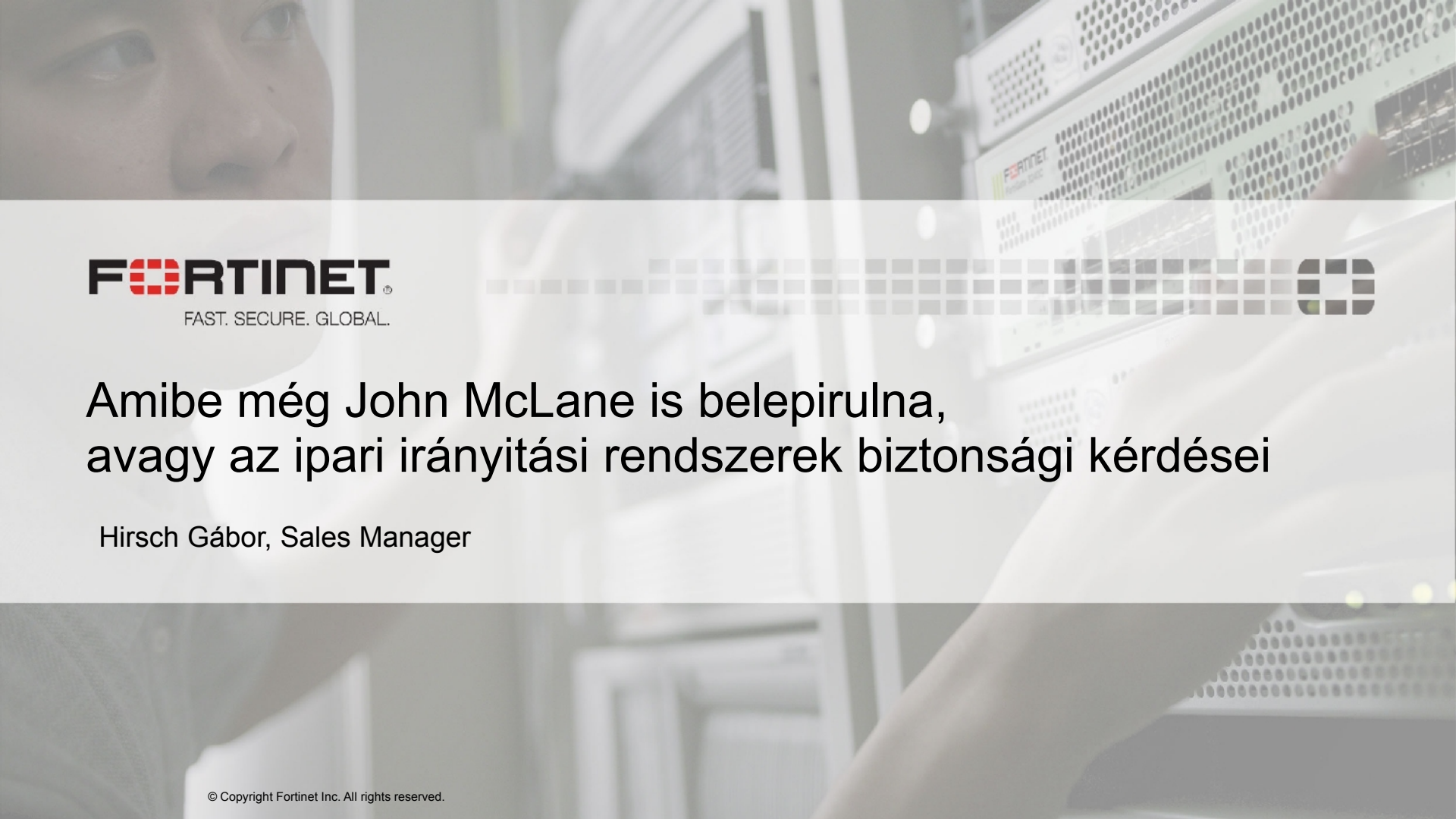


FAST. SECURE. GLOBAL.

