

# Účinná technická opatření a bezpečnostní řešení v praxi

Pojďme k té pozitivnější části

# Bezpečnost OT není stav, je to boj o čas

## RÁNO JSTE SLYŠELI

# Útočník má čas.

6 měsíců v síti.  
Čeká na pokyn.  
Vy máte termín kolaudace stavby.

## A TADY JE ODPOVĚĎ

# Obrana čas zkracuje.

Z „6 měsíců, než si všimneme“  
na „6 hodin, než zasáhneme“.

Cíl: zkrátit jeho čas, prodloužit ten váš.

## ČTYŘI PILÍŘE

# Jak útočníkovi zkrátit čas a nám prodloužit ten váš

01

### HARDENING

Zmenšit prostor,  
kde může útočník působit

02

### MONITORING

Vidět, když se  
přesto něco děje

03

### SOC

Reagovat 24/7  
se znalostí OT

04

### THREAT MGMT

Učit se rychleji,  
než se útočník vyvíjí

# 1. Hardening: udělat útočnickovi práci těžší

## MFA

### Dvoufaktor na každém vzdáleném přístupu

Dodavatel, údržba, integrátor — každý přes jump server s MFA.

Radio-Stop bylo otevřené rádio. VPN bez MFA je totéž v IT.

## JUMP

### Jump servery jako povinná cesta

Žádný přímý RDP/SSH do OT zóny.

Logování, nahrávání session, schvalovací workflow. Dodavatel vidí jen to, co má vidět.

## EDR

### Monitoring endpointů v OT zóně

Inženýrské stanice, HMI terminály, dispečerské PC jsou Windows.

Patří tam EDR v režimu, který nezasahuje do provozu.

**Hardening není o tom zakázat dodavatelům přístup. Je o tom vědět, kdo kdy co udělal.**

## 2. Monitoring: vidět, co se děje

### PASIV

#### Pasivní monitoring OT sítě

Span port / TAP. Žádný zásah do protokolů, žádní agenti v PLC.

Nástroj pouze poslouchá a učí se normální provoz.

### ANOM

#### Detekce anomálií, ne jen signatur

Signatury přijdou pozdě. Anomálie přichází včas.

Nová IP v síti, nová komunikace mezi PLC, změna firmwaru.

### INTG

#### Integrace na dispečink

Dispečer nechce vidět SIEM. Chce vědět, že něco je špatně.

200 alertů za den na stole nikdo nehce, místo toho 1 incident připravený pro dispečink.

**Nemusíte vědět o každém síťovém paketu. Musíte vědět, když se něco změní.**

# 3. SOC: lidé, kteří se dívají 24/7

## PROČ NE VLASTNÍMI SILAMI

OT security analytik je vzácnější než ICS inženýr.  
3 lidé pro 24/7. Přes 8 mil. Kč ročně.

## CO SOC REÁLNĚ DĚLÁ

Triage (99 % false positives, 1 % reálných).  
Eskalace. Vedení reakce. Ladění detekce.

## PROČ OT-AWARE SOC

Klasický SOC: „Modbus je divný.“  
OT-aware SOC: „Modbus dělá, co dělat nemá.“

## 3:17 RÁNO V GENERICKÉM TUNELU

### KLASICKÝ IT SOC

Vidí pokus o přihlášení na inženýrskou stanici.  
Eskaluje jako „brute-force attack“.  
Volá v noci OT lidi. Zbytečně.

### OT-AWARE SOC

Ví, že v 3:15 byl plánovaný restart po firmware update.  
Neruší nikoho.

Ale když stejné přihlášení přijde v neděli v 11:00,  
eskaluje do několika desítek minut.

# 4. Threat management: učit se rychleji než útočník

LEDEN



Nová taktika  
ruské APT

ÚNOR



Zero-day  
v Siemens PLC

BŘEZEN



Ransomware  
cílí HMI

CO TO ZNAMENÁ PRO VÁS

72 h

od pozorování nové hrozby v zahraničí po naši schopnost ji detekovat u vás.  
Žádná detekce nastavená loni dnes nestačí — threat intel musí být živý proces.

# Čtyři pilíře, jeden cíl: náskok proti útočníkovi

## 01 · HARDENING

Zmenší  
prostor pro útočníka

## 02 · MONITORING

Vidí, když  
se něco děje

**NÁSKOK**

## 04 · THREAT MGMT

Zlepšuje  
detekci

## 03 · SOC

Interpretuje  
a reaguje

# Tři věci, které si z toho odnese

## NEINVAZIVNÍ

**Žádný zásah do řídicích systémů.**

Žádní agenti v PLC. Žádné omezení provozu.

Monitoring se připojí na span port. OT vrstva o něm ani neví.

## MLUVÍME S OT

**Ne jazykem compliance.  
Jazykem technologie.**

Víme, proč nemůžete restartovat HMI uprostřed dne.

Víme, že inženýrská stanice je kritická.

Integrujeme se na dispečink, ne přes něj.

## SIGNÁL, NE ŠUM

**Dispečink dostává jen to, co stojí za pozornost.**

Z tisíců alertů denně se na stůl operátora dostane to nejdůležitější.

S popisem. S kontextem. S návrhem kroků.

# Když to chcete udělat pořádně

## VIDĚT

1

Nezačínejte nákupem technologie.  
Začněte tím, že víte,  
co vlastně máte.

## PRIORIZOVAT

2

Neřešte všechno najednou.  
Viditelnost → hardening →  
SOC → threat management.

## SPOJIT SÍLY

3

Nedefinujte a nestavte to sami. Než si  
postavíte vlastní tým,  
útočník už bude uvnitř.

**První krok není koupit. První krok je vidět.**

Ráno jste slyšeli, proč je to vážné.

Teď jste slyšeli, čím se to dá řešit.

Infrastruktura, kterou stavíte na 50 let,  
**si zaslouží obranu, která obstojí výzvám  
kybernetické bezpečnosti.**