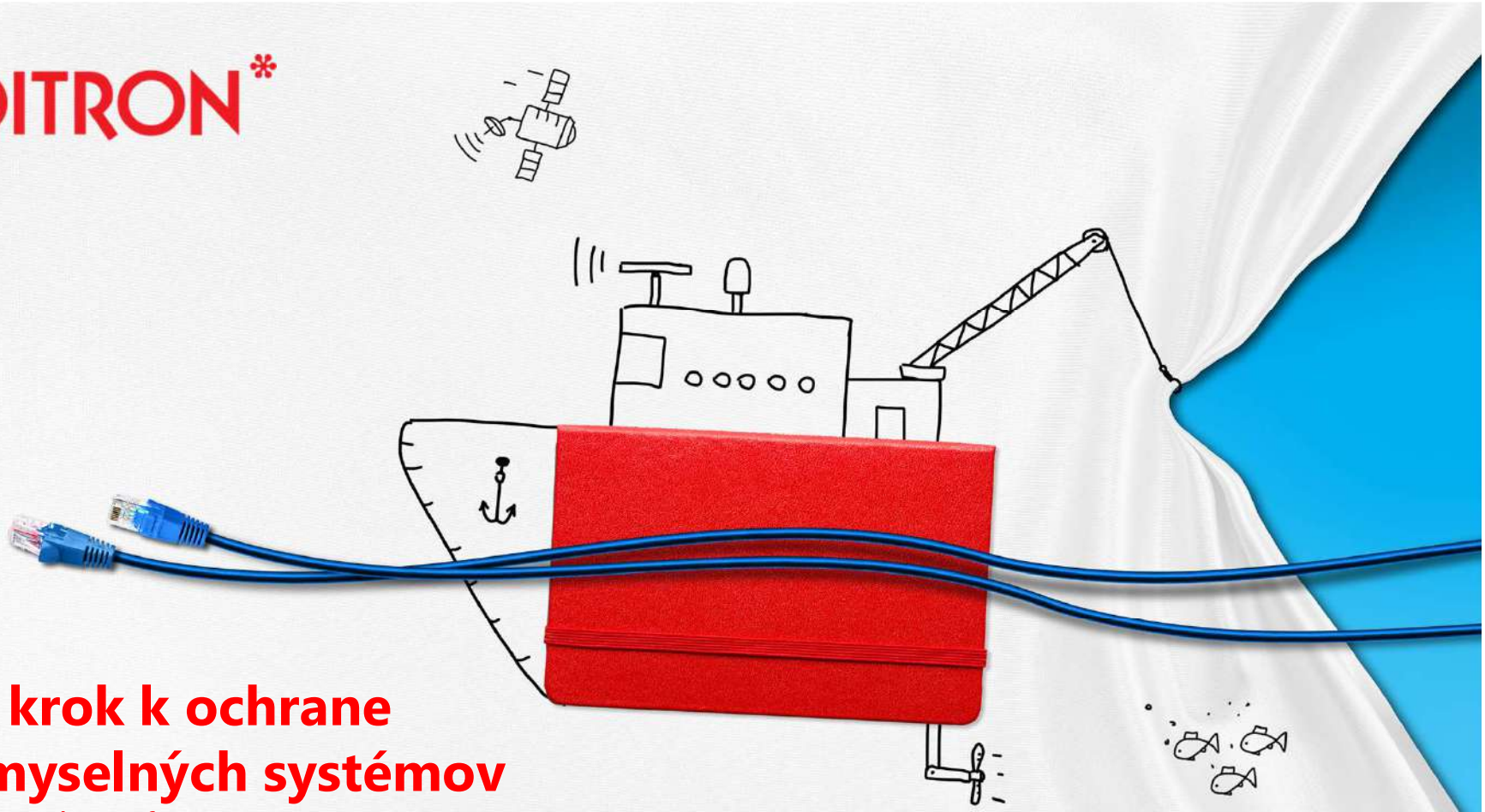
SOITRON



Prvý krok k ochrane priemyselných systémov

Martin Vozár, Defense 2019

Agenda

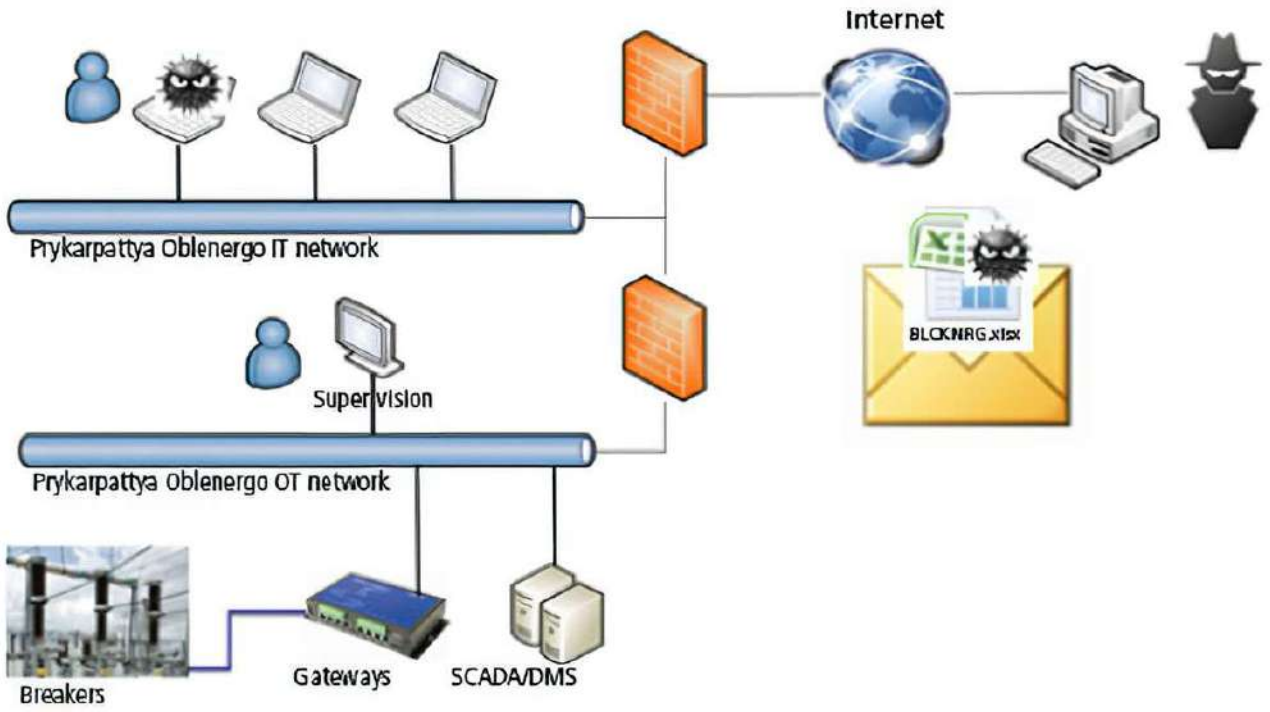
- Známy príklad z Ukrajiny
- Sentryo ICS Cybervision

Známy príklad z Ukrajiny (prvý)

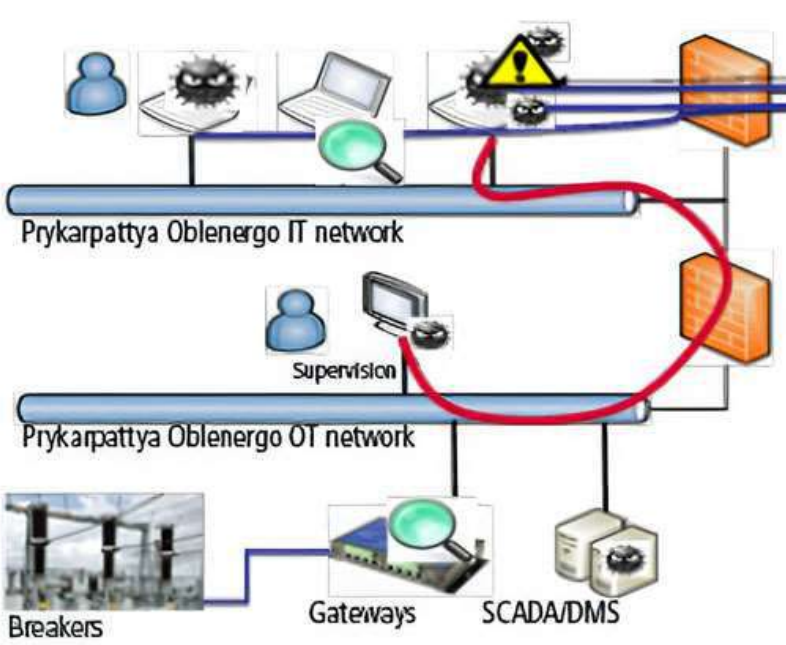
Prvý útok

- Analýza útoku z decembra 2015 dostupná na adrese https://automation.isa.org/lessons-learned-forensic-analysis-ukrainian-power-grid-cyberattack-malware/ pod názvom „Lessons Learned From a Forensic Analysis of the Ukrainian Power Grid Cyberattack“
- Dvaja zo štyroch autorov pracujú v Sentryo
- Spôsobený výpadok napájania vo významnej geografickej oblasti

Jar 2015, zamestnanec otvoril .xlsx nakazený BlackEnergy

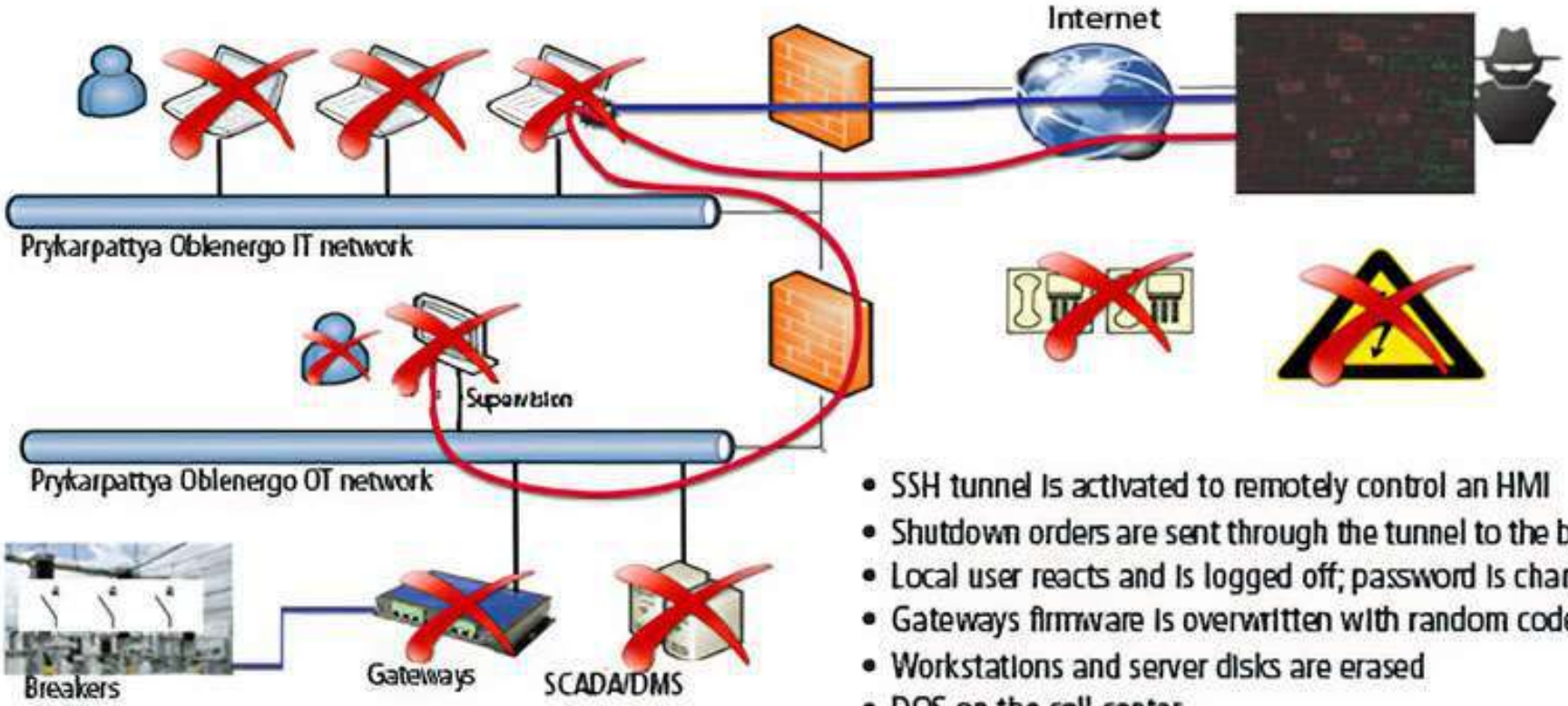


Šírenie po sieti, prieskum, príprava na neskoršiu aktiváciu



- Malware connects to distant C&C server
- Network scan, hops to another host
- Detects an open SSH tunnel to OT
- Keyboard stroke recording (passwords, etc.) for future use
- While user away, opens SSH tunnel, connects to other systems, and installs further malware on vulnerable hosts
- Cleanup and installation on a low-profile persistent threat, ready for activation

Útok a „upratovanie“



- SSH tunnel is activated to remotely control an HMI
- Shutdown orders are sent through the tunnel to the breakers
- Local user reacts and is logged off; password is changed
- Gateways firmware is overwritten with random code
- Workstations and server disks are erased
- DOS on the call center
- UPS are shut down

Sentryo ICS CyberVision

Kto je Sentryo

- Francúzska spoločnosť založená 2014
- Hlavné sídlo: Lyon
- Pobočky: Francúzsko, Nemecko, USA
- V roku 2019 akvizovaná spoločnosťou **Cisco**

- Hlavný produkt: **ICS CyberVision**
- OT Security platforma navrhnutá OT inžiniermi
- Poskytuje viditeľnosť, integritu a bezpečnosť prostredníctvom IT Asset manažmentu a detekcie anomálií, ktoré redukujú riziko vystavenia sa problémom + deteguje hrozby v komplexných distribuovaných resp. legacy priemyselných systémoch

Nové výzvy pre priemysel

- **Digitalizácia** vytvára nové hodnoty, ale zároveň **zvyšuje** už aj tak široký **attack surface**.

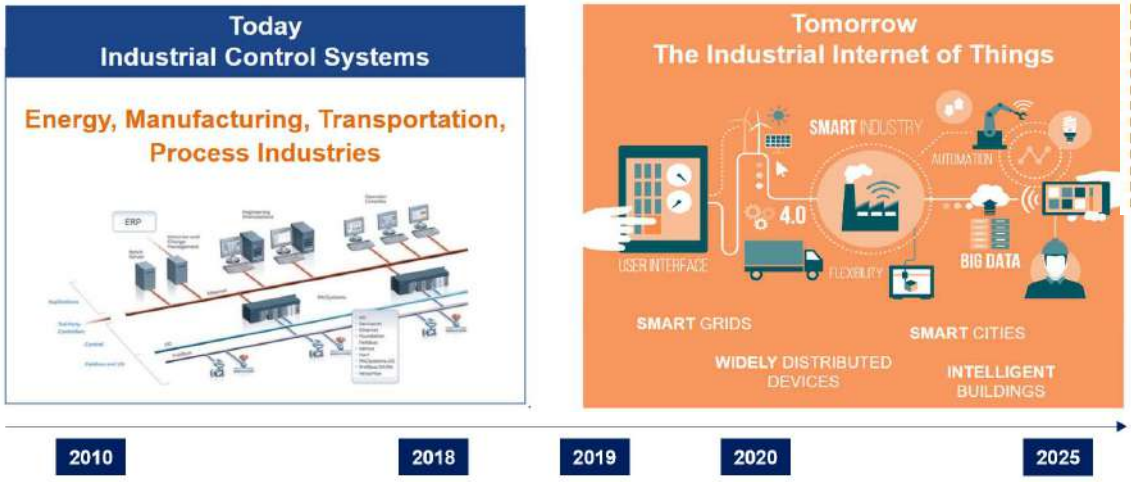
- Kľúčové je v prvom rade poznať **čo je v sieti** a ako vzájomne **komunikuje** (+payload).
- Rozdiel medzi IT a OT pri incidente:
- **IT** – iba finančná strata (downtime)
- **OT** – **ohrozenie zdravia, životov**

ICS are hard to secure without OT knowledge:

Lack of asset and behavior visibility

IT Security tools are for "expert"

OT personnel has no extra time slots

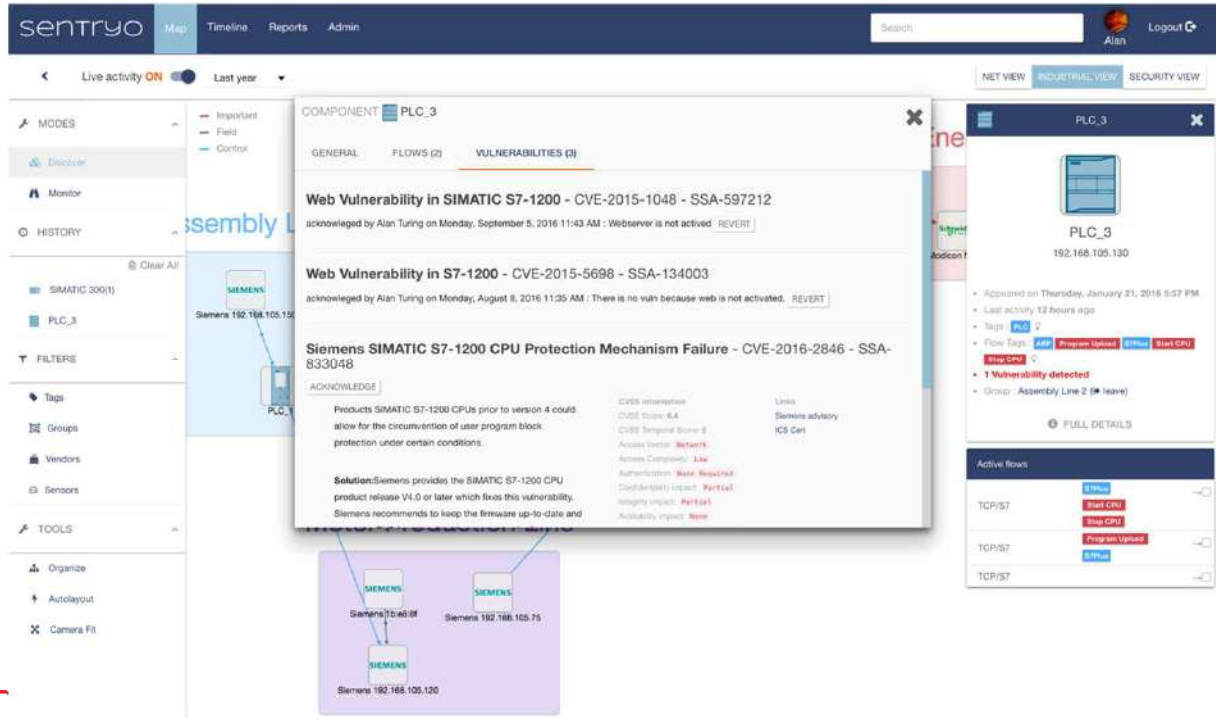


Čo je ICS CyberVision

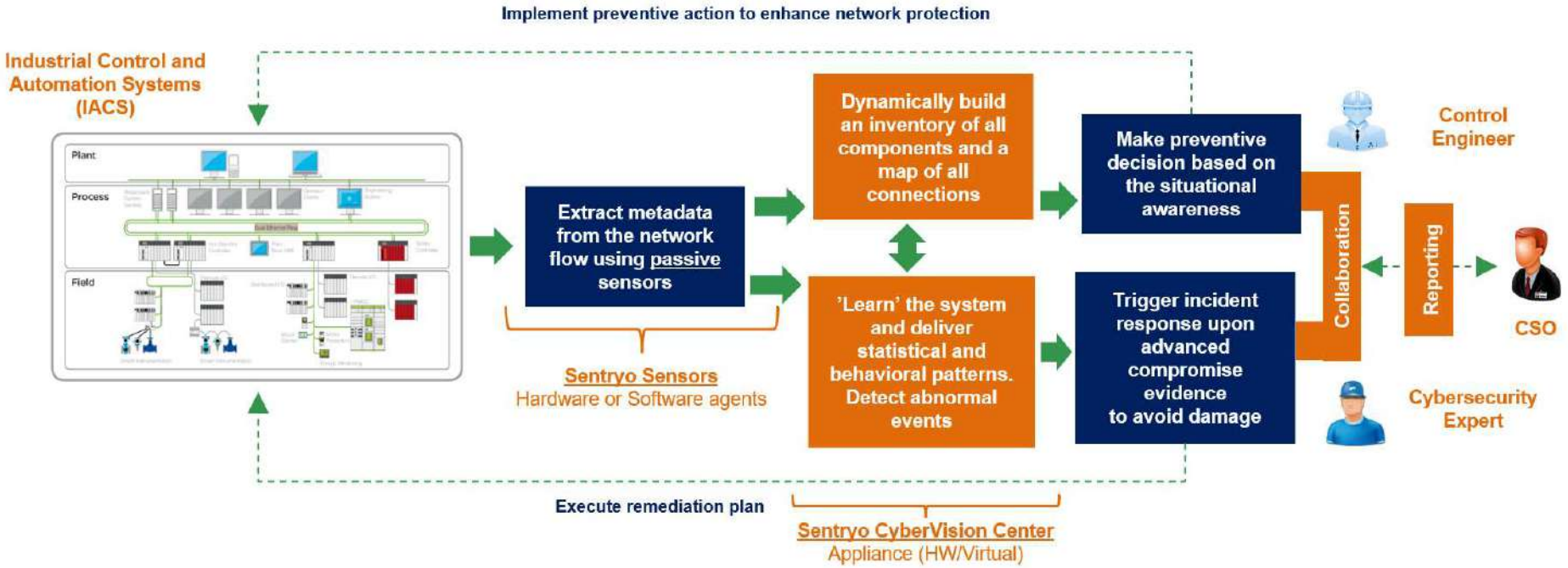
- Sieťová monitorovacia platforma, ktorá zvyšuje bezpečnostnú odolnosť Industrial Control Systems (ICS) a SCADA sietí
- Komponenty:
  - Senzory
  - Centrálna vizualizácia dát a analytický software
- **Pasívne** analyzuje sieťovú komunikáciu
- Poskytuje **významné informácie o assetoch a pokročilú detekciu anomálií**
- **V reálnom čase upozorňuje na hrozby**

ICS CyberVision benefity

- Znalosť OT protokolov (vrátane payload-u)
- Vizualizácia dát (čo s čím, ako, ...)
- Zero configuration – machine learning
- 100% pasívne

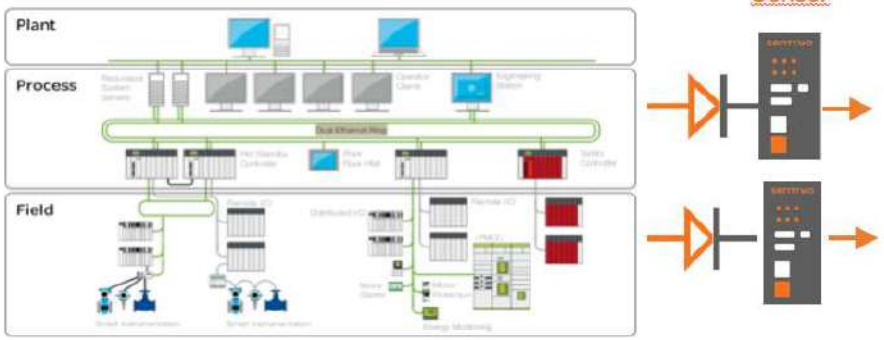


ICS CyberVision – princípy



ICS CyberVision – kľúčové vlastnosti (1/4)

1 **Use DPI technology to extract meaningful information (data & metadata) from OT networks using 100% passive sensors.**



ICS CyberVision
Sensor

ICS CyberVision
Center

COLLECT

- **Inventory:**
  - Devices, Modules;
  - Firmware.
- **Process Control:**
  - System Messages;
  - Programs;
  - Register IDs.
- **Network:**
  - Metadata;
  - Statistics.

Benefits
Store all data collected within the CyberVision center database, export or link to other systems (CMDB).