Amibe még John McLane is belepirulna, avagy az ipari irányitási rendszerek biztonsági kérdései

Hirsch Gábor, Sales Manager

Agenda

Fenyegetések alakulása

ICS Bemutatás

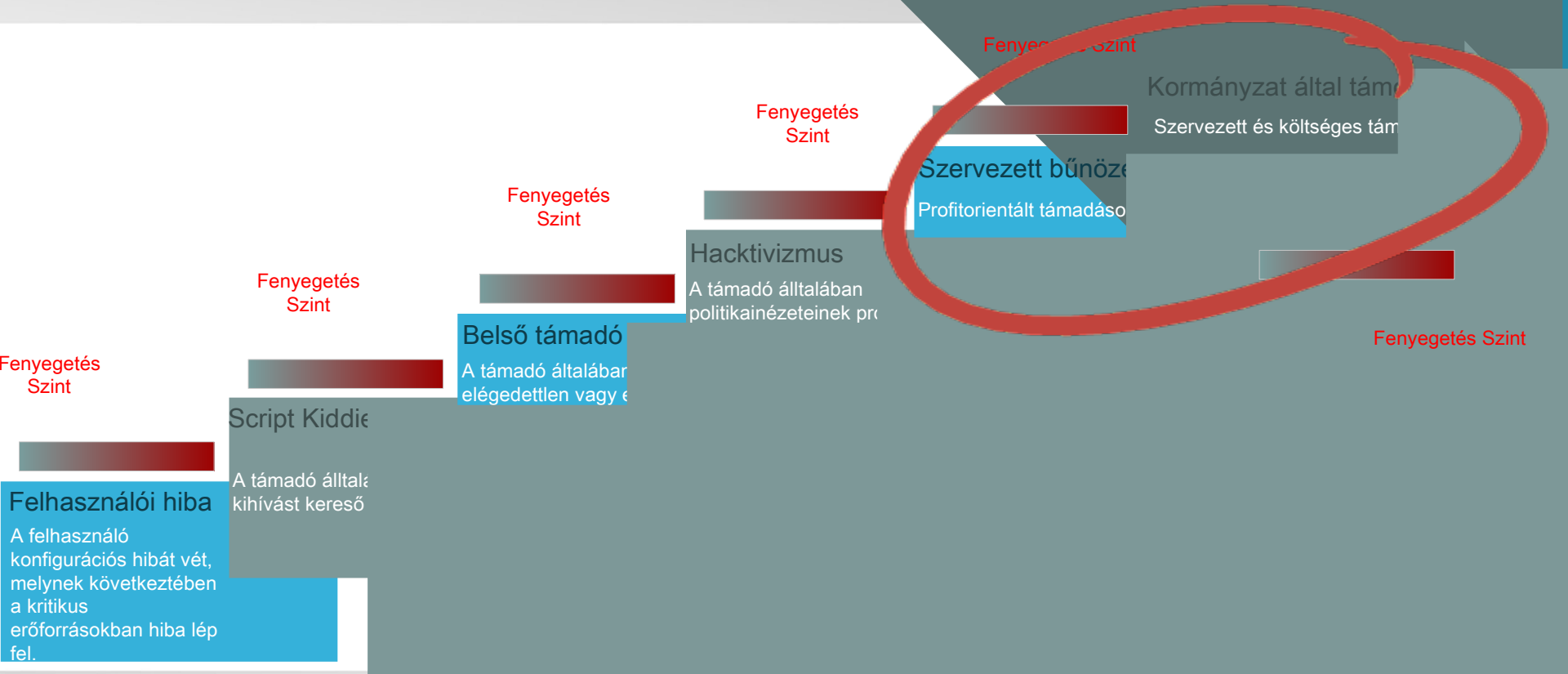
Miért problémás az ICS / SCADA rendszerek biztonsága

ICS / SCADA és a biztonság

A Shodan keresőmotor

ICS kockázatok

Fenyegetések evolúciója



FORTINET

Digitális Mohács Forgatókönyv

- **A forgatókönyv alapjai**:
  - Információgyűjtés
  - PSYOP (psychological operations)
  - Infrastruktúrák **KOMPLEX** támadása
- **A támadás sorrendje**:
  - Média, műsorszórás és internetes média
  - Pénzügy
  - Közlekedés
  - Telekommunikáció és internet
  - Villamos-energia szolgáltatás

