	Identifier	Severity ▼2	Last update ▼1	Title	Detector	Step	Use
		I		243511e7-be92-000c-29e8-a88eb0c172e2	🟥 High	34m 51s	BPIDS incident - Unknown Process Key	ossim1	Resolution	
		I		243511e7-be92-000c-29e8-a88eb1fb2c02	🟨 Low	38m 11s	BPIDS incident - Unknown Process Key	ossim1	Resolution	
		I	(4)	13b411e7-8412-000c-29e8-a88e8bd98bcc	🟨 Low	1h 56m 27s	BPIDS incident - Unknown Process Key	ossim1	Resolution	
		I	(1)	0e4011e7-8412-000c-29e8-a88e69abd6fa	🟥 High	2h 7m 35s	BPIDS Incident - Unexpected Process Activity	ossim1	Resolution	
		I		241911e7-be92-000c-29e8-a88e95c7820e	🟨 Low	2h 21m 59s	BPIDS incident - Unknown Process Key	ossim1	Resolution	

A	I	V	C		Role	IP address	Country	Ports	Applications	Files	Users	Commands	Urls	Tools	More
⊟															
				?	Target	0.0.0.0	?								
⊟ IP-devices															
	🟥		🟩		Source	192.168.192.11	?								

(5 / 5) results (1 selected) | No search | Copyright © 2006-2016 by Cassidian CyberSecurity, All Rights Reserved.

ECOSSIAN capabilities

- **Gathers incidents reported by the OSOC and evaluate the cyber security status per CI**

Cymerius **orchestrates** the incident management

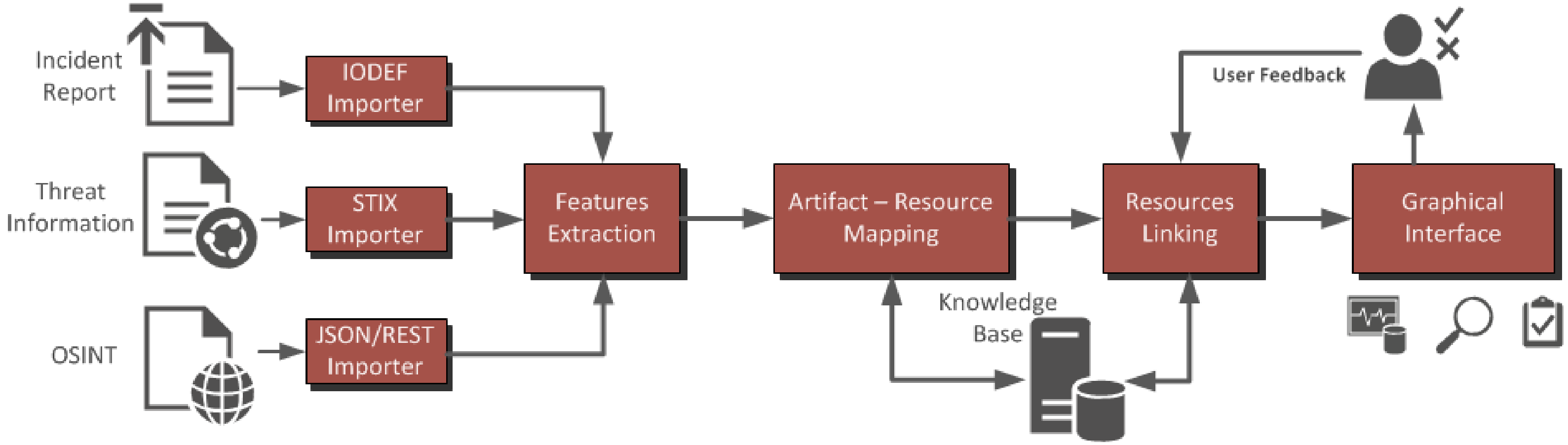
- **Integrates AM** to get incidents reported by OSOCs

- **Integrates CAESAIR** both ways (analysis request and results)

