TXONE NETWORKS

11 Practical Tips for Breweries to Avoid Production Downtime Due to OT Risks

Practical Guide for Brewery OT Leaders

Executive Summary

European breweries face a paradox. The equipment that makes beer is the least tolerant of downtime and the least tolerant of security tools that cause downtime. Every fermentation batch interrupted, every bottling line halted, every CIP cycle broken has a measurable cost. NIS2 is in force. Attackers increasingly target food and beverage operations. IT keeps asking for security controls that break the line the first time they are tried.

This guide is for the brewery OT Leader who is tired of choosing between two kinds of outage. Eleven practical tips, operations-first. Five (Tips 4, 5, 9, 10, 11) can be put in place this week with no capital spend and no technology. The remaining six describe a prevalent industry problem and the range of approaches the industry uses to solve it; in each, TXOne is named as one OT-native option among the broader options. Every tip cites its proof and its NIS2 tie-in.

> Carlsberg Group, the Denmark-originating global brewing company with 140+ brands, deployed TXOne Stellar three years ago to safeguard legacy endpoints where enterprise endpoint protection fell short. A penetration test at one of their breweries verified the result: "TXOne Networks reacted as we anticipated. The test was an undeniable success." That outcome, operational continuity verified, NIS2-aligned, with a tiered rollout across the group, is the bar this guide sets [1].

This guide sits in a set of three. Guide 2 covers the same eleven risks from the IT Manager perspective (NIS2, architecture, IT/OT handoff). Guide 3 is the same-week action checklist for teams that need to do something without waiting for a capital cycle.

Why this guide, why now

Picture a Saturday morning, 02:14, during a scheduled CIP maintenance window on your packaging line. A contractor plugs a service laptop into the line-side engineering workstation. The laptop carries an unscanned USB drive. By 02:18, ransomware has encrypted the engineering workstation. By 08:00 the morning shift arrives to a cold line and an incident report that NIS2 auditors will read.

The attack took four minutes. The response took most of the night.

Five anchor facts hold this guide together. Each tip below maps back to one or more of them; the citations are verbatim, dated, and audit-defensible.

The 11 Tips

11 PRACTICAL TIPS • EUROPEAN BREWERIES

Stop production downtime from OT cyber risk

OT LEADER LENS • 5 quick wins (no procurement) • 6 industry moves

Quick win (no procurement)
Industry move (TXOne is one option)

1 INDUSTRY MOVE

Segment by Purdue zone

Enforce L3/L2/L1 separation so an IT compromise cannot reach the brewhouse PLC unchallenged.

2 INDUSTRY MOVE

Hardware bypass first

Inline IPS with fail-safe relay keeps packets flowing even if the appliance reboots or fails.

3 INDUSTRY MOVE

Protect HMIs without reboot

Endpoint baseline lock for Windows HMIs that have not been patched in years and cannot be rebooted.

4 NO SPEND

Contractor media policy at reception

Every external USB scanned and signed-off at the gate. No exceptions, even for the OEM engineer.

5 NO SPEND

Walk the brewery, write the register

Two-hour walkdown produces an asset register the IT team has never had. Free, immediate, audit-ready.

6 INDUSTRY MOVE

Lock the brewhouse PC baseline

Application allowlisting on brewhouse and packaging PCs blocks anything not on the approved list.

7 INDUSTRY MOVE

Close the 4-min window inline

Sub-second inline blocking eliminates the 35-45 minute detect-to-respond gap ransomware exploits.

8 INDUSTRY MOVE

Virtual-patch the unpatchable PLC

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

9 NO SPEND

Maintenance-window media policy

Approved USBs only during scheduled windows. Logged, reviewed, retired after use. Zero ad-hoc media.

10 NO SPEND

Weekly IT/OT review + decision-rights

30-minute standing meeting with named owners. Closes the IT/OT handoff gap that 67% of orgs cite.

