Fator Humano na Proteção das IIC

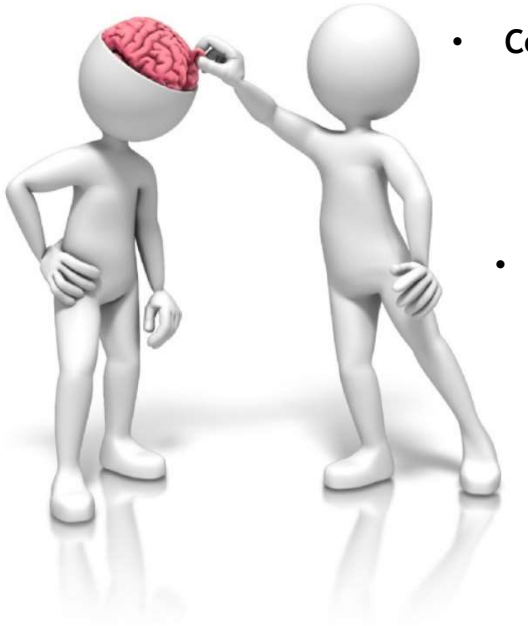
SOC; Exercícios e CyberRange EDP

Fator Humano na Proteção das IIC
Contexto

Prevenção

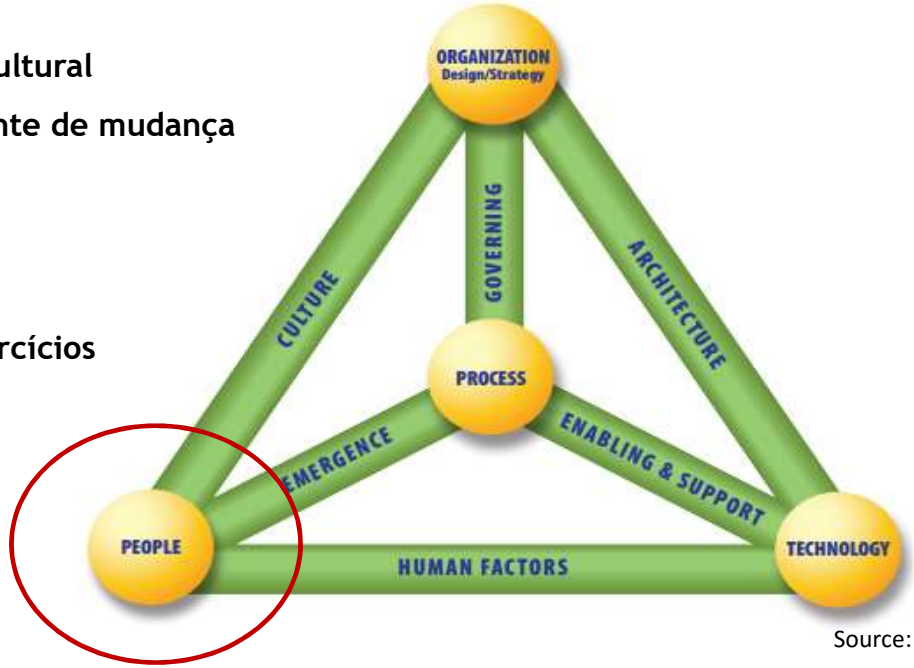
Deteção

Resposta



