Ecossian

European Control
System Security
Incident Analysis
Network

Italian Demonstration

Roma 8 Novembre 2016

Posteitaliane

ECOSSIAN FP7 PROJECT:

Protection of Critical Financial Infrastructures against advanced Cyber-attacks

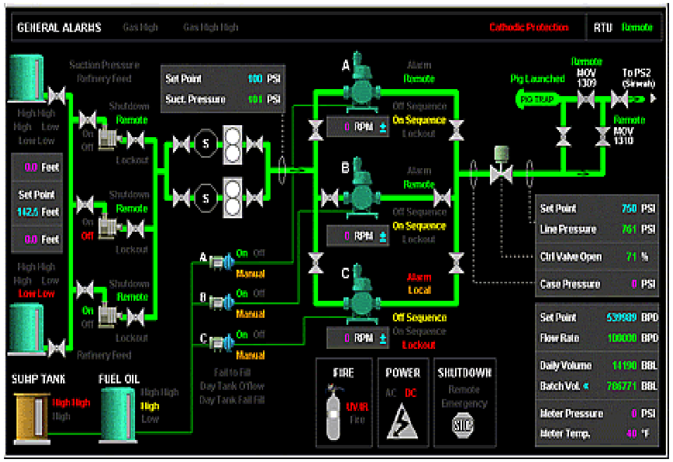
Poste Italiane, 8th November 2016

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

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 …



Set Point 100 PSI
Suct. Pressure 101 PSI

0.0 Feet
Set Point 142.5 Feet
0.0 Feet

0 RPM

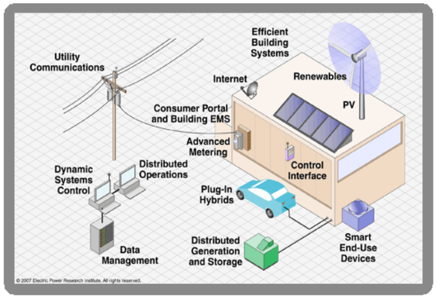
Set Point 750 PSI
Line Pressure 761 PSI
Ctrl Valve Open 71 %
Case Pressure 0 PSI

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

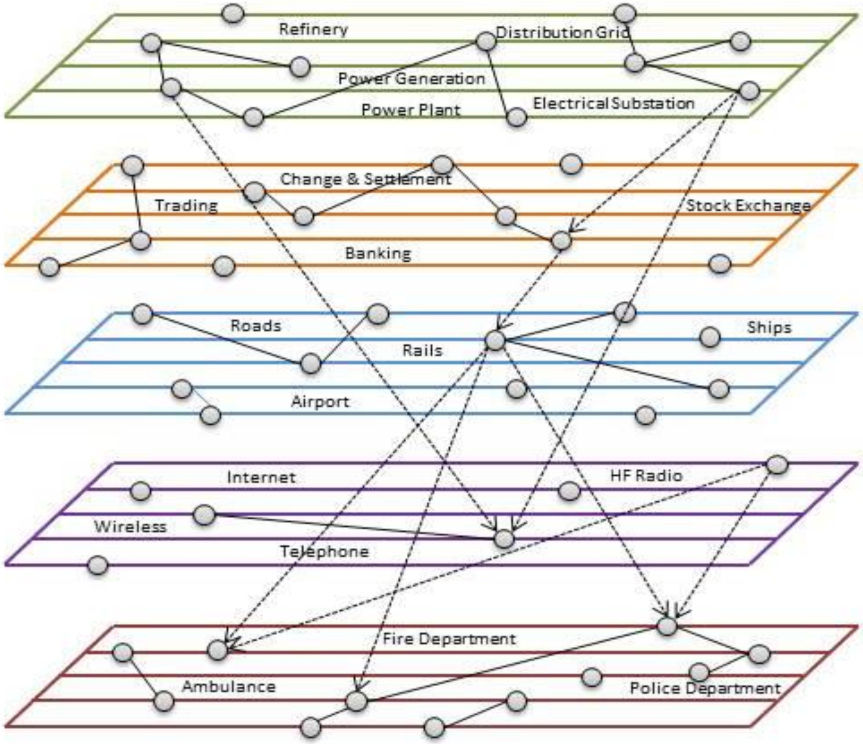
- Attack surface to critical infrastructures is continuously growing because:
  - **Deployment of COTS-products**
  - Change from proprietary protocols and products to common technologies coming from the pure IT world“
  - Losing the „Air-Gaps“ through convergence
  - **More and more use of mobile devices 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.



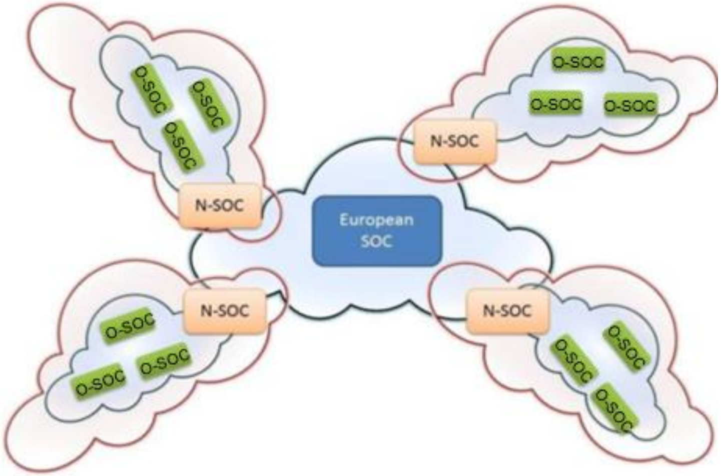
Motivation

- Interdependencies between critical infrastructure (CI)



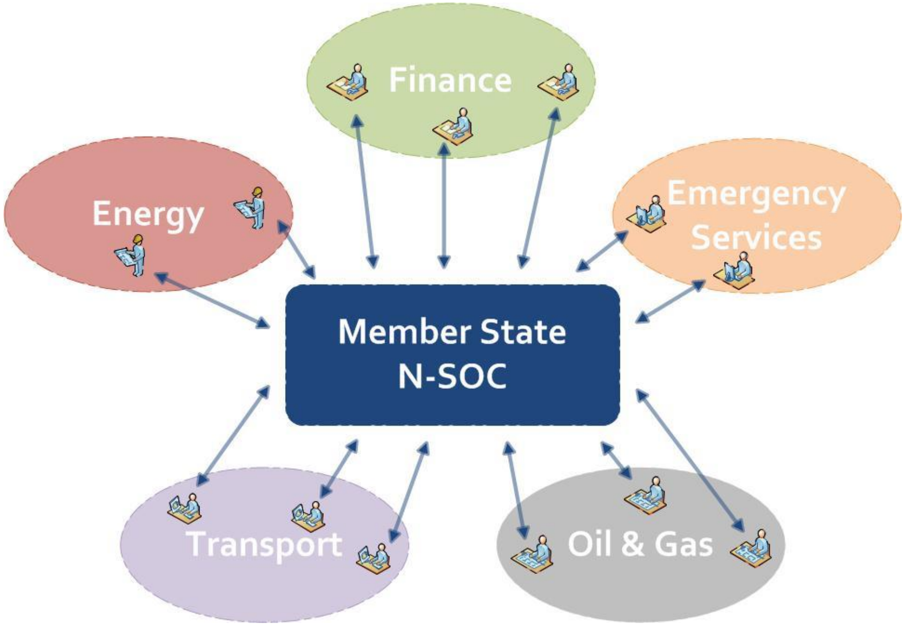
Project goals

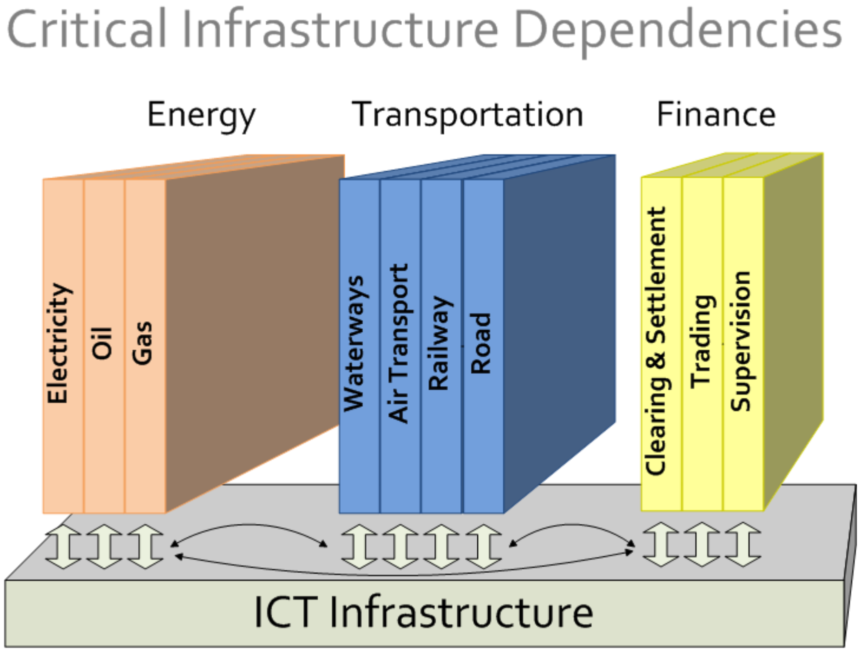
- Development of a cross-border European early warning system for critical infrastructures
- Three tiers of collaborative, interconnected Secure Operation Centres (SOCs)
  - **Local/sub-state SOC (O-SOC)**
    early detection and data collection with aggregation
  - **National SOC (N-SOC)**
    Situational Awareness using aggregated and correlated data
  - **Transnational SOC with command and control capabilities with inclusion of member state SOCs (E-SOC)**
    Transnational Situational Awareness and coordinated and consistent crisis management



Project goals

- Development of a cross-border European early warning system for critical infrastructures





