Trellix

Join us at the EMEA Security Summit

Barcelona, Spain

17-19 JUNE 2024

Trellix

Key Principles, Challenges and Trellix Solutions to Secure OT and ICS

Diarmuid O’Boyle

Tanja Hofmann

Speaker Introduction

Diarmuid O'Boyle

Senior Solutions Engineer – OEM, Embedded

Tanja Hofmann

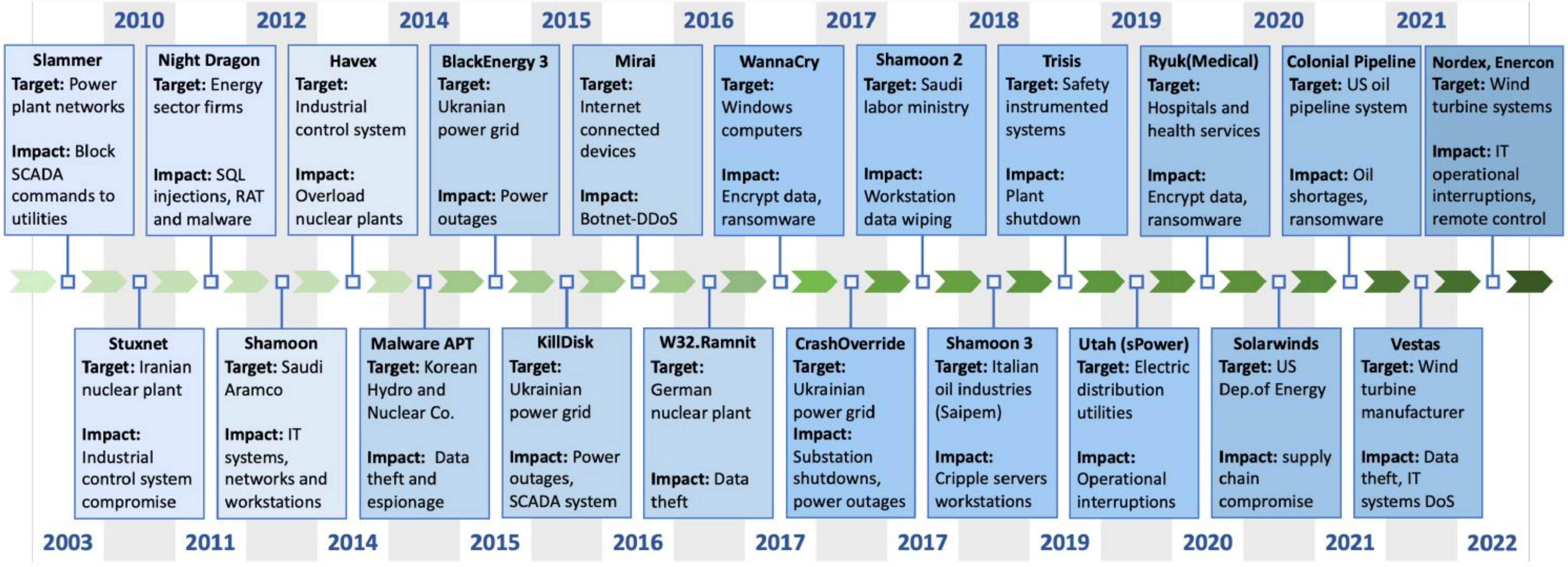
Senior Solutions Engineer

ICS Cyber Attacks

A brief history

Trellix

Cyber Attacks on Critical Infrastructure: A Historical Timeline



2003
Slammer
Target: Power plant networks
Impact: Block SCADA commands to utilities

2010
Stuxnet
Target: Iranian nuclear plant
Impact: Industrial control system compromise

2011
Night Dragon
Target: Energy sector firms
Impact: SQL injections, RAT and malware

2012
Shamoon
Target: Saudi Aramco
Impact: IT systems, networks and workstations

2014
Havex
Target: Industrial control system
Impact: Overload nuclear plants

2014
Malware APT
Target: Korean Hydro and Nuclear Co.
Impact: Data theft and espionage

2015
BlackEnergy 3
Target: Ukranian power grid
Impact: Power outages

2015
KillDisk
Target: Ukrainian power grid
Impact: Power outages, SCADA system

2016
Mirai
Target: Internet connected devices
Impact: Botnet-DDoS

2016
W32.Ramnit
Target: German nuclear plant
Impact: Data theft

2017
WannaCry
Target: Windows computers
Impact: Encrypt data, ransomware

2017
CrashOverride
Target: Ukrainian power grid
Impact: Substation shutdowns, power outages

2017
Shamoon 2
Target: Saudi labor ministry
Impact: Workstation data wiping

2018
Shamoon 3
Target: Italian oil industries (Saipem)
Impact: Cripple servers workstations

2019
Trisis
Target: Safety instrumented systems
Impact: Plant shutdown

2019
