OT Security Operations Center

Designing and Operating a SOC for Industrial Environments

OT Security Learning Series

Document 560 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

A Security Operations Center (SOC) provides centralized monitoring, detection, and response capabilities. While IT SOCs are well-established, extending security operations to Operational Technology environments requires different approaches, skills, and tools.

Information

This document covers the design and operation of SOC capabilities for OT environments. It addresses organizational models, staffing requirements, technology considerations, and the unique challenges of monitoring industrial control systems while maintaining operational safety and availability.

2 SOC Models for OT

2.1 Organizational Approaches

Organizations can structure OT security operations in several ways:

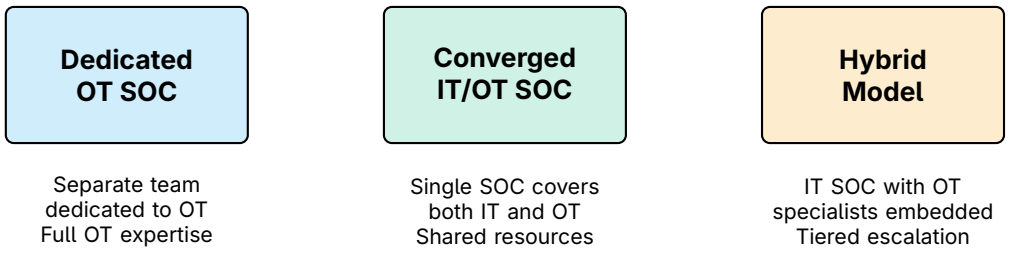

Figure 1: SOC organizational models for OT

2.2 Model Comparison

Aspect	Dedicated OT	Converged	Hybrid
OT expertise	Deep	Limited	Tiered
Cost	High	Lower	Medium
Coverage	24/7 challenging	24/7 easier	24/7 possible
Coordination	Separate processes	Unified	Defined handoffs
Best for	Large OT footprint	Small OT presence	Most organizations

Table 1: Comparison of SOC organizational models

Key Point

Recommendation: Most organizations benefit from a hybrid model—IT SOC provides 24/7 monitoring with OT-trained analysts who escalate to OT specialists for investigation and response.

3 Staffing and Skills

3.1 Required Competencies

OT SOC analysts need skills beyond traditional IT security:

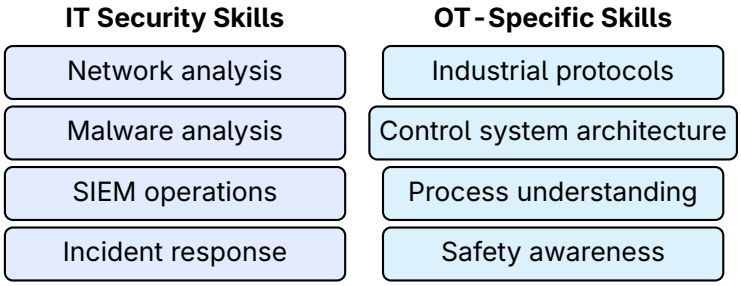

Figure 2: Required skill sets for OT SOC analysts

3.2 Staffing Tiers

Tier	Role	OT Requirements
Tier 1	Alert triage	Basic OT awareness, protocol recognition
Tier 2	Investigation	OT network analysis, ICS malware knowledge
Tier 3	Advanced response	Deep OT expertise, vendor coordination
OT SME	Subject matter expert	Control system engineering background

Table 2: SOC tier structure with OT requirements

Warning

OT security talent is scarce. Consider cross-training IT analysts in OT fundamentals and partnering with OT engineering teams for deep expertise during incidents.

4 Technology Stack

4.1 Core Components

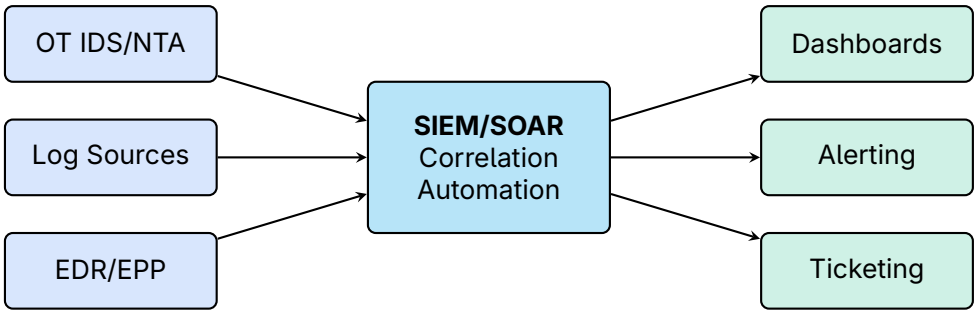

Figure 3: OT SOC technology stack overview

4.2 OT-Specific Tools

- **OT Network Monitoring** – Deep packet inspection for industrial protocols
- **Asset Inventory** – Automated discovery and tracking of OT devices
- **Vulnerability Management** – OT-aware scanning and assessment
- **Threat Intelligence** – ICS-specific threat feeds and IOCs
- **Secure Remote Access** – Monitored vendor and engineer access

4.3 Integration Considerations

Challenge	Approach
Protocol support	Ensure SIEM can parse industrial protocols (Modbus, DNP3, etc.)
Data volume	Filter and aggregate at source; prioritize security-relevant events
Network isolation	Use data diodes or secure forwarders from OT to SOC
Real-time correlation	Tune for OT-relevant use cases, not IT patterns

