在想要哭的那一天之後
The Day After WannaCry

Steven Hsu
Director, Trend Micro.
PMM TXOne Networks

May 12, 2017

300,000 computers in approximately 150 countries across the globe by WannaCry

How about now

100+

More than 100 countries are still impacted by WannaCry and other ransomware attacks

1M+

More than 1 Million internet-connected endpoints are still vulnerable

8Billion

Ransomware cost businesses more than $8 billion in the past year

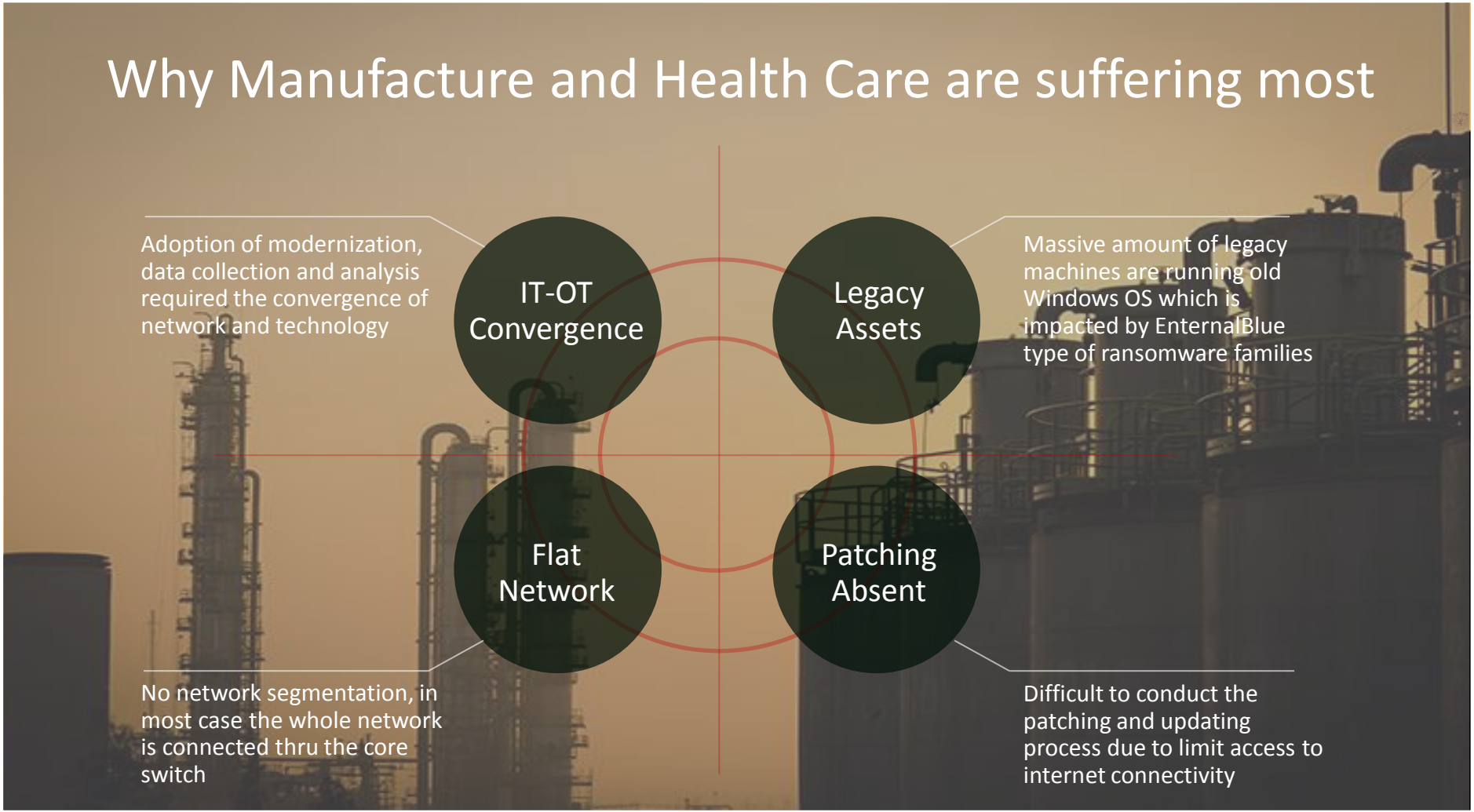
90%+

Manufacture and Health Care are still suffering the Ransomware attack

https://www.shodan.io/report/S8dhzrSn
https://safeatlast.co/blog/ransomware-statistics/#gref

