Staying ahead of malicious and unintentional insider threats with behavior-based detection solutions

EXECUTIVE ORDER (EO) 13587, along with the White House Memorandum on National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, direct all executive branch departments and agencies that have access to classified information to implement an insider threat detection and prevention program. During a time of declining budgets and resource constraints, agencies with varying levels of existing (or non-existent) capabilities face significant challenges in implementing the minimum standards and policy. Some of the standards are easier to implement than others. Training employees on insider threats and reporting responsibilities, for example, is more straightforward than implementing a user activity monitoring capability with trained staff who can detect, monitor, and analyze anomalous events. The latter requirement takes significant time and planning to program for the resources and technology tools required for implementation.

In the private sector, a variety of regulatory compliance laws and audits establish requirements for threat prevention and detection programs. In the healthcare industry, the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act (HIPAA) require the protection of personally identifiable information (PII). Know-your-customer (KYC) guidelines prevent banks from being used, intentionally or unintentionally, by criminal elements for money-laundering activities. Bankers’ access to key information, networks, and systems can provide them with an opportunity to turn a blind eye or knowingly approve an illicit transaction. Organizations must determine if their bankers are conducting transactions within their normal job role and not in collusion with criminals. An organization’s reputation and bottom line can also suffer from the impacts of an insider threat. Failure of internal controls can influence the public’s confidence in an organization’s ability to safeguard their critical information (e.g., credit cards) or result in an organization losing millions of dollars of intellectual property. In order to tackle the resource and implementation challenges associated with these mandates, organizations need a multi-layered solution to detect, prevent, and respond to malicious or unintentional insiders.

“It can take up to 32 months to detect a fraudulent event by an insider.”

–CERT Carnegie Mellon University Insider Threat Study: Illicit Cyber Activity Involving Fraud in the US Financial Services Sector

INSIDER4SIGHT MULTI-LAYERED SOLUTION
Booz Allen Hamilton, a leading strategy and technology consulting firm, can help. Insider4Sight is a multi-layered solutions approach tailored specifically to an organization’s mission, critical assets, and risk profile. Booz Allen’s solution considers the existing maturity of capabilities, desired end-state, analytic tradecraft, IT and data architecture, case management, and training of insider risk staff and the workforce. At the core of our Insider4Sight solution is a tool-agnostic centralized hub where analysts collect and analyze data from host and network sensors and other disparate data sources to make analytic judgments that are escalated to appropriate adjudicative and investigative authorities. Our solution:

INSIDER4SIGHT IN ACTION
By trending contextual data over time against expected role behaviors, Booz Allen’s team of experts reduced the number of false positives for one government client from more than 200 per day to 23 per week, dramatically reducing the number of labor hours required to investigate false positive alerts.
+ Reduces implementation total cost and time by fully articulating a program that addresses insider challenges based on the organization’s mission, critical assets, and risk profile
+ Provides governance and change management best practices to coordinate and integrate key stakeholders as part of a program
+ Enhances detection capability using behavior-based detection tools to identify indicators of potential malicious and unintentional insiders before significant damage might occur
+ Applies tactics, techniques, and procedures (TTP) employing user activity monitoring with the automated baselining of normal network behavior to more quickly identify outliers and events
+ Provides a continuous evaluation data fusion platform to parse through disparate data sources and assign a risk score, ensuring analysts focus on critical alerts and fuse personnel security data
+ Provides a tailorable case management tool with repeatable workflows that ensures the right stakeholders are involved and collected data will stand up to chain-of-custody rules
+ Provides leadership with information that can be used to inform policy and awareness program updates (e.g., continued violations of acceptable use policy items).

### SERVICES

**Program Design Services**
Program Design to assess and establish a roadmap for compliance, taking into consideration organizational risk, change management, governance and the unique environment for which it will be implemented.

**Maturity Assessments & Benchmarking**
Assessing an organization’s insider threat program maturity, by using a reference model to assess risk across people, process and technology dimensions. The maturity model defines functional and components of an insider threat program measured against industry best practices. The result is a baseline maturity score and a roadmap to enhance program maturity.

**Human Analytics Services**
Analytic Tradecraft to apply human intelligence to assess motivation and intent and apply analytic judgment for adjudication, based on tool set collections and contextual data. Near real time alerts are assessed against contextual information resulting in an analytic judgment that is distributed to appropriate stakeholders for disposition.

### TECHNICAL SOLUTIONS

**Data & Architecture Services**
Evaluation of existing applications and available data to establish a baseline technology architecture for an insider threat program. Data fusion to collect and aggregate available data sources and develop algorithms to parse the data in order to generate smart alerts for immediate notification.

**Insider Threat Detection & Response Services**
Managed analytic services to survey your enterprise using a customized alerting dashboard to assess events detrimental to an organization. We continuously update and evolve expected role behaviors, triggers, machine analytics, and analytic tradecraft to increase the probability of detecting bad events while minimizing false positives.

**BEACON**
Automated Workflow and Analytic Environment Workflow and Case Management for repeatable processes that includes data gathering, reporting, and response options, while maintaining chain of custody.

### FOR MORE INFORMATION

**Thomas Chandler**
Principal
chandler_thomas@bah.com
301-821-8968

**Cynthia Lear**
Senior Associate
lear_cynthia@bah.com
301-444-4063

---

**About Booz Allen**

Booz Allen Hamilton is a leading provider of management consulting, technology, and engineering services to the US government in defense, intelligence, and civil markets, and to major corporations and not-for-profit organizations. Booz Allen is headquartered in McLean, Virginia, employs more than 22,000 people, and had revenue of $5.48 billion for the 12 months ended March 31, 2014. (NYSE: BAH)