Найкраща практика захисту SCADA систем

Роман Чорненький

Trend Micro

TREND MICRO™

30+ years of cybersecurity expertise

txOne™ networks

Industrial Cybersecurity. Simplified.

MOXA®

30+ years of OT and ICS expertise

Network Segmentation

Beyond ICS Detection

TXOne Technologies

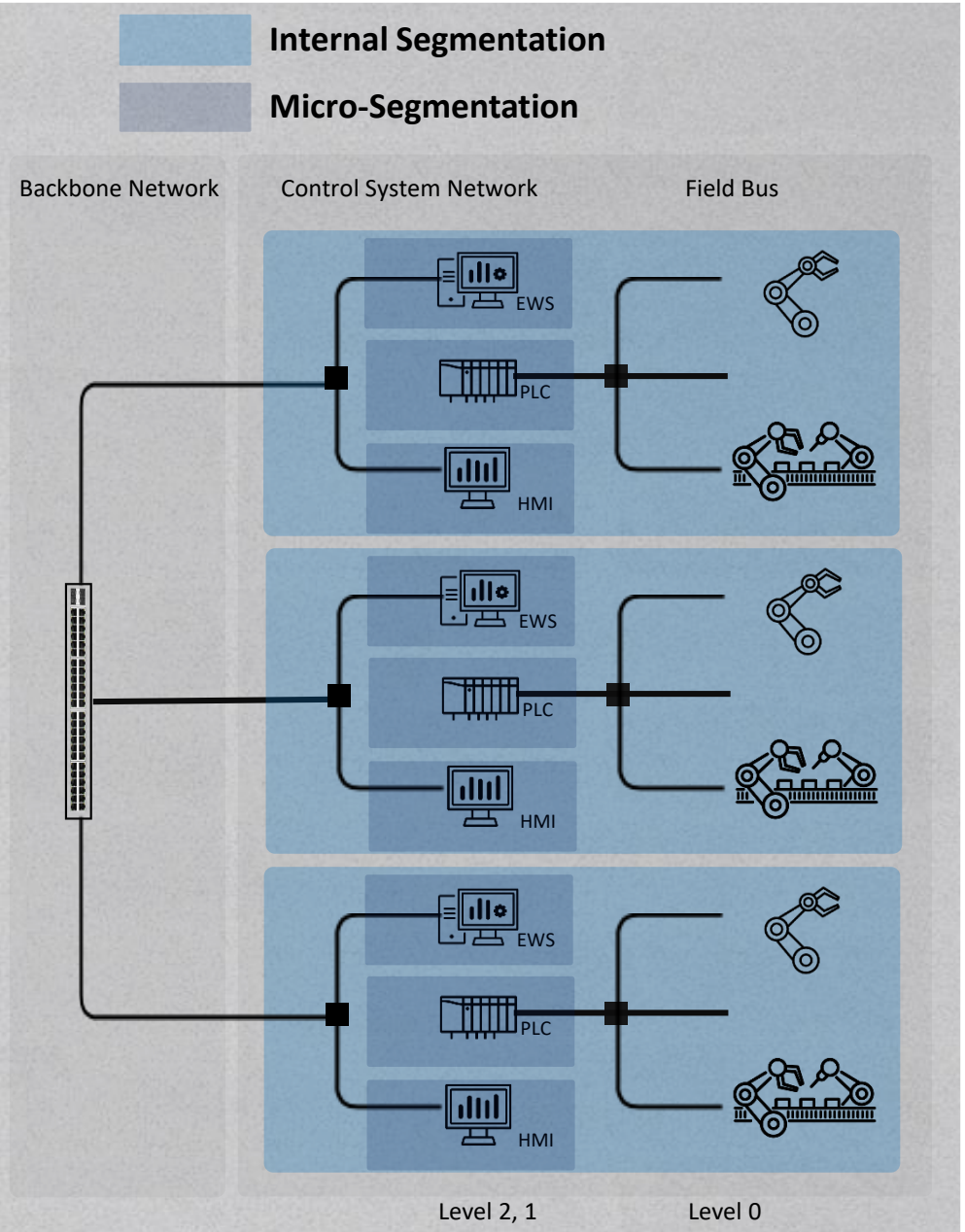
- Virtual Patch
- Protocol Enforcement
- Flexible Deployment

