ECOSSIAN - European Control System Security Incident Analysis Network

Demonstração Portuguesa

16 de Fevereiro de 2017, Lisboa

Ecossian POLÍCIA JUDICIÁRIA inov inesc • inovação Infraestruturas de Portugal IP Telecom

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.

Infraestruturas de Portugal

IP Telecom

POLÍCIA JUDICIÁRIA

inov inesc • inovação

ECOSSIAN FP7 PROJECT

Proteção das Infraestruturas de Transportes contra ataques informáticos

Lisboa, 16 de Fevereiro de 2017

European Control System Security Incident Analysis Network

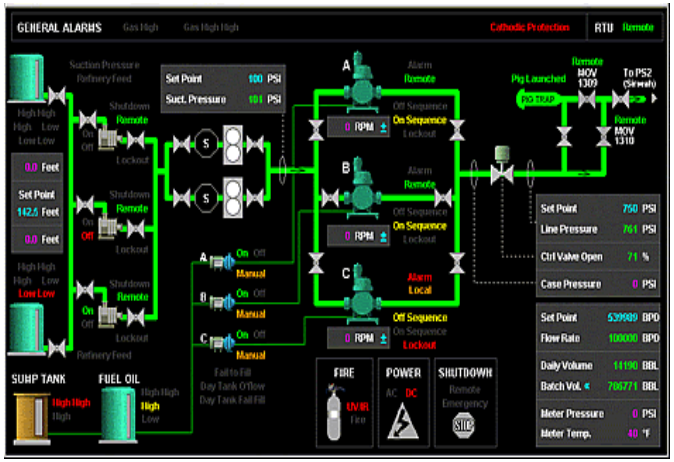
Contexto

- Uma **Sociedade Moderna** depende fortemente da **fiabilidade** e da **contínua disponibilidade** dos serviços fornecidos pelas **Infraestruturas Críticas**.

•Uma **séria disrupção** desses serviços poderá colocar em risco a vida de pessoas e provocar um forte impacto social e económico.

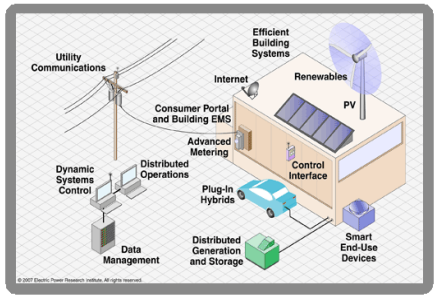
• As Infraestruturas Críticas são cada vez mais **alvo de ataques** com origem no espaço cibernético.

  - Terroristas
  - Governos
  - Concorrência/Espionagem industrial
  - Piratas informáticos e …



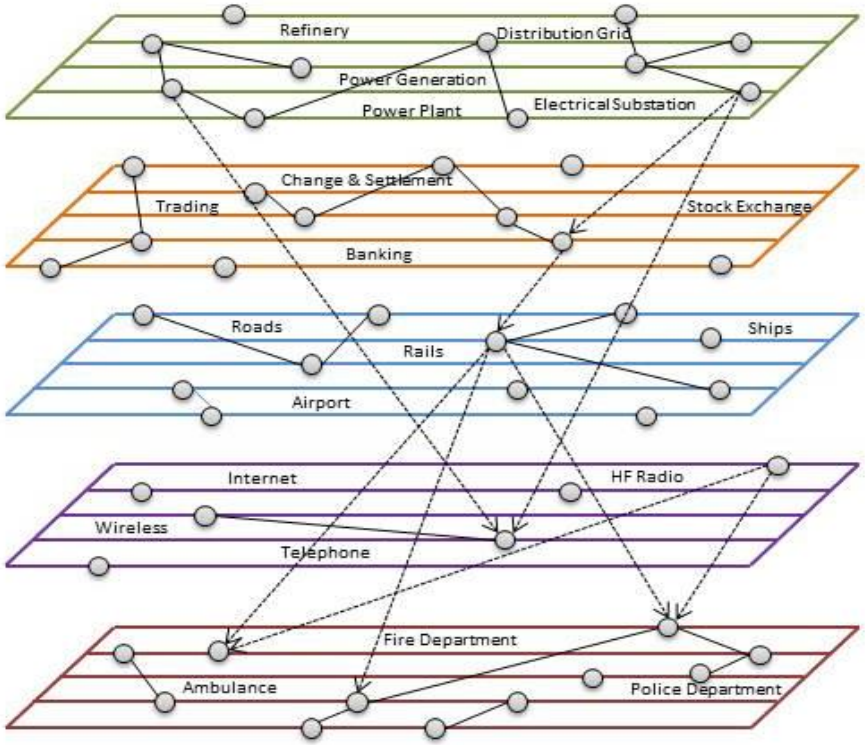
Motivação

- A superfície de ataque das infraestruturas críticas tem estado continuamente a crescer devido a:
  - **Instalação de produtos e sistemas COTS**
  - Alteração de protocolos proprietários e produtos para tecnologias usadas em IT
  - Uma maior convergência das tecnologias utilizadas
  - **A utilização cada vez mais alargada de dispositivos móveis e serviços**
  - **Tempo de vida muito prolongado de produtos (10-25 anos)**
  - **A segurança das tecnologias utilizadas encontra-se desfasada entre 5 a 10 anos comparativamente com as usadas no mundo empresarial de TI**
  - Os sistemas de proteção de segurança informática atuais são de aplicação limitada neste tipo de infraestruturas devido às suas especificidades ex. resposta em tempo real



Motivação

- Interdependências entre infraestruturas críticas



Energy, Oil & Gas

Finance

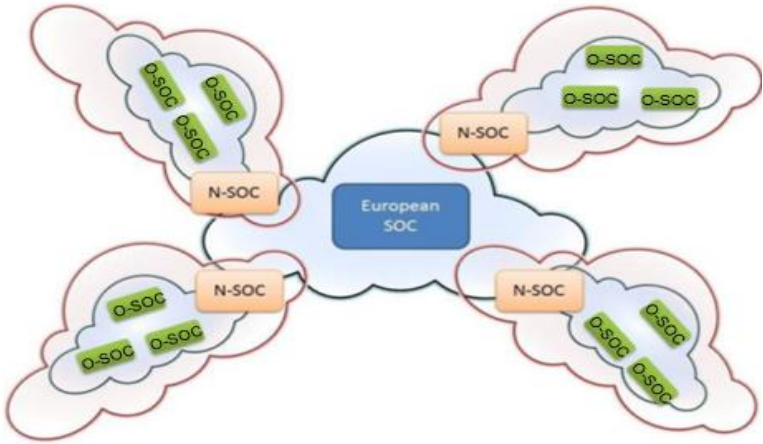
Transportation

Information & Telecom

Emergency Services

Objetivos do Projeto

- Desenvolvimento de um sistema Europeu de alerta precoce transfronteiriço para as infraestruturas críticas
- Três níveis de colaboração, Centros Operacionais de Segurança (SOC - Secure Operation Centres)
  - **SOC Local/Operador (O-SOC)**
    Deteção precoce e aquisição / agregação de dados
  - **SOC Nacional (N-SOC)**
    Visão nacional usando os dados agregados e correlacionados
  - **SOC transnacional com capacidades de com dos estados membros europeus (E-SOC)**
    Visão transnacional e coordenada para uma gestão de crise consistente



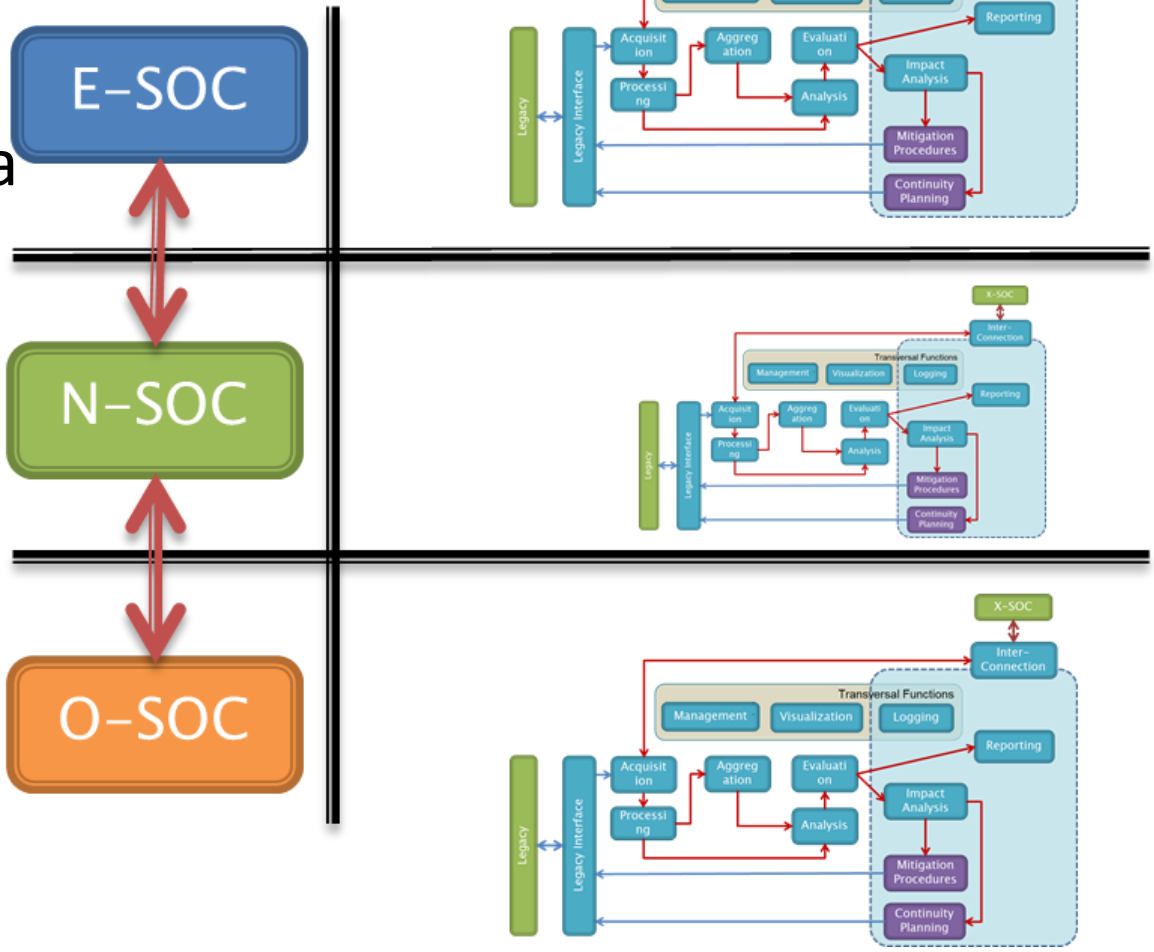
Resumo dos objetivos do projeto

Uma arquitetura para um sistema pan-europeu de cooperação e gestão de ameaças, de alertas precoces e providenciando uma visão global:

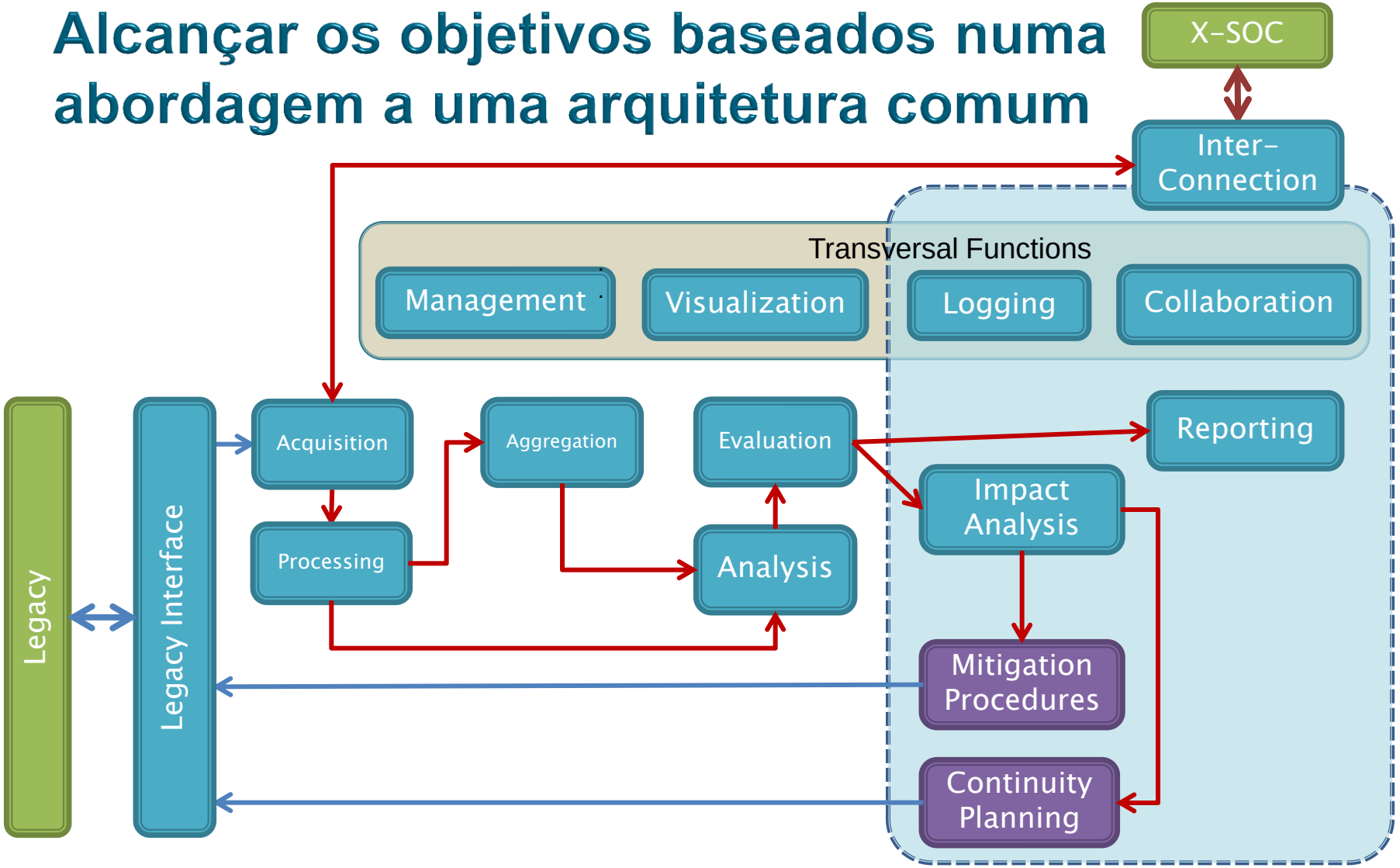
- Colaboração transfronteiriça e transectorial
- Preservando o anonimato e a privacidade (confidencialidade) para todos os membros
- Partilha de informação segura e uma plataforma colaborativa que respeita a legislação em vigor entre outros requisitos
- Deteção quase em tempo real de ataques informáticos
- Tecnologias e processos para monitorização e deteção de ameaças/incidentes
- Análise de dados, agregação, correlação e visualização
- Mitigação de ataques, análise de impactos , interdependências e gestão de incidentes
- Avaliação das condições regulamentares, sociais e económicas
- **Demonstração em larga escala de todas as componentes** integradas do ECOSSIAN a todos os níveis (O-SOC, N-SOC, E-SOC)

Arquitetura

- A mesma arquitetura em cada nível SOC, mas
- As implementações e as tecnologias podem variar.

