GREYCORTEX

Efektivní využití nástroje GREYCORTEX Mendel pro ochranu OT sítí

| **SCADA SECURITY CONFERENCE** |

Ondřej Hubálek

GREYCORTEX **MENDEL**

Visibility

All the network communication, devices with inventory details, and user behavior

Detection

From misconfigurations, performance problems, or policy violations to undetected malware, ransomware, and hacker activities which are able to bypass existing security tools

Response

Rapid attack response, and incident investigation and management

\+

SCADA/ICS Monitoring

Application Performance Monitoring

Asset Inventory (2021)

Network Detection and Response / NDR

Advanced artificial intelligence, machine learning, data analysis and more traditional detection methods

GREYCORTEX

Endpoint | EDR | Server | Workload protection | Cloud | Email | Mobile | Firewall | Switch | Wireless | ZTNA

Network Detection and Response

Open APIs

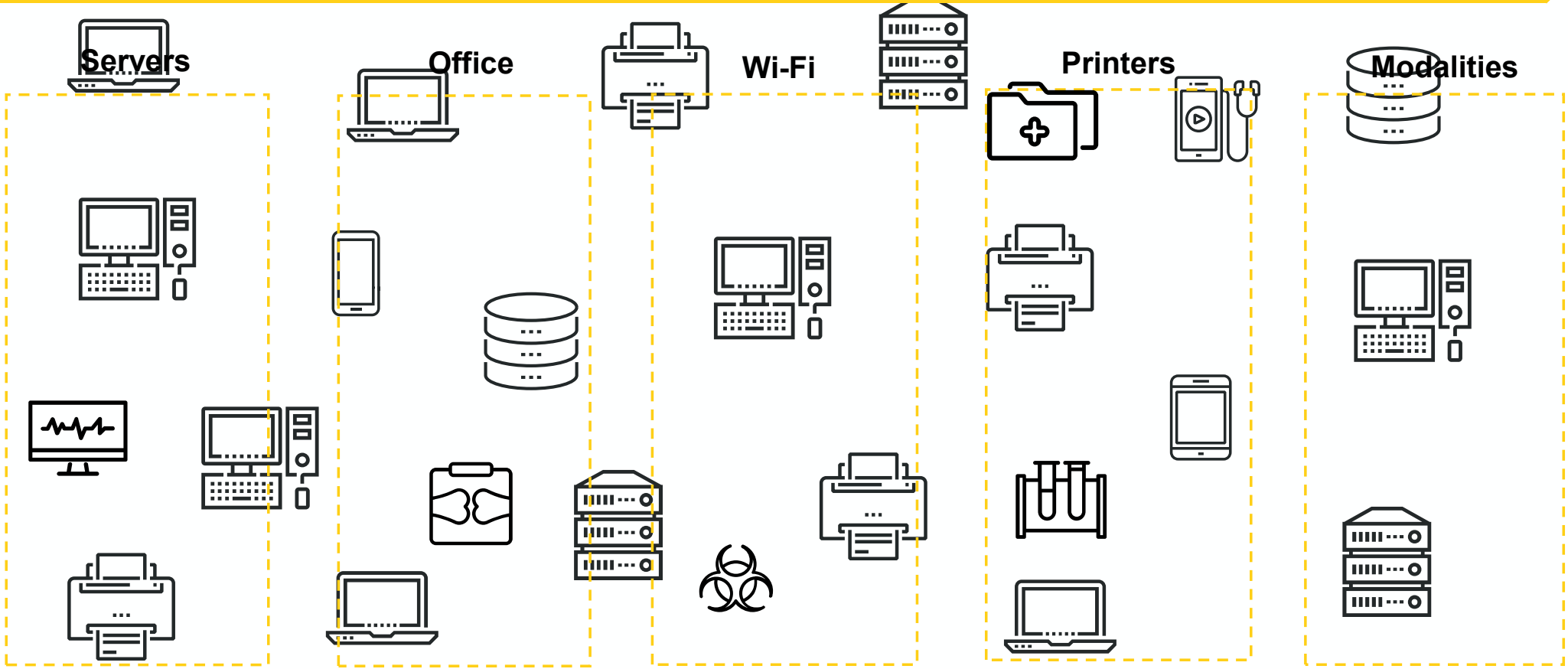
- Industry/Developer
- Service Provider
- Administrator
- Security Operations

