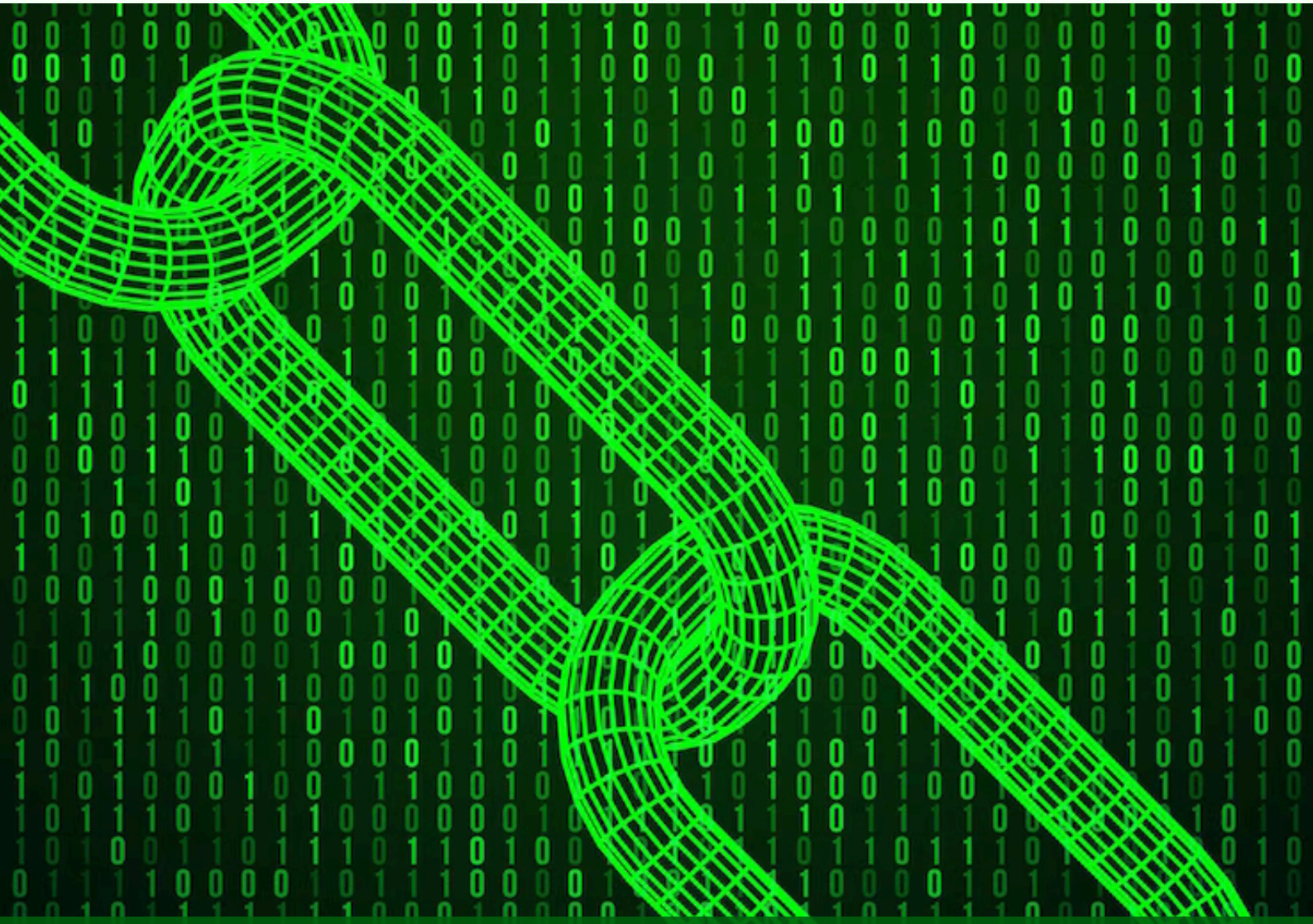
ÆGIS

TRUST THE EDGE



AEGIS BUILDING OT SOC WITH SPLUNK AND SOAR

Bridging the IT/OT Divide with Resilient Security Operations

PIERFELICE ROCCO

SECURITY RESEARCHER

WWW.AEGIS-OT.COM

AEGIS

As digital transformation intensifies, the convergence of IT and OT networks presents new cybersecurity challenges. Many industrial organizations now face increased exposure due to remote access, shared credentials, and unsecured ICS assets lacking proper segmentation. Despite these risks, studies show only 21% have achieved adequate ICS/OT cybersecurity maturity.

Organizations often struggle with:

- Cultural dissonance among OT engineers, IT staff, and security professionals
- Incompatibility between IT best practices and OT realities
- Ambiguity in cyber risk ownership and governance

To overcome these obstacles, evolving your SOC with integrated IT and OT capabilities is crucial. By developing industrial SOC competencies and aligning them with enterprise security operations, organizations can implement a defensible architecture to manage tomorrow's OT risks.