11 NO SPEND

Rehearse the 02:14 shutdown

Tabletop the night-shift ransomware scenario. Who decides to halt the line? Who calls the brewer?

THE SPLIT

5 NO-SPEND + **6** INDUSTRY

Five tips you can run this week without procurement. Six tips where TXOne is one OT-native option among broader approaches.

Every tip cites its proof and its NIS2 tie-in. See Section 2 for the full text.

GUIDE 1 OF 3 • EU BREWERY 2026

INDUSTRY MOVE · TXONE IS ONE OPTION

TIP 01

Segment your brewery network by Purdue zone before an IT-side compromise reaches the brewhouse.

The downtime risk: a flat, bridge-able network lets an IT-side compromise ride into the brewhouse PLC segment in minutes. Fewer than 10% of OT networks have any monitoring deployed [7]; a credential leak on the IT side rides onto the brewhouse network before anyone sees it.

What the industry typically does: three approaches. VLAN-only separation (does not enforce; lateral movement is well documented). IT-style next-generation firewalls at the IT/OT boundary (see Modbus and Profinet as generic TCP; require IP addressing and PLC-side cooperation). OT-native inline appliances installed transparently between brewhouse, utilities, and packaging segments (inspect at the command level, designed to behave correctly when the line is upset). The architectural test: can the device install transparently with zero IP and understand what is on the wire?

What works in a brewery specifically: fermentation and CIP controllers exchange OPC-UA, Profinet, Modbus, and vendor-specific protocols. The conduit most worth protecting (brewhouse to packaging) is also the one where IT firewall reconfigurations create the most production risk because it is in the active production path.

The TXOne option: TXOne Edge meets the test for European breweries. EdgeIPS for single-cell deployments. EdgeFire for OT-native NGFW + IPS + VPN at remote sites. Both deploy transparently with zero IP. AI-powered auto-rule learning generates the initial policy in days. Deep packet inspection across 180+ industrial protocols at the command level — a Modbus function-code abuse blocked without interrupting the legitimate heat-exchange cycle on your lauter tun.

TIMING

Foundational move. Plan a 60-minute Proof of Value on one cell first; full rollout is staged, not same-week.

NIS2 ARTICLE 21

Network segmentation is an expected technical measure.

4.0

TXOne Network Segmentation score (out of 5.0)

[8]

The Purdue model is how the brewery is already drawn on the wall: Level 0 sensors and actuators, Level 1 controllers, Level 2 HMIs, Level 3 site operations, Level 3.5 DMZ, Level 4 enterprise. Protecting the conduits between those layers is what stops IT-side compromise from reaching the brewhouse.

Defense-in-depth by Purdue zone.

INDUSTRY MOVE · TXONE IS ONE OPTION

TIP 02

Make sure the device protecting the line cannot stop the line by failing.

The downtime risk: the second-worst thing after a cyber incident on your bottling line is a security-device failure that stops the line anyway. Both events end with trucks queuing at the dock.

What the industry typically does: most security devices placed in OT today were designed for IT data centers. Climate-controlled rack rails. Cloud connectivity expected. Power-blip reboots. When they fail in line, traffic stops. The OT-native alternative adds physical hardware bypass: a relay closes if the device powers off or self-tests fail, and line traffic continues uninterrupted. The procurement choice is between accepting the security device as a new single point of failure or specifying relay-level fail-safe behavior from the start.

What works in a brewery specifically: you already protect the brewery from physical failure with backup pumps, redundant valves, and interlocked safeties. The same engineering philosophy applies to a security device sitting in the bottling-line traffic path. Hardware bypass is what protects the brewery from the security system itself, not just from the attacker.

The TXOne option: TXOne Edge appliances ship with fail-safe hardware bypass at every brewery-floor cell. The LE 102 (2-port compact) suits a small cellar drop; the Pro 2016F (16-port fiber) suits a central packaging line. Industrial operating envelope: minus 40 to 75 C, fanless, DIN-rail next to the PLC cabinet. EdgeFire 1012 and 1014 carry 700,000 hours MTBF.

