ANTICIPATORY AND ACTIONABLE INTELLIGENCE TO FIGHT ADVANCED CYBER THREATS

CYBER4SIGHT®

Predictive Threat Intelligence Services
Cyber attacks are evolving faster than organizations can mount effective defenses

Advanced threats are increasingly targeting corporations and government agencies with industrial espionage, undermining business operations, and sabotaging critical infrastructure. Most organizations rely on static defenses that identify known vulnerabilities and then fix them one by one. This is a reactive strategy where they wait to be attacked and are locked into a never-ending react-and-fix loop. This is an inefficient and antiquated approach. It can’t keep up with threat actors who are too fast, too many, and too sophisticated for static defenses alone.

An effective security posture requires anticipatory intelligence to enable an organization to remain ahead of these threats, assess risks, and take appropriate defensive actions—before an attack actually occurs. Cyber4Sight® products and services from Booz Allen Hamilton provide proactive, predictive threat intelligence from the world’s leader in cybersecurity. With probability-based warnings of future cyber attacks, your organization is able to anticipate an attack and understand the chances of an attacker’s success. This actionable threat intelligence enables an organization to take defensive action before the attack occurs.

Primary benefits include avoiding the cost of data recovery and remediation, enterprise brand damage, and the theft, destruction, and public release of critical information.

Preparing for advanced cyber threats
COMMODITY SERVICE PROVIDERS OFFER GENERIC REPORTS OF VULNERABILITIES THAT MIGHT (OR MIGHT NOT) AFFECT AN ORGANIZATION’S CYBER ASSETS

Cyber4Sight solutions are uniquely differentiated due to their predictive nature. Cyber4Sight services quickly tailor and deliver anticipatory threat intelligence by collecting and analyzing the motivations, intentions, objectives, and capabilities of specific threat actors who pose a risk to your enterprise. The threat actors may include nation states and their proxies, hacktivist groups, crime syndicates, and rogue insiders. Cyber4Sight services are built on decades of Booz Allen’s intelligence analysis and cybersecurity experience derived from close partnerships with federal government agencies and commercial clients. Three differentiators provide your organization with “headlights in the dark” guidance.

THE CYBER4SIGHT DIFFERENCE: FAST, FOCUSED ALERTS OF PENDING ATTACKS

OUR PROPRIETARY DATA SUPPLY CHAIN DELIVERS REAL-TIME CYBER THREAT & RELATED DATA

REAL-TIME DATA FEEDS TO MONITOR

16
LIVE SOCIAL MEDIA FEEDS. (Facebook, Twitter, YouTube, etc.)

166k
REAL-TIME FEEDS AND DIRECTED COLLECTION FROM PROPRIETARY AND OPEN SOURCES, including blogs, forums, news sources, and IRC channels in multiple languages

89m+
MALWARE

87m+
UNIQUE IP ADDRESSES

300m+
NETWORK ACCESS POINTS

50m+
MALICIOUS URLs

90k
KNOWN MALICIOUS THREATS

CLIENT-SPECIFIC NETWORK DATA

20+ Countries
SECURITY EVENT MONITORING (SEM) SENSORS DEPLOYED GLOBALLY TO DETECT INDICATORS OF COMPROMISE (IOC)
I: TRADECRAFT-DRIVEN INTELLIGENCE ANALYSIS

We deploy Booz Allen’s industry-leading tradecraft to detect, collect, and analyze real-time threat actor activities using highly experienced intelligence analysts, native language linguists, and socio-cultural analysts. Our vast team operates 24/7, year-round in a state-of-the art Cyber Fusion Center. Operating in the Deep Web environment, we assess the risk and rapidly provide anticipatory threat alerts enabling a client to take appropriate defensive actions immediately. Cyber4Sight services analyze an organization’s dynamic attack surface as a threat actor would. Our holistic, integrated, and actionable insights provide the client with a dynamic defensive solution against high-risk, high-consequence cyber threats. Cyber4Sight links external human intelligence with technical intelligence derived from a client’s network environment. Our advanced analysis uses behavioral-based detection within our proprietary algorithms to analyze an organization’s network data such as network traffic, server logs, web cache/proxy, firewall data, and mail services. Cyber4Sight services use all these data sources to “connects the dots” and determine whether threat actors are present within the client’s environment—or if they may be in the beginning stages of an advanced attack. All alerts are specific and immediately actionable.

2: AUTOMATING RAPID DELIVERY OF ALERTS

Speed is a major benefit of Cyber4Sight services. Typical threat intelligence services provide generic vulnerability alerts days after a potential threat arises. Cyber4Sight services, however, provide operationally specific contextual intelligence, often within minutes of discovery. Our services accelerate analysis and alert delivery thanks to Booz Allen’s multi-million dollar investment in a real-time, global intelligence collection and analysis system. Advanced automation and visualization capabilities enable our intelligence analysts to quickly identify emerging threats specific to our clients in near real time. Our goal is providing clients with the shortest possible time to discovery and notification of threats that matter most.