- Transformação cultural
- Colaborador agente de mudança

- Equipas e Exercícios

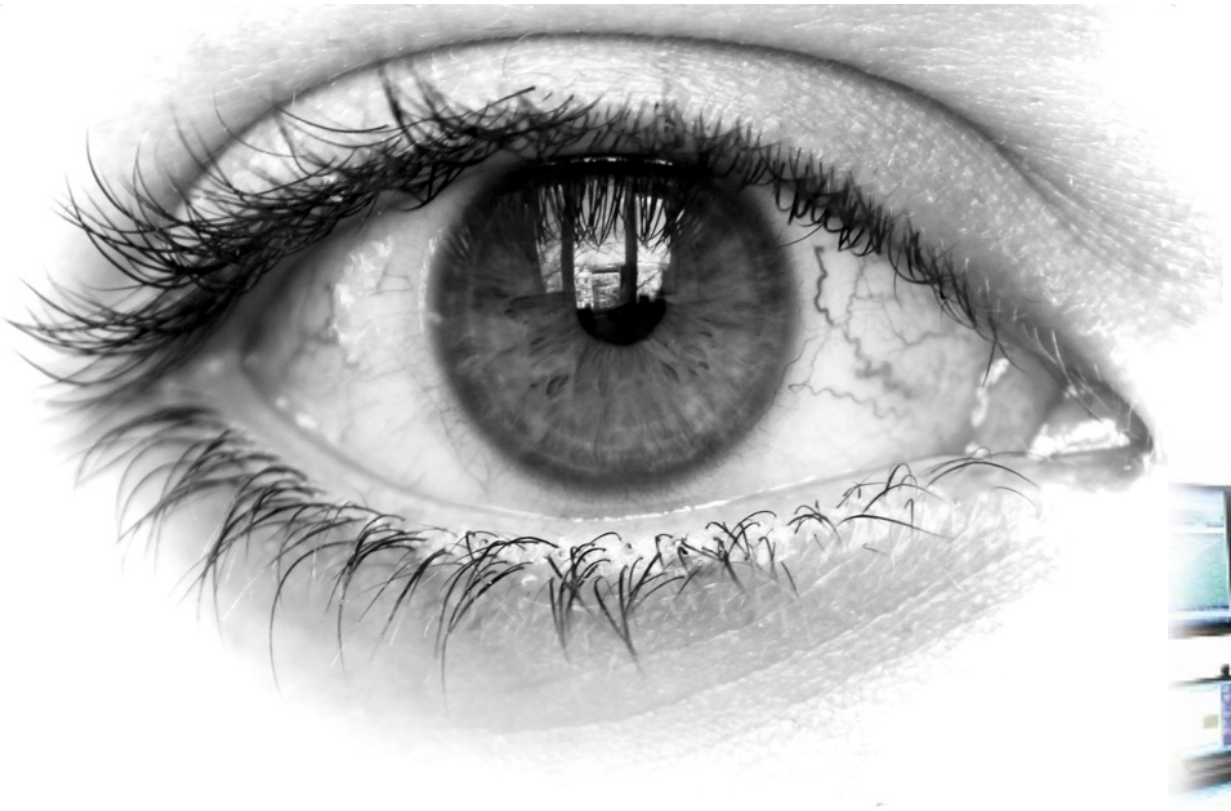


Source: ISACA

- Competências tecnológicas (ex: SIEM)
- Conhecimento do Contexto de Negócio