Utah (sPower)
Target: Electric distribution utilities
Impact: Operational interruptions

2020
Ryuk(Medical)
Target: Hospitals and health services
Impact: Encrypt data, ransomware

2020
Solarwinds
Target: US Dep.of Energy
Impact: supply chain compromise

2021
Colonial Pipeline
Target: US oil pipeline system
Impact: Oil shortages, ransomware

2021
Vestas
Target: Wind turbine manufacturer
Impact: Data theft, IT systems DoS

2022
Nordex, Enercon
Target: Wind turbine systems
Impact: IT operational interruptions, remote control

Trellix

Reference: https://www.researchgate.net/publication/360784464

Top 10 OT\ICS Cyber Attacks 2023

1. **US - Dole Food Company – Feb 2023**
Industry: Food Production
Actor: Ransomeware
Cost: $10.5M

2. **Germany - SAF-Holland – March 2023**
Industry: Vehicle Manufacturer
Actor: ALPHV\Blackcat Ransomware
Cost: €41M

3. **Israel – Galil Sewage – April 2023**
Industry: Wastewater
Actor: GhostSec
Cost: No Disclosed – Production Down 1 Day

4. **Germany – Baden Steel Works – April 2023**
Industry: Steel Plant
Actor: Unknown
Cost: No Disclosed – Production Down

4. **US – Americold – April 2023**
Industry: Cold Storage
Actor: Cactus Ransomware
Cost: No Disclosed – Production Down 1 Week

6. **Denmark – Danish Critical Energy – May 2023**
Industry: Critical Energy
Actor: Sandworm Group
Cost: Unknown

7. **India – Granules India – May 2023**
Industry: Drug Manufacturer
Actor: Lockbit
Cost: Undisclosed – Production Down 40+ Days

8. **US – Brunswick Corp – June 2023**
Industry: Marine Manufacturing
Actor: Unknown
Cost: $85M+

9. **US – MGM Resorts – Sept 2023**
Industry: Casino and Resorts
Actor: ALPHV\Scattered Spider
Cost: $110M

