TXONE NETWORKS

11 Proven Ways for IT Managers in Breweries to Secure Their Production

IT Security Architecture Playbook

Executive Summary

If you are the IT security leader responsible for your brewery group's OT environment, the next audit is not the problem. The next board presentation is not the problem. The real problem is the **33% of security incidents that occur at the IT/OT integration point** [1], the SANS finding that **19% of OT incidents take more than a month to remediate fully** [2], and the Claroty Team82 reality that **82% of observed attacks abuse exposed VNC clients on internet-facing CPS assets** [3]. Coordination between IT and OT cannot win a race against attacker tooling that operates at machine speed.

> **33% of security incidents occur at IT/OT integration points** [1]. The IT/OT handoff is the statistical epicenter, and coordination cannot beat machine-speed attacker tooling.

This guide is for the IT Security Leader at a European brewery group. Eleven proven ways to secure production, implementable without losing operational autonomy at the sites, without replacing the IT security tooling already in place, and without creating a NIS2 compliance nightmare. Five (Ways 4, 5, 9, 10, 11) are governance, policy, and procedure moves your team can drive without buying anything; they harden the IT/OT boundary on documentation alone and produce audit evidence as a byproduct. The remaining six describe a prevalent OT security problem and the broader set of architectural approaches the industry uses to address it; in each, TXOne is named as one OT-native option among the broader options. Each way maps to a specific NIS2 Article 21 measure, an IEC 62443 zone or conduit, and (where relevant) a SIEM forwarding path.

Carlsberg Group (Denmark, global brewing operations, 140+ brands) runs a version of this playbook [4]. They validated the result without losing operational continuity. The case notes carry the IT Security Leader narrative, the audit-defensible artifacts, and the technology stack they settled on.

The real problem on the IT Security Leader's desk

The next NIS2 audit, incident, or quarterly review is asking a question your current security program cannot answer: "Is the production environment actually protected, or do we just have visibility into it?" Detection-only platforms document threats. IT security tools extended into OT produce agent crashes, reboot demands, and exception tickets that never close. The IT/OT handoff happens at Level 3.5 of the Purdue reference model, where 33% of OT security incidents occur [1].

The math. LockBit-class ransomware encrypts in approximately 4 minutes [5]. Detection-to-enforcement coordination between the SOC, the OT team, and the firewall operations team takes 35 to 45 minutes [6]. Any attack that reaches Level 3.5 without being blocked inline has already executed. The only move that changes the outcome is enforcement at machine speed at the conduit itself. The eleven ways below are organized across the same risks Guide 1 covers, so IT and OT leadership see the same map from opposite sides. Each way identifies the specific gap an IT Security Leader is accountable for, names the NIS2 Article 21 measure it satisfies, and (where applicable) specifies the SIEM-consumable artifact that lands in your existing console.

The 11 Ways

11 PROVEN WAYS • EUROPEAN BREWERIES

Secure brewery production from the IT Security Leader desk

IT SECURITY LEADER LENS • 5 governance moves (no procurement) • 6 architectural moves

Governance move (no procurement)
Architectural move (TXOne is one option)

1 ARCHITECTURAL

Segment at L3.5 with OT-aware enforcement

Conduit control that reads OPC-UA, Modbus, and Profinet at the command level, not as generic TCP.

2 ARCHITECTURAL

Hardware bypass as an IT requirement

Inline prevention with fail-safe relay so a security appliance never becomes the cause of a line stop.

3 ARCHITECTURAL

Cover the legacy endpoint exception

Endpoint agent that runs Windows 2000 SP4 to 11 and never reboots. Closes the legacy HMI gap.

4 NO SPEND

Contractor media policy, IT/OT-joint

Signed-off USB validation at reception with end-to-end audit evidence the NIS2 reviewer can read.

5 NO SPEND

Centralize the per-site asset register

One register across sites, owned by IT, refreshed on cadence. The living NIS2 evidence artifact.

6 ARCHITECTURAL

Lock the brewhouse baseline

Application allowlisting on brewhouse and packaging PCs blocks anything not approved. No signature chase.

7 ARCHITECTURAL

Close the coordination gap inline

Sub-second deep packet inspection at the conduit eliminates the 4-vs-35-minute detect-to-respond window.

8 ARCHITECTURAL

Virtual-patch the unpatchable PLC

IPS signatures shield legacy PLCs from known CVEs without ever touching the controller firmware.

9 NO SPEND

In-plant USB as a maintenance procedure

Approved USBs only, logged, reviewed, retired. Audit evidence ladders up from operator to NIS2 sign-off.