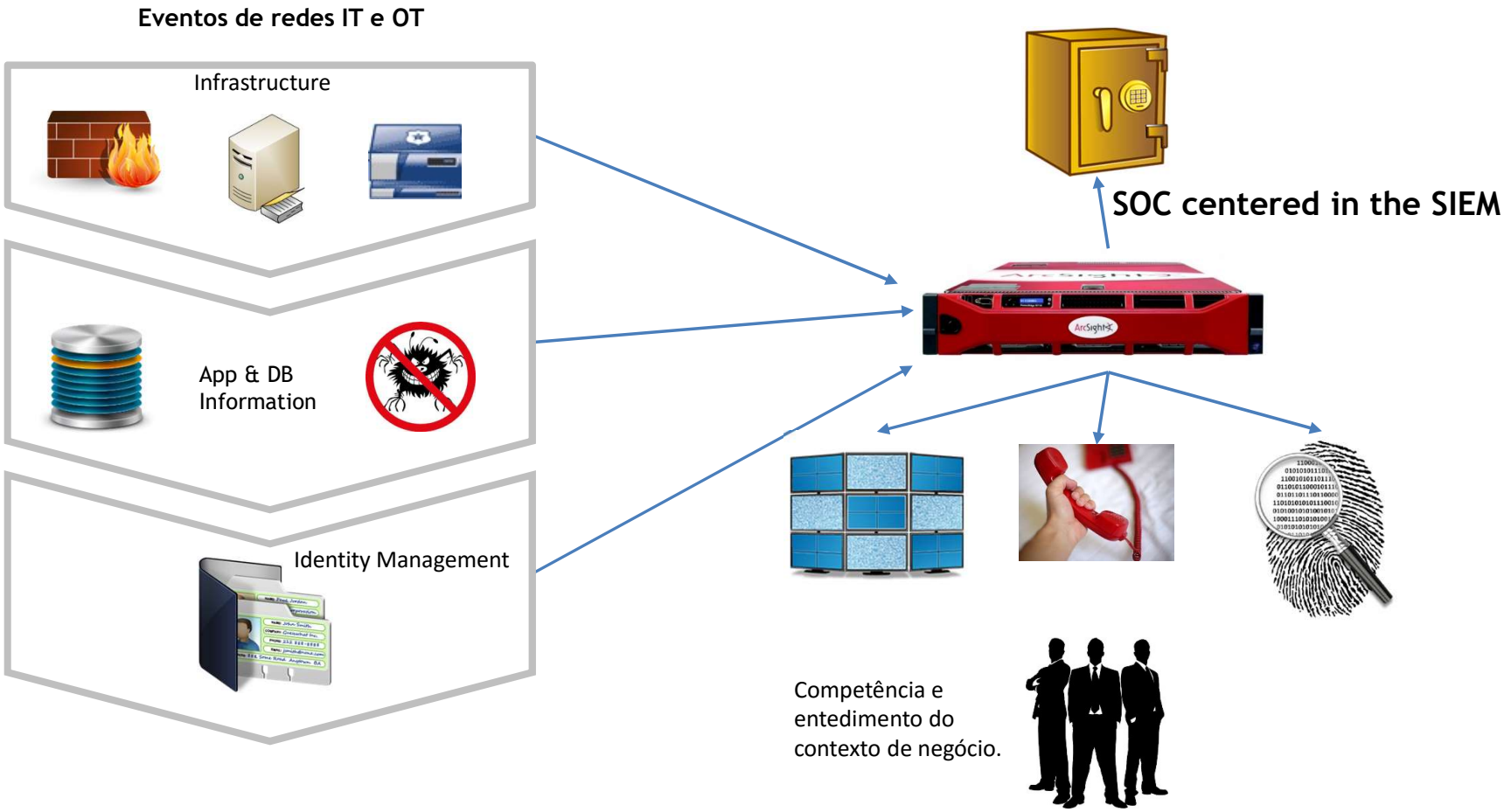
Fator Humano na Proteção das IIC

SOC EDP (Security Operations Center)



Uma Visão para a Segurança Operacional

Fator Humano na Proteção das IIC
SOC EDP (Security Operations Center)

