CLAROTY

Evolving CPS Cybersecurity: The Journey to Exposure Management

CLAROTY

What is exposure management?

“Exposure management is a cybersecurity practice that involves identifying and addressing potential vulnerabilities and risks before they can be exploited. The goal is to reduce the attack surface and maintain an acceptable level of risk”

Connectivity That Drives Change

Expanded Connectivity

Digital transformation and the push for increased productivity have led to converged IT and OT networks

Heightened Threat Activity

Increased attack surface at a time when cybercrime is more accessible & deployable than ever

Regulatory Pressure

Governments act to protect environments that underpin national security & public safety

CLAROTY

Digitization is Driving Innovation

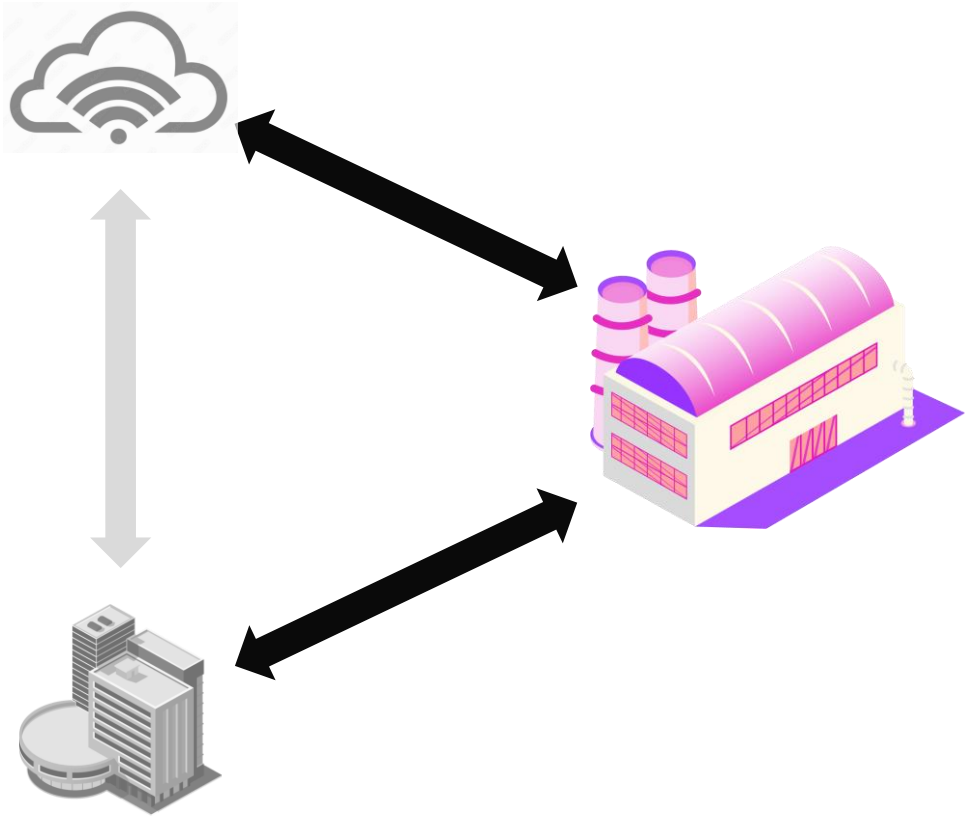
Automation & Robotics

Digital Twins

5G Networks

Edge Computing

Innovation is Being Disrupted by CPS Cyber Attacks



2024 — **Fuxnet Attack in Russia**

Ukrainian intelligence deploys custom malware that severely disrupts emergency response capabilities in Moscow..

2023 — **US Water Systems Targeted**

Iran's CyberAv3ngers demonstrate access to Israel-made PLCs at U.S. water facilities

2023 — **Change Healthcare Attack**

Ransomware attack disrupts services from U.S.'s largest healthcare payment provider and servicer.

2023 — **Volt Typhoon Embeds in CI**

Attack tools attributed to Chinese APT found embedded in US critical infrastructure.

2023 — **Dole, Clorox Ransomware Attacks**

Ransomware caused global food and giants to shut down production sites, impacting deliveries, causing shortages.

2023 — **Tallahassee Memorial Healthcare**

Cyber attack forced hospital to operate under emergency downtime procedures for two weeks.