Threat Intelligence

Artificial Intelligence

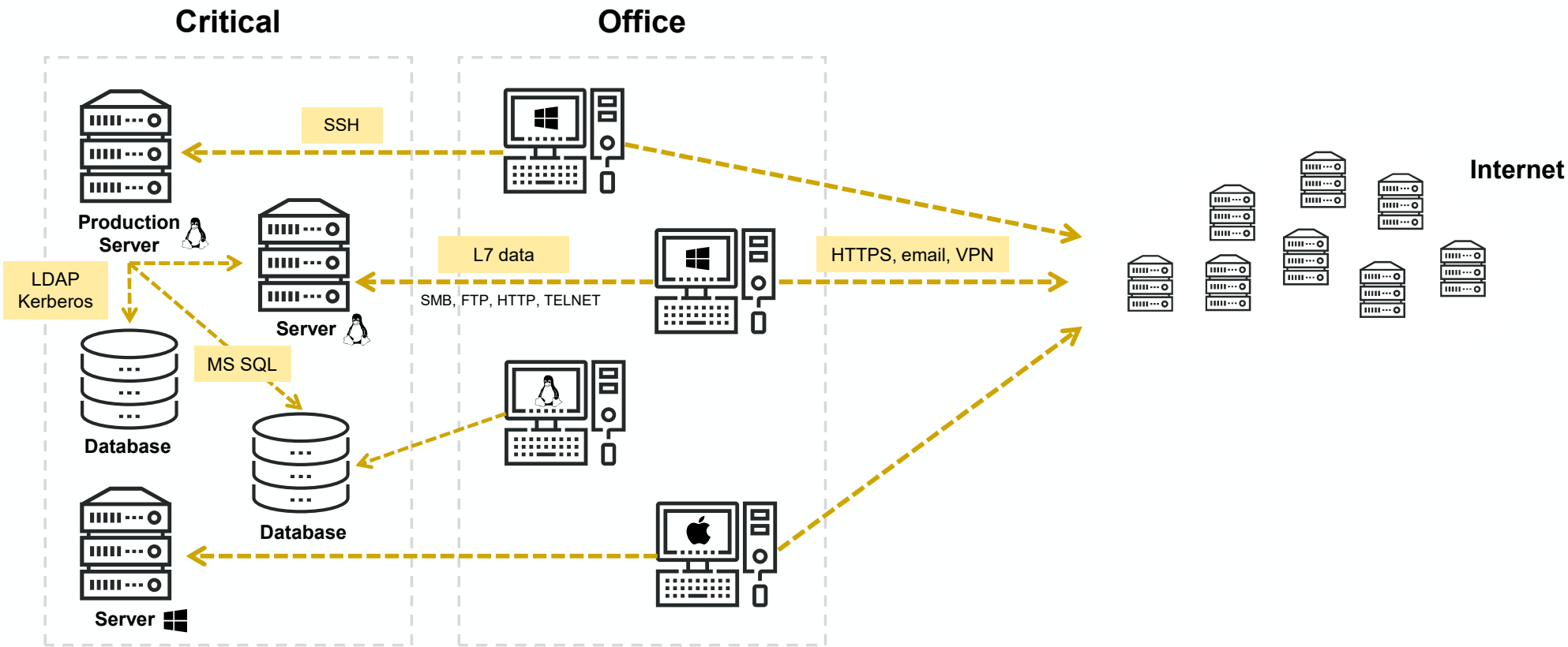
Data Lake

Visibility



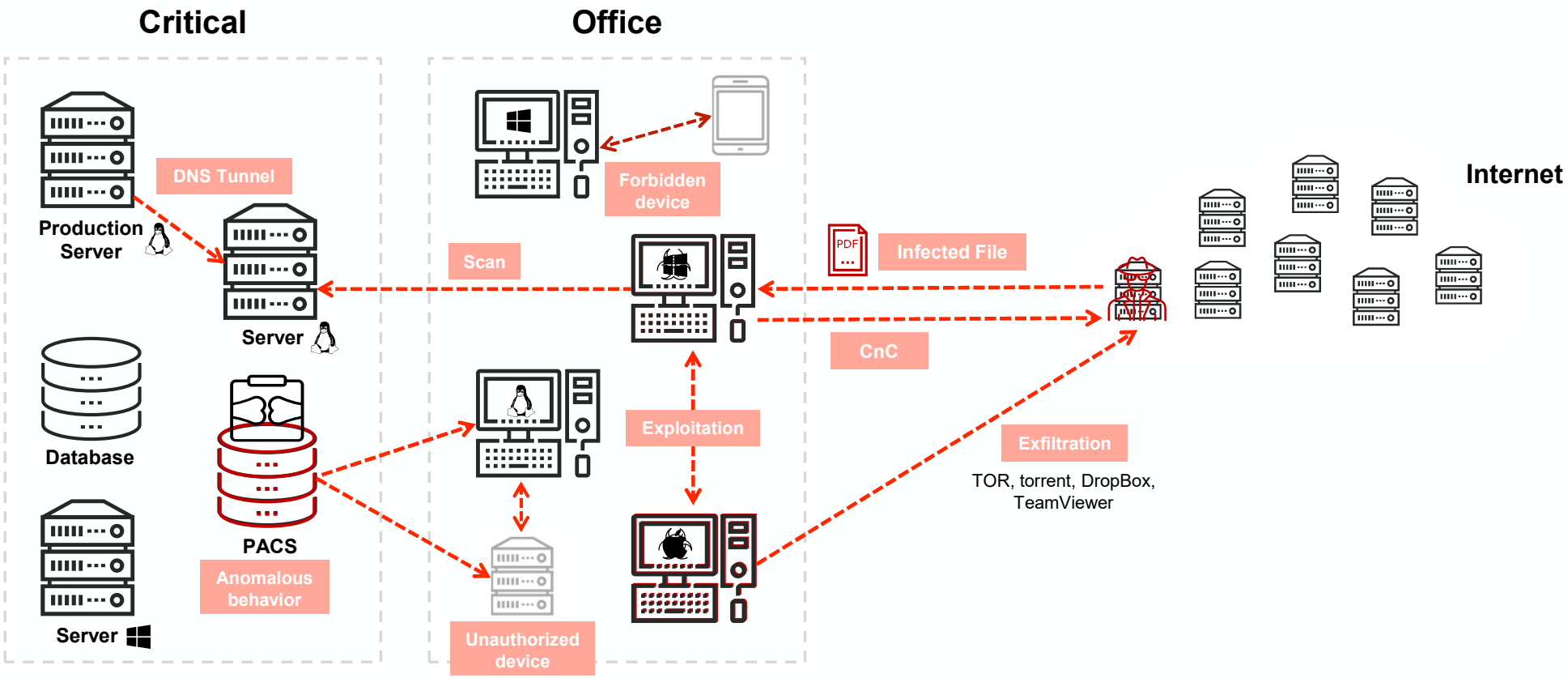
GREYCORTEX

Visibility



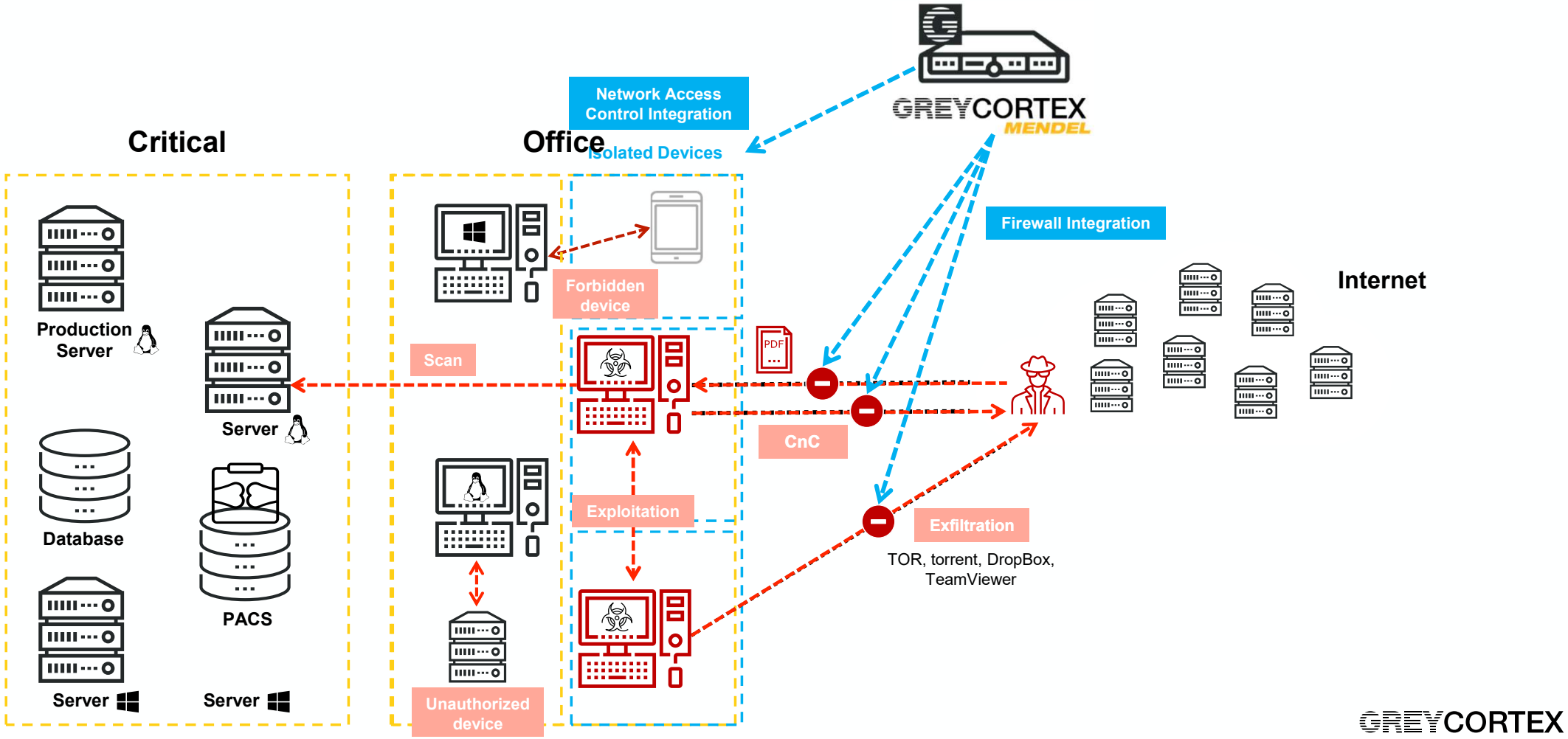
GREYCORTEX

Detection

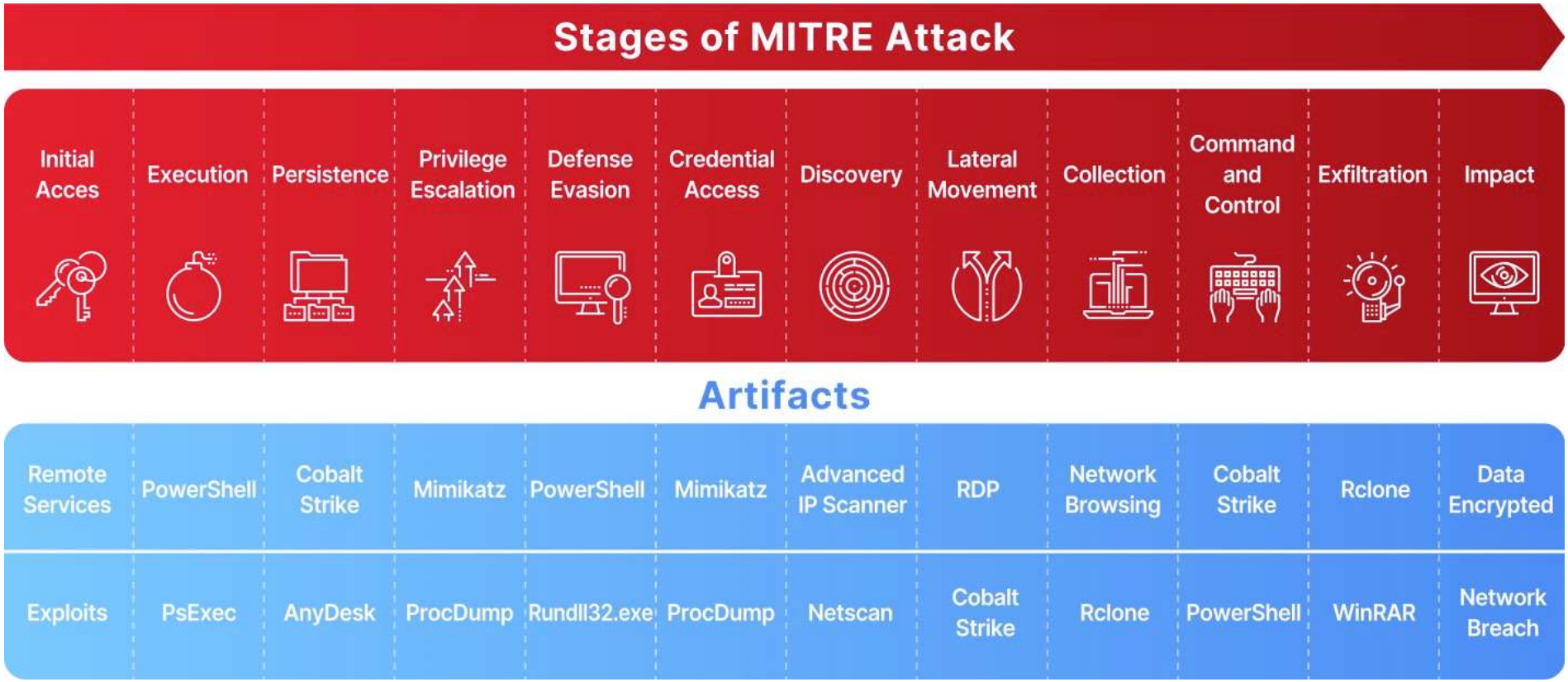


GREYCORTEX

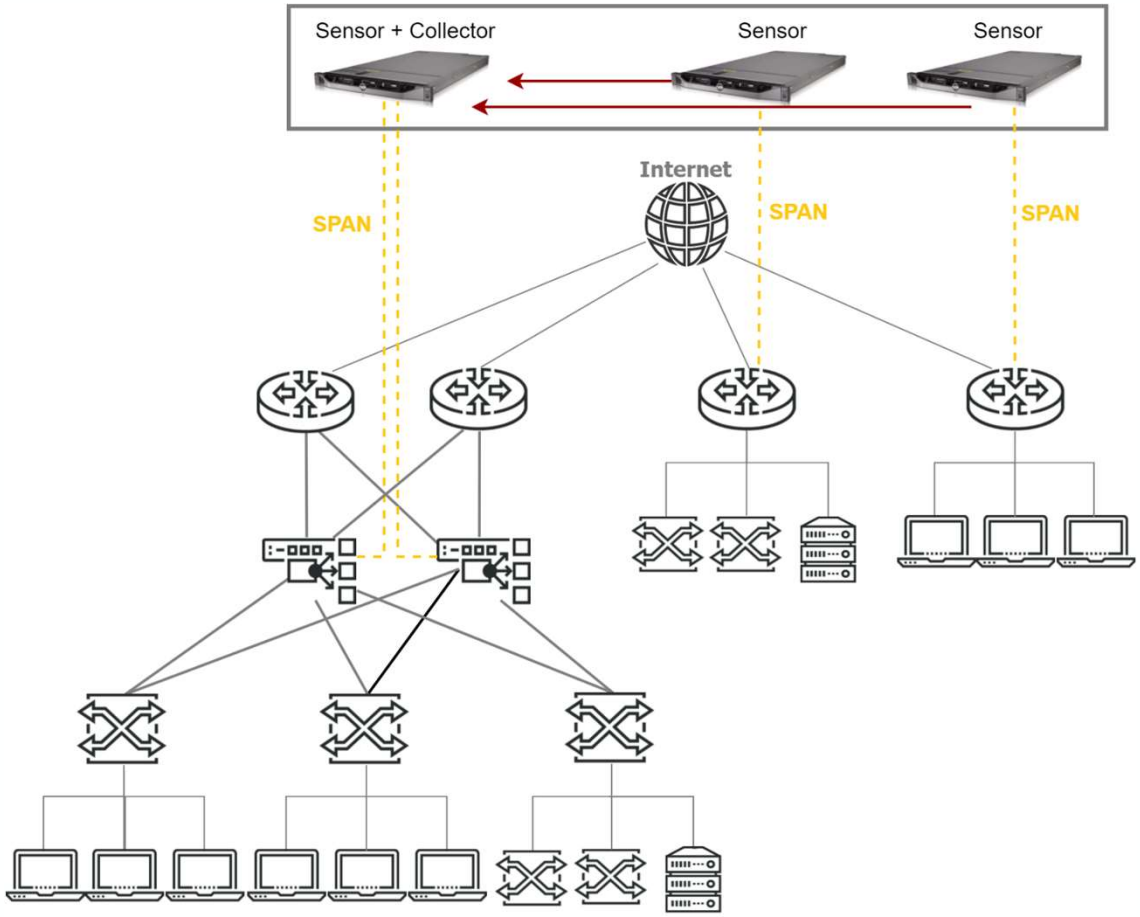
Response


Network Access Control Integration
GREYCORTEX MENDEL
Critical
Office
Isolated Devices
Firewall Integration
Internet
Production Server
Server
Database
PACS
Server
Server
Forbidden device
Scan
PDF
CnC
Exploitation
Exfiltration
TOR, torrent, DropBox, TeamViewer
Unauthorized device
GREYCORTEX

Adversaries Exploit Legitimate It Tools



Deployment



Sensors

- Port Mirroring (SPAN, RSPAN, ERSPAN)/TAP
- ASNM output (= 0,5% - 2% of traffic)
- Up to 100Gbps/sensor

Collectors

- 1 collector = 50+ sensors
- Aggregated input up to 100Gbps+
- Central collector for Events visualization

Devices

- Hardware
- Virtual (VMware ESXi, Hyper-V, KVM, …)
- Cloud (AWS, Azure, GCP)