TIMING

Same-week at a first site; staged rollout across multi-site brewery groups.

NIS2 ARTICLE 21

Business continuity is a named pillar.

3,600+

global TXOne deployments with zero unplanned downtime [9]

INDUSTRY MOVE · TXONE IS ONE OPTION

TIP 03

Protect HMIs and engineering workstations without forcing a reboot during a batch.

The downtime risk: a forced reboot of an HMI during fermentation risks a batch. A refused endpoint agent leaves the HMI exposed to ransomware, wipers, and living-off-the-land techniques.

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

What works in a brewery specifically: fermentation and filtration HMIs often run Windows 7, Windows XP, or Server 2008. The thick clients on top (WinCC, iFIX, Ignition) are the actual production interface. Any agent that destabilises the thick client costs you the next shift.

The TXOne option: TXOne Stellar ICS deploys on every HMI, engineering workstation, and brewhouse PC that can accept the full agent. Single policy from Windows 2000 SP4 through Windows Server 2025 and Windows 11. Automated per-device baseline. **70,000+ OT application recognition repository** [10] knows what WinCC, iFIX, and Ignition are supposed to do. Stellar Kiosk is the lite variant for very old XP or Win 2000 cells. Stellar Discover is a 1-minute user-space install for compatibility validation that upgrades remotely later.

TIMING

Same-week. Stellar ICS deploys without reboot; Stellar Discover is a 1-minute install when compatibility validation is wanted first.

NIS2 ARTICLE 21

Endpoint hardening expectation.

100%

of surveyed organizations operate legacy Windows in their OT environment [4]

QUICK WIN · NO CAPITAL SPEND

TIP 04

Put a contractor media policy on the wall at reception this week.

The downtime risk: 25% of top OT security incidents were triggered by USB plug-and-play events [14]. Breweries depend on maintenance contractors who arrive with their own programming laptops and firmware media. The gate is where a malicious file is cheapest to stop.

Do this (no capital spend, no technology required):

- Add a written contractor media policy to the existing safety and insurance sign-in flow at reception. Include vendor laptops, USB drives, SD cards, and external hard drives.
- Require contractors to declare the media they will plug in and the systems they intend to plug it into, before they are badged in.
- Maintain a paper or shared-spreadsheet media log: who, what device serial, what time, what cabinet. This is internal accountability and audit evidence at the same time.
- Train reception and shift supervisors on the policy. Add a two-line item to the daily handover.

Why it works in a brewery: a contractor sign-in desk already exists for safety and insurance reasons. Layering a media declaration onto an existing process is a same-week move. The policy alone changes contractor behavior: knowing that media is declared and may be inspected is a deterrent against the casual "I'll just use my own stick" pattern that creates most incidents.

When to bring in a tool: the policy plus log is the floor. The next layer is a media kiosk that scans every device at the entry point. **The TXOne option:** TXOne Safe Port is the OT-native kiosk: 7,200 files per minute, LED pass/fail indicator, glove-compatible touchscreen, run by reception as part of the existing sign-in flow.

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.

1,826

distinct threats detected targeting OT through removable media [14]

QUICK WIN · NO CAPITAL SPEND

TIP 05

Walk the brewery and write down what is on the network.

The downtime risk: NIS2 auditors expect an accurate asset inventory. Manual inventories age the moment they are finished, and "we cannot prove what is on our network" invites an audit scope that grows during the audit itself.

Do this (no capital spend, no technology required):

- Walk the brewhouse, cellar, packaging line, utilities, and warehouse with the OT engineer. Record nameplate data on every PLC, HMI, switch, and engineering workstation: vendor, model, firmware version, location, owner.
- Capture in a shared spreadsheet with date stamp. Label every row with Purdue level (1, 2, 3) and primary process.
- Add a "what does this asset talk to" column so the inventory carries the basic communication picture.
- Schedule a quarterly nameplate refresh, owned by the OT engineer, signed by the Head of OT.

Why it works in a brewery: a brewery has a known and finite asset population. Most European brewery sites operate 50 to 200 OT assets per site, walkable in a day or two. The dated, signed spreadsheet is what the auditor wants to see; the auditor wants evidence the asset register exists and is maintained. The walkdown surfaces shadow assets and forces the question "who owns this device" while the OT engineer is in front of it.

When to bring in a tool: the manual inventory ages between refreshes. **The TXOne option:** SenninRecon is the OT-native passive-discovery option (SPAN-port deployment, no agents, no inline footprint, VSAR scoring that ranks vulnerabilities by operational context); Stellar Discover layers in for endpoint-level software inventory and active malware visibility on reachable endpoints.

TIMING

Same-week. Two-person walkdown completes a 50 to 200-asset site in a day or two.

NIS2 ARTICLE 21

Asset management is a foundational expected measure.

30%

of IR cases were discovered because "something seemed wrong"

7

INDUSTRY MOVE · TXONE IS ONE OPTION

TIP 06

Lock the brewhouse PC baseline so fileless malware cannot execute.

The downtime risk: 81% of interactive intrusions are malware-free, relying on living-off-the-land techniques [11]. 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 to fileless threats on a Windows endpoint. 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 (mailbox access, browser activity, OAuth flows) 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.

What works in a brewery specifically: a brewhouse PC runs a known, finite set of applications: WinCC or iFIX or Ignition, a few logging tools, a few vendor utilities. Anything outside that set is, by definition, not part of beer making. The architectural test is whether the lockdown can baseline itself per device (no manual allow-list) and whether it can run fully on the legacy OS the brewhouse PC actually has.

The TXOne option: TXOne Stellar ICS includes automated per-device baseline generation and application lockdown. The baseline generates without manual allow-list authoring. Anything outside the baseline cannot execute, including novel fileless and script-based attacks. CPSDR (the TXOne behavioral-anomaly engine) compares live behavior against the learned baseline; deviations are flagged and, where policy permits, blocked. Stellar Discover sensors can run alongside on lower-criticality endpoints to feed telemetry into SenninOne's VSAR scoring.

TIMING

Same-week on select high-value endpoints; full rollout follows Tip 3.

NIS2 ARTICLE 21

Endpoint hardening and integrity controls expectation.

81%

of interactive intrusions are malware-free [11]

INDUSTRY MOVE · TXONE IS ONE OPTION

TIP 07

Close the 4-minute window with inline prevention, not 35-minute coordination.

The downtime risk: LockBit-class ransomware encrypts in approximately 4 minutes [5]. Detection-to-enforcement coordination takes 35 to 45 minutes. By the time your SOC has coordinated with the firewall team and pulled the brewery runbook, the filling line is already encrypted.

What the industry typically does: the standard architecture in detection-led OT security is "see it and route it." A passive sensor on a SPAN port 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 alternative is inline enforcement at the conduit itself: the device that sees the traffic also blocks it, in milliseconds, without leaving the traffic path. Detection tools on their own are fire alarms; without an inline suppression layer, the alarm tells you the building is burning but does not stop the fire.

What works in a brewery specifically: 82% of observed attacks abuse exposed VNC clients on internet-facing CPS assets [12]. The brewery does not have minutes to spare and does not have an OT-trained SOC at 02:14 on a Saturday. The architectural test is whether enforcement is a function of the same device that sees the traffic, and whether the device fails safe if it itself fails.

The TXOne option: TXOne Edge sits inline at the brewhouse/packaging and brewhouse/utilities boundaries with automated blocking enabled and sub-second enforcement at wire speed. Connecting Edge into SenninOne keeps detection-to-enforcement on a single product path rather than a multi-vendor handshake. If you already run a visibility platform, build on it: keep the investment for visibility, add Edge as the inline enforcement layer those platforms cannot deliver.