- **Integrates the SGW** to share incident reports to both OSOCs and the ESOC

CÆSAIR

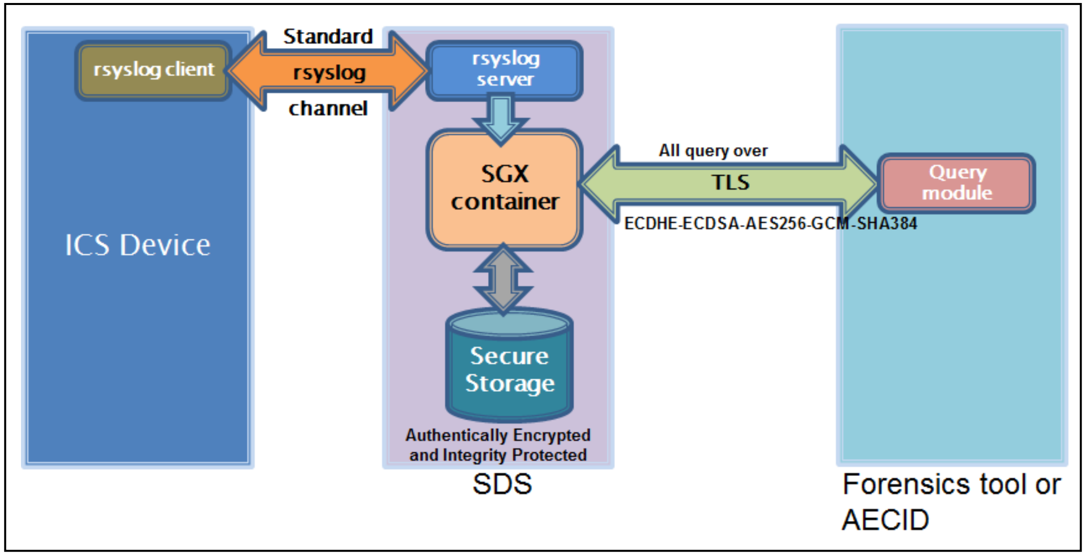
- Design and development of **CAESAIR**: a collaborative analysis engine for situational awareness and incident response
  - Designed for the **deeper investigation of incident reports** not handled by Cymerius
  - Automated import of external security sources (CVE, TI) to build up a **body of knowledge**
  - Automatically **discovers related resources** and harnesses the **human's capabilities to validate findings**
  - Application in ECOSSIAN:
    - Supports the N-SOC human operator in advanced incident analysis tasks,
    - Compliant with several data types (STIX threats, IODEF incidents, CVEs & CPEs, etc.)
    - Handles ~100k incidents and reports
    - Performs (near) real-time Resource linking (correlation)



Forensics and logging

- Once an event is registered by ECOSSIAN at any of the O-SOC, N-SOC or E-SOC layers:
  - The Secure Data Storage Stores data in a forensically sound manner.
    - The event can then be interpreted and traced back to its origin,
    - Making it possible to understand “who did what, where and when”.

- Log server integrated with Intel SGX secure container.
- Query functionality to get specific logs from the storage.



Mitigation & feedback sharing (lesson learned)

Mitigation

- The NSOC operator sends the incident report along with the NSOC analysis report
- The O-SOC operator **updates the incident report with complementary information** on how the incident was open, analysed and closed.

Detection and mitigation feedback sharing

- **Sharing of feedback information on detection and mitigation procedures at national and European levels**.

ECOSSIAN capabilities

- **National support:** Collaboration and support at national level to help the SOC at Operator level solving the incidents they are facing.
- **Preparedness of Critical Infrastructures and SOC Operators in Portugal and in Europe.**

N-SOC warnings: National & European awareness

ECOSSIAN capabilities

▪Situational awareness at National & European levels

- **Warnings sharing:** warnings issued by the O-SOC are forwarded to the SOCs at national and European levels
- **Threat information sharing:** broadcast by the N-SOC to the **other critical infrastructures** that could suffer from the same kind of attack.
- **Secure communication (Secure Gateway)**
- **Encryption capabilities (Attribute-Based Encryption)**

Operational demonstration

Phase 5: Situation awareness and alerting capabilities at E-SOC level

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607577.