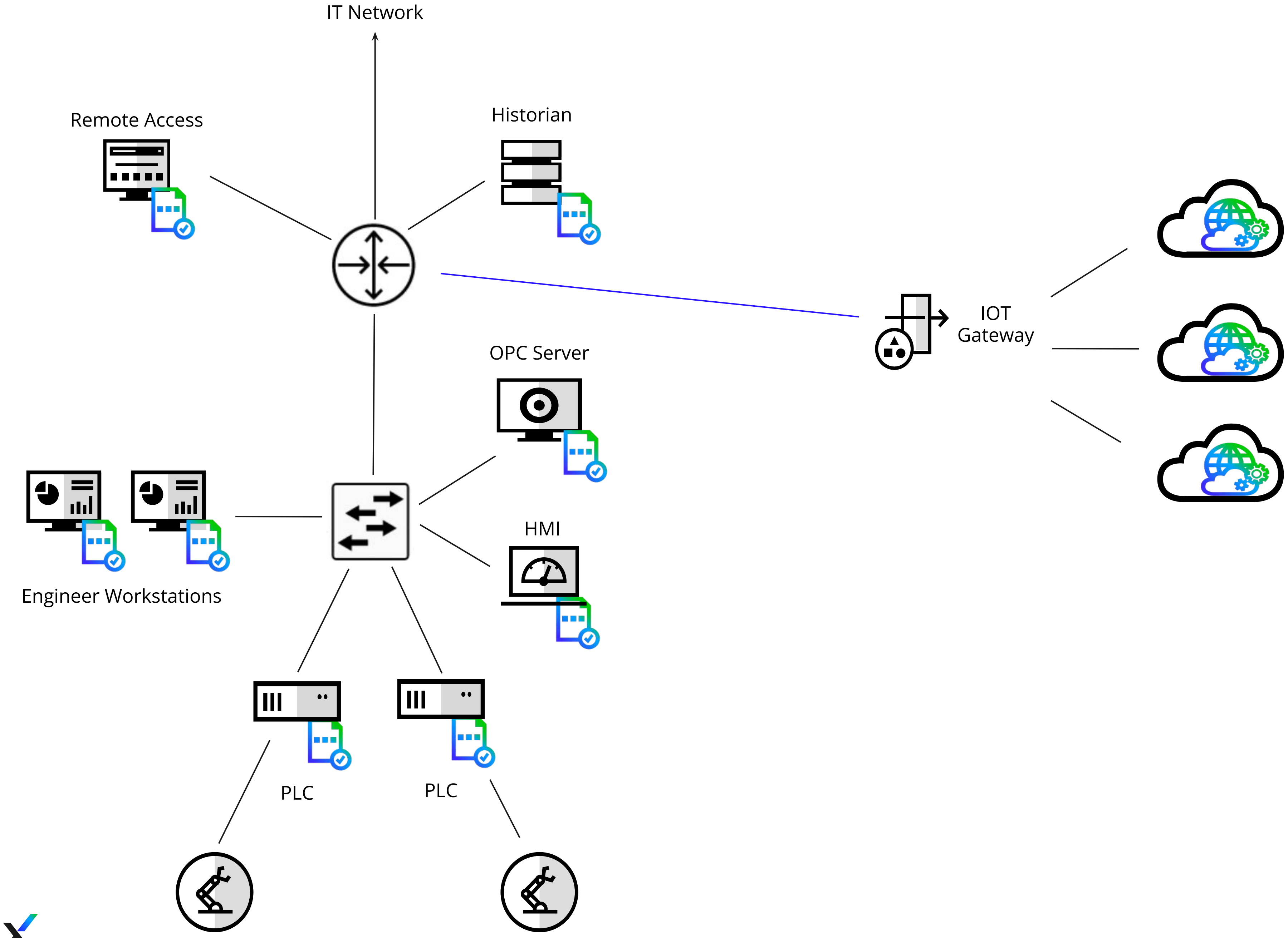
10. **Australia – DP World Australian Ports – Nov 2023**
Industry: Transportation
Actor: Unknown
Cost: 10 Day Backlog of 30K containers

