BAE SYSTEMS

Cyber incident response services

Introduction

In today's connected world, the threat landscape is becoming increasingly complex with attacks that are more specific, agile and sophisticated in nature. Cyber security threats continue to challenge the operation of your business, employee safety and protection of your digital assets and intellectual property. The growing sophistication of cyber criminals demands even greater advances in information security practices, which drives the increased need for qualified information security staff.

When your business is the target of the inevitable cyber attack, how will you respond? Do you have an agile and up-to-date incident response plan and approach? Is your response team prepared to perform well in a crisis situation through regular plan testing? Do you have the appropriate resources pre-arranged and available to ensure a swift response to an incident?

To effectively respond to a cyber attack, you must have a solid plan, be prepared to execute, and have your resources ready to respond. Without a well-planned and rehearsed response capability, incidents will quickly become unmanageable, unpredictable and even chaotic situations. Every organization is different, each with its unique risks and threats, which requires a comprehensive incident response program that is up-to-date and tailored to the environment.

Without a well-planned response, incidents will quickly become unmanageable, and even chaotic situations.

Premier provider of cyber security services

BAE Systems has a proven track record in delivering high quality cyber security services for commercial and government clients around the globe. Moreover, our security operations centers, staffed with uniquely qualified specialists, give us unparalleled insight into the latest cyber threats.

Services that will help organizations protect their most vital information assets are central to our success. The experience and qualifications of our talented and professional cyber security consulting staff gives you access to knowledge and capability that is almost impossible to maintain internally. Their day to day experience across a wide range of government and industry groups provides them with insight that can be available to your organization.

We know how difficult it is to fully address these security demands in today's fast-paced business environment. You need help, we have solutions. We provide the resources and expertise to help ensure you are prepared and ready to respond to the inevitable cyber attack against your business.

Our affiliations and certifications

CESG Certified Service Cyber Incident Response

CPNI Centre for the Protection of National Infrastructure

CREST

FINANCIAL SERVICES Information Sharing and Analysis Center AFFILIATE

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR™

Planning for an incident

Being well prepared for a cyber incident is essential in ensuring your incident response team can successfully navigate the tasks required to recover successfully. An effective cyber incident response capability relies on an agile and up-to-date incident response plan that is tailored to the organization's environment as well as confirmed access to experienced resources to supplement your in-house capabilities.

Our incident planning service provides a detailed evaluation of the current state of your organization's threat detection and incident response program against our best practices, national and international standards and understanding of current attacker methodology. The resulting information provides the foundation for creating an updated incident response plan that includes guidance on preparation, anomalous behavior detection, incident management, technical response and communications plans.

Preparing for an incident

Practice makes perfect is especially true when it comes to being prepared to execute an incident response plan, make sound decisions under duress and produce results in a difficