Enhancing OT Security Monitoring with SOAR – a guide to PoC with a commonly applied use case

Implementing SOAR in an OT environment requires a structured, phased approach that aligns security automation with operational reliability. By strategically placing SOAR at the IT/OT boundary and developing tailored playbooks, you can demonstrate:

- Reduced response time from hours to minutes with automated workflows
- Improved compliance with IEC 62443, NIS2, and NERC CIP standards
- Enhanced resilience by proactively mitigating cyber threats in OT environments.

A full-scale SOAR deployment can be complex, so a Proof of Concept (POC) is essential before large-scale rollout.

A common use case in OT environments is the unauthorised connection of unknown devices, such as a rogue laptop that can introduce malware or enable unauthorised access to critical systems. A good scenario is a possibility that the security team detects an unauthorised device connecting to the OT network. The response workflow differs significantly between manual monitoring vs automated SOAR driven approach.

Criteria	Manual Process	Automated Process	Efficiency
Trigger Event	Unauthorised device detected in OT network	Unauthorised device detected in OT network	0 min (Same trigger)
Detection Method	Manual log review or SIEM alert	Automated ingestion by SOAR from OT monitoring tool	30-60 min
Asset Identification	SOC analyst manually checks asset inventory	SOAR cross-references asset database automatically	30-90 min
Threat Intelligence Check	Manual lookup in external sources	Automated enrichment with threat intelligence feeds	20-40 min
Alert Correlation	Manual correlation with past incidents	Automated correlation with SIEM, threat intelligence, and logs	30-60 min
Response Time	Hours to days due to manual investigation	Minutes due to automated triage and response	4-8 hours
Containment Action	Requires manual intervention to block device via NAC/firewall	SOAR automatically triggers containment actions (e.g., NAC block)	2-6 hours
Escalation Process	SOC manually escalates to OT engineers	SOAR auto-notifies SOC and OT teams based on severity	30-60 min
Incident Documentation	Manually documented by SOC/OT teams	Automatically logged and documented for compliance (NIS2, IEC 62443)	60-120 min
Compliance Readiness	Requires additional effort for reporting and audits	Automated compliance reporting ensures audit readiness	2-4 hours per incident
Analyst Workload	High, SOC spends time on triage, correlation, and response	SOAR handles repetitive tasks, allowing focus on critical incidents	50-70% reduction in manual effort

How this efficiency is achieved:

Faster Incident Detection & Response

With automation, alerts are ingested, correlated, and enriched within minutes, accelerating triage and response.

Automated Containment & Threat Mitigation

Without automation, security teams manually block unauthorised devices using firewalls or NAC systems. SOAR automates device quarantine, ensuring threats are contained immediately.

Reduced Analyst Workload & Improved Efficiency

Analysts spend 50-70% of their time on repetitive investigation tasks.

SOAR automates asset verification, threat intelligence lookups, and alert correlation, allowing analysts to focus on critical threats.

Compliance & Audit Readiness

SOAR automatically generates incident reports aligned with NIS2, IEC62443, and other compliance standards.

SOAR Placement in OT Network Zones

In an Operational Technology (OT) network, SOAR platform should align with security and network segmentation principles to ensure efficient monitoring, response, and minimal disruption to industrial control processes.

Zone	Description	Components
Level 5 - Enterprise Zone	Used by the SOC, IT security, and compliance teams for incident response and reporting.	SOAR (Cloud or On-Prem), SIEM, SOC tools
Level 4 - IT/OT DMZ	Ideal for log aggregation, correlation, and playbook automation, while maintaining OT security segmentation.	Firewalls, SIEM, SOAR (On-Prem for hybrid deployments)
Level 3 - Operations Zone	SOAR interacts with OT SIEM, firewalls, IDS/IPS, but direct automation is limited to avoid disrupting operations.	OT SIEM, Network Intrusion Detection (NIDS), SOAR
Level 2 - Control Zone	Contains SCADA**,** DCS, and HMIs; SOAR should not directly automate responses here to prevent downtime.	SCADA, ICS firewalls
Level 1 - Process Zone	Low-latency operations, SOAR automation could interfere.	PLCs, RTUs, DCS
Level 0 - Field Zone	Automation could cause safety and reliability risks.	Sensors, robots, valves

A SOAR playbook automates the response process when an unauthorised device connects to an OT network. Below is a structured playbook workflow following the IEC62443 security zones and best practices for OT security monitoring.