10 NO SPEND

Recurring IT/OT governance forum

30-minute weekly forum with named decision-rights closes the handoff gap that 67% of organizations cite.

11 NO SPEND

Rehearse the NIS2 incident

Production, OT, IT, quality, and legal at one table. Tabletop the night-shift attack before it happens.

THE SPLIT

5 NO-SPEND + **6** ARCHITECTURAL

Five governance moves your team can drive without procurement. Six architectural moves where TXOne is one OT-native option.

Each way names its NIS2 Article 21 measure and (where applicable) the SIEM forwarding artifact. See Section 2.

GUIDE 2 OF 3 • EU BREWERY 2026

WAY 01

Segment the brewery at Level 3.5 with a control that understands what is on the wire.

The brewery risk: a flat, bridgeable network lets an IT-side compromise move laterally into brewhouse PLC segments faster than any SOC can coordinate a response. The IT/OT DMZ at Purdue Level 3.5 is both the highest-value conduit and the statistical epicenter of OT incidents.

What the industry typically does: three approaches. VLAN-only segmentation (does not enforce; blind to OT protocols). IT next-generation firewalls at the boundary (port-aware but blind to industrial protocol semantics; often requires re-IP and PLC-side cooperation). OT-native inline appliances at the conduit (deep packet inspection at the command level; zero IP; designed to fail safe). The test: can the device read OPC-UA, Profinet, Modbus at the command level, or is it inspecting them as generic TCP?

The TXOne option: TXOne EdgeIPS. AI-powered auto-rule learning generates the initial policy in days. Deep packet inspection across 180+ industrial protocols. Zero-IP deployment. EdgeIPS forwards blocked-traffic events, protocol violations, and policy changes to Splunk, QRadar, or Microsoft Sentinel via syslog/CEF in real time.

ARCHITECTURE

Transparent, zero-IP deployment at the IT/OT DMZ. AI-supervised policy generation during a baseline window. No PLC reconfiguration, no network team ticket for readdressing.

NIS2 ARTICLE 21 / IEC 62443

Network segmentation is a required technical measure. IEC 62443 places the IT/OT DMZ between Zones 3 and 4; the conduit is the highest-priority control point.

4.0

TXOne Network Segmentation score (out of 5.0)

15

ARCHITECTURAL MOVE · TXONE IS ONE OPTION

WAY 02

Treat hardware bypass as an IT-side requirement, not an OT nice-to-have.

The brewery risk: a security device failure on the bottling line stops production the same way a cyber incident does. The IT Security Leader is accountable either way. OT teams who have experienced a security-tool-induced outage can veto any future deployment.

What the industry typically does: most security devices placed in OT today were designed for IT data centers; they fail closed and stop traffic. The alternative is to specify physical hardware bypass: a relay closes if the device powers off or fails its self-test; traffic continues uninterrupted. The OT-native security class adds inspection and enforcement to the same fail-safe form factor. No mainstream IT firewall vendor offers physical relay bypass in a DIN-rail form factor with industrial operating range; specify it in procurement before deployment is approved.

The TXOne option: TXOne Edge and EdgeFire include physical relay bypass. EdgeFire 1012 and 1014 carry **700,000 hours MTBF** in industrial DIN-rail form factor with minus 40 to 75 C operating range. EdgeOne records bypass-state changes and failure events; forwards to the SIEM as a critical-severity event.

PROCUREMENT

Specify fail-safe hardware bypass on every inline OT security device before deployment is approved. The OT veto is earned; relay-level bypass is the answer.

NIS2 ARTICLE 21 / IEC 62443

Business continuity is a named pillar. IEC 62443 treats redundancy and fail-safe behavior as baseline requirements for conduit devices.

3,600+

global TXOne deployments with zero unplanned downtime [8]

ARCHITECTURAL MOVE · TXONE IS ONE OPTION

WAY 03

Close the legacy endpoint exception with an agent that can actually run on the legacy estate.

The brewery risk: every security program documents the same exception, "HMIs running legacy Windows cannot run our IT EDR," and the exception list grows with every audit. The IT Security Leader defends the exception to the board and owns the incident when it lands there.

What the industry typically does: three endpoint approaches. IT EDR adapted for OT (CrowdStrike, SentinelOne, Microsoft Defender) refuses or destabilizes legacy platforms (Win 7, XP, Server 2008) and demands reboots production cannot grant. Application allowlisting alone catches what is on the list and nothing else. OT-native baseline-locked agents combine multi-engine scanning, behavioral detection, and per-device baseline lockdown across the full Windows range. The test: does the agent install without a reboot, baseline the machine without manual allow-list authoring, and recognize the OT applications already running?

