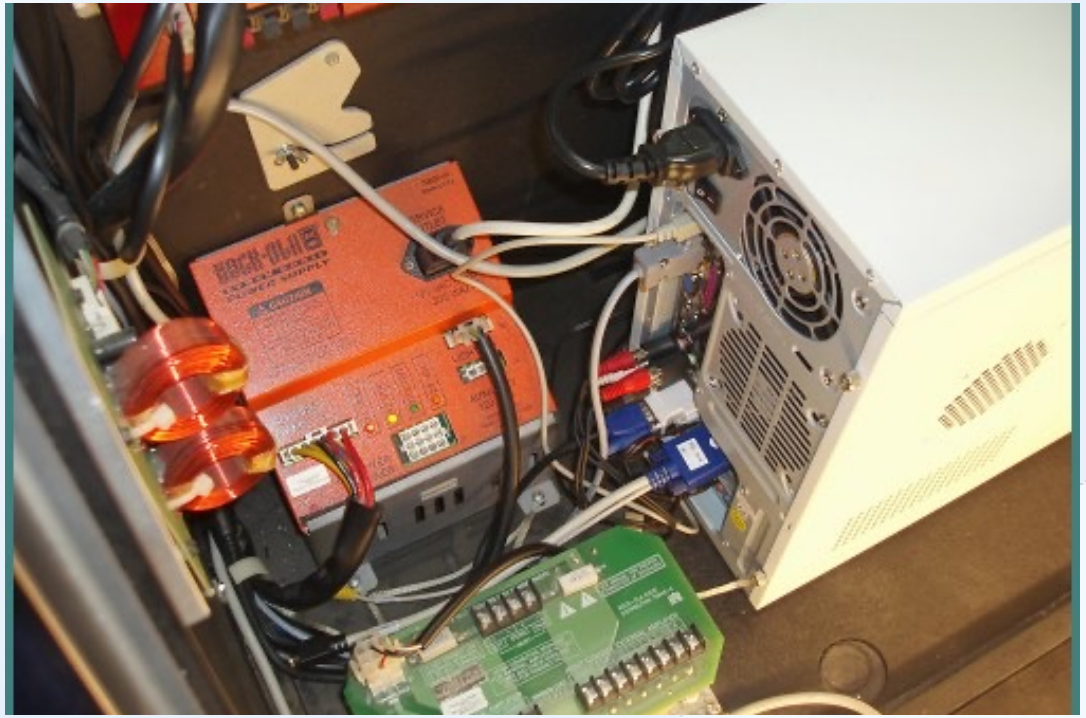
Progress® Flowmon®

SCADA SECURITY Konference

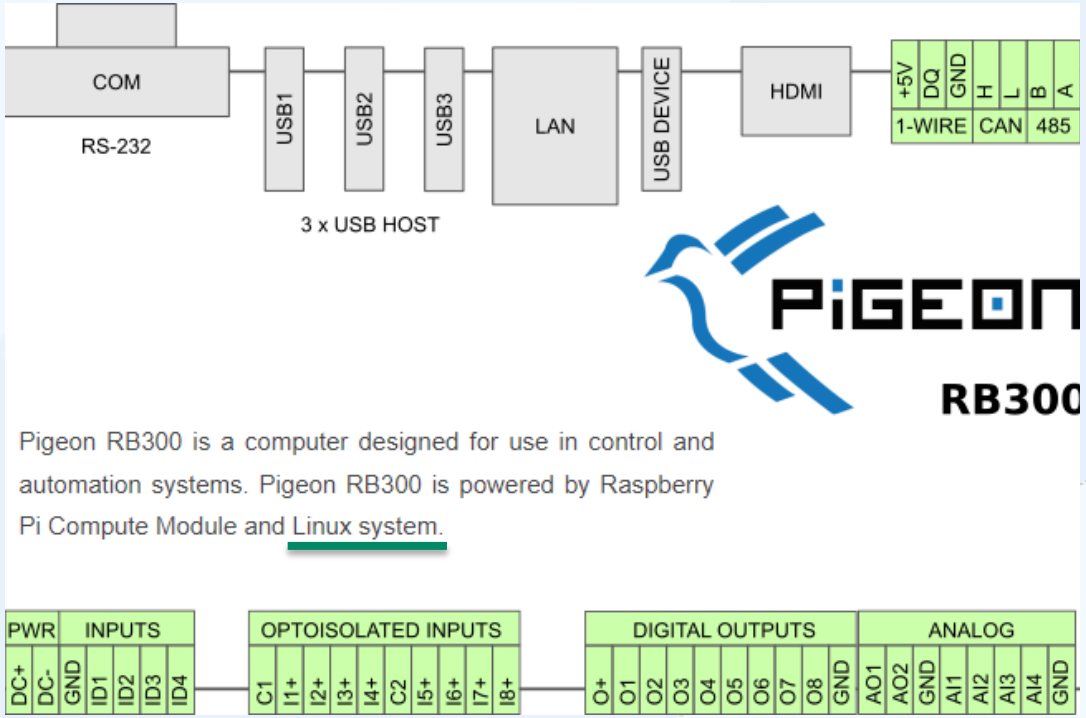
IT a OT jsou si blíže, než se zdá

Pavel Minařík
Vice President of Technology
27. dubna 2023

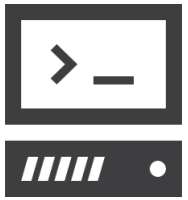


Product Description

- 1.5T active shield superconducting magnet
- Gradient System (Performance Controls Incorporation, U
- RF System: Spectrometer: All-digital (MR Solutions Ltd., UK
- RF Amplifier: Peak power: 18KW (Analogic, USA)
- Transmitting Coil
- Computer system: CPU: dual core ≥2.8GHz; RAM: ≥2GB;
- Main display: ≥24´´LCD TFT monitoring
- Console: New communication user software interface, b
- Operation system: Windows XP Professional Monitoring d monitoring, multi-parameter monitoring