E-SOC level: European Situation Awareness and Alerting

Interdependency Model

- Support situational awareness and find out interdependencies
- CIs dependant of the service of the disturbed CI

E-SOC Cymerius Portal

- European Situation Awareness: Maps and dashboards

SEC (Simple Event Correlator)

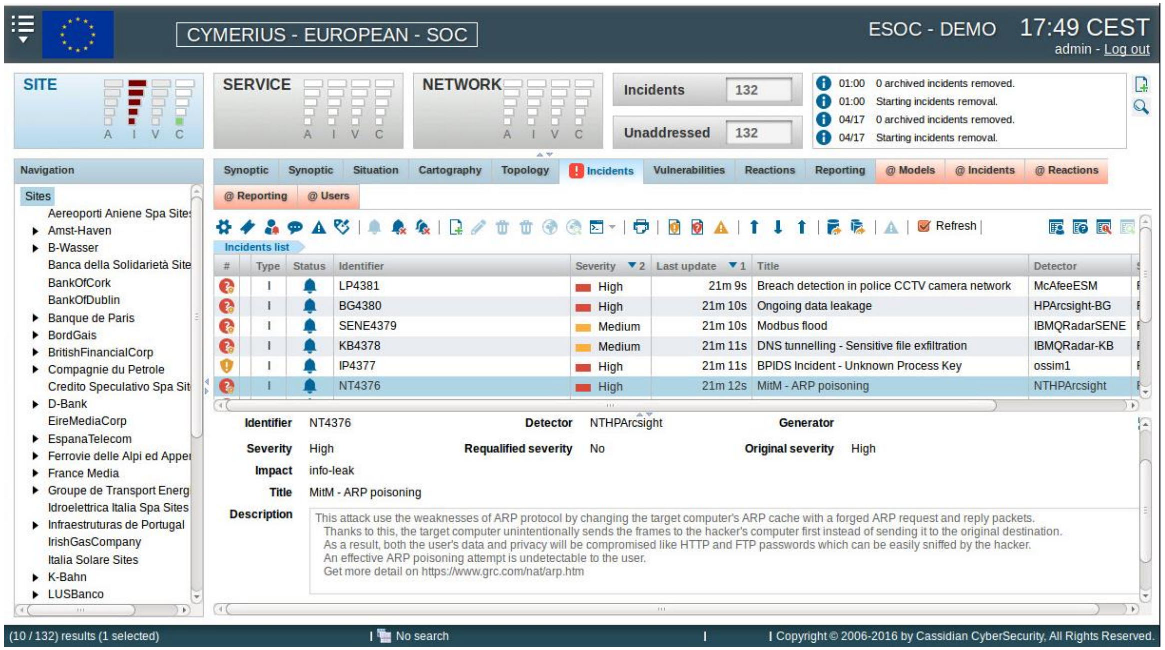
- Correlated situations

SGW and Cymerius

ECOSSIAN capabilities

- **European Situation awareness**
- **Alerting and preparedness at European level:** alerting of the Irish N-SOC

ESOC Cymerius



Incidents	132
Unaddressed	132

01:00	0 archived incidents removed.
01:00	Starting incidents removal.
04/17	0 archived incidents removed.
04/17	Starting incidents removal.

Aereoporti Aniene Spa Sites
Amst-Haven
B-Wasser
Banca della Solidarietà Site
BankOfCork
BankOfDublin
Banque de Paris
BordGais
BritishFinancialCorp
Compagnie du Petrole
Credito Speculativo Spa Sit
D-Bank
EireMediaCorp
EspanaTelecom
Ferrovie delle Alpi ed Apper
France Media
Groupe de Transport Energ
Idroelettrica Italia Spa Sites
Infraestruturas de Portugal
IrishGasCompany
Italia Solare Sites
K-Bahn
LUSBanco