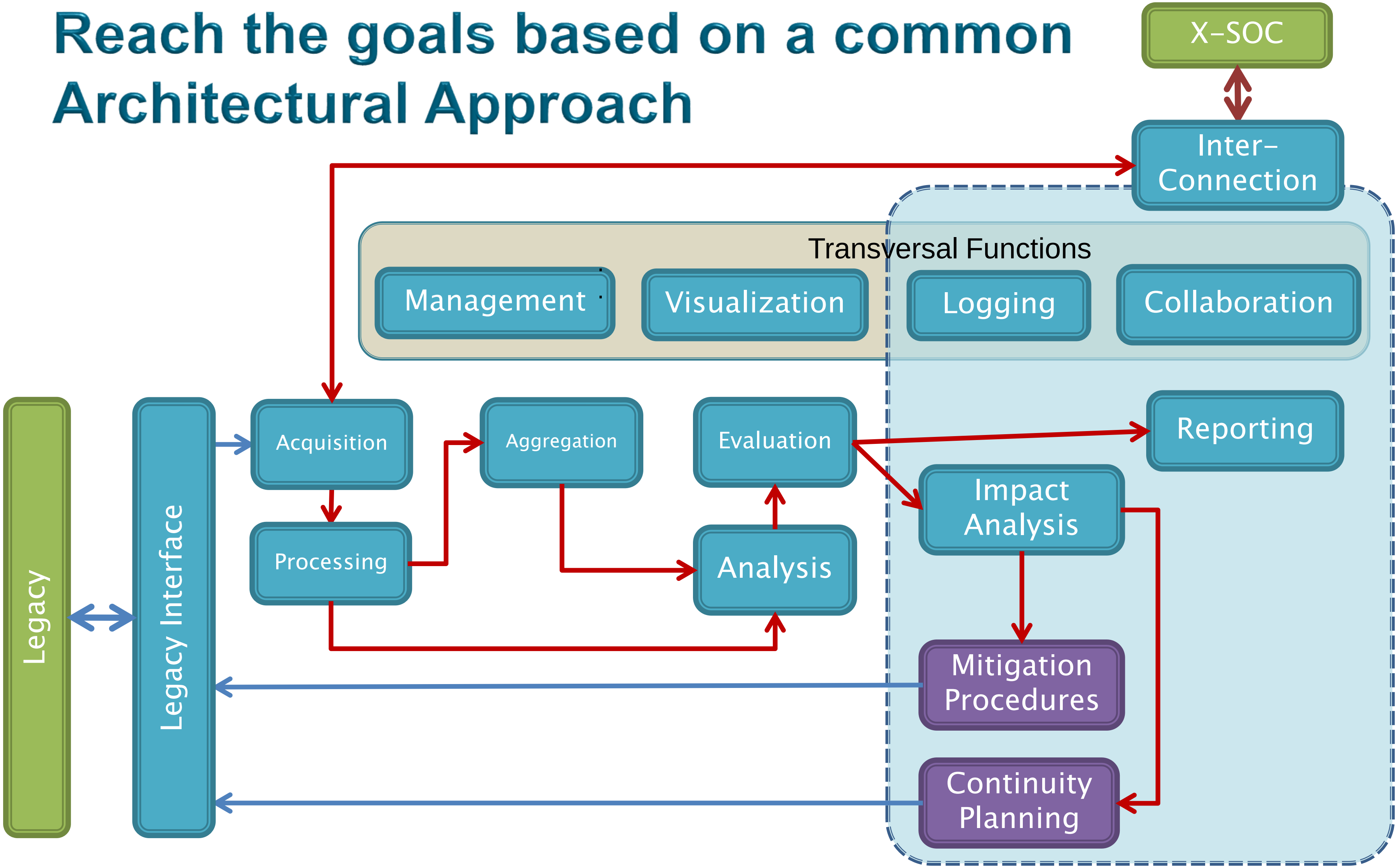
Project goals summary

A layered system architecture for a pan-European

cooperative threat management, early-warning and situational awareness:

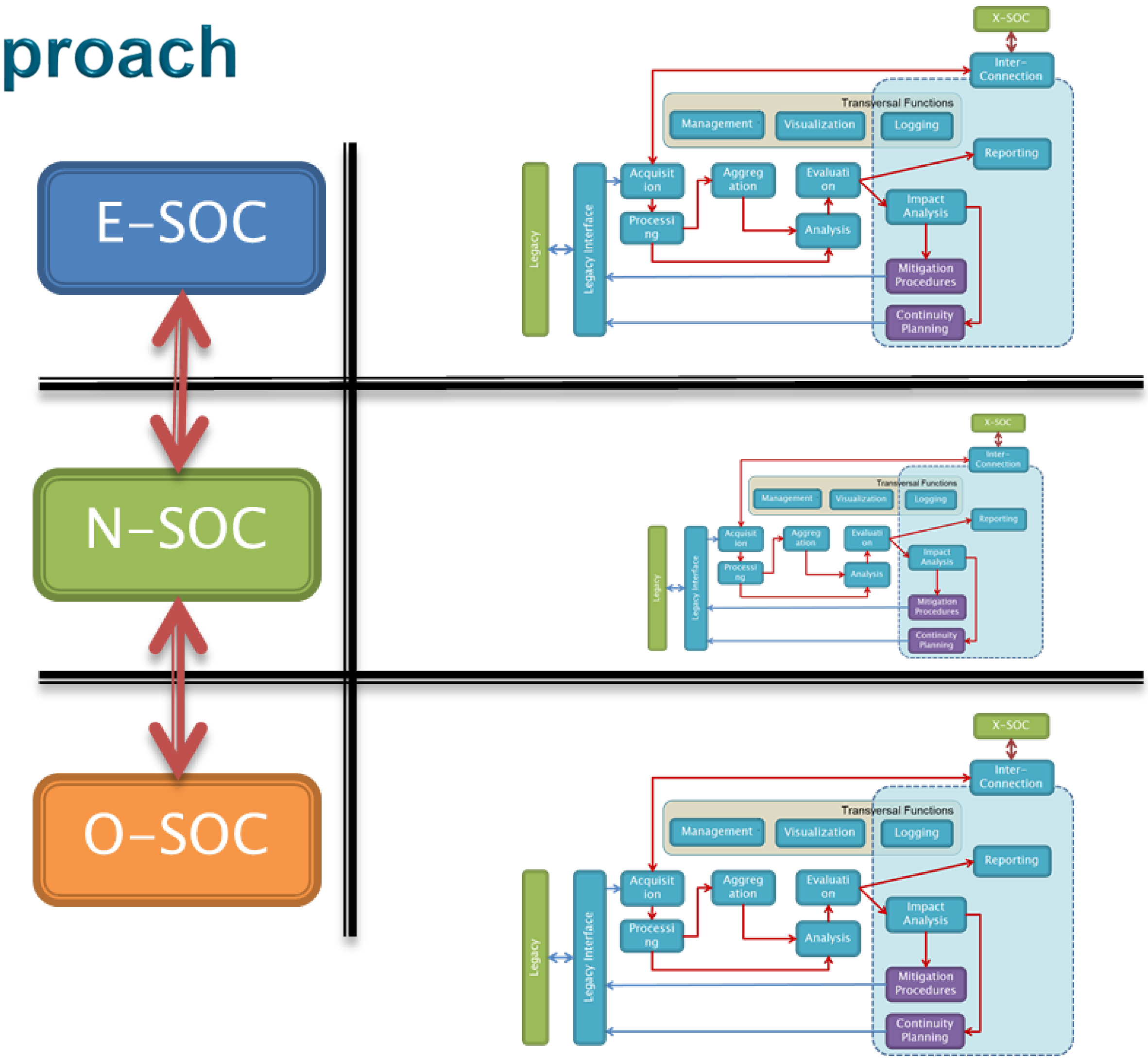
- Cross-country and cross-sectorial collaboration
- Anonymity and privacy (confidentiality) preserving for all joining members
- Secure information sharing and collaboration platform compliant to legal and other regulatory requirements
- Near-real-time detection of attacks
- Technologies and processes for monitoring and threat/incident detection
- Data analysis, aggregation, correlation and visualization
- Threat mitigation, impact analysis, interdependencies and incident management
- 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)

Reach the goals based on a common Architectural Approach



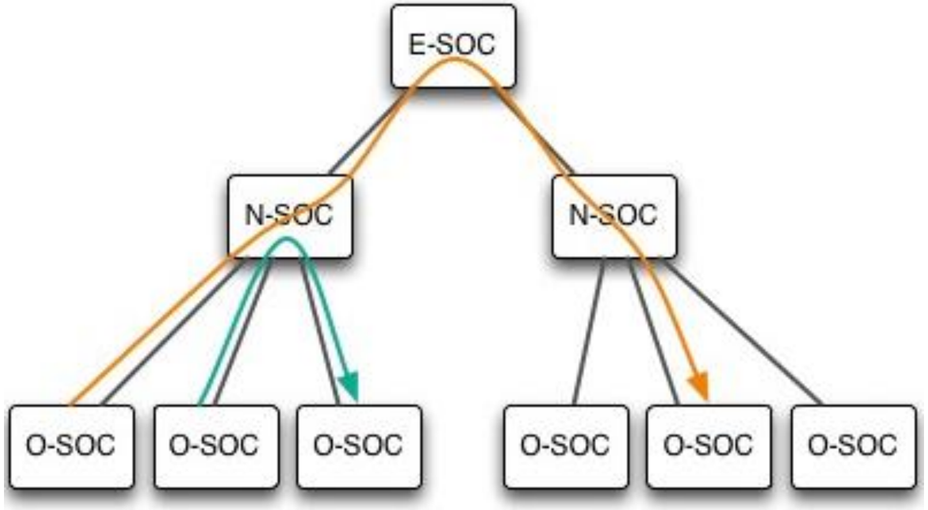
Architectural Approach

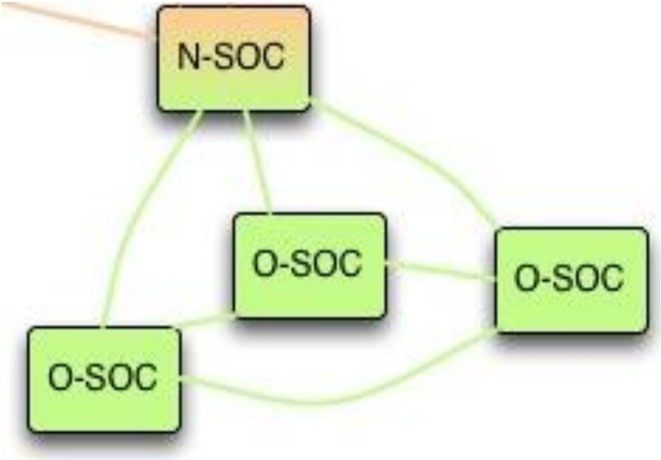
- Same architecture at each SOC level, but
- Detailed implementations and technologies may differ



