Mapping the Landscape: Top 10 Cybersecurity Trends in Critical Infrastructure for 2024

Mars Cheng

PSIRT and Threat Research, TXOne Networks Inc.

August 9, 2024 @DEF CON 32

Mars Cheng from Taiwan 🇹🇼



- **Threat Research Manager, PSIRT and Threat Research at TXOne Networks**
  - **Executive Director**, Association of Hackers in Taiwan (HIT/HITCON)
  - **General Coordinator of HITCON CISO Summit 2024**
  - ICS/SCADA, IoT, Malware Analysis, Threat Hunting and Enterprise Security
  - Spoke at Black Hat USA/Europe/MEA, RSA Conference, DEF CON, TROOPERS, HITCON, FIRST, CODE BLUE, SecTor, HITB, SINCON, ICS Cyber Security Conference USA and Asia, and CYBERSEC
  - Instructor of Global Cybersecurity Camp (GCC) 2024, HITCON Training 2022/2021/2020/2019, CCoE Taiwan, Ministry of National Defense, Economic Affairs, Education, and Finance in Taiwan, and Listed companies
  - Cyber Security Auditor of Taiwan Government
  - General Coordinator of HITCON CISO Summit 2023, HITCON PEACE 2022 and 2021
  - 10+ CVEs and 3 SCI Journals
  - Member of CHROOT Study Group

HIT Hacks In Taiwan Conference

txOne networks



Top 10 Cybersecurity Status/Dilemmas of Critical Infrastructure

txOne networks

Survey Background – 2023 and 2024

	2023			2024			
	Germany (n=100)	USA (n=100)	Japan (n=100)	Germany (n=101)	USA (n=102)	UAE (n=100)	Japan (n=102)
General Manufacturing	34%	34%	34%	-	50%	-	-
Automotive Manufacturing	33%	33%	33%	50%	-	-	50%
Pharmaceutical Manufacturing	33%	33%	33%	50%	-	-	50%
Chemical Manufacturing	-	-	-	-	50%	-	-
Oil & Gas	-	-	-	-	-	50%	-
Oil & Gas Logistics	-	-	-	-	-	50%	-
I am responsible for my organization's OT cybersecurity management	65%	71%	65%	79%	98%	92%	75%

1

Policy

Renewed Government Regulatory Focus on Cybersecurity



txOne networks

2

People

Security Awareness/Training of OT Operators is Still Not Enough

Type of OT Security Incident

	2023				2024				
	Total (n=145)	Germany (n=47)	USA (n=57)	Japan (n=41)	Total (n=186)	Germany (n=54)	USA (n=49)	UAE (n=42)	Japan (n=41)
Phishing emails aimed to penetrate systems	**37%**	**47%**	33%	32%	27%	30%	31%	21%	27%
Employee Actions - Malicious Motives	**34%**	30%	**44%**	27%	20%	31%	18%	10%	20%
Ransomware attack	**32%**	26%	37%	32%	**47%**	37%	**51%**	**52%**	**49%**
Vulnerability of unpatched systems	32%	30%	28%	**39%**	**38%**	**50%**	31%	33%	34%
Employee Actions - Human Error (unintentional)	**32%**	30%	33%	32%	**35%**	31%	35%	33%	41%
Identity theft, fake login credentials	31%	38%	33%	20%	22%	28%	22%	24%	12%
Third-party vendor or supplier compromise	31%	21%	33%	**39%**	13%	7%	18%	17%	10%
Advanced Persistent Threat (APT) attack	30%	32%	37%	20%	35%	41%	31%	31%	37%
Virus or malware infiltration	29%	23%	32%	32%	**37%**	26%	47%	48%	27%
Distributed Denial of Service (DDoS) attack	27%	30%	28%	22%	30%	31%	20%	29%	39%

txOne networks

3

People

Human Resource Gap on OT Security Professional

Shortage of Cybersecurity Professionals

	2023			
	Total (n=300)	Germany (n=100)	USA (n=100)	Japan (n=100)
Lack of integration between IT and OT security teams	**40%**	35%	37%	**47%**
Talent gap and difficulty in hiring qualified security professionals	**36%**	**37%**	38%	33%
Management apathy towards cybersecurity	**36%**	35%	34%	38%
Insufficient technical capabilities of current security team	**36%**	30%	**44%**	33%
Outdated cybersecurity knowledge practices	32%	33%	39%	25%
Insufficient security personnel	32%	28%	30%	38%
Insufficient security awareness among non-security employees	30%	36%	27%	27%
Lack of integration between security team and the rest of organization	29%	32%	35%	21%
Limited budget for security team	27%	28%	21%	23%

