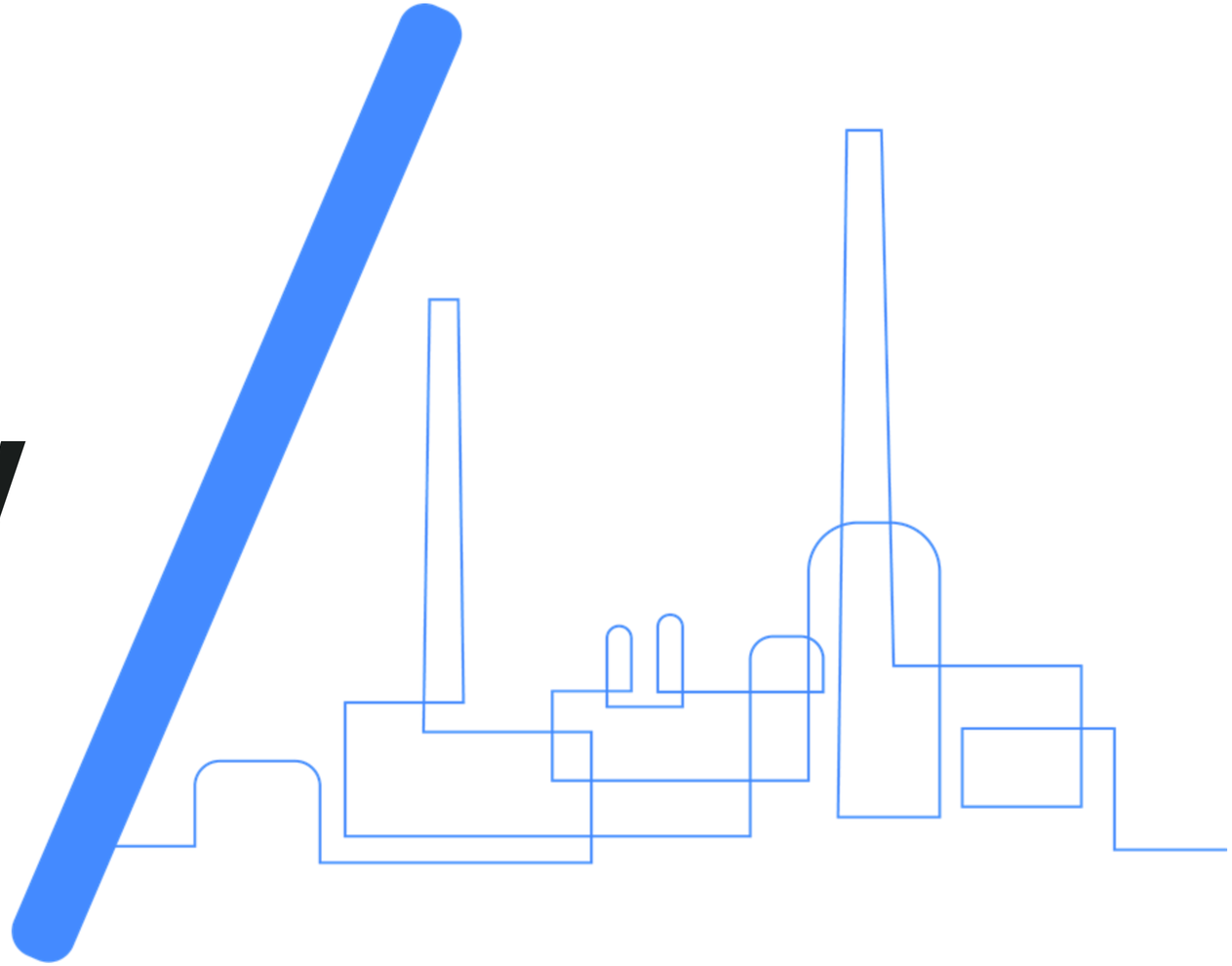