ICS bemutatása

Rövidítések definíciói

ICS - Industrial Control System

IACS - Industrial Automation and Control System

SCADA - Supervisory Control and Data Acquisition

DCS - Distributed control system

HMI - Human Machine Interface

PLC - Programmable Logic Controller

ICS Komponensek

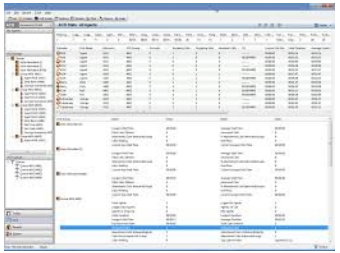
szabályzók

szenzorok

PLC

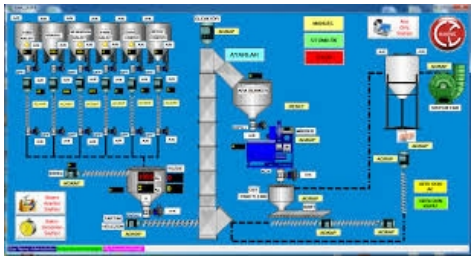
HMI

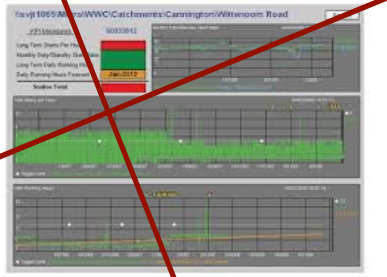
Felügyeleti rendszer



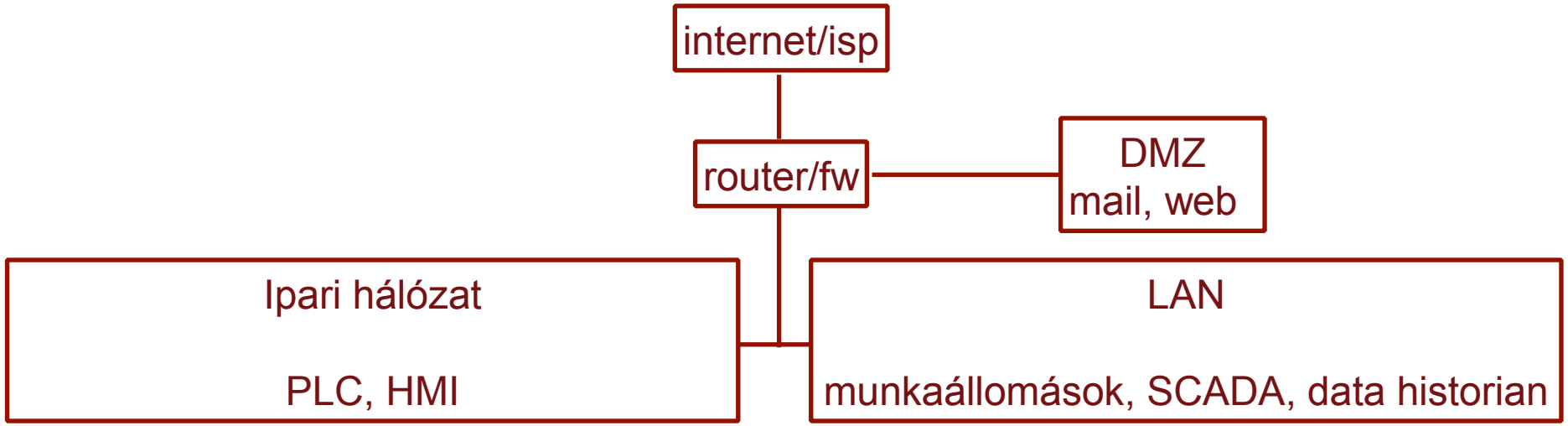
SCADA

Data historian





Tipikus hálózati diagram - ICS & LAN



Miért problémás az ICS / SCADA rendszerek biztonsága?