UNDERSTANDING AND MANAGING ICS/OT RISK

ICS/OT cyber incidents take an average of 316 days to detect and remediate, costing organizations nearly $3M per event. The reason? Visibility gaps, expanding threat surfaces, tool complexity, lack of OT-skilled resources, and SOC inefficiencies.

Key differences in IT vs OT risk:

Aspect	IT	OT
Devices	Servers, laptops, PoS, etc.	PLCs, RTUs, HMIs
Updates	Patch/update software regularly	Often restricted due to system uptime
Protocols	DNS, HTTPS, etc.	Dozens of proprietary industrial protocols
Risk	Data loss, IP theft	Loss of safety systems, grid, or plant operations

OT systems have distinct threats, limited patch windows, and different operational priorities. Therefore, ICS/OT risk cannot be managed effectively through traditional IT-centric SOC practices alone.

EVOLVING THE RISK EQUATION

The traditional risk formula:

Risk = Consequence x Threat x Vulnerability

...falls short in OT environments. Threats and vulnerabilities constantly increase, and the formula ignores resilience measures already in place. This can lead to exaggerated risk perceptions and fatigue among executives.

ÆGIS proposes a more refined model:

Risk = (Consequence x Threat x Vulnerability) / Resilience

Where "resilience" reflects:

- Technical, managerial, and procedural countermeasures
- Physical failsafes (e.g., pressure release valves)
- Incident response and recovery capabilities

This approach aligns better with OT priorities like availability and safety, enabling more accurate risk assessment and better investment decisions.

BUILDING OT CYBER RESILIENCE

Resilience means more than prevention—it includes detection, response, and recovery. An OT-aware SOC supports this through:

- Real-time monitoring and OT asset visibility
- Risk-based analytics to prioritize response
- Integrated IT/OT data for unified decision-making

Example: If a PLC shows abnormal behavior, but a physical failsafe is in place, the actual risk is lower. The resilience factor accounts for this reality, helping SOCs avoid overreaction and focus on critical threats.

DESIGNING TOMORROW'S SOC

SANS defines a defensible architecture as one that minimizes risk through design while enabling defenders. A future-ready SOC must:

- Centralize IT and OT operations
- Ingest OT-specific data and intelligence
- Enable context-rich analytics
- Support rapid, effective incident response

Rather than separating OT security, integrating it within a unified SOC framework leads to faster detection, shared context, and collaborative resolution.

Key Capabilities:

- Visibility into OT systems without disrupting them
- OT-specific threat intelligence
- Fusion-center model for joint IT/OT collaboration

VISIBILITY AND THREAT INTELLIGENCE

OT monitoring tools must:

- Detect active threats across the industrial network
- Support protocol-aware inspection
- Operate passively to ensure system safety

Threat intelligence should:

- Be sourced from experts tracking OT-specific adversaries
- Contextualize vulnerabilities with real-world threat behaviors

A modern SOC blends internal telemetry with external insights to prioritize and triage effectively.

ANALYTICS AND AUTOMATION

With terabytes of security data, analytics is essential. SOCs must:

- Aggregate and correlate IT + OT signals
- Enrich alerts using behavior-based scoring
- Reduce false positives and alert fatigue

Example: An off-hours PLC login alone may not trigger alarms. But when correlated with IT access logs and user behavior, it could reveal malicious activity.

Playbooks built on real-world OT incidents offer:

- Repeatable incident response workflows
- Semi-automation at level 4 of the Purdue Model
- Integration across IT and OT environments

CRITICAL CONTROLS TO SUPPORT RESILIENCE

SANS highlights five pillars for effective ICS cybersecurity:

- ICS-specific incident response plan
- Defensible network architecture
- Continuous ICS network visibility
- Secure remote access
- Risk-based vulnerability management

A centralized SOC designed around these elements ensures cyber resilience and fast MTTR reduction.

ÆGIS + SPLUNK: UNIFIED OT/IT SOC ENABLEMENT

ÆGIS integrates with Splunk Enterprise Security to:

- Enrich OT visibility (assets, logs, traffic, protocols)
- Correlate threat activity across IT and OT
- Drive prioritized incident response
- Support security orchestration and automated playbooks

Platform benefits:

- Seamless data ingestion and analysis
- Support for MITRE ATT&CK for ICS
- Visual SOC dashboards combining IT + OT insights