Information sharing

- Definition of a tailored **hybrid sharing model**, combining hierarchical and P2P sharing models
  - O-SOC ←→N-SOCs ←→ E-SOC: **Hub-and-Spokes**
  - O-SOC ←→ O-SOC: **Post-to-All**





Information sharing

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

Attribute-Based-Encryption

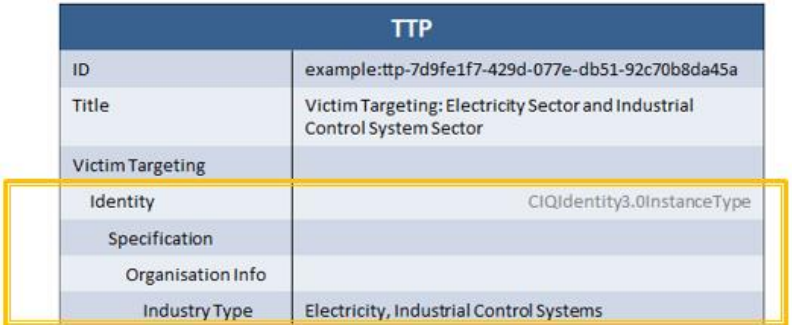
Attributes Definition

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

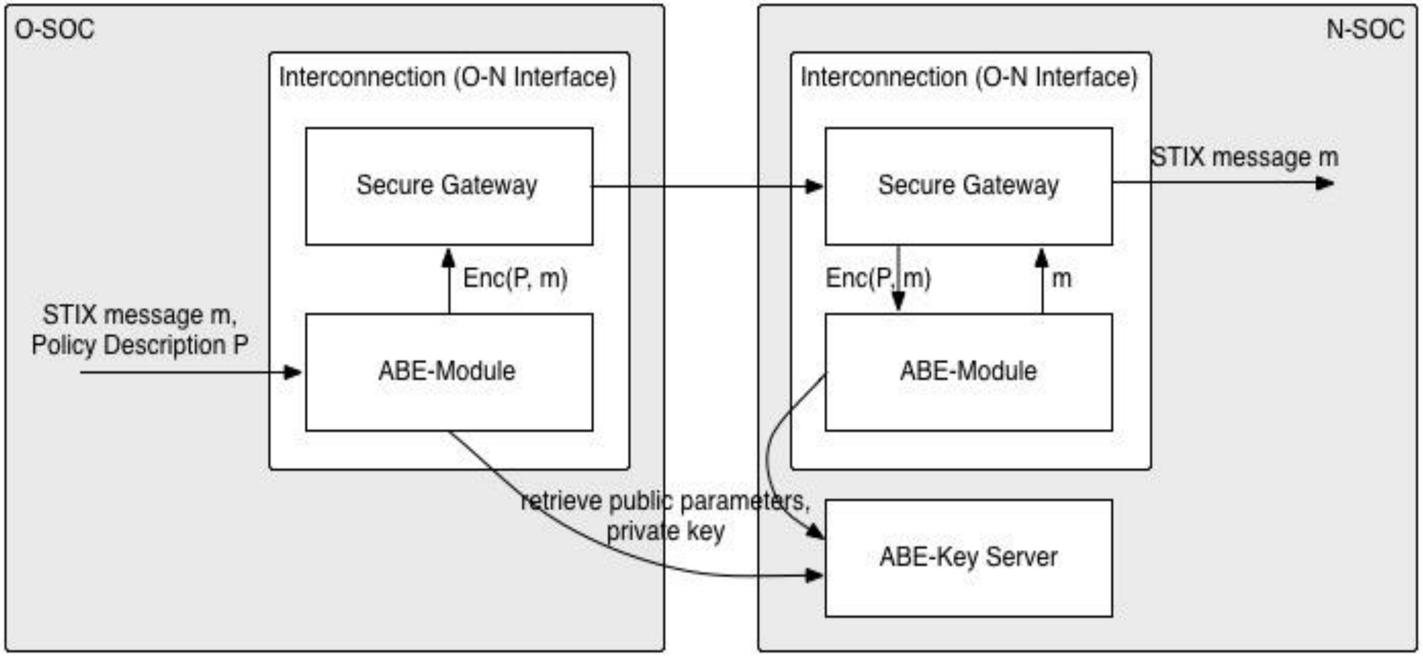


TTP	
ID	example:ttp-7d9fe1f7-429d-077e-db51-92c70b8da45a
Title	Victim Targeting: Electricity Sector and Industrial Control System Sector
Victim Targeting	
Identity	CIQIdentity3.0InstanceType
Specification	
Organisation Info	
Industry Type	Electricity, Industrial Control Systems

Policy: E-SOC, Electricity, ICS

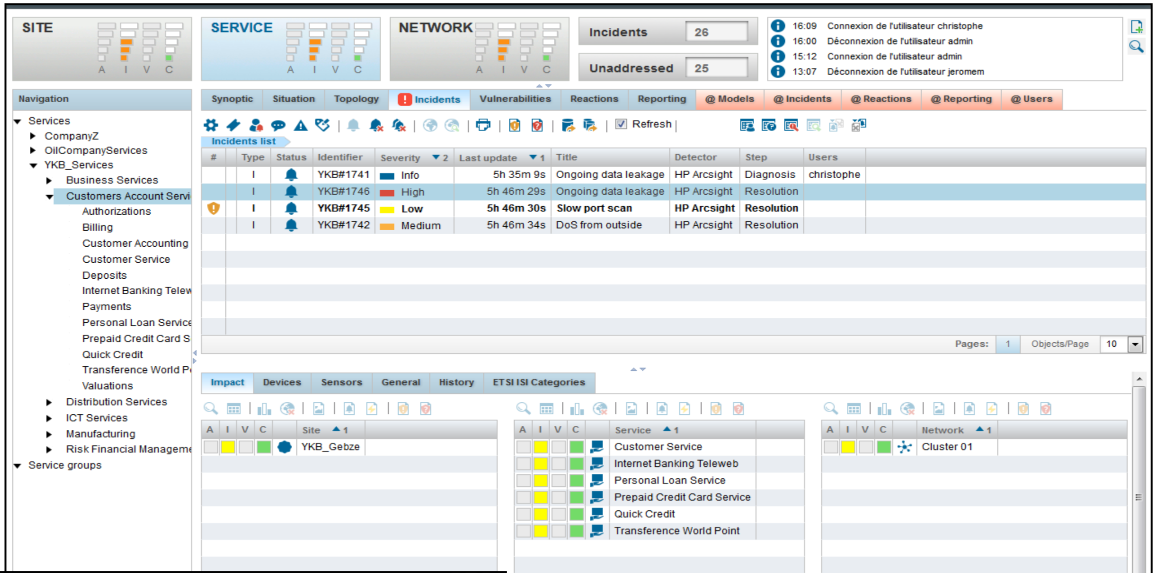
Information sharing

- Development and integration of the **ABE Module**



Cymerius

Cymerius Dashboard



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

- 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

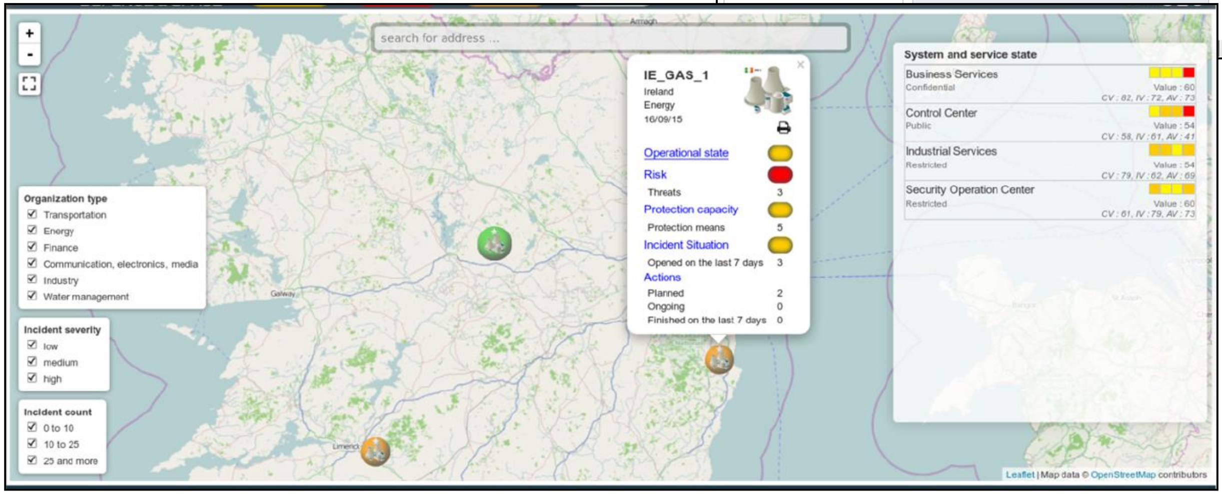
A	I	V	C		Site ▲1
	🟨		🟩	●	YKB_Gebze

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



Organization type
☑ Transportation
☑ Energy
☑ Finance
☑ Communication, electronics, media
☑ Industry
☑ Water management