TREND MICRO

Why Manufacture and Health Care are suffering most



IT – OT Convergence - an easy way explanation

I am the Answer

I am Cloud, I am AI

I am Internet

I am Internet

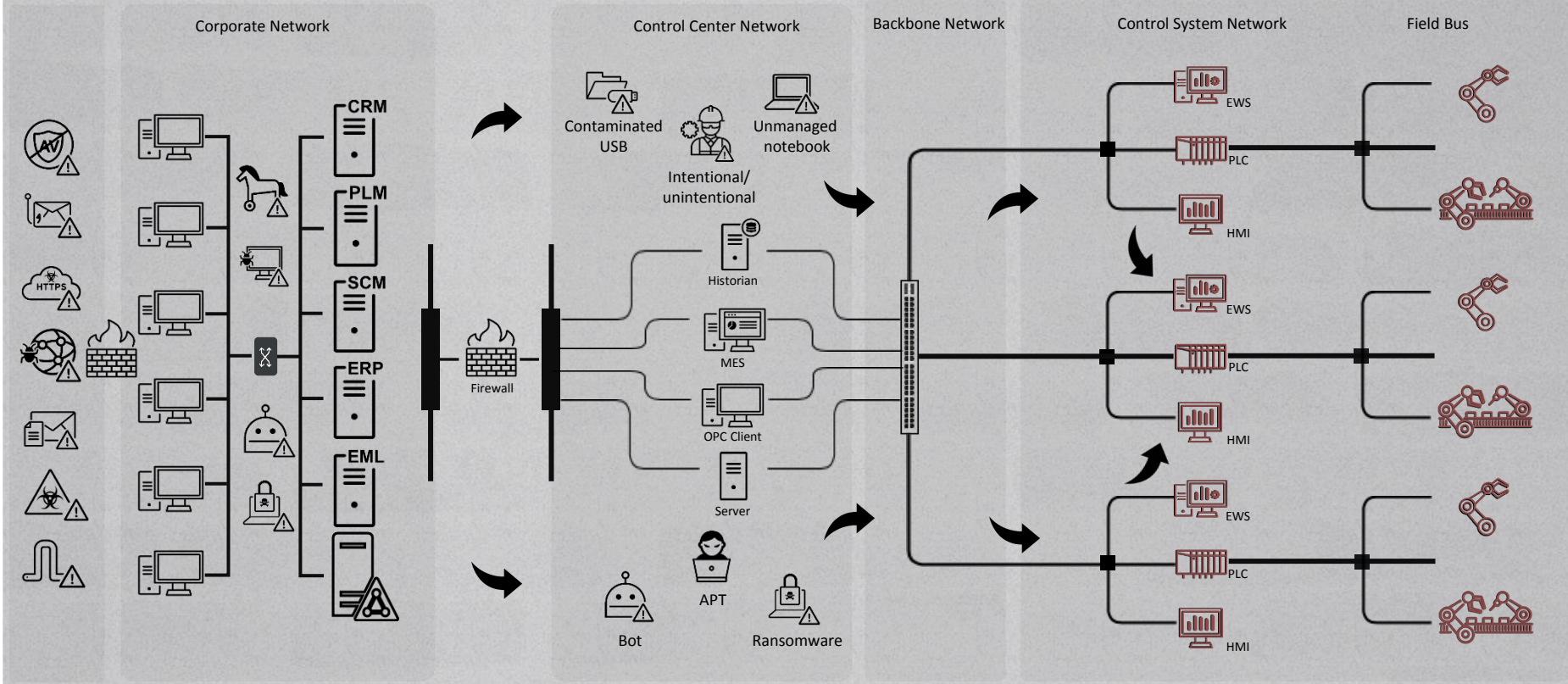
I am PC

We are IT

I am Mac

We are OT

Typical ICS Cybersecurity attack



TREND MICRO

txOne networks


The Day After WannaCry Changes Three Things
Aggressive Law Enforcement Attitude
Threat Paradigm Shift in ICS Security
More attention on ICS Cybersecurity
TREND MICRO

Aggressive Law Enforcement Attitude

Encourage victims reach out Law enforcemenet and file a case

- FBI requests victims to file a complaint with Internet Crime Complaint Center

Multi nations jointed force to assist ransomware vicitims

- “No More Ransom” project is an initiative by the National High-Tech Crime Unit of the Netherlands' police, Europol's European Cybercrime Centre, and security researchers. Now have more than 188 countries joined.
- This public-private partnership had helped more than 200,000 ransomware victims recover their files and save more than US$ 108 Million in ransom

TREND MICRO

Threat Paradigm Shift in ICS Security

Threat Paradigm Shift in ICS Security

Critical Infrastructure attack

- 2010 Stuxnet, Flame
- 2011 DUJQU
- 2012 Flamer, Gauss Shamoon
- 2014 Havex/Dragonfly
- 2015 Black Energy 3
- 2016 Industoyer
- 2016 Shamoon 2
- 2017 Triton/Trisis

