GUIDEPOINT® SECURITY

OPERATIONAL TECHNOLOGY INCIDENT RESPONSE (OTIR) SERVICES

Maintain Control When OT Environments are Under Attack

Cyberattacks on OT environments threaten operational continuity, public safety, and regulatory standing, yet most incident response programs are built for IT, not industrial control systems.

Preserve operational continuity and safety before, during, and after a cyber incident. Purpose-built for industrial environments, GuidePoint Security's Operational Technology Incident Response (OTIR) services combine OT-specific expertise with proven incident response (IR) methodologies to accelerate response, reduce the blast radius, and keep critical systems running. Organizations gain the specialized knowledge, tested processes, and 24x7 response capabilities needed to contain threats and recover quickly, without compromising the operational continuity and safety that IT response approaches can put at risk.

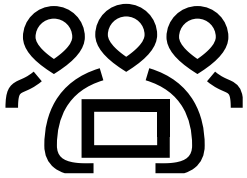
OT Incident Response Without Disruption

Operational Technology (OT) environments demand a fundamentally different approach to incident response (IR) than IT systems. Safety systems, legacy infrastructure, proprietary protocols, and operational continuity requirements create constraints that IT-focused IR teams may not be equipped to navigate.

GuidePoint Security's Operational Technology Incident Response (OTIR) services address the full needs of IR in specialized environments, from readiness and planning through active incident support and recovery. GuidePoint OT, digital forensics, and incident response experts ensure organizations can respond with precision, protect people and operations, and meet compliance obligations, even while under pressure.

GuidePoint's OTIR experts tailor solutions to each unique environment, maturity level, and goals so they can:

- **Respond faster and with greater precision** with OT-specific plans, playbooks, tabletop exercises, and trained responders on retainer
- **Reduce operational impact** through safety-aware containment and recovery procedures
- **Close the gap between IT and OT response** with integrated, joint IR capabilities
- **Meet regulatory requirements** including IEC 62443, NIST SP 800-82, and NERC CIP
- **Ensure recoverability** with regular OT backup and restore validation
- **Stay ahead of threats** with specialized OT threat hunting exercises
- **Navigate breach correspondance** with experts who are pre-approved by most major cyber insurance carriers and maintain established processes with external counsel and breach coaches



Stronger Together. Protecting What's Next.

Working with GuidePoint, your organization will be backed by our elite team of highly trained cybersecurity engineers, architects and consultants who come from organizations of all sizes, including Fortune 100 companies, the Department of War, and U.S. intelligence agencies.

Prepare, Respond, and Recover Across Every Stage of an OT Cyber Incident

GuidePoint Security's OT security and DFIR (Digital Forensics and Incident Response) experts specialize in investigating cyberattacks, containing breaches, and restoring OT and IT environments. Our complete portfolio of OT incident response services are designed for the constraints of OT environments, including proprietary systems, air-gapped networks, vendor dependencies, and operational safety requirements. Services include:

OTIR Retainers

During an active incident, organizations can't afford procurement delays. An OTIR Retainer provides 24x7x365 access to dedicated OTIR experts and an IT IR team member on every engagement, with priority response SLAs, defined escalation paths, and post-incident reporting.

OT IR Plan Development and Refresh

GuidePoint helps develop or modernize OT IR plans aligned to IEC 62443, NIST SP 800-82, and other relevant frameworks to ensure. Each plan includes gap assessments, defined roles and responsibilities, decision matrices, escalation paths, and OT/IT alignment guidance.

OT IR Playbook Development and Refresh

During an active OT incident, responders need clear, pre-approved procedures. GuidePoint helps develop scenario-specific playbooks with decision trees, containment steps, and recovery procedures tailored to OT constraints and coordinated with existing IT IR playbooks.

Tabletop Exercises

Tabletop exercises ensure that gaps surface during practice, not live incidents. GuidePoint facilitates three formats:

- **Technical:** Tests detection, containment, and recovery with operators, engineers, and security teams
- **Executive:** Tests crisis communications, regulatory notification, and business continuity decisions
- **Joint IT/OT:** Simulates combined scenarios to test cross-team coordination and handoffs

OT Backup and Recovery

Incomplete or untested backups are often discovered only during an active incident. GuidePoint assesses backup posture, develops OT-specific strategies, and provides tooling guidance, recovery documentation, and integrity validation to support operational continuity.

OT Threat Hunting

Adversaries often maintain persistent OT access for months before acting, and traditional IT tools are frequently blind to OT-specific protocols. GuidePoint conducts proactive, hypothesis-driven hunts using passive, read-only techniques, delivering a prioritized findings report with risk-based remediation recommendations.

Why GuidePoint Security

When cyber threats target operational technology systems, you want the best on your side. GuidePoint Security designs, deploys, and delivers tailored OTIR services that protect operations and help keep critical systems online. We integrate solutions across any environment, faster, smarter, and with less risk to strengthen your defenses. Accelerate your business with confidence and protect what matters most.

About Us

GuidePoint Security brings together proven expertise, great relationships, and leading technologies to solve our client's most complex cybersecurity challenges. As a trusted cybersecurity advisor and partner, GuidePoint keeps people, data, and operations safe. We deliver tailored cybersecurity services that adapt to safeguard the nation's leading organizations today and provide complete confidence in their cybersecurity tomorrow. Stronger Together. Protecting What's Next.

GUIDEPOINT® SECURITY

1900 Reston Metro Plaza, Suite 701 • Reston, VA 20190
guidepointsecurity.com • info@guidepointsecurity.com • (877) 889-0132
DS.OTIR.2606