GREYCORTEX

SCADA/ICS

www.greycortex.com

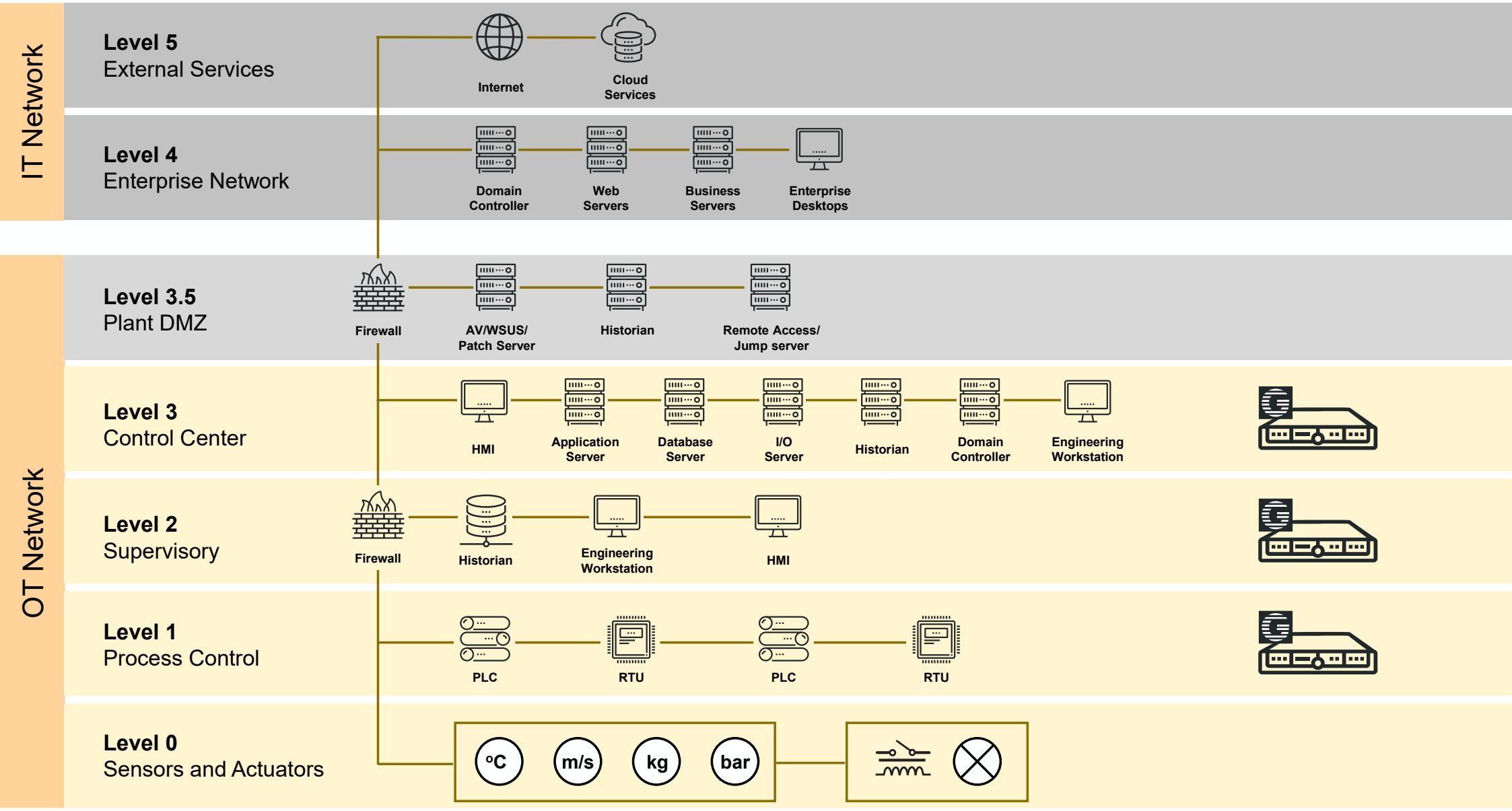
Běžné problémy v OT světě

- CyberSec v OT je kompletně nová disciplína.
- Pokud má zákazník špatnou CyberSec v IT, v OT neexistuje vůbec.
- Žádná segmentace, Žádné řízení přístupu.
- No Vulnerability Scans, No Patch-management.
- Staré protokoly - No Authentication, No Encryption.
- Jsme naprosto odděleni… a je tomu skutečně tak?