2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020

IT-based ransomware attack

2017
WannaCry
NotPetya
Bad Rabbit

OT-based ransomware attack

2019 - 2020
LockerGoga, Ekans
DoppelPaymer ClodLock
MegaCortex

TREND MICRO

Threat Paradigm Shift in ICS Security

GE

VMware

Honeywell

ICS targeted ransomware attack

DoppelPaymer, LockerGoga, Maze, MegaCortex, Nefilim and SNAKEHOSE

2020

ccflic0.exe
ccflic4.exe
healthservice.exe
ilicensesvc.exe
nimbus.exe
prlicensemgr.exe
certificateprovider.exe
proficypublisherservice.exe
proficysts.exe
erlsrv.exe
vmtoolsd.exe

managementagenthost.exe
vgauthservice.exe
epmd.exe
hasplmv.exe
spooler.exe
hdb.exe
ntservices.exe
n.exe
monitoringhost.exe
win32sysinfo.exe
inet_gethost.exe

taskhostw.exe
proficy administrator.exe
ntevl.exe
prproficymgr.exe
prrds.exe
prrouter.exe
prconfigmgr.exe
prgateway.exe
premailengine.exe
pralarmmgr.exe

TREND MICRO

Threat Agents required Top Security Agents

3J + 1E

Jame Bond
Jason Bourne
Jack Ryan
Ethan Hunt

MSPCT + 2F

McAfee
paloalto NETWORKS
Symantec
FIREEYE
CISCO
FORTINET
TREND MICRO

TREND MICRO

WHO WE ARE

A Joint venture company of

Trend Micro Inc. and Moxa Inc.

30 years+ Cybersecuirty Threat Intelligent

30 years+ OT Network Expertise

To accelerate Industrial world to secure automation and data exchange


Recommendation from TXOne Networks for ICS Cybersecurity

Prevention and Mitigation in the production environment

DEFENSE

1.

Ensure all endpoints install antivirus protection

2.

Deploy the latest patches and AV signature update to all the endpoints

SHIELD

3.

Adopt the virtual patch method to shield vulnerable assets to stop propagation

4.

Hardening the critical asset by whitelisting solution

SEGMENTATION

5.

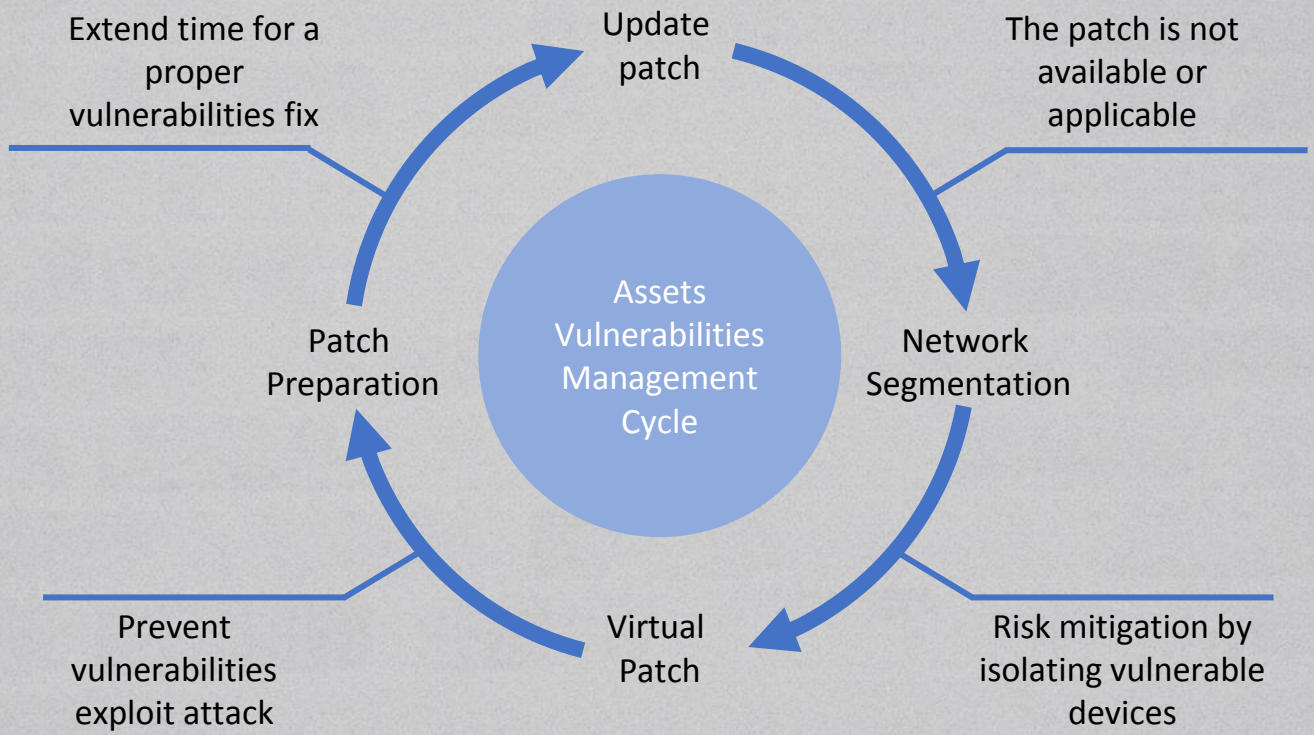
Conduct a proper network segmentation to reduce future attack impact

6.

Level up the prevention defense by implementing the in-depth micro-segmentation to eliminate attacker surfaces.

