BAE SYSTEMS
INSPIRED WORK

BAE Systems Business Defense
2017

The evolution from cyber security to business defense

Businesses today find themselves overwhelmed with the breadth and depth of investment they need to make to keep pace with today's evolving cyber threat landscape:

Threat Intelligence - to provide situational awareness and to help prepare defenses

Security Technology - to prevent known attacks across as many areas as possible

Around-the-Clock Monitoring Capability - to detect unknown attacks and stop breaches

Well Developed and Rehearsed Response Plans - to minimize the impact of attacks

Combatting the full spectrum of cyber threats isn't possible for start-ups or amateurs. At BAE Systems we take a different approach to traditional security vendors. We approach information security using the same techniques, analytics and intelligence we pioneered to defend nations and we view them as a system. We bring experience at military-class levels to defend corporate assets. We call this Business Defense.

The nature of the threat has changed. Cyber threats no longer just come from mischievous hackers playing games. They come from organized, smart, well-funded criminal groups and nation states, looking to steal intelligence and capital from businesses of all sizes.

We achieve Business Defense for our clients through a combination of on-premise software, SaaS-based solutions, managed security services as well as cyber advisory and technical services, always deployed for each individual customer's need. Organizations can no longer rely on point solutions, they must consider a more holistic view that encompasses all aspects of their cyber security. Business Defense breaks this down into four critical objectives: Prepare, Protect, Monitor and Respond.

	Managed Security Services	Threat Analytics	Threat Intelligence Management	Email Security	Cyber Consulting
PREPARE	⊗		⊗		⊗
PROTECT	⊗	⊗	⊗	⊗	⊗
MONITOR	⊗	⊗	⊗	⊗	
RESPOND	⊗	⊗	⊗		⊗

BAE Systems spends over $200m each year on cyber security research and development to stay in front of the evolving threat landscape

Business defense solutions and services

For decades, BAE Systems has been defending the largest, most targeted businesses and nations against advanced threats in both the digital and physical world. We have a well-developed pedigree in cyber security and provide solutions and services across the globe that defend many different types of businesses against today's cyber-attacks. We offer a comprehensive set of products and services that uniquely position BAE Systems to provide nation state level defense to commercial organizations.

SOLUTION AREA	SOLUTION / COMPONENTS	CAPABILITIES / BENEFITS
Managed Security Services (Security Monitoring, Security Device Management, Managed Detection and Response, Threat Hunting, Remediation Recommendations)	Available with regional data residency, we manage and monitor security infrastructure from dedicated 24x7 Security Operations Centers, or alleviate the pressure on security departments in areas where help is needed. Managed Security Services eliminate the need to staff an internal security team around the clock. Our team handles complicated device updates and configurations, freeing up IT teams to focus on strategic business activities. Security analysts utilize advanced techniques including event correlation, data mining, and behavioral modelling to detect complex threats that are difficult for in-house teams to discover. We help customers to enhance and develop their security operations in line with their unique business challenges and security objectives. Our experience protecting thousands of customer environments enables us to identify and quickly react to emerging security threats. • **Monitoring:** Collects and analyzes data from any directed source including logs, events, network traffic and feeds from security and network equipment, endpoints, servers and cloud. Monitoring of security devices and logs to ensure the integrity of these systems and regular reporting for regulatory compliance, including PCI, GLBA, NERC CIP and HIPAA. Alerts are triaged and investigated based on the unique risk profile of the customer. • **Management:** Improves operational efficiency, reduces redundant security technology investment, and provides better protection coverage. Collects and analyzes log data to understand your network, finds known weak points in your system before an attacker can exploit them, and ensures network infrastructure functions as designed, continuously, efficiently, and always up to date. Information is retained for compliance needs and further investigation into potential incidents. • **Managed Detection and Response**: Integrates, collates, and correlates network, endpoint, and cloud data sources and applies complex rules and analytics for detection of known and unknown threats. This extended version of our Threat Analytics capabilities (delivered as a managed service) protects organizations from advanced attacks efficiently without the typical costs associated with creating a large data repository and staffing an advanced attack detection team. • **Threat Hunting:** Allows analysts to hunt for threats in a multi-source data repository to expose hidden activities which are an indication of compromise. • **Remediation Recommendations:** Provides remediation advice for all incidents, and hands-on assistance for response to serious threats.	• Complete endpoint-to-cloud visibility and response capability • Coverage of biggest cloud vendors - AWS, Azure, O365 • Full coverage or IaaS as if it was on-premise • Comprehensive authentication and access monitoring for rogue account detection • Dedicated, proactive and continuous approach to Threat Hunting • Integrated incident response from qualified, certified response experts • Dedicated big data and managed SIEM platform