> “The shortage of cybersecurity talent is one of the key challenges to OT due to the difficulty of hiring qualified security professionals from a limited talent pool”

IT and OT Security Teams Need to Collaborate

Increase Hiring of Qualified OT Security Professionals

People

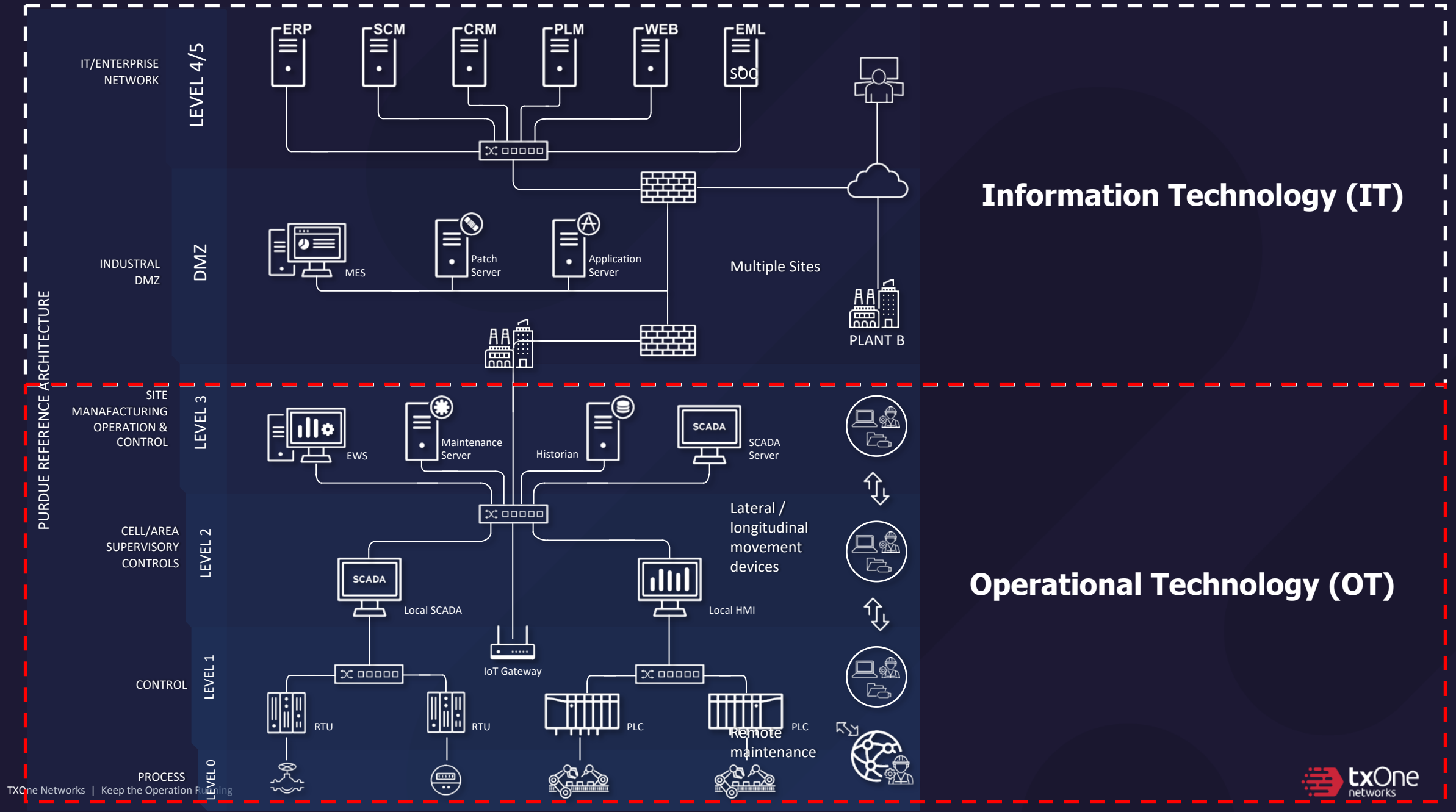
Establish Commitment of Management to OT Cybersecurity