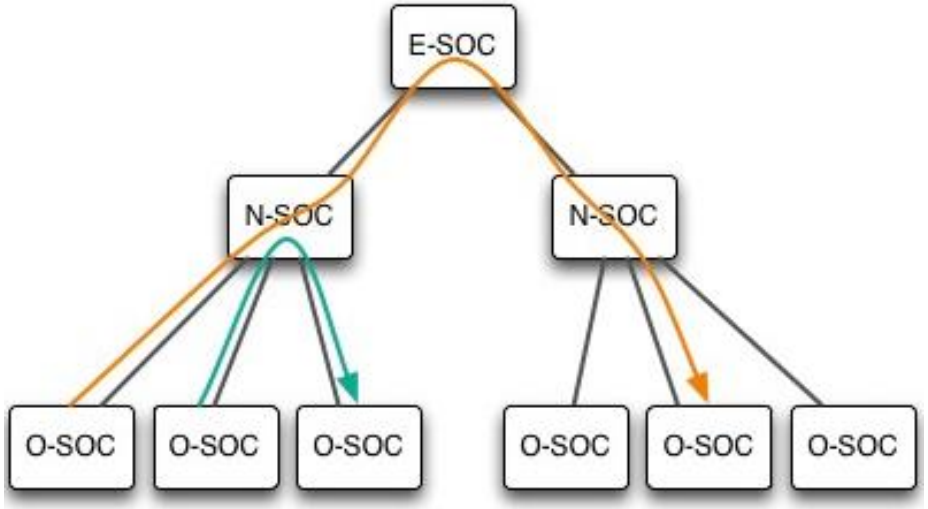


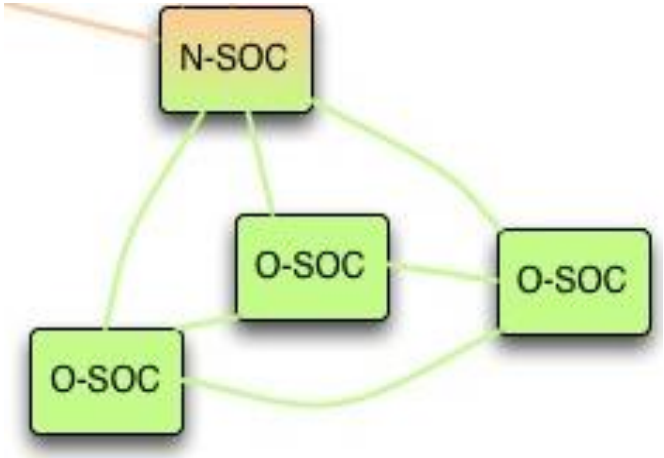
Alcançar os objetivos baseados numa abordagem a uma arquitetura comum



Partilha de informação

- Desenvolvimento de um modelo híbrido de partilha, combinando os modelos hierárquico e de ponto-a-ponto (P2P)
  - O-SOC ←→N-SOC ←→ E-SOC: **Hub-and-Spokes**
  - O-SOC ←→ O-SOC: **Post-to-All**





Resumo do Consórcio

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
- Infraestruturas de Portugal, SA
- 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

Ecossian

Demonstração Portuguesa

16 de Fevereiro de 2017, Lisboa

Ecossian | POLÍCIA JUDICIÁRIA | inov inesc • inovação | Infraestruturas de Portugal | IP Telecom

Ecossian

Apresentação do cenário

Proteção das Infraestruturas de Transportes contra ataques informáticos

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

POLÍCIA JUDICIÁRIA

inov inesc • inovação

Infraestruturas de Portugal

IP Telecom

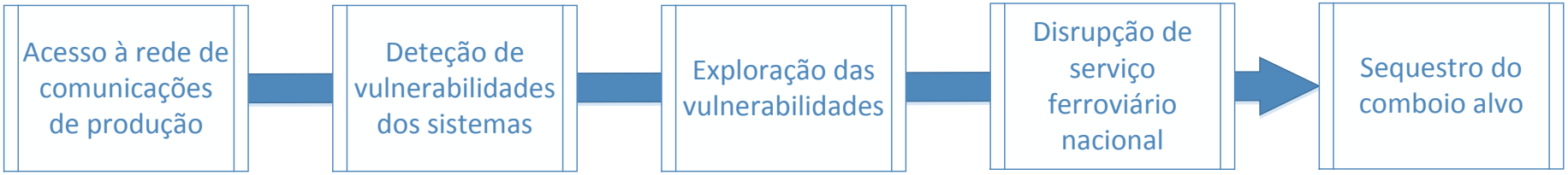
European Control System Security Incident Analysis Network

Atacante

- Motivação
  - Uma organização internacional terrorista procura um meio para tornar a sua causa bem visível. Para tal tenta orquestrar um ataque de escala Europeia que seja capaz de instalar o medo e ameaçar o “Mundo Ocidental”.
- Objetivo
  - Lançar uma serie de ataques com o propósito de causar uma forte disrupção de serviço na operação ferroviária nacional. Estes ataques servirão como uma manobra de distração para encobrir o objetivo final que é sequestrar um comboio especifico.

Atacante

- Método
  - Ganhar a acesso à rede de comunicações ferroviária;
  - Reunir as informações e detetar vulnerabilidades sobre os sistemas;
  - Explorar as vulnerabilidades e causar disrupção de serviço;
  - Atingir objetivo com paragem do comboio alvo.



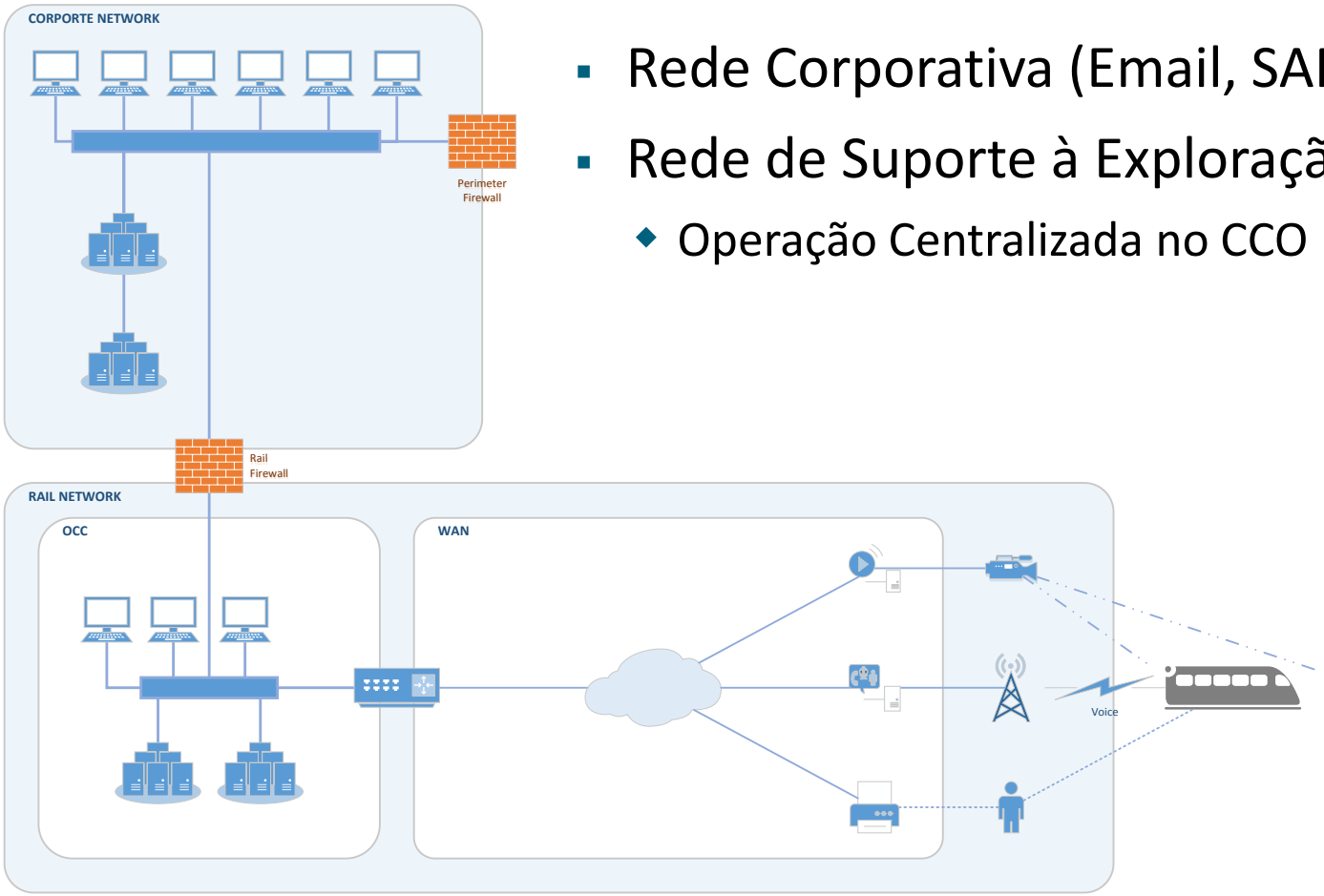
Objetivo e fluxo de demonstração

- Objetivo:
  - Deteção de um ataque informático a uma infraestrutura critica ferroviária.
- Fluxo de Demonstração:
  - Fase 1: Intrusão na rede
  - Fase 2: Manipulação do sistema de limite de velocidade
  - Fase 3: Ataque ao sistema SCADA
  - Fase 4: Sequestro de comboio
- Relevância
  - Abordar os incidentes e eventos que atualmente representam verdadeiras ameaças às infraestruturas críticas de transporte existentes.

Apresentação da arquitetura interna da IP

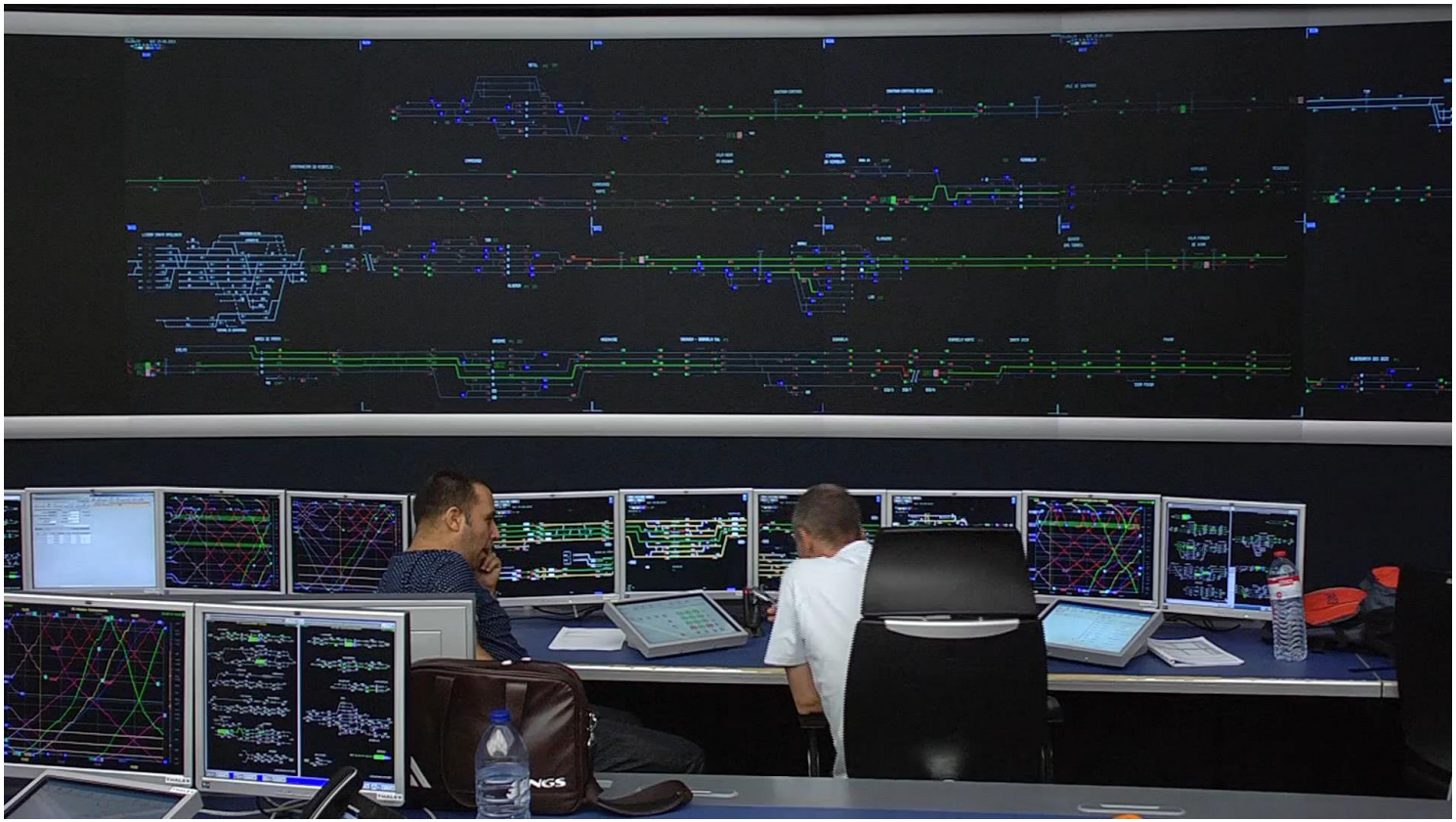
- Sistemas intervenientes na demostração
  - Sistema de limitação de velocidade;
  - Sistemas SCADA (Supervisão Técnica de Infraestruturas e Telecomando de Energia);
  - Sistema de Deteção de Obstáculos;
  - Sistema de Radio Solo Comboio;
  - Sistema de Videovigilância;
  - Infraestrutura de rede (Switch, Firewall).