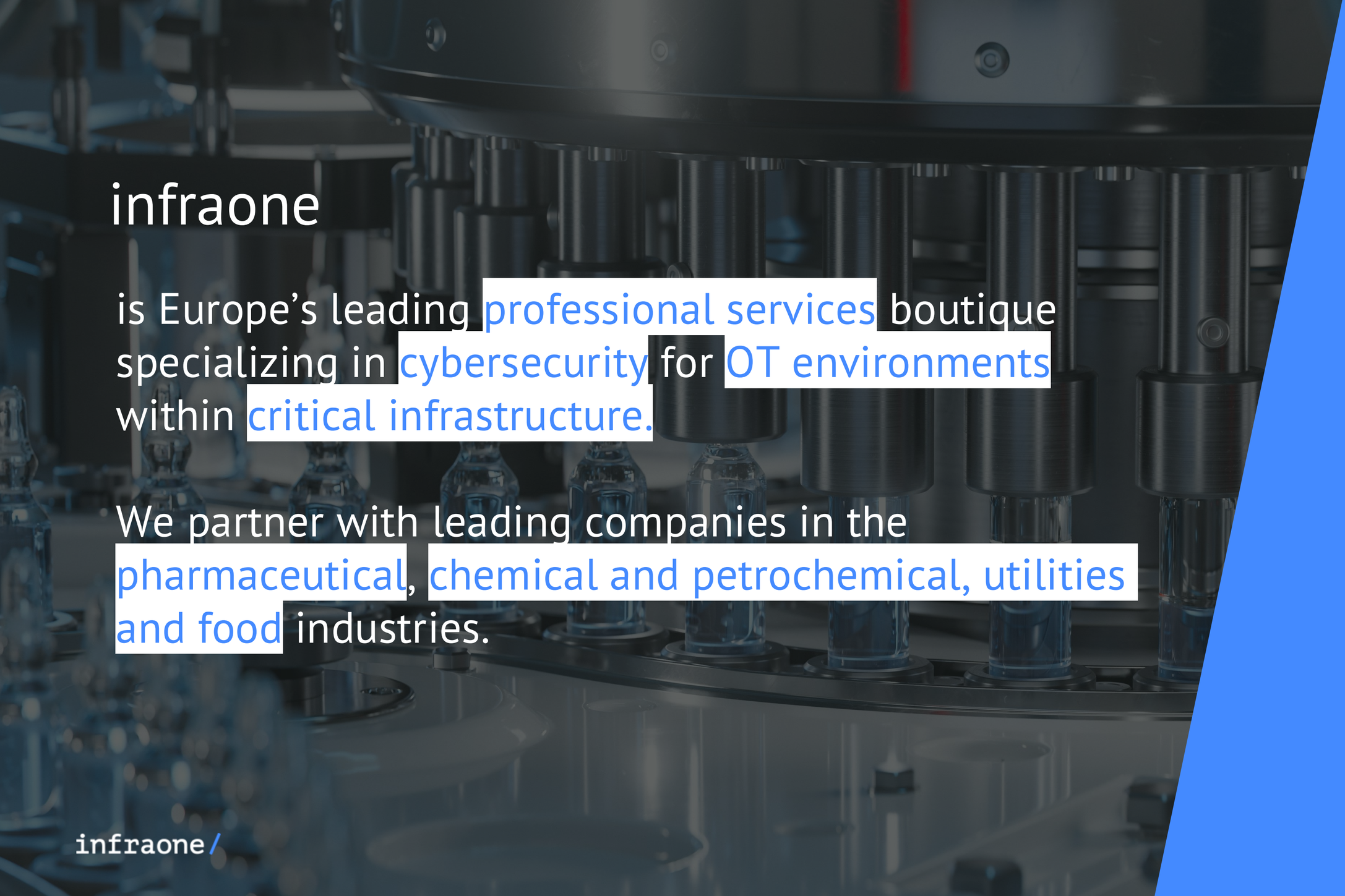
November 12th, 2025