Incident severity
☑ low
☑ medium
☑ high

Incident count
☑ 0 to 10
☑ 10 to 25
☑ 25 and more

IE_GAS_1
Ireland
Energy
16/09/15

Operational state	●
Risk	●
Threats	3
Protection capacity	●
Protection means	5
Incident Situation	●
Opened on the last 7 days	3
Actions	
Planned	2
Ongoing	0
Finished on the last 7 days	0

System and service state

Business Services
Confidential
Value : 60
CV : 82, IV : 72, AV : 73

Control Center
Public
Value : 54
CV : 58, IV : 61, AV : 41

Industrial Services
Restricted
Value : 54
CV : 79, IV : 62, AV : 69

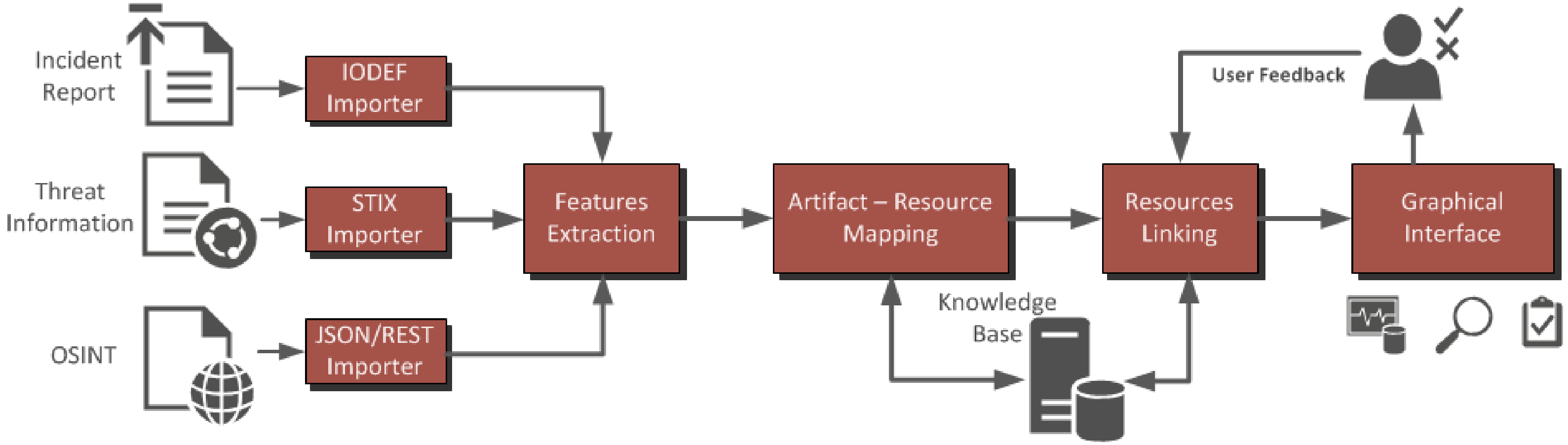
Security Operation Center
Restricted
Value : 60
CV : 61, IV : 79, AV : 73

Leaflet | Map data © OpenStreetMap contributors

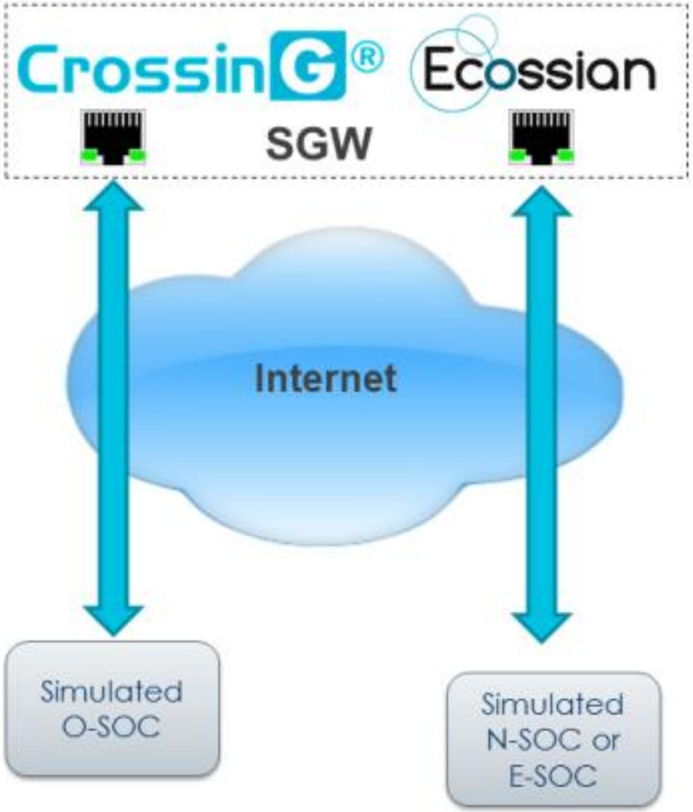
Cymerius Portal Dashboard

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)



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**.

Attribute-Based Encryption

- Encryption and decryption of a message based on a set of selected attributes while a message is sent through the Secure Gateway.
- Enforcement of the access control to the incident report by ensuring that only EU FINANCE institutions may be able to decrypt this information.

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 (Cymerius and CAESAIR).

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™

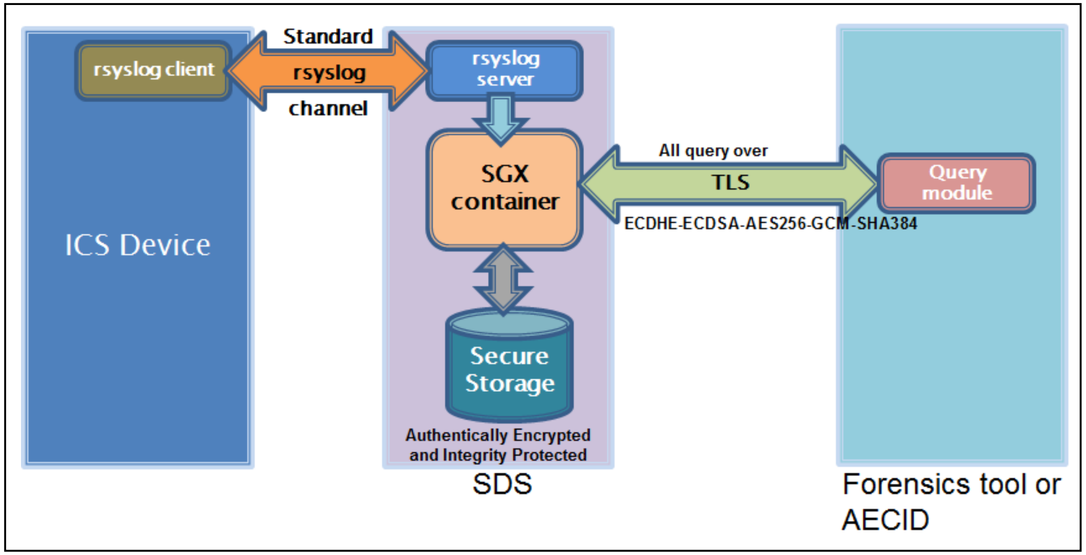
{JSON}

CPE™ common platform enumeration

Forensics and logging

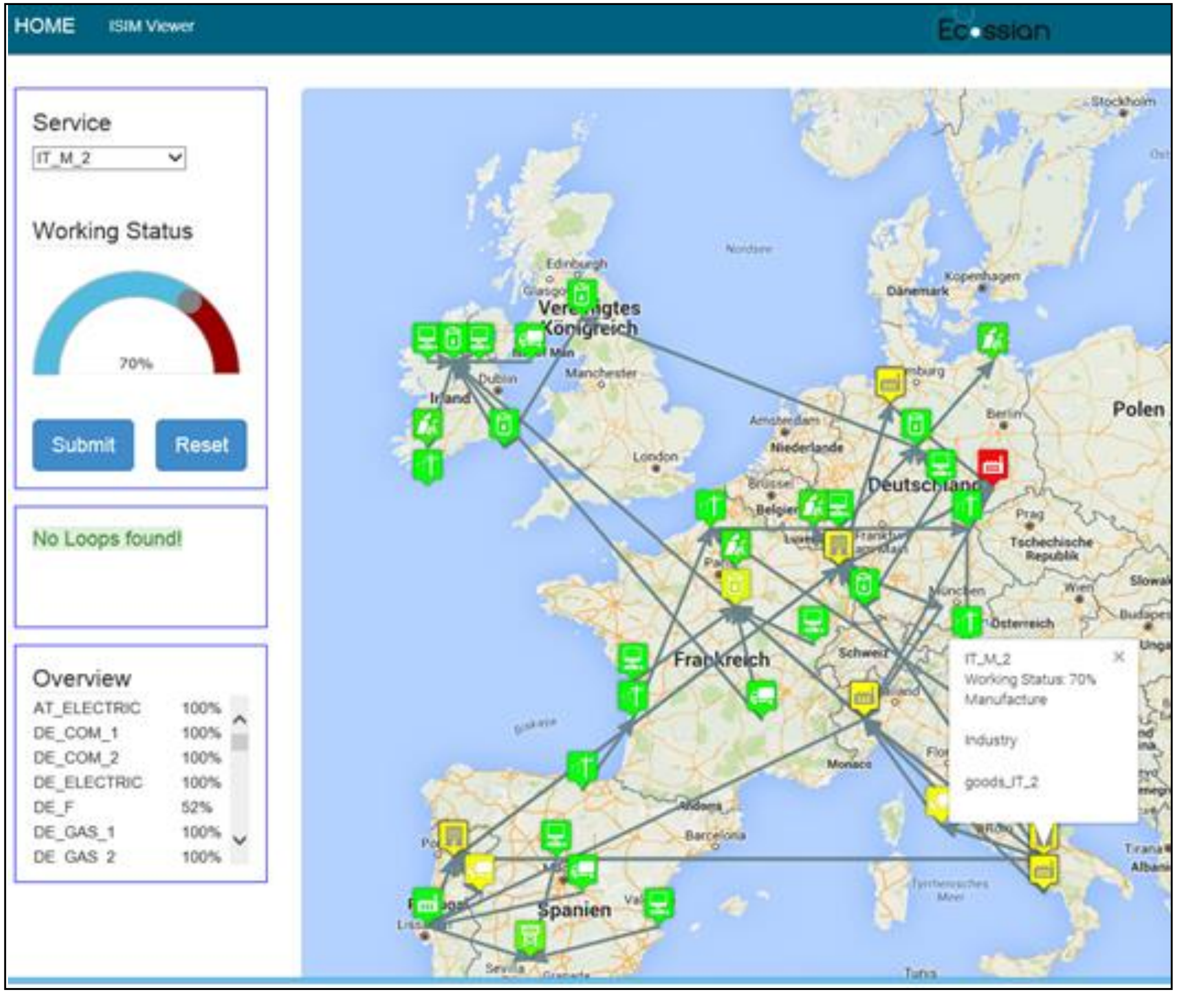
- Once an event is registered by ECOSSIAN at any of the O-SOC, N-SOC or E-SOC layers:
  - The Secure Data Storage Stores data in a forensically sound manner.
    - The event can then be interpreted and traced back to its origin,
    - Making it possible to understand “who did what, where and when”.