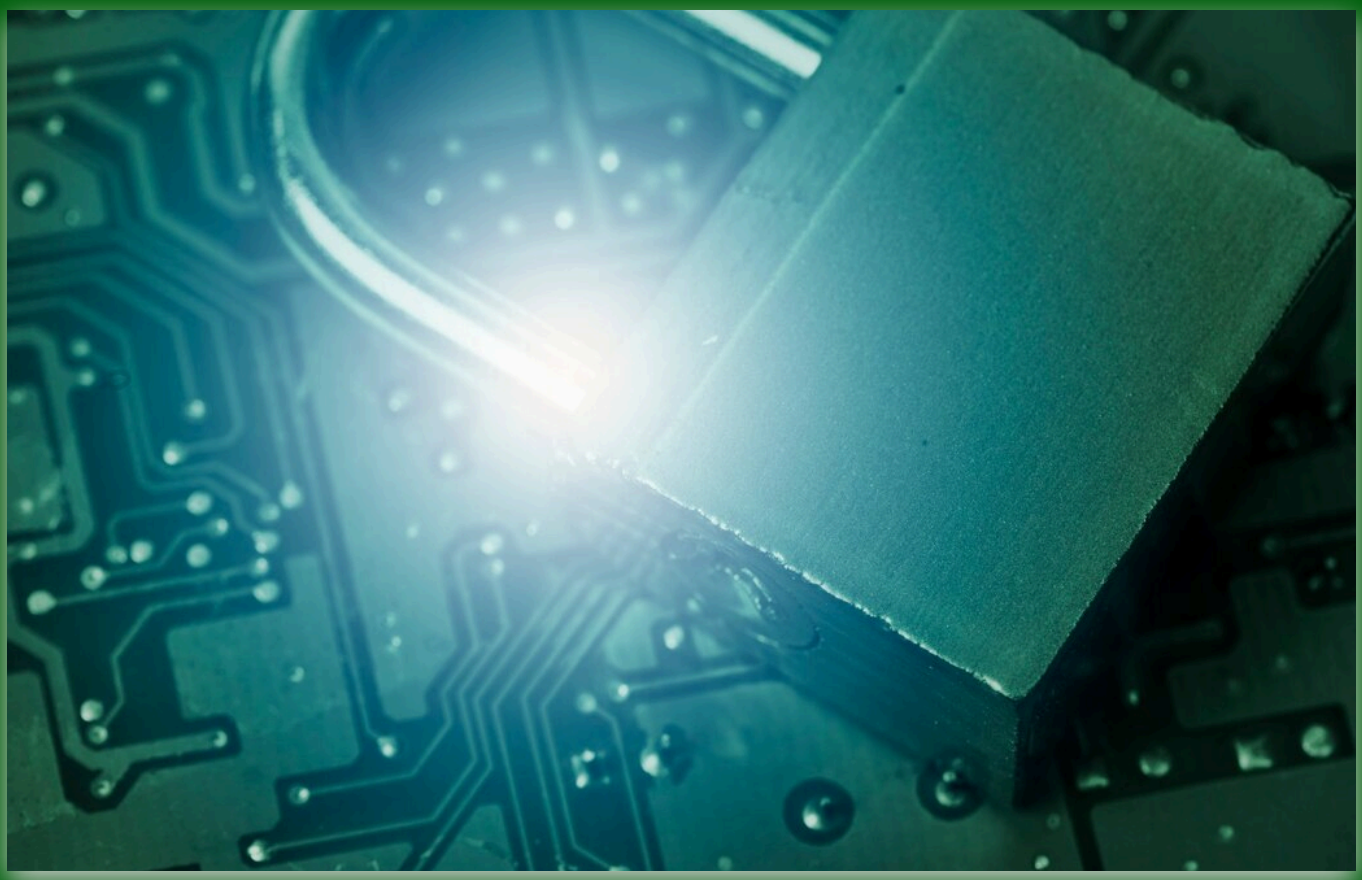
USE CASE: REMOTE ACCESS & PLC CHANGE

Scenario: A contractor connects via RDP after hours. Unusual, but not alarming in IT. Simultaneously, a PLC configuration changes without authorization—a serious OT incident.

Playbook activation: ÆGIS flags both events and prompts correlation through Splunk. The SOC now has:

- RDP logs
- PLC keystate events
- Firewall rules
- User account actions

Result: Fast triage and escalation, bridging IT and OT perspectives.



CONCLUSION: A RESILIENT, UNIFIED APPROACH

By uniting IT and OT telemetry, risk intelligence, and response workflows into a modern SOC architecture, organizations gain:

- Reduced detection and response times
- Lower risk exposure
- Improved cyber resilience

The future belongs to SOCs that break silos and bridge the IT/OT divide. ÆGIS is helping build that future today.

ÆGIS
TRUST THE EDGE

ABOUT ÆGIS

Ægis was born from a clear mission — to bring enterprise-grade cybersecurity into the heart of operational technology. In a world where OT networks are increasingly connected, exposed, and targeted, protecting critical infrastructure is no longer optional. It's a strategic necessity. Ægis is more than a product. It's a platform built from the ground up to secure complex, distributed, real-time environments — power plants, energy transport networks, automation systems, and industrial control infrastructure. Our team combines deep field experience in cybersecurity, OT engineering, and infrastructure resilience, delivering a platform that reflects the realities of operational risk, compliance, and performance.

CONTACT

www.aegis-ot.com

info@aegis-ot.com

Aegis

THANK YOU