

Riadenie incidentov v OT prostredí

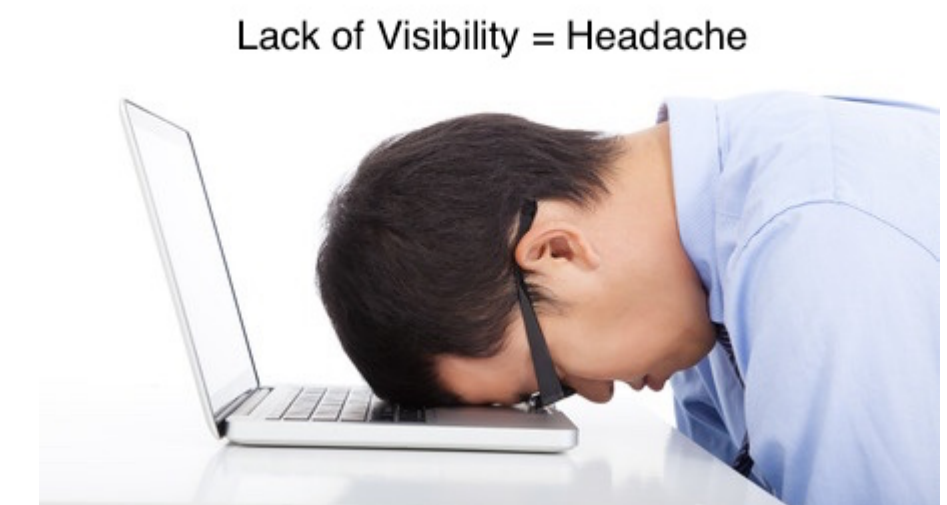


Martin Fábry, Accura s.r.o
CISSP, GICSP, CISA, CSSA, GRID, IEC 62443

(Ne)Riadenie OT incidentov = ~~Detekcia~~

Detekčné schopnosti kybernetického incidentu na Slovensku sú v OT mizerné:

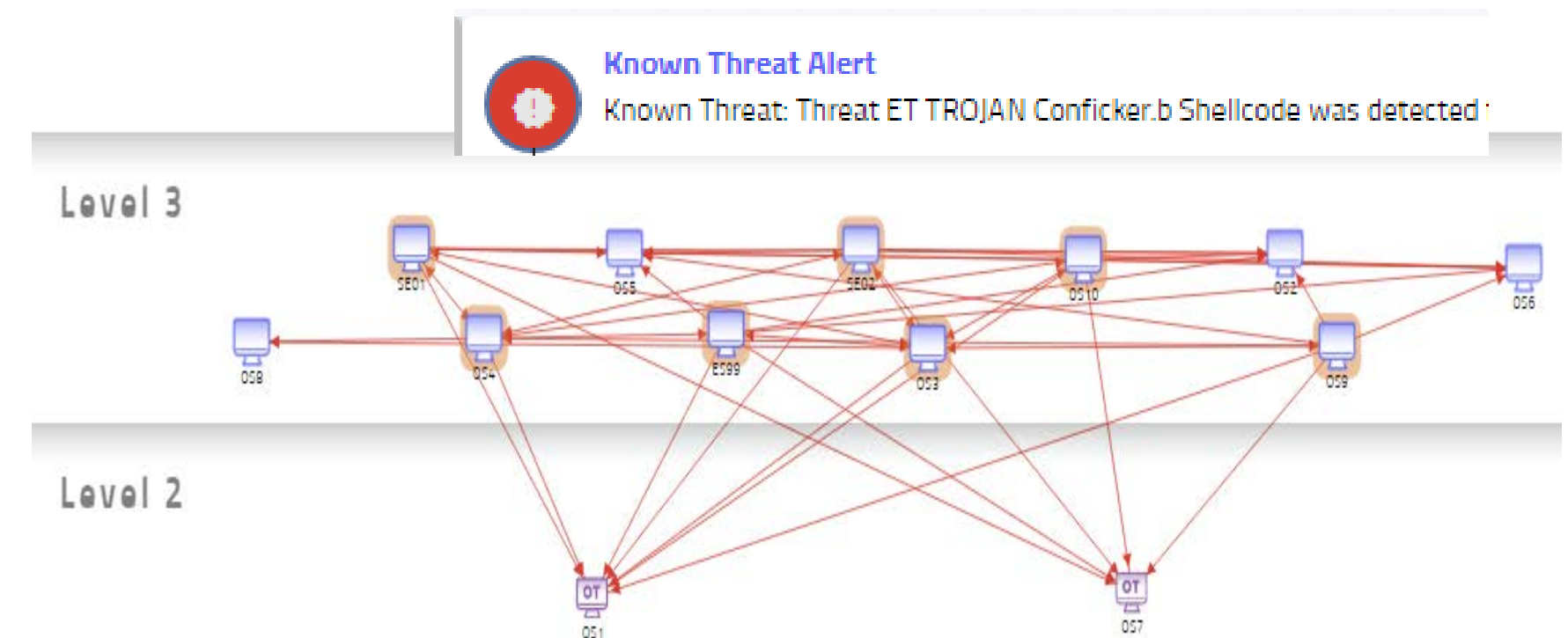
- 80% OT prostredí na Slovensku nemá nasadený OT Network Intrusion Detection System
- Centralizovaný log manažment je v OT raritou
- SIEM je v OT neznámy pojem, vzhľadom na špecifiká prostredia a jeho kontext
- Antivírus v OT nie je nasadený, alebo je out-of-date
- Komponenty riadiaceho systému DCS/PLC/RTU/IED negenerujú žiadne security logy
- Jediná možnosť detekcie sú často len MS Windows logy a IT/OT perimeter firewall (ak nejaký)
- Detekcia incidentu je často **ex-post**, keď sú **dopady incidentu viditeľné a citeľné**