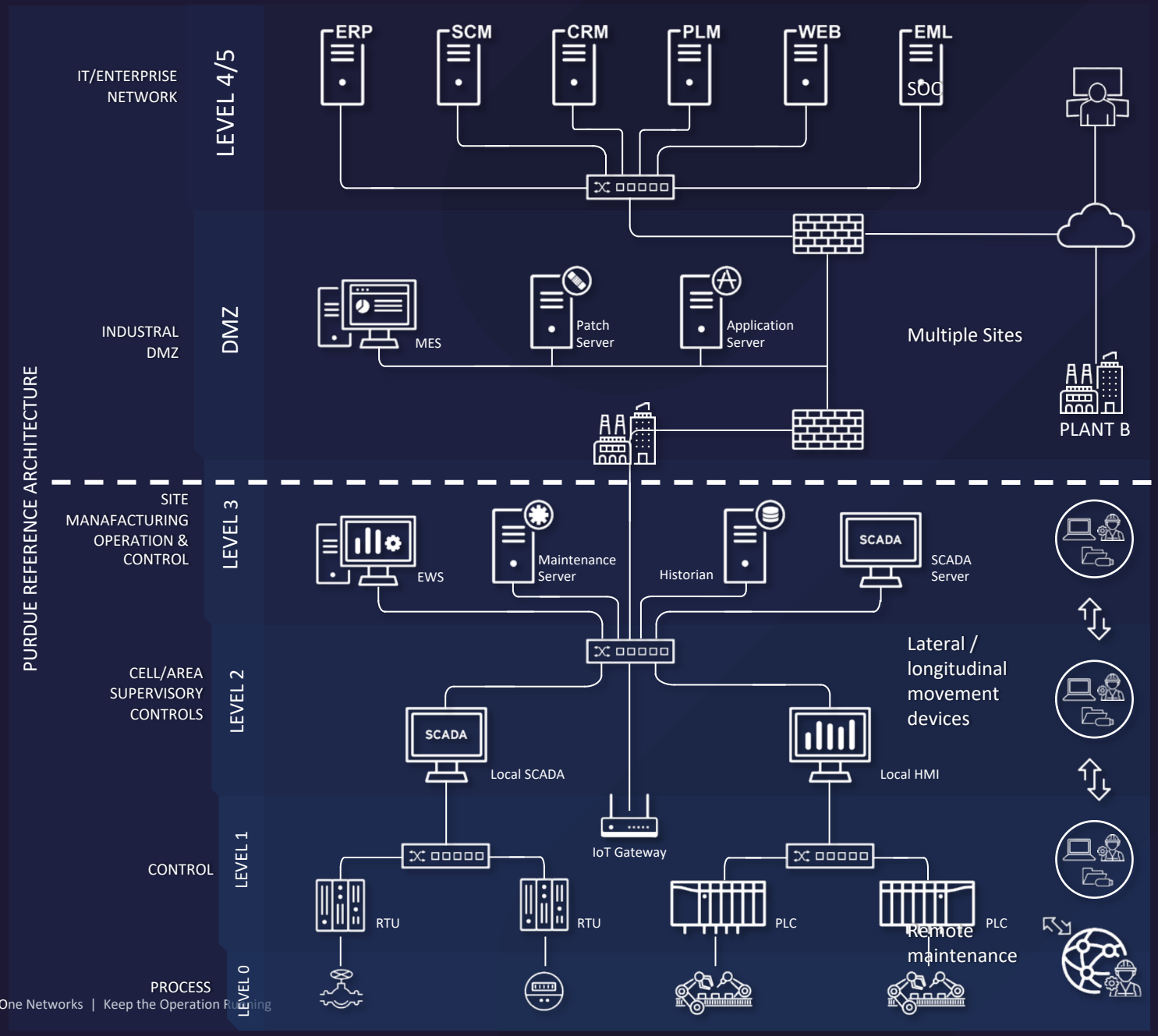
Proactively Mitigating Cybersecurity Complexity Can Reduce Negative Impact

