BOOZ ALLEN AND SPLUNK: EXPANDING THE CYBERSECURITY ECOSYSTEM

In 2013, Booz Allen was evaluating a number of Security Information and Event Management (SIEM) tools for several federal government clients. The goal was to procure a versatile and highly functional security monitoring system to serve as the backbone of the firm's monitoring services. They found their answer in an up-and-coming SIEM manufacturer named Splunk.

This bottom-up approach led to discussions and the two firms quickly identified the benefits of combining the power and flexibility of Splunk's award-winning security tools with Booz Allen's deep operational consulting expertise in cyber engineering, policy, and intelligence analysis.

Booz Allen and Splunk have formed a strategic partnership that delivers highly flexible data analytics and threat intelligence tools to help organizations meet the toughest operational, policy, and compliance demands.

When Booz Allen examines a cybersecurity issue, its analysts take a holistic approach that cuts across multiple lenses:

- ✓ Policy: Experience drafting the nation's cyber policy for defense and homeland security clients provides valuable insight in helping them adhere to federal compliance standards.
- ✓ Analysis: Supporting federal intelligence and law enforcement agencies with real-time and future threat analysis informs customers of the latest tactics and strategies used by threat actors.
- ✓ Engineering: The firm's engineering expertise drives the solutions its engineers develop to deploy the latest technology in manner specifically designed for its client's core mission.

Splunk's analytics-driven security solutions provide a comprehensive approach to cybersecurity, including advanced techniques like machine-learning and behavioral analytics. These techniques help security teams quickly identify, investigate and respond to threats based on a broader security context than is possible with legacy security products.

The two firms are constantly on the forefront of emerging cybersecurity challenges and risks. Merging the best-in-class solutions with a 100-year tradition of intelligence tradecraft provides a living cyber-ecosystem that continually feeds upon, learns, and improves itself.

HUMAN-DERIVED INTELLIGENCE + ANALYTICS-DRIVEN SECURITY = ACTIONABLE THREAT INSIGHTS

Booz Allen Cyber4Sight® for Splunk (C4S) is a security solution with the goal of making analysts not only smarter, but faster.

C4S fuses Booz Allen's human-derived intelligence context from Cyber4Sight's Managed Security Service with the analytic power of Splunk's analytics-driven security to deliver actionable threat insights.

Threat insights allow security experts to detect and mitigate current attacks while preparing for future attacks. With a focus on quality over quantity, analysts can more easily find the right alerts instead of more alerts. Threat insights provide deeper context for managing threats more quickly and anticipating the adversary's potential next moves.

As increasingly sophisticated threats target organizations around the world, these combined insights from Splunk and Booz Allen will equip customers with the detailed information to proactively combat cyber adversaries.

C4S enriches Splunk ES with valuable threat data collected by Booz Allen's diverse group of expert cyber analysts to provide intelligence monitoring services culled from over 170,000 targeted sources from the open and closed internet. Intelligence gained from these sources is fed into C4S, providing customers with a wealth of new information on threat actors and their tactics, techniques and procedures (TTPs). This new platform connects and centralizes profiles of threat actors and their methods in a new online database, which enables customers to more quickly and effectively combat attacks.

With C4S, Splunk ES customers of all sizes gain access to actionable threat intelligence on a subscription basis, while expanding detection, investigation and response capabilities provided by the Splunk security analytics platform. This human-curated, ready-to-use content helps correlate data and events in Splunk ES, enabling actionable intelligence for a wide range of security scenarios. As increasingly sophisticated threats target organizations around the world, these combined insights from Splunk and Booz Allen will equip customers with the detailed information to proactively combat cyber adversaries.

JOINT OPERATIONAL TECHNOLOGY SOLUTIONS

Electricity, water, and large manufacturing plants all have one thing in common: They are operated and managed by industrial control software (ICS). One of the highest concerns of federal officials is the growing number of cyberattacks and penetrations against the corporate offices and plants that run our nation's infrastructure. Recent analysis shows a record-breaking number of incidents involving ICS operators occurred in the last two years. Analysts predict the number of attacks are likely to increase at the hands of nation-states and cyber criminals.