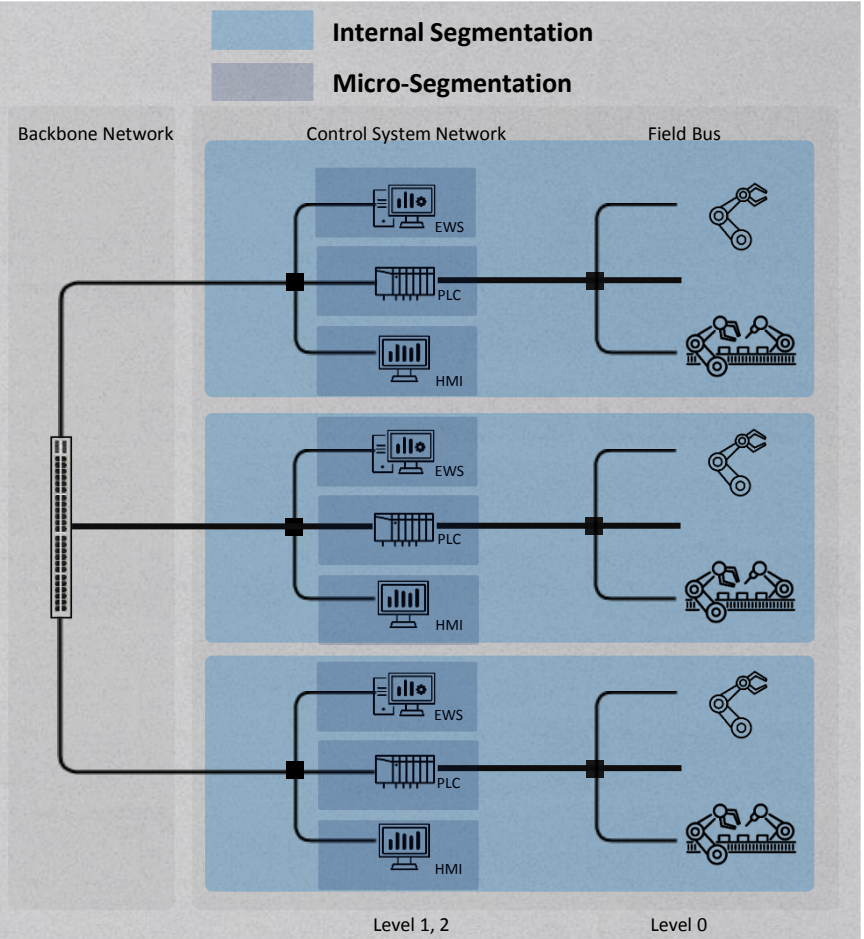
TREND MICRO txOne networks

Deal with vulnerable assets



Why Network Segmentation

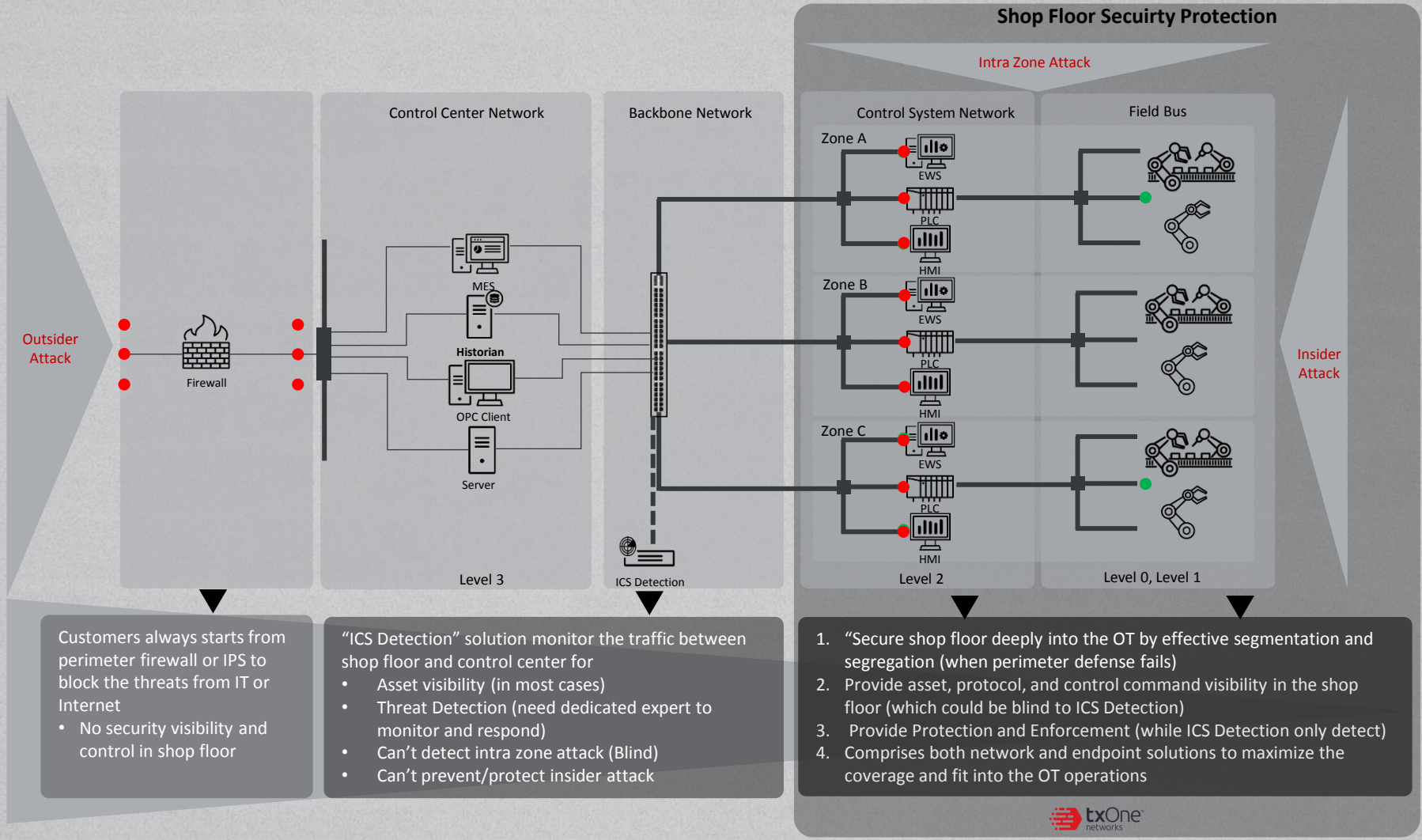
- Risk Mitigation
- Prevent Lateral Movement
- Outbreak Prevention
- Deal with Massive IoT Adoption
- Future Private 5G Connection
- Zero Trust Network



