KYBERNETICKÁ OCHRANA PRIEMYSELNÝCH TECHNOLÓGIÍ

Marek Gajarský

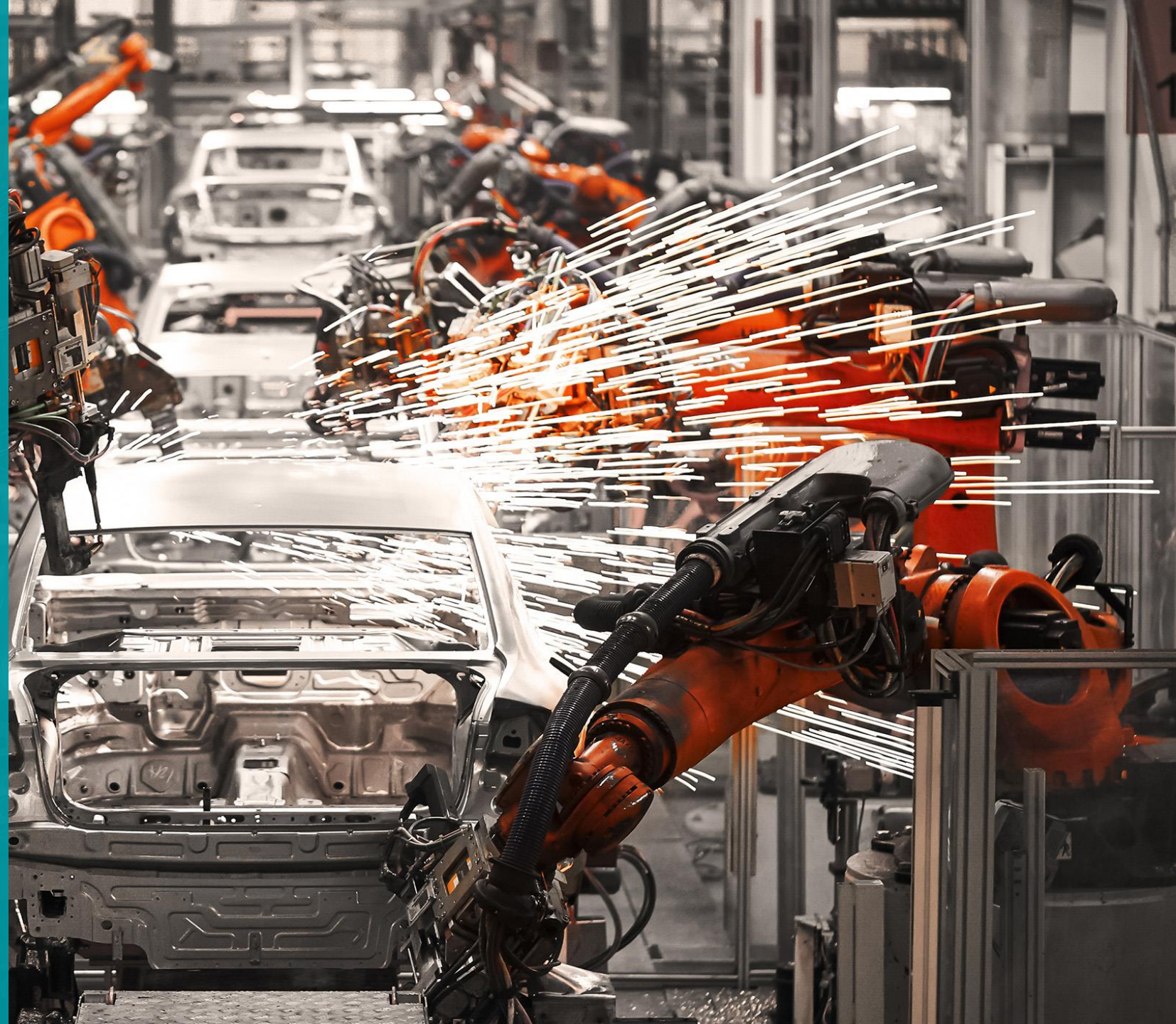
Digital Security
Progress. Protected.