TIMING

Plan an Edge POV. Foundational, with the fastest payback once the first cell is covered.

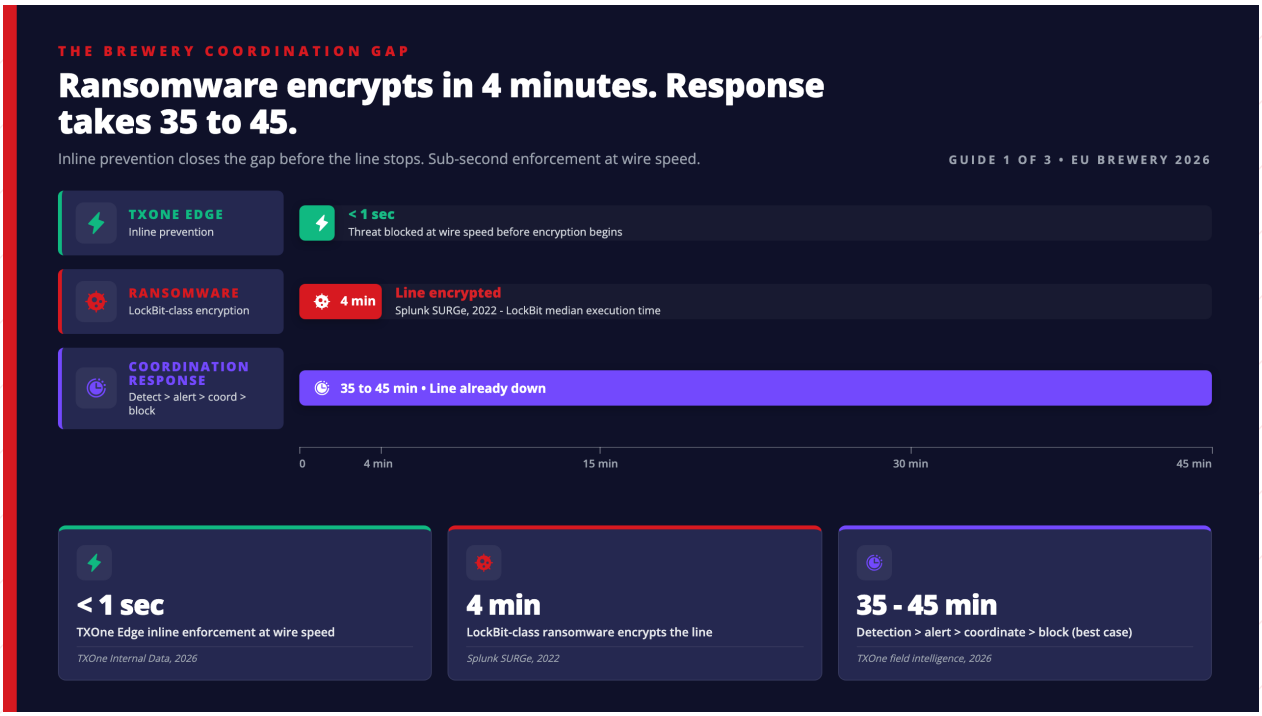
NIS2 ARTICLE 21

Incident handling and business continuity: prevention inside the 4-minute window.

82%

of attacks against internet-facing CPS assets abuse exposed VNC clients [12]

The gap between the 4-minute ransomware clock and the 35-to-45-minute human response is where most brewery incidents become production events. Inline prevention collapses that gap.



INDUSTRY MOVE · TXONE IS ONE OPTION

TIP 08

Virtual-patch the vulnerable controller you cannot take offline.

The downtime risk: 26% of CISA ICS vulnerability advisories released over the past five years offered no patch, and 18% had no patch and no documented mitigation [13]. Where patches exist, the asset often cannot be taken offline during peak season. The vulnerability and the operational constraint coexist and the attacker wins.