TREND MICRO
txOne networks

TXOne Networks Solution for ICS Cybersecurity

TREND MICRO™ txOne networks™


Shop Floor Secuirty Protection
Intra Zone Attack
Outsider Attack
Firewall
Control Center Network
MES
Historian
OPC Client
Server
Level 3
Backbone Network
ICS Detection
Control System Network
Zone A
EWS
PLC
HMI
Zone B
EWS
PLC
HMI
Zone C
EWS
PLC
HMI
Level 2
Field Bus
Level 0, Level 1
Insider Attack
Customers always starts from perimeter firewall or IPS to block the threats from IT or Internet
• No security visibility and control in shop floor
"ICS Detection" solution monitor the traffic between shop floor and control center for
• Asset visibility (in most cases)
• Threat Detection (need dedicated expert to monitor and respond)
• Can't detect intra zone attack (Blind)
• Can't prevent/protect insider attack
1. "Secure shop floor deeply into the OT by effective segmentation and segregation (when perimeter defense fails)
2. Provide asset, protocol, and control command visibility in the shop floor (which could be blind to ICS Detection)
3. Provide Protection and Enforcement (while ICS Detection only detect)
4. Comprises both network and endpoint solutions to maximize the coverage and fit into the OT operations
txOne networks

Solution Portfolio Summary

Easier Deployment on the Rack** or in the Cabinet

Robust Hardware to support wide temperature and survive long MTBF

Fail-safe without interrupting the production even upon hardware failure

No software installation on the target ICS

Easy operation for dummy users to perform the scanning

Support Air-gapped environment for pattern update

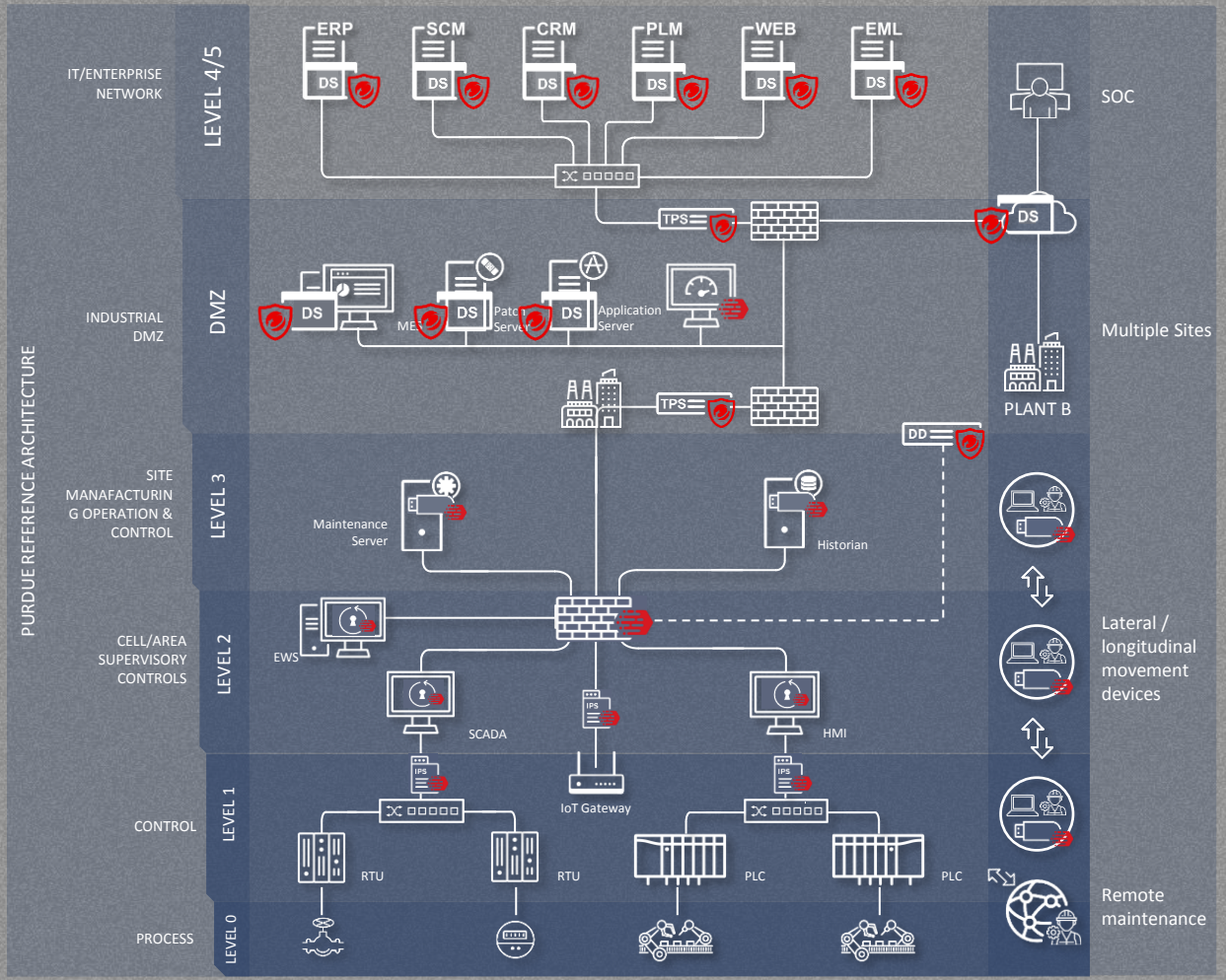
Minimal downtime for mass deployment

Low operational cost for maintaining the whitelist

Virtually no impact to system performance and computing resources on target ICS

TREND MICRO™ txOne networks™

Solution Map



Trend Micro Solutions for IT Security

L4/L5/DMZ Protection

Hybrid Cloud and Servers Protection

Deep Security
Anti-malware, Virtual Patch and Log Inspection

Gatekeeper IPS

TippingPoint Threat Protection System
Block malicious traffic ensure network availability

APT Prevention

Deep Discovery Inspector
Network-Wide Detection of Targeted Attacks

TXOne Solutions for Shop Floor Cybersecurity

Malwares Defense for ICS Endpoints

Periodical Health-Check Process

Portable Security
Installess anti-malware utility

Lockdown Mission-Critical Assets

SafeLock
Safe run with AWL (Applications Whitelisting)