#	Type	Status	Identifier	Severity ▼2	Last update ▼1	Title	Detector
	I	🔔	LP4381	🟥 High	21m 9s	Breach detection in police CCTV camera network	McAfeeESM
	I	🔔	BG4380	🟥 High	21m 10s	Ongoing data leakage	HPArcsight-BG
	I	🔔	SENE4379	🟧 Medium	21m 10s	Modbus flood	IBMQRadarSENE
	I	🔔	KB4378	🟧 Medium	21m 11s	DNS tunnelling - Sensitive file exfiltration	IBMQRadar-KB
	I	🔔	IP4377	🟥 High	21m 11s	BPIDS Incident - Unknown Process Key	ossim1
	I	🔔	NT4376	🟥 High	21m 12s	MitM - ARP poisoning	NTHPArcsight

Identifier NT4376 **Detector** NTHPArcsight **Generator**

Severity High **Requalified severity** No **Original severity** High

Impact info-leak

Title MitM - ARP poisoning

Description This attack use the weaknesses of ARP protocol by changing the target computer's ARP cache with a forged ARP request and reply packets.
Thanks to this, the target computer unintentionally sends the frames to the hacker's computer first instead of sending it to the original destination.
As a result, both the user's data and privacy will be compromised like HTTP and FTP passwords which can be easily sniffed by the hacker.
An effective ARP poisoning attempt is undetectable to the user.
Get more detail on https://www.grc.com/nat/arp.htm

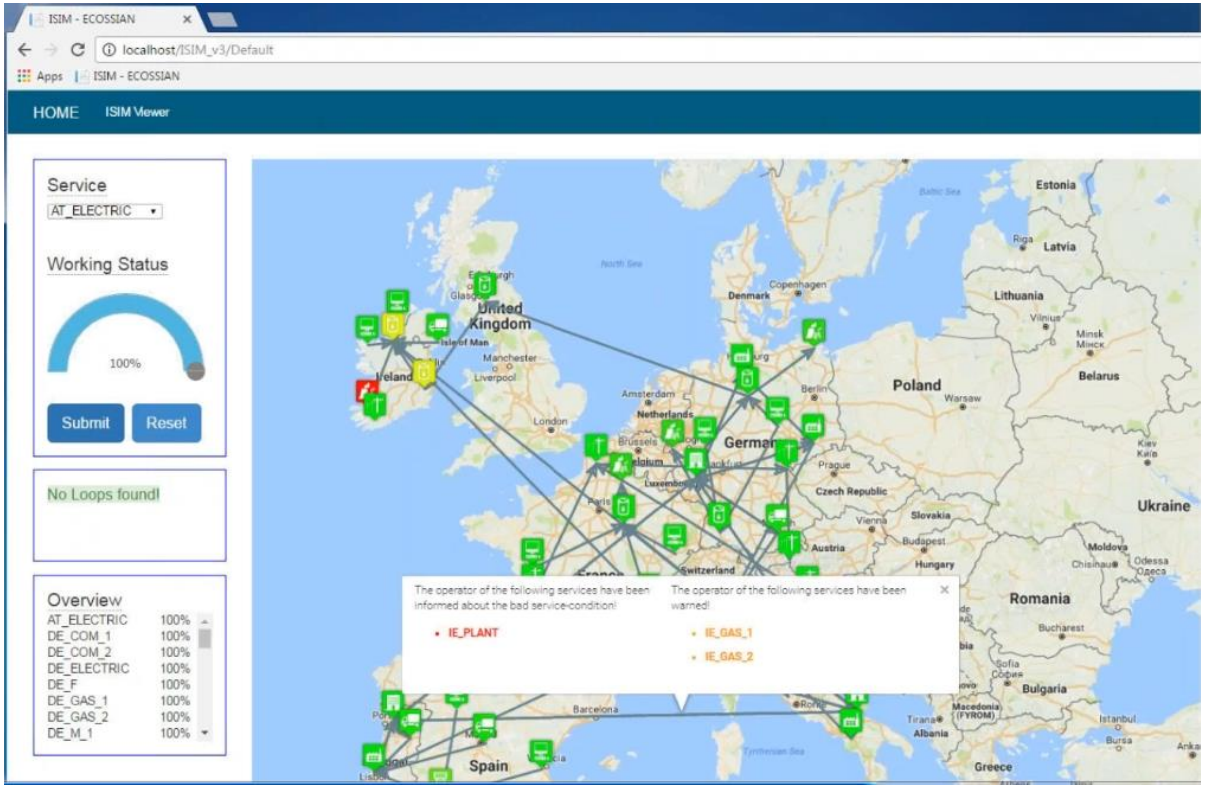
(10 / 132) results (1 selected) | No search | | Copyright © 2006-2016 by Cassidian CyberSecurity, All Rights Reserved.