4

Threat

More Attack Vectors Target Critical Infrastructure/OT than Enterprise Networks


PURDUE REFERENCE ARCHITECTURE
IT/ENTERPRISE NETWORK
LEVEL 4/5
ERP
SCM
CRM
PLM
WEB
EML
SOC
INDUSTRAL DMZ
DMZ
MES
Patch Server
Application Server
Multiple Sites
PLANT B
Information Technology (IT)
SITE MANAFACTURING OPERATION & CONTROL
LEVEL 3
EWS
Maintenance Server
Historian
SCADA
SCADA Server
CELL/AREA SUPERVISORY CONTROLS
LEVEL 2
Lateral / longitudinal movement devices
SCADA
Local SCADA
Local HMI
IoT Gateway
CONTROL
LEVEL 1
RTU
RTU
PLC
PLC
Remote maintenance
PROCESS
LEVEL 0
Operational Technology (OT)

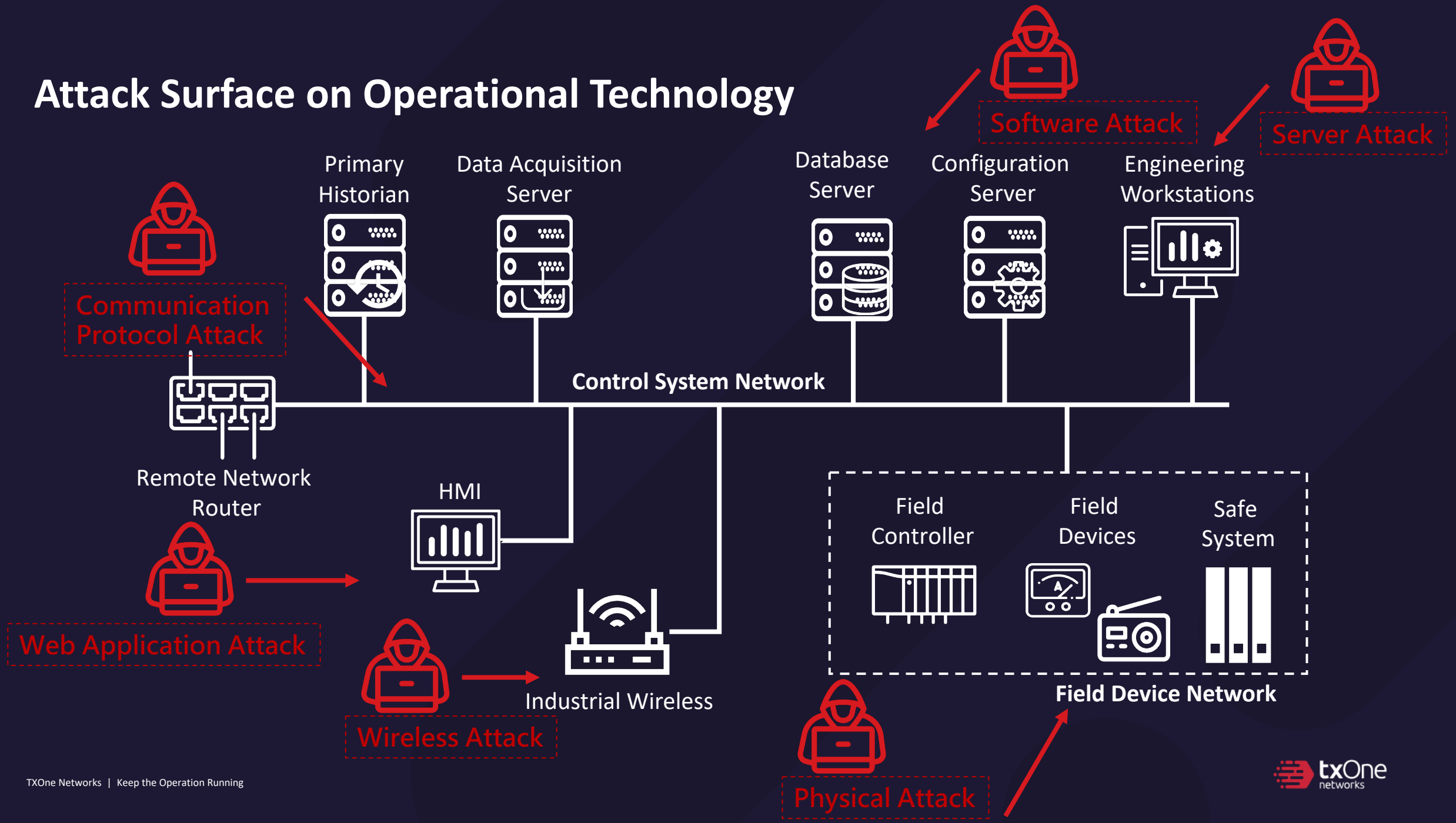


Information Technology (IT)