The TXOne option: TXOne Stellar ICS. Automated per-device baseline generation. Zero-reboot deployment. Single policy from Windows XP and Server 2000 SP4 through the latest Windows 11 and Server 2025. **70,000+ OT application recognition repository** [9]. Stellar Kiosk for constrained endpoints; Stellar Discover for compatibility validation. StellarOne forwards endpoint events, application-deviation events, USB-device events, and malware detections to the IT SIEM via syslog/CEF.

BOARD NARRATIVE

Changes from "we have documented the legacy exception" to "we have eliminated the legacy exception." Zero-reboot install across the full Windows range.

NIS2 ARTICLE 21 / IEC 62443

Endpoint hardening expectation. IEC 62443 Zone 2 supervisory control.

100% / 51%

of orgs operate legacy Windows in OT; 51% of EU orgs had a legacy Windows incident in the past 12 months [10]

ARCHITECTURAL MOVE · TXONE IS ONE OPTION

WAY 06

Stop fileless attacks at the brewhouse PC by locking the baseline, not by chasing signatures.

The brewery risk: 81% of interactive intrusions are malware-free, relying on living-off-the-land techniques [7]. Signature-based detection cannot see them. Volt Typhoon-class intrusions hide in legitimate administrative tools and dwell for days before acting.

What the industry typically does: three approaches. Signature-only AV catches the named-malware case and misses the rest. EDR with behavioral analytics fires on suspicious behavior but is calibrated for IT user context that does not exist on a brewhouse PC. Application lockdown with an automatically-generated baseline simply denies anything outside the operational baseline; the fileless attack runs into a wall because powershell-launched-by-svchost is not in the baseline.

The TXOne option: TXOne Stellar ICS includes automated per-device baseline generation and application lockdown. CPSDR (the TXOne behavioral-anomaly engine) compares live behavior against the learned baseline; deviations are flagged and, where policy permits, blocked.

IT-SIDE CONTROL

Deploy automated baseline lockdown on every brewhouse PC and engineering workstation. The baseline generates without manual allow-list authoring. Anything outside the baseline cannot execute.

NIS2 ARTICLE 21 / IEC 62443

Endpoint hardening and integrity controls. IEC 62443 application whitelisting and behavioral anomaly detection are foundational endpoint controls.

81%

of interactive intrusions are malware-free

7

WAY 07

Close the coordination gap with sub-second inline prevention at the conduit.

The brewery risk: ransomware encrypts in approximately 4 minutes [5]. Detection-to-enforcement coordination takes 35 to 45 minutes [6]. The IT Security Leader is responsible for math that does not work.

What the industry typically does: detection-led OT security is "see it and route it." A passive SPAN-port sensor detects suspicious traffic; the SOC opens a ticket; the firewall team writes a rule; the rule is staged and deployed; the line is contained. On paper, the model works. In practice, the line stops first. The architectural alternative is inline enforcement at the conduit itself: the same device that sees the traffic also blocks it, in milliseconds, without leaving the traffic path.

The TXOne option: TXOne Edge sits inline at the conduit boundaries with automated blocking enabled, sub-second enforcement at wire speed, and hardware bypass for fail-safe continuity. Connect Edge into SenninOne so the detection-to-enforcement path is a single product path, not a multi-vendor handshake. Block events forward to the IT SIEM within seconds; the SOC sees "blocked" instead of "coordinated response in progress."

TIMING

Inline enforcement at the conduit. The 4-minute ransomware clock vs the 35-to-45-minute coordination window — math that only inline prevention can win.

NIS2 ARTICLE 21 / IEC 62443

Prevention, not only detection. IEC 62443 conduit enforcement is explicitly an inline responsibility at the zone boundary.

82%

of observed attacks abuse exposed VNC clients on internet-facing CPS assets [3]

ARCHITECTURAL MOVE · TXONE IS ONE OPTION

WAY 08

Virtual-patch the controllers your maintenance window cannot.

The brewery risk: 26% of CISA ICS vulnerability advisories released over the past five years offered no patch, and 18% had neither a patch nor a documented mitigation [11]. Where patches exist, controllers cannot be taken offline during peak season. The IT Security Leader owns the vulnerability management program and the exception that says "unpatched, production-critical, next window October."

