IoT and OT Security

Protection for Internet-of-Things and Operational Technology environments, where availability and safety constraints make conventional security approaches unworkable.

The question it answers

In an operational estate the standard playbook can be actively harmful. Aggressive scanning can stop a process. A patch window may not exist. An agent may void support or fall outside what the platform can run at all.

The question is not which controls are best practice. It is what security looks like when the usual moves are unavailable, and where the remaining leverage actually is.

Constraints first, then controls

Availability and safety are treated as fixed inputs rather than obstacles to negotiate, in the same way residency and classification are on every other engagement.

The work is passive by default. Where an active technique is warranted, it is agreed in advance with the people who own the process, and scheduled around it.

What the work covers

Attack surface and architecture review

How the estate is actually connected, including the routes between corporate IT and the operational network that were never intended to exist and rarely appear on a diagram.

Segmentation

Where boundaries are, where they are assumed to be, and what would actually cross them. Guidance shaped to what the environment can support without interrupting the process.

Monitoring guidance

What can be observed without touching the devices themselves, and which signals are worth collecting given the protocols and platforms in use.

Threat modeling

Modeling against the systems and protocols specific to the environment and the adversaries that target them, rather than against a generic IT threat set.

AT A GLANCE

APPLIES TO
OT and IoT estates, and the IT boundary

FIXED CONSTRAINTS
Availability and safety, never negotiated

DEFAULT POSTURE
Passive. Active techniques only by agreement

OUTPUT
Architecture, segmentation and monitoring guidance

DELIVERY
Principal-level operator, start to finish

WHO THIS IS FOR

- Operators whose security programme was written for IT and does not survive contact with the plant.
- Organizations connecting operational estates to corporate networks or to cloud services.
- Teams that cannot answer what an intrusion in IT would mean for the operational side.
- Estates where a conventional assessment has already been declined as too risky to run.

How an engagement runs

01 Scope and constraints

What the organization needs from the engagement is established alongside what must never be disturbed. Both are agreed in writing before anything begins.

02 Profile the environment

The estate, its technology, its protocols and its threat exposure are profiled in detail. Engagements here are never planned on assumptions.

03 Review and model

Architecture, connectivity and segmentation are reviewed, and threat modeling is performed against the specific systems and protocols in use.

04 Report

Findings are delivered so they are both understood and actionable: technical detail the engineering team can execute against, and an account that translates exposure into operational terms.

05 Enable

Walkthroughs with the teams that run the estate, so the recommendations are clear and implementable within the constraints that produced them.

WHY ALEXSTA

- Senior hands only. The operator whose experience you are buying does the work, rather than reviewing it.
- Recommendations are shaped to what the environment can actually support, not drawn from a catalogue of IT controls.
- Conclusions carry their evidence and a stated confidence level, including what the evidence does not settle.

WHAT WE NEED TO SCOPE IT

- Type of environment and what it produces or controls.
- Approximate device count, vendors and protocols in use.
- How the operational estate connects to corporate IT and the internet.
- Availability and safety constraints, including maintenance windows.

What you receive

Architecture and exposure review

How the estate is connected in practice, where the boundaries actually sit, and which paths present real exposure rather than theoretical exposure.

Segmentation guidance

Recommended boundaries and the sequence to introduce them in, ordered so that each step is achievable without interrupting the process.

Monitoring recommendations

What to observe, how to observe it without touching the devices, and what each signal would actually tell you.

Threat model

The adversaries and techniques relevant to these systems and protocols, with the scenarios that matter most for this estate identified explicitly.

Request an engagement

The first conversation is about constraints, not controls. Tell us what cannot be interrupted and we will tell you what is assessable within that.

contact@alexsta-cybersecurity.com
+41 76 76 44884
alexsta-cybersecurity.com