&

SME KONFERENCIE

Priemyselné technológie (OT)

- Výroba
- Rozvodné siete
- Doprava
- Skladovanie a logistika
- Zdravotníctvo
- Inteligentné mestá a budovy

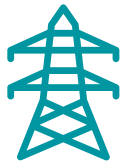


- Systémy s fyzickou izoláciou (Air Gapped)
- Systémy s čiastočnou izoláciou (Semi-Air Gapped)
- Technologické silá
- Technologická evolúcia
- Priemysel 4.0 (Industry 4.0)
- Priemysel 5.0 (Industry 5.0)

Kybernetické útoky na priemyselné odvetvie

2016

Industroyer – Ukrajina: Malvér zameraný na priemyselné riadiace systémy v elektrických rozvodniach.



2017

Triton - Saudskoarabský petrochemický závod: Malvér zameraný na bezpečnostné systémy s cieľom spôsobiť rozsiahle fyzické škody.

2019

LockerGoga - Norsk Hydro: Ransomvérový útok spôsobujúci výrazné narušenie prevádzky.

2020

DarkSide - Colonial Pipeline: Ransomvér vedúci k prerušeniu dodávok paliva

2021

Conti – Írsko Health Service Executive: Ransomvér spôsobujúci narušenie zdravotnej starostlivosti.

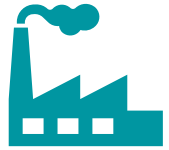
2022

SolarWinds - Útoky na dodávateľské reťazce: Cielené útoky na zraniteľnosti v OT prostrediach v rámci dodávateľských reťazcov.

2023

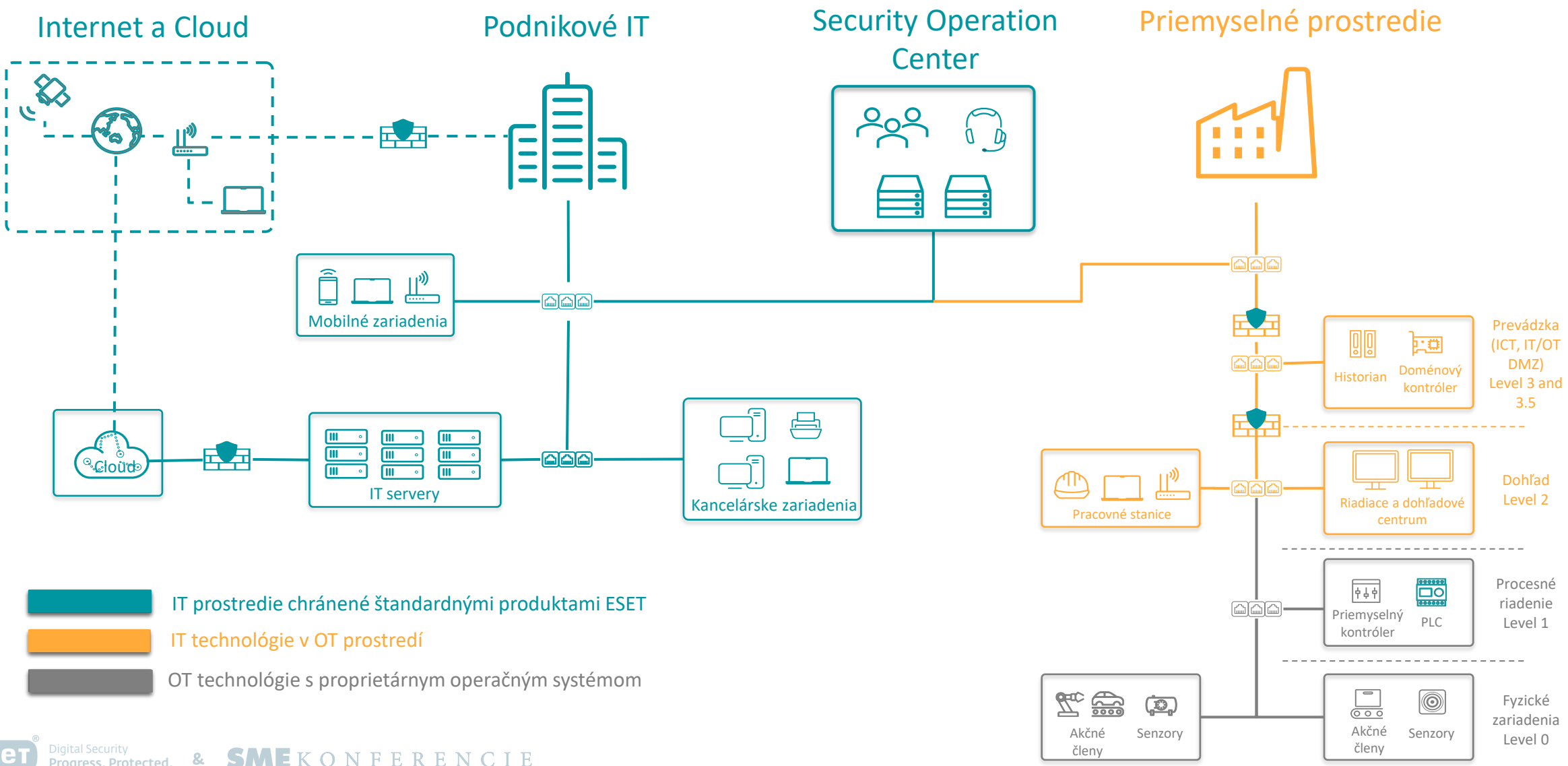
CyberAv3ngers - Vodáreň Aliquippa: Cielený útok na priemyselný riadiaci systém.