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



Impact analysis (at N-/E-SOC)

- **Interdependency tool** to support creating situational awareness and find out interdependencies
  - CIs dependant of the service of the disturbed CI
  - System-of-systems approach



Service

IT_M_2

Working Status

70%

No Loops found!

Overview

AT_ELECTRIC	100%
DE_COM_1	100%
DE_COM_2	100%
DE_ELECTRIC	100%
DE_F	52%
DE_GAS_1	100%
DE_GAS_2	100%

IT_M_2
Working Status: 70%
Manufacture

Industry

goods_IT_2

Consortium Overview

Germany

- EADS Deutschland GmbH
- Fraunhofer AISEC
- ifak Institut für Automation und Kommunikation e.V.
- CESS GmbH Centre for European Security Strategies
- Cassidian Cybersecurity GmbH
- *BSI Federal Office for information security **

France

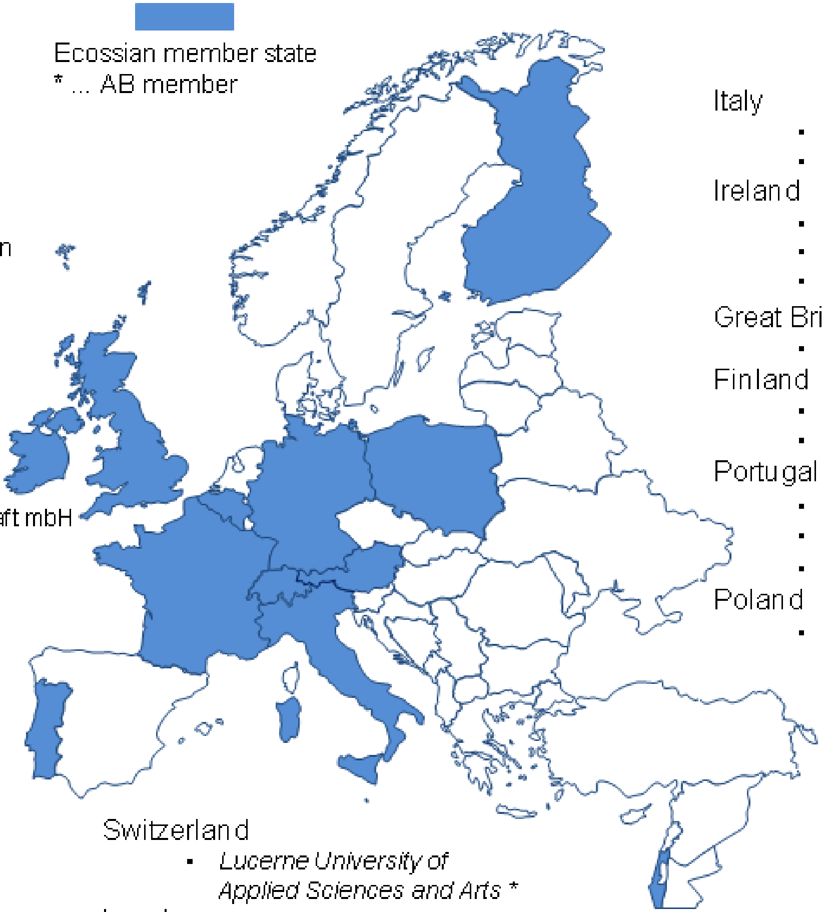
- Cassidian Cybersecurity France
- Bertin Technology

Austria

- Technikon Forschungsgesellschaft mbH
- Austria Institute of Technology
- *Austrian Ministry of Interior **
- *Austrian Federal Ministry of Defence and Sports **
- *OMV Refining**

Belgium

- ICRI KU Leuven



Italy

- Poste Italiane SPA
- University of Bologna

Ireland

- Bord Gais
- Espion Group
- *UCD Dublin**

Great Britain

- *EADS UK (subcontractor)*

Finland

- VTT
- *Finish Interior Ministry **

Portugal

- INOV Inesc Inovação
- REFER
- Ministerio da Justiça

Poland

- Police Academy in Szczytno

Switzerland

- *Lucerne University of Applied Sciences and Arts **

Israel

- *White Cyber Knight WCK **

Global

- *Europol **
- *University of California/ICSI **

Ecossian

European Control
System Security
Incident Analysis
Network

Italian Demonstration

Roma 8 Novembre 2016

Posteitaliane

Overall scenario presentation:

Protection of Critical Financial Infrastructures against advanced Cyber-attacks

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

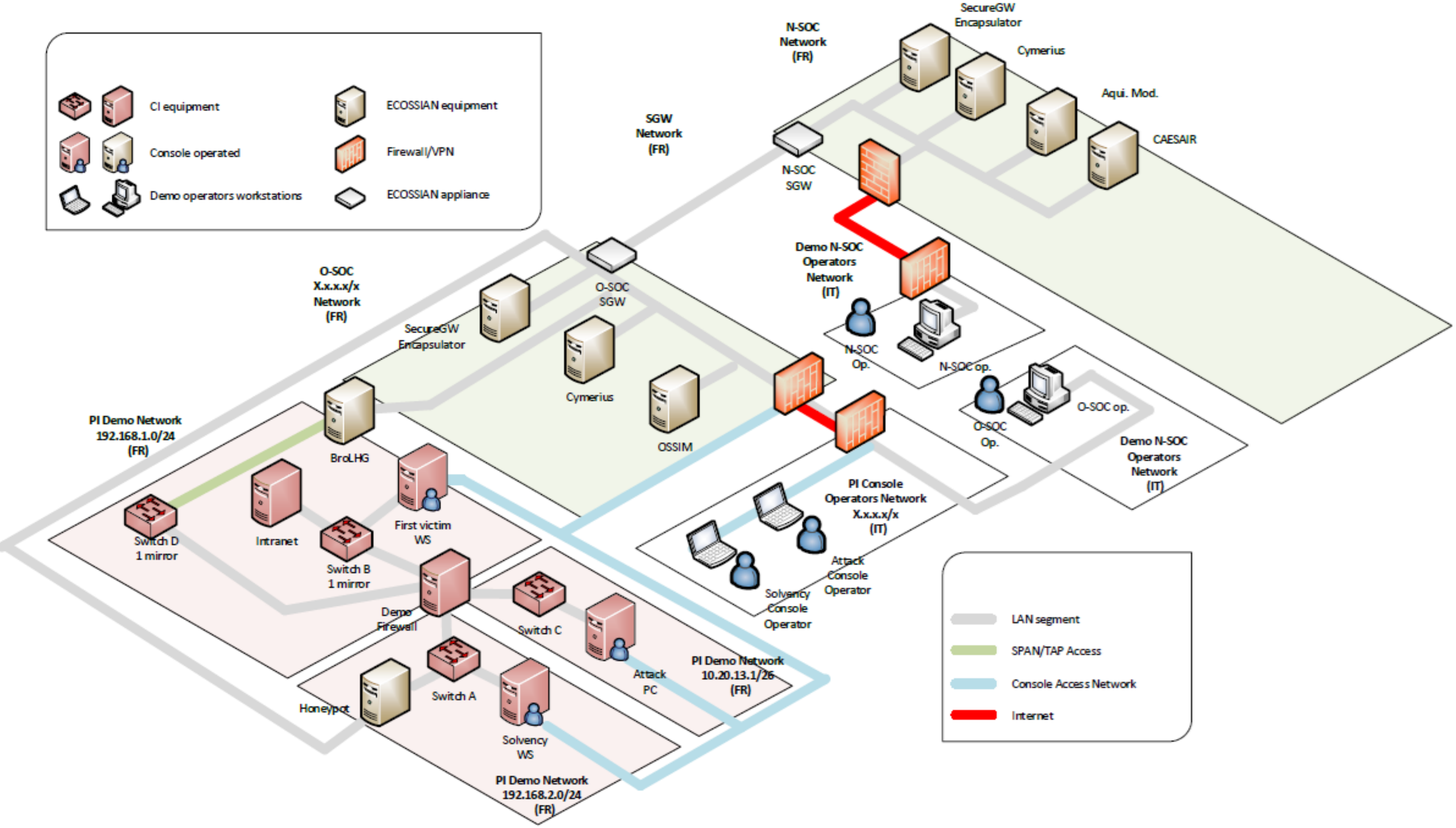
European Control System Security Incident Analysis Network

