The Game Has Changed

Global, social, and mobile interconnectivity has changed the nature of cyber threats. In addition to hactivists intent on mischief, sophisticated and organized criminal groups, terrorists and nation-state adversaries are increasingly targeting organizations, corporations and governments to conduct industrial espionage, undermine operations, and sabotage infrastructure. Adding more and more tools is no longer sufficient to protect a global enterprise — adversaries are too many, too fast and too sophisticated.
An Integrated Perspective

To address this challenge, Booz Allen has developed a comprehensive approach that helps clients anticipate, prevent, detect and respond to global threats with real-time actionable insight about their enterprise — internally, externally, globally and socially — so they can take action to be ready, to manage risk, to protect assets and to thrive. By proactively anticipating and preventing critical attacks from happening or from reaching their full objectives; organizations can significantly lessen the negative impacts of a successful attack.

<table>
<thead>
<tr>
<th>THREAT INTELLIGENCE</th>
<th>OPERATIONAL INTELLIGENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>// How do I identify salient threats to my global operations, executives and workforce?</td>
<td>// How compliant is our cyber security and supply chain vulnerabilities program with emerging regulations?</td>
</tr>
<tr>
<td>// How do we anticipate future attacks and take defensive actions before the attacks occur?</td>
<td>// What type of cyber incidents or breaches do we detect in a normal week?</td>
</tr>
<tr>
<td>// How can I detect subtle but potentially violent shifts in local threat environments?</td>
<td>// How trained is our workforce to prevent, detect and respond to a cyber breach?</td>
</tr>
<tr>
<td>// How can we provide timely, actionable intelligence to executive decision makers?</td>
<td>// What is the status of my incident response activities and are we ready and prepared?</td>
</tr>
</tbody>
</table>
Intelligence-Driven Operations

Booz Allen’s integrated “intelligence to operations” lifecycle combines anticipatory threat intelligence and actionable insights with real-time security resources and a rigorous method of mitigating cyber risks. This holistic approach combines specialized tradecraft, big data & analytics, technology and workforce solutions to pro-actively protect clients inside the firewall, outside the firewall and across the enterprise.

OUTSIDE THE FIREWALL

Threat Intelligence
Threat Actors
Actionable Insights
Early Detection

INSIDE THE FIREWALL

Command and Control
Malware Detection
Breach Response
Risk Management
Policy Compliance

Access timely and accurate threat intelligence to pro-actively inform cyber operations from boardroom to control centers

Threat readiness and incident response solutions to actively secure data, networks, and operations across the enterprise.
Threat Intelligence Solutions

OUTSIDE THE FIREWALL

CYBER4SIGHT THREAT INTELLIGENCE

Cyber4Sight

Cyber4Sight™ Threat Intelligence products and services use open-source data feeds to collect and analyze global cyber threat information, cyber security incidents and trends, with native language linguistic and socio-cultural analysis to discover threat actor activities, plans and capabilities.

CYBER4SIGHT SERVICES

// SCARAB
Open-Source Information Research and Investigation System

// DIGS
Digital Information Gathering Systems

// OSIRIS
Open Source Information Research and Investigation System

CYBER4SIGHT PRODUCTS

// Trip-Wire Alerts
Warning of highly-probable future attacks

// Situation Reports
Follow-up reporting for each Trip-Wire Alert

// Spot Reports
High-interest threats, vulnerabilities and exploits

// Summary Products
Daily, Weekly & Monthly Summary Products

// Specialized Studies
On-demand in-depth analysis

CYBER4SIGHT KNOWLEDGE REPOSITORY

ThreatBase

ThreatBase™ Web-based knowledge repository for queries linking thousands of cyber threat “objects” for trend and pattern analysis, enabling aeCERT intelligence analysts in executing their day-to-day operations.
CyberReady Threat Solutions

INSIDE THE FIREWALL

CYBERREADY PLATFORM

CyberReady
CyberReady™ products and services enable clients to pro-actively anticipate and prioritize threats, and take pre-attack defensive actions to maintain an effective security posture. All CyberReady services are mission-specific solutions tailored to IT infrastructure priorities, leverage existing software, and invest in the places of highest vulnerability.

CYBERREADY PRODUCTS & SERVICES

DASHBOARDS
// C-Suite Dashboards
What are the key risks?
How compliant is my organization to my Cyber policies?
How should a specific external threat be handled?

// Analyst Dashboards
What are my top vulnerabilities?
Is everything configured correctly?
What is running on my network?

// IF/AFR Dashboards
What is the status of my incident response activities?
What assets have been compromised?

CYBERREADY ADVANCED ANALYTICS

CyberReady ingests, fuses, and stores internal and external threat intelligence with telemetry from IT infrastructure to create all-source data for real-time situational awareness.

HOST & NETWORK SENSORS / NETFLOWS & PCAP / SIEM & IDS FEEDS / COTS TOOLS DATA / APT SCANS / EXTERNAL INDICATORS / APPLICATION TELEMETRY / DIGITAL FOOTPRINTS / EXTERNAL SOURCES

KNOWLEDGE REPOSITORY

ThreatBase
ThreatBase™ Web-based knowledge repository for queries.
Integrated Results

Booz Allen’s “intelligence to operations” lifecycle provides end-to-end solutions that protect organizations. We create partnerships with our clients, developing long-term solutions and programs that are suited to your specific needs. Let us show you how we can apply leading experience and tradecraft to your organization — to protect your IT infrastructure, get better value from your existing software, and invest in the places where you are most vulnerable.