SIEM for OT Environments

Security Information and Event Management for industrial systems

OT Security Learning Series

Document 530 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

Security Information and Event Management (SIEM) platforms aggregate, correlate, and analyze security data from across the enterprise. Extending SIEM to OT environments provides unified visibility but requires careful consideration of OT-specific data sources and operational constraints.

SIEM benefits for OT security:

- **Unified visibility:** Single view across IT and OT security events
- **Correlation:** Detect attacks spanning IT/OT boundaries
- **Compliance:** Centralized logging for regulatory requirements
- **Incident response:** Faster investigation with correlated data
- **Historical analysis:** Long-term storage for forensics

2 SIEM Architecture for OT

2.1 Data Flow Architecture

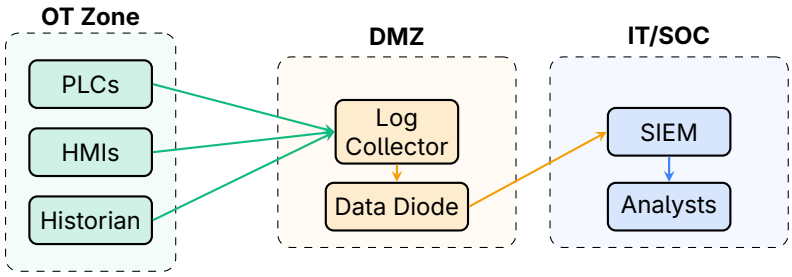

Figure 1: OT SIEM Data Flow Architecture

Warning

One-Way Data Flow: Log data should flow from OT to IT/SIEM, never the reverse. Use data diodes or strict firewall rules to prevent SIEM access back into OT networks.

2.2 Deployment Options

Option	Advantages	Considerations
Unified SIEM	Single platform, IT/OT correlation	Requires OT protocol support
Separate OT SIEM	OT-focused, isolated	Limited IT correlation
Federated	Local OT + central IT	Complex management
Cloud SIEM	Scalable, managed	Data sovereignty concerns

Table 1: SIEM Deployment Options for OT

3 OT Data Sources

3.1 Log Sources by Zone

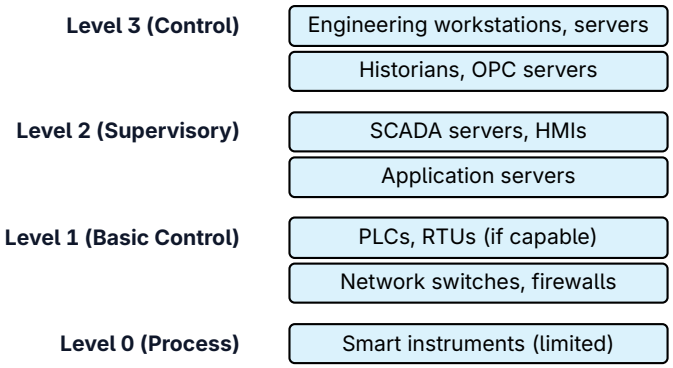

Figure 2: OT Log Sources by Purdue Level

3.2 Data Types for OT SIEM

Data Type	Examples
Authentication logs	User logins to HMIs, engineering workstations
Network traffic	Firewall logs, IDS alerts, NetFlow
System events	Windows/Linux events, service status
Application logs	Historian queries, SCADA events
Configuration changes	PLC logic modifications, setpoint changes
Physical security	Badge access, camera systems
Process alarms	Safety alerts, limit violations

Table 2: OT Data Types for SIEM

3.3 Challenges with OT Log Collection

Warning

OT Logging Limitations:

- Many PLCs have no logging capability
- Legacy systems may lack syslog support
- Bandwidth constraints in some OT networks
- Time synchronization issues affect correlation
- Proprietary formats require custom parsing

4 Use Cases and Detection Rules

4.1 OT-Specific Detection Rules

Use Case	Detection Logic
Unauthorized remote access	VPN/RDP from unexpected IP or outside hours
Engineering workstation compromise	Malware detection, unusual outbound connections
PLC logic modification	Configuration change without change ticket
Protocol anomaly	Unknown function codes, new communication pairs
Cross-zone traffic	IT device communicating directly to OT
Credential abuse	Multiple failed logins, privilege escalation