Apresentação da arquitetura interna da IP



- Rede Corporativa (Email, SAP, etc.)
- Rede de Suporte à Exploração Ferroviária
  - Operação Centralizada no CCO

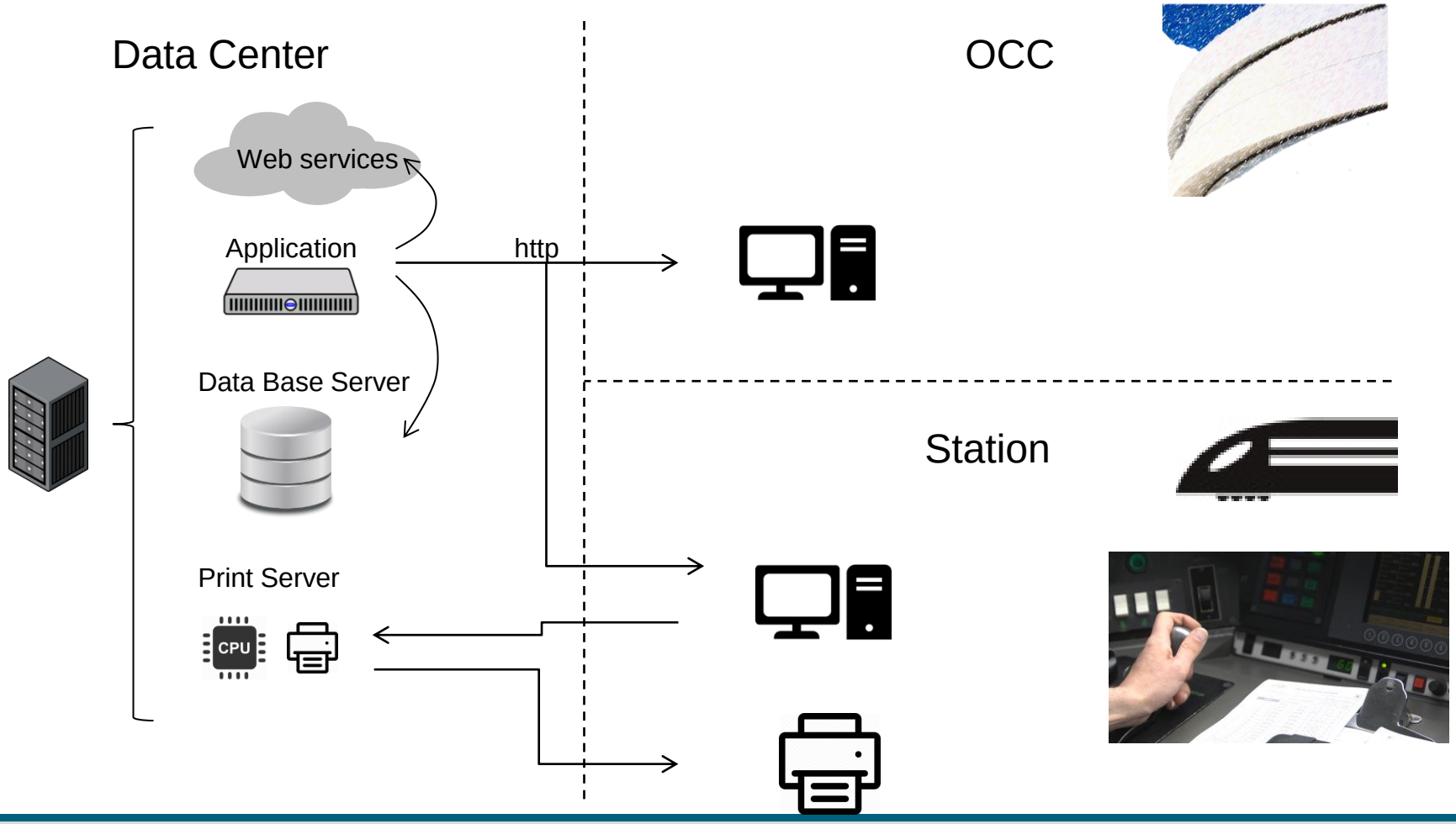
Operação Centralizada no CCO



Sistema de limitação de velocidade

- Sistema constituído por três serviços.
  - Serviço Central
    - Consultar as Limitações de Velocidade estabelecidas e em vigor nas suas áreas de comando;
    - Criar Limitações de Velocidade numa linha, via, sentido e par de pontos quilométricos;
    - Criar Limitações de Velocidade para uma dependência, via, sentido e par de pontos quilométricos;
    - Terminar Limitações de Velocidade estabelecidas;
  - BackOffice
    - Diariamente, para as LV que estão programadas, o sistema deverá identificar os comboios que serão afetados na sua marcha;
    - Preparará os modelos 99-003 que enviará aos serviços de estação onde os modelos deverão impressos e entregues aos operadores;
  - Serviço Estação
    - Mantém atualizados, produz e imprime os modelos 99-003 a entregar aos comboios que tem como origem ou passagem essa estação;
    - Disponibiliza ainda ao Operador uma interface que lhe permite monitorizar o estado deste serviço, bem como identificar, consultar e imprimir manualmente os modelos 99-003 anteriormente referidos.

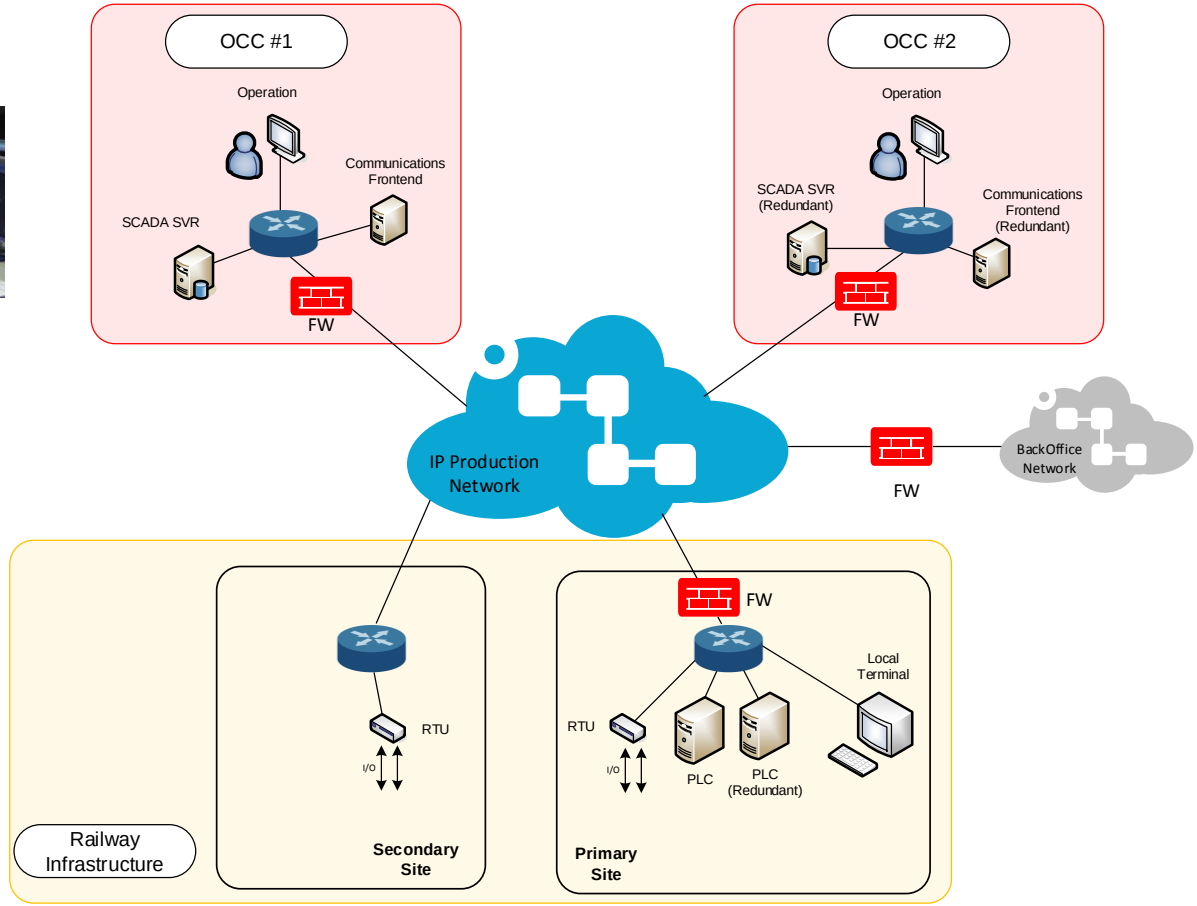
Sistema de limitação de velocidade



Sistema SCADA

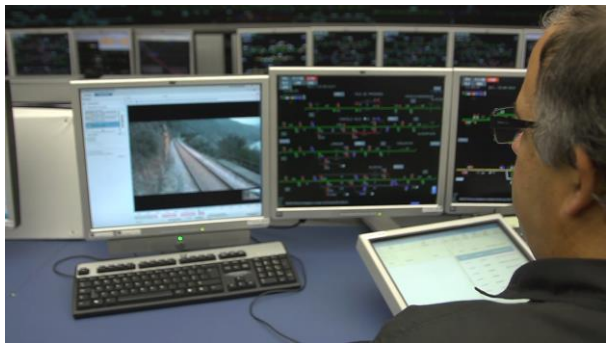
- Permite de uma forma centralizada, monitorizar e controlar em tempo real o funcionamento de diversos sistemas ferroviários
  - Supervisão Técnica de Infraestrutura
  - Telecomando de Energia
- Baseado numa arquitetura distribuída em três níveis distintos:
  - Aquisição (RTU);
  - Automação (PLC);
  - Aplicação (Servidores SCADA).

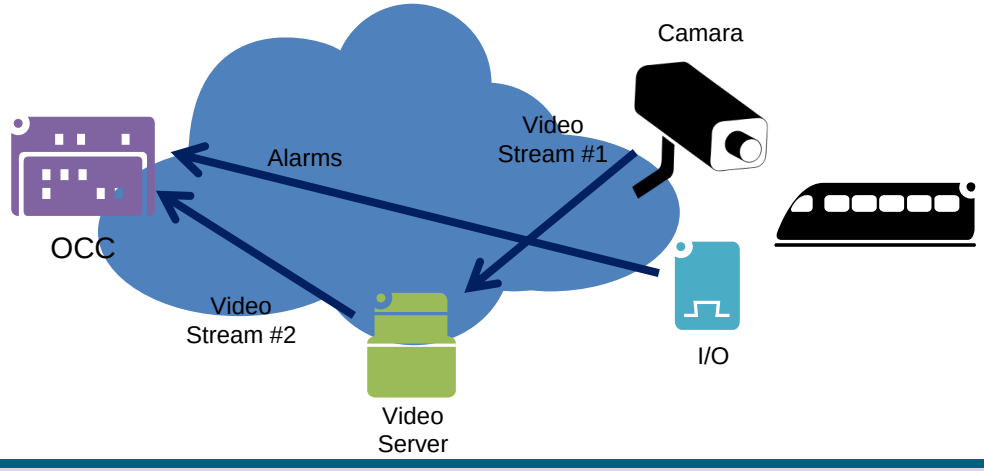
Sistema SCADA



Sistema de deteção de obstáculos

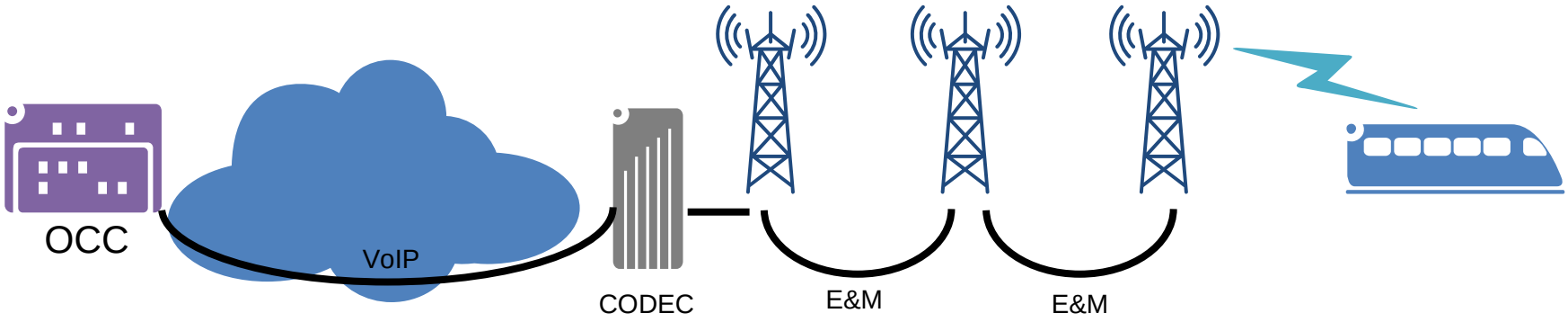
- Em zonas de risco de queda de rochas, permite a deteção de obstáculos na via;
- Recorre a fibras instaladas ao longo da via para deteção e geram um alarme;
- O sistema de videovigilância serve de auxilio, onde em caso de deteção o operador poderá requisitar visualizar a camara no local.