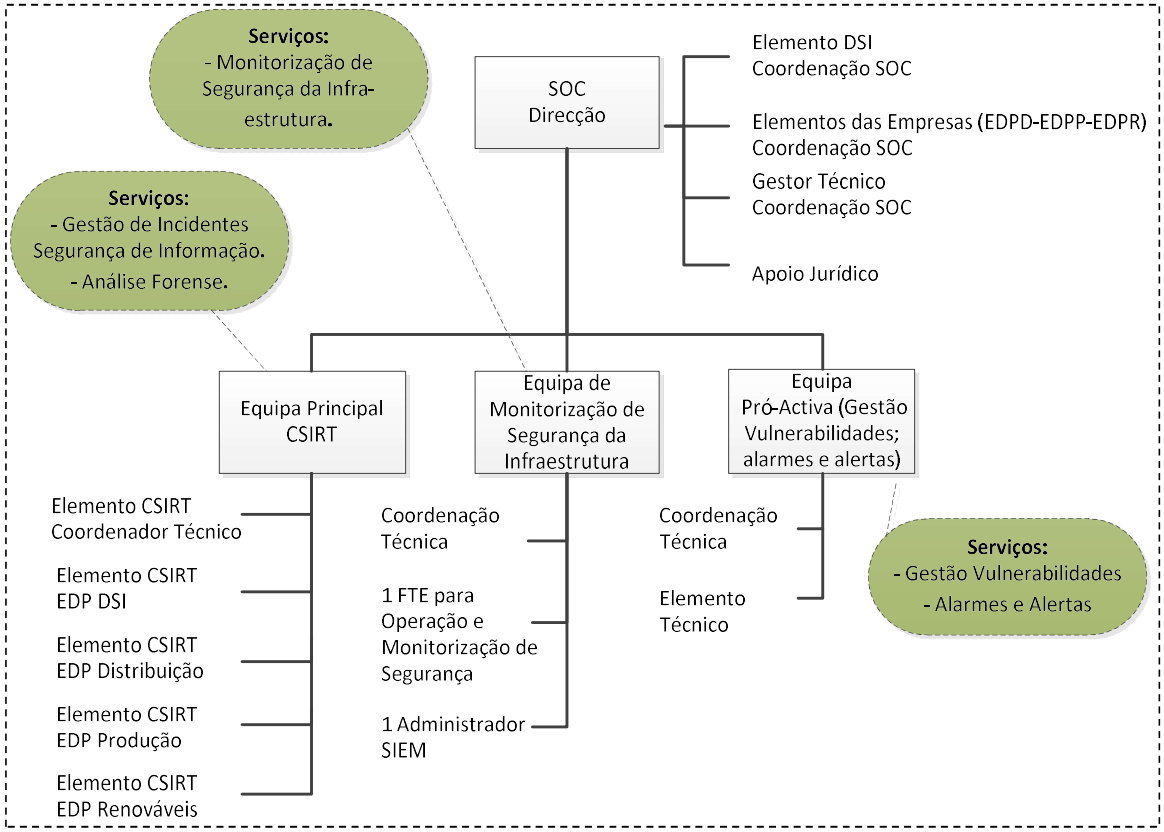


Fator Humano na Proteção das IIC

SOC EDP (Security Operations Center)

Serviços SOC EDP				
Monitorização de segurança	Gestão de incidentes de segurança	Análise Forense	Gestão de vulnerabilidades	Alarmes e alertas de segurança

Proposta de modelo organizacional



Números

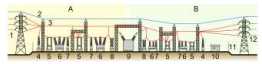
- 10 k eventos / segundo
- 2 K após agregação e filtragem
- 14 tecnologias integradas
- + 100 recursos tecnológicos

Fator Humano na Proteção das IIC

Exercícios CiberSegurança

Fator Humano na Proteção das IIC

Exercício CIBER PERSEU – Contexto do exercício para o grupo EDP



edponline

mibel MERCADO IBÉRICO DE LA ELECTRICIDAD

- **O Grupo EDP tem operações em praticamente toda a cadeia de valor do sector energético (produção; distribuição; *trading* e comercialização).**
- **Constituiu-se uma equipa transversal, reunindo elementos das várias empresas e direcções do Grupo (11 elementos no total):**
  - **DSI – Direcção de Sistemas de Informação (*Holding*);**
  - **EDP Distribuição;**
  - **EDP Produção;**
  - **EDP Renováveis;**
  - **UNGE – Unidade de Negócio de Gestão de Energia.**
- **Numa primeira reunião interna de planeamento concebe-se um macro cenário de ataque com impacto em todo o grupo e outros stakeholders.**

