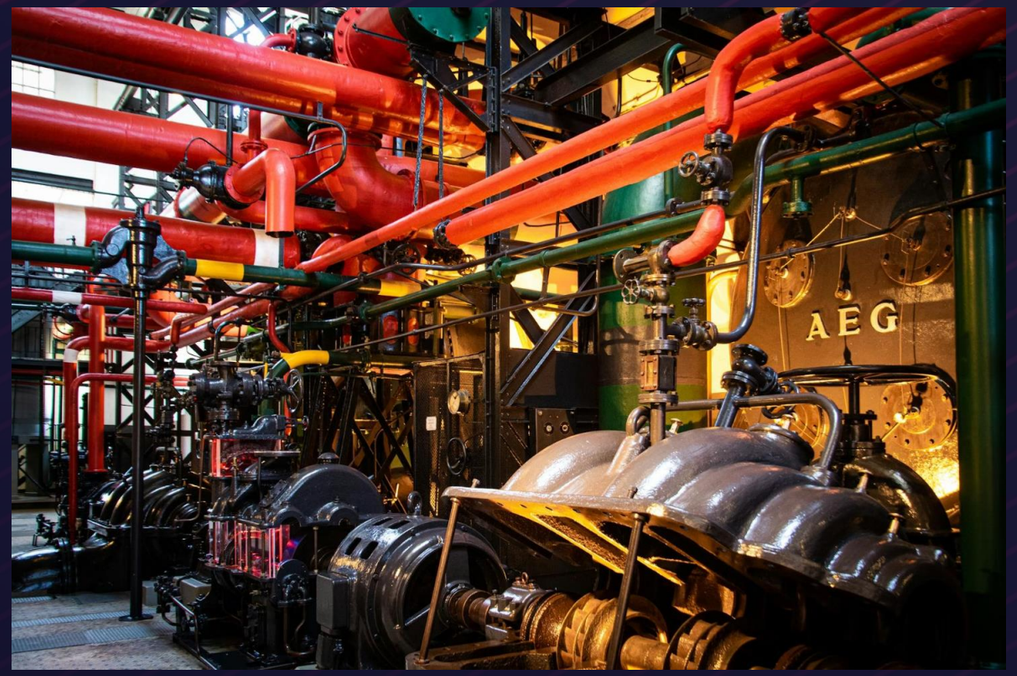
Making Progress in OT Security

Building Defensible Architecture with the SANS Five Critical Controls

Dan Cartmill

Sr. Director Product and Solution Marketing

The Gap Between Framework and Factory Floor



20+ Year Lifecycles

Equipment outlasts frameworks

Zero Downtime Tolerance

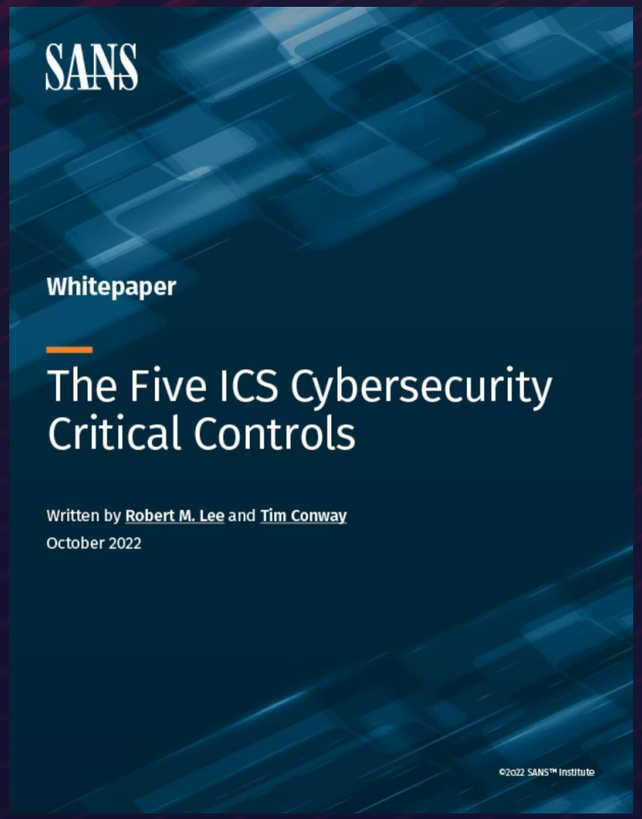
Operations cannot pause

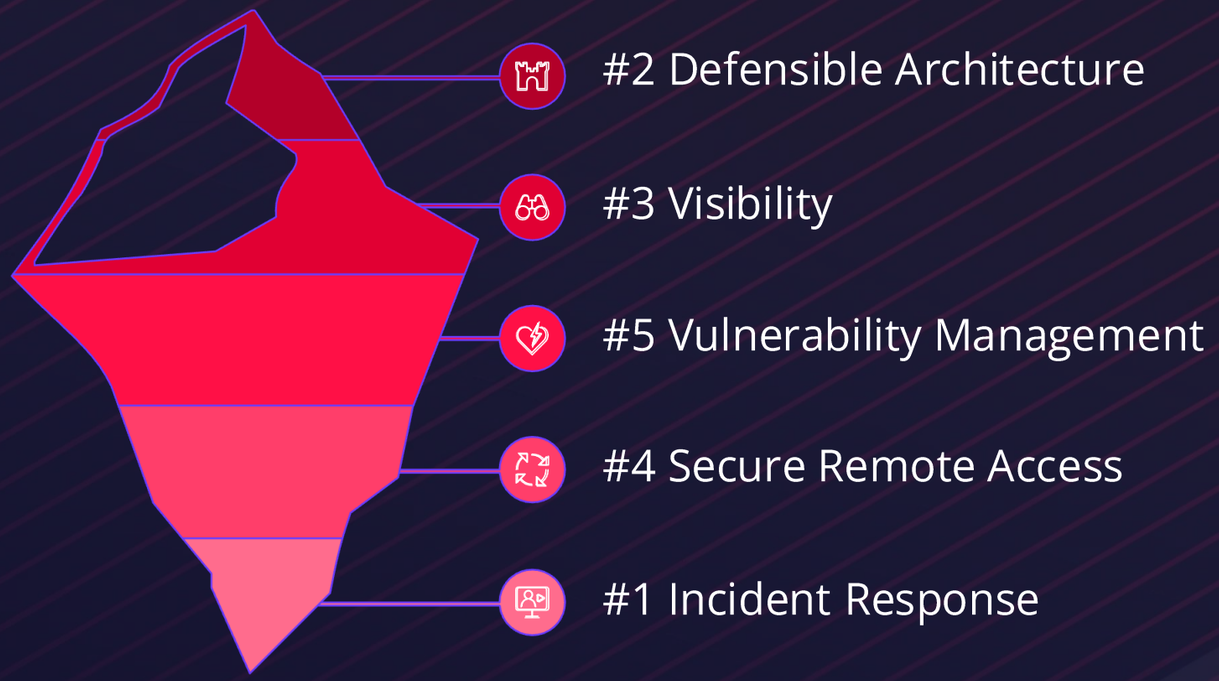
No "Rip and Replace"

Legacy constraints are real

The question is not what is ideal, but what actually moves the needle.

A Defensible Architecture Is Where Value Is Realized





Scenarios drive requirements. Architecture delivers outcomes.

→

Every other control either feeds the architecture or depends on it.

txOne networks

Outputs Without Action Are Just Reports

Generating Outputs

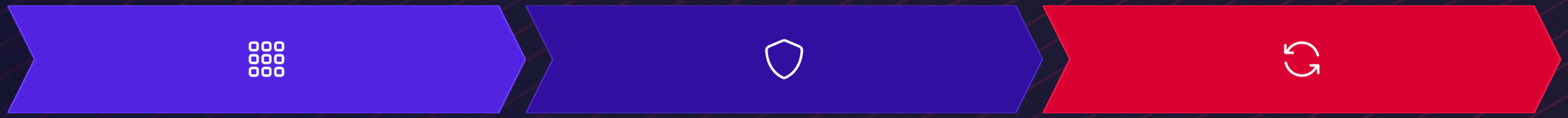
- 2,400 assets discovered
- Anomalous traffic detected
- 347 CVEs identified
- Dashboards updated

Driving Outcomes

- Process-critical assets segmented
- Unauthorized commands blocked
- Vulnerabilities shielded
- Risk reduced, operations protected

Most OT attacks use native functionality, not vulnerability exploitation. - SANS

Defensible Architecture as a Living System



Segment

Micro-segmentation at asset level

Reduce pathways, create choke points

Enforce

Protocol-aware control at command level

Beyond port/protocol filtering

Adapt

Different sites, different approaches

Design models are a guideline, not gospel

"It is the human element that allows a defensible architecture to become a ***defended*** architecture." **- SANS**

Visibility That Drives Architectural Action

Identify Commands

Detect specific commands and patterns.

Feed Enforcement

Supply policies to enforcement engine.

Protocol-aware DPI

Inspect OT protocols and payloads.

Block Unauthorized

Inline drop of malicious commands.