Sistema de Radio Solo Comboio

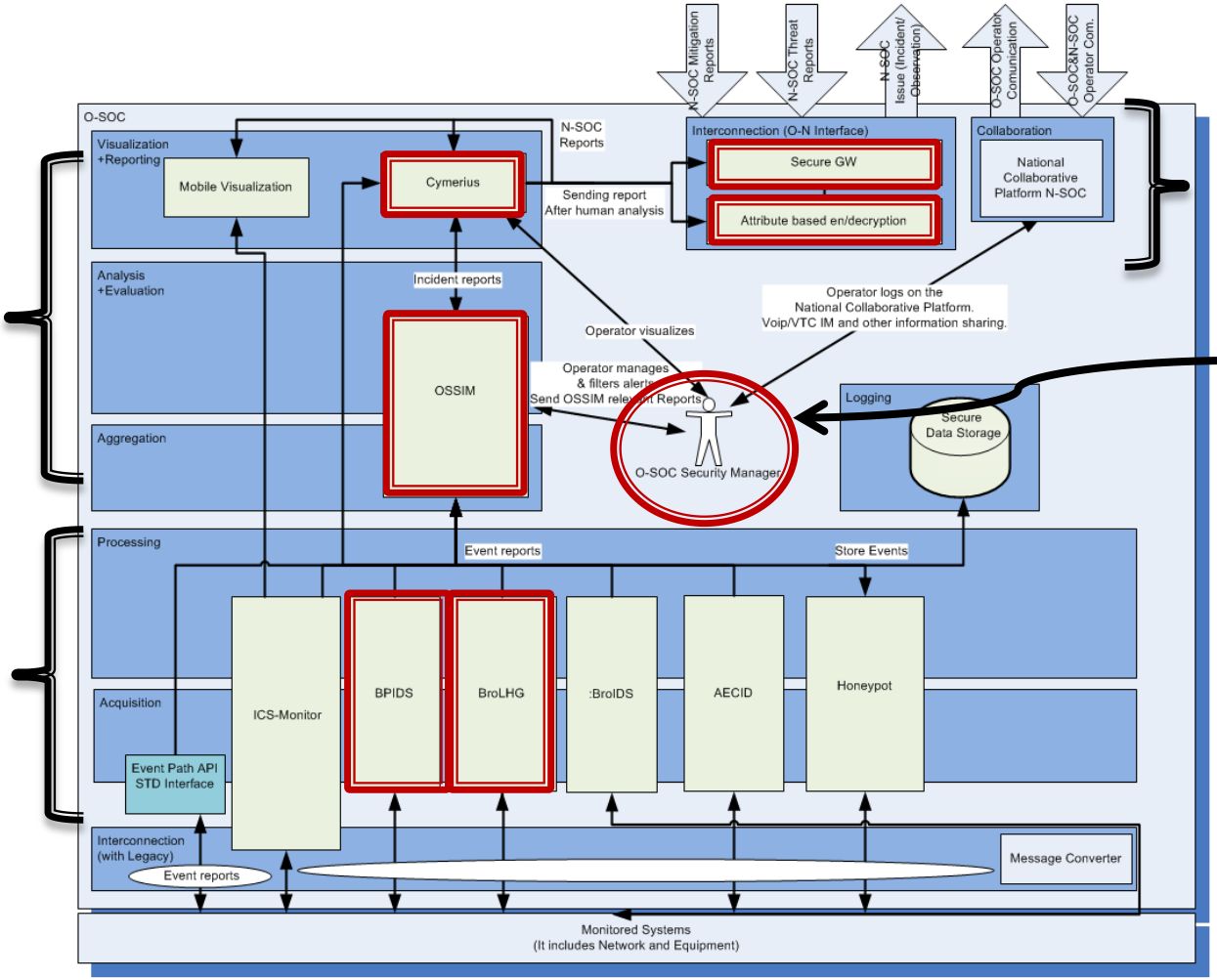
- Permite a comunicação entre o operador e o maquinista;
- Comunicação via radio analógico;
- Canais analógicos (E&M) são codificados em VoIP com G.711;
- Após codificação a comunicação é efetuada utilizando o protocolo Multicast entre o CCO e os comboios.



Componentes do ECOSSIAN demonstradas (O-SOC)

O-SOC supervision:
- OSSIM
- Cymerius

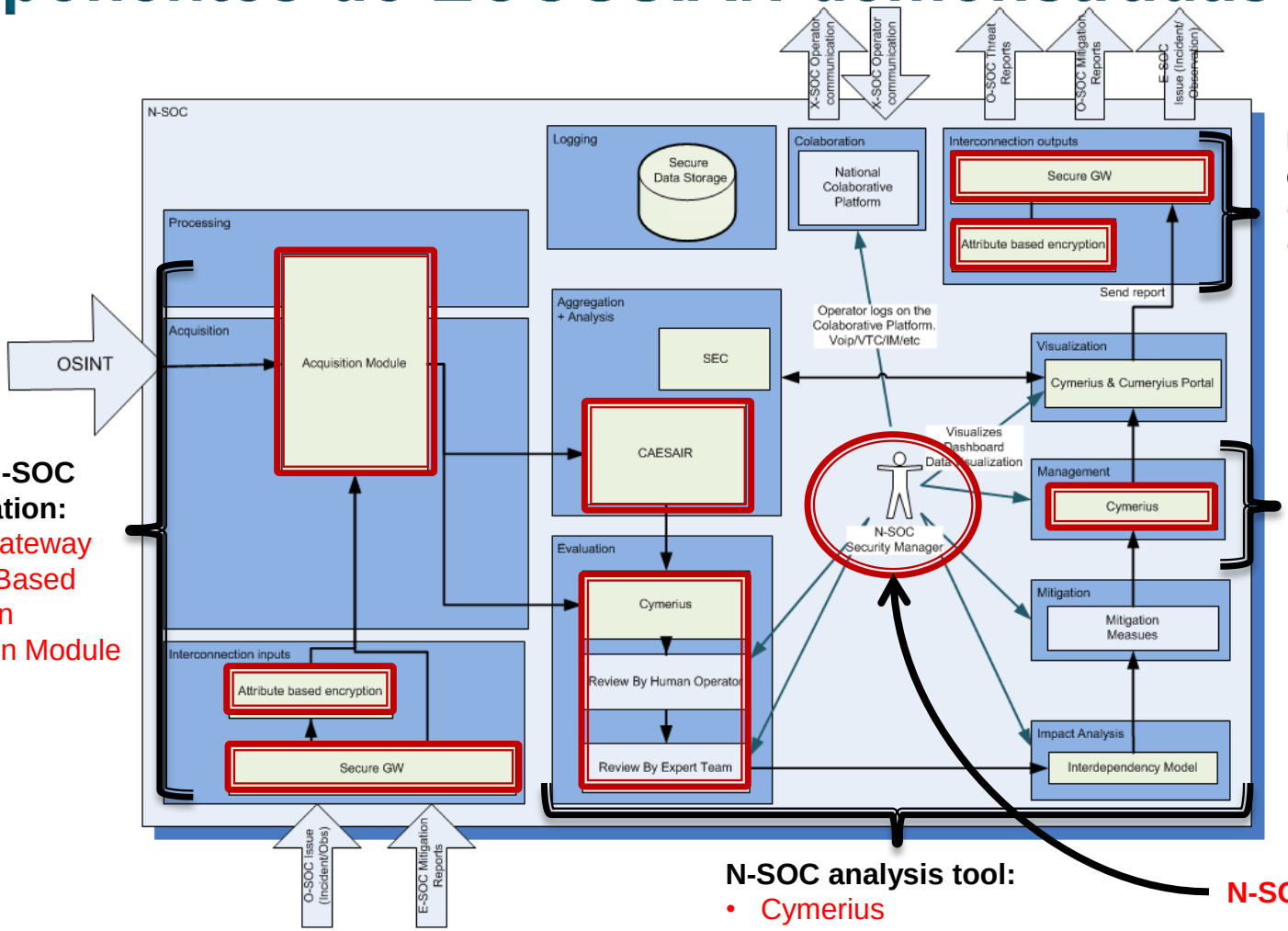
Sensors:
- BPIDS
- BroLHG



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

O-SOC operator

Componentes do ECOSSIAN demonstradas (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:
- Cymerius
- CAESAIR

N-SOC operator

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.

POLÍCIA JUDICIÁRIA

inov inesc • inovação

Infraestruturas de Portugal

IP Telecom

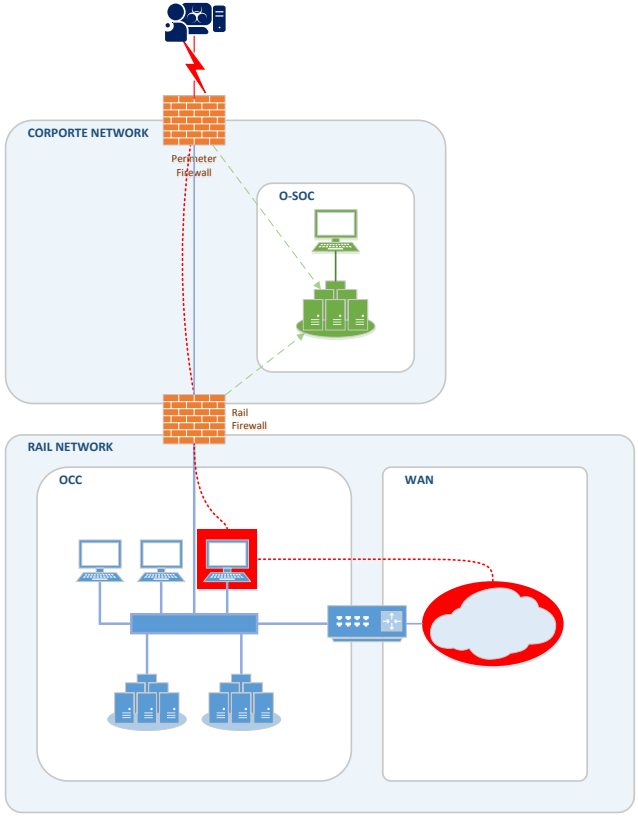
Demonstração Operacional

Fase 1: Intrusão na rede

European Control System Security Incident Analysis Network

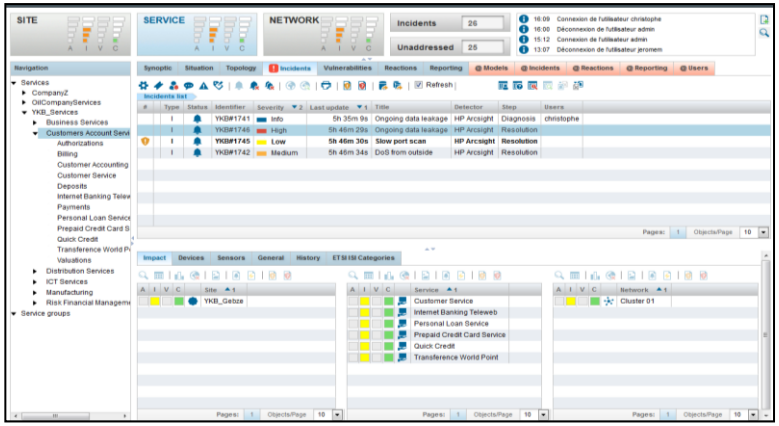
Introdução

- **Objetivo: Obter informação privilegiada dos sistemas a atacar**
- **Alvo: Máquina de Operação no CCO**
- **Método:**
  - **Engenharia Social para obter credenciais de uma VPN**
  - **Comprometer máquina no CCO**