Cell to Zone Segmentation for L2

Management & Visibility

OT Defense Console
Plant defense field management

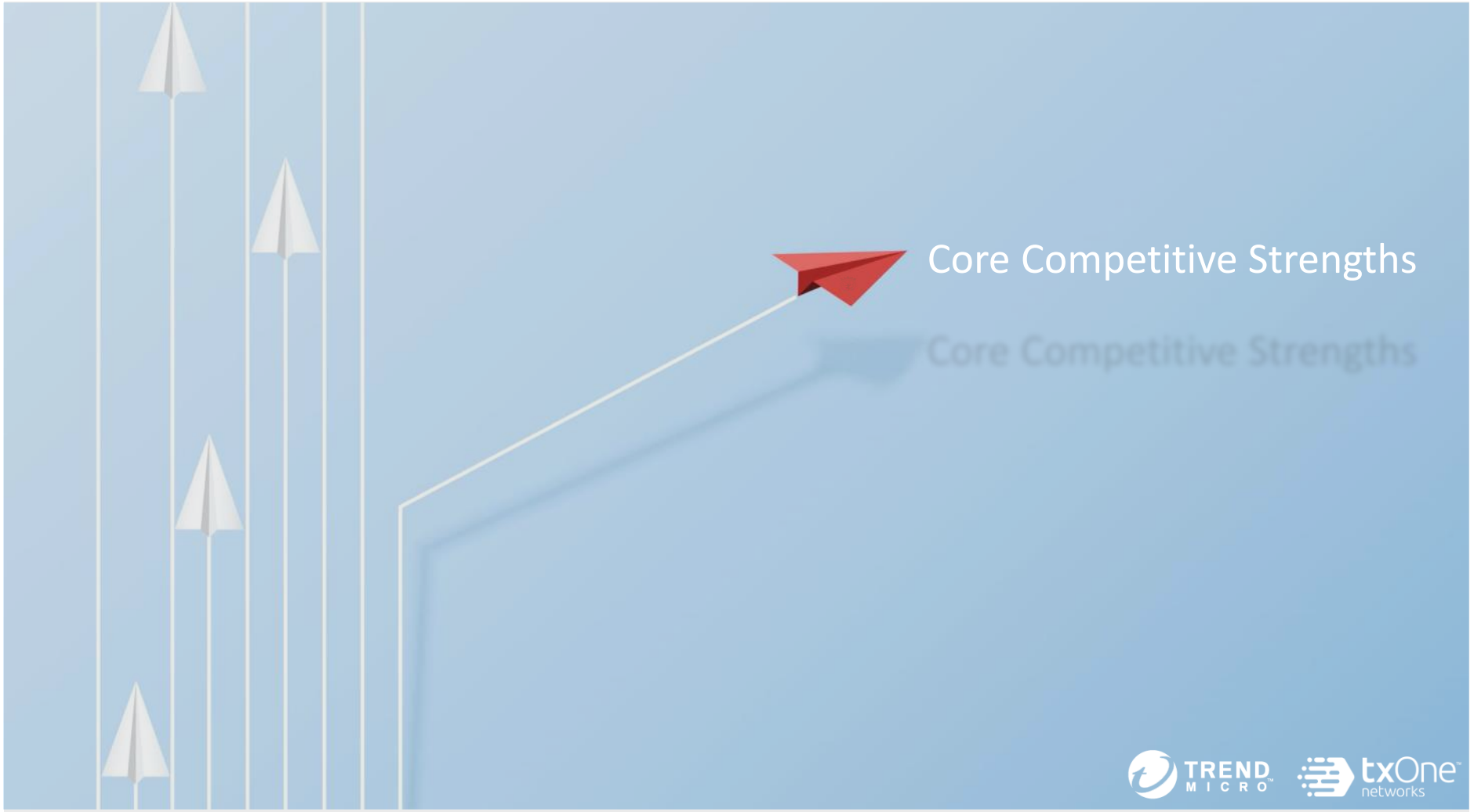
Granular Network Access Control

EdgeFire
Zonal Marking Defense in plant Network

Cell Segmentation and Virtual Patch

EdgeIPS
Marking Defense in plant network

Core Competitive Strengths



In-Depth OT Protocols Knowledge

2019 GM		2020 H1		2020 H2	
TXODI-Decoder	Signature-Visibilty	TXODI-Decoder	Signature-Visibilty	TXODI-Decoder	Signature-Visibilty
Modbus	OPC UA	IEC 104	IEC 60870-5 (part of IEC 62351)	DCS protocols	ANSI C12.22
EthernetIP/CIP	Modbus	IEC61850-MMS	IEC 61850 (part of IEC 62351)	OPC UA	LAquis SCADA (Access)
Siemens S7COMM	EtherNet IP/CIP	DNP3	GOOSE	ICCP	atvise scada (Access)
Siemens S7COMM+	Niagara Fox		OPC Classic(DA/AE/HAD)	HART-IP	PCWorx (Access)
OMRON FINS	BACnet		DICOM	IEC61850-GOOSE	inVIEW WebSCADA (Access)
MITSUBISHI-SLMP	SIEMENS S7Comm		Health Level 7		CODESYS (Access)
SECS/GEM	SIEMENS S7Comm Plus		TriStation		Ecava IGX Web SCADA
	DNP3		Crimson		ProConOS (Access)
	HART-IP		CAN-ETH		Unitronics PCOM (Access)
	OMRON Fins		GE-SRTP via TCP		ClearSCADA (Access)
	Bechoff ADS		Modbus Schneider Modicon Ladder Logic (Access)		EtherCAT (Access)
	IEEE C37.118		OpenSCADA User Interfaces (Access)		ScadaBR (Access)
	IEC 61850-5		Rapid SCADA User Interfaces (Access)		CAN-ETH (Access)
	MITSUBISHI-SLMP		EtherSBus (UDP)		Cat MineStar System (Access)
	MELSOFT		EtherSIO (UDP)		Red Lion Crimson V3
	Modbus Schneider		Ethernet Powerlink (Access)		Ethernet Global Data Protocol
	CC-LINK IE		Moxa Device Discovery (UDP)		
	IEC 60870-5-104		Advantech WebAccess SCADA Access (TCP)		
	FATEK PLC		IGSS (TCP/SSL)		

2019 1st GM → 2020 2nd/3rd release

TXODI™

-TXOne One-Pass DPI for Industrial

Visibility

- Provide device, protocol, and control command visibility to network managers

OT-Aware Operational Intelligence

- Comprehensive whitelisting on device, protocol, and operation. For example, "***PLC1*** can communicate with ***Workstation1*** with ***Modbus protocol*** for ***Read Operation*** ONLY"