What the industry typically does: three options for an asset that cannot be patched in-window. Accept the risk and document the exception (the one the auditor scopes against). Replace the asset (capital cycle, often years away). Apply a compensating control. Virtual patching at the network layer is the most operationally-honest option: exploit traffic is blocked inline by a device upstream of the controller; the controller is never touched; the vulnerability moves from "open" to "compensating-control-active" in the register. Detection-only platforms cannot virtual-patch from a SPAN port. IT firewalls cannot read OT protocol semantics. Inline OT-native enforcement closes both gaps in one device.

The TXOne option: TXOne Edge delivers virtual patching at the network layer with rule-to-CVE mapping. Apply at the conduit upstream of the unpatchable controller. Virtual-patch policy changes and blocked exploit attempts forward to the IT SIEM with CVE mapping; the rule itself is the audit evidence.

IT-SIDE CONTROL

OT-native virtual patching at the network layer. Exploit traffic blocked inline; the controller itself is not touched. Extend asset life to the next planned shutdown.

NIS2 ARTICLE 21 / IEC 62443

Vulnerability management. IEC 62443 compensating controls are formally recognized when the physical patch is infeasible.

26% / 18%

of CISA ICS advisories had no patch / no patch and no mitigation [11]

NO-PROCUREMENT GOVERNANCE

WAY 04

Make contractor media validation a documented IT/OT-joint policy with audit evidence.

The brewery risk: 25% of top OT security incidents start with a USB plug-and-play event [12]. Breweries depend on contractors who arrive with their own laptops and firmware media. The IT Security Leader is accountable for the supply-chain security control under NIS2 Article 21.

Do this (no procurement, IT/OT joint procedure):

- Publish a contractor media policy as a joint IT/OT procedure. Specify which media classes are allowed, at which Purdue levels, and with what authorization. Owner: IT Security Manager. Co-signer: Head of OT.
- Add a declared-media field to the existing reception sign-in flow: device serial, target system, time of insertion. Maintain a spreadsheet; the log is the chain-of-custody record.
- Brief reception, shift supervisors, and the contractor pool. Add the policy to the supplier onboarding contract.

Why it works in a brewery: the contractor sign-in already exists for safety and insurance reasons. Layering a media declaration onto an existing process is administrative work, not capital. The signed log is what the NIS2 Article 21 supply-chain security obligation expects.

SIEM forwarding (no tool required): export the log into the SIEM during the migration period as a structured CSV import. The artifact lands in the audit folder regardless of the technical layer.

When to bring in a tool: TXOne Safe Port is the OT-native kiosk for technical enforcement, replacing the manual log with a deterministic event stream. Every visitor scan generates a SIEM event with pass/fail disposition, file hashes, and contractor metadata.

TIMING

Put it in place this week. No capital spend. Brief reception on shift handover.

NIS2 ARTICLE 21

Supply-chain security. Contractor access is called out explicitly in enforcement guidance.

25%

of top OT security incidents start with a USB plug-and-play event [12]

NO-PROCUREMENT GOVERNANCE

WAY 05

Centralize the per-site asset register and treat it as a living NIS2 evidence artifact.

The brewery risk: every site claims to have an asset register; few central IT functions have a consolidated view. NIS2 auditors expect both. **30% of IR cases were discovered because "something seemed wrong"** rather than by detection tools [13]. Until the register exists, the OT team is defending what it cannot enumerate.

Do this (no procurement, IT/OT joint procedure):

- Coordinate per-site OT asset walkdowns. Standard schema: vendor, model, firmware, location, owner, Purdue level, primary process, "talks to" column, date stamp.
- Centralize each site's signed register on the IT side. Review quarterly with the Head of OT. The signed register is the audit evidence.
- Define a refresh-cadence calendar invitation owned by the OT engineer at each site, signed by the IT Security Manager.

Why it works in a brewery: brewery sites have a known and finite asset population (50 to 200 OT assets each). The dated, signed spreadsheet is what the auditor wants. Central IT collation makes the audit answer multi-site instead of site-by-site.

SIEM forwarding (no tool required): the asset register is a flat-file evidence artifact, not a SIEM feed. Once the SenninRecon layer arrives, the register becomes a live overlay on the manual baseline.

When to bring in a tool: TXOne SenninRecon is the passive-discovery option that runs on a SPAN port at any single brewery and overlays a live, vulnerability-scored asset inventory on the manual register. Zero agents. Zero PLC touches. VSAR scoring ranks vulnerabilities by operational context, not raw CVSS.

TIMING

Walkdown completes a 50 to 200-asset site in a day or two. Centralize at group level. Review quarterly.