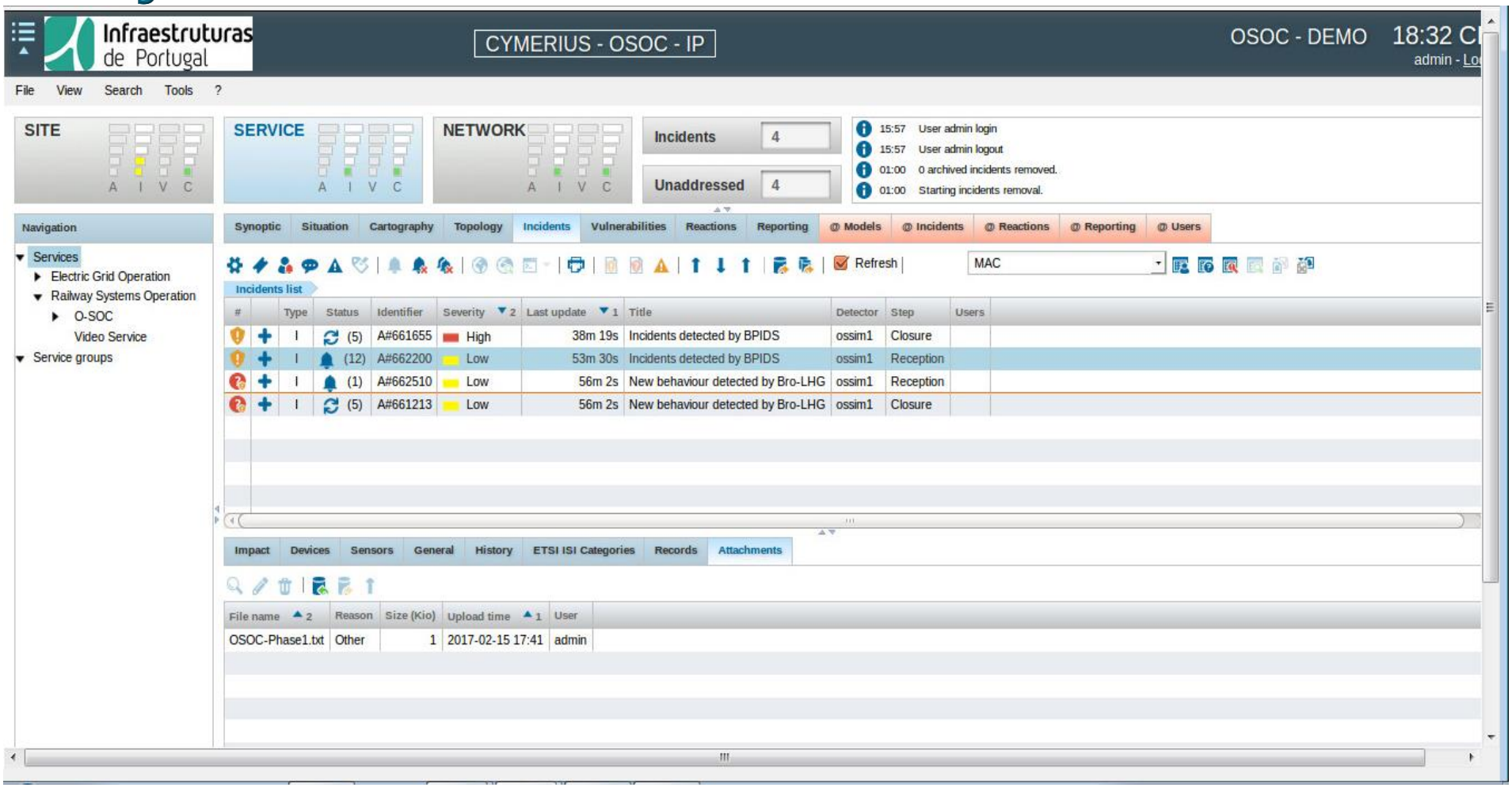


Cymerius

- Solução de “*Situation awareness*”
  - Avaliação de indicadores de Ciber segurança
  - Dashboards (mapas, evolução da situação, vista de incidentes)
- Suporte ao apoio à decisão
  - Análise automática do impacto dos incidentes com informação geolocalizada
  - Auxilio na mitigação de incidentes
  - Resolução passo-a-passo
    - *Guidelines*
  - Invocação remota de sistemas



Cymerius


Infraestruturas de Portugal
CYMERIUS - OSOC - IP
OSOC - DEMO
File View Search Tools ?
SITE
SERVICE
NETWORK
A I V C
Incidents 4
Unaddressed 4
15:57 User admin login
15:57 User admin logout
01:00 0 archived incidents removed.
01:00 Starting incidents removal.
Navigation
Services
Electric Grid Operation
Railway Systems Operation
O-SOC
Video Service
Service groups
Synoptic Situation Cartography Topology Incidents Vulnerabilities Reactions Reporting @ Models @ Incidents @ Reactions @ Reporting @ Users
Refresh
MAC
Incidents list
Type Status Identifier Severity Last update Title Detector Step Users
I (5) A#661655 High 38m 19s Incidents detected by BPIDS ossim1 Closure
I (12) A#662200 Low 53m 30s Incidents detected by BPIDS ossim1 Reception
I (1) A#662510 Low 56m 2s New behaviour detected by Bro-LHG ossim1 Reception
I (5) A#661213 Low 56m 2s New behaviour detected by Bro-LHG ossim1 Closure
Impact Devices Sensors General History ETSI ISI Categories Records Attachments
File name Reason Size (Kio) Upload time User
OSOC-Phase1.txt Other 1 2017-02-15 17:41 admin

Demonstração Operacional

Fase 2: Manipulação de limites de velocidade

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

POLÍCIA JUDICIÁRIA

inov inesc • inovação

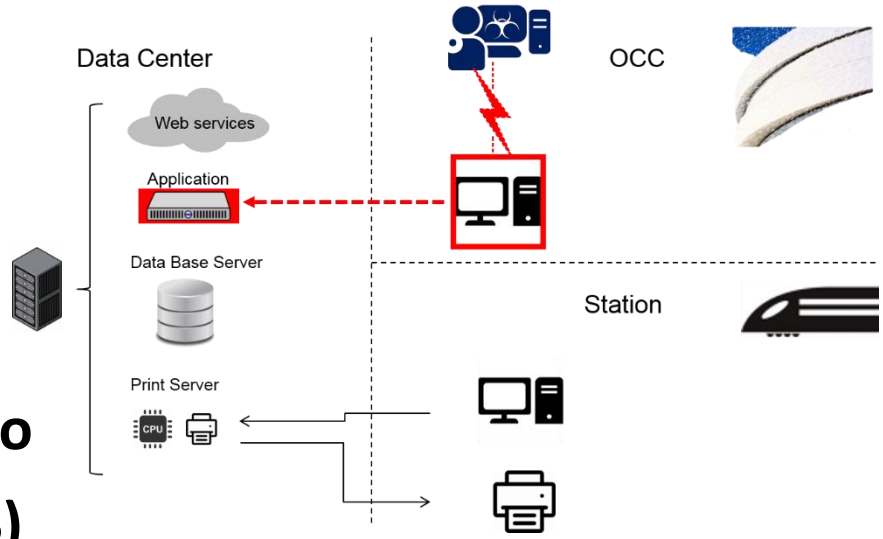
Infraestruturas de Portugal

IP Telecom

European Control System Security Incident Analysis Network

Introdução

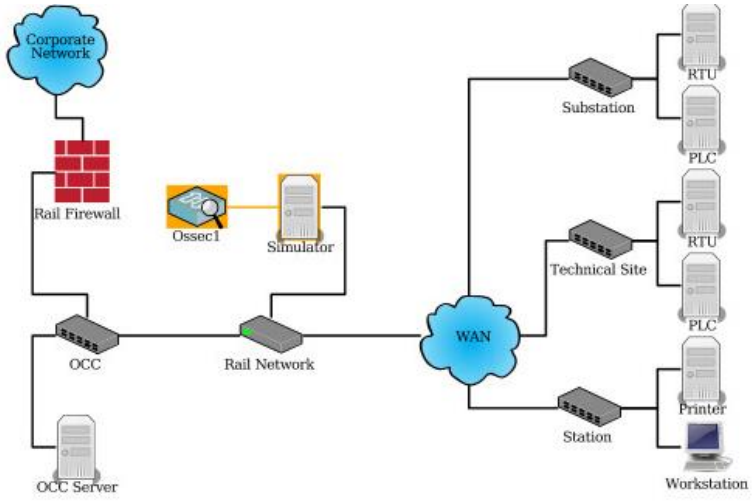
- **Objetivo: Emissão errónea de modelos de limite de velocidade**
- **Alvo: Sistema de Limitação de velocidade**
- **Método:**
  - **Comprometer servidor do sistema**
  - **Adulterar dados da aplicação**
    - **Número de comboio**
    - **Estação**
- **Deteção: Verificação do processo de emissão dos modelos (BPIDS)**

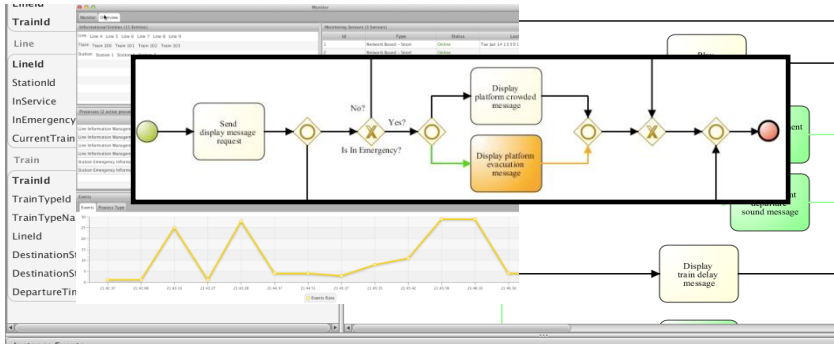


BPIDS

Sistema de deteção de intrusões baseado em especificações dos processos de negócio:

- Deteta desvios ou inconformidades dos processos críticos de negócio definidos:
  - Entrada: Aquisição em tempo de real de pacotes de rede capturados passivamente por sensores existentes. Ou estado interno de sistemas (ficheiros de log, etc.). Estes eventos são posteriormente mapeados em atividades.
  - Saída: Análise dos desvios :
    - Informação contextual indicando qual o processo de negócio onde o desvio ocorreu (Sistemas envolvidos, histórico de execução, atividades do processo esperadas, etc.)

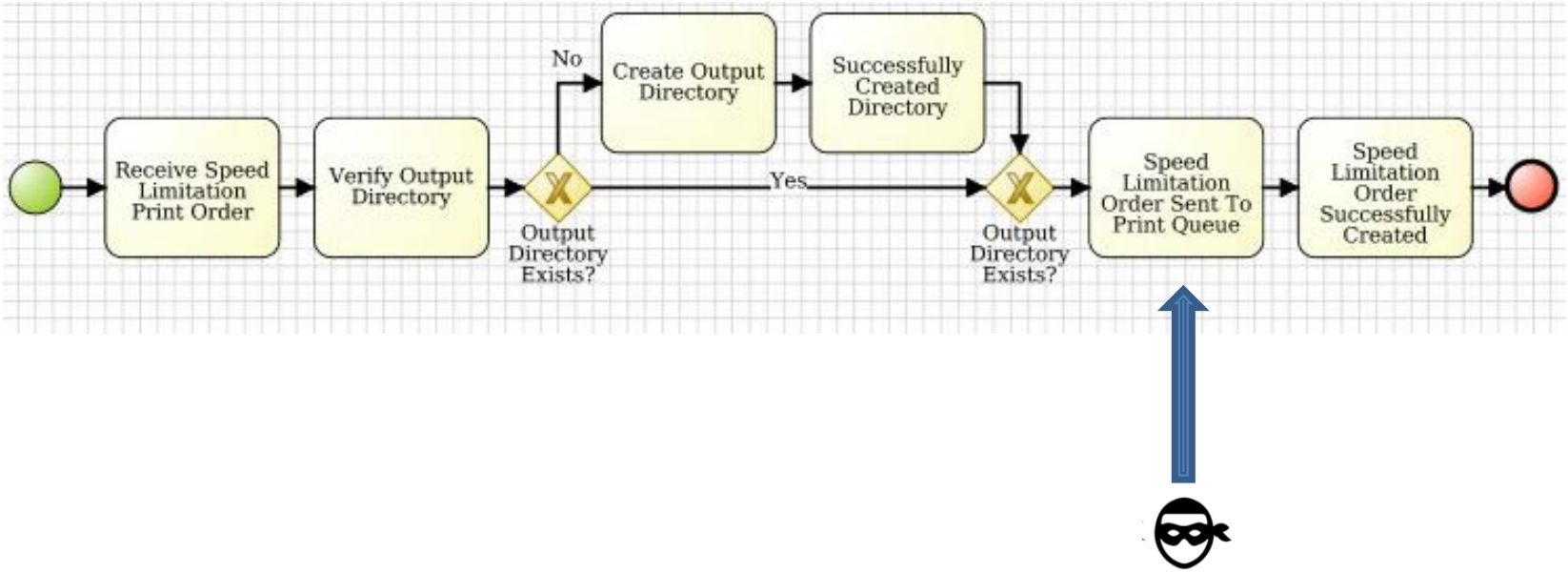




Sensor – Business Process IDS

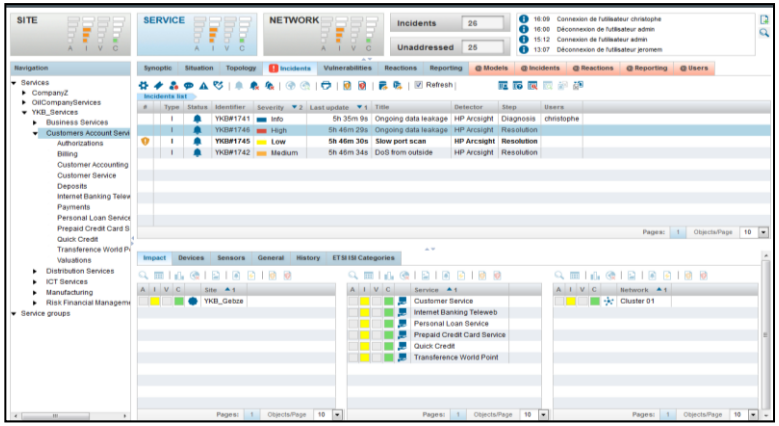
Deteção do Ataque:

1. O BPIDS irá verificar que o processo de emissão do documento de Limitação de Velocidade ocorrido na estação foi forjado ao analisar que os números dos comboios e estação não correspondem os modelos emitidos.