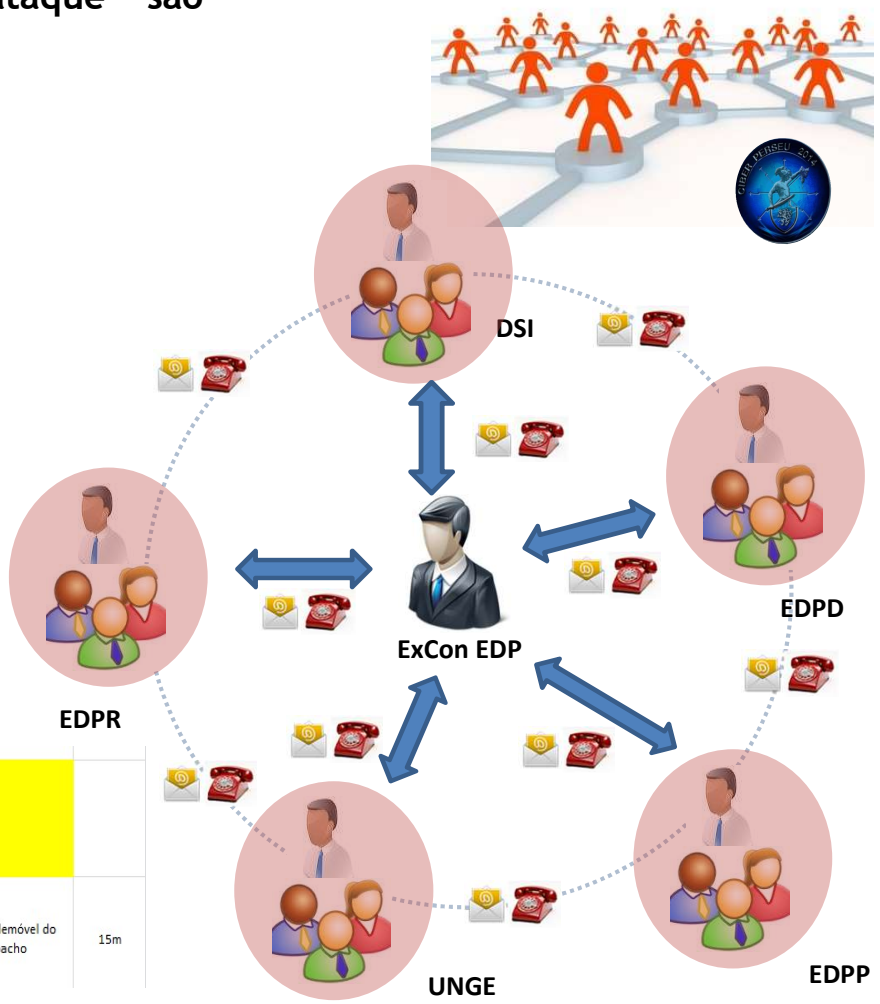
Fator Humano na Proteção das IIC

Exercício CIBER PERSEU – Contexto do exercício para o grupo EDP

- Após a definição do macro cenário de ataque são identificadas:
  - as audiências de treino.
  - os procedimentos a testar.

- Identificam-se os *injects* que materializam os objectivos de treino.