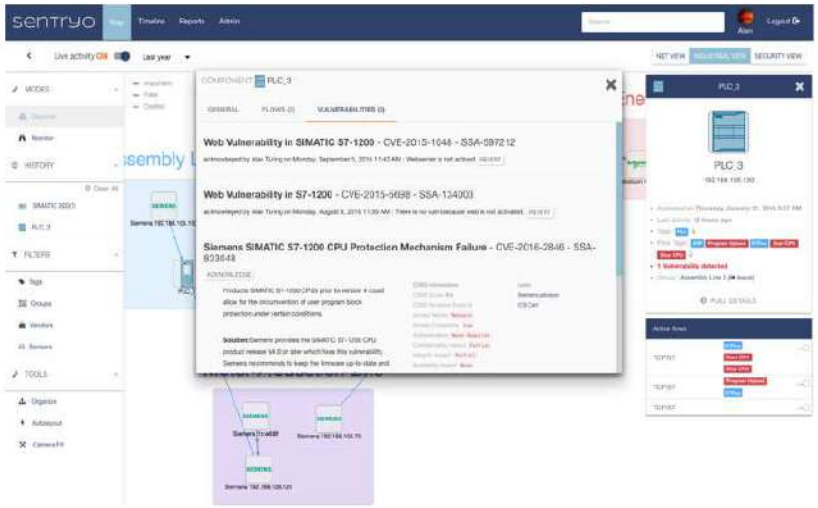
Offline Mode

Isolated Workshop

ICS CyberVision – kľúčové vlastnosti (2/4)

2

- Combine collected data to understand “process & network” behaviors;
- Correlate with Threat Intelligence feeds;
- Interact with Control Engineer to add business context.



CONTROL

- Dynamic asset inventory.
- Connection mapping.
- Passive vulnerability Management.

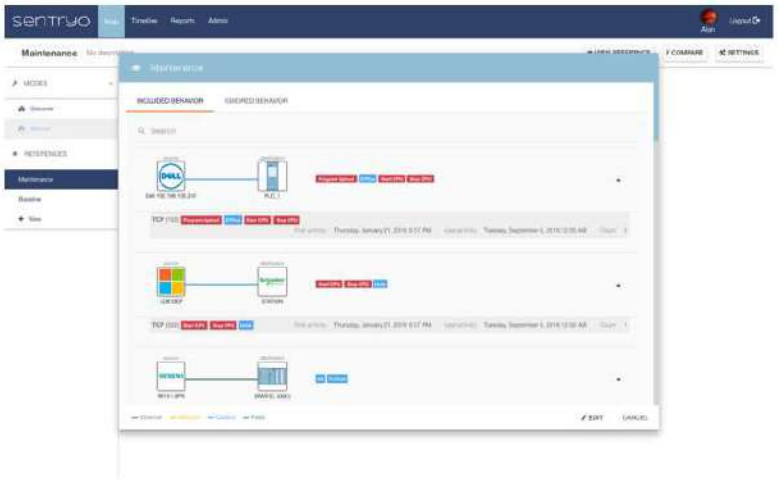
Benefits

Provide situational awareness and empower OT staff to reduce attack surface.

ICS CyberVision – kľúčové vlastnosti (3/4)

3

- Create *Baselines* as a set of behaviors;
- Add known malicious behaviour (IoC) through API;
- Use machine learning to classify behaviors and continuously improve detection.

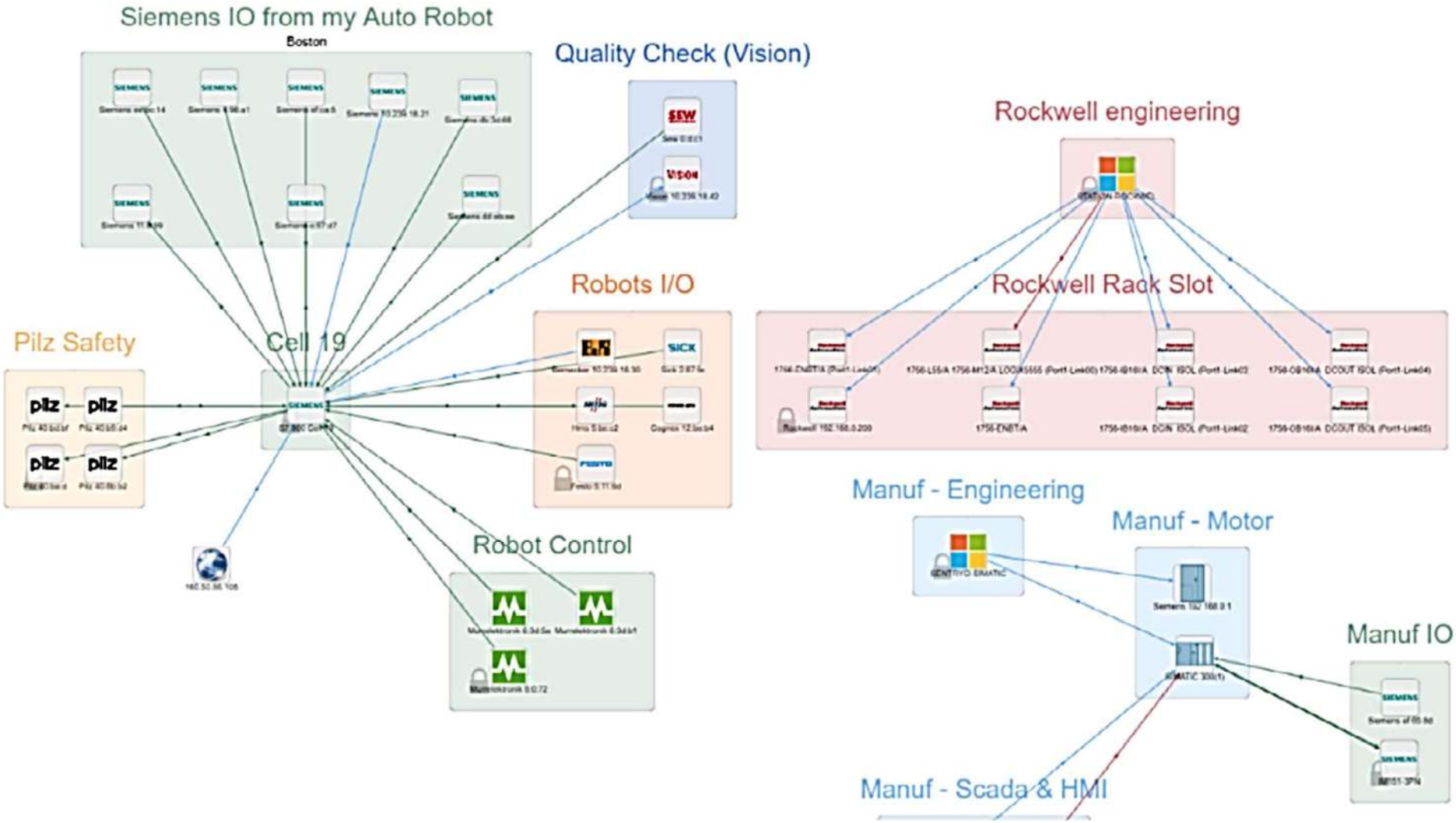


ALERT

- Detect abnormal events.
- Foster IT/OT collaboration to raise doubts and pinpoint the incident.