What the industry typically does: three options for an asset that cannot be patched in-window. Accept the risk and document the exception (the most common option, and the one the auditor scopes against). Replace the asset (capital cycle, often years away). Apply a compensating control. The most operationally-honest compensating control for an unpatchable inline-critical controller is virtual patching at the network layer: exploit traffic is blocked inline by a device upstream of the controller, the controller itself is never touched, and the vulnerability moves from "open" to "compensating-control-active" in the register.

What works in a brewery specifically: your bottling-line PLC runs 24 hours a day during peak season. Planned shutdown is not an option. The auditor wants to see either the patch or the documented compensating control. Virtual patching satisfies both: the controller is patched-in-place from the attacker's perspective without anyone touching firmware, and the rule itself is the audit evidence.

The TXOne option: TXOne Edge delivers virtual patching at the network layer with rule-to-CVE mapping for documentation. Apply at the conduit upstream of the unpatchable controller. Extend asset life to the next planned shutdown — typically October for most European breweries. Revisit at every planned maintenance window: either apply the physical patch and retire the virtual one, or retain it.

TIMING

Same-week for known-exposed protocols; revisit at every planned maintenance window.

NIS2 ARTICLE 21

Vulnerability management. Virtual patching is a valid compensating control.

26% / 18%

of CISA ICS advisories had no patch / no patch and no mitigation [13]

QUICK WIN · NO CAPITAL SPEND

TIP 09

Write the maintenance-window media policy this week, before the next contractor visit.

The downtime risk: Tip 4 catches what comes through the gate. It does not catch what a contractor already badged in tries to plug directly into an HMI, engineering workstation, or brewhouse PC during a live maintenance window.

Do this (no capital spend, no technology required):

- Write a maintenance-window media policy that names every category of media (USB, SD card, external drive, programming dongle, vendor laptop) and the rule for each.
- Add a signed media line item to every maintenance work order: device serial, owner, target system, time of insertion, time of removal, signed by the maintenance engineer and the contractor.
- Define an escort rule: contractors do not plug anything into a cabinet without a brewery employee present. The escort signs the log alongside the contractor.
- Brief the maintenance team and the contractor pool. Update the safety induction. Re-brief at every contract renewal.

Why it works in a brewery: Tip 4's gate control and this in-plant control are two different layers. The brewery's existing 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 auditors want and the chain-of-custody record an incident response would later need.

When to bring in a tool: the policy plus signed log plus escort is the floor. **The TXOne option:** Stellar ICS includes USB device control across the full Windows range; pair with TXOne Portable Inspector in every maintenance kit so technicians can scan devices on the line before insertion.

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

Logging (Art. 21) and incident-evidence obligations (Art. 23).

81.9%

of USB-based suspicious activity in OT environments is file transfers [3]

QUICK WIN · NO CAPITAL SPEND

TIP 10

Stand up a weekly IT/OT review before you stand up a console for it.

The downtime risk: multi-site brewery groups manage OT security site by site. When the audit arrives, so does the spreadsheet scramble. When an incident happens at one site, visibility into whether it affects the others depends on who is on shift.

Do this (no capital spend, no technology required):

- Stand up a weekly 30-minute IT/OT joint review with named attendees from each site. Standing agenda: open incidents, planned maintenance windows, vulnerabilities pending action, NIS2 evidence-folder status.
- Maintain a shared incident log accessible to both teams. One row per event, regardless of severity.
- Define a documented 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 single quarterly cross-site evidence review. Every site assembles the audit evidence it would produce if the auditor arrived next week. The first review will surface what is missing.

Why it works in a brewery: the IT/OT handoff at most brewery groups is negotiated incident-by-incident on a Teams call rather than designed in advance. A weekly cadence converts the handoff from a crisis into a rhythm. Auditors reward demonstrated governance cadence as much as they reward tooling.