FORTINET

Az ICS biztonsági incidensek kiváltó okai

Nem támadások kivédésére tervezték

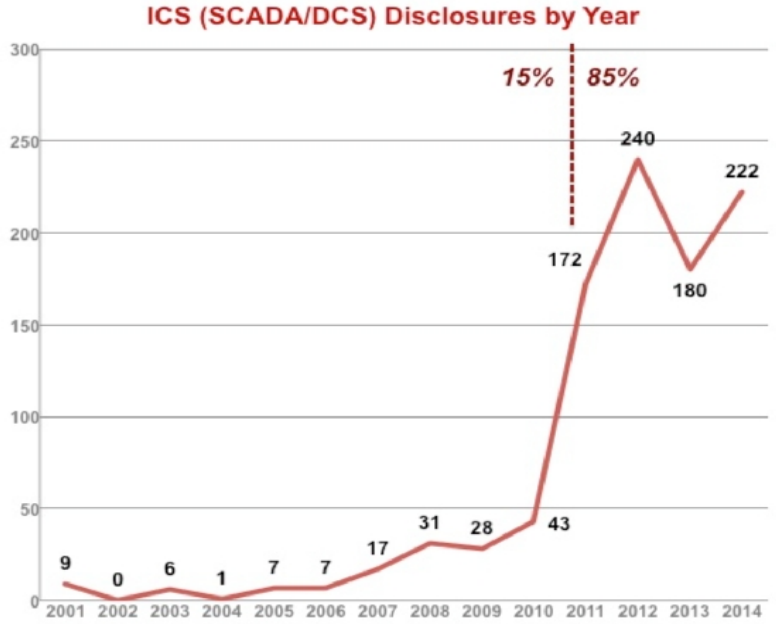
Hálózati támadások szokatlanok ICS környezetben

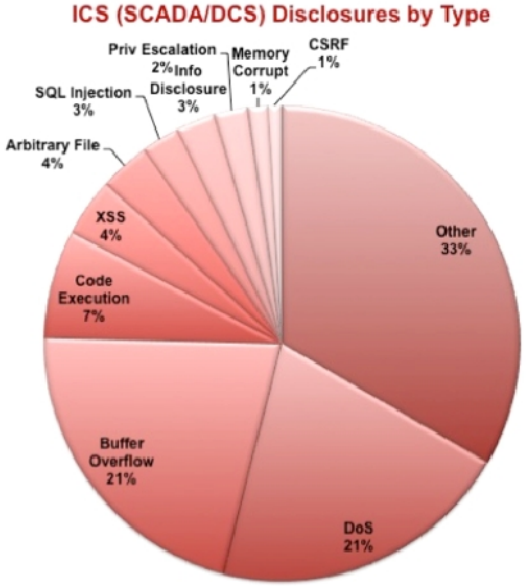
Biztonsági javítások alkalmazása nagyon nehéz