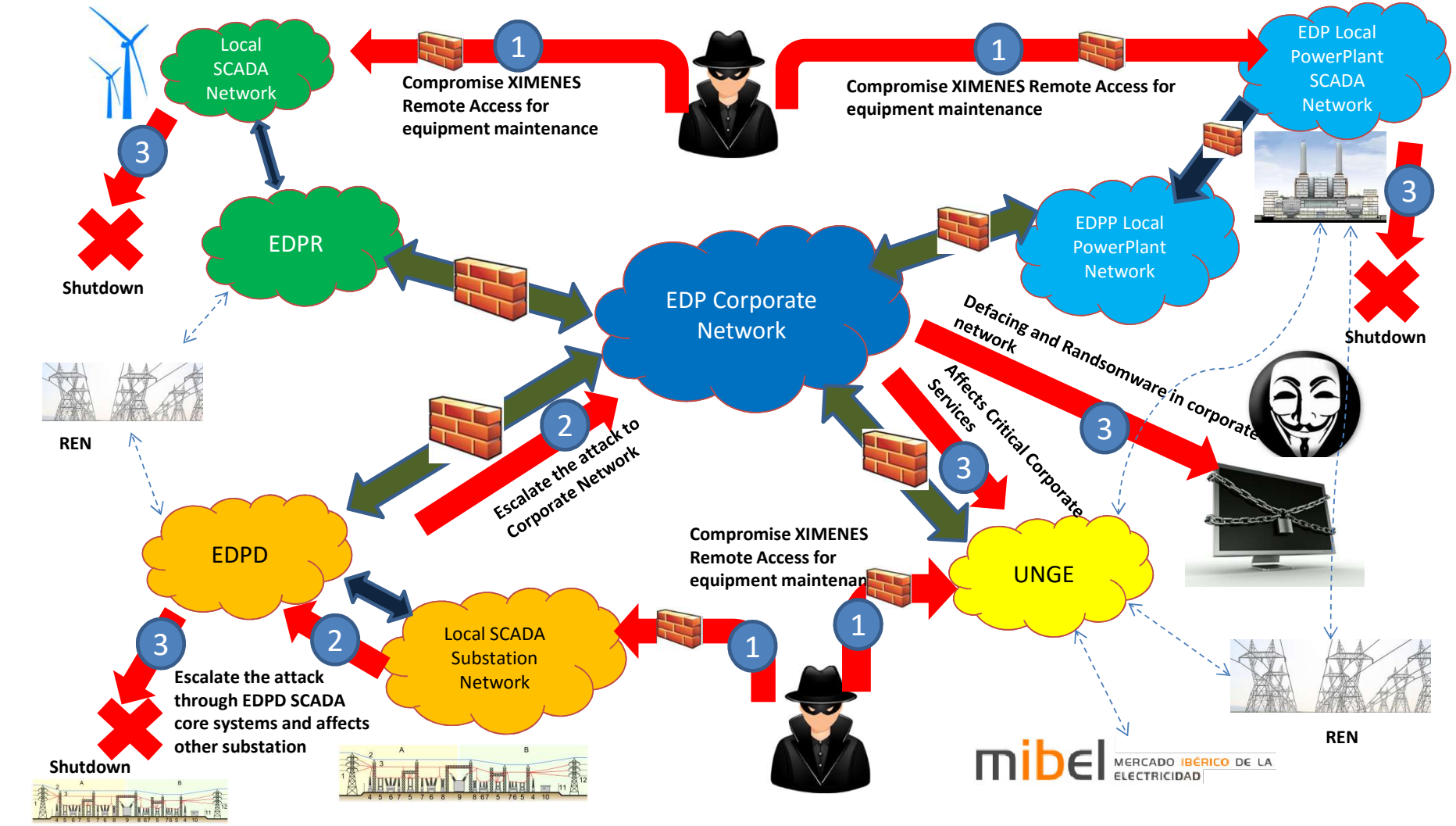
- Ajustam-se os *injects* de modo a integrar de forma articulada as narrativas e cenários do Exército e dos outros jogadores.



7							
8	Falha na recepção de eventos de sensor SCADA	Procedimentos de recuperação de erros	D1	10:45	Operadores EDPP		
	Falha ou sobrecarga dos telefones (chamadas constantes de faxes a bloquearem as linhas telefonicas)	Procedimentos de recuperação de erros	D1	11:00	Operador UNGE	Utilizar telemóvel do despacho	15m