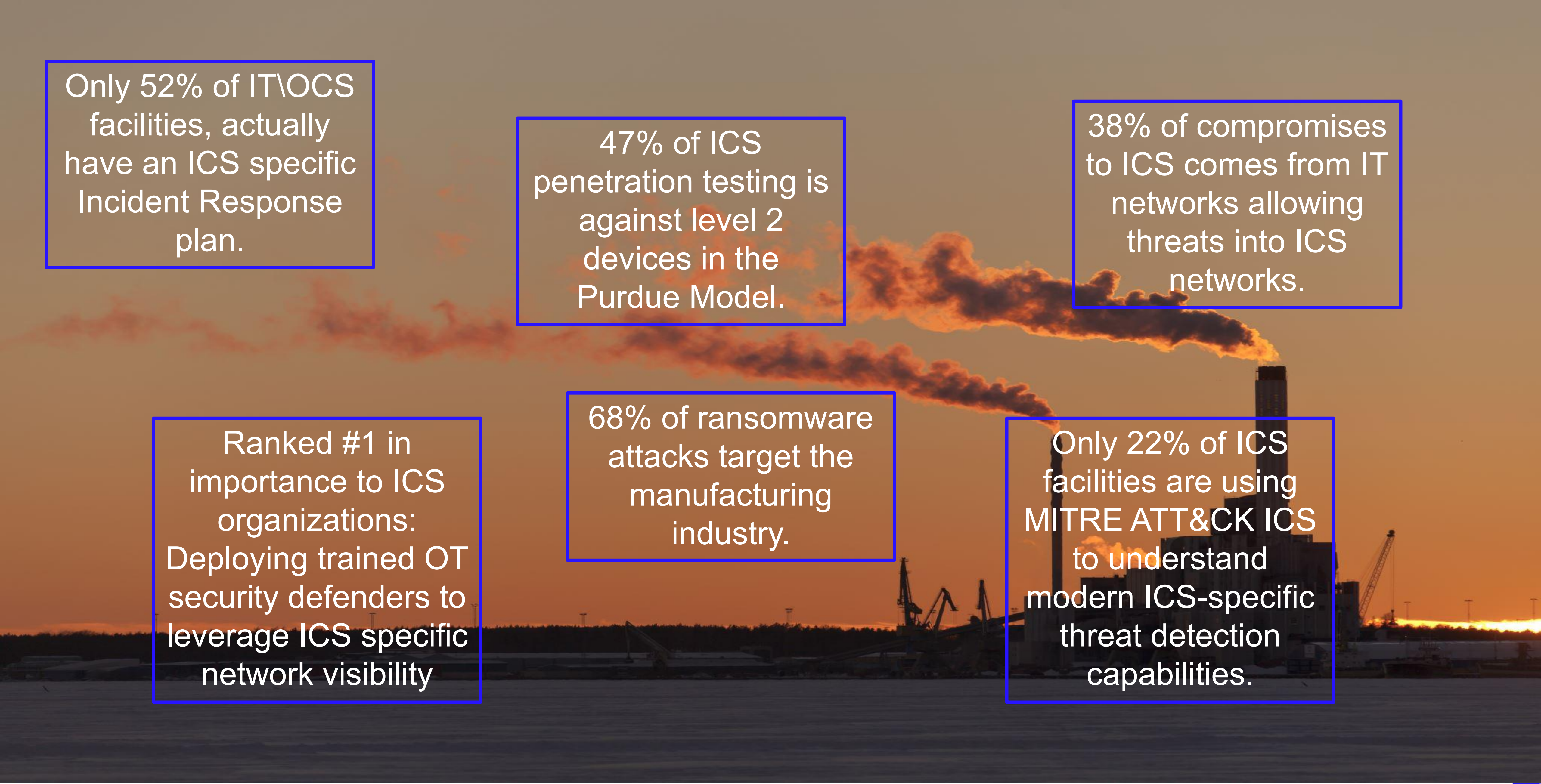
Trellix

Reference: Waterfall Threat Report

The Scenario

A brief overview


IT Network
Remote Access
Historian
IOT Gateway
OPC Server
HMI
Engineer Workstations
PLC
PLC



Only 52% of IT\OCS facilities, actually have an ICS specific Incident Response plan.

47% of ICS penetration testing is against level 2 devices in the Purdue Model.

38% of compromises to ICS comes from IT networks allowing threats into ICS networks.