Attacking Vectors

- Worm Propagation
- Ransomware Spread
- PLC Misuse

Changing Infrastructure

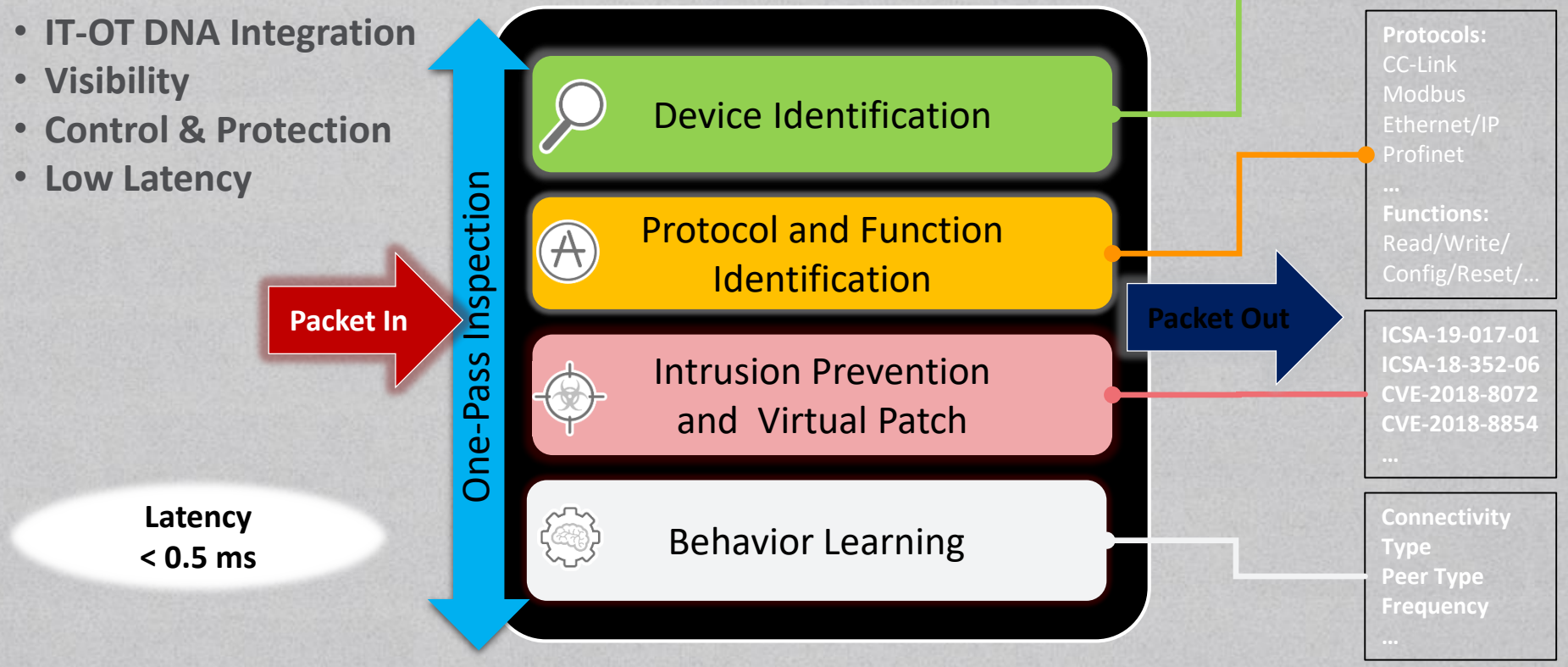
- Massive IoT
- Edge Computing
- Virtualization