SOLUTION AREA	SOLUTION / COMPONENTS	CAPABILITIES / BENEFITS
Threat Analytics (Threat Analytics, Threat Intelligence Management)	Security Analytics helps organizations to detect new, advanced or targeted attacks that are evading current security controls and reduce the time and resources required to investigate and respond to these attacks. Our threat analytics engine enhances a company's ability to process massive amounts of data, detecting real cyber threats and generating customizable alerts that facilitate the rapid investigation of attacks. • **Threat Analytics (BAE Systems Security Analytics solution):** The application of advanced analytics across data on a massive scale to automatically detect threats. The solution generates customizable alerts on anomalous network activity – indicative of known, new, and evolving threats – and presents them for investigation by your existing team of security analysts. The investigator GUI provides contextual data and visualization tools that enable analysts to triage and investigate alerts quickly and report on their findings. • **Threat Intelligence Management (TIM):** Translates threat information from both internal and multiple external threat data sources into intelligence upon which one can act. Information is presented in the Investigator GUI to provide context for SOC analysts. This additional perspective on both the nature and details of threat actors and their preferred techniques helps the organization prepare, protect and respond to specific threats.	• We provide unique protection based on our insight into attack behaviors from our experience with tier 1 financial companies, nation states, our enterprise MSS and internal SOCs • Our analytics reduce risk by finding hidden threats at multiple stages of the attack kill chain • The prioritization and context we provide with alerts streamlines the time and effort required in investigations • Operationalized threat intelligence speeds detection, investigation and response activities
Email Protection Services (Zero Day Prevention, Insider Threat Prevention, Email Data Loss Prevention, Email Encryption, Email Security (AV/AS), Email Compliance Archiving, Email Continuity)	BAE Systems helps organizations of all sizes defend against the most popular threat vector – email. Our Email Protection Services (EPS) are fully integrated, easily controlled with a unified and intuitive security management console, and provide organizations with full security and control over inbound and outbound corporate messaging. • **Zero Day Prevention:** Defends against targeted attacks, spear phishing, and advanced zero-day exploits by identifying and defeating unknown and not-yet known malware. Applies advanced techniques to detect and prevent attacks, even without signatures and provides protection at click time by rewriting URLs • **Insider Threat Prevention:** Helps guard against motivated malicious insiders and accidental negligence by employees to greatly reduce corporate data loss. Includes industry-specific policy packs to help with the compliance of GLBA, HIPAA, and PCI DSS for hardened protection against confidential and proprietary information loss • **Email Data Loss Prevention:** Blocks or encrypts sensitive, inappropriate, and risky messages with advanced content filtering and DLP capabilities • **Email Encryption:** Intuitive policy-based and user level message encryption • **Email Security (AV/AS):** Reduces risk exposure and corporate liability by safeguarding email with anti-virus and anti-spam technologies that block known malware and spam at the gateway • **Email Compliance Archiving:** Comprehensive eDiscovery, archiving, and mobile archive access • **Email Continuity:** Always available email access and usage – even when email server is down	• Our inline approach is faster and provides a better end user experience than traditional out-of-band sandboxing • Unlike appliance vendors, our service can't be reverse engineered and exploited • We provide customizable policy and workflow capabilities to match customer needs • EPS is part of a broader portfolio including world class threat analytics, intelligence and response capabilities