Működés = pénz

Igen magas MTBF

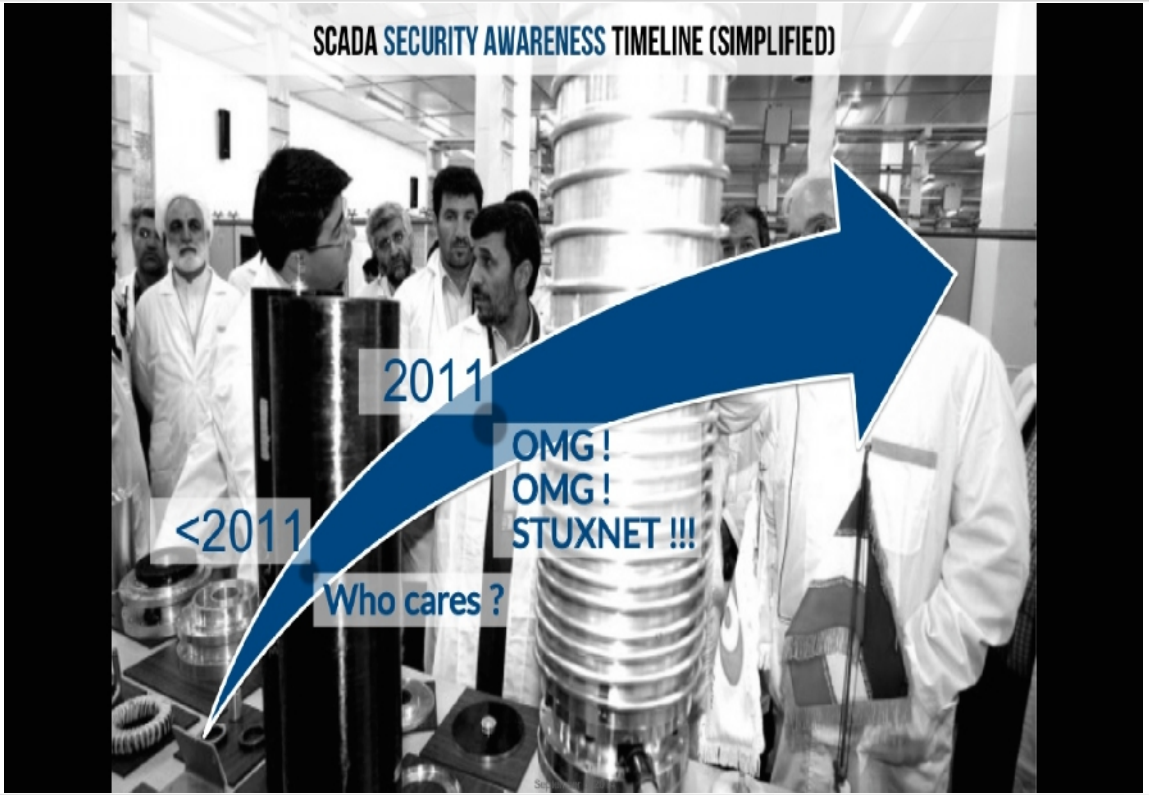
ICS Sérülékenységek





https://www.scadahacker.com

Mi történt 2011-ben?



Mi a különbség a PLC és PC között

FORTINET

PLC

Computer - CPU x MHz, x kB RAM, x MB flash

Valós időben dolgozik

Integrált input, output

Mostoha körülményekre tervezték

A kulcs alkatrészei HA redundánsak

PLC és PC – mi a különbség?

Garantált válaszidő

START / STOP mód

Program nem kerülhet végtelen ciklusba

- Az elejétől a végéig lefut
- A fő ciklust a PLC kontrollálja
- Nincsenek hurkok a programban
- Hardveres időzítők

Statikus kód

Felhasználói program megállítás nélkül frissíthető

PLC program

Scan ciklus

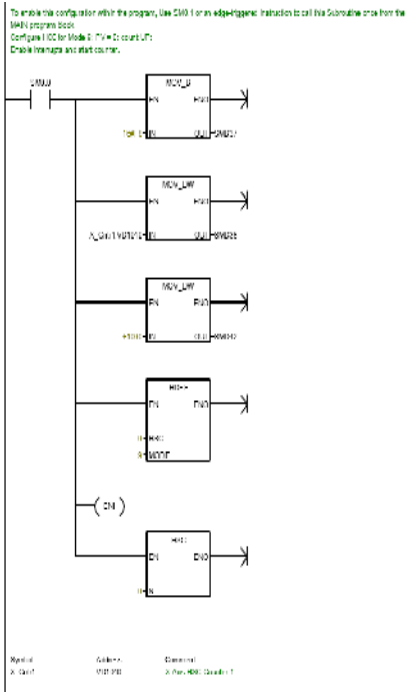
Procedura:

- inputs reading
- user program single scan
- setting of outputs

A „last one takes all” szabály

Egyszerű programnyelv

- assembler
- Létra diagram



PLC kommunikációs interfész

Master / slave

Valós idejű működés

Nyílt és zárt protokollok

NINCS azonosítás

NINCS titkosítás

NINCS jogosultsági szintek

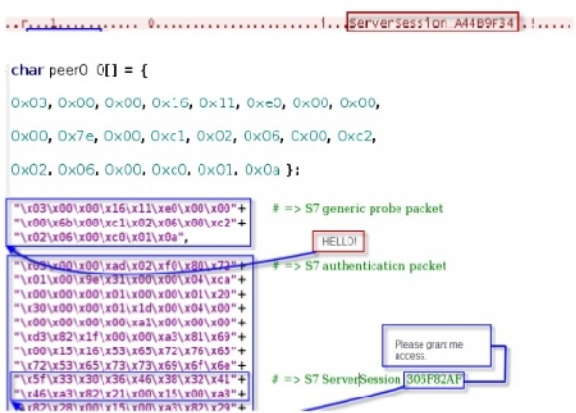
NINCS / hiányos naplózás

Közvetlen hozzáférés HW/input/output

Visszafejthetőség

We don't need the 'password'

Packet2Hex



ICS / SCADA és a biztonság

ICS biztonság - vissza a ’90 évekbe

- Azonosítás – általában a gyártó által nem támogatott
  - » funkcióvesztés
  - » session hijakinggel kikerülhető
  - » beégetett szerviz accountok
  - » általában csak a PLC program védett - nem az I/O
- Kommunikációs hierarchia
  - » támadó master, PLC slave
  - » visszajátszásos támadás
  - » MITM támadás

ICS - valóság

SCADA - Windows XP

Windows XP Embedded

Patch management – ne piszkáld amíg működik

NINCS végponti védelem

all-all-any tűzfal policy

Sok céleszköz egy-egy kisebb feladatra

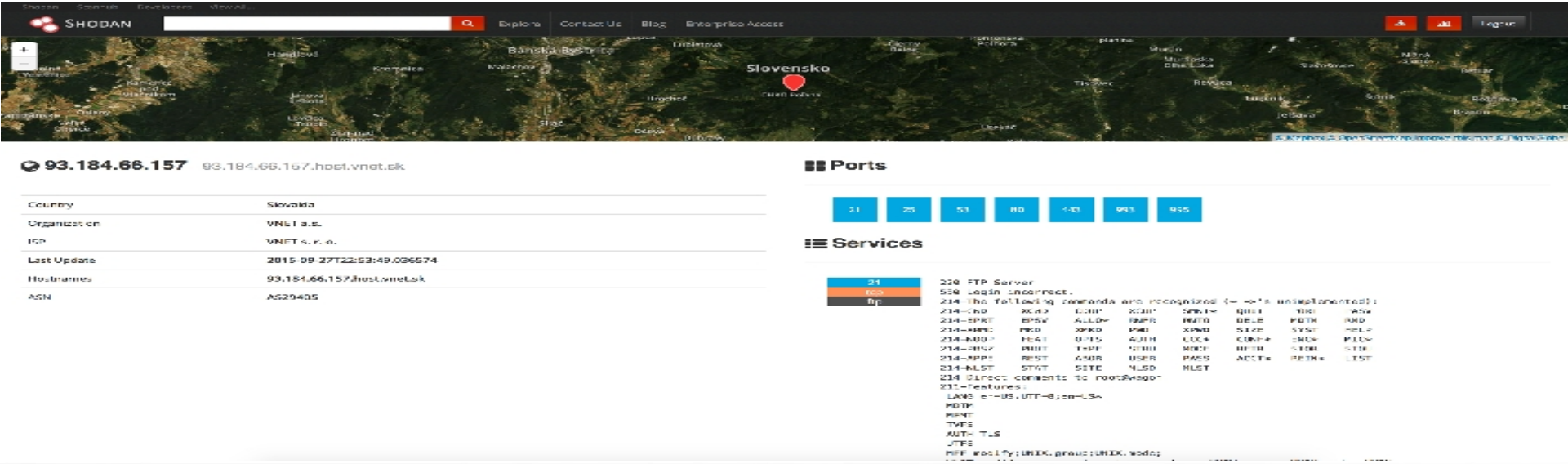
ICS rendszerek elérhetőek a LAN-on

ICS rendszerek elérhetőek az interneten

A Shodan keresőmotor

Shodan - the bad search engine

A SHODAN megvizsgálja a portokat és a kapott fejléc információkat indexeli (nem a webes tartalmat), teszi kereshetővé.