ECOSSIAN capabilities

▪Gathers incidents reported by the NSOC and evaluate the cyber security status per CI.

Information is shared to the situation portal and SEC respectively to display a cyber picture and find some correlated situations

Interdependency Model



Service
AT_ELECTRIC

Working Status
100%

No Loops found!

Overview

AT_ELECTRIC	100%
DE_COM_1	100%
DE_COM_2	100%
DE_ELECTRIC	100%
DE_F	100%
DE_GAS_1	100%
DE_GAS_2	100%
DE_M_1	100%

The operator of the following services have been informed about the bad service-condition!

- IE_PLANT

The operator of the following services have been warned!

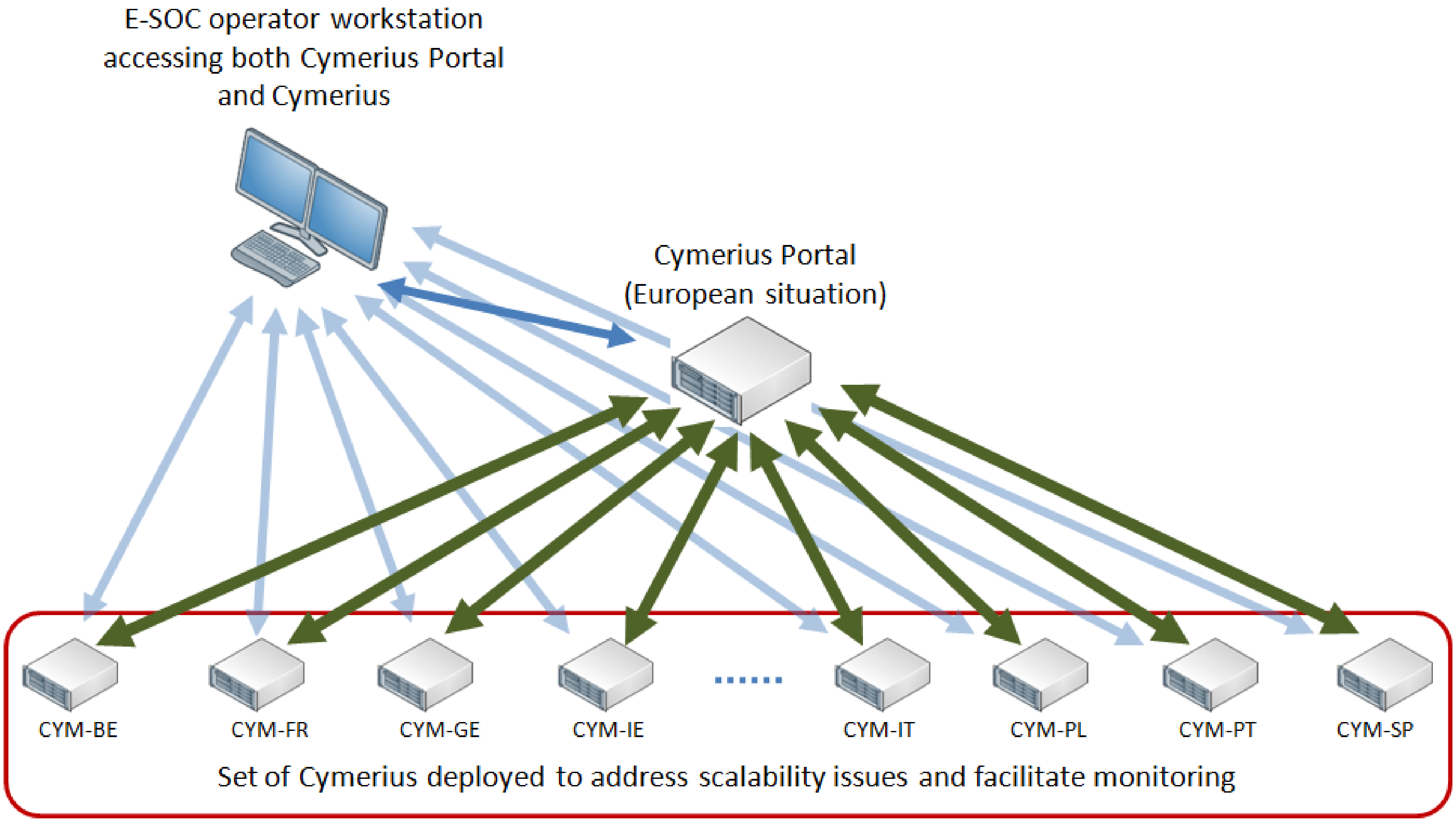
- IE_GAS_1
- IE_GAS_2

ECOSSIAN capabilities

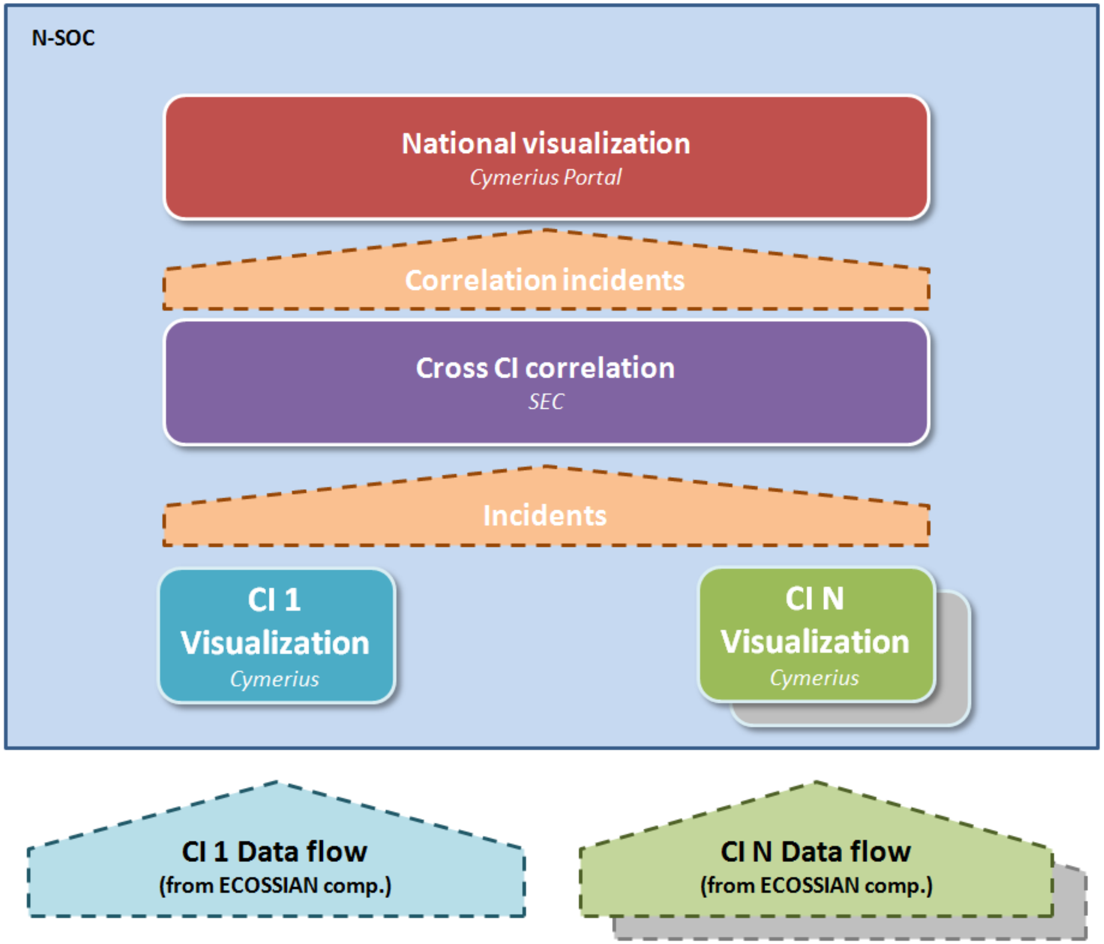
- **The Interdependency Model presents all CIs and their location in Europe. After the attack the model highlights all affected CIs and shows a list of immediately affected CIs and their availability.**