3: CLARITY WITH BIG DATA ANALYTICS

With access to a client’s internal network data, our alerts and warnings become more targeted and effective. We maintain and continuously update a library of algorithms to detect patterns of anomalous behaviors and evidence of a threat actor’s presence inside of a client’s networks. This creates the analytic speed needed to keep pace with advanced persistent threats as they rapidly evolve. Our big data analysis answers the “so what” and “why should we care” questions, making the alerts and warnings concrete and highly actionable. These differentiators allow our products and services to provide an organization with an early warning capability at a fraction of the cost of building a comparable intelligence analysis center internally.

OUR BIG DATA ANALYSIS ANSWERS THE “SO WHAT” AND “WHY SHOULD WE CARE” QUESTIONS.

This makes alerts and warnings highly actionable.
CASE STUDY

Global Financial Institution Repels Frequent Distributed Denial-of-Service Attacks

+ **Problem**—A global financial institution had a deep bench of in-house talent but needed a cyber defense system that could better identify, analyze, and prioritize cyber threats. The goal was to cost-effectively reduce risk and protect its customers’ sensitive data, particularly from frequent Distributed Denial-of-Service (DDoS) attacks causing millions of dollars in lost revenue and damages.

+ **Solution**—Cyber4Sight Threat Alert and Warning Services

+ **Results**—Prior to engaging Cyber4Sight services, the cost of a single DDoS attack was $129.6 million on one day. Now, early detection and warnings significantly mitigate the impact of DDoS attacks and deliver further immeasurable benefits by preventing future breaches. In addition, Cyber4Sight services have allowed the client to better use its in-house staff, saving the company more than $1 million annually in cyber threat intelligence collection, analysis, and timely warning.

CASE STUDY

Global Financial Institution Defends IP and Trade Secrets with Cyber4Sight services

+ **Problem**—A global enterprise services firm with large-scale government and commercial clients was stung by a string of network breaches that undermined its intellectual capital and market reputation. The client’s reactive cyber defense posture provided no intelligence to prioritize resource allocation and thwart dangerous threats that compromised its networks.

+ **Solution**—Cyber4Sight Threat Alert and Warning Services

+ **Results**—In the first four months, Cyber4Sight services delivered more than 100 serialized threat intelligence summaries and 700 analytic insights. Daily threat intelligence briefings helped guide the client’s ongoing tactical operations, fostering an anticipatory approach that exponentially decreased cyber events. The insight provided by Cyber4Sight services now allows the client to prepare for major cyber events before they occur, saving billions of dollars in lost Intellectual Property (IP) and brand equity.
DIRECT BENEFITS FOR FINANCIAL SERVICES

Financial services companies are a primary target of organized criminals and hackers. A cyber breach can harm the reputation of a financial services firm, lower consumer confidence, and trigger massive losses. Predictive intelligence provided by Cyber4Sight services helps companies to effectively manage key risks to financial services.

PREVENT EXPOSURE OF PII AND IP:
The loss or theft of confidential information is a major risk. This includes Personally Identifiable Information (PII) of customers and a company’s Intellectual Property (IP). Actionable, predictive intelligence from Cyber4Sight services helps prevent unauthorized exposure of confidential data.

ENSURE COMPLIANCE:
Financial institutions operate under strict regulations for cybersecurity. Cyber4Sight services will help enterprises comply with regulations by providing data that confirms when specified controls are operating in accordance with federal requirements.

PROTECT BUSINESS CONTINUITY:
Denial of Service (DOS) attacks can block customers from accessing their accounts and processing financial transactions. Cyber4Sight services provide advance warnings of specific DOS attacks that allow a company to take preventative action and ensure continuity of operations.

AVOID COSTS:
As a managed service, Cyber4Sight enables significant cost avoidance while providing more scale, depth, and breadth of capability than creating a comparable internal resource. The cost of data feeds alone often exceed $1 million a year, not including the costs of sustaining 24/7 operations with a large crew of subject matter experts in security analytics, linguistic, and socio-cultural analysis.

Learn More
With Cyber4Sight services, your organization will receive actionable intelligence of future attacks in near real time. Our solutions will provide your organization with an early warning capability at a fraction of the cost to build a comparable intelligence analysis center internally. Cyber4Sight services provide anticipatory cyber threat situational awareness, serving as your organization’s “headlights in the dark” to avoid tactical or strategic surprise.

For More Information

SHADE SANFORD
Vice President
Sanford_Shade@bah.com

CHARLES AUDET
Senior Associate
Audet_Charles@bah.com

PATRICK NAGEL
Senior Lead Engineer
Nagel_Patrick@bah.com
About Booz Allen

Booz Allen Hamilton has been at the forefront of strategy and technology for more than 100 years. Today, the firm provides management and technology consulting and engineering services to leading Fortune 500 corporations, governments, and not-for-profits across the globe. Booz Allen partners with public and private sector clients to solve their most difficult challenges through a combination of consulting, analytics, mission operations, technology, systems delivery, cybersecurity, engineering, and innovation expertise.

With international headquarters in McLean, Virginia, the firm employs more than 22,500 people globally, and had revenue of $5.27 billion for the 12 months ended March 31, 2015. To learn more, visit www.boozallen.com. (NYSE: BAH)

© 2016 Booz Allen Hamilton Inc.
c.01.059.18
02/24/16