CLAROTY

Cyberattacks are Offsetting Gains from Innovation

Real threats

Real money

Real impact

69% victims pay ransoms[1]

$1.1B in ransoms paid in 2023[2]

$870M quarterly impact: Change HC[3]

1 Claroty, "The Global State of Industrial Cybersecurity 2023"
2 FBI Internet Crime Report 2023
3 UnitedHealth Group Earnings Call, Q1 2024

CLAROTY

Regulations & Frameworks For Critical Infrastructure

ISA/IEC-62443

NIS2 Directive

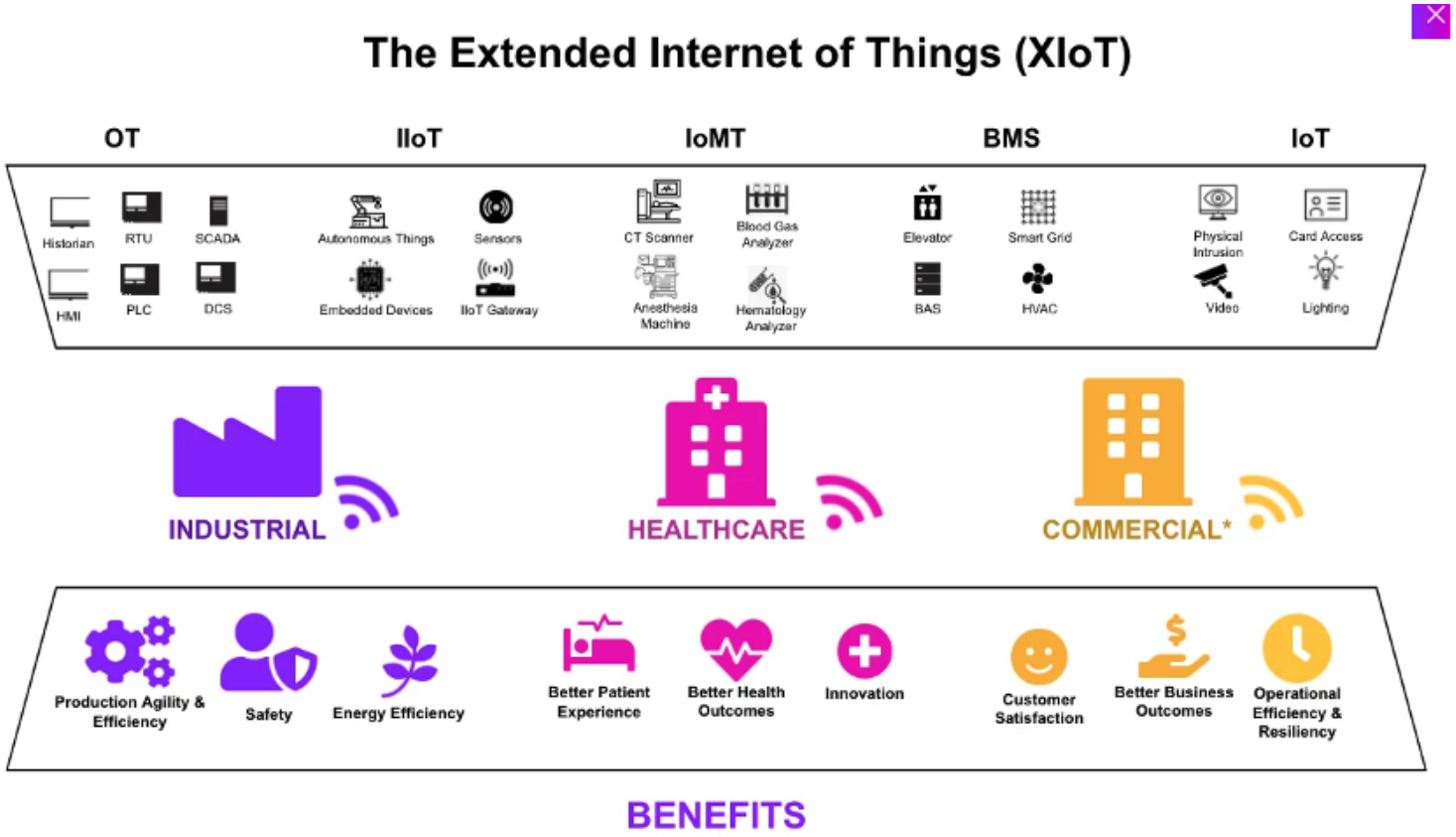
NIST Cybersecurity Framework

Cyber Assessment Framework

NPSA – UK – CNI Guidance*

GDPR

What are Cyber-Physical Systems (CPS)



Cyber-physical systems (CPS) are integral to modern operations, combining hardware and software to control physical processes.

These systems, which include smart grids, autonomous vehicles, and patient monitoring, are increasingly interconnected with IT networks, enhancing efficiency but also expanding the attack surface for cyber threats.

