Reimagine Your Cyber Defense **with AI**

Booz Allen®

Empower Your Security Team with AI-Driven Tools

With the right information at the right time, Security Operations Center (SOC) teams can react quickly to neutralize threats. However, the volume and velocity of alerts, telemetry, CTI and other data feeds, compounded by insufficient staffing, creates significant challenges for most organizations. Automated data enrichment, analysis, and decision support, powered by AI, creates efficiency gains and enables decision making for security leaders and SOC customers alike.

The Modern SOC Struggle

GAPS IN DETECTION
As the number and sophistication of cyberattacks continue to escalate, commercial detection tools often fail to detect the movements of advanced actors like nation-states and hacktivists.

INEFFECTIVE ALERT MANAGEMENT
With a continuous stream of critical alerts, SOC analysts are often overwhelmed and challenged to identify meaningful signals among an overabundance of false positives.

OPERATIONAL INEFFICIENCIES
Cross-referencing historical information, the constant "swivel-chair" between applications, and a lack of integration among teams lead to fatigue and miscommunication.

Reimagining the SOC with AI

REDUCE COGNITIVE LOAD by automatically scoring, filtering, and serving relevant information to the analyst.

REDUCE RESPONSE TIME by providing relevant insights, information, and context.

IMPROVE SOC EFFICIENCY AND INCREASE MATURITY by generalizing defensive capabilities and enabling rapid information gathering.

AI-POWERED INCIDENT ANALYSIS

THE CHALLENGE
Traditional automation techniques focus on particular indicators of compromise (IoC) to detect adversarial presence. While these are easy to implement, they quickly become ineffective as adversaries make frequent, minor changes to IP addresses or malware, for which threat actors are themselves using AI tools. ***Manually rewriting those rules is nearly impossible.*** Plus, many IoCs are identified by a pattern rather than a single value (e.g., domain names combining 20 random characters or encoded commands with too many special characters). While trained analysts can identify these patterns, manual human review causes fatigue and does not scale.

THE SOLUTION
AI-powered solutions can generalize defenses to be less restrictive on the indicator and identify more suspicious patterns. ***We quantify the presence of typical English words in domain names from zero (no English words) to one (very likely one or more English words), which allows analysts to prioritize the information they consider rather than reading every event line-by-line.*** This and many other similar analytics enrich available data to increase efficiency, while also maintaining visibility into the data needed to remediate alerts. Using AI in this way relieves analyst fatigue and reduces alert remediation time.

Copyright © 2025 Booz Allen Hamilton Inc.

Is Your Organization AI-Ready?

AI cybersecurity tools work best when deployed alongside strong foundational cybersecurity practices. They must also be implemented in proportion to an organization's current level of trust in AI/automated solutions. The AI maturity journey, described below, is one where organizations gradually build maturity, and as they do so, will likely identify more ways for AI to accelerate their SOC's efficiency.

Stage 1:
Establishing Cyber Foundations

Functional team structure, operational security workflows, alerting infrastructure, data collection and management

Stage 2:
Introducing AI into Existing Workflows

Available data, backlog of remediated incidents, AI deployment infrastructure, AI governance

Stage 3:
Augmenting Analysis with AI

Defined playbooks, basic automation, feedback loops

Stage 4:
Automating with AI

Understanding of risk, familiarity with automation, advanced tech stack, and automation oversight



BOOZ ALLEN OFFERINGS - CYBER AI IN ACTION

Advanced Analytics Repository

Automates workflows to prepare data for analyst consumption. Includes more than 1,700 Sigma rules and 30 AI models that perform real-time data enrichment to address tactics, techniques, and procedures (TTPs) ranging from beaconing to obfuscated PowerShell.
(Ideal for Stage 2 and above)

Expert Assistance

Introduces AI into existing workflows to spot patterns, eliminate bottlenecks, and facilitate decision making. Replaces manual, repetitive tasks with AI-assisted anomaly detection (e.g., scanning network logs; finding auto-generated filenames and obfuscated command lines).
(Ideal for Stage 3 and above)

Automated Detection Engineering

Uses relevant context (e.g., network diagrams, system documentation, audit data, CTI, etc.) to identify likely attack paths, discover gaps in detection, and provide localized and tailored detection logic and direction for threat hunters.
(Ideal for Stage 4)

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

Why Booz Allen

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.