OT/SCADA/ICS challenges



Endpoint security difficult to enforce

Absence of network visibility

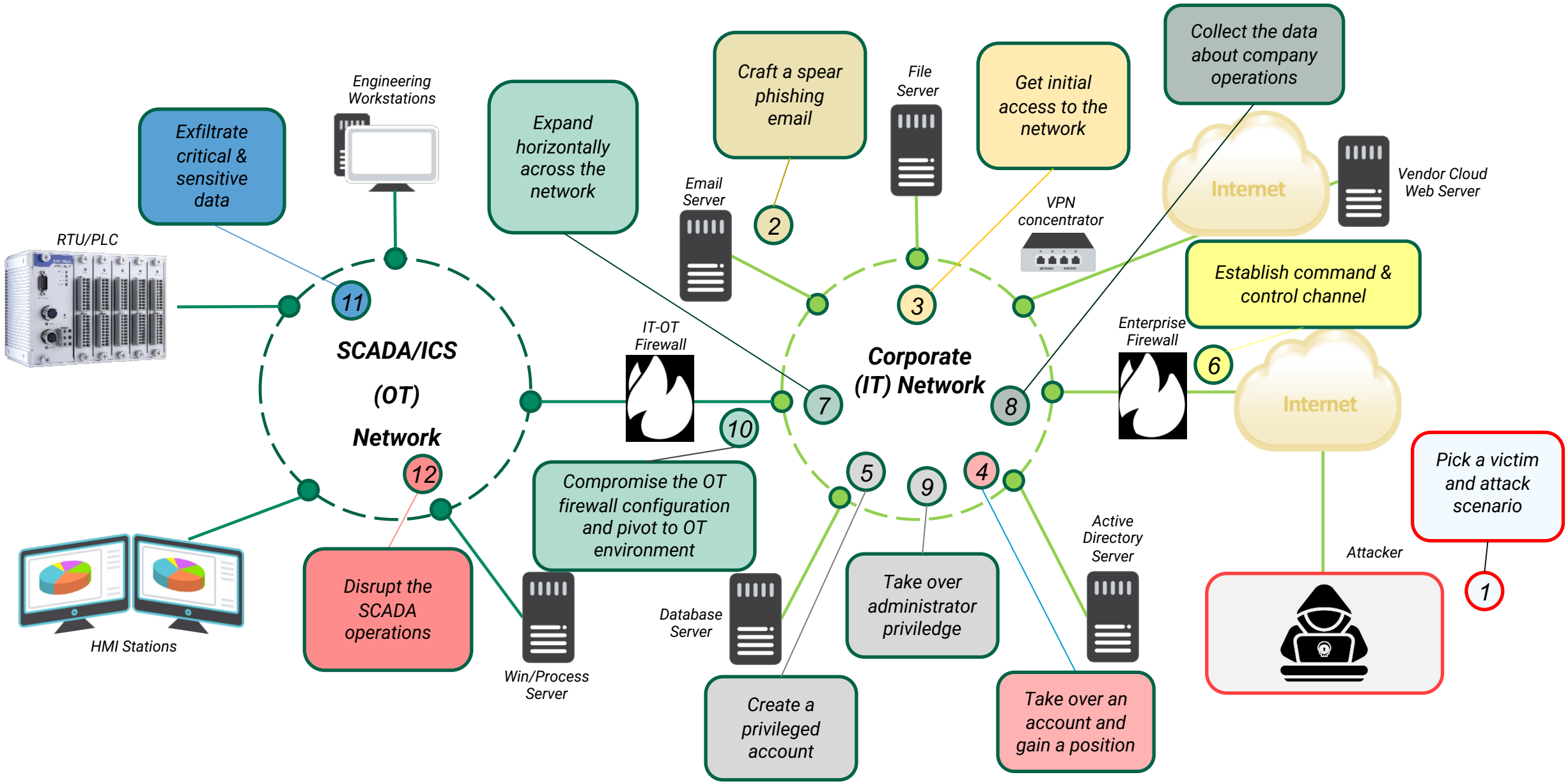
"An important drawback derived from the connection to intranets and communication networks, is the increased vulnerability to computer network-based attacks."