2024

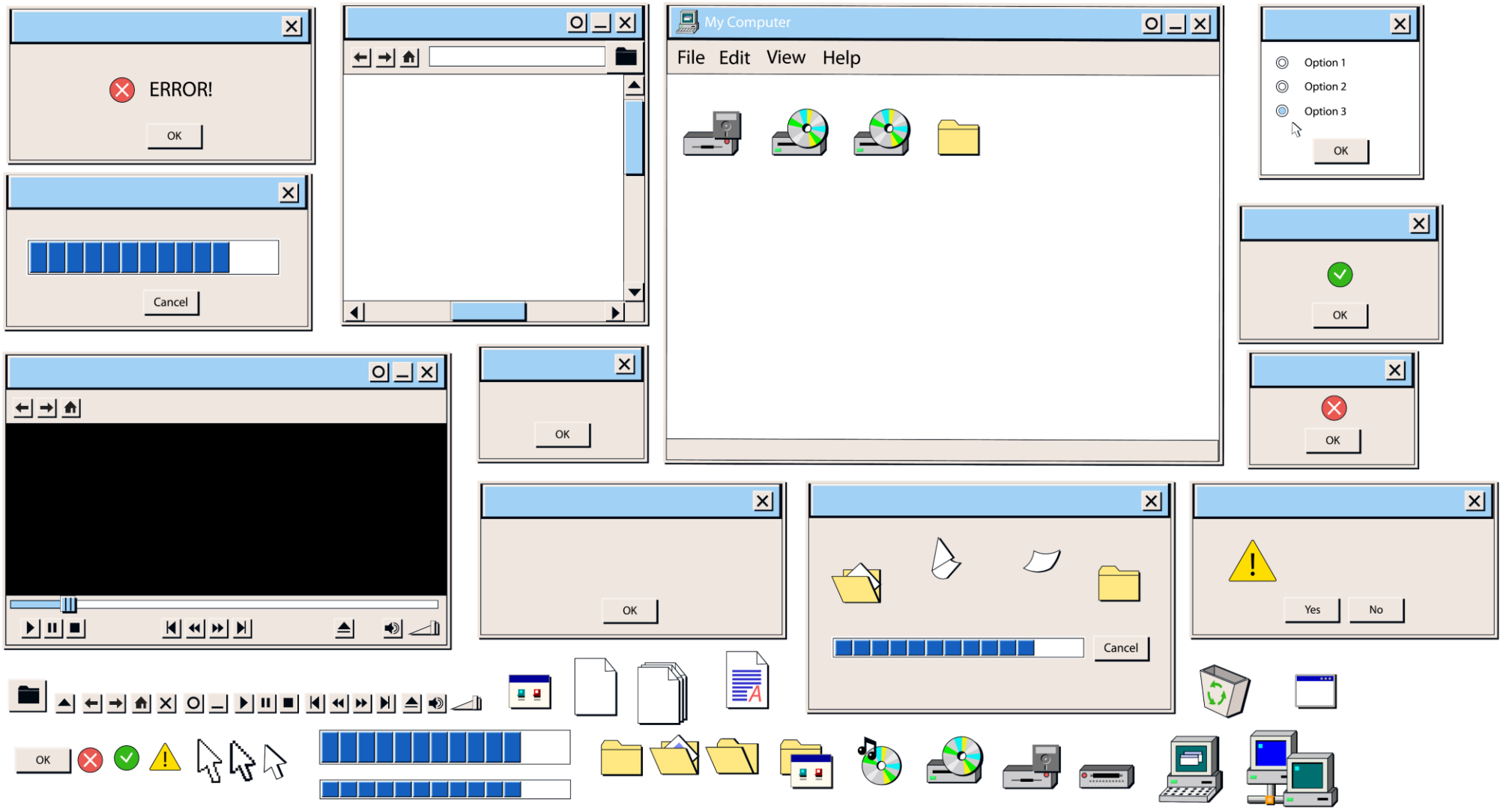


Volt Typhoon - Kritická infraštruktúra USA: Čínska štátna skupina opakovane využívajúca