CLAROTY

OT Environments Require A Different Approach

	IT Environments	OT Environments
	IT Systems (servers, laptops, etc)	Cyber-physical systems (OT, BAS, IoT)
	Confidentiality, Integrity, Availability	Safety, Reliability, Productivity
	Standard protocols and device types	Proprietary protocols and diverse assets
	Standard security controls apply	Operational context drives security
	Compatible with most security solutions	Incompatible with most security solutions

CLAROTY

Prioritize: Business Impact Assessment Centric Priority

CLAROTY

Going Beyond Vulnerability Management (VM)

Zero-day vulnerabilities are **rarely the primary cause** of a breach

2-7% of vulnerabilities are ever actually exploited[1]

VM **does not account for broader exposures** and attack vectors

- And Notably -

Vulnerability management **does not consider business outcomes** as a factor in remediation priority

CLAROTY

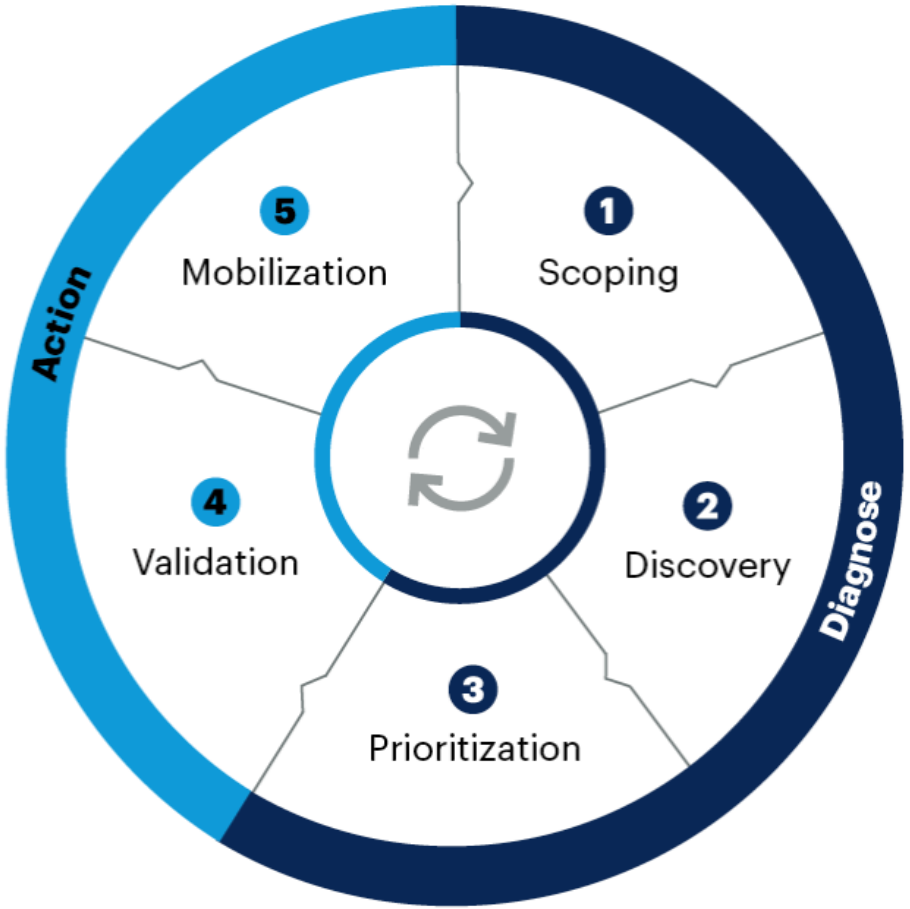
[1]The EPSS model. FIRST — Forum of Incident Response and Security Teams.

CPS Requires Exposure Management

Continuous Threat Exposure Management - CTEM

What is Exposure Management?

"The objective of CTEM is to get a consistent, actionable security posture remediation and improvement plan that business executives can understand and architecture teams can act upon."



Source: Gartner
763954_C

CLAROTY

Gartner, Innovation Insight: CPS Secure Remote Access Solutions, Katell Thielemann, Abhyuday Data, Wam Voster, 18 April 2024.

BIA Informs Severity Levels

Severity	Business impact					Technical attributes	
Tier	Safety	Legal	Regulatory	Financial	Reputation	Data classification	Operations
4. Cyber crisis	Severe injuries/ death	Significant impact	Fines: $Z+	Loss: $Z+	Global media	Top secret	Catastrophic outage
3. High	Serious injuries	Moderate impact	Fines: $Y-$Z	Loss: $Y-$Z	National media	Secret	Major outage
2. Medium	First aid	Low impact	Fines: $X-$Y	Loss: $X-$Y	Local media	Internal	Minor outage
1. Low	No injuries	No impact	No violations	No loss	No harm	Public	No outage

Gartner

Exposure Management Considerations

- Think beyond CVSS scores
- How exposed are you?
- Device criticality
- Business Impact
- KEV? Remotely Exploitable?
- Remediation likelihood?
- Compensating controls?

Key Takeaways

- Digital transformation is exposing cyber-physical systems (CPS)
- State actors and criminal gangs are relentlessly targeting CPS
- Ransom payments, safety & regulations are challenging security leaders
- Imperative to understand exposures beyond prioritizing critical vulnerabilities
- Critical assets, wide exposure, Insecure connectivity and KEV’s are priority #1