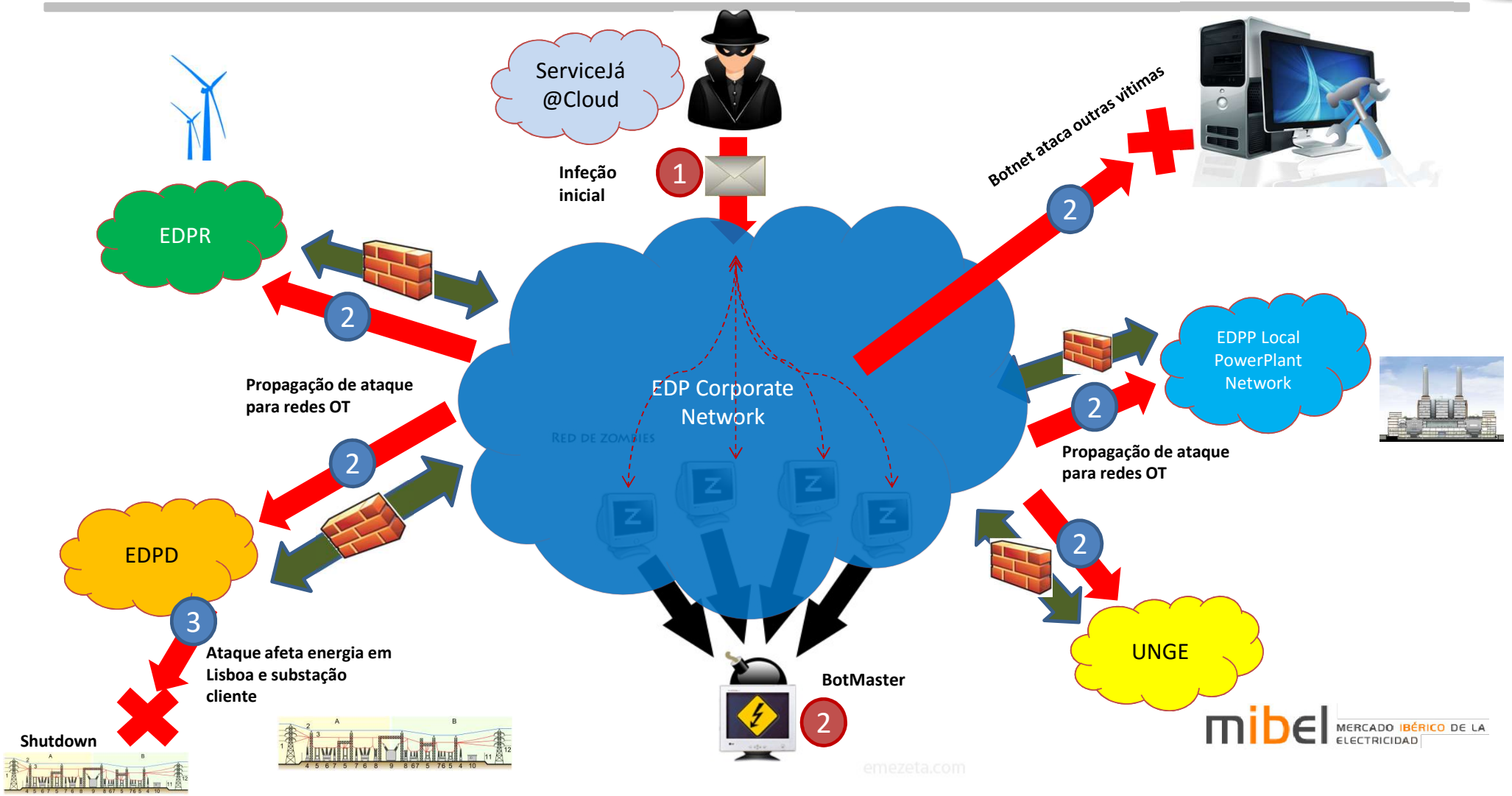
Fator Humano na Proteção das IIC

Macro cenário de ataque ao grupo EDP – CiberPerseu 2014



Fator Humano na Proteção das IIC

Macro cenário de ataque ao grupo EDP – CiberPerseu2015

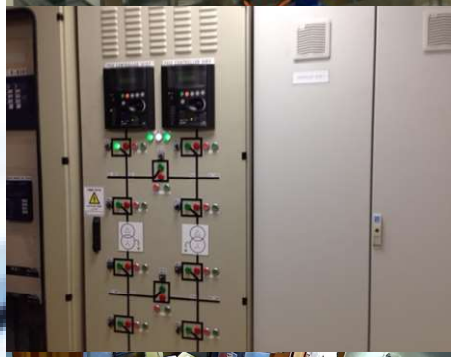


Fator Humano na Proteção das IIC

Exercício CIBER PERSEU – Mais Valias

- **Um entendimento mais profundo das interacções e dependências dos diversos sectores na defesa do ciberespaço nacional.**
- **Maior conhecimento sobre o enquadramento legal da segurança informática.**
- **Estabelecimento de *networking* entre organizações que cria laços e relações importantes, não só para o desenvolvimento de trabalhos futuros mas para uma cooperação mais eficiente numa situação real de ataque.**
- **Maior compreensão das capacidades da organização para reacção e ataques de segurança informática.**

Fator Humano na Proteção das IIC
Cyber Range EDP



Fator Humano na Proteção das IIC
Cyber Range EDP

Cyber Range EDP (objetivos)

Laboratório Segurança

Infraestrutura onde se poderão realizar testes a novos equipamentos, softwares ou protocolos, com objetivo de testar as capacidades de segurança na defesa das infraestruturas tecnológicas e de energia do Grupo EDP.

Arena para Exercícios de Segurança

Quer no âmbito de corporação com outras organizações (ex: CiberPerseu) quer no plano interno (ex: continuidade de negócio), constituir o CyberRange EDP como infraestrutura para a realização de exercícios de cibersegurança, treinando as nossas capacidades para detetar e reagir a ciberataques.

Formação

Constituir uma valência capaz de formar os colaboradores das área de TI e colaboradores que operam infraestruturas criticas de energia do Grupo EDP para detetarem e reagirem a incidentes de cibersegurança.

CaracteristicasFormação

- Constituída por 5 módulos diferentes (atualizáveis ao longo do tempo).
- Cada módulo tem a duração de 2 dias.
- A aprendizagem é realizada no modelo de wargames (equipas atacante e defesa)
- Abrange colaboradores de TI e operadores de sistemas que gerem infraestruturas criticas.

Fator Humano na Proteção das IIC
Cyber Range EDP - Módulos

Incident response

- **The training**
  The "First-responder" is the in-house employee called to handle suspicious computer events. The "First-responder" is the qualified figure to determine if the event is indeed a cyber-event, and if so to react according to protocol in order to mitigate the event.