The information are sent to Cymerius and **integrated into the incident report** for a **comprehensive evaluation of the criticality of the incident**.

Cymerius Portal


E-SOC operator workstation accessing both Cymerius Portal and Cymerius
Cymerius Portal (European situation)
CYM-BE
CYM-FR
CYM-GE
CYM-IE
......
CYM-IT
CYM-PL
CYM-PT
CYM-SP
Set of Cymerius deployed to address scalability issues and facilitate monitoring

SEC – Correlated situations



N-SOC

National visualization
Cymerius Portal

Correlation incidents

Cross CI correlation
SEC

Incidents

CI 1 Visualization
Cymerius

CI N Visualization
Cymerius

CI 1 Data flow
(from ECOSSIAN comp.)

CI N Data flow
(from ECOSSIAN comp.)

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607577.

Operational demonstration

Conclusion

Conclusions (1/2)

A layered system architecture for a pan-European cooperative threat management, early-warning and situational awareness:

- Cross-country and cross-sectorial collaboration – providing a secure information sharing environment;
- Anonymity and privacy (confidentiality) preserving for all joining members – usage of attribute based encryption and anonymization techniques at the Secure Gateway;
- Secure information sharing and collaboration platform compliant to legal and other regulatory requirements – cryptography and privacy protecting mechanisms;
- Technologies and processes for monitoring and threat/incident detection and near-real-time detection of attacks – set of advanced sensors for detecting threats in ICS;

Conclusions (2/2)

- Data analysis, aggregation, correlation and visualization – tools at O and N level;
- Threat mitigation, impact analysis, interdependencies and incident management – recommendations on good practices;
- Evaluation of the regulatory, social and economic boundary conditions
- **Full-scale demonstration** of the integrated ECOSSIAN system on all levels (O-SOC, N-SOC, E-SOC):
  - 3 National demonstrations (O and N level)
    - **Ireland**
    - **Italy**
    - **Portugal**
  - **1 European wide demonstration in France (O, N and E level);**
- **Project ends on May 2017.**

Ecossian

This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607577.

Thank you for your attention

Questions?

European Control System Security Incident Analysis Network

ECOSSIAN FP7 PROJECT:

Questionnaire

This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607577.

European Control System Security Incident Analysis Network

Agenda

- Welcome
- Introduction of the ECOSSIAN project
  - Daniel Meister (Airbus Defence and Space GmbH)
- ECOSSIAN national demonstrations (Summary and Feedback)
  - **Italian Demonstration** - Early Warning System on Cyber-attacks targeting Critical Financial Infrastructures: Cécile Abdo (Airbus Cybersecurity)
  - **Irish Demonstration** - Detection of Attack on Gas Provider: Paul Gaynor (Gas Networks Ireland)
  - **Portuguese Demonstration** - Support for Forensic Analysis of Attack on Transportation Infrastructure: José Carlos Gonçalves (Serviços de Telecomunicações, S. A.)
- Legal, Ethical and Social aspects
  - Jessica Schroers (Katholieke Universiteit Leuven)
- Break
- Operational demonstration
- Q&A and evaluation
- **Cocktail & ECOSSIAN technology exhibition**