Operational Technology (OT)

txOne networks

Attack Surface on Operational Technology



Attack Surface on Critical Infrastructure

- Malware/Ransomware Threats
- Insider Threats
- GPS/PNT Jamming or Spoofing Threats
- Third-Party and Supply Chain Threats
- 5G Security Related Threats
  - Sensory Channel Threats
  - Data Spoofing Threats

5

Threat

Endless Ransomware Attacks with 0-day, Supply Chain, and AD attacks

Threat Evolution 2023

- Ransomware-as-a-Service (RaaS) remains a primary money-making strategy for cybercriminals
- Hackers start to use AI cybercrime tools (such as WormGPT and FraudGPT) to craft phishing emails and malwares, making attack tools more accessible
- The ongoing Russia-Ukraine conflict, coupled with the recent escalation in the Israel-Palestine conflict, has led to increased activity among hacker groups associated with these nations

2023 OT & IT Cyberattack Incidents Overview

1

SandWorm Group

Ukrinform

SandWorm deployed 5 different wiper to destroy information channel of Ukraine but failed

Unknown

DNV

Affected 1000 vessels and impacted 70 customers

2

LockBit 3.0

Águas do Porto

Customer Service were limited due to company's restricted response

Unknown

MKS

MKS estimated this incident will cause $200 million lost in revenue

3

Cl0p

Hitachi Energy

Be breached due to supply chain attack that use GoAnywhere

UNC4736

3CX

3CXDesktopApp been detected as malware by customers, affected numerous customers

4

BlackCat/ALPHV

Bernina International

Customer, employee, NDA contracts, and drawing designs be stolen

Money Message

Micro-Star

Source code be stolen and be demanded $4 million ransom

5

Black Basta

ABB

Hundreds of devices have been attacked and exfiltrated data

Data Leak

Toyota

Vehicle data of 2 million customers been exposed

SandWorm

Danish Energy

Up to 22 critical infrastructure been attacked and shut down operation

6

Cl0p

Siemens Energy

Victim of MOVEit attack chain

7

LockBit 3.0

YKK Group

YKK, a leading Japanese zipper manufacturer confirmed its US network was targeted in a cyberattack, which was swiftly contained by YKK USA

8

Unknown

HCA healthcare

11 million patient data across 20 states be stolen and sold on dark web

Ukraine IT Army

Russian railway

Website and mobile app were down for several hours

LockBit 3.0

Nagoya Port

Port operations forced to shutdown until the next day

9

Uknown

Poland railway

Emergency stoppage were triggered in northwestern Poland causing delays

Unknown

CloudNordic

Causing closure on several systems and majority of customer data couldn't be recovered

10

Dark Angel

Johnson Control

Several systems and operations be disrupted, within 27TB data be stolen

Lazarus Group

CoinEX

$70 million be stolen by utilized the hacked hot wallet private key

11

BlackCat/APLHV

Henry Schien

Devices been encrypted and up to 35TB data be stolen

Cl0p

SONY

Victim of MOVEit, more than 6000 employee's data exposed

Unknown

Cisco

Up to 40000 devices were shutdown via unpatched vulnerability

12

LockBit 3.0

Boeing

43GB data be published and be demanded to pay ransom

Unknown

DP World Australia

Ports service were forced to shutdown via the failure patch vulnerability, causing huge delay

The industry only has IT

The industry has OT

txOne networks

6

Threat

IT and OT are Highly Convergence!

OT Environment Impacted by IT Incidents

	2023				2024				
	Total (n=143)	Germany (n=42)	US A (n=62)	Japan (n=39)	Total (n=227)	Germany (n=72)	USA (n=53)	UAE (n=49)	Japan (n=53)
Yes, strongly affected	**47%**	28%	45%	69%	**29%**	29%	28%	45%	15%
Yes, slightly affected	**47%**	60%	52%	26%	**68%**	67%	70%	55%	**79%**
Did not affect	5%	10%	3%	5%	3%	4%	2%	0%	4%
Don't know	1%	2%	0%	0%	0%	0%	0%	0%	2%

94% of IT security incidents affect the organization's OT environment

97% of IT security incidents affect the organization's OT environment

OT Security Incident in the Past 12 Months?