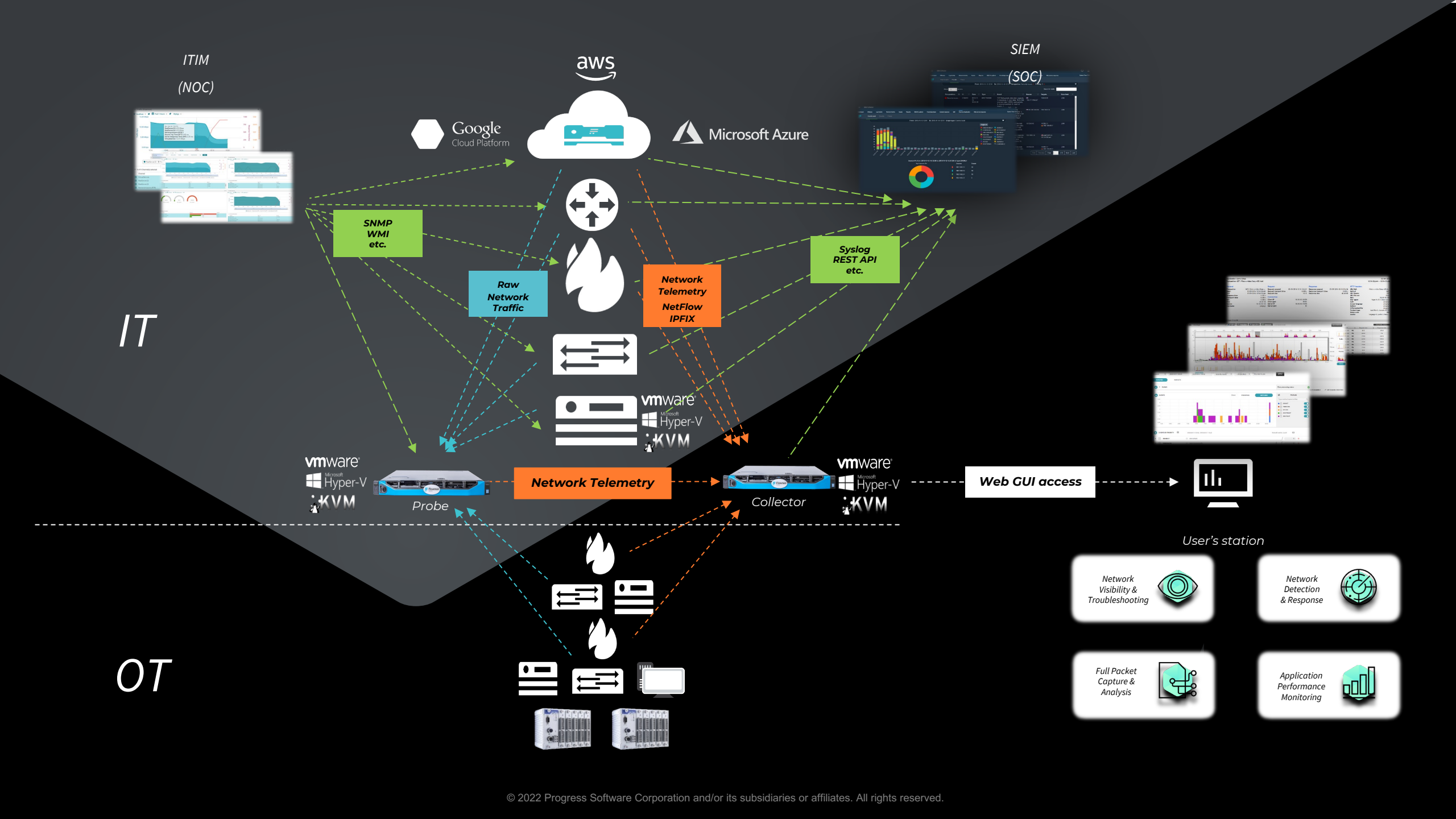
Source: European Union Agency for Network and Information Security

Absence of security design and processes

Non-existing or irregular patching of systems

Obsolete equipment and OS





You Cannot Secure What You Cannot See

Single source of truth across both IT/OT environment

Time matters, threat actors shall be detected as early as possible

See each packet traversing your environment

Detect indicators of compromise in both IT/OT using a single tool

Progress

Případová studie

Provozní stav naší sítě má přímý dopad na více než milion domácností a podniků, o které se staráme. Jakékoli pochybení při dodávkách elektřiny by mohlo způsobit nevyčíslitelné škody.“