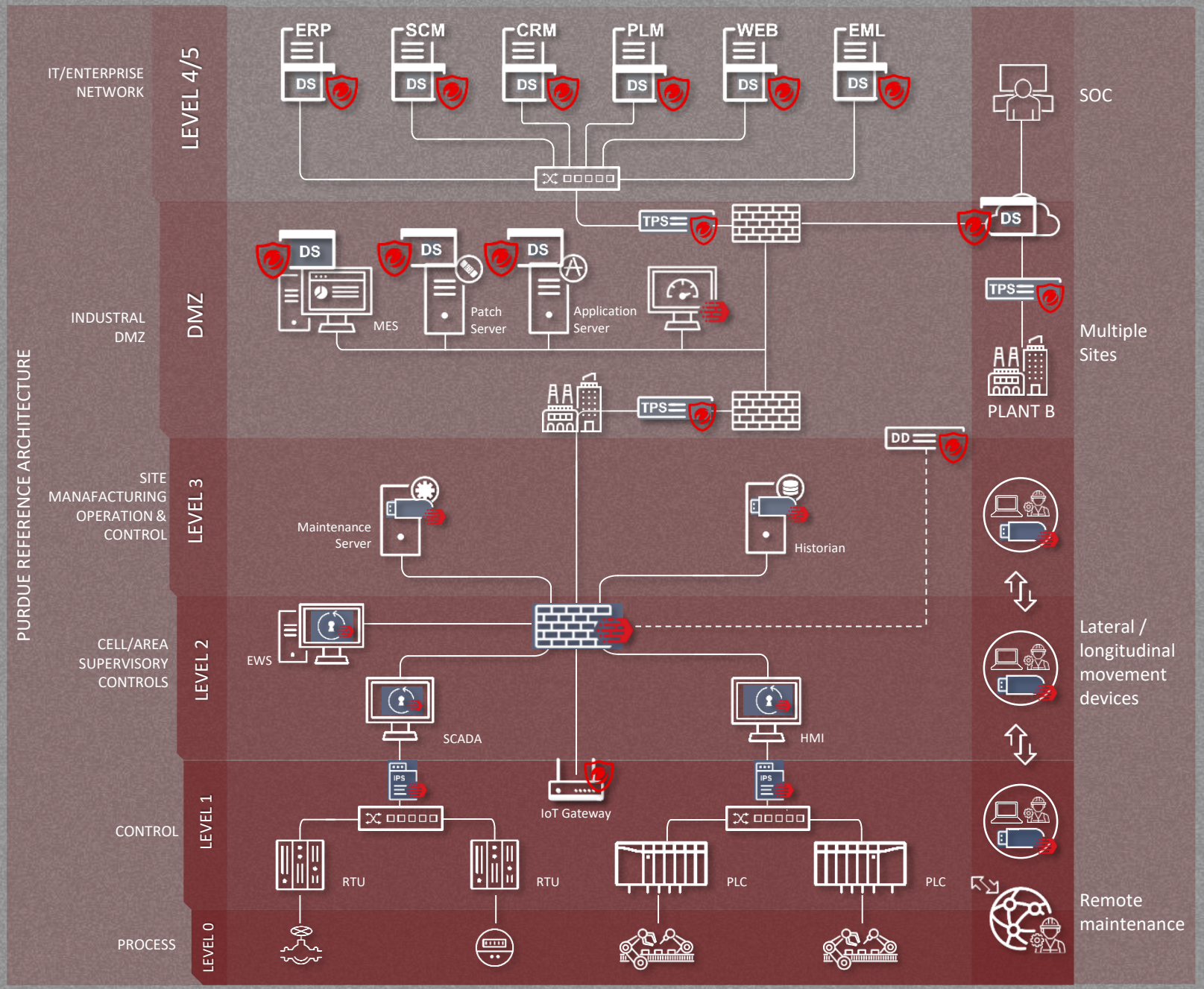
txOne networks

TXOne Ключевые возможности: TXODI™ -TXOne One-Pass DPI for Industrial

- IT-OT DNA Integration
- Visibility
- Control & Protection
- Low Latency



txOne networks



IT Centric solution

L4/L5/DMZ Protection

Hybrid Cloud and Server Protection
Trend Micro Cloud One (Deep Security)
Anti-malware, Virtual Patch and Log Inspection