When to bring in a tool: the weekly cadence and shared log are the floor. **The TXOne option:** TXOne Sennin (SenninOne for unified Edge/Stellar/Element correlation; SenninRecon for assessment) is the platform layer once the cadence is in place: one console, role-based access, IT-proposes/OT-approves workflow, VSAR for prioritization.

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

2

QUICK WIN · NO CAPITAL SPEND

TIP 11

Rehearse the shutdown you never want to have, before the attacker rehearses for you.

The downtime risk: 88% of tabletop exercises revealed degraded detection capability under stress [7]. If the first time your brewery rehearses ransomware on the bottling line is the real thing, the muscle memory is built under maximum pressure and maximum cost.

Do this (no capital spend, no technology required):

- Run a brewery-specific tabletop on your highest-fear attack chain. The standard scenario is ransomware on the bottling line during a Saturday morning shift, entering through a contractor USB during the previous night's CIP maintenance window.
- Include production, maintenance, IT security, OT, SOC, quality, and logistics. The incident will involve all of them.
- Measure time-to-contain and time-to-recover. Compare against the production shift schedule, not against a theoretical response-time benchmark.
- Re-run quarterly. Record what changed.

Why it works in a brewery: the muscle memory of "what do we do at 2:14 AM" is built once, under pressure, with the operations crew, not in a slide deck. The tabletop also surfaces decisions the OT Leader needs to make before the incident: who has authority to stop the line, who has authority to isolate a cell, who has authority to continue operating with a compensating control.

TIMING

Schedule within 30 days. Re-run quarterly.

NIS2 ARTICLE 21

Incident response readiness and business continuity evidence.

88%

of tabletop exercises revealed degraded detection capability under stress [7]

How Carlsberg did it

Carlsberg

Context. Carlsberg Group, originating in Denmark. A global brewing company with 140+ brands. Mission: "secure the brew." Treats OT security as a distinct discipline from IT, with a separate program. Operational deployment work runs through a third-party service partner.

Challenge. Close the legacy endpoint coverage gap where enterprise endpoint protection fell short. Specific example: a Windows XP HMI on a packaging line where replacing the entire line costs millions of euros, financially unfeasible at multi-site scale. Trust the guiding principle: "If an enterprise-grade product is implemented in OT and it fails, trust in that product is immediately lost."

Response. TXOne Stellar deployed via a service partner approximately three years ago. Phased, region-by-region rollout led by top-priority facilities first. Stellar analyses the processes running on each asset and locks them in place; no active scanning, no operational disruption.

Result. A penetration test conducted at one of Carlsberg's breweries confirmed the technology reacted as anticipated. Stellar is now a key component of the group's technology stack, NIS2-aligned, with operational continuity preserved [1].

> **"TXOne Networks gives me confidence that it won't disrupt my operations."**
> **Chris Thompson, Director of Brewery OT Security, Carlsberg Group** [1]

3 yrs

TXOne Stellar in Carlsberg's group technology stack; safeguarding legacy endpoints where enterprise EPP fell short

[1]

Carlsberg: Stellar process-lock, no scanning.

Your 30/60/90 next move

The eleven tips sequence cleanly into three phases. Governance leads, technology accelerates, foundation sustains.

> **A note on the budget conversation.** Industry analyses of unplanned manufacturing downtime in food and beverage operations place the cost of a stopped production line typically in the range of approximately €50,000 to €500,000 per hour, varying by line size, in-process inventory at risk, and downstream supply commitments. A single avoided four-hour incident in peak season usually clears the cost of every technology layer below.

Next 30 days (no-capital quick wins). Put the contractor media policy on the wall (Tip 4). Walk the brewery and write down the asset inventory (Tip 5). Write the maintenance-window media policy and the signed-log line item (Tip 9). Stand up the weekly IT/OT review and the shared incident log (Tip 10). Schedule the first brewery tabletop on the 02:14 scenario (Tip 11). Five tips, zero capital, most done inside a fortnight.