Ranked #1 in importance to ICS organizations: Deploying trained OT security defenders to leverage ICS specific network visibility

68% of ransomware attacks target the manufacturing industry.

Only 22% of ICS facilities are using MITRE ATT&CK ICS to understand modern ICS-specific threat detection capabilities.

Trellix Solutions

An Overview

Trellix

Trellix Integrity Control

Trellix

Trellix Integrity Control

Solidcore - Application Control - Change Control

Application Control

- Dynamic Whitelisting
- Memory Protection
- Legacy System Support
- Reputation based Execution

Change Control

- File Integrity Monitoring
- Read/Write Deny for Files and Registry Keys

Trellix XDR and SIEM

Trellix

Trellix XDR and SIEM

1. Broad data Ingestion

Open and
native integrations

2. Detections:

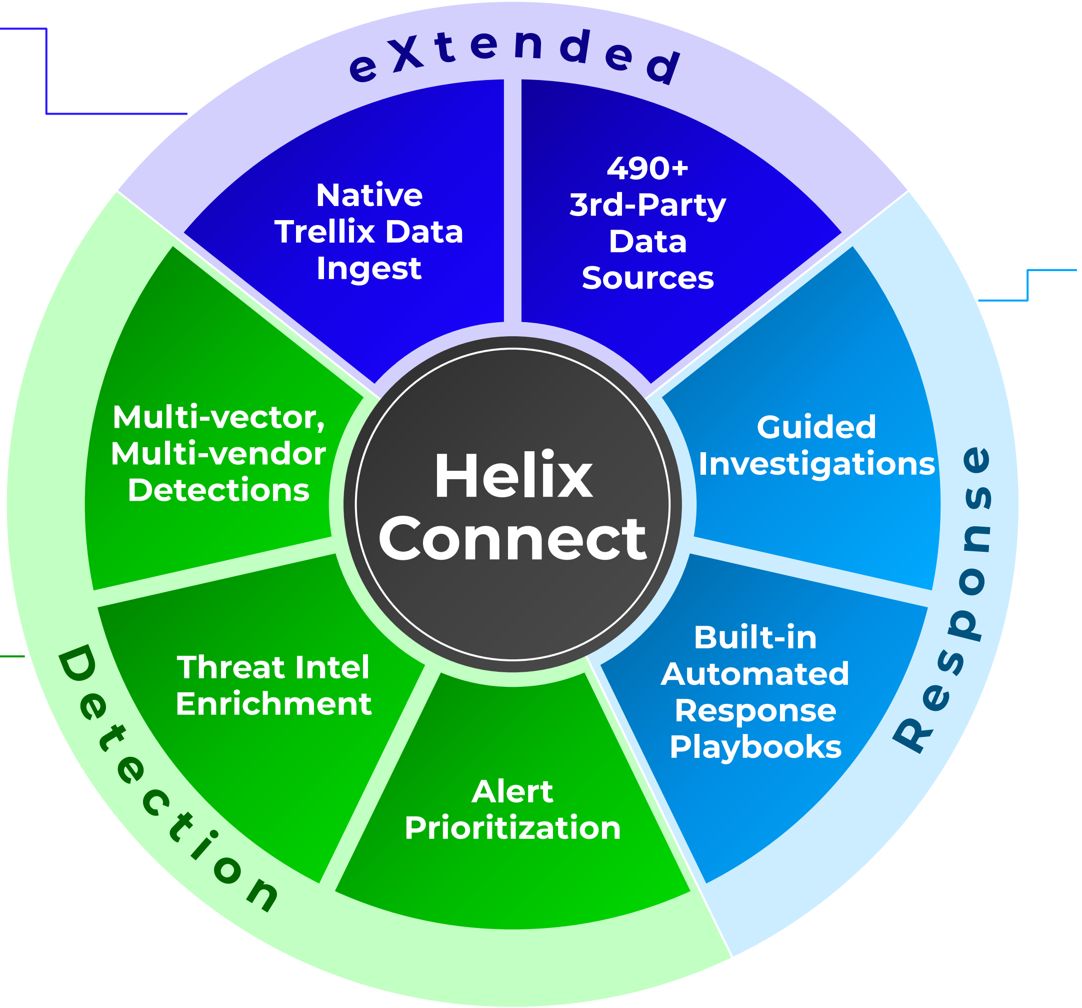
Analytics

Automated
threat elimination

Noise suppression

Enrichment

Prioritization


eXtended
Native Trellix Data Ingest
490+ 3rd-Party Data Sources
Guided Investigations
Built-in Automated Response Playbooks
Alert Prioritization
Threat Intel Enrichment
Multi-vector, Multi-vendor Detections
Helix Connect
Response
Detection

3. Response

On-prem / cloud
orchestration
and response

AI-guidance

Pre-built,
customizable
playbooks

Trellix

Trellix IVX

Trellix IVX - Cloud and on premise

How can Sandboxing help in IOC environments?

A play area where kids can build, destroy, and experiment without causing any real-world damage.