In today's threat landscape, understanding the impact an attack could have on your system and how to prevent it is critical. This solution provides multiple operational views in addition to visibility into specific OT-Sec use-cases that have been identified in the majority of cyber attacks. The data derived is analyzed using anomaly detection and other algorithms in order to identify when attackers attempt to gain network access, perform reconnaissance, and eventually conduct attacks.

SECURING THE FEDERAL GOVERNMENT'S NETWORKS

Booz Allen has teamed up with Splunk in the development of the Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) program. Here the two firms joined forces to improve the resilience of more than 4 million devices across 66 federal departments and agencies. Booz Allen's CDM solution—selected to cover more than 80% of these devices—uses Splunk technology to raise awareness of the cybersecurity risks each agency faces.

For the first time, the deployment of the CDM program gives security managers and directors the ability to provide ready answers to the questions: "Where am I vulnerable?" and "What is my highest risk?"

The program has three primary goals, identifying:

1. What devices are on the network.
2. Who's using them.
3. What type of activities are being conducted on the entire network.

The data collected as part of this process is used to calculate a cybersecurity "risk score" for each participating agency. The program identifies cyber risks continuously, prioritizes them based on potential impacts, and mitigates the most significant problems first.

Splunk platforms store the Master Device Record (MDR) that keeps the data from each tool synchronized, offering a single 'record of truth' about what is on the network. Booz Allen's solution identifies each network-connected device and stores current characteristics about each device, regardless of where the device is located on the network.

PROVIDING A MISSION-CENTERED FOCUS TO CYBERSECURITY

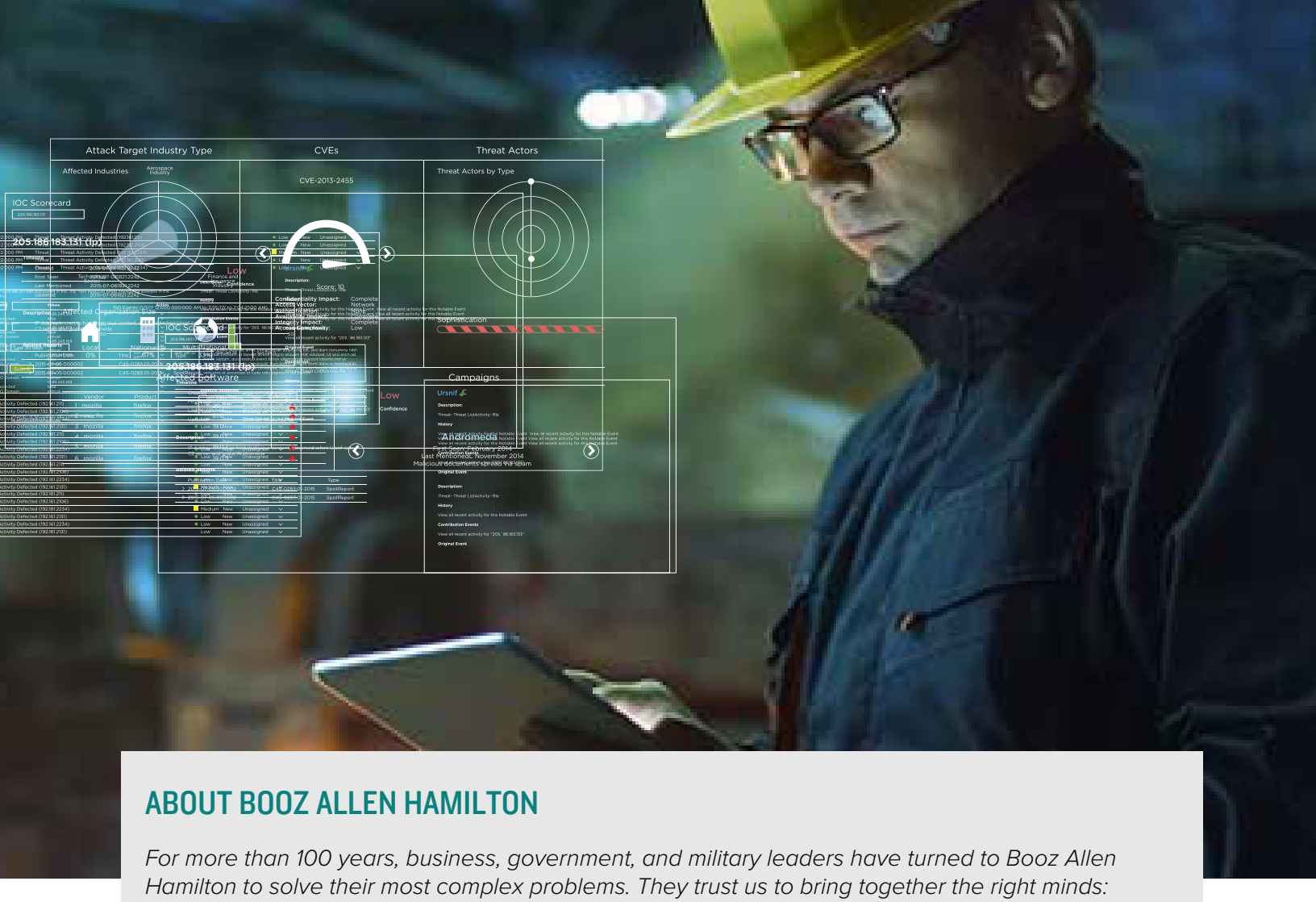
Every SOC faces the same dilemma: The ability to detect security events far outpaces the human resources available to respond. Every organization makes a careful calculation of which security events are important to investigate, and which events to drop.