zero-day zraniteľnosti v rámci OT prostredí.

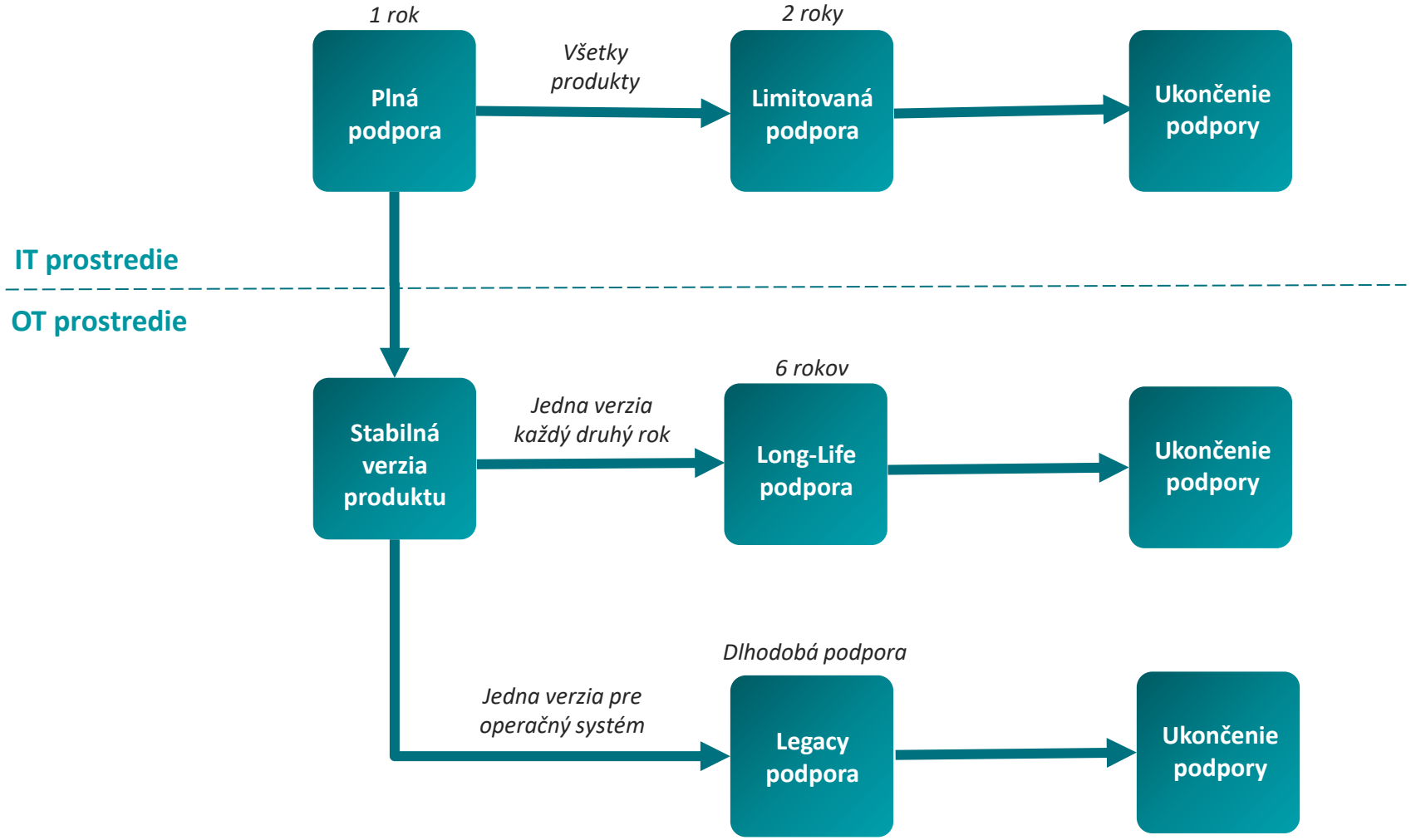
Referenčná architektúra IT/OT prostredia



