Industrial Cyber Security Tools

Everything in war is simple, but the simplest thing is difficult.
Es ist im Kriege alles sehr einfach, aber das Einfachste ist schwierig.

von Clausewitz

Pavel Osinski
osinski@softprom.com

SOFTPROM by ERC
Value Added Distributor #1999 - 2019

2019
Industrial Cyber Security, Tools – Potential Threats, Internal, External

DCS \ SCADA \ DMZ

Direct connection to devices

Wireless connections

External Memory cards

SCADA/DCS server

Switch

PLC

HMI panel

Frequency Convertor

SD
Industrial Cyber Security, Tools – Potential Threats
Internal Threats - STUXNET
Industrial Cyber Security, Tools – Potential Threats
Remote Threats - TRITON (TRISIS, HATMAN)

ERP level

MES  DMZ

DCS \ SCADA  DMZ

Generator

BLACKOUT

Value Added Distributor

Pavel Osinski 2019
Industrial Cyber Security, Tools – Potential Threats
Remote Threats – BlackEnergy 3 – Substation Severnaya

ERP level

SCADA

BLACKOUT

Off

Value Added
Distributor
Pavel Osinski 2019
Define operators of essential services

Transpose NIS-directive to National Legislation

Create CSIRT for all members

Define national NIS strategy

Cooperation Group Launch

Following the assessment of either the information provided by an operator of essential services or the results of a security audit, the competent authority may issue binding instructions to the operator of essential services to remedy its operations.
Industrial Cyber Security, Tools
Market Leaders of Industry 4.0
Industrial Cyber Security, Tools – Tools
IDS for IACS – Indegy solution

Value Added Distributor

Pavel Osinski 2019
Industrial Cyber Security, Tools – Tools
IPS for IACS – Cyberbit solution - SCADASchield
Industrial Cyber Security, Tools – Tools
IPS for IACS – Cyberbit solution - SCADASchield

Database of Vulnerabilities
- ICSA-19-134-07
- CVE-2019-13923
- CVE-2019-13919
- ICSA-19-162-04
- ICSA-19-227-04
- ICSA-19-008-01
- CVE-2019-1226
- ICSA-17-068-01

Policies
- Firmware Change
- PLC upload
- PLC download
- IP conflict
- Intrusion Detection
- New asset discovered
- Change in controller state
- Module #3 Not Seen

Events
- 360 Intrusion Detection
- 359 PLC-Sie#35 code download
- 358 PLC-Rckwl#15 New Module Discovered
- 357 PLC-Sie#47 Module #3 Not Seen
- 356 HMI-Sch#04 Change in controller state
- 355 Intrusion Detection
- 354 IP Conflict IP 190.145.0.3
- 353 New asset discovered IP 190.145.0.3
- 352 Asset not seen HMI-Sch#04
- 351 PLC-Sie42 Module #5 Not Seen
- 350 PLC-Rckwl#15 code upload
- 349 Intrusion Detection
- 348 Asset not seen PLC-Sie#37
- 347 IP Conflict IP 190.145.0.25
- 346 New asset discovered IP 190.145.0.25
- 345 PLC-Rckwl#15 Change in controller state

Active Engine
- Name and Location
- IP Address and MAC Address
- First and Last Time Seen
- Device Classification (PLC, RTU, HMI, Digital I/O, Analog I/O, Communications Card etc.)
- Device Maker and Model
- Part Number
- Firmware Version
- Serial Number
- State
- Memory Consumption
- Controller Scan Time
- Backplane/Chassis Configuration
- Open Network Ports
Industrial Cyber Security, Tools – Tools
IPS for IACS – Deception Solution – TRAPX- How It Works

Real SCADA Server
Real PLC
Real PLC

Virtual SCADA Server
Virtual PLC
Virtual PLC

Virtual LAN

Value Added Distributor Pavel Osinski 2019
Industrial Cyber Security, Tools – Tools
IPS for IACS – Unidirectional Security Gateways - WATERFALL

Value Added Distributor
Pavel Osinski 2019