Booz Allen holds deep experience in the operational discipline of cybersecurity. The firm's analysts understand the full scope of the cyber environment—from risks to threats—their clients are facing. The firm's long history and close working relationships with military services and defense agencies has created a mission-focused culture that provides substantial benefits when transferred to clients in the commercial sector. For Booz Allen, it's not just about information technology—the computers, networks, and web pages of a client. It's about understanding, measuring, and studying all the various factors that could impact an organization's primary operations.

Every cybersecurity consulting firm provides some level of basic protection services to its clients. Booz Allen, however has extensive experience helping clients solve very unique operational use cases. These can range from building a custom protection platform with Splunk ES designed to monitor or protect complex manufacturing controls, the internet of things (IOT), or applied systems that require unique, specialized knowledge.

Booz Allen has helped advanced clients deal with intricate insider-threats, mergers and acquisitions (M&A), or divestitures requiring custom-made tools to quantify and monitor unique variables. New-use cases have included harnessing new or unintended uses for the highly flexible monitoring capabilities of Splunk, such as layering SIEMs to monitor and evaluate operations of a nuclear launch facility or oil and gas supply chains.

Booz Allen recently devised a system to correlate certain sets of client-tailored rules to aggregate risk into a more complete picture. This unique exercise enabled the client to identify a significant insider threat and take actions to prevent a high-risk event.



ABOUT BOOZ ALLEN HAMILTON

For more than 100 years, business, government, and military leaders have turned to Booz Allen Hamilton to solve their most complex problems. They trust us to bring together the right minds: those who devote themselves to the challenge at hand, who speak with relentless candor, and who act with courage and character. They expect original solutions where there are no roadmaps. They rely on us because they know that—together—we will find the answers and change the world.

We solve the most difficult management and technology problems through a combination of consulting, analytics, digital solutions, engineering, and cyber expertise. With global headquarters in McLean, Virginia, our firm employs more than 23,300 people and had revenue of $5.80 billion for the 12 months ended March 31, 2017. To learn more, visit BoozAllen.com. (NYSE: BAH) To learn more about Cyber4Sight, visit https://www.boozallen.com/s/product/cyber4sight.html.

ABOUT SPLUNK

Splunk Inc. (NASDAQ: SPLK) is the market leader in analyzing machine data to deliver Operational Intelligence for security, IT and the business. Splunk® software provides the enterprise machine data fabric that drives digital transformation. More than 13,000 customers in over 110 countries use Splunk solutions in the cloud and on-premises. Join millions of passionate users by trying Splunk software for free: http://www.splunk.com/free-trials.