NIS2 ARTICLE 21

Asset management and risk analysis are foundational expected measures.

30%

of IR cases were discovered because "something seemed wrong" [13]

NO-PROCUREMENT GOVERNANCE

WAY 09

Make in-plant USB control a maintenance-window procedure with audit evidence.

The brewery risk: maintenance windows stop the line and allow contractors to plug devices directly into HMIs. Way 4's gate control catches media entering the facility. It does not catch a laptop already badged in and plugged into a cabinet at 02:00 on a Saturday.

Do this (no procurement, IT/OT joint procedure):

- Publish a maintenance-window media policy as a joint IT/OT procedure. Specify allowed media classes by Purdue level. Owner: IT Security Manager. Co-signer: Head of Maintenance.
- Add a signed media line item to the maintenance work order: device serial, owner, target system, time of insertion, time of removal, two signatures. The work-order system is the chain-of-custody record.
- Define the escort rule: contractors do not plug into a cabinet without a brewery employee present.
- Brief the contractor pool annually. Add the policy to the supplier onboarding contract.

Why it works in a brewery: the maintenance work-order system already records who entered the cabinet; layering a media line item is administrative work, not capital. The signed log is what NIS2 Article 23's incident-evidence obligation expects.

When to bring in a tool: TXOne Stellar USB device control: only serial-validated media can mount; unknown devices blocked at the OS level. TXOne Portable Inspector in every maintenance kit: technicians scan media on the line before insertion. Pro Edition adds AES-256 hardware encryption for tamper-evident chain of custody. Every USB mount attempt and every Portable Inspector scan forwards to the IT SIEM.

TIMING

Policy in place this week. Stellar USB control on the top-five HMIs plus one Portable Inspector per kit is a same-week add.

NIS2 ARTICLES 21 & 23

Supply-chain security (Art. 21) and incident-evidence obligations (Art. 23). IEC 62443 Zone 2 and Zone 1 endpoint controls.

81.9% / 10.5%

of USB-based OT suspicious activity is file transfers; 10.5% is malicious USB devices [14]

NO-PROCUREMENT GOVERNANCE

WAY 10

Make IT/OT governance a recurring meeting before you make it a console.

The brewery risk: NIS2 Article 23 requires 24-hour early warning, 72-hour notification, and 1-month final report for significant incidents. Group CISOs at brewery groups with 3 to 12 sites are aggregating evidence across multiple consoles on a spreadsheet during the incident, which is when it is most expensive to aggregate.

Do this (no procurement, governance only):

- Stand up a weekly 30-minute IT/OT joint review with named site attendees. Standing agenda: open incidents, planned maintenance windows, security pending actions, NIS2 evidence-folder status.
- Maintain a shared incident log accessible to both teams. One row per event, regardless of severity.
- Publish an IT/OT decision-rights map: who decides on a network-segmentation rule change, who decides on an endpoint-policy change, who can authorize an emergency stop. Keep it short, post it on the wall.
- Run a quarterly cross-site evidence dry-run.

Why it works in a brewery: the IT/OT handoff at most brewery groups is negotiated incident-by-incident on a video call rather than designed in advance. A weekly cadence converts the handoff from a crisis into a rhythm.

When to bring in a tool: TXOne Sennin is the platform layer once the cadence is in place: one console, role-based access for IT and OT leadership, IT-proposes/OT-approves workflow built in, VSAR ranks vulnerabilities by operational context. Sennin is not a SIEM replacement; it is the OT-specific correlation layer that makes OT events legible to the IT security program. SenninOne forwards correlated multi-sensor incidents with asset details, VSAR scores, rich context to any SIEM platform.

