OT Incident Response

Responding to Security Incidents in Industrial Environments

OT Security Learning Series

Document 600 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Incident response in OT environments requires different approaches than traditional IT incident response. The presence of physical processes, safety systems, and operational constraints means that standard IR playbooks may be inappropriate or even dangerous.

Critical

Standard IT incident response actions (isolate, reimage, restore from backup) can cause serious harm in OT environments. Disconnecting a PLC or rebooting a control system can stop production or create safety hazards.

1.1 Key Differences from IT IR

Aspect	IT Response	OT Response
Primary goal	Protect data	Maintain safe operations
Isolation	Disconnect immediately	May not be possible
System restart	Common remediation	Can disrupt process
Forensics	Image drives	May lack storage access
Timing	Business hours focus	24/7 operations
Expertise	IT security team	Requires process knowledge

2 Incident Response Phases

2.1 Preparation

Key Point

OT-specific preparation requirements:

- Cross-trained team (IT security + OT engineering)
- OT-specific playbooks reviewed by operations
- Network diagrams and asset inventory available
- Backup configurations for critical devices
- Relationships with OT vendors established
- Safe shutdown procedures documented

2.2 Detection and Analysis

Sources of OT incident detection:

- **OT network monitoring:** Anomalous traffic, unauthorized commands
- **Process anomalies:** Unexpected behavior reported by operators
- **IT security alerts:** Threats moving toward OT networks
- **Vendor notifications:** Vulnerability or compromise advisories

2.3 Containment

Warning

Containment in OT requires extreme caution:
- Consult operations before any network changes
- Understand process dependencies before isolation
- Consider safety implications of any action
- Document everything—changes may need reversal

Containment options (least to most disruptive):

1. **Monitor only:** Observe while gathering intelligence
2. **Block at firewall:** Stop specific traffic without isolation
3. **Segment:** Isolate affected zone, maintain internal operations
4. **Controlled shutdown:** Safe process stop if necessary
5. **Emergency stop:** Only for imminent safety threat

2.4 Eradication and Recovery

- **Restore from known-good:** Use verified configuration backups
- **Vendor involvement:** May need vendor support for restoration
- **Staged recovery:** Bring systems back incrementally
- **Verification:** Confirm process operates correctly
- **Enhanced monitoring:** Watch for reinfection

3 OT-Specific Considerations

3.1 Safety First

Critical

Safety always takes precedence over security:
- Never disable safety instrumented systems
- Ensure safe state before any remediation
- Involve process safety personnel in decisions
- Document safety implications of all actions

3.2 Operational Constraints

Consider before taking action:

- **Process state:** Can the process be safely interrupted?

- **Production schedule:** Critical batches or orders in progress?
- **Maintenance windows:** When can changes be made?
- **Staffing:** Are qualified operators available?
- **Dependencies:** What else will be affected?

3.3 Evidence Collection

OT forensics challenges:

- **Limited logging:** PLCs may not log security events
- **Volatile memory:** Evidence lost on restart
- **No disk imaging:** Embedded systems lack standard storage
- **Network captures:** Primary source of forensic data
- **Historian data:** Process values may indicate compromise

4 Team Structure

4.1 Required Expertise

OT Incident Response Team

- **IT Security:** Malware analysis, network forensics
- **OT Engineering:** Process knowledge, control systems
- **Operations:** Current process state, safe shutdown
- **Safety:** Risk assessment, safety system expertise
- **Management:** Decision authority, communications
- **Vendors:** System-specific expertise (as needed)

4.2 Communication

- **Out-of-band:** Don't rely on potentially compromised networks
- **Stakeholder updates:** Operations, management, regulators
- **Vendor coordination:** May need under NDA
- **Information sharing:** ISAC, CISA (as appropriate)

5 Post-Incident Activities

5.1 Lessons Learned

- **What happened:** Root cause and attack timeline
- **What worked:** Effective detection and response actions
- **What failed:** Gaps in monitoring, procedures, or tools
- **Improvements:** Specific actions to prevent recurrence

5.2 Documentation

- Complete incident timeline with evidence
- Actions taken and their outcomes
- Recommendations for security improvements
- Updates to IR procedures based on lessons learned

6 Further Reading

Standards and Guidelines

- **NIST SP 800-82 Rev. 3** – Guide to OT Security (Incident Response)
  https://csrc.nist.gov/pubs/sp/800/82/r3/final
- **IEC 62443-2-1** – Security Management System
  https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

Resources

- **CISA** – ICS Incident Response
  https://www.cisa.gov/resources-tools/resources
- **SANS ICS** – Incident Response Resources
  https://www.sans.org/blog/