Protection

- Detect protocol anomaly, vulnerability, and corresponding threats

TREND MICRO txOne networks

Leverage the world-leading Threat Research of Trend Micro

Leader in Anti-Malware technology

Gartner

Named a Leader Once Again

in the Gartner Magic Quadrant for Endpoint Protection Platforms, Jan 2018

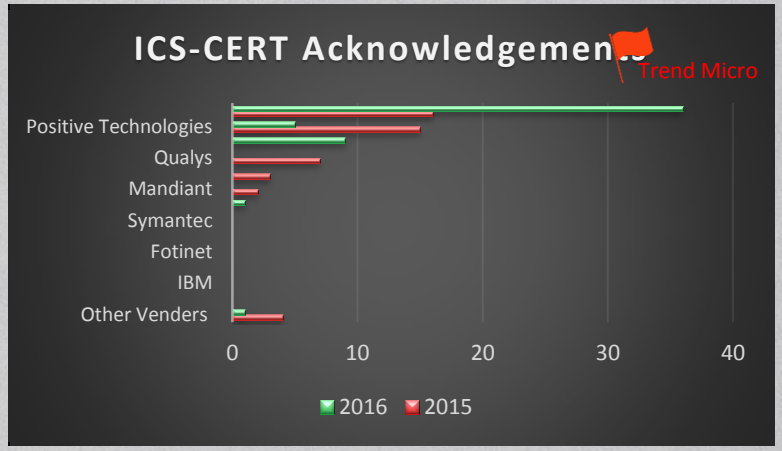
AV-TEST

BEST Protection

with outstanding performance

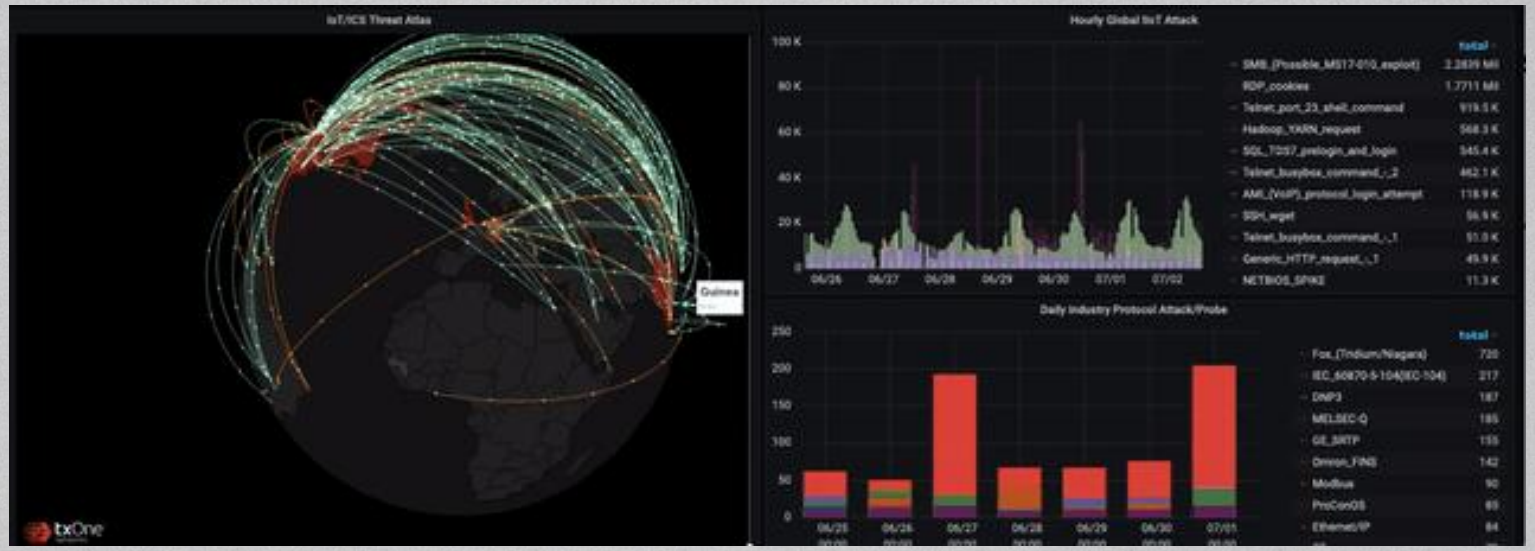
Leader in ICS Vulnerability Research

This graph is number of acknowledged reports for ICSA(ICS Advisories) of ICS-CERT by DHS



TREND MICRO txOne networks

World's first IoT/ICS Threat Atlas



Analyzed more than 45TB of traffic.

Detected 1.1 billion attacks

Searched more 400 million malicious IPs

Analyzed more than 1 million malicious files

Searched more than 30 million malicious domains

https://www.tr.txone-networks.com

TREND MICRO txOne networks

Key takeaways

- IT-OT Convergence is leading ICS more connected and moderized
- State Sponsored attacks to ICS is not noing to stop
- Cybercriminal aims for ICS may be the next attack trend
- Cybersecuirty solutions for ICS should consider diiferent conditions

When you feel sad and wanna cry because of in charge of cybersecurity

Needs a shoulder to lean on ...

Please Call ...

Trend Micro ... for help

Thank You