Industrial Cybersecurity

Key insights

Diego Martín
diego.martin@infraone.com





infraone

is Europe’s leading professional services boutique specializing in cybersecurity for OT environments within critical infrastructure.

We partner with leading companies in the pharmaceutical, chemical and petrochemical, utilities and food industries.

What is an Industrial Environment?

Industrial environments: real-world consequences

An industrial environment refers to the physical and digital ecosystem where industrial processes take place — typically involving Operational Technology (OT) systems that monitor and control equipment, machinery, and critical infrastructure.

Key Components

- → Operational Technology (OT): Hardware and software that directly monitors or controls industrial processes.
- → Industrial Control Systems (ICS): Includes PLCs, SCADA, DCS and other automation systems.
- → Physical assets: Pumps, motors, valves, sensors, conveyors, reactors, etc.
- → Communication protocols: (Modbus, Profibus, OPC UA, etc.) connecting machines and control systems.

Industrial environments bridge cyberspace and the physical world — meaning a digital intrusion can cause real-world consequences.

Evolution of the Industrial Environment

IT meets OT

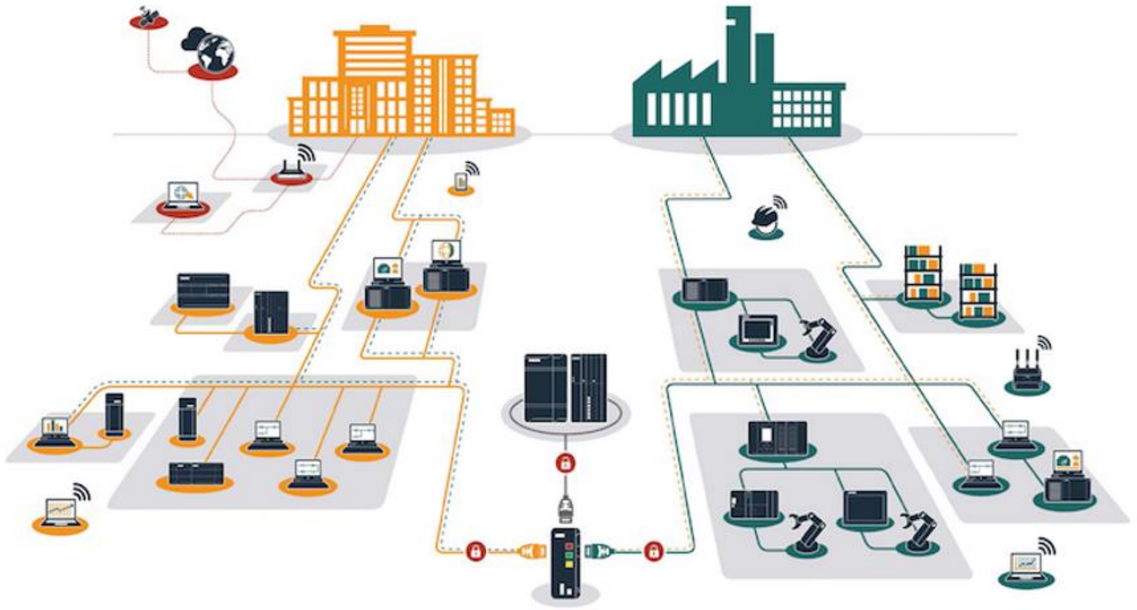
infraone/

Evolution of the Industrial Environment

Toward Hyperconnectivity

Traditional Factory

- → Separate automation “islands”
- → Opaque processes
- → Manual processes
- → No central alarms
- → Legacy systems



Connected Industry

- → Full automation
- → Process interoperability
- → Vertical integration
- → Transparent processes
- → Energy efficiency
- → Resource optimization

infraone/

Main Difference from IT

	IT	OT
Priority	Confidentiality	Availability and Integrity
Focus	Data processing & communication	Physical process control
Impact of failure	Data loss	Physical damage, production loss, safety indicents
Criticality over time	Tolerates delays and interruptions	Real-time response is critical
Cybersecurity Maturity	Generally high and standardized	Often lower, legacy systems and limited visibility
Lifecycle Duration	3–5 years (frequent upgrades)	15–25 years (long operational lifespan)
Typical Protocols Used	HTTPS, SMTP, FTP, SSH	Modbus, S7, Bacnet, OPC UA, DNP3
Environment	Office networks, data centers	Industrial plants, production lines, utilities

Cybercrime:
Fun or Business?

Cybercrime: Key Statistics

Why Is Cybersecurity a Critical Factor?

infraone/

Manufacturing

Main Cybercrime Statistics

→ Worldwide cybercrime costs are estimated to hit $10.5 billions annually by 2025, emphasizing the need for enhanced cybersecurity measures. (Statista)

→ In 2024, the global average cost of a data breach was $4.88M. (IBM)

→ Manufacturing was the most targeted industry in the first half of 2024, seeing a 41% increase in attacks. (Ontinue)

→ Manufacturing led all other industries in ransomware and database leak attacks in the first half of 2024. (Critical Start)

→ Manufacturing accounted for 29% of global ransomware attacks in Q2 2024, a 56% year-over-year increase. (Check Point Research)

→ Attackers targeting manufacturing industry victims typically gained initial access through spearphishing attachments and exploitation of remote services and public-facing applications. (Critical Start)

Real-World OT Cyberattacks

When Cyber Impacts the Physical World

infraone/

Criminal, political, and personal

Motivations Behind a Cyberattack

1

Criminal: Economic Gain

→ The most common motivation — attackers seek direct financial profit.