TIMING

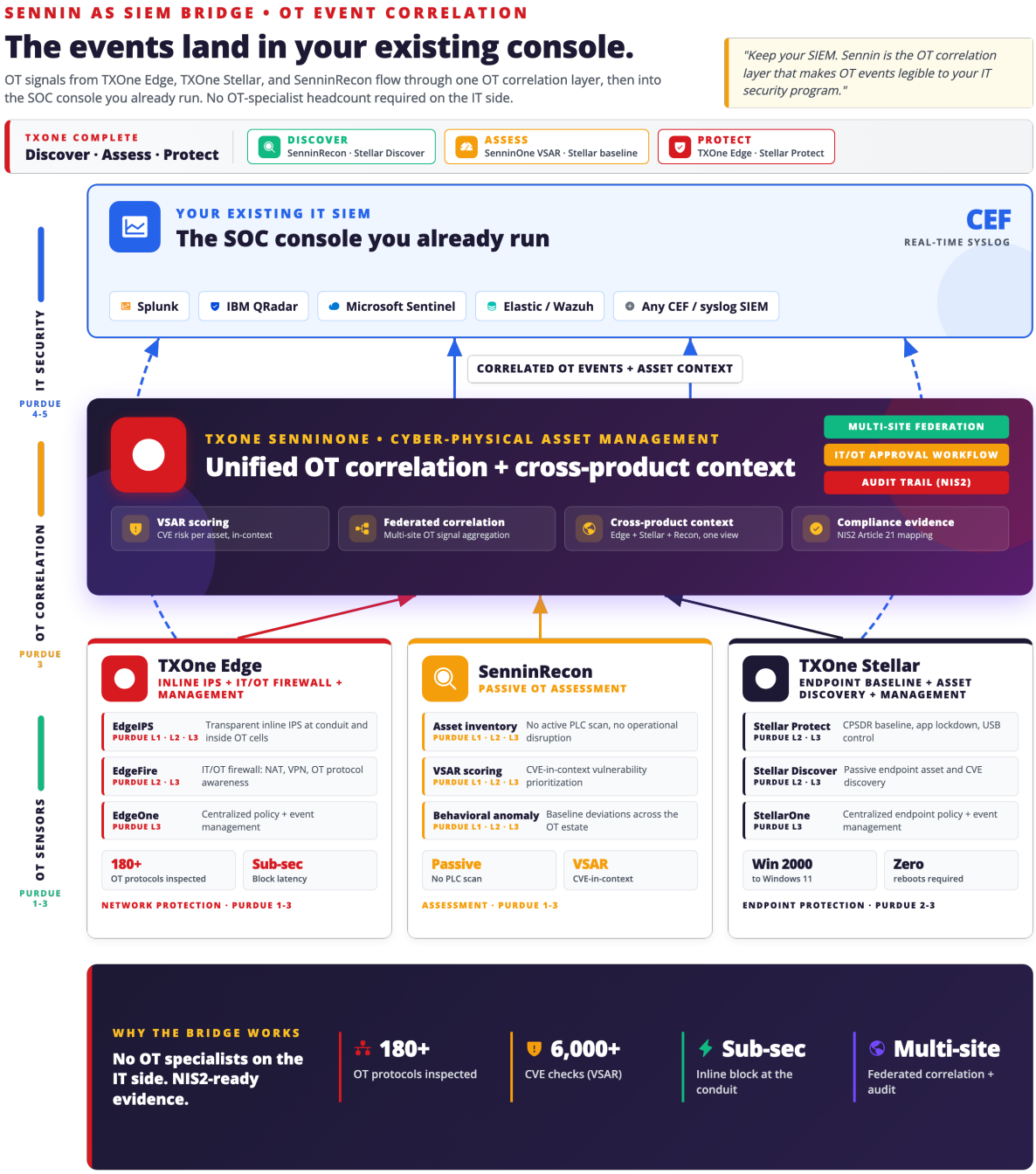
Cadence in place this week. Sennin sequences after the Edge and Stellar foundation.

NIS2 ARTICLE 23

Incident reporting and governance. The cadence is governance evidence on its own.

67%

of organizations struggle with unified IT and OT visibility [1]



Sennin as the OT correlation layer: OT sensors feed SenninOne, SenninOne forwards correlated events to your existing IT SIEM.

NO-PROCUREMENT GOVERNANCE

WAY 11

Rehearse the NIS2 incident with production, OT, IT, quality, and legal before the attacker does.

The brewery risk: 88% of tabletop exercises reveal degraded detection capability under stress [13]. Just **14%** of OT organizations felt fully prepared for emerging threats [2]. The IT Security Leader's career-defining incident will not be a practice run.

Do this (no procurement, governance and rehearsal):

- Run a quarterly NIS2 incident tabletop. Owner: IT Security Manager. Co-signer: Legal counsel. Readiness sign-off: Business Leader.
- Include production, OT, IT security, SOC, quality, and legal. The scenario assumes Article 23's 24-hour and 72-hour windows are already running; the team produces first-pass drafts of each report form.
- Measure time-to-contain, time-to-notify, time-to-restore.
- Document RACI snapshot, runbook version, and the gap list. The documents themselves are NIS2 Article 23 readiness evidence.
- Re-run quarterly. Promote the gaps from the previous run into action items in the IT/OT cadence (Way 10).