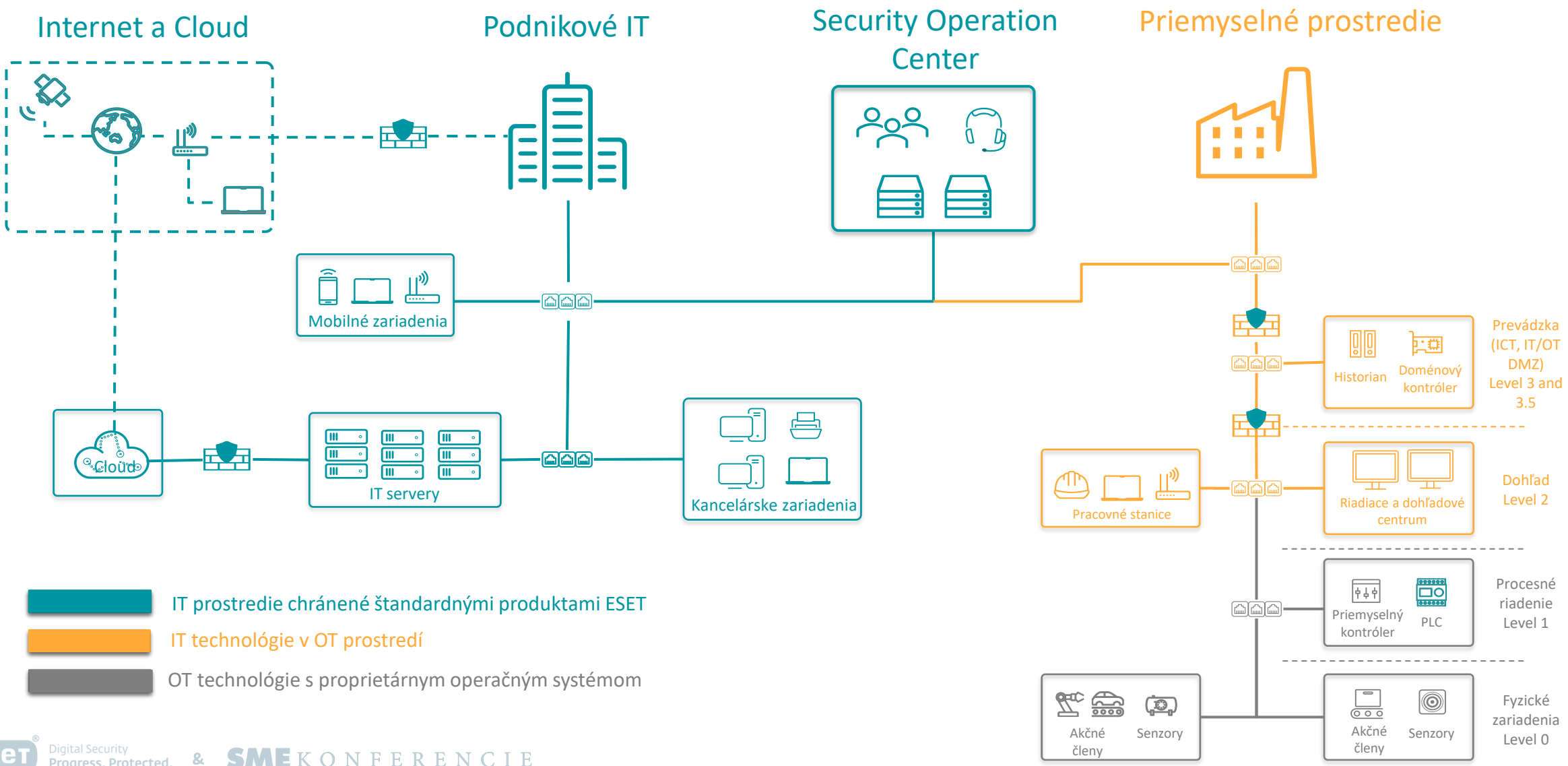
Životný cyklus priemyselného softvéru



Životný cyklus ochrany