IVX is executing software in a restricted operating system environment, thus controlling the resources (e.g. file descriptors, memory, file system space, etc.) that a process may use to determine if a file is acting malicious or not.

Trellix Network Detection and Response (NDR)

Trellix

Trellix NDR

Complete network detection, protection and visibility

Visibility Dashboards
Track changes in Network Activity, Explore Ports, Protocols and Assets for advanced threat hunting

Detection Dashboards
Intuitive visualization of traffic patterns on attacker scope and techniques. Integration with Threat Intel and MiTRE ATT&CK Mapping

Asset Discovery
Extend visibility and automatically map discovered assets to device type, including new devices. Additional correlation with sensor telemetry

Analytics & Correlation
Continue to innovate differentiated high fidelity detection technologies building on a proven foundation of adaptable technologies

Enrichment & Prioritization
Improves situational awareness and risk posture for SOC Analyst.
Enriches network data with threat modelling based on attacker Tactics and Techniques

Investigative Workflow
Alerts combine into Incidents that are actionable. Incident workflow leverages XDR elements

Trellix OEM\Embedded

An Overview

Trellix

Trellix OEM Footprint

❑ 50% of the water supply in the United States

❑ Offer security to 90% of the world's utilities

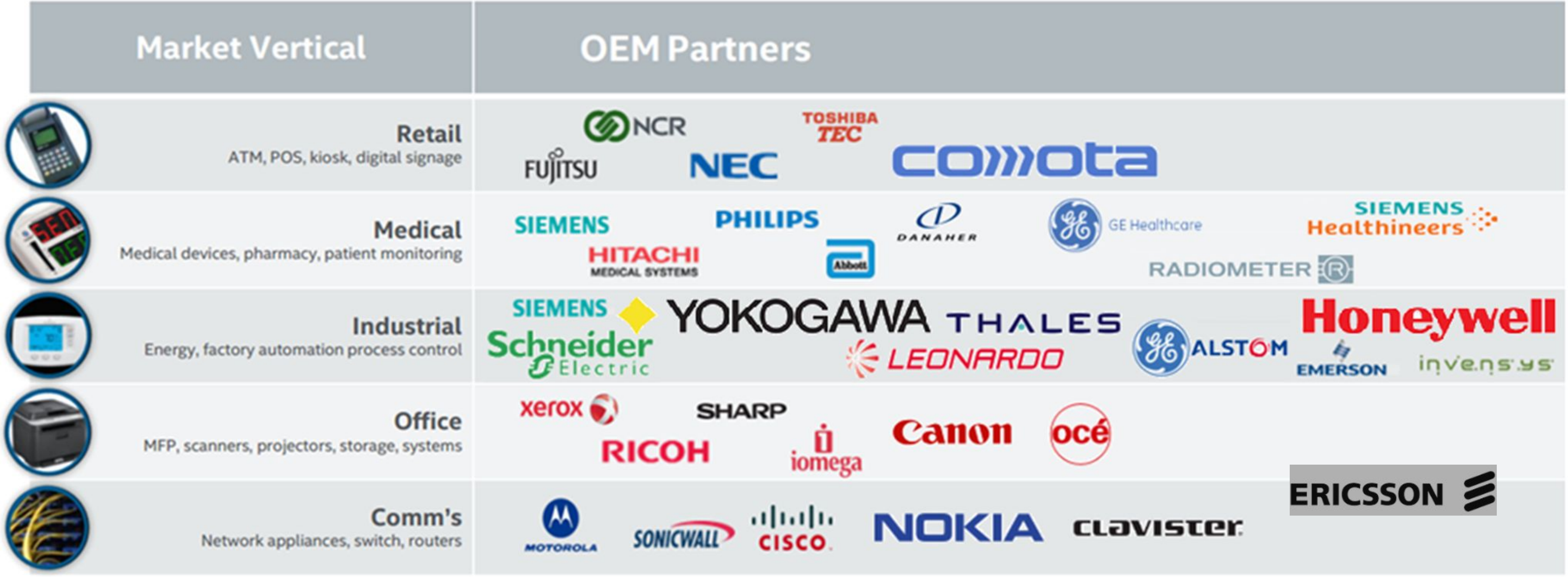
❑ #1 Security solution for ATM and POS Systems