	2024				
	Total (n=405)	Germany (n=102)	USA (n=101)	UAE (n=100)	Japan (n=102)
Yes	**46%**	53%	48%	42%	40%
No OT security incidents, and no forensics or assessments were performed	**13%**	16%	15%	6%	17%
No OT security incidents, but with forensics and assessment performed regularly to ensure that there were no security incidents	40%	31%	37%	51%	42%
Don't know	1%	0%	0%	0%	1%

59% of organizations are at risk.
Almost half suffered an OT incident

Real-time recovery from OT attacks remains a challenge for most organizations

	Time to Recover and Gain Resilience After an OT Security Attack, Total							
	Real-time (less than 1 minute)	Close to Real-time (between 1-5 minutes)	Between 5 minutes and 1 hour	Between 1 hour and 1 day	Between 1 day and 1 week	Between 1 week and 1 month	More than 1 month	Unsure
Virus or malware infiltration	15%	16%	**25%**	21%	13%	7%	3%	-
Ransomware attack	6%	13%	24%	**25%**	23%	9%	-	-
Vulnerability of unpatched systems	4%	17%	19%	**30%**	19%	11%	-	-
Phishing emails	6%	18%	16%	**22%**	16%	18%	4%	2%
Advanced Persistent Threat (APT) attack	5%	17%	12%	20%	**28%**	14%	3%	2%
Distributed Denial of Service (DDoS) attack	5%	8%	16%	24%	**33%**	13%	-	2%
Employee Actions - Human Error (unintentional)	6%	14%	15%	20%	**22%**	18%	3%	2%
Employee Actions - Malicious Motives	8%	13%	18%	11%	**32%**	16%	-	3%
Identity theft, fake login credentials	10%	10%	17%	17%	**44%**	2%	-	-
Third-party vendor or supplier compromise	21%	**29%**	4%	21%	21%	4%	-	-

7

Threat

Huge Impact on Critical Infrastructure/OT

Most Concerning Impact of Security Incidents

	2023				2024				
	Total (n=300)	Germany (n=100)	USA (n=100)	Japan (n=100)	Total (n=405)	Germany (n=101)	USA (n=102)	UAE (n=100)	Japan (n=102)
Compromised operational functionality, productivity loss	**1.1**	**1.3**	**1.2**	0.8	**0.99**	**1.33**	**1.03**	0.67	0.94
Distrust from customers, partners	**0.9**	0.9	0.7	**0.9**	0.59	0.51	0.62	0.69	0.53
Loss of operational control, safety issues	**0.8**	0.8	0.6	**0.9**	**1.00**	1.14	0.97	0.81	**1.10**
Psychological stress to workers	0.8	0.8	0.8	0.7	0.53	0.61	0.47	0.47	0.58
Disqualification from industry associations	0.7	0.6	0.8	0.8	0.42	0.34	0.26	0.52	0.56
Reputational damage	0.7	0.6	0.7	0.7	**0.78**	0.70	0.79	0.82	0.81
Revenue loss	0.6	0.5	0.6	0.6	**0.68**	0.55	0.90	**0.83**	0.44
Lawsuits, fines	0.5	0.5	0.6	0.5	0.41	0.37	0.29	0.56	0.44

OT security incidents are resulting in real financial losses impacting business

	2024				
	Total (n=186)	Germany (n=54)	USA (n=49)	UAE (n=42)	Japan (n=41)
Less than US$10,000	3%	0%	0%	10%	2%
US$10,000-49,999	13%	7%	**20%**	14%	10%
US$50,000-99,999	12%	13%	16%	14%	5%
US$100,000-149,999	**21%**	**35%**	18%	12%	15%
US$150,000-199,999	14%	6%	18%	12%	22%
US$200,000-299,999	11%	7%	8%	**21%**	7%
US$300,000-399,999	18%	28%	12%	5%	**27%**
US$400,000-499,999	5%	2%	6%	2%	12%
US$500,000 and above	3%	2%	0%	10%	0%

8 Strategic

Enterprises are aware of the cyber security of OT and gradually construct it from a strategic perspective

