SPLUNK AND BOOZ ALLEN HAMILTON: FUSING HUMAN INTELLIGENCE WITH ANALYTICS SECURITY TO DELIVER ACTIONABLE THREAT INSIGHTS.

A new generation of advanced cyberthreats pose increased challenges and risks for today's security analysts. Advanced persistent threats, ransomware, intrusions on enterprise networks, and point-of-service attacks, to name a few, are becoming greater in number and sophistication. The increasing attack tempo forces analysts to spend more time sifting through the mounting number of alerts on their systems. As they work to differentiate false positives from real attacks, chances increase that a truly dangerous piece of malware will slip through the cracks.

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

Splunk and Booz Allen Hamilton have partnered to provide a more powerful solution for prioritizing the array of cyber threats facing organizations. Booz Allen's Cyber4Sight® for Splunk (C4S) is a security solution with the goal of making analysts not only smarter, but faster.

C4S seamlessly fuses the best of two worlds—human-derived intelligence from Booz Allen and the power of analytics-driven security from Splunk—to deliver actionable threat insights.

Booz | Allen | Hamilton

BOOZ ALLEN
CYBER4SIGHT
FOR SPLUNK

splunk>

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.

SEAMLESS INTEGRATION

Leveraging Splunk's Adaptive Response Framework and Booz Allen's rich, full-context, readable threat information, C4S automatically correlates data and events in Splunk Enterprise Security (ES), an analytics SIEM, to operationalize intelligence and turn alerts into action. Curated context is accessible within the SIEM with the touch of a mouse. Analysts no longer have to pivot into another portal, conduct time-consuming research, or manually integrate external intelligence into their dashboard, saving Splunk customers significant amounts of time.

HUMAN-DERIVED INTELLIGENCE

People are what set C4S apart. Its number one differentiator against competitors is that knowledgeable and experienced analysts are creating intelligence based on the traditional intelligence cycle. C4S's human-derived intelligence provides insights on the latest attacks and campaigns. A diverse group of analysts evaluate how those campaigns have evolved over time. Every single alert and every piece of information is processed by highly experienced human hands.

ACTIONABLE INTELLIGENCE REPORTS

Actionable context is provided on bad actor types, their sophistication, campaign information, malware family tactics, and behaviors—allowing analysts to understand the motives for today's attacks as well as where they might strike next. Industry-specific daily and monthly reports detail the most recent campaigns from nation states, hacktivist groups, and criminal syndicates. These reports go beyond arbitrary risk scores and provide detailed threat-actor context connecting indicators to adversaries and their intent. The combination of detailed intelligence reports, tactics, techniques, and procedures (TTPs), indicators of compromise (IOCs), and other types of threat-centric context allows subscribers to prioritize, anticipate, and take action on the most urgent threats. C4S provides actionable intelligence across the full spectrum of cyber threats and the unique motivations of bad actors.

With a focus on quality over quantity, analysts can more easily find the right alerts instead of more alerts.

CURATED IOCS

C4S gives analysts the ability to instantly match IOCs to guard systems against all the different types of malware that could impact enterprise networks and systems. Vetted IOCs available include: IP addresses, domain names, file names, file paths, hashes, YARA signatures, mutexes, strings, URLs and URIs from over 170,000 targeted surface web sources, 400 dark web sources, and beyond.

DETAILED TTPS

Thorough context on the latest TTPs is provided in C4S. Data on specific types of malware, adversaries, and the latest campaigns is augmented with threat context provided by a diverse team of analysts with native fluency in nearly 20 languages. C4S is comprised of intelligence analysts, incident responders, computer forensics experts, malware reverse engineers, journalists, linguists, academics, anti-fraud specialists, private investigators, lawyers, and former law-enforcement professionals.

API INTERFACE

C4S automatically integrates the full spectrum of Booz Allen's intelligence data to provide a more robust SIEM platform. The API interface is an always-available access point to connect and download intelligence feeds to populate the Splunk dashboard on a continuous basis.