Benefits

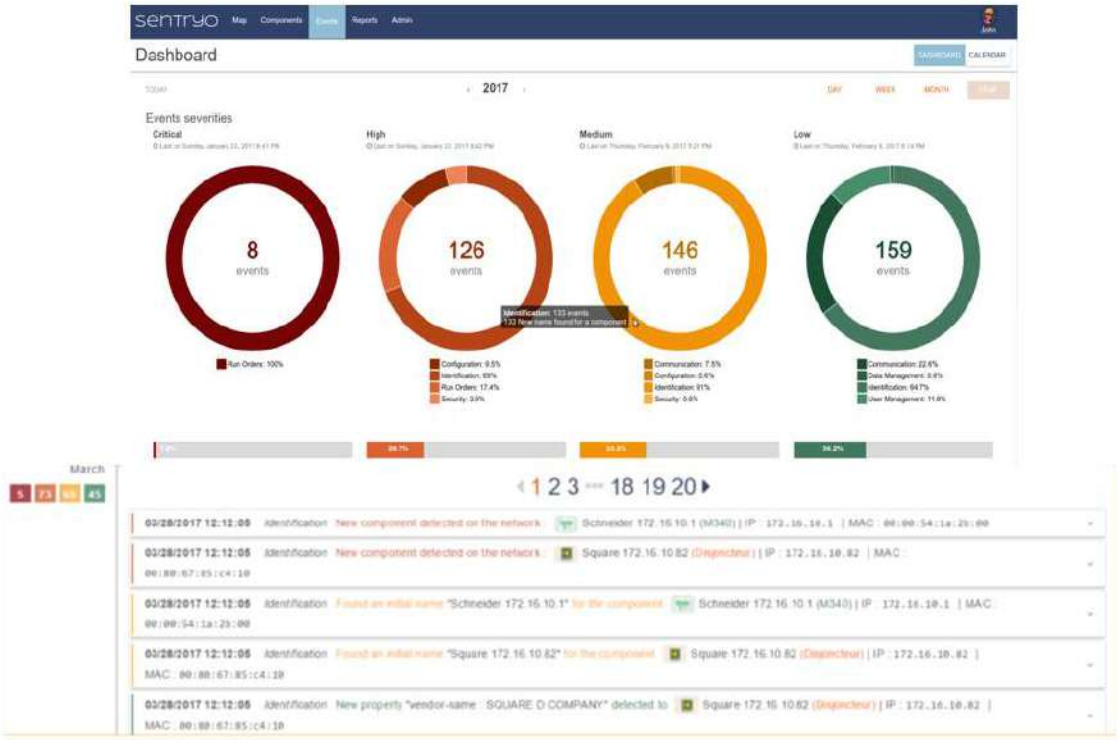
Identify malicious behaviors.


Siemens IO from my Auto Robot
Boston
Quality Check (Vision)
Rockwell engineering
Rockwell Rack Slot
Robots I/O
Pilz Safety
Cell 19
Robot Control
Manuf - Engineering
Manuf - Motor
Manuf IO
Manuf - Scada & HMI

ICS CyberVision – kľúčové vlastnosti (4/4)

4

- Record and store all extracted data and events
- Provide ongoing rolling full packet capture



RESPONSE

- Visualize and understand all current and past behaviors.
- Compare reference points.

