Experience Matters

Incident Response

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

A Comprehensive Approach to Incident Response

Booz Allen provides streamlined incident response solutions to help our clients quickly and effectively plan for, prepare for, and respond to cybersecurity incidents. Our teams leverage timely and actionable intelligence, along with deep analytical insights and a comprehensive business approach, to enable resilience across the organization. Incident response begins before an incident occurs and concludes long after the emergency has deescalated. Our subject-matter experts, with specialized 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 organizational objectives, incident-specific playbooks, and defined roles with escalation criteria, as well as identifying key external partners.

- Financial Impact Assessments
- Critical Systems and Impacts
- Crisis Management Planning
- Geopolitical Threat Analysis
- Compromise Assessment
- Tabletop Exercises and Wargaming
- IR Playbook and Runbook Development
- Penetration Testing

Digital Forensics & Incident Response:

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.

- Evidence Collection and Preservation
- Host, Network and Mobile Forensics
- Database, Cloud, and OT/ICS Forensics
- Insider Threat Investigations
- Threat Actor Communications
- Malware Reverse Engineering
- Incident Containment Support
- Incident Recovery and Remediation
- Ransomware Investigations and Recovery Support
- Crisis Management and Incident Command
- Business Email Compromise Investigations
- Data Mining and Manual Review
- Cryptocurrency Settlement Oversight
- Blockchain Investigations
- Infrastructure Agnostic Threat Hunt
- Emergency Staff Augmentation Support

Post-Incident & Ongoing Support:

Program Enhancements and Optimized Operations

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

- Threat Intelligence Operations
- Continuous IR Intelligence Engagement
- Pre-Paid Incident Response Retainer Services, supporting both IR and proactive engagements without limitation
- Continuous Cybersecurity Testing and Assessments
- Managed Detection and Response (MDR)
- Managed Cyber Threat Intel (CTI)
- Managed Hunt and Testing

Copyright © 2025 Booz Allen Hamilton Inc.

WHY BOOZ ALLEN FOR INCIDENT RESPONSE?

- A globally respected incident response team, trusted by clients, 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.
- Global footprint, with forensic labs located in the US and UK
- Deep experience leading responses across a broad range of markets and sectors, including financial services, health and life sciences, manufacturing, energy, transportation, critical manufacturing, government, defense, commercial facilities, and oil and gas.

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 organization-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

- **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

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

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

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

Booz Allen is the advanced technology company delivering outcomes with speed for America's most critical defense, civil, and national security priorities. We build technology solutions using AI, cyber, and other cutting-edge technologies to advance and protect the nation and its citizens. By focusing on outcomes, we enable our people, clients, and their missions to succeed, accelerating the nation to realize our purpose: Empower People to Change the World®.

Copyright © 2025 Booz Allen Hamilton Inc.