SOLUTION AREA	SOLUTION / COMPONENTS	CAPABILITIES / BENEFITS
Cyber Consulting and Services (Strategy/Advisory Services, Technical Services and Testing, Incident Response Services, Threat Intelligence)	The BAE Systems consulting team provides a range of strategic, technical and incident response services to help organizations prepare, protect and respond. • Strategy/Advisory Services: Includes program evaluations, risk assessments, compliance reviews and gap analysis, as well as improvement plans and implementation assistance as required. • Technical Services and Testing: Security architecture assessments and various types of testing ensure that products, applications and networks are sufficiently robust to cope with cyber threats. Penetration testing allows comprehensive and relevant recommendations to be produced which enable organizations to determine the best way to readjust or allocate resources to further enhance their protection and more effectively mitigate those vectors susceptible to attack or any other identified gaps in protection. • Incident Response Services: We offer a full range of expert Cyber Incident Response services to both help organizations develop plans or to enable companies to act rapidly and effectively once an incident is detected. We combine technical skills with strategic guidance to make sure an organization makes the right decisions at the right times to limit the impact of attacks. • Threat Intelligence: Our cyber threat intelligence team investigates and tracks cyber-attacks against organizations around the world. From this we build rich profiles of high-priority threat actor campaigns – which we continuously update as new information is obtained. Threat Intelligence customers receive technical data feeds and contextualized reports via a secure portal to enhance threat detection and provide greater situational awareness. We also support additional methods including STIX and TAXII.	• We are CREST and CBEST certified and provide threat intelligence services to regulated financial institutions as well as a broader set of commercial and government organizations • BAE Systems is certified to provide cyber incident response services to government, critical national infrastructure and other operators of nationally significant networks

For more information on our Business Defense solutions and services please visit:
www.baesystems.com/cybersecurity

We are certified to ISO27001, the international best practice standard for an Information Security Management System (ISMS)

Accreditations

Through our involvement with some of the world's largest and heavily targeted operating environments, we understand the importance of consistency and reliability in delivery. To support this reliability, we have invested heavily in our people, processes and infrastructure, and currently hold the following accreditations:

- We are certified to ISO27001, the international best practice standard for an Information Security Management System (ISMS)
- We hold PCI-DSS Qualified Security Assessor (QSA accreditation)
- We are certified to BS25999, the international standard for the requirements for a Business Continuity Management System (BCMS) for all our services
- We are part of CLAS – the CESG Listed Advisor Scheme for Security Practitioners into HM Government. CLAS was created by approving a pool of high quality consultants to meet the increasing demand for authoritative Information Assurance advice from Government Departments and other organizations. All CLAS Consultants hold a formal HMG Security Clearance (a min of SC)
- Part of a select group of CREST Approved companies, we are certified by CREST to provide global penetration testing services. In the UK CREST works closely with both CESG and the CPNI and their individual ethical hacking qualifications are now recognized by the CESG CHECK scheme as well as being used by the US government as part of the NIBSE training academy
- We are certified by CESG and the CPNI as a quality-assured cyber incident response provider, as part of their Cyber Incident Response Scheme. The scheme is a UK HMG quality-assured service provided by industry that organizations can turn to for assistance when they have suffered a cybersecurity incident

We are BAE Systems

At BAE Systems, we provide some of the world's most advanced technology defense, aerospace and security solutions.

We employ a skilled workforce of 82,500 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, protect people and national security, and keep critical information and infrastructure secure.

BAE Systems
265 Franklin Street
Boston
MA 02110
USA
T: +1 (617) 737 4170

BAE Systems
154 University Avenue, 2nd Floor
Toronto, ON
M5H 3Y9
Canada
T: +1 (647) 777 2000

BAE Systems, 265 Franklin Street, Boston, MA 02110, USA

E: learn@baesystems.com | W: baesystems.com/businessdefense

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai

Victim of a cyber attack? Contact our emergency response team on:

US: 1 (800) 417-2155
UK: 0808 168 6647
Australia: 1800 825 411
International: +44 1483 817491
E: cyberresponse@baesystems.com

CREST CESG Certified Service Cyber Incident Response CPNI Centre for the Protection of National Infrastructure