Objectives and demonstration flow

- **Objective:**
  - **Protection from an APT (Advanced Persistent Threat) attack on the Solvency Department of a Financial Critical Infrastructure.**

- Demonstration flow:
  - Phase 1: Attack
  - Phase 2: Detection
  - Phase 3: Incident response & Mitigation

Demonstration setup

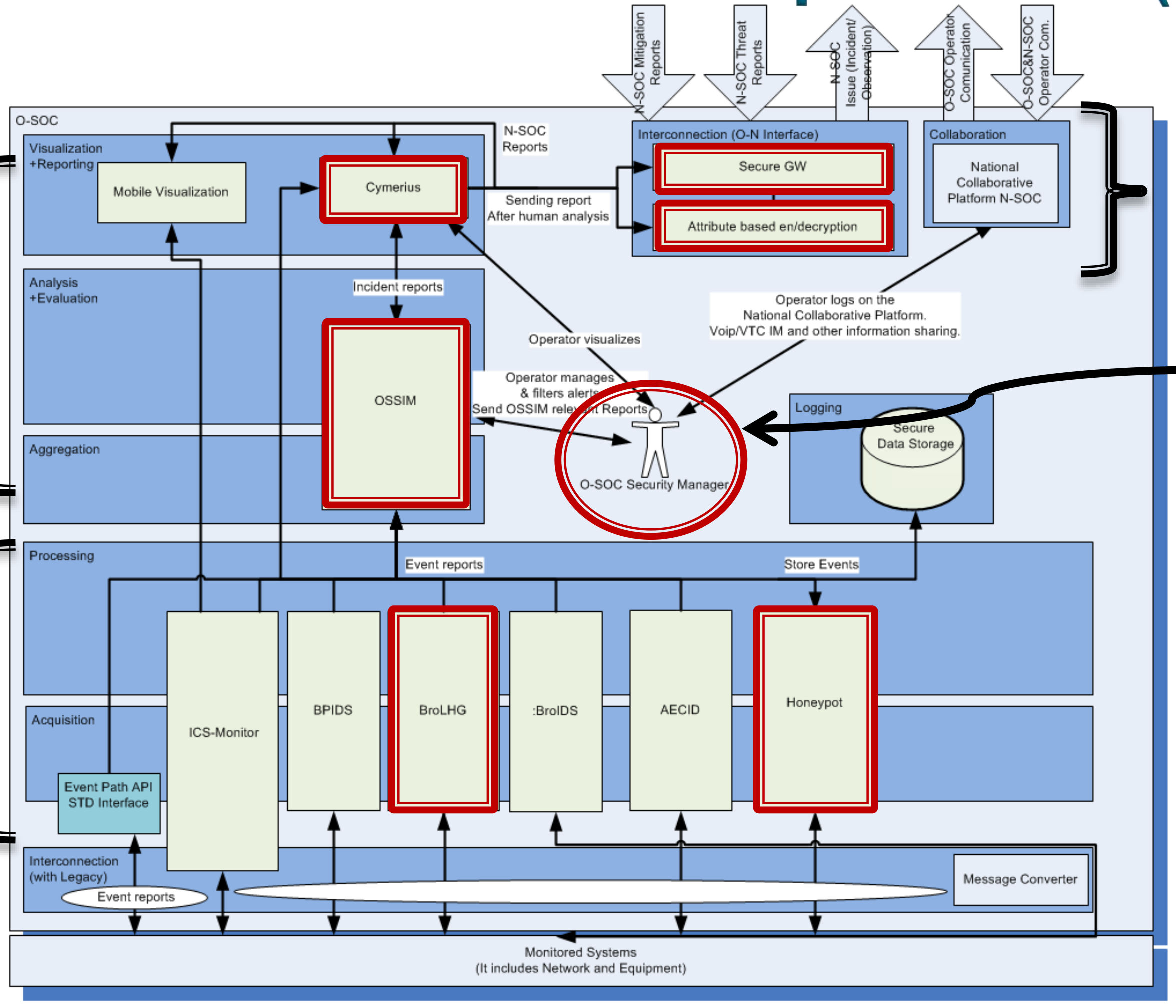


Internal network of a financial company, based on existing systems, technologies and organizational structures.

Demonstrated ECOSSIAN capabilities (O-SOC)

O-SOC supervision:
- OSSIM
- Cymerius

Sensors:
- BroLHG
- Honeypot

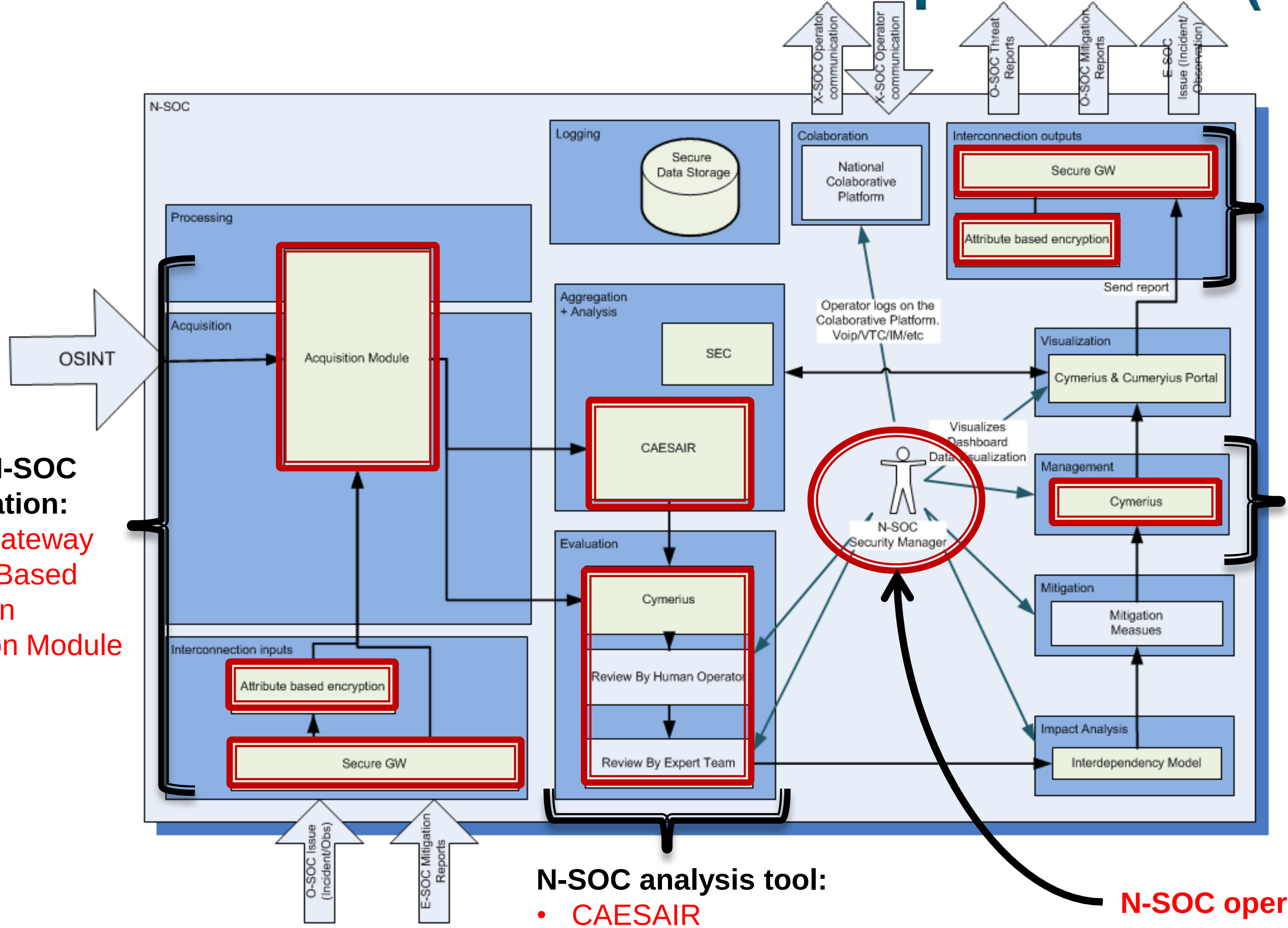


N-SOC Mitigation Reports
N-SOC Threat Reports
N-SOC Issue (Incident/ Observation)
O-SOC Operator Comunication
O-SOC&N-SOC Operator Com.
O-SOC
Visualization +Reporting
Mobile Visualization
Cymerius
N-SOC Reports
Sending report After human analysis
Interconnection (O-N Interface)
Secure GW
Attribute based en/decryption
Collaboration
National Collaborative Platform N-SOC
Analysis +Evaluation
Incident reports
OSSIM
Operator visualizes
Operator logs on the National Collaborative Platform. Voip/VTC IM and other information sharing.
Operator manages & filters alerts
Send OSSIM relevant Reports
O-SOC Security Manager
Logging
Secure Data Storage
Aggregation
Processing
Event reports
Store Events
ICS-Monitor
BPIDS
BroLHG
:BroIDS
AECID
Honeypot
Acquisition
Event Path API STD Interface
Interconnection (with Legacy)
Event reports
Message Converter
Monitored Systems (It includes Network and Equipment)

O-SOC / N-SOC communication:
- Secure Gateway
- Attribute Based Encryption

O-SOC operator

Demonstrated ECOSSIAN capabilities (N-SOC)



N-SOC to O-SOC communication:

- Secure Gateway
- Attribute Based Encryption

O-SOC to N-SOC communication:

- Secure Gateway
- Attribute Based Encryption
- Acquisition Module

N-SOC supervision:

- Cymerius

N-SOC analysis tool:

- CAESAIR
- Cymerius

N-SOC operator

Operational demonstration

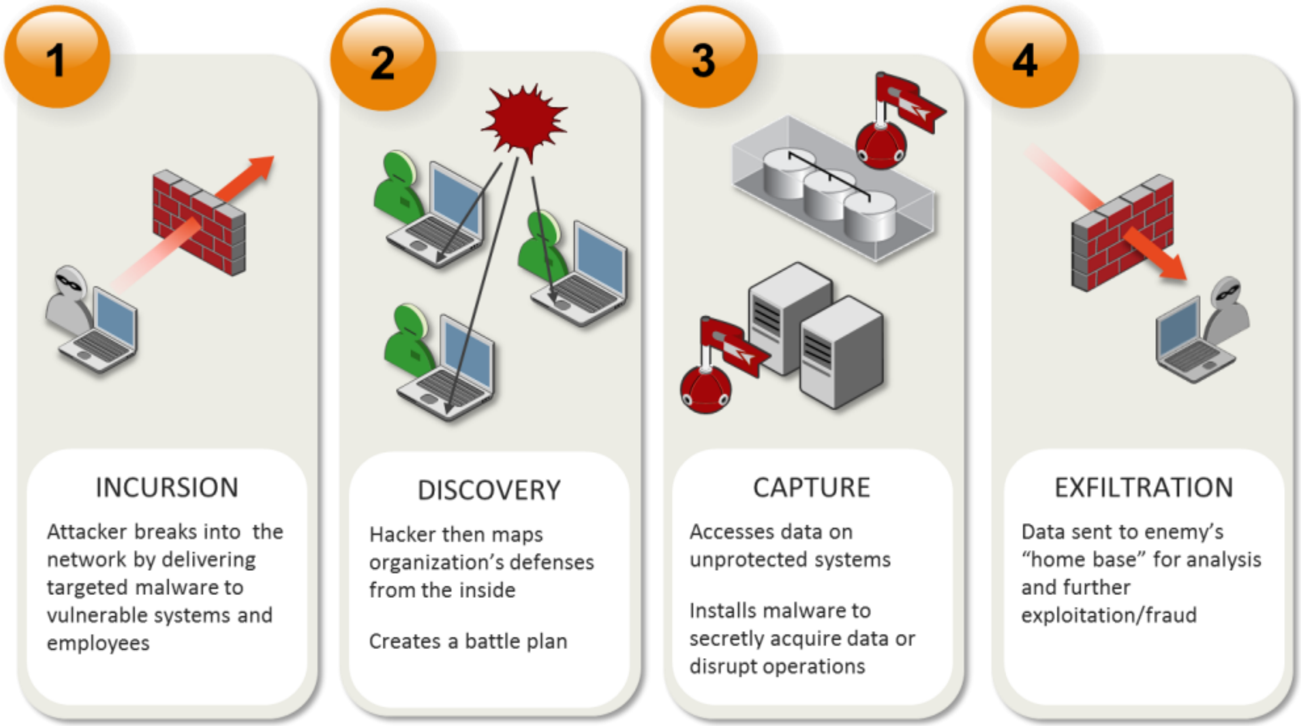
Phase 1: Attack

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

- **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

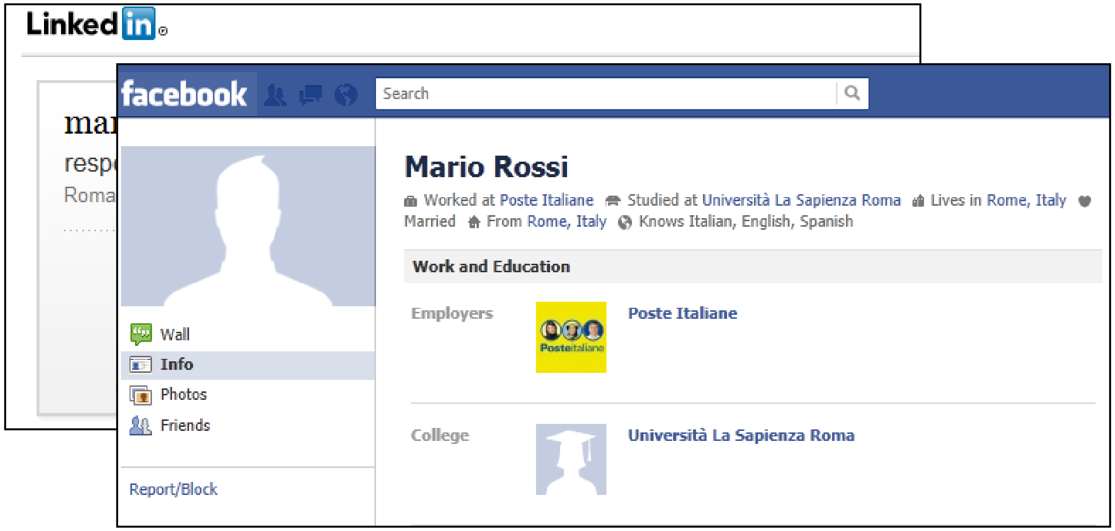
Data sent to enemy's "home base" for analysis and further exploitation/fraud

- Attacker
- Victim

Source: Symantech

Information Gathering

Social Engineering & Spear Phishing Attack

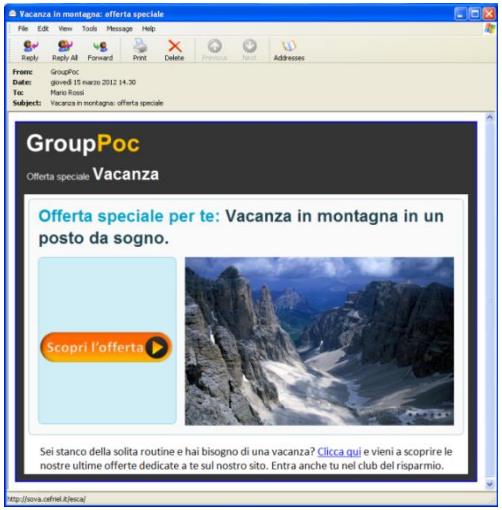


Mario Rossi

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



Vacanza in montagna: offerta speciale

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

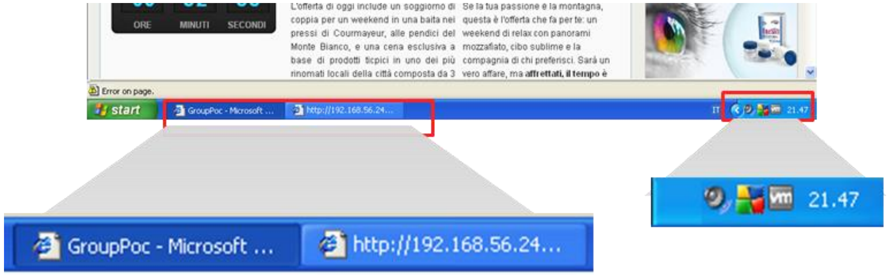
GroupPoc

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/



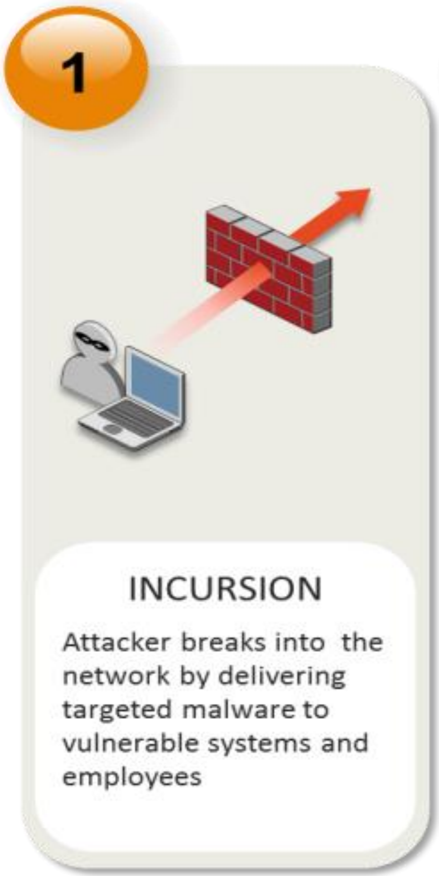
L'offerta di oggi include un soggiorno di coppia per un weekend in una baita nei pressi di Courmayeur, alle pendici del Monte Bianco, e una cena esclusiva a base di prodotti tipcici in uno dei più rinomati locali della città composta da 3

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**

Incursion

An employee PC gets infected by a malware the attacker sends through a malicious email.

A zero-day vulnerability is exploited.



INCURSION

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

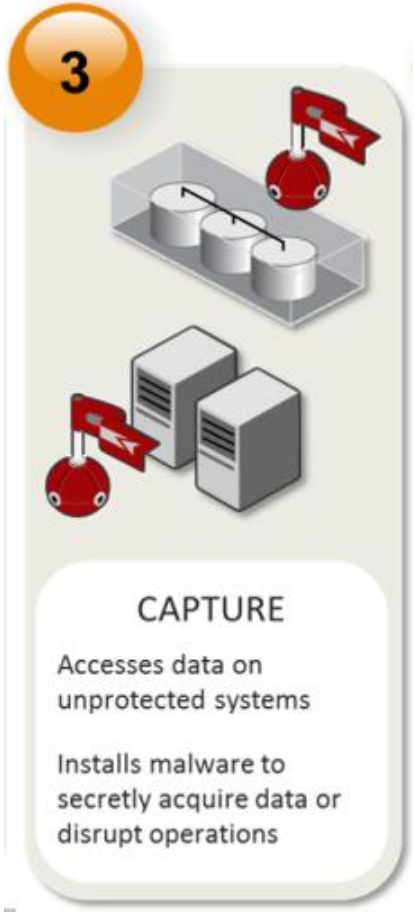
Network topology discovery

The attacker explores the network topology and scans for active services while keeping a low-profile to avoid detection by O-SOC operators.

