Experience Matters

Incident Response for Converged OT/IT

Our elite, intelligence-driven forensics and incident response capabilities empower companies to rapidly detect, respond to, and recover from advanced cyber threats, enabling resilience and business continuity amid a shifting regulatory landscape and an evolving technology ecosystem.

A Comprehensive Approach to Converged OT/IT Incident Response

Booz Allen provides streamlined incident response solutions to help our customers quickly and effectively plan for, prepare for, and respond to cybersecurity incidents across their industrial OT and enterprise IT environments. We are uniquely positioned to coordinate across the organisation with an ability to meet the demands of regulators, national security, and law enforcement authorities. Our teams leverage timely and actionable intelligence, along with deep analytical insights and a comprehensive business approach, to enable resilience across the organisation. Incident response begins before an incident occurs and concludes long after the emergency has deescalated. Our subject-matter experts, with specialised skills across different types of incidents and workflows, partner with a broad spectrum of stakeholders to ensure an entire enterprise is ready to face the threats of today and tomorrow.

Continuous Planning & Readiness:

Incident Response Planning

Establishing clear organisational objectives, incident-specific playbooks, and defined roles with escalation criteria, as well as identifying key external partners.

- Critical Systems & Impacts
- Plant Operations & Process Analysis
- Geopolitical Threat Analysis
- IR Playbook and Runbook Development
- OT Packet Capture Analysis & Live Network Monitoring
- OT Resilience & Security Assessments
- Cyber Incident Site Safety Analysis
- Physical Site Walkthroughs
- Electromagnetic Spectrum Evaluations
- Supply Chain Impact Analysis
- Financial Impact Assessments
- Crisis Management Planning
- OT Specific Tabletop Exercises & Wargaming
- Compromise Assessment
- Penetration Testing

Digital Forensics & IR:

Identify, Protect, Detect, Respond & Recover

Rapidly identifying, containing, and eradicating malicious activity to quickly restore business operations, satisfy regulatory obligations, and deliver defensible results designed to withstand regulatory inquiry and third-party scrutiny.

- OT Cybersecurity Support , from over 55+ GICSP and GRID certified OT professionals
- PLC/HMI Log and Config Review
- Embedded Firmware & Binary Analysis
- Process Historian and SOE Data Analysis
- Evidence Collection & Preservation
- Threat Actor Communications
- Incident Containment Support
- Incident Recovery & Remediation
- Crisis Management & Incident Command
- Cryptocurrency Settlement Oversight
- Blockchain Investigations
- Investigations & Recovery & Support
- Cloud, Network, System, and OT-IACS Forensics

Post-Incident & Ongoing Support:

Program Enhancements and Optimised Operations

Intelligence-driven strategy, guidance, and support, including cyber fusion center design and build, environment hardening, and operational optimisations to defend against future threats and enhance your security posture.

- Pre-Paid Incident Response Retainer Services, supporting both IR and proactive IT and/or OT engagements without limitation
- Post-Mortem Assessments & Lessons Learn
- Continuous Cybersecurity Testing & Assessments
- OT-Specific Assessments available for frameworks including but not limited to NIST CSF, IEC-62443, OG-86, and NIS2
- Threat Intelligence Operations
- Continuous IR Intelligence Engagement
- Managed Cyber Threat Intel (CTI)
- Managed Hunt and Testing
- Managed Detection and Response (MDR)

Why Choose Booz Allen?

- A globally respected incident response team, trusted by customers, of all sizes and complexities, across all critical infrastructure sectors and regulated environments.
- Extensive experience: more than 1,000 discrete incident response engagements per year.
- More than **300 experienced in-house incident response practitioners** globally, with over 8,000 practitioners across the broader company with relevant skillsets.
- Over **83 cyber insurance panel** appointments.
- We secure **40 of the Fortune 100.**
- OT-Specific expertise and skill sets brought **200+ OT Cyber professionals** including personnel with OT engineering backgrounds and **55+ GICSP and GRID-certified professionals**
- Global footprint, with forensic labs located in the US and UK.
- Deep experience leading responses across a broad range of markets and sectors, including critical manufacturing, health & life sciences, energy & utilities, oil & gas, maritime, logistics, defence, financial services, aviation, automotive, and building management systems (BMS).

Our People

- Highly credentialed and certified digital forensics and incident response experts.
- Forensics practitioners with extensive breach and legal investigation experience.
- Dedicated malware analysts with advanced nation-state and criminal toolset reverse engineering expertise.
- Experienced hunters with offensive and defensive backgrounds.
- Crisis management experts to support organisation-wide response and coordination with the board, regulators, legal counsel, and law enforcement.
- 2 National Security Agency certifications.
- 4 CREST CSIR certifications.

Certified IR Processes & Procedures

- **United States National Security Agency (NSA) CIRA certified** – CIRA accreditation certifies that Booz Allen's IR procedures, processes, and playbooks meet the standards for responding to National Security incidents experienced by our nation's most critical systems.
- **CREST CSIR** – Booz Allen is CREST CSIR accredited meaning our IR processes meet the standards used by many government, educational, and financial institutions throughout the British Commonwealth and beyond.

Languages Spoken

- English
- Albanian
- Dutch
- French
- German
- Greek
- Hungarian
- Polish
- Portuguese
- Russian
- Spanish
- Swedish
- Turkish
- Arabic
- Chinese (Mandarin)
- Hindi
- Japanese
- Swahili
- Tamil (India)
- Telugu
- Urdu (Pakistan)

TO LEARN MORE, CONTACT BOOZ ALLEN:
INCIDENT@BAH.COM

NOTIFY US OF AN INCIDENT
UK/EU IR Hotline: *+44 (808) 296-8080*
U.S./Canada/Global IR Hotline: *+1 (888) 266-9478*