Why it works in a brewery: the IT/OT handoff and the regulator-facing handoff are the same thing under stress. Sites with documented compliance had approximately 50% fewer financial losses and safety impacts than peers [2] — the rehearsal is a financial control, not just a security one.

When to bring in a tool: the technical accelerator the rehearsal will surface is the SenninOne-to-SIEM evidence pipeline. If the SOC cannot pull the incident timeline in 30 minutes during the tabletop, that is the priority fix; TXOne Sennin's correlated, MITRE-mapped event stream into Splunk/QRadar/Sentinel is the natural answer.

TIMING

Schedule within 30 days. Re-run quarterly.

NIS2 ARTICLES 21 & 23

Incident handling (Art. 21) and reporting (Art. 23). IEC 62443 response-and-recovery requirements.

88%

of tabletop exercises reveal degraded detection capability under stress [13]

NIS2 MAPPING • IT SECURITY LEADER LENS

NIS2 Article 21 & 23: measure → product → evidence

Edge · Stellar · Element · Sennin

ARTICLE 21 Technical & organizational measures — *Required to prevent and minimize incidents*

NIS2 ARTICLE 21 MEASURE	TXONE PRODUCT	EVIDENCE ARTIFACT (SIEM-READY)
Network segmentation	Edge	Policy changes plus blocked-traffic events to SIEM
Endpoint hardening	Stellar ICS	Baseline deviations, app lockdown events
Supply-chain security	Element + Safe Port	Scan pass/fail per badge ID, chain-of-custody
Asset management	SenninRecon	Machine-generated, audit-dated inventory plus VSAR
Vulnerability management	Edge (virtual patch)	Blocked exploits with CVE mapping
Business continuity	Edge (HW bypass)	Bypass-state and failure events as critical
Incident handling	SenninOne	MITRE ATT&CK for ICS correlated events
Crypto / access control	PI Pro (AES-256)	Encrypted media audit trail

ARTICLE 23 Incident reporting windows — *Significant incidents, to competent authority*

WINDOW	REPORT TYPE	EVIDENCE FROM TXONE STACK	PRODUCT
24 hours	Early warning	Initial alert with asset context and MITRE technique	SenninOne
72 hours	Incident notification	Correlated evidence timeline, blocked-vs-executed distinction	SenninOne + Edge
1 month	Final report	Root cause, affected assets, remediation, compliance artifacts	Sennin (full stack)

NIS2 Article 21 + 23 mapped to evidence artifacts.

How Carlsberg executed this

Carlsberg Group (IT Security Leader lens)

Context. Carlsberg Group, originating in Denmark, a global brewing company. OT security is treated as a distinct discipline, with a Director of Brewery OT Security accountable to the group.

Challenge. The IT security program needed to extend coverage to legacy endpoints (Windows XP HMIs on packaging lines and similar) where the enterprise EPP fell short. Replacing the lines costs millions of euros per facility, infeasible at multi-site scale, and any new agent had to avoid imposing operational risk on the production line.

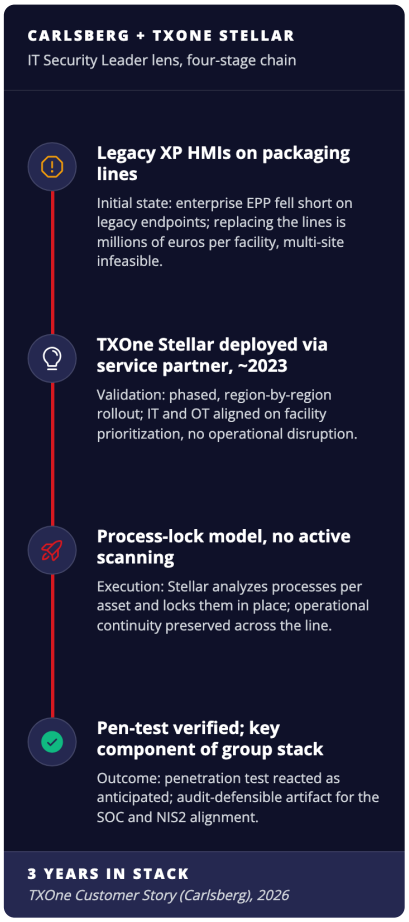
Response. TXOne Stellar deployed via a service partner approximately three years ago, phased region by region. Stellar analyzes the processes running on each asset and locks them in place. No active scanning. No agent-driven instability. The IT/OT trust contract is enforced through the service partner relationship.

