cabreza

RESILIENCE & DETECTION · January 2026

The Gap Between Detection and Resilience in ICS/OT Security

Why visibility without response capability produces data without outcomes

EXECUTIVE SUMMARY

Organizations detect threats faster than ever, yet 19% of incidents still take over a month to remediate. This whitepaper examines the gap between detection and resilience—why visibility alone doesn't produce outcomes, what the evidence shows about investment priorities, and how to build response capabilities that convert alerts into action.

The Problem

The ICS/OT security industry has made remarkable progress in detection. Organizations now detect threats faster than ever—50% of incidents are identified within 24 hours. Asset inventory adoption has grown from 33% in 2019 to over 52% today. Network monitoring platforms have matured. Threat detection rules update in near-real-time based on intelligence feeds.

Yet remediation timelines remain stubbornly slow. 19% of incidents still take over a month to fully remediate. Nearly half of organizations need a week or more to recover operations. The gap between seeing a problem and solving it has become one of the most significant blind spots in industrial security.

Detection is working. The question is whether detection alone produces the outcomes organizations actually need.

The Evidence: Detection Improves, Recovery Lags

Visibility has improved dramatically:

YEAR	ORGANIZATIONS LACKING OT VISIBILITY
2019	90%
2022	80%
2024	45%

This represents real progress. A decade ago, most industrial organizations operated blind. Today, a majority have deployed asset discovery, network monitoring, or threat detection.

But recovery tells a different story:

METRIC	FINDING
Detection within 24 hours	50%
Containment within 48 hours	55-65%
Remediation takes 2-7 days	22%
Remediation takes >1 month	19%
Recovery takes >1 week	49% (Claroty)

The SANS 2025 report describes this as a "two-speed reality"—detection and containment are faster than ever, but full post-breach restoration remains slow. Organizations can identify threats quickly. Translating that identification into restored operations takes far longer.

Consider what this means operationally: organizations are getting better at knowing they've been compromised. That knowledge isn't producing faster recovery of critical operations.

Why Frameworks Emphasize Resilience Over Detection

The detection-resilience gap isn't a new observation. Federal frameworks have been articulating this distinction for years. The industry just hasn't caught up.

Idaho National Laboratory's CCE methodology begins with a foundational assumption that contradicts detection-centric strategies:

> *"CCE begins with the assumption that if a critical infrastructure system is targeted by a skilled and determined hacker, the targeted network can and will be penetrated."*

Andy Bochman, INL's Senior Grid Strategist, puts it directly: "If you are in critical infrastructure you should plan to be targeted. And if you are targeted, you will be compromised. It's that simple."

The CCE approach focuses on consequence—identifying which operations must not fail and engineering protections that work even when cyber defenses don't.

NIST SP 800-160 Volume 2 makes an even more explicit statement:

> *"Cyber resiliency is based on the recognition that adversaries can establish and maintain a covert presence in systems. Therefore, many cyber resiliency techniques and approaches are not predicated on the assumption of successfully detecting adversity, including cyber-attacks."*

NIST explicitly acknowledges that some adversaries will evade detection—and that resilience strategies must work when detection fails.

Presidential Policy Directive 21 defines resilience as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions."

The framing matters: resilience is about withstanding and recovering, not detecting and preventing. Detection is a tool in service of resilience, not a substitute for it.

The Investment Imbalance

Where organizations put their money reveals their priorities:

High investment (detection/technology):

- Logging, monitoring, and detection capabilities: 72%
- Asset inventory and management tools: 67%
- Secure remote access platforms: 52%

Low investment (process/resilience):

- Process improvements: 31% (8th place)
- ICS-specific tabletop exercises: 17%
- SOAR: 12% (lowest)

Detection tools generate alerts. Process and organizational capability determine whether those alerts produce outcomes. Most organizations are buying visibility while underinvesting in the ability to act on what they see.

The vulnerability data illustrates this starkly. Organizations can now identify vulnerabilities with precision—but 90% of OT vulnerabilities lack patches. 38% of the highest-risk devices are missed entirely by CVSS-based prioritization. 74% of advisories have no mitigation available when announced.

Detection without the ability to remediate produces dashboards of known problems, not improved security posture.

What the Data Shows Actually Works

Regulated sites perform better—but not because they prevent more incidents.

The SANS 2025 survey found that regulated sites experienced approximately 50% fewer financial losses and safety impacts compared to unregulated peers. The key finding: they didn't have fewer incidents. They had better capabilities to contain and recover when incidents occurred.

Regulations that require incident response plans, testing, and assessment produce value not through preventing compromise but through ensuring organizations have practiced responding to it.

Tested backups produce 85% reduction in downtime. The cost of implementing and testing OT backup capabilities is far less than the savings from a single shortened incident.

Training multiplies capability. Organizations including field technicians in tabletop exercises report readiness levels 1.7x higher than those that don't. Same tools, dramatically different outcomes.

Detection speed matters—but only if response follows. Dale Peterson captured the dynamic perfectly: a customer praised their detection vendor's product as "fantastic"—but admitted they never looked at the alerts because they didn't want another screen in the SOC. Detection that doesn't drive action produces data without outcomes.

The Path Forward

Detection is necessary but insufficient. A more balanced approach requires:

1. **Start with consequences** — Identify which operations must not fail and work backward from there. This is the core insight of INL's CCE methodology.
2. **Invest in process alongside technology** — Detection without response capability produces data without outcomes. IR plans, tabletop exercises, and organizational coordination deserve budget alongside monitoring tools.
3. **Build recovery capability** — Tested backups, documented procedures, practiced restoration. The 85% downtime reduction from tested backups represents exceptional ROI.
4. **Accept that detection will fail** — Build resilience mechanisms that function even when detection doesn't. NIST's framework explicitly acknowledges this necessity.
5. **Measure outcomes, not just activity** — Time-to-recovery matters more than alerts generated. Financial impact of incidents matters more than vulnerabilities discovered.

Detection finds the fire. Resilience keeps the lights on while you fight it.

Sources

- SANS Institute, State of ICS/OT Security 2024: https://www.sans.org/blog/the-2024-state-of-ics-ot-cybersecurity-our-past-and-our-future
- SANS Institute, State of ICS/OT Security 2025: https://www.sans.org/white-papers/state-of-ics-ot-security-2025
- Dragos, OT Cybersecurity Year in Review: https://www.dragos.com/ot-cybersecurity-year-in-review
- Claroty, Global State of CPS Security 2024: https://claroty.com/resources/reports/the-global-state-of-cps-security-2024-business-impact-of-disruptions
- Idaho National Laboratory, CCE Methodology: https://inl.gov/national-security/cce/
- NIST SP 800-160 Volume 2: https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final
- Dale Peterson, Industry Analysis: https://dale-peterson.com/2025/09/02/we-won-we-lost-part-1/