koncových zariadení ESET



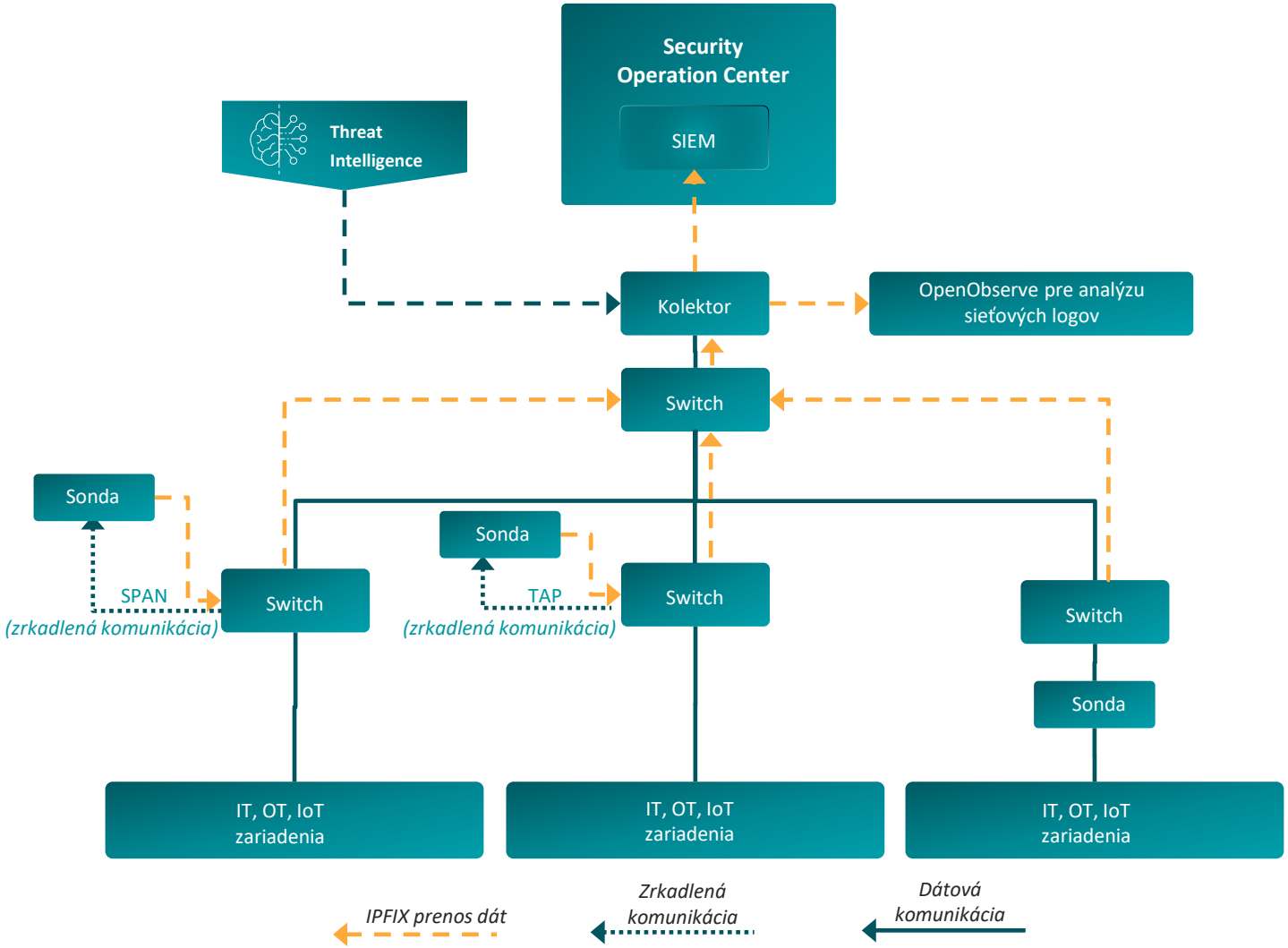
Referenčná architektúra IT/OT prostredia