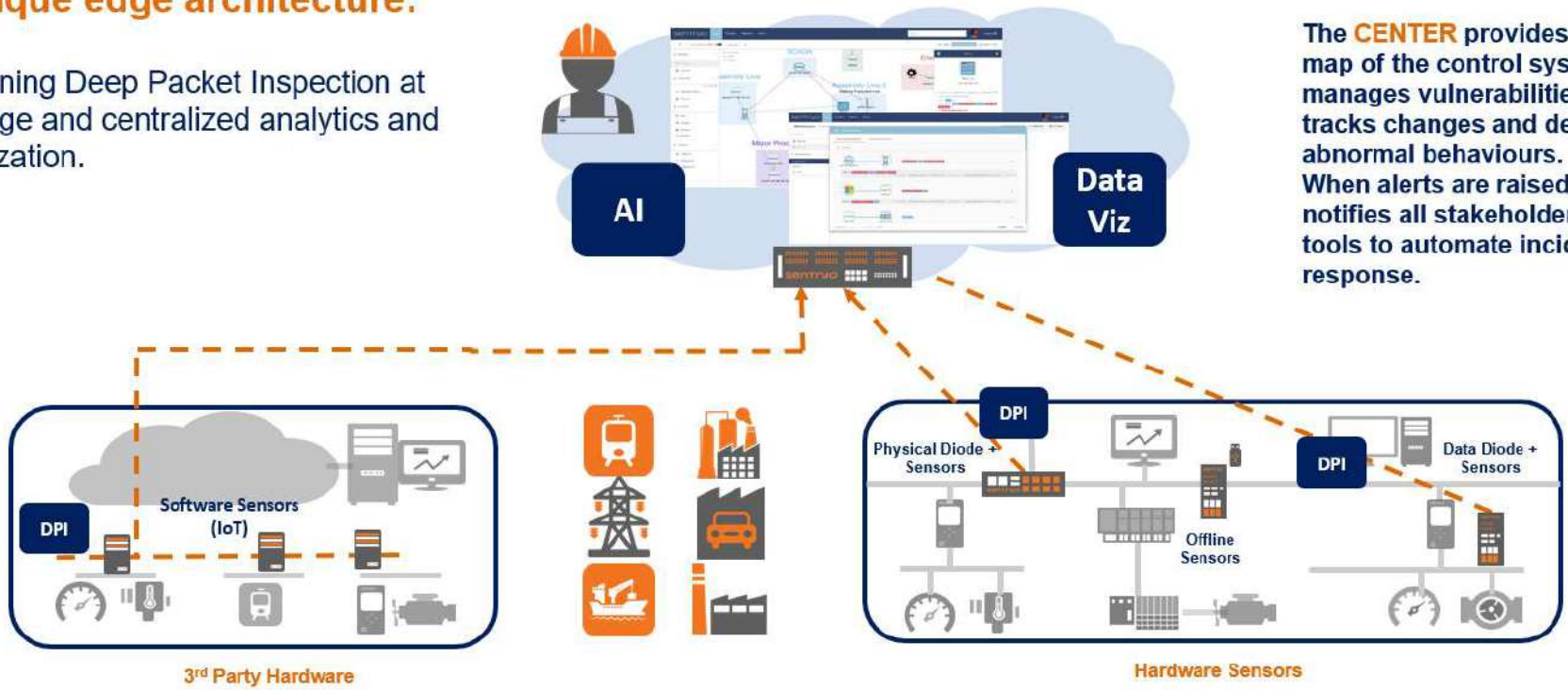
Benefits

Enable and streamline incident response
Accelerate remediation & recovery.

Globálna/všeobecná architektúra

A unique edge architecture:

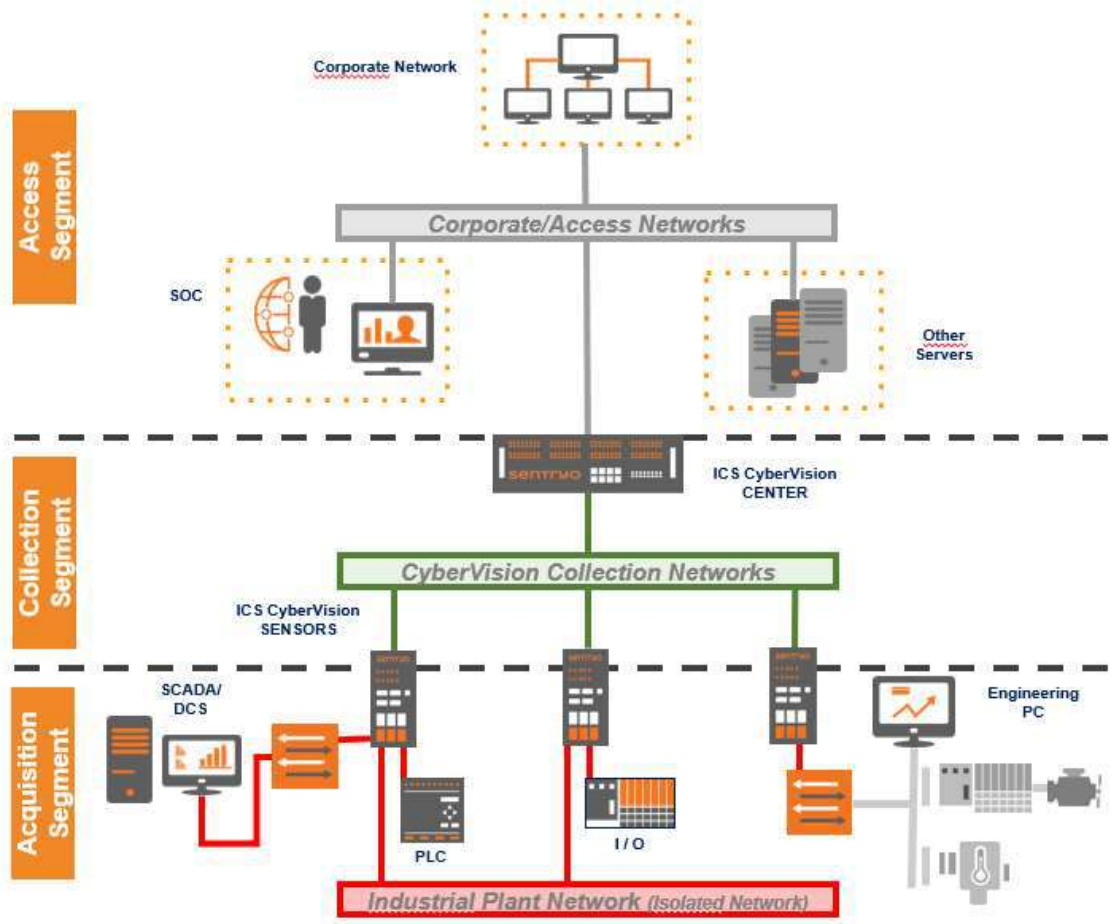
Combining Deep Packet Inspection at the Edge and centralized analytics and visualization.



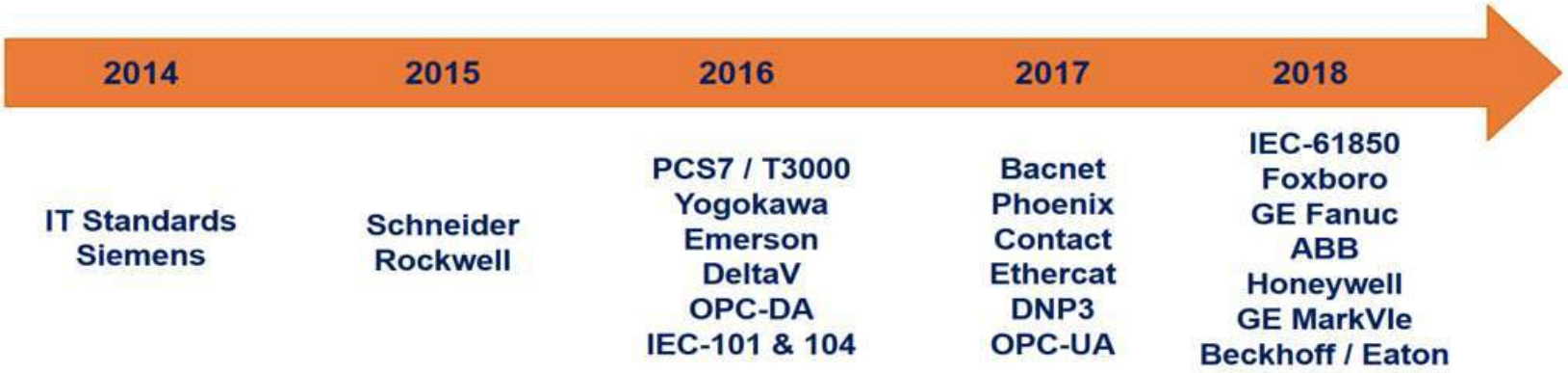
The CENTER provides a visual map of the control system, manages vulnerabilities, tracks changes and detects abnormal behaviours.
When alerts are raised, it notifies all stakeholders and IT tools to automate incident response.