Martin Keprt

Vedoucí správy kybernetické a fyzické bezpečnosti eg.d

Fakta

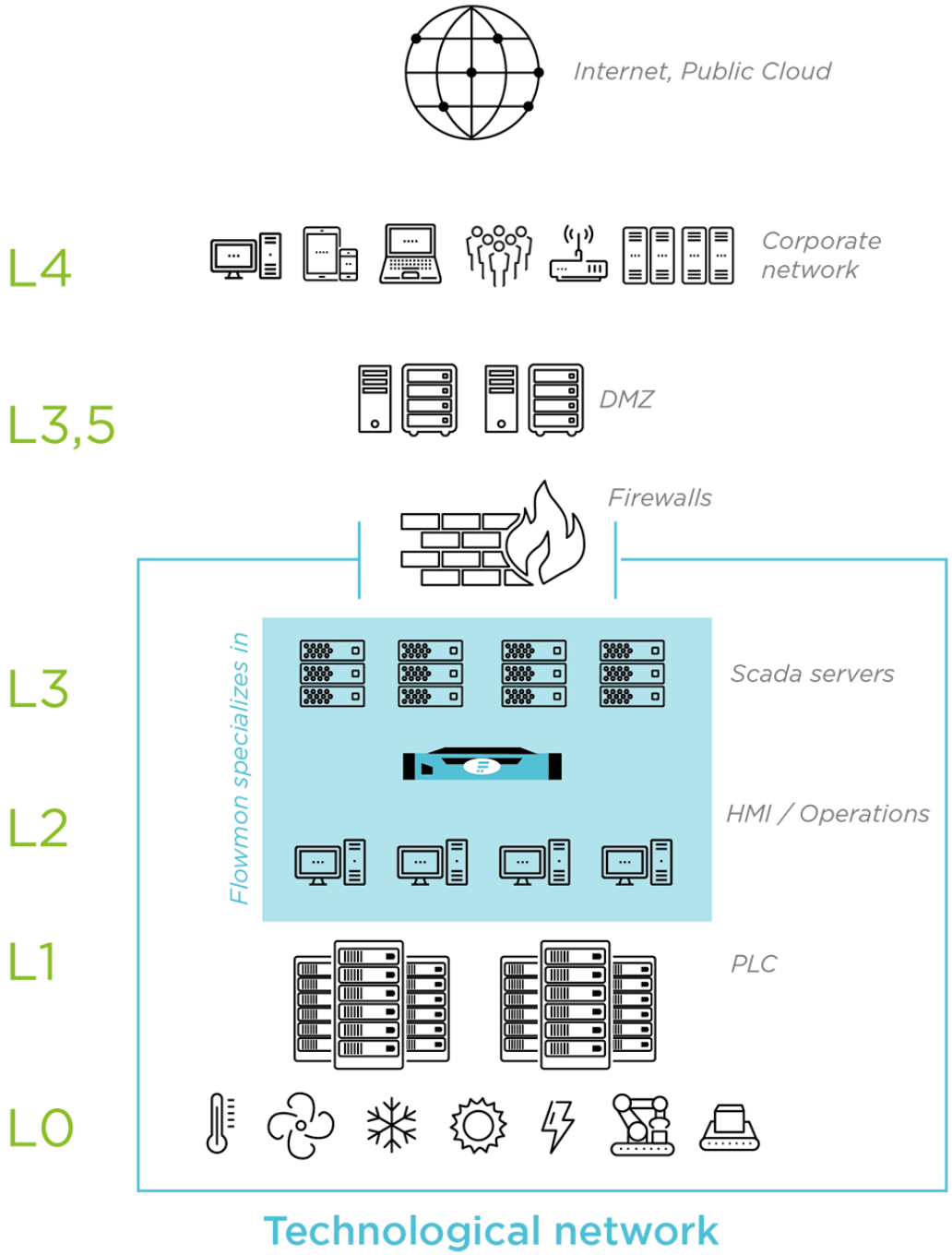
- Nasazeno více než 90 monitorovacích sond v klíčových bodech sítě v kombinaci s se sběrem dat z existujících routerů
- Integrace dat a výstupů do systému SIEM
- Podpora specifických protokolů IEC 104 a IEC 61850
- Pokryto prostředí OT i LAN

Ihned po nasazení nám systém pomohl identifikovat několik chybně nakonfigurovaných zařízení. Umožňuje nám vidět veškerý provoz na jednom místě a dokáže nás varovat před případnými problémy. Poskytuje nám informace o využití sítě, poukazuje na potenciální úzká místa, odhaluje hrozby v síti a podává zprávy o různých anomáliích síťového provozu.“

Martin Keprt

Vedoucí správy kybernetické a fyzické bezpečnosti EG.D

Progress



Reference

- Případová studie EG.D [URL]
- Flowmon pro ICS/SCADA [URL]
- SCADA hack demo video [URL]
- Nezávislá studie řešení Flowmon na základě testu NISTIR 8219 realizovaného VUT Brno [URL]


Progress®