Gatekeeper IPS
TippingPoint Threat Protection System
Block malicious traffic

APT Prevention
Deep Discovery Inspector
Network-Wide Detection of Targeted Attacks

OT centric solution for Shop Floor

Malwares Defense for ICS Endpoints

Installation-less malware scanning tool
Trend Micro Portable Security 3
Periodical Health-Check Process

Lockdown Mission-Critical Assets
Trend Micro Safe Lock TXOne Edition
Safe run with AWL (Applications Whitelisting)

Cell to Zone Segmentation for L2

Industrial Central Management Console
OT Defense Console
Plant defense field management

Industrial Next-Generation Firewall
EdgeFire
Secure network segmentation

Industrial Next-Generation IPS
EdgeIPS
Cell segmentation for critical assets protection

Secure GW

Secure endpoint SDK for IoT device makers
Trend Micro IoT Security
Secure low resource devices

XDR (Cross Detection & Response)

Integrate with Trend Micro XDR Service

IT

Cloud

End point

Network

Server

Email

OT

PLC

EWS

HMI

SCADA

Current

Roadmap

Data Lake

Product Data Lake

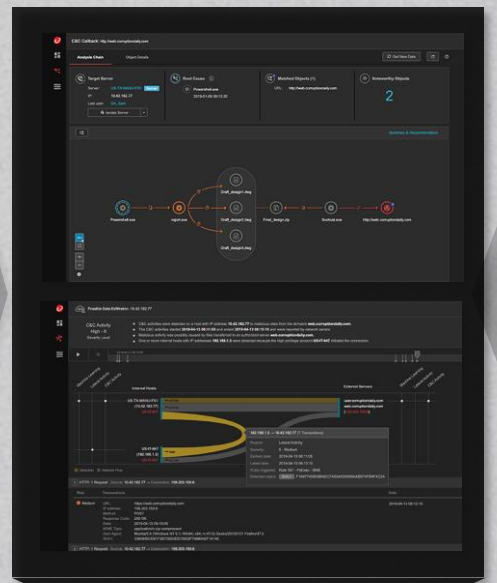
Product Data Lake

Product Data Lake

Product Data Lake

Product Data Lake

Managed XDR Service



SIEM

Security information and event management

SOAR

Security Orchestration, Automation and Response

Detection

- 24/7 critical alert monitoring and correlation
- On-demand Indicator of Compromise (ICO) sweeping
- Proactive indicator of Attack (IOA) hunting

Investigation

- Incident prioritization and investigation
- Correlated root cause and impact analysis

Response

- Threat response
- Remediation and preventative measures recommendations
- Incident reporting and executing summaries

Reference Video https://www.youtube.com/watch?v=TG8GFI41Eps

txOne networks

Asset Visibility Management

Threat Prevention → Network Segmentation → CTD (DDI, DDAN, ApexOne, TP, SOC); XDR → Operation Protocol OT Access Control

SIEM platform partners

IBM QRadar, ArcSight An HP Company, splunk>

ODC admin configures the syslog settings:
- server address & port
- protocols: TCP/UDP
- format: CEF/LEEF
- facility level
- log level
- log types

TXOne ODC

ICS detection partners

NOZOMI NETWORKS, DRAGOS SAFEGUARDING CIVILIZATION, CLAROTY, CyberX Trusted. Industrial. Cybersecurity.

1. **User configure the ODC IP address on 3rd-Party products**
2. **3rd-Party product notifies ODC to block nodes or links via RESTful APIs**
3. **Once confirmed, the blocking lists will be added to the Edge devices**

txOne networks

Спасибо за внимание!