Sensors deployed at the Edge of the network extract meaningful information from OT and Industrial IoT protocols.

3-úrovňová architektúra



Podporované OT protokoly



Information Extracted	Integrity (OT)	Security (IT)
Inventory	Assets Identification	Vulnerability Remote Access
Process control information	Process Control Configuration (Download, Stops, etc..) Process Control Operation (variables, registers)	Reconnaissance detection Hacking tool identification
Network Information	System Dependencies	Indicator of Compromise matching

ICS CyberVision komponenty - podrobnejšie

CyberVision CENTER

Hardware appliance / Software appliance / Cloud deployment

CENTER10 & CENTER30
Hardware Appliance

CENTER VM
Software Appliance

CENTER CE
Cloud Edition

CyberVision SENSORS

Hardware appliance / 3rd Party appliance / Software appliance

Critical infrastructure → Industrial IoT*

SENSOR7
Fail-safe 1GB/s
TAP and Hardware
Data diode
included

SENSOR3
Industrial DIN
form factor

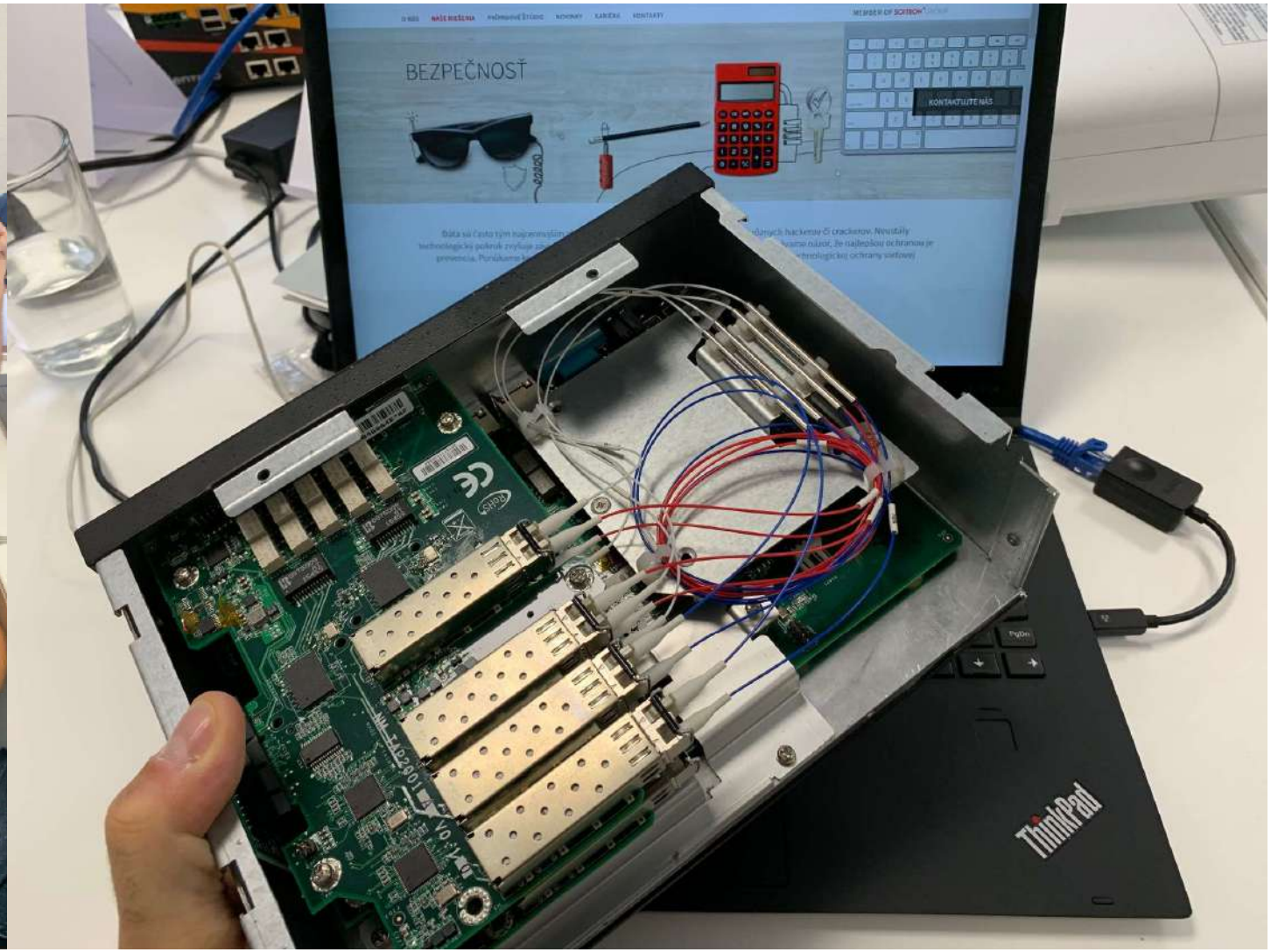
Siemens Nanobox & Microbox
Industrial PC

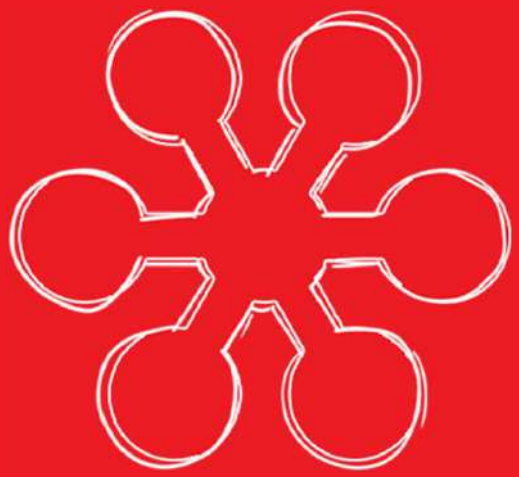
Cisco IE4K Industrial Switches
IoX Software
containers

Ruggedcom
Industrial switches

Software Appliance
Virtual Machine


sentryo


BEZPEČNOSŤ
KONTAKTUJTE NÁS
ThinkPad



SOITRON