Result. A penetration test at one brewery confirmed the technology reacted as anticipated. Stellar is now a key component of Carlsberg's group technology stack and underwrites NIS2 alignment for the legacy endpoint estate [4].

> **"TXOne Networks gives me confidence that it won't disrupt my operations."**
> **Chris Thompson, Director of Brewery OT Security, Carlsberg Group** [4]

3 years

TXOne Stellar in Carlsberg's group technology stack, pen-test verified, operational continuity preserved [4]



Carlsberg: Stellar locks the process.

Your 30/60/90 as an IT Security Leader

Next 30 days (no-procurement governance moves). Publish the contractor media policy and the chain-of-custody record (Way 4); add to the supplier onboarding contract. Coordinate the per-site OT asset walkdown and centralize the dated, signed asset register (Way 5). Publish the maintenance-window media policy and the signed work-order line item (Way 9). Stand up the weekly IT/OT joint review and publish the decision-rights map (Way 10). Schedule the first quarterly NIS2 incident tabletop (Way 11).

Next 60 days (technology accelerators). Schedule a SenninRecon assessment on one brewery (SPAN port, no production touch) and use the output as the live overlay on the manual asset register from Way 5. Deploy Stellar Discover on HMIs where compatibility validation is wanted; feed the assessment into the board presentation. Install a Safe Port kiosk at one facility entry; convert the signed paper log from Way 4 into a structured event stream into the SIEM. Run a 60-minute Edge Proof of Value on the highest-risk IT/OT conduit; the IT security analyst leads the POV, validates inline blocking on live traffic, and tunes the initial AI-learned ruleset before expansion.

Next 90 days (foundation). Extend Edge plus Stellar across the group; plan Stellar ICS upgrade from Discover on endpoints that showed active malware or critical vulnerabilities. Establish the IT/OT approval workflow in Sennin so the first production policy deployment is governed by the cadence (Way 10). Produce the first quarterly NIS2 evidence package from Sennin; re-run the Article 23 tabletop. Feed cross-product events into the IT SIEM with MITRE ATT&CK for ICS mapping.

Take the Next Step

- **Primary:** Schedule a SenninRecon assessment on one brewery and get the NIS2 evidence pipeline flowing in 30 days.
- **Secondary:** Read Guide 1, "11 Practical Tips for Breweries to Avoid Production Downtime Due to OT Risks," and share with your OT counterpart so both sides of the handoff are reading the same map.
- **Tertiary:** Read Guide 3, "11 Steps to Stable OT Systems Without Interrupting Production," and share with your IT operations and security engineering teams so the no-procurement governance work starts this week.

Ready to make "is the production environment actually protected" an answerable question?

Contact your TXOne Networks partner or visit txone.com to schedule a SenninRecon assessment.

Schedule a SenninRecon Assessment

When the no-procurement governance moves are in place, when Sennin sits on top of them as the reporting infrastructure, when the IT/OT handoff is a governance workflow and not a Teams call at 2 AM, and when every endpoint coverage exception is closed rather than documented, the board presentation changes. "Is the production environment actually protected?" becomes a question with a sourced, auditable, multi-site answer.

Sources

1 TXOne Networks / Omdia OT Security Survey, 2023.

2 SANS State of ICS/OT Security Survey, 2025.

3 Claroty Team82 Threat Intelligence Report, 2026, p. 5.

4 TXOne Customer Story (Carlsberg), 2025.

5 Splunk SURGe, 2022.

6 TXOne field intelligence, 2026.

7 CrowdStrike Threat Hunting Report, 2025.

8 TXOne Internal Data, 2026.

9 TXOne Product Documentation, 2026.

10 TXOne Legacy OT Cybersecurity Report, 2026.

11 Gartner CPS Security Requires Specialized Vulnerability and Patch Management, 2025, citing Claroty.

12 Honeywell 2025 Cyber Threat Report.

13 Dragos 9th Annual OT/ICS Cybersecurity Year in Review, 2026.

14 Nozomi Networks 1H 2025 OT/IoT Security Report, p. 22.

15 Gartner Critical Capabilities for CPS Protection Platforms, 2026.

About TXOne Networks

TXOne Networks specializes in OT-native cybersecurity for critical infrastructure and industrial control systems. Our solutions are deployed across energy, manufacturing, water, food and beverage, and transportation sectors globally.

As the operations-first OT security partner, TXOne helps industrial organizations protect critical operations, securely extend asset life, and build security programs without operational disruption. This guide is part of the European Brewery OT Security series.

Visit txone.com

txOne networks