Beépített szűrők

country: kétbetűs országkódra

city: városnévre

hostname: hostnévre, vagy domainre

geo: koordináták alapján

net: adott IP range vagy subnet alapján

os: adott operációs rendszerre

port: specifikus szolgáltatásokra

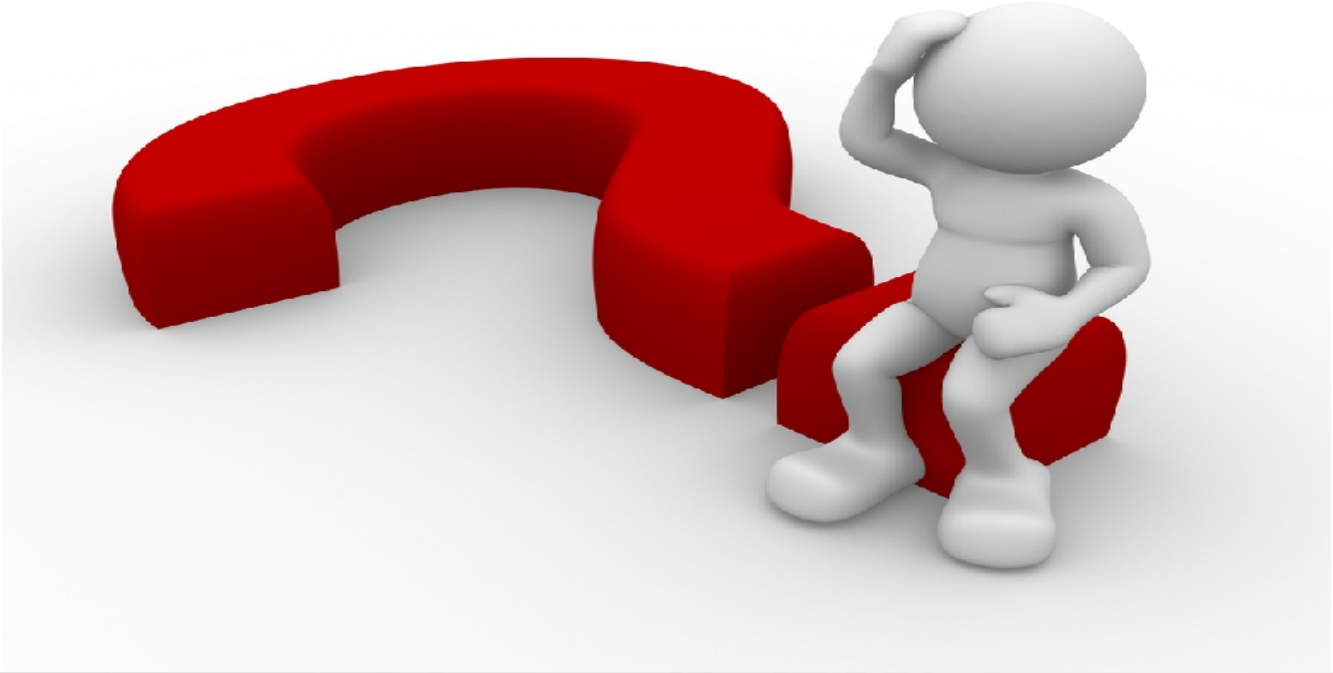
timeframe: időintervallumra

ICS kockázatok

A legnagyobb ICS kockázatok

1) Emberi hiba és szabotázs
2) Illetéktelen hozzáférés az erőforrásokhoz
3) A távoli karbantartási hozzáférés illetéktelen használata
4) Online támadás az irodán/vállalati hálózaton keresztül
5) Támadás a sztenderd ICS hálózati elemeken keresztül
6) A hálózati elemek támadása
7) Károkozó kód bejuttatása adathordozón vagy külső hardveren
8) (D)DoS támadás
9) Üzenet küldése és olvasása ICS hálózaton keresztül
10) Technikai hiba és előre nem látható körülmények

Kérdés?



Köszönöm a figyelmet!