→ Ransomware, data theft, fraud, extortion.

→ They operate like businesses: with structure, investment, and profitability goals.

2

Political: Espionage and Manipulation

→ State-sponsored groups.

→ They aim to gather strategic information, conduct sabotage, or destabilize countries, companies, or critical sectors.

→ They act over the long term and with a high level of sophistication.

3

Cyberwarfare: Conflicts Between States

→ Attacks designed to paralyze infrastructures, sow chaos, or gain geopolitical advantages.

→ Key sectors: energy, transportation, telecommunications, and defense.

→ Highly coordinated, scalable, and often covert.

Examples of Organizations

→ CHERNOVITE (Rusia)
- → Active: 2020 – Present
- → Specialty: Sabotaje industrial y ciberespionaje OT
- → Notable attacks in the last 2 years : Desarrollo del malware PIPEDREAM / INCONTROLLER, diseñado para afectar dispositivos industriales de Schneider Electric, Omron, OPC UA, etc.

XENOTIME (Rusia)
- → Active: 2022 – Present
- → Specialty: Ataques a sistemas de seguridad industrial (SIS).
- → Notable attacks in the last 2 years : Triton / Trisis: Malware dirigido a sistemas Triconex de Schneider Electric, capaz de provocar fallos catastróficos en plantas químicas o refinerías., ...

→ LockBit (Rusia)
- → Active: 2019 – Present
- → Specialty: Ransomware (RaaS).
- → Notable attacks in the last 2 years : 1.700 ataques en 12 meses (91M$ conocidos)

Oldsmar Water Treatment Plant

Florida, EE.UU., feb 2021

What happened

A hacker gained remote access to the control system of the Oldsmar water treatment plant through TeamViewer, a remote desktop software used by operators. Once connected, the attacker increased the sodium hydroxide (NaOH) — caustic soda — level in the water from about 100 parts per million (ppm) to 11,100 ppm.

Technical details

- → The attacker exploited weak remote-access security and lack of network segmentation between IT and OT systems.
- → The incident didn't use advanced malware or exploits — just unauthorized access via poorly secured remote management software.
- → The plant quickly disconnected remote access and notified authorities.

Impact and Lessons learned:

- → Had the change gone unnoticed, it could have poisoned the city's water, causing serious chemical burns or illness to thousands of residents.
- → The case illustrates that even a small local facility can be a critical target — and that simple misconfigurations can lead to life-threatening consequences.

Sandworm —Ukraine's Power Grid

2022

What happened

In October 2022, the Sandworm group (linked to Russia's GRU) launched a coordinated cyberattack on a Ukrainian power substation. The attackers remotely tripped circuit breakers, causing a temporary power outage in part of the country. Two days later, they deployed CaddyWiper malware to erase traces and disrupt recovery.

Technical details

→ Attackers had long-term access to the OT network prior to the incident.

→ They used "living-off-the-land" techniques, leveraging legitimate admin tools to send control commands.

→ Combined with wiper malware on IT systems, creating both operational disruption and forensic blindness.

Impact and Lessons learned:

→ Caused a real power outage affecting civilians — showing cyberattacks can have direct physical consequences.

→ Demonstrated coordination between cyber and kinetic operations during active conflict.

The foundations of a resilient and safe industrial environments

How to mitigate Threats in OT

infraone/

Cybersecurity Initiatives

Implemented & On-going projects

1

Asset Inventory and Visibility

Identify all connected devices, including PLCs, HMIs, sensors, and engineering workstations.

You can’t protect what you don’t know exists.

2

Network Segmentation

Divide IT and OT networks into clearly defined zones and implement strict communication controls.

Reduces lateral movement of threats and isolates critical assets.

3

Secure Remote Access

Control and monitor all remote connections to the OT network using VPNs, MFA, and jump servers.

Prevents unauthorized access and minimizes exposure.

4

Visibility and Anomaly Analysis

Implement continuous monitoring and anomaly detection tools to identify unusual network or process behavior.

Detects potential intrusions or malfunctions early, before they cause impact.