#1

Security Control

Ranked by mature ICS organizations - SANS 2024

1/8

Full Visibility

Organizations achieving ICS Kill Chain visibility - SANS 2025

⚠ Traditional firewalls see ports. OT-native inspection sees commands.

txOne networks

Vulnerability Management That Changes Architecture

Dragos 2025

Key question: "If this vulnerability were patched, could an adversary achieve the same outcome with direct network access?" ***- SANS***

46%

apply compensating controls

51%

default to more monitoring

77%

of ICS vulnerabilities require direct access to the ICS segment

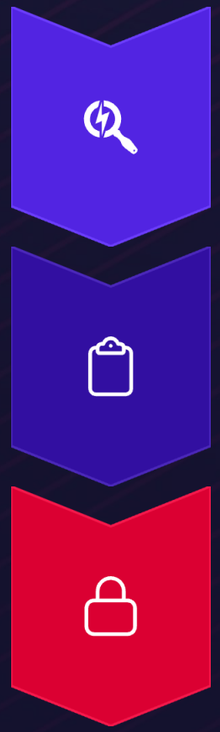
Frost & Sullivan 2024, Dragos 2025

txOne networks

Inside the Architecture, Not Beside It

The Complete Journey From Detection to Prevention

TXOne's Discover, Assess, Protect methodology maps directly to the critical controls:



Discover

Asset identification and network mapping supports Controls #2 and #3

Assess

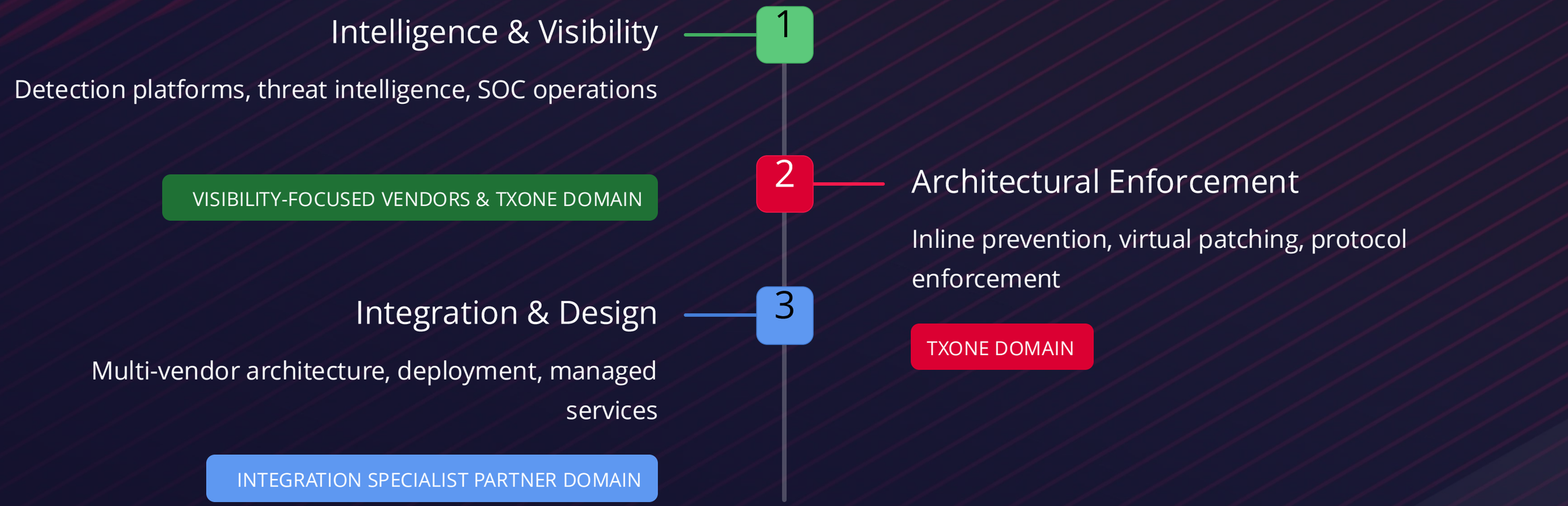
Vulnerability assessment with operational context supports Control #5

Protect

Inline prevention blocks threats in sub-second response time, supporting Controls #2 and #3

txOne networks

OT Security is a Team Sport



Visibility Vendors generate the inputs

TXOne enforces them in the architecture

Integration Partners bring it together

What You're About to See

TXOne Complete: Network. Endpoint. Inspection — Unified.

Network Security

TXOne Edge

Inline prevention, 180+ OT protocols, hardware bypass continuity

Endpoint Protection

TXOne Stellar

Legacy and modern systems, Windows XP through 11,

Security Inspection

TXOne Element

Agentless, air-gapped, constrained environments, supply chain validation

One partner. One platform. Zero unplanned downtime. This is what it looks like to run it.

The Demo Begins Now

Network security enforcement

Live traffic, live blocking

Endpoint protection on legacy systems

No patches, no reboots

Security inspection at the perimeter

Air-gap to enterprise

Discover. Assess. Protect.

Schedule a proof of value for your environment today

txOne networks

Making Progress in OT Security

Building Defensible Architecture with the SANS Five Critical Controls