Table 3: Technology integration challenges

5 Data Sources and Visibility

5.1 Critical Log Sources

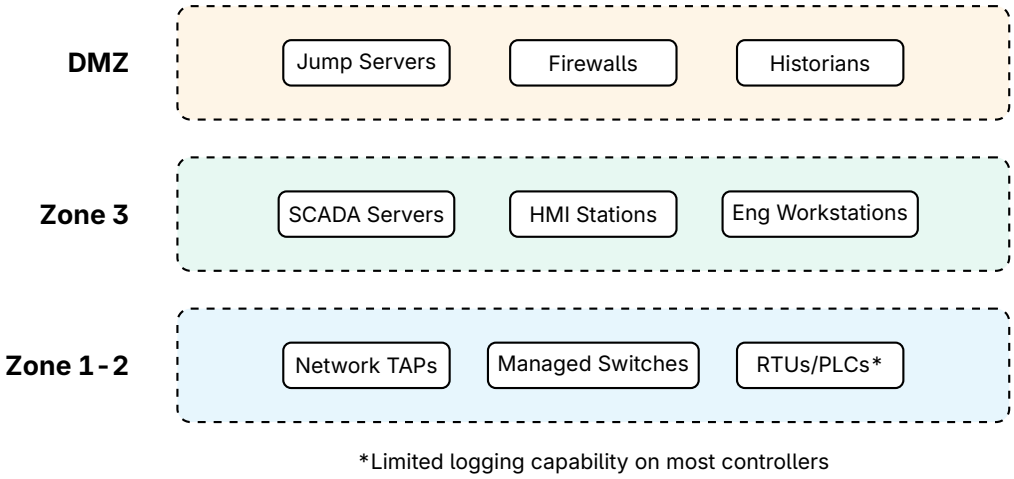

Figure 4: Log sources by Purdue zone

5.2 Network Traffic Analysis

Network monitoring provides visibility where endpoint logging is limited:

- **Protocol metadata** – Source, destination, function codes, registers
- **Baseline deviations** – New connections, unusual commands
- **Asset discovery** – Passive identification of OT devices
- **Threat detection** – Known attack signatures and anomalies

Critical

Many OT devices cannot run agents or forward logs. Network traffic analysis is often the only visibility into Level 0 - 1 activity. Deploy monitoring at strategic points to maximize coverage.

6 Detection Use Cases

6.1 OT-Specific Detection Rules

Use Case	Detection Logic
Unauthorized engineering access	PLC programming commands from non-engineering stations
New device on OT network	ARP/DHCP for unknown MAC addresses
Protocol anomaly	Invalid function codes or malformed packets
Lateral movement	IT protocols (SMB, RDP) in control network
Configuration change	Write commands to PLCs outside change windows
Remote access abuse	VPN/jump server access at unusual times

Table 4: Example OT detection use cases

6.2 Alert Prioritization

Not all alerts require immediate response in OT:

- CRITICAL Safety system alerts – Immediate escalation
- HIGH Control system changes – Verify with operations
- MEDIUM Network anomalies – Investigate within shift
- LOW Policy violations – Queue for review

Tip

Coordinate alert thresholds with OT operations. Some activities that look suspicious (firmware updates, configuration changes) may be planned maintenance. Integrate with change management systems to reduce false positives.

7 Operations and Processes

7.1 Runbooks and Playbooks

OT incidents require modified response procedures:

- **Escalation paths** – Include OT engineering and operations contacts
- **Response constraints** – Document what actions are safe vs. risky
- **Coordination requirements** – When to involve plant operations
- **Communication protocols** – Who to notify, in what order

7.2 Shift Handoff

Critical information for OT SOC shift changes:

- Active incidents and investigation status

- Planned maintenance and change windows
- Known operational anomalies (process upsets)
- Vendor access sessions in progress

Warning

OT SOC analysts must understand the operational context. A spike in network traffic during a batch process is normal; the same spike at 3 AM is suspicious. Build relationships with operations teams.

8 Metrics and Reporting

8.1 Key Performance Indicators

Metric	Description
Mean time to detect (MTTD)	Time from event occurrence to SOC awareness
Mean time to respond (MTTR)	Time from detection to initial response action
Alert volume by zone	Distribution of alerts across Purdue levels
False positive rate	Percentage of alerts that are not true incidents
OT asset coverage	Percentage of OT assets with monitoring visibility
Change correlation	Alerts matched to authorized changes

Table 5: OT SOC key performance indicators

9 Summary

Key Takeaways

- **Hybrid Model:** Most organizations benefit from IT SOC with embedded OT expertise and defined escalation paths
- **Specialized Skills:** OT SOC analysts need industrial protocol knowledge, control system understanding, and safety awareness
- **Network-Centric Visibility:** Use network traffic analysis where endpoint logging is limited or unavailable
- **OT-Specific Use Cases:** Detection rules must account for industrial protocols and operational context
- **Operational Coordination:** Integrate with change management and maintain close relationships with OT operations teams
- **Modified Response:** Runbooks must include safety considerations and coordination requirements before taking action

10 Further Reading

Standards and Guidelines

- **NIST SP 800-82 Rev. 3** – Guide to OT Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final
- **IEC 62443-2-1** – Security Program Requirements for IACS Asset Owners
  https://webstore.iec.ch/publication/7030

Resources

- **SANS ICS** – Industrial Control Systems Security
  https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials
- **MITRE ATT&CK for ICS** – Adversary Tactics and Techniques
  https://attack.mitre.org/techniques/ics/
- **CISA** – Industrial Control Systems Security
  https://www.cisa.gov/topics/industrial-control-systems

Books

- Knapp, Eric D. – *Industrial Network Security* (Syngress)
- Muniz et al. – *Security Operations Center* (Cisco Press)

Part of the OT Security Learning Series