Playbook: Unauthorized Device Detection in OT Network

Trigger Event:

An unauthorised device (e.g., unknown laptop, USB device) is detected in the OT network.

Detected via OT SIEM, NAC, firewall logs, or network anomaly detection (NIDS/NIPS).

SOAR Playbook Workflow (Automated Response Steps)

Step	Description	Automated SOAR Action	Interaction Zone
1. Trigger Event	SIEM/NAC detects unauthorised device connection	SOAR ingests alert from SIEM, NAC, or firewall	Level 3 (Operations Zone)
2. Asset Identification	Verify device against approved OT asset inventory	SOAR queries CMDB/OT asset management system	Level 3 (Operations Zone)
3. Threat Intelligence Enrichment	Check if device IP/MAC appears in threat feeds	SOAR queries MITRE ATT&CK, OT threat intelligence	Level 4 (IT/OT DMZ)
4. Correlation	Compare with previous similar security events	SOAR fetches logs from SIEM & past alerts	Level 4 (IT/OT DMZ)
5. Risk Classification	Determine severity based on location, device type, and threat intelligence	SOAR assigns risk score (low, medium, high, critical)	Level 4 (IT/OT DMZ)
6. Containment Action (If High Risk)	Block or isolate unauthorised device	SOAR triggers NAC/firewall rule to block device	Level 3 (Operations Zone)
7. Notify Security Teams	Alert OT SOC and Incident Response (IR) teams	SOAR sends email, Teams/Slack alert, or ServiceNow ticket	Level 5 (Enterprise Zone)
8. Forensic Data Collection	Gather logs, network traffic, and device information for investigation	SOAR extracts forensic logs from OT SIEM and firewalls	Level 3 & 4 (Operations & IT/OT DMZ)
9. Compliance & Documentation	Generate incident report for audits (IEC 62443, NIS2, NERC CIP)	SOAR automatically generates a report and updates SIEM	Level 5 (Enterprise Zone)
10. Incident Closure & Lessons Learned	SOC reviews response, updates playbook for future cases	SOAR updates playbook based on findings	Level 5 (Enterprise Zone)

Key Success Metrics

- **Detection Speed (MTTD)** – How fast does SOAR detect threats?
- **Response Time (MTTR)** – How quickly does SOAR automate actions?
- **False Positive Rate** – Does SOAR reduce unnecessary alerts?
- **Compliance Readiness** – Does the SOAR workflow align with audit requirements?

Go Decision (Proceed with Deployment if the Following Are Met)

- SOAR successfully detects and responds to OT threats within defined KPIs.
- No disruptions to critical OT processes during testing.
- Stakeholders approve automation playbooks with defined manual approvals where needed.
- Integration with existing OT security tools is validated.
- Clear ROI (e.g., reduced incident response time, improved efficiency, enhanced compliance reporting).

Set and measure KPI Targets: (What good looks like)
MTTD < 1 min (from alert ingestion)
MTTR < 5 min (from detection to containment)
False Positives Reduced by 30%

No-Go Decision (Reassess If the Following Issues Arise)

- Excessive false positives or missed detections impacting SOC workflows.
- Latency issues affecting OT system performance (SOAR queries slowing down OT firewalls).
- Stakeholder pushback due to operational risks or lack of trust in automation.
- Technical integration challenges preventing SOAR from ingesting necessary OT security data.

Conclusion:

In this document, I've consolidated my experience working on OT Security Monitoring projects and the crucial role automation plays in enhancing efficiency and effectiveness. For project managers, understanding the value of automated security monitoring is key to managing risk and ensuring robust protection against cyber threats. In this guide, I've tried to share insights from my experience, outlining the benefits of automation in OT security monitoring, the challenges it helps address, and practical steps to integrate it into your projects.

Implementing SOAR in an OT environment requires a strategic approach that balances security**,** automation, and operational reliability. As a project manager, your role is to ensure alignment between IT and OT teams and orchestrate integrations without disrupting industrial processes.