Cymerius

- Situation awareness solution
  - Avaliação de indicadores de Ciber segurança
  - Dashboards (mapas, evolução da situação, vista de incidentes)
- Suporte ao apoio à decisão
  - Análise automática do impacto dos incidentes com informação geolocalizada
  - Auxilio na mitigação de incidentes
  - Resolução passo-a-passo
  - Guidelines
  - Invocação remota de sistemas



Demonstração Operacional

Fase 3: Ataque aos sistemas SCADA

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

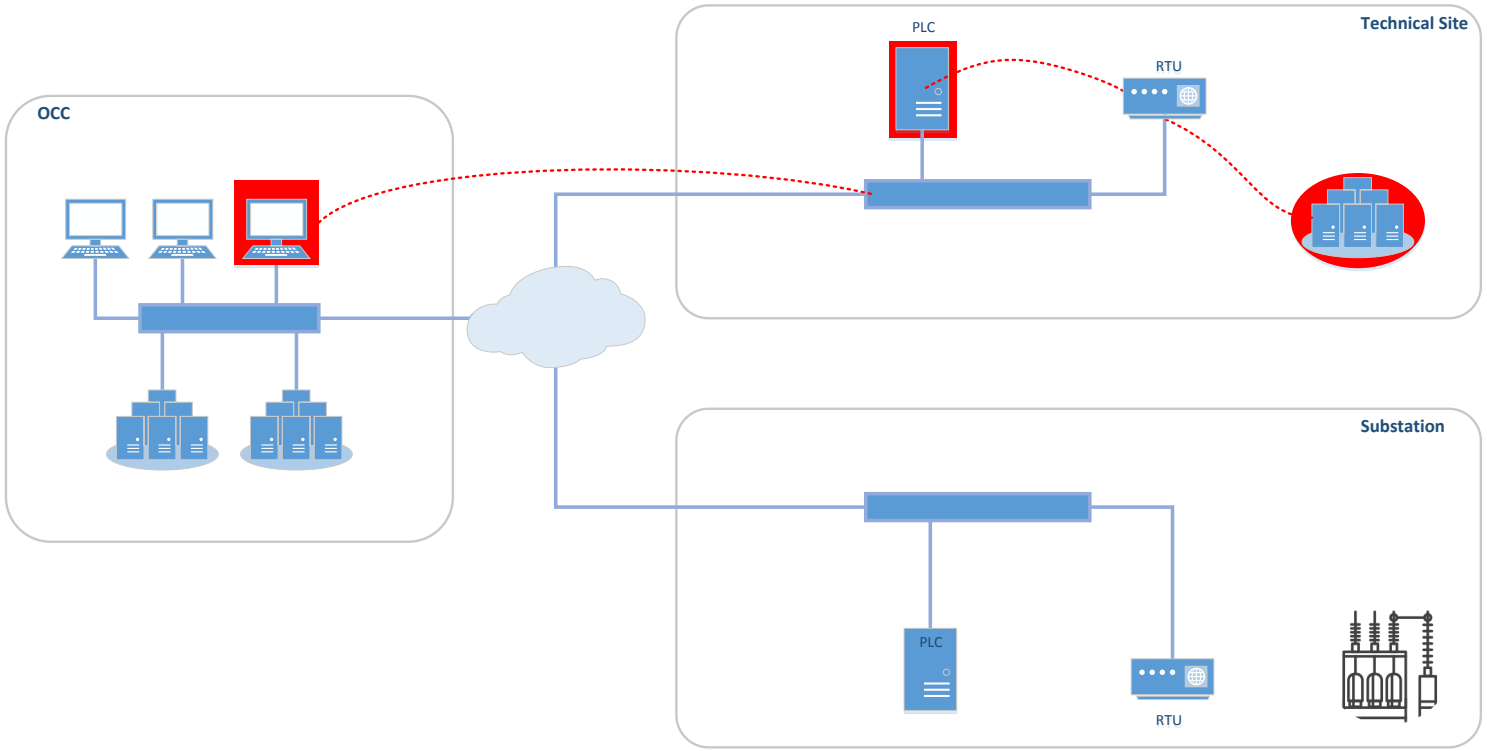
European Control System Security Incident Analysis Network

Introdução

- **Objetivo: Execução de comandos SCADA a nível local sem perceção do CCO**
- **Alvo: Sistemas SCADA - Supervisão Técnica de Infraestruturas e Telecomando de Energia;**

- **Método:**
  - **Comprometimento de máquina SCADA (PLC)**
  - **Execução de comandos (abertura de disjuntores e seccionadores)**
  - **Omissão de Logs para o CCO**
- **Deteção:**
  - **Observação de trafego anómalo (BroLHG)**
  - **Verificação do processo de execução de comandos SCADA (BPIDS)**

Cenário de Ataque - Supervisão Técnica de Infraestruturas



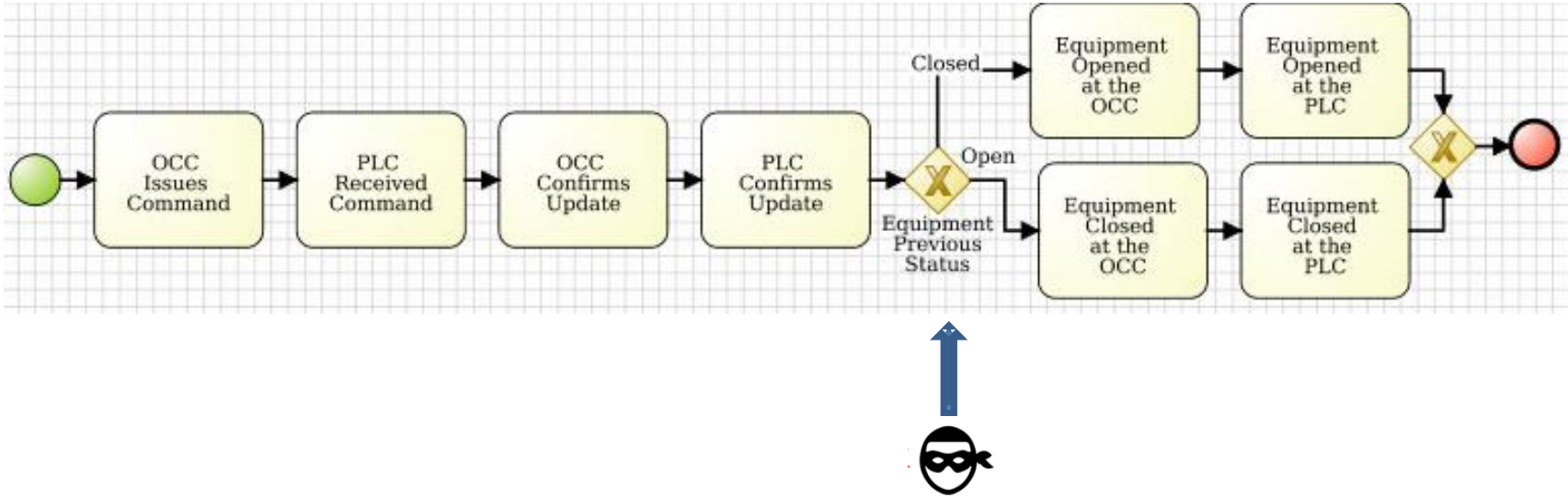
Sensor BroLHG – Deteção de alterações no comportamento da rede

- Analisa o comportamento de sistemas (identificados pelo endereço MAC, IP ou uma combinação destes dois)
- Comportamentos como:
  - Serviços ativos (portos) disponibilizados
  - Serviços usados (portos)
  - Ligações para outros sistemas dentro da mesma LAN
- Permite um mapeamento de alto nível usando poucos recursos computacionais
- Funciona melhor em redes fechadas (etc. redes de controlo industrial), onde as alterações de comportamento são raras
- Deteta alterações causadas por:
  - Varredura de portos (port scanning)
  - Utilização não autorizada de recursos na rede
  - Aparecimento de novos serviços (etc. canais de controlo de bots e ataques leapfrog)
  - Hardware não autorizado
- BroLHG complementa um sistema de monitorização de rede BRO

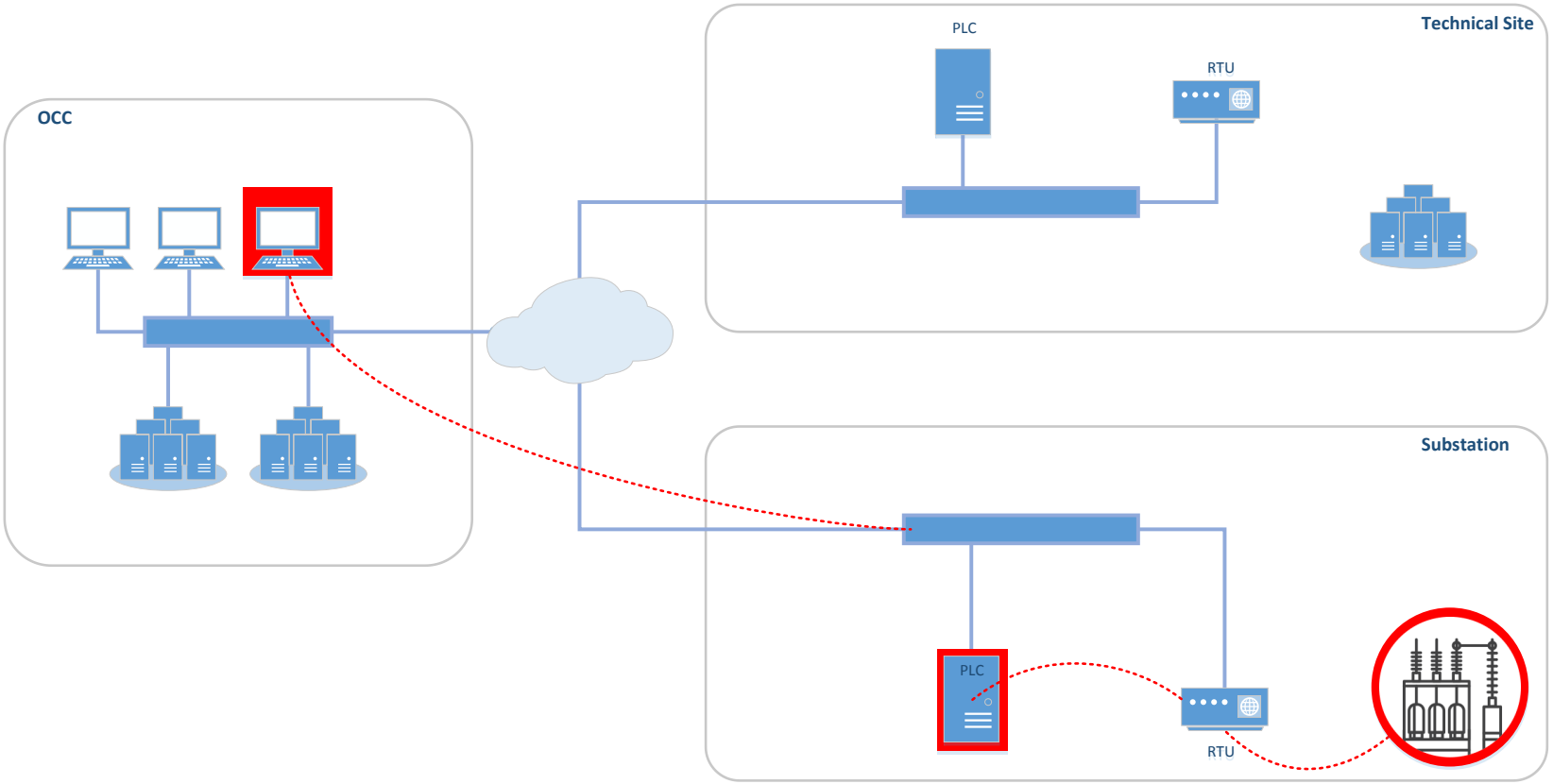
Sensor – Business Process IDS

Deteção do Ataque:

- O BPIDS irá verificar se a execução de comandos SCADA através dos PLC tiveram origem no SCADA Server **– abertura de disjuntor** de uma sala técnica remota



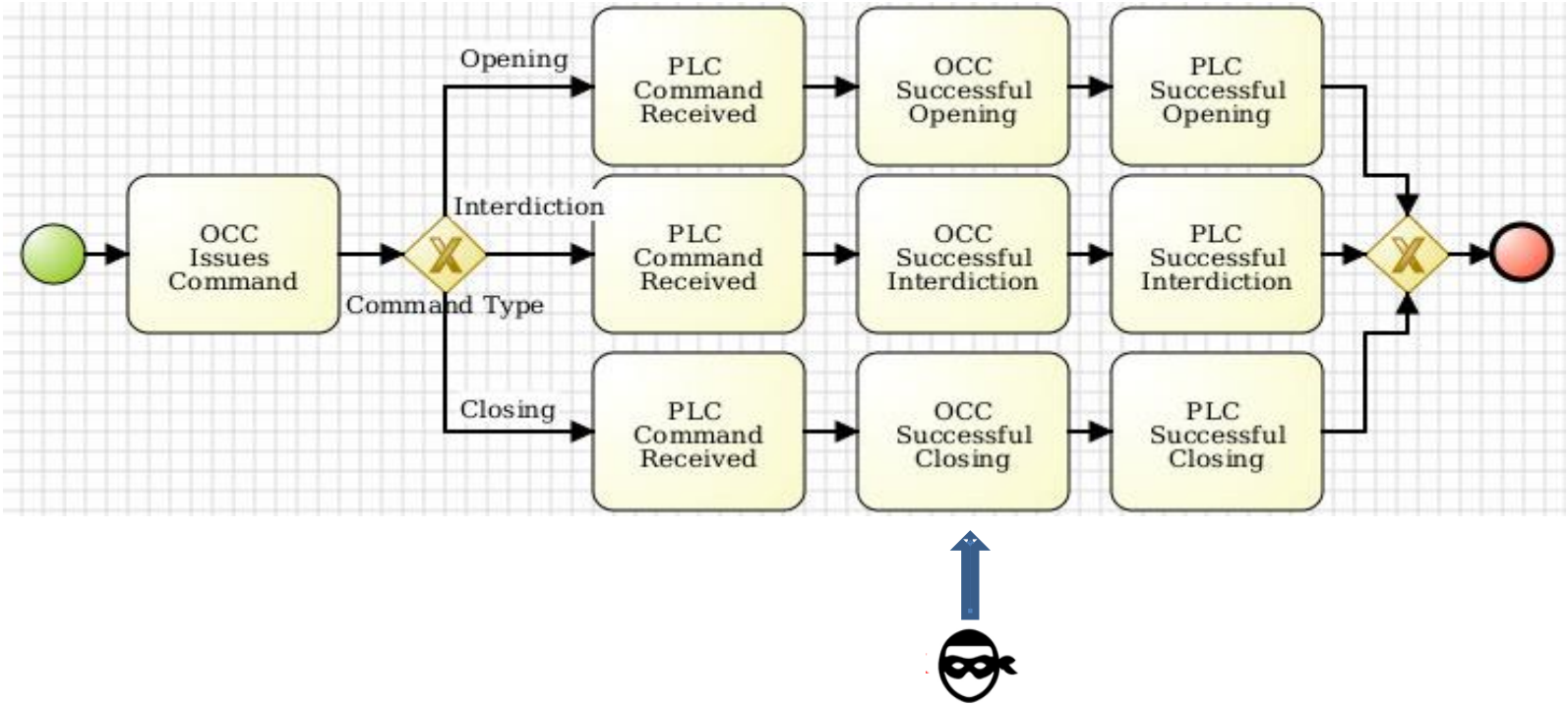
Cenário de Ataque - Telecomando de Energia



