Booz | Allen | Hamilton

MANAGED DETECTION & RESPONSE SERVICES

Today there are a number of nefarious actors that operate with a variety of motivators such as: business disruption, insight into core business practices, theft of sensitive information for financial gain, and many more. At an unprecedented rate, the distinction between threats facing world governments and the boardroom is rapidly blurring. Sophisticated tools can be obtained more easily than ever by attackers and their reach continues to expand. Organizational cyber security events are an inevitability. Booz Allen Hamilton's Managed Detection and Response (MDR) is designed to meet that challenge.

Booz Allen's proven approach to MDR combines attack detection, threat hunting, incident response, and tailored threat intelligence to deliver continuous monitoring and response to cyber threats. This 24x7 threat detection, investigation and response service is delivered through full-packet capture network monitoring, email monitoring, and ENDGAME-powered managed endpoint threat-hunting capabilities. The Booz Allen service is powered by industry-leading analysts, tailored threat intelligence, and NSA-CIRA accredited incident responders to bring your organization deep security tradecraft combined with years of front-line experience.

The Booz Allen Managed Detection and Response Service is delivered in three ways:

- Managed Detection and Response for Network
- Managed Endpoint Detection and Response (Managed EDR™)
- Managed Detection and Response for Email

EXPECTED OUTCOMES

Through the Booz Allen MDR services, your organization will have deep security tradecraft combined with decades of front-line experience. Industry-leading analysts, threat intelligence tailored for the threats against your organization, and National Security Agency (NSA) Certified Incident Response Assistance (CIRA) accredited incident responders power the Booz Allen service.

This results in vastly reduced detection times.
Booz Allen customers experience one-hour mean time to detect threats against an industry average of 214 days.

Comprehensive Visibility

Full packet capture, complete endpoint visibility, and Booz Allen's global industry insights deliver the deep visibility needed to identify and stop known and unknown threats.

Advanced Threat Detection

Proprietary detection capabilities and battle-tested methodologies are used as we combine your existing tools and our own to uncover the most difficult to locate cyber threats.

Complete Analysis

Reduce alert fatigue and improve SOC efficiency with industry leading analysts who investigate every alert and can quickly assess and scope the entirety of an attack.

Full Response

National Security Agency accredited Incident Responders, malware reverse engineers, and our ability to rapidly develop custom detection designed to flush attackers out of all their hiding spots in your environment.

Remediation

Rapid response and containment to each validated threat is performed by a Threat Analyst that is your point of contact through the lifecycle of the remediation effort. The investigation and response efforts are tightly communicated as the Booz Allen team uncovers the full extent of the attack.

Morphing Defensive Postures

Stop the attack and the attacker by staying one step ahead. Booz Allen MDR analysts partner with your security program to monitor and continually tune your organization's defenses based on the threats targeting your company.

CONTACT INFO

Wade Alt
alt_wade@bah.com
+1-202-346-9083

WHAT PROBLEM IN THE MARKET DOES THIS SOLVE FOR?

There are two fundamental challenges in cybersecurity.

1. People. SOC analyst talent shortages and the resulting alert fatigue are well documented. The subsequent selling of fear, uncertainty and doubt further compounds the talent problem by making it seem impossible to fix. Organizations are fighting an asymmetric battle and are often unprepared for an incident.

2. Technology. Limited enterprise-wide visibility prevents organizations from even being able to see potential threats. Complex tools that don't work well together plague the industry. Even on their own, these solutions are difficult to deploy and maintain. This leads to static defenses that do not adapt to the evolving threat landscape.

WHY BOOZ ALLEN MANAGED THREAT SERVICES?

Understanding the history of adversaries and adapting to the evolution of their behavior, techniques, and targets is critical in the ability to understand the current posture of the cyber security space. Booz Allen's MDR provides the unique ability to straddle the commercial and federal markets to accurately predict and address future cyber security issues and get ahead of problems.

We Understand the Threat Landscape

Organizations are seeking clarity, strategy and scalable capabilities during, before and after a cyber security event. Booz Allen Hamilton Managed Detection and Response can create transformative strategies grounded in dynamic adversary intelligence and operational experience. Equipped with the right cyber intelligence and technology mastery, customers across all industries, verticals and sectors can secure their environments and create defensive solutions for the future.

The Strategy & Technology Needed to Stop Today's Advanced Threats

Booz Allen partners with clients to deliver a clear vision and a set of guiding principles that ensure all decisions, strategic to tactical, are in line with ensuring the health of the broader business. Diligently manage enterprise risk through our proven approach combining advanced attack detection, threat hunting, incident response, and tailored threat intelligence. Validated Threat Notifications help you understand the threats you face and execute change across your environment. Never face the same attack twice as our patented software delivers morphing defensive postures.

Our Practitioner Experience & Approach

Security challenges aren't solved with a product alone—they are honed through experience, expertise, and supporting processes. Booz Allen Hamilton has been there. From the earliest days of cyber warfare to the current ever-evolving landscape, the firm has addressed security problems at the highest levels of governments and organizations all over the world. Booz Allen MDR provides the transformative, adaptive approach backed by hands-on experience clients need to fight today's threats.