Next 60 days (technology that accelerates the quick wins). 60-minute Proof of Value on TXOne Edge against your live traffic at the highest-risk conduit (begins Tip 1; advances Tip 7). Validate Stellar Discover or ICS on five pilot HMIs (Tip 3). Layer a Safe Port kiosk over the contractor sign-in policy (Tip 4 acceleration). Layer Stellar USB control on the top-five HMIs over the maintenance-window media policy (Tip 9 acceleration). Validate the SenninRecon passive inventory layer over the manual one (Tip 5 acceleration).

Next 90 days (foundation). Stage the rollout of Edge segmentation and hardware bypass across the cells (Tips 1, 2, 7, 8). Plan Sennin as the orchestration layer over the IT/OT cadence (Tip 10 acceleration). Re-run the tabletop (Tip 11) and produce the first audit-ready evidence package.

NIS2 EVIDENCE CHECKLIST • ARTICLES 21 + 23

Governance documentation first. Technology strengthens it.

Governance baseline (no procurement)

Technology accelerator (TXOne is one option)

ARTICLE	MEASURE	GOVERNANCE BASELINE	TECHNOLOGY ACCELERATOR	TIPS
Art. 21	**Network segmentation**	Documented zone-and-conduit architecture	TXOne Edge inline + virtual patching logs	1, 7, 8
Art. 21	**Endpoint hardening**	Documented endpoint program	TXOne Stellar ICS baseline + lockdown records	3, 6
Art. 21	**Supply-chain / contractor access**	Signed contractor media policy + chain-of-custody log	TXOne Safe Port + Portable Inspector audit logs	4, 9
Art. 21	**Asset management**	Dated, signed asset register from walkdown	TXOne SenninRecon inventory + Stellar Discover	5
Art. 21	**Business continuity**	Hardware-bypass attestation in maintenance procedure	TXOne Edge hardware bypass attestation	2
Art. 21	**Incident response readiness**	Quarterly tabletop with brewery operations crew	TXOne SenninOne timeline correlation for AAR evidence	11
Art. 21	**Vulnerability management**	Documented exception register + compensating controls	TXOne Edge virtual patching with rule-to-CVE mapping	8
Art. 23	**Incident reporting + governance**	Weekly IT/OT review minutes + decision-rights map + tabletop AAR	TXOne SenninOne correlation + IT/OT approval workflow	10, 11

Start with the governance column. The auditor wants evidence the program exists.

GUIDE 1 OF 3 • EU BREWERY 2026

Take the Next Step

- **Primary:** Book a 60-minute brewery readiness review. A TXOne OT specialist will walk one cell of your brewery and map the eleven tips against what you have already, what you have partially, and what is missing.
- **Secondary:** Read Guide 2, "11 Proven Ways IT Managers in Breweries Secure Production," and hand it to your CISO or corporate IT security lead.
- **Tertiary:** Read Guide 3, "11 Steps to Stable OT Systems Without Interrupting Production," and pick one no-capital action for this week.

Ready to keep production running while coverage grows?

Contact your TXOne Networks partner or visit txone.com to schedule a brewery readiness review.

Book a Brewery Readiness Review

When the no-capital quick wins are in place and the technology layers are stacked on top of them in the order that fits your operations, the choice between security and production is resolved. Production keeps running. Coverage keeps growing. Safe beer and safe bytes are the same project.

Sources

1 TXOne Customer Story (Carlsberg), 2025.

2 Omdia OT Security Survey, 2023.

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

4 TXOne Legacy OT Cybersecurity Report, 2026.

5 Splunk SURGe, 2022.

6 TXOne field intelligence, 2026.

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

8 Gartner Critical Capabilities for CPS Protection Platforms, 2026.

9 TXOne Internal Data, 2026.

10 TXOne Product Documentation, 2026.

11 CrowdStrike Threat Hunting Report, 2025.

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

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

14 Honeywell 2025 Cyber Threat Report.

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

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