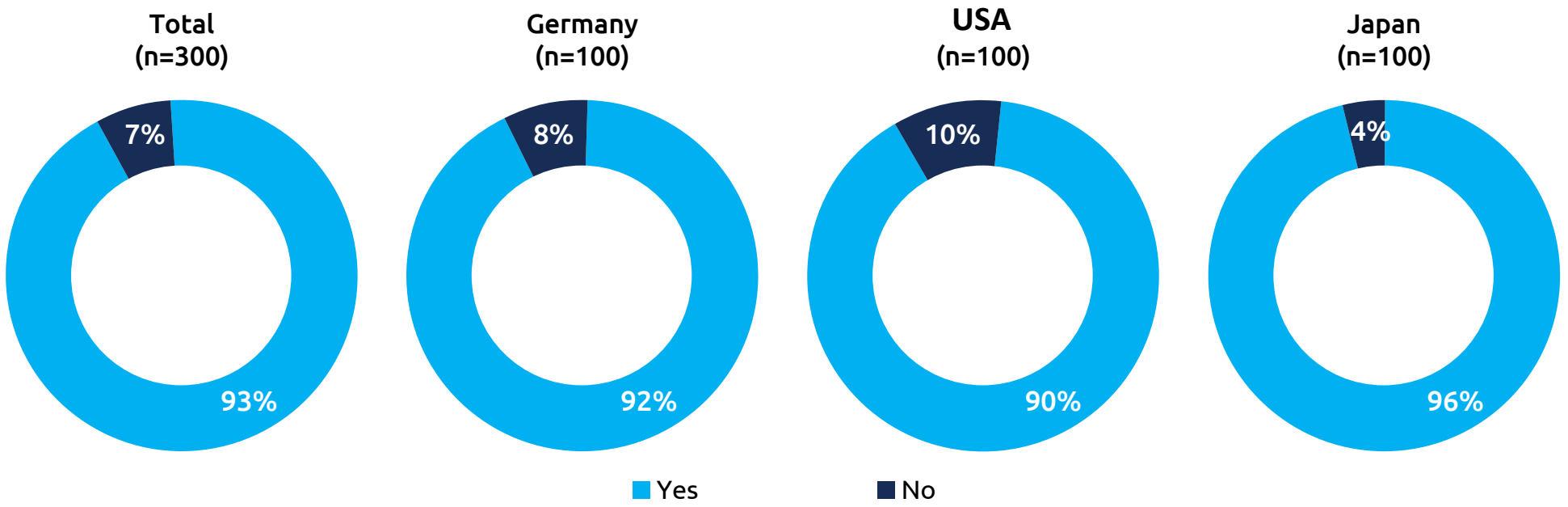
Budget Allocation

	2023				2024				
	Total (n=300)	Germany (n=100)	USA (n=100)	Japan (n=100)	Total (n=405)	Germany (n=101)	USA (n=102)	UAE (n=100)	Japan (n=102)
Increase	**76%**	65%	78%	86%	**68%**	67%	69%	77%	59%
Decrease	1%	0%	1%	0%	4%	0%	1%	5%	**10%**
Remain the same	23%	35%	21%	14%	21%	27%	24%	14%	22%
Share budget with IT security	-	-	-	-	6%	6%	6%	4%	10%
Don't know	0%	0%	0%	0%	1%	0%	1%	0%	0%