GREYCORTEX

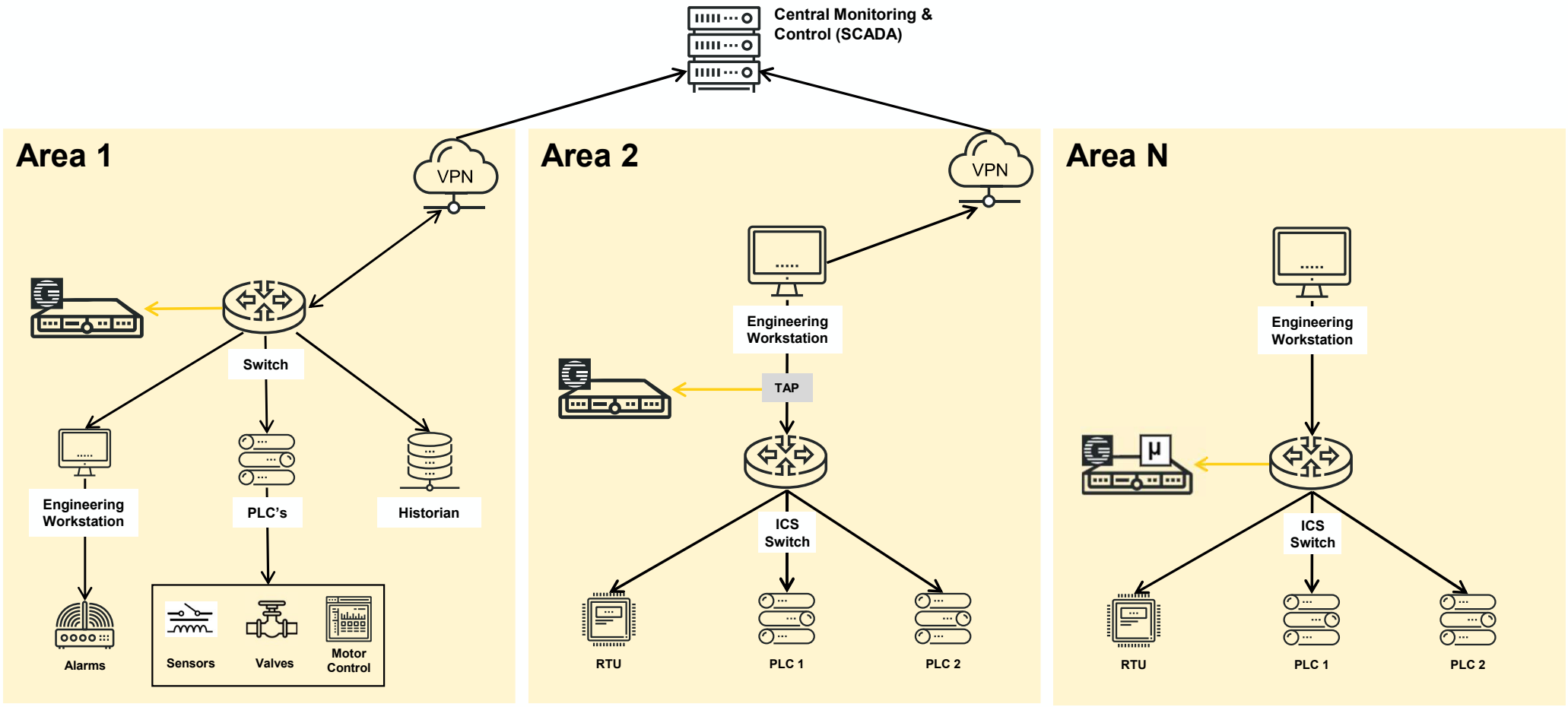
Možné typy útoků

- Získání přístupu k jednotlivým zařízením
- Modifikace nastavení
- Restart jednotlivých zařízení
- Zápis neznámého registru
- Přehrávání smyčky provozu PCAP-loop
- Škodlivý update firmware
- Cílené vyřazení jednotlivých zařízení


IT Network
OT Network
Level 5
External Services
Internet
Cloud Services
Level 4
Enterprise Network
Domain Controller
Web Servers
Business Servers
Enterprise Desktops
Level 3.5
Plant DMZ
Firewall
AV/WSUS/ Patch Server
Historian
Remote Access/ Jump server
Level 3
Control Center
HMI
Application Server
Database Server
I/O Server
Historian
Domain Controller
Engineering Workstation
Level 2
Supervisory
Firewall
Historian
Engineering Workstation
HMI
Level 1
Process Control
PLC
RTU
PLC
RTU
Level 0
Sensors and Actuators
°C
m/s
kg
bar

GREYCORTEX

Možnosti nasazení v OT



GREYCORTEX

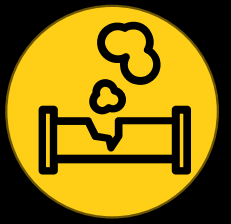
Zpracovávané OT protokoly

- **BACnet**
- **CoAP**
- **DLMS/COSEM**
- **DNP3**
- **ENIP**
- **EtherCAT**
- **GE SRTP**
- **HART-IP**
- **IEC 60870-5-104 (IEC-104)**
- **IEC 61850 GOOSE**
- **IEC 61850 MMS**
- **IEC 61850 SV**
- **Modbus**
- **MQTT**
- **OPC Parser**
- **Profinet**
- **Profinet IO DCE/RPC**
- **Siemens S7**
- **CC-Link**
- **Mitsubishi**

GREYCORTEX Mendel chrání

Výroba a distribuce energií

Průmyslová výroba



Kritická infrastruktura

Správa budov

GREYCORTEX

GREYCORTEX

www.greycortex.com