CÁTEDRA INCIBE

Digitalización y Ciberseguridad Hídrica

CYBERCHALLENGE

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Universitat de Girona

Universitat de Girona Fundació UdG: Innovació i Formació

CÁTEDRA INCIBE
Digitalización y Ciberseguridad Hídrica

PRESENTACIÓ

Característiques:

- 3 Reptes de ciberseguretat compostos per diferents flags (mini-reptes), nivell creixent amb el temps
- Participació per equips entre 2 i 5 persones
- 2 setmanes per resoldre cada repte i enviar les solucions

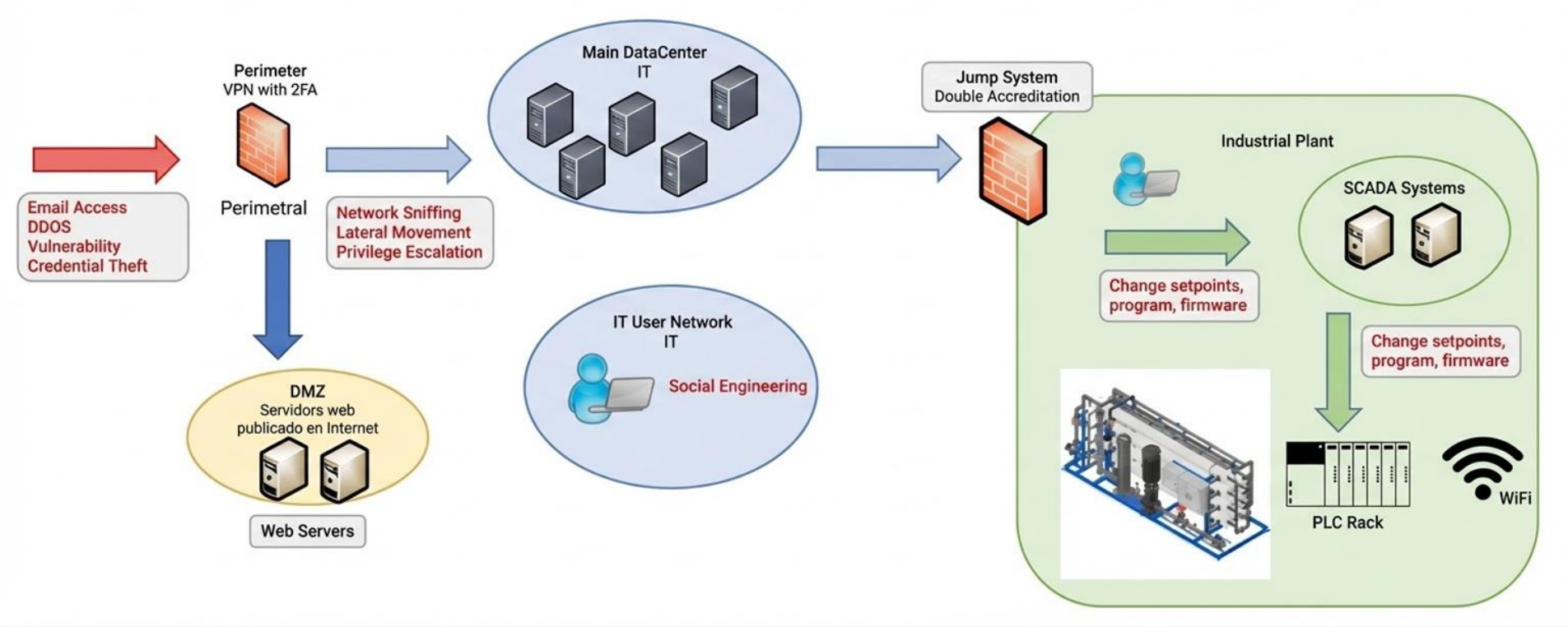
Dades de participació:

Participants inscrits | **Equips actius** | Equips amb 2 reptes resolts | Equips amb 3 reptes resolts

Financiado por la Unión Europea NextGenerationEU
incibe_
Universitat de Girona
Universitat de Girona Fundació UdG: Innovació i Formació

PRESENTACIÓ

En el transcurs dels reptes s'han posat a prova la resiliència del cicle de l'aigua.
Els escenaris han estat inspirats amb l'entorn AGBAR i han intentat emular entorns reals.



CÁTEDRA INCIBE
Digitalización y Ciberseguridad Hídrica

PRESENTACIÓ

Experiència dels guanyadors

Dels 8 equips que han resolt els 3 reptes, s'ha valorat la rapidesa i la manera i creativitat a l'hora de resoldre.

IRONHACKERS

DORAEMON

LA ÚLTIMA FILA

PRESENTACIÓ

Repte 01: Intel·ligència de Fonts Obertes (OSINT)

Exposició Pública: Eines com Shodan permeten localitzar infraestructures crítiques (PLCs i sistemes de telecontrol) exposades directament a Internet.

Rastre Digital: Mitjançant Google Hacking (operadors com `filetype:pdf`) es possible trobar documentació tècnica i dades sensibles.

Capa Oculta: La seguretat no és només el que es veu; s'han d'auditar metadades, registres DNS i l'històric de la Wayback Machine.

PRESENTACIÓ

Repte 02: Explotació de sistemes i escalada de privilegis

Configuracions perilloses: Han après que serveis aparentment inofensius com NFS obert o NTP poden filtrar des de flags fins a fitxers .env amb credencials crítiques.

Injecció de comandaments: No aplicar bones pràctiques en el procés de desenvolupament permet l'execució remota de comandes (RCE).

Contenidors i escalada: Un contenidor no és una barrera infranquejable; mitjançant la monitorització de processos (pspy) i permisos en Docker, es possible accedir al sistema host i obtenir accés total com a root

CÁTEDRA INCIBE
Digitalización y Ciberseguridad Hídrica

PRESENTACIÓ

Repte 03: Entorns OT i IA

Seguretat en la Xarxa Interna (OT): El programari utilitzat en entorns industrials (OPC UA, Node-RED) pot estar menys protegit.

Escalat en sistemes mal configurats: Servidos mal configurats poden esdevenir amb una fuga d'informació o escalada de privilegis.

Noves Amenaces (IA): Bonus track. Els agents d'IA també tenen vulnerabilitats i es poden manipular mitjançant prompt injection per exfiltrar secrets.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
incibe_
Universitat de Girona
Universitat de Girona Fundació UdG: Innovació i Formació