2
DISCOVERY
Hacker then maps organization's defenses from the inside
Creates a battle plan

Data Capture

The attacker gains control over servers and workstations and looks for valuable information he could collect



CAPTURE

Accesses data on unprotected systems

Installs malware to secretly acquire data or disrupt operations

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

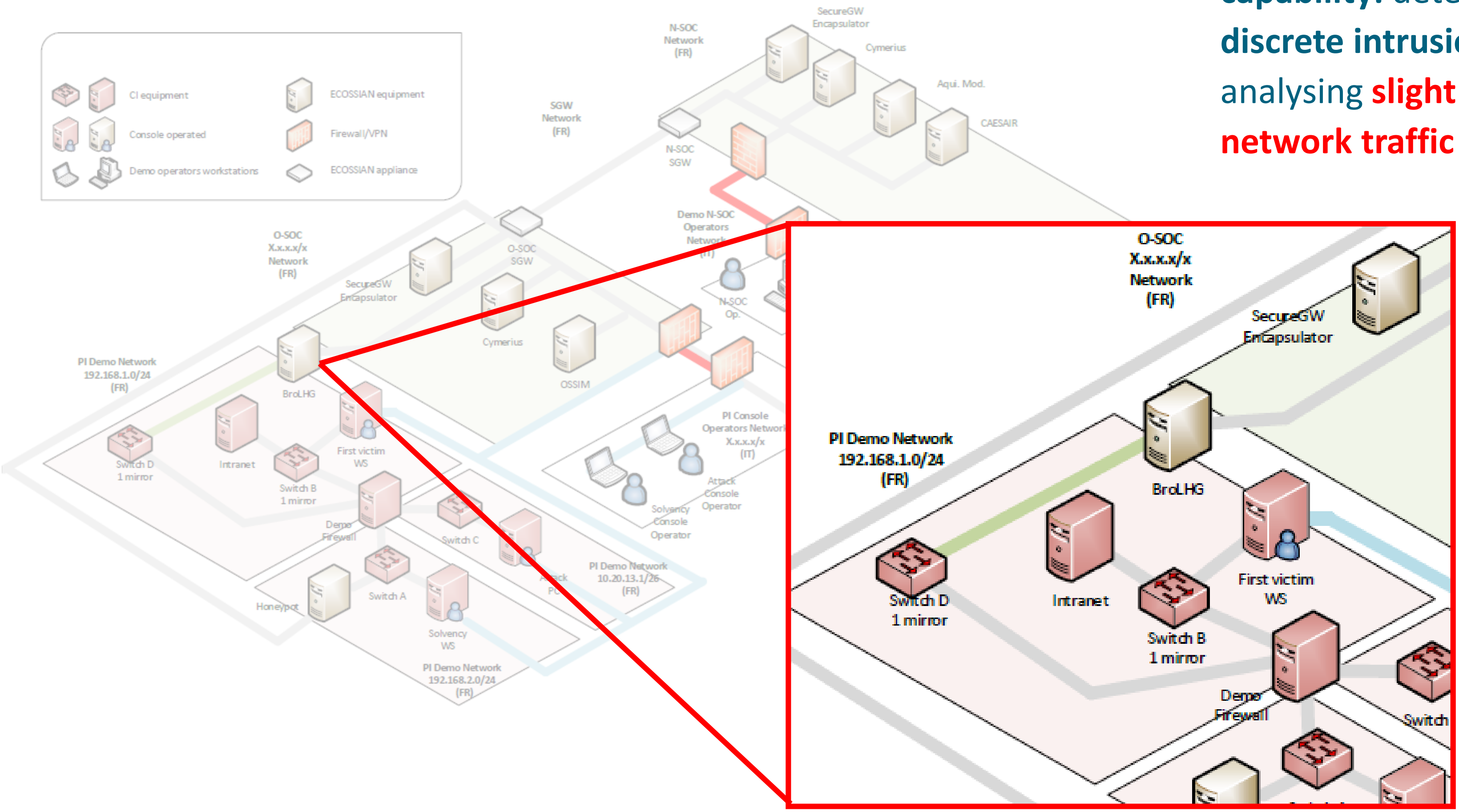
European Control System Security Incident Analysis Network

Introduction

- **Detection of the intrusion by two sensors of the ECOSSIAN system: BroLHG and Honeypot.**
  - The internal 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.

- 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.

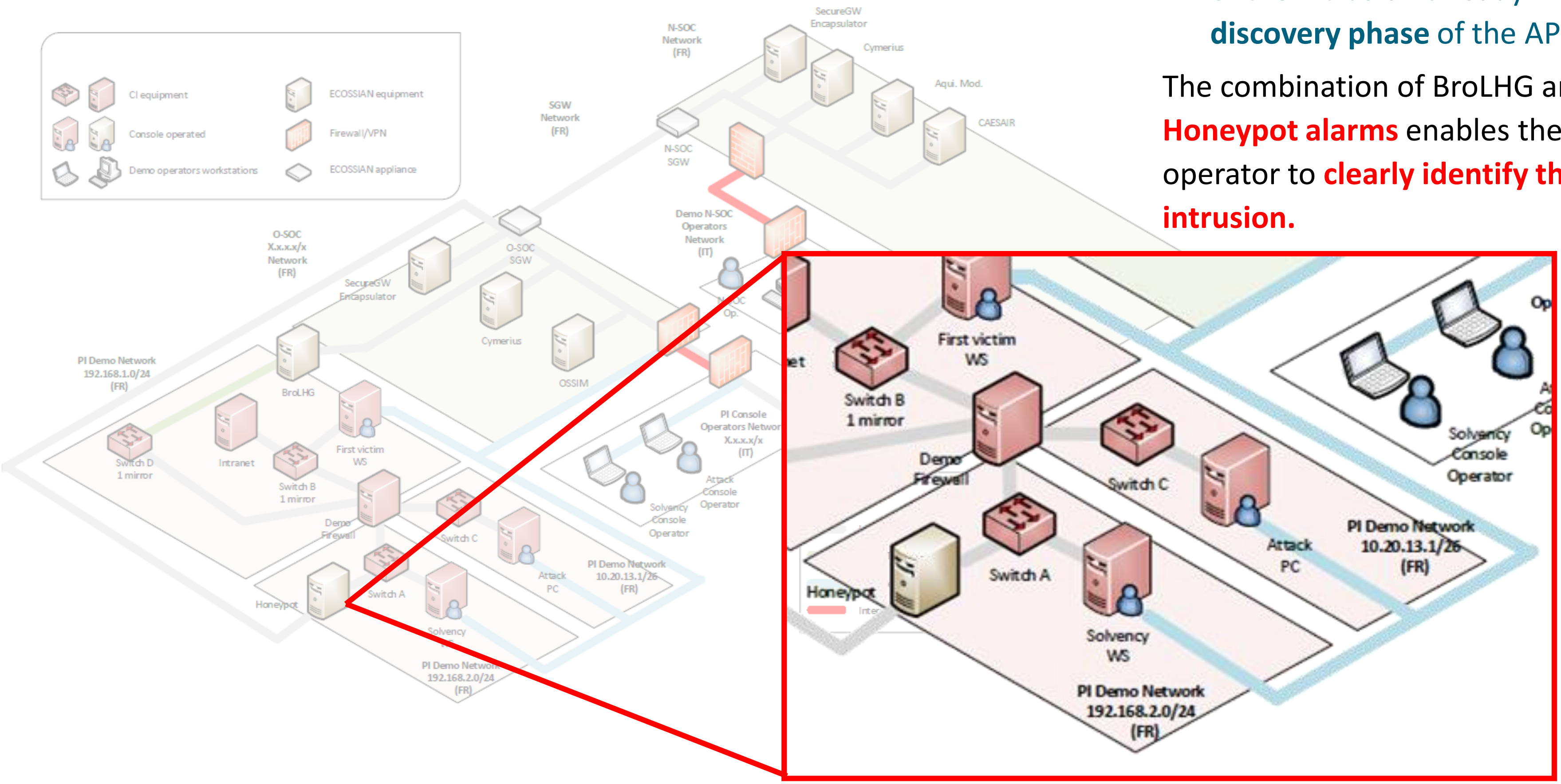
Detection #1: BroLHG



ECOSSIAN capabilities

- **Advanced detection capability:** detection of a **discrete intrusion** of by analysing **slight anomalies in network traffic patterns**.

Detection #2: Honeypot



ECOSSIAN capabilities

- **Advanced persistent threat detection capability:** detection of the intrusion already in the **discovery phase** of the APT.

The combination of BroLHG and **Honeypot alarms** enables the O-SOC operator to **clearly identify the intrusion.**

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).

Operational demonstration

Phase 3: Incident response and mitigation

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. Incident supervision and analysis (O-SOC level)
  2. National collaboration and support for solving the incident (O-SOC to N-SOC incident forwarding)

- 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**

O-SOC to N-SOC: incident forwarding

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 (Cymerius and CAESAIR).
- Compliant with the most widely adopted data formats and protocols for cyber incident and threat information description and exchange.

N-SOC Cymerius

- Incident received on the N-SOC operator console

ECOSSIAN capabilities

- **National awareness:** situation awareness on **security issues at national level**
- Based on the possibility of **sharing threat information** between the O-SOC and N-SOC, in a **secure and encrypted way** (thanks to the SGW and the ABE module).

N-SOC level: analysis

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**

N-SOC Cymerius

- Import of CAESAIR analysis

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
- **Centralised database:** Centralise useful information (such as **threat patterns**).

N-SOC warnings: national 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)**

Mitigation & feedback sharing (lesson learned)

Mitigation

- 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 Italy and in Europe.**