9 Solution

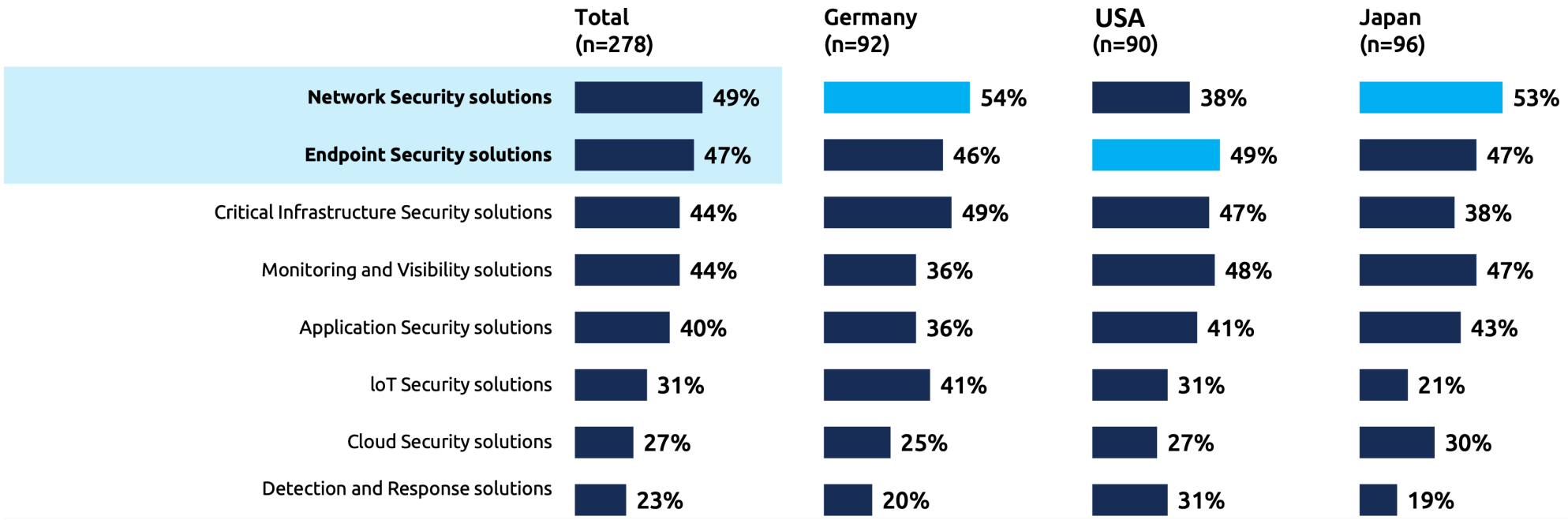
The Deployed Solution Cannot Solve Problems Practically

Current Using Solutions



“ ***93%*** of companies have already used cybersecurity solutions, which have been applied in OT environments ”

Current Using Solutions



> ***49%*** of respondents stated that Network Security solutions have been deployed, followed by ***47%*** for Endpoint Security solutions

Current Using Solutions

	Time Taken To Validate a Solution					
Incident	**Less than a month**	**Between 1-3 months**	**Between 3-6 months**	**Between 6-9 months**	**Between 9-12 months**	**More than 12 months**
Endpoint Security solutions	13%	12%	**14%**	1%	2%	1%
Network Security solutions	5%	11%	**20%**	6%	3%	0%
Critical Infrastructure Security solutions	3%	11%	**17%**	8%	1%	0%
Application Security solutions	7%	8%	**14%**	8%	0%	1%
Cloud Security solutions	4%	**9%**	5%	5%	2%	0%
loT Security solutions	3%	7%	**12%**	6%	1%	0%
Monitoring and Visibility solutions	6%	**17%**	12%	3%	2%	1%
Detection and Response solutions	3%	6%	**8%**	3%	1%	0%

“ Solution typically takes ***3 to 6 months*** for solution validation ”

Current Using Solutions

- Using IT solutions rather than OT cybersecurity solutions in the OT environment
  - Around 70% of organizations are considering reusing previously deployed IT solutions in the OT space
- Insufficient manpower
  - 26% Staff only 1 staff for every 200+ devices
- Human Error
- Outdated systems unable to receive enough technical support

10

Solution

Unprotected Windows Devices in OT Environment are Common

Endpoint Protection Solution

	2023				2024				
	Total (n=264)	Germany (n=87)	USA (n=90)	Japan (n=87)	Total (n=375)	Germany (n=89)	USA (n=94)	UAE (n=99)	Japan (n=93)
Around 25%	**6%**	14%	4%	1%	**1%**	2%	1%	0%	2%
Around 50%	**19%**	20%	21%	15%	**31%**	51%	11%	30%	**32%**
Around 75%	**36%**	38%	24%	45%	**45%**	35%	54%	44%	44%
Almost 100%	33%	23%	46%	31%	16%	8%	24%	15%	17%
100%	6%	6%	4%	8%	7%	4%	10%	10%	4%

61% of organizations have unprotected Windows devices

77% of organizations have unprotected Windows devices

“There is still growth potential for Endpoint Security solutions”

> Organizations should **prioritize OT proactive defense strategies** including supply chain security, asset inspection, endpoint detection and threat intelligence, network segmentation, vulnerability management, patching, and continuous monitoring to prevent and respond to OT cyber threats that may arise in 2024

Thank you for your attention

Keep the operation running!