- **The goal**
  Training IT and information security personnel for the role of the "First Responder" in the organization.
- **Target audience**
  The Incident-Response team as defined by the organization

Distribution

- **The training**
  The distribution process is unique, as such it requires qualified employees that are trained to handle targeted cyber-events on this process, allowing them to determine what has occurred and giving them the tools to mitigate the event.
- **The goal**
  Training the employees to detect, react and mitigate cyber-attacks on the distribution process.
- **Target audience**
  Sub-station employees that are part of the distribution department: system, security, communication, inspectors and management.

Penetration Testing

- **The training**
  In today's reality, every organization is at risk of a cyber-attack. The best way to prepare for cyber-attacks is to know your own weaknesses in advance. By conducting penetration tests on your organization you will be able to fix your breaches before the hacker will reach them.
- **The goal**
  Training the employees how to be a penetration testing team within the organization and how to handle cyber-security events.
- **Target audience**
  Employees from different organizational disciplines: monitoring, system, communication, IT, security

ICS Security – Detection & Response

- **The training**
  The ICS/SCADA training is aimed to expose the target audience to the world of cyber-attacks on industrial and operational systems and procedures.
- **The goal**
  Introducing the world of cyber-attacks to the trainees, in order to achieve cyber awareness in the production process.
- **Target audience**
  ICS system operators, control-room operators, engineers, inspectors

Management & Senior Management Workshops

- **The goal**
  In this workshops we aim to provide the managers with the knowledge and management tools that would assist them to make responsible decisions "under-fire". The workshops combine relevant case-studies, round-table discussions and demonstrations that demands a decision making process.
- **Target audience**
  All levels of organizational management, from junior to senior.