Conclusions

Key Takeaways

Conclusions

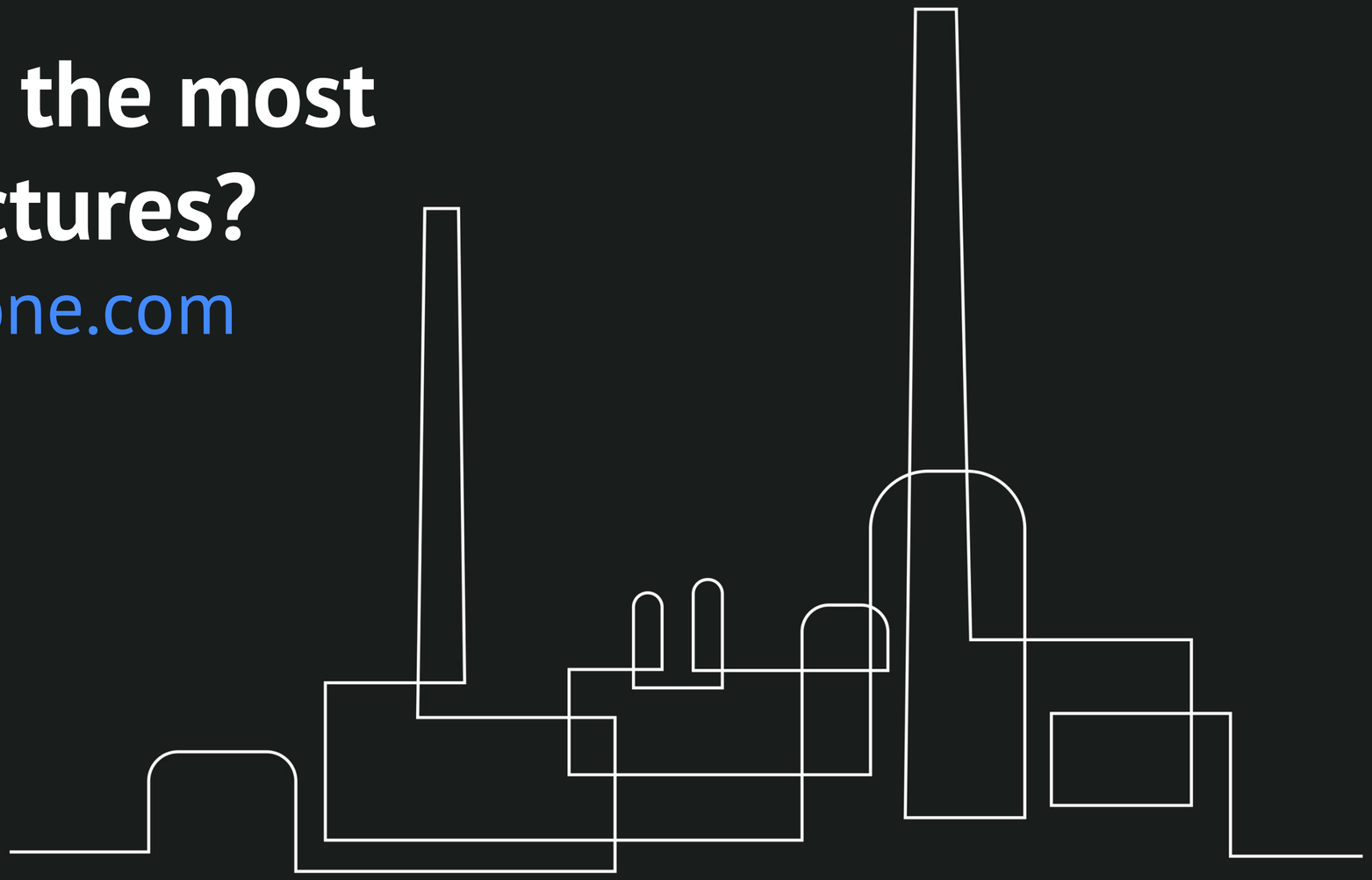
Key Takeaways

- → Cybersecurity in OT is about protecting lives, not just data. Attacks on industrial systems can cause physical damage and human harm.
- → Visibility is the foundation. You can't defend what you don't know exists — asset inventory is step #1.
- → Segmentation and monitoring save lives. Separating IT and OT networks and detecting anomalies early are critical.
- → Collaboration between people, processes, and technology is essential. Operators, engineers, and cybersecurity teams must work together.
- → Resilience over reaction. It's not just about preventing incidents — it's about ensuring safe recovery when they occur.

In industrial cybersecurity, we protect more than information — we protect operations, communities, and lives.

Ready to protect the most critical infrastructures?

diego.martin@infraone.com



infraone/