Table 3: OT SIEM Detection Use Cases

4.2 Correlation Rules

Key Point

Multi-Source Correlation Examples:

1. VPN login + firewall allow + HMI access = normal remote session
2. VPN login + firewall deny + repeated attempts = potential attack
3. Badge out + remote access from inside = credential sharing/theft
4. IT malware alert + OT traffic anomaly = possible lateral movement

4.3 Alert Prioritization

CRITICAL	Safety system modifications
HIGH	PLC logic changes, unauthorized access
MEDIUM	Protocol anomalies, failed logins
LOW	Informational events, normal deviations

Figure 3: Alert Priority Levels

5 Implementation Considerations

5.1 Network Architecture

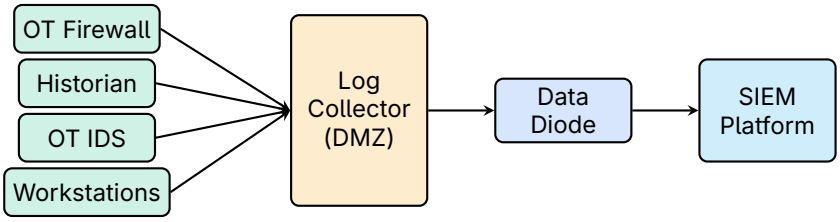

Figure 4: OT Log Collection Architecture

5.2 Time Synchronization

Critical

Critical: All OT and IT systems must use synchronized time sources (NTP/PTP). Without accurate timestamps, event correlation is impossible and forensic analysis is unreliable.

Time synchronization requirements:

- Deploy NTP servers in OT network (isolated from internet)
- Synchronize all logging sources
- Use UTC for log timestamps
- Monitor for time drift
- Document timezone handling

5.3 Storage and Retention

Data Type	Typical Retention	Regulatory Driver
Security events	1–3 years	NERC CIP, IEC 62443
Authentication logs	1–2 years	Compliance, forensics
Network flows	90 days–1 year	Capacity, forensics
Raw packet capture	7–30 days	Storage cost
Configuration changes	3–7 years	Audit requirements

Table 4: Log Retention Guidelines

6 Integration with SOC

6.1 SOC Operating Model

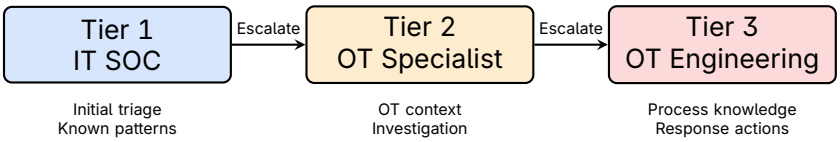

Figure 5: Tiered SOC Model for OT

6.2 OT Context Requirements

Tip

SOC analysts need OT context:

- Asset criticality information
- Normal communication patterns
- Maintenance schedules and change windows
- Contact information for OT personnel
- Response constraints (no automatic blocking)

7 Summary

Key Takeaways

- **Unified visibility:** SIEM enables IT/OT correlation
- **One-way flow:** Logs flow from OT to SIEM, not reverse
- **OT data sources:** Historians, HMIs, firewalls, IDS
- **Protocol support:** SIEM must parse OT-specific data
- **Time sync critical:** Accurate timestamps enable correlation
- **OT context:** SOC needs asset and process knowledge
- **Tiered response:** Escalate to OT specialists for context

8 Further Reading

Standards

- **IEC 62443-2-1** – Security management system requirements
  https://webstore.iec.ch/publication/7030
- **NIST SP 800-82 Rev. 3** – Guide to OT Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final

Resources

- **CISA** – Logging and Monitoring Guidance
  https://www.cisa.gov/resources-tools/resources
- **SANS** – Building an ICS Security Operations Center
  https://www.sans.org/white-papers/

Part of the OT Security Learning Series