Prerekvizity efektívneho riadenia incidentov

Čo treba urobiť aby to s riadením incidentov v OT fungovalo

- ✓ OT komponenty nevedia detegovať podozrivé activity a negenerujú security eventy → treba dodatočné opatrenia.
- ✓ Nasadiť špecializovaný pasívny NIDS, ktorý rozumie OT prostrediu (IT nástroje a open source nie je riešenie)
 - cybersecurity alerty
 - integrity alerty – dôraz na schopnosť detekcie manipulácie s automatizačným procesom)
- ✓ Nasadiť aspoň nejaký centralizovaný log management
- ✓ SIEM s OT kontext modulom (keď sa podarí nasadiť)
- ✓ Antivírus s validovanými patchmi od výrobcu vhodný pre OT prostredie
- ✓ OT SOC personál rozumejúci OT prostrediu



Prerekvizity splnené, podme riadiť

Nastavme governance a procesy IM

Životný cyklus incidentu:

1. Príprava a plánovanie
2. Detekcia a analýza
3. Izolácia a eradikácia
4. Post-incident aktivity (forenzná analýza)

Izolácia a Eradikácia

Špecifiká riadenia incidentov v OT

Reakcia na incident v OT:

- ☐ Iniciovanie organizovanej rýchlej reakcie je kritické
- ☐ Načasovanie je zásadné.
- ☐ Niektoré systémy ICS si ponechajú iba určité množstvo časovaných údajov

Izolácia kompromitovaného komponentu v OT:

- ☐ Môže zhoršiť dopad
- ☐ Môže negatívne ovplyniť functional safety
- ☐ Musí byť prevedená v spolupráci s OT personálom prípadne dodávateľom

Forenzná Analýza

Špecifiká riadenia incidentov v OT

Základná forenzná analýza:

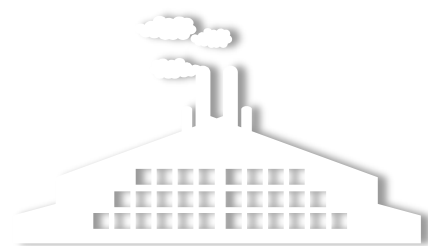
- ☐ Akvizícia
- ☐ Dôkazy
- ☐ Analýza
- ☐ Reportovanie

Výzvy v OT:

- ☐ Neexistujúce alebo limitované forenzné nástroje v ICS, napr. pre PLC, RTU, IEC napr. potrebné pre analýzu firmware
- ☐ Limitovaný expertný personál



Ďakujem za pozornosť



GET IN TOUCH

We Protect Your Critical Assets



Accura s.r.o
Mileticova 500/1
821 08
Bratislava
Slovakia
accura@accura.io