Fázy kybernetického útoku

Fáza útoku	Koncový bod	Sieť
Skenovanie a objavovanie		✓
Počiatočný prístup		✓
Prenos škodlivého SW	✓	✓
Spustenie škodlivého SW	✓	
Zvýšenie oprávnení	✓	
Zhromažďovanie informácií	✓	✓
Bočný pohyb		✓
Velenie a riadenie (C2)		✓
Prenos zákazníckych údajov		✓

ESET sieťová sonda pre pokročilú analýzu dátového toku



Sonda: Nasadená v kľúčových sieťových bodoch na zabezpečenie analýzy prevádzky.

Prenos dát a telemetria: Sonda odosiela dáta pomocou štandardného NetFlow (IP, port, protokol) cez UDP IPFIX do kolektora. Rozšírená telemetria pridáva výstupy (domény, protokoly, adresy URL) do štandardného NetFlow.

Kolektor: Agreguje dáta, aplikuje pravidlá detekcie (pomocou ESET Threat Intelligence) a označuje škodlivú prevádzku.

Export údajov: Kolektor odosiela optimalizované údaje IPFIX/JSON s detekčnými hlavičkami do SIEMu.

OpenObserve: Umožňuje hĺbkovú kontrolu logov sieťovej prevádzky.

Eliminácia podozrivých sieťových aktivít

Viacúrovňová kybernetická ochrana

On-prem
Cloud

Threat Intelligence
APT reports

Úroveň 1
Centralizované riadenie
SIEM
SOAR

Úroveň 2
Centralizované komponenty
ESET Cloud Office Security
ESET Protect
ESET Inspect
ESET Net Protect
ESET Network Protect
3rd Party Solutions

Úroveň 3
Decentralizované komponenty
ESET Server Security
ESET Endpoint Security
Mobile Threat Defense
ESET Mail Security
SharePoint Security
Identity & Data Protection
Vulnerability & Patch Mgmt.
Deep Packet Inspection
Embedded Security
3rd Party Components

Chránený perimeter
Cloud Mail
Cloud Storage
Cloud Platforms
MS Cloud Collaboration
Endpoints
Servers
Mail
Mobiles & Tablets
Networks
SharePoint
Industrial Servers
Industrial Endpoints
Legacy Endpoints
Industrial Smart Devices
OT Networks
Telecom Networks
PLC & Control Processors
IoT Devices & Sensors
Devices & Technologies
IoT & LoRa Networks

PURDUE Model
Cloud a externé systémy
Podnikové systémy
Level 5, 4
Prevádzkové a riadiace systémy
Level 3
Procesné technológie
Level 2, 1, 0

Úroveň 4
Long Life
Legacy OS
Regulations
Dark Web
Emergency
Attack Simulations
Additional Services

SECURITY DAYS

Ďakujem za pozornosť

Digital Security
Progress. Protected. & SME KONFERENCIE