Sensor – Business Process IDS

Deteção do Ataque:

- O BPIDS irá verificar se a execução de comandos SCADA através dos PLC tiveram origem no SCADA Server – **abertura de seccionador de catenária de energia**



Demonstração Operacional

Fase 4: Sequestro de comboio

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

POLÍCIA JUDICIÁRIA

inov inesc • inovação

Infraestruturas de Portugal

IP Telecom

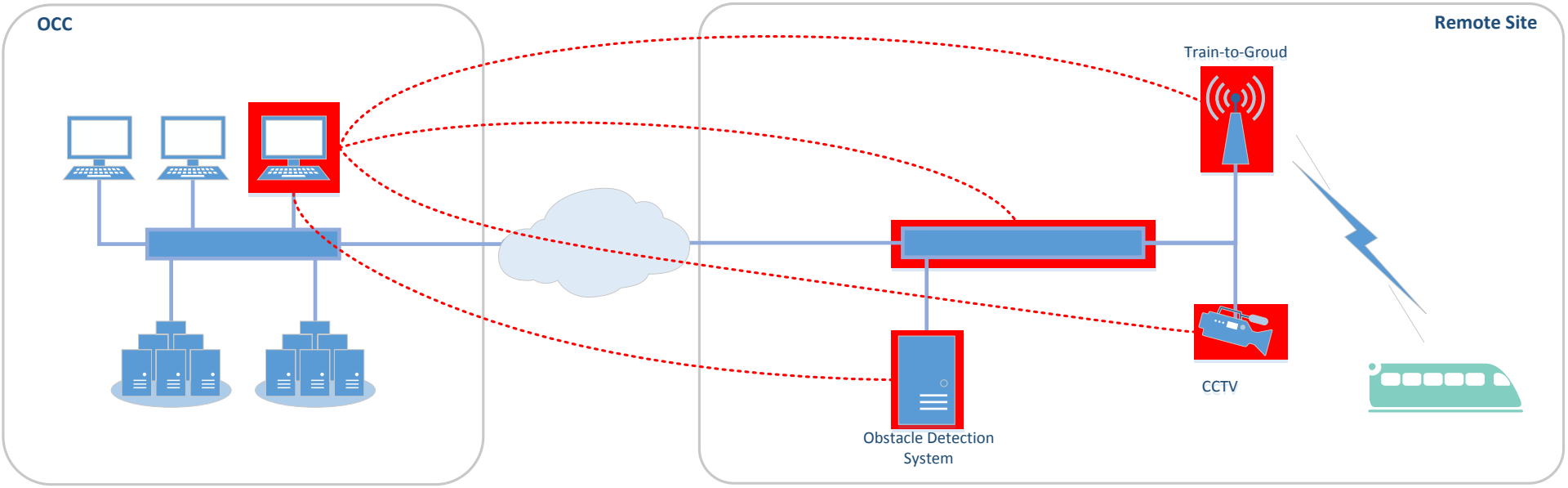
European Control System Security Incident Analysis Network

Introdução

- **Objetivo: Paragem de um comboio especifico**
- **Alvo: Sistema de Deteção de Obstáculos**
- **Método:**
  - **Comprometimento de máquina do CCO e switch**
  - **DoS do Sistema de Videovigilância**
  - **Injeção de alarmes no Sistema de Deteção de Obstáculos**
  - **DoS do Sistema de Radio Solo Comboio**

- **Deteção:**
  - **Observação de trafego anómalo (BroLHG)**
  - **Verificação do processo de deteção de obstáculos (BPIDS)**

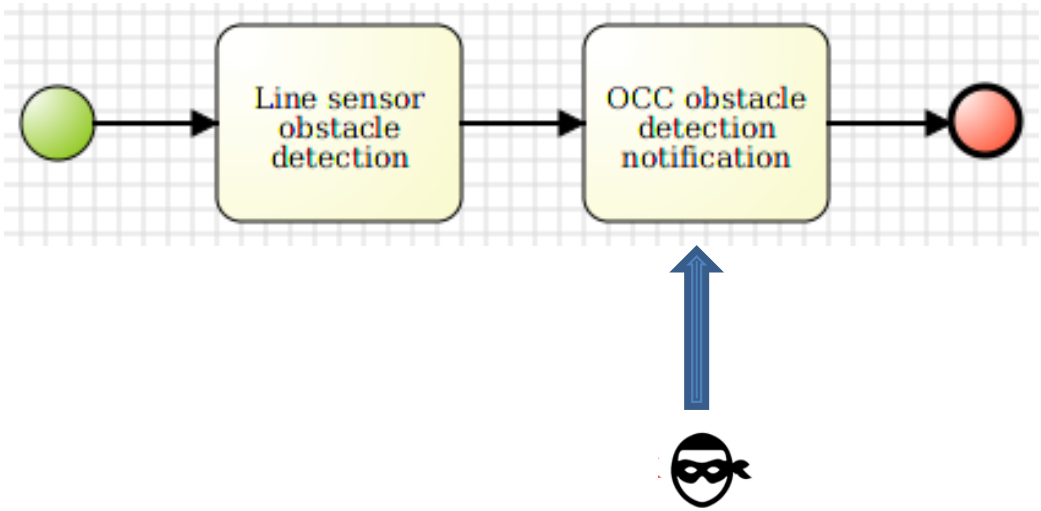
Cenário de Ataque



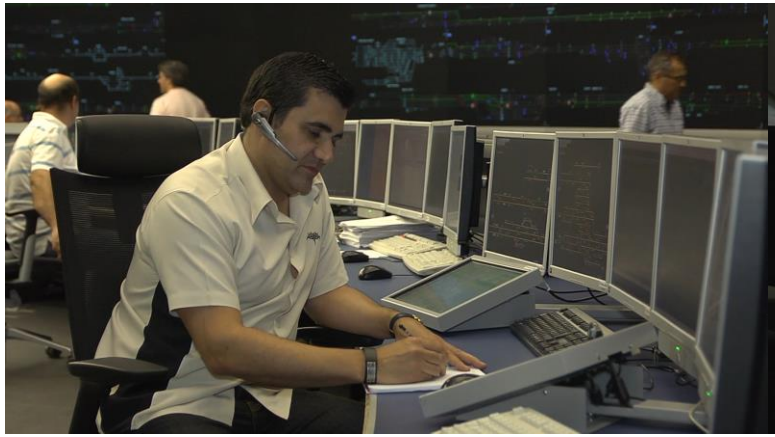
Sensor – Business Process IDS

Deteção do Ataque:

- O BPIDS irá verificar que o centro de controlo (CCO) recebeu um **alarme** indicando a presença de um obstáculo na via sem que este tivesse origem no sensor local.



Comunicação radio e paragem de comboio



Paragem de comboio

Ecossian

Demonstração Operacional

Partilha de informação para o N-SOC

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

POLÍCIA JUDICIÁRIA

inov inesc • inovação

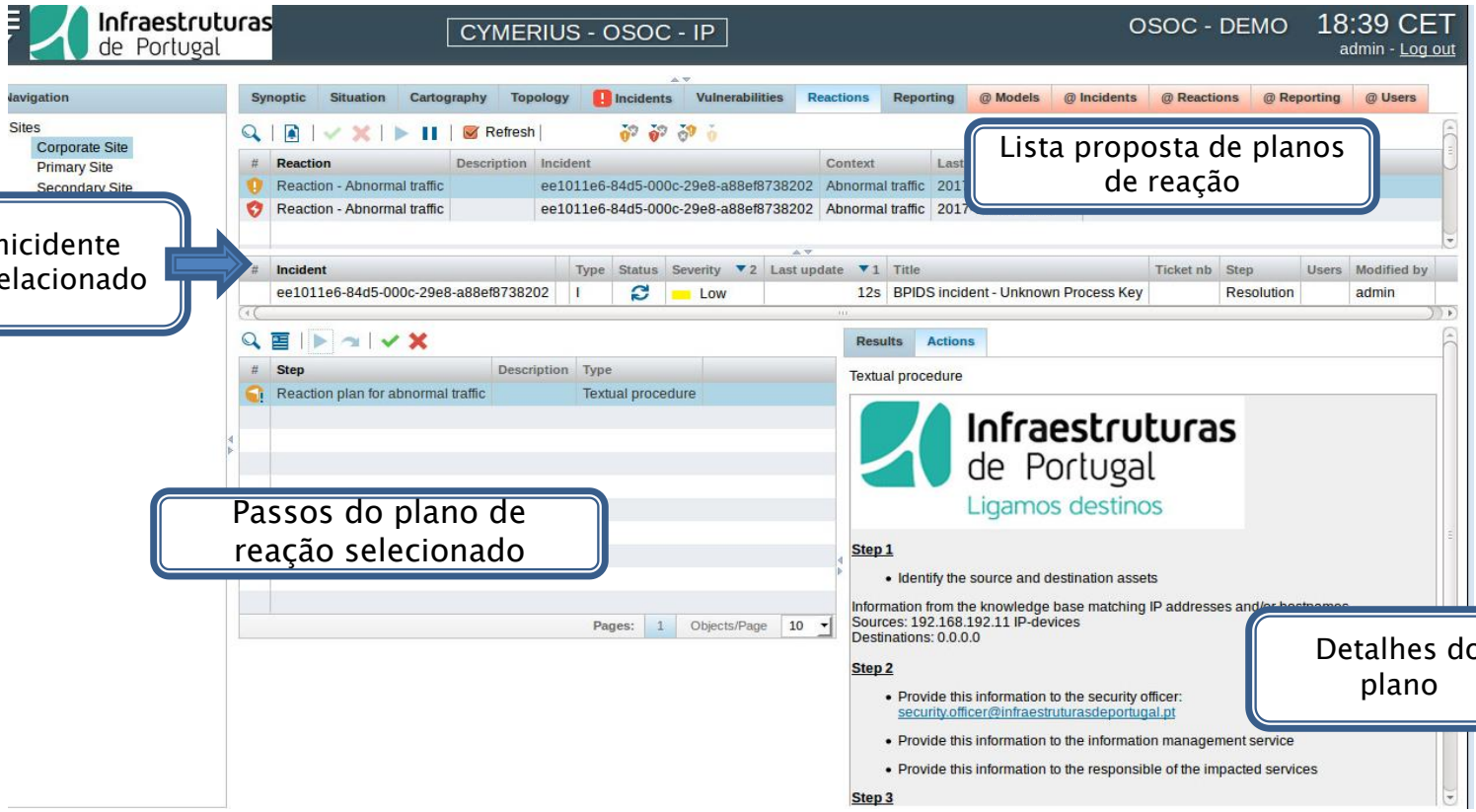
Infraestruturas de Portugal

IP Telecom

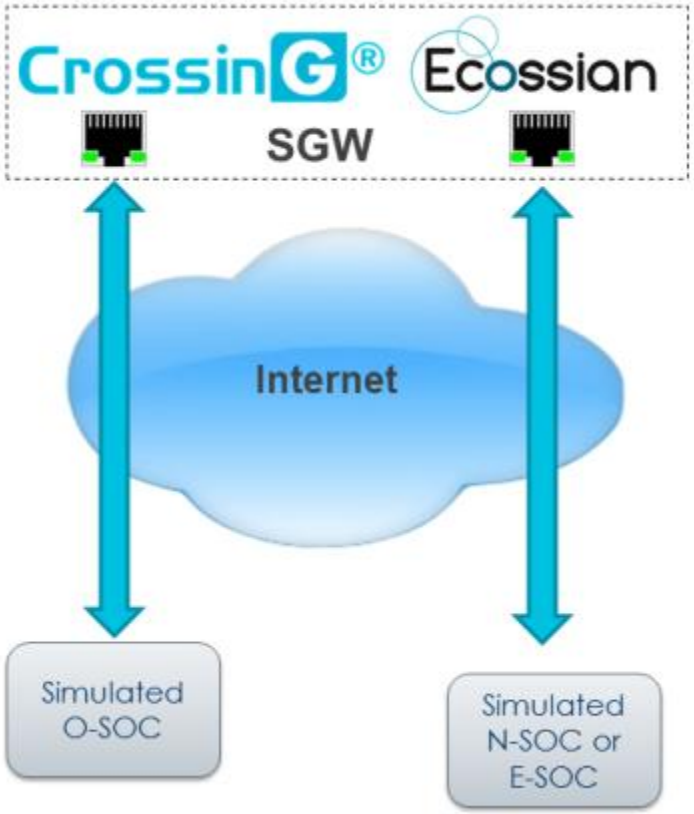
European Control System Security Incident Analysis Network

Cymerius - reação

O Cymerius analisa o conteúdo do incidente, pesquisa se existem contextos de reação aplicáveis e propõe medidas/ações corretivas incluindo procedimentos e execução de comandos remotos (e.g., data collection, alterações de blacklist, criação de tickets, etc)



O-SOC para N-SOC: reencaminhamento de incidentes



Gateway Segura (SGW)

- Interface encapsuladora
- Canal de informação unidirecional
- Verificação de Vírus e software malicioso
- Verificação segura de etiquetas (labels)
- Registo de eventos (logging)
- Anonimização garantida pelo módulo de encapsulamento
- Todas as mensagens enviadas a partir de um SOC tem que ser **aprovadas por um gestor do SOC**

Cifra de Atributos (Attribute-Based Encryption)

ABE – Cifra de atributos

- Providencia um mecanismo de confidencialidade na partilha de informação
- **Controlo de acessos criptográfico**: o desenho da cifra e decifra de uma mensagem é baseada num conjunto selecionado de atributos no momento em que esta é enviada através da SGW – Gateway Segura

Definição de Atributos

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

Formulação de Politicas de Acesso

Policy: ((“NSOC” AND “PT” AND “Transportation”) OR (“TLP-Red”))

Cifra Parcial da Mensagem

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

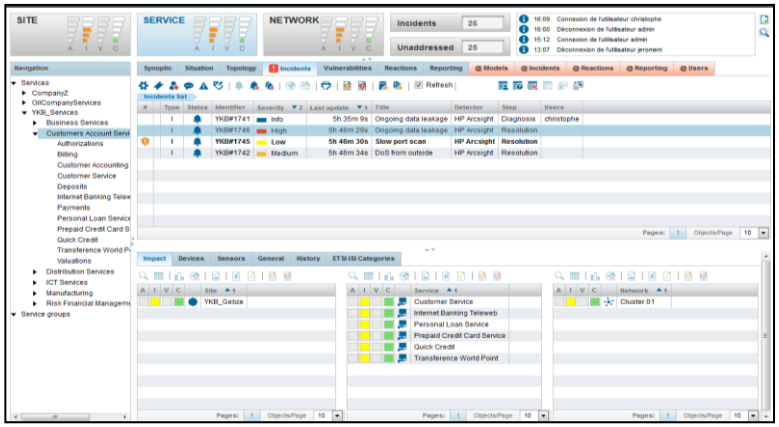
Acquisition module

Recolhe dados reportados pelos O-SOC e por fontes publicas, guarda-os temporariamente e disponibiliza-os para as componentes de análise.