❑ #1 in Japan Embedded Market (1.3M Devices)

❑ Partner with the largest automation vendors:

ABB, Emerson, Yokogawa, Rockwell Automation, Honeywell, Siemens, Schneider Electric

Trellix Market Verticals



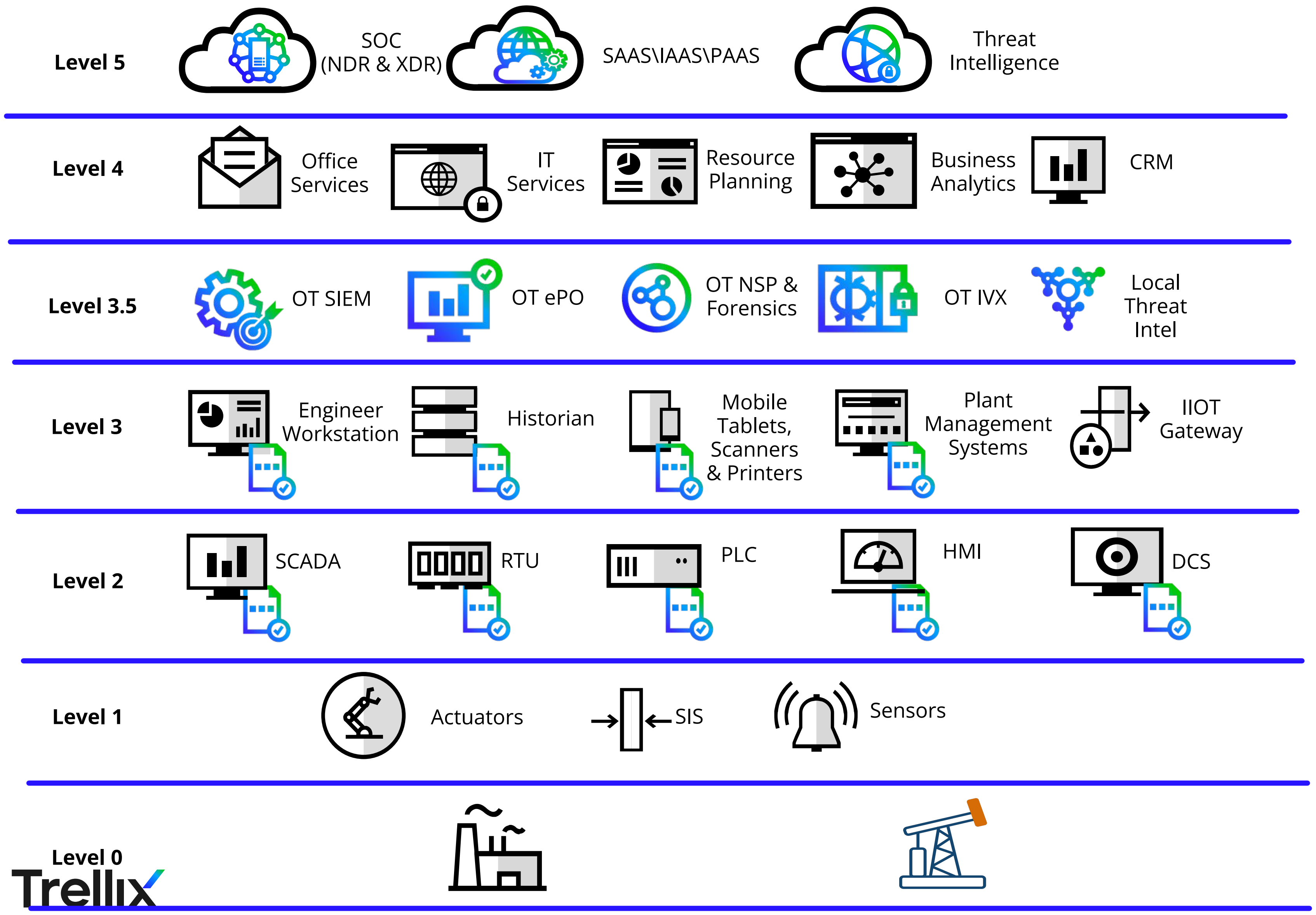
Market Vertical	OEM Partners
Retail ATM, POS, kiosk, digital signage	NCR TOSHIBA TEC FUJITSU NEC comota
Medical Medical devices, pharmacy, patient monitoring	SIEMENS PHILIPS DANAHER GE Healthcare SIEMENS Healthineers HITACHI MEDICAL SYSTEMS Abbott RADIOMETER
Industrial Energy, factory automation process control	SIEMENS Schneider Electric YOKOGAWA THALES LEONARDO GE ALSTOM Honeywell EMERSON invensys
Office MFP, scanners, projectors, storage, systems	xerox SHARP RICOH iomega Canon océ
Comm's Network appliances, switch, routers	MOTOROLA SONICWALL CISCO NOKIA clavister ERICSSON

Trellix Security Solutions

Industrial Control Systems

Trellix

Trellix Product Portfolio – OT Security Reference



Level 5: SOC (NDR & XDR) · SAAS\IAAS\PAAS · Threat Intelligence

Level 4: Office Services · IT Services · Resource Planning · Business Analytics · CRM

Level 3.5: OT SIEM · OT ePO · OT NSP & Forensics · OT IVX · Local Threat Intel

Level 3: Engineer Workstation · Historian · Mobile Tablets, Scanners & Printers · Plant Management Systems · IIOT Gateway

Level 2: SCADA · RTU · PLC · HMI · DCS

Level 1: Actuators · SIS · Sensors

Level 0

Trellix and Sky-High Partnership provides CASB, DLP, Web Security and Threat Protection for multi-cloud services

Helix Connect Extended Detection and Response Platform (XDR)

Threat Intelligence Insights, GTI, DTI , ATLAS, IntaaS

SIEM On-premises next generation SIEM, analytics, log storage and anomaly detection

ePO centralized management and automated responses

NSP & Network Forensics advanced malware attack detection, lateral movement and forensics

Intelligent Sandbox next generation sandbox technology and integrations

Local Threat Intelligence on premises threat intelligence and immediate remediation

Endpoint Security Anti-Malware, EDR, Forensics, Integrity Control and Device Control