É compatível com os formatos e protocolos usados e assumidos pela indústria em incidentes de cyber segurança e partilha de informações de ameaças.

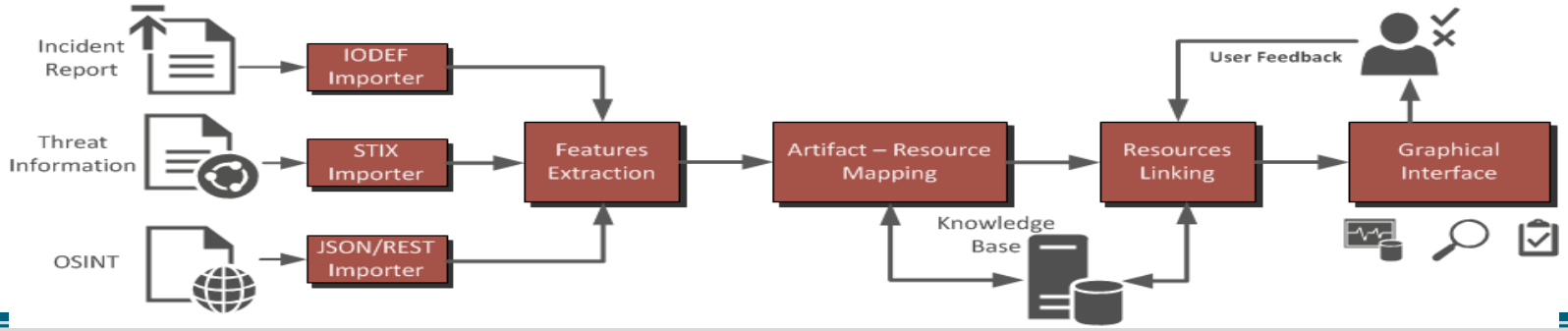
Cymerius – Nível N-SOC

- Mantém os propósitos:
  - Situation awareness solution
  - Suporte ao apoio à decisão
- Visualização distinta:
  - Monitorização de diferentes IC
  - Recebimento de informação básica sobre incidentes
  - Capacidade de comunicação com o O-SOC para:
    - Comunicação expontânea resultante de incidentes recebidos
    - Recolha de informação adicional perante o operador
    - Resposta com informação avancada – potenciada pelo componente **CÆSAIR**



CÆSAIR

- Desenho e desenvolvimento do **CAESAIR**: Um motor de análise colaborativa para respostas a incidentes e visão situacional
  - Desenhado para uma investigação mais profunda de relatórios de incidentes que não são suportados pelo Cymerius.
  - Importação automática de fontes de cyber segurança (CVEs, TI) de forma a criar uma base de dados de conhecimento
  - Automaticamente descobre novas fontes relacionadas e complementa as capacidade de pesquisa humana
  - A sua aplicação no ECOSSIAN:
    - Auxilia o operador do N-SOC em tarefas avançadas de análise
    - Utilização de formatos padrão conhecidos (STIX para ameaças, IODEF para incidentes, CVEs & CPEs, etc.)
    - Suporta mais de ~100k incidentes e relatórios
    - Efetua (quase) em tempo real associações de artefactos (correlação)



Ecossian

Demonstração Operacional

Partilha de informação para o O-SOC

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

POLÍCIA JUDICIÁRIA

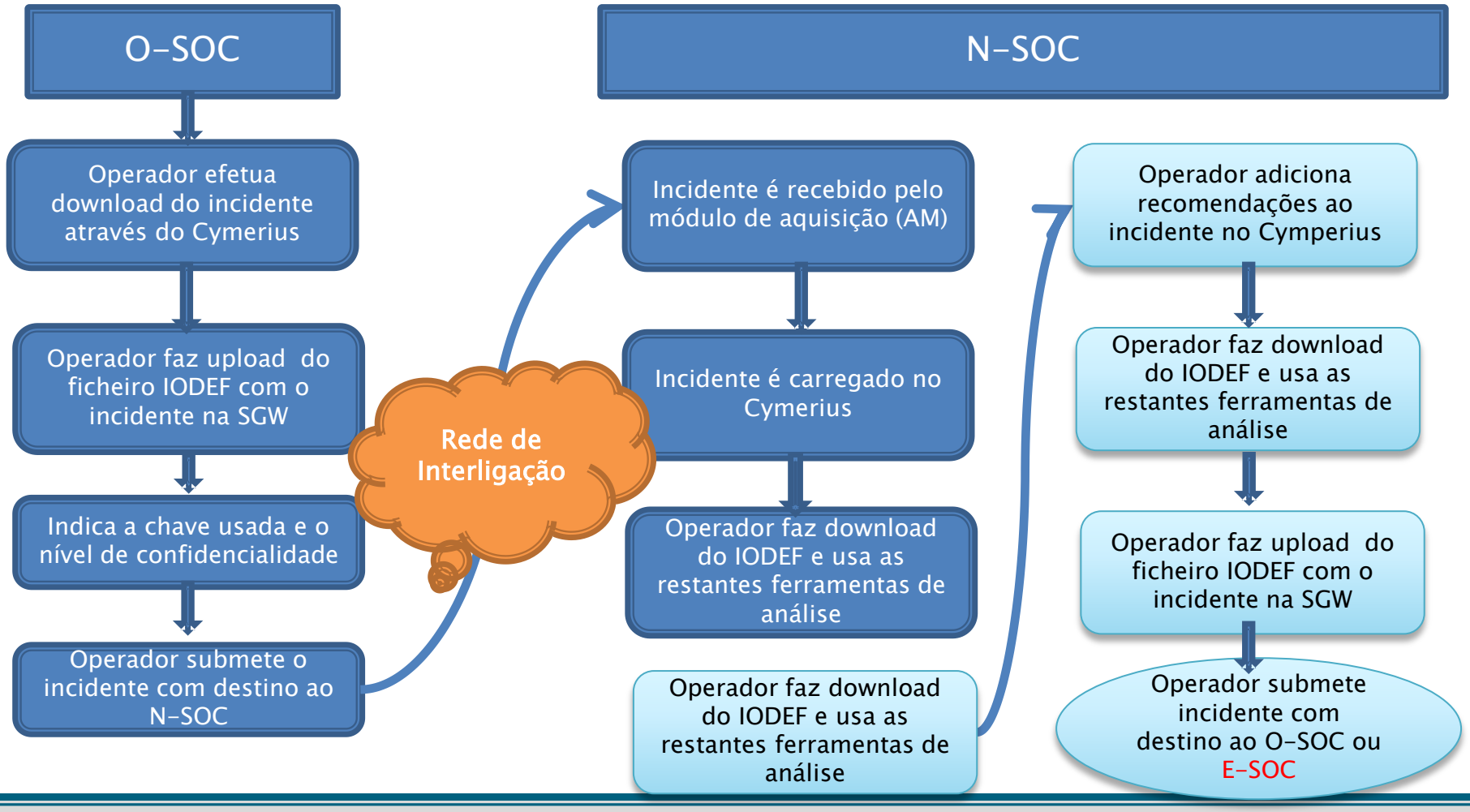
inov inesc • inovação

Infraestruturas de Portugal

IP Telecom

European Control System Security Incident Analysis Network

Partilha de informação para o O-SOC



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.

Infraestruturas de Portugal

IP Telecom

POLÍCIA JUDICIÁRIA

inov inesc • inovação

Demonstração Operacional

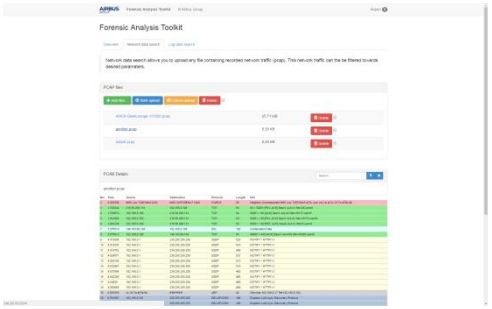
Análise Forense

European Control System Security Incident Analysis Network

Intervenção de Law Enforcement

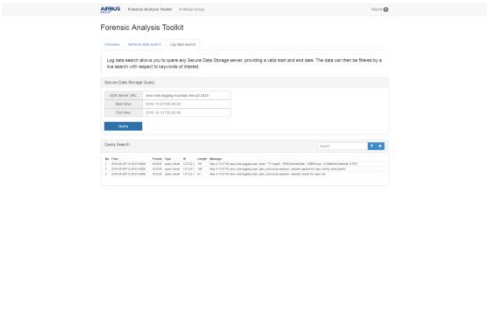
- As características do incidente sofrido implicam a chamada de intervenção das autoridades policiais competentes;
- Entre as diligências desencadeadas de imediato, ocorre também a deslocação de meios às instalações da IP para recolha de informação;
- Todos os elementos passíveis de recolha serão analisados, designadamente os registos de comunicações eletrónicas, vector usado para a consumação dos ataques;
- Nesta análise assumem relevo:
  - Ficheiros de análise de tráfego (PCAP)
  - Registos dos sensores, armazenados no componente SDS e lidos através do Forensic Toolkit

Forensic Toolkit



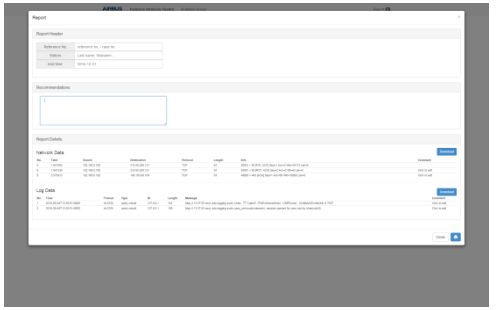
- Carregamento de PCAPs
- Resumo dos pacotes
- Visão detalhada de pacotes
- Camada ISO/OSI
- Aplicação de filtros
  - Origem, Destino, Segmento
  - Porto, Protocolo etc.
- Drag&Drop de evidências para o relatório

Network data analysis



- Questionar o SDS (base de dados cifrada com controlo de integridade)
- Selecionar a origem & Intervalo de tempo
- Pesquisa em tempo real
- Drag&Drop de evidências para o relatório

Log data analysis



- Geração do relatório tendo em conta evidências recolhidas
- Adicionar meta dados
- Adicionar comentários
- Adicionar recomendações
- Impressão do relatório
- Exportação de dados em formato CSV

Report Generation

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.

POLÍCIA JUDICIÁRIA

INOV inesc • inovação

Infraestruturas de Portugal

IP Telecom

Demonstração Operacional

Cooperação Europeia

European Control System Security Incident Analysis Network

Conclusão 1/2

Uma arquitetura para um sistema pan-europeu de cooperação e gestão de ameaças, de alertas precoces e providenciando uma visão global:

- Colaboração transfronteiriça e transectorial
  - Através da rede estabelecida de SOC (Operadores Locais, Centros Nacionais e Centro Europeu).
- Preservando o anonimato e a privacidade (confidencialidade) para todos os membros
  - Através da Gateway Segura e o módulo de encapsulamento de atributos
- Partilha de informação segura e uma plataforma colaborativa que respeita a legislação em vigor entre outros requisitos
  - Através do OSSIM e Cymerius®
- Deteção quase em tempo real de ataques informáticos
  - Através dos sensores existente: BPIDS, BroLHG entre outros desenvolvidos no seio do projecto
- Tecnologias e processos para monitorização e deteção de ameaças/incidentes
  - O Workflow forçado pelas ferramentas Cymerius e OSSIM em conjungação com os restantes sensores

Conclusão 2/2

- Análise de dados, agregação, correlação e visualização
  - **Através do OSSIM e Cymerius**
- Mitigação de ataques, análise de impactos e gestão de incidentes
  - Através das ferramentas de análise forense disponibilizadas às entidades policias competentes
- Avaliação das condições regulamentares, sociais e económicas
  - **Garantido pela anonimização e pela aprovação de gestores superiores**
- Modelo de *governance* em discussão
- **Demonstração final pan-europeia em Paris em Abril de 2017**
- **Projeto conclui-se em Maio de 2017 com a avaliação da plataforma desenvolvida**

ECOSSIAN Grant Agreement No. 607577

"The **ECOSSIAN** project has received funding from the European Union's Seventh Framework Programme ([FP7/2007-2013]) under grant agreement number SEC-607577."

If you need further information, please contact the coordinator:
TECHNIKON Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a, 9500 Villach, AUSTRIA
Tel: +43 4242 233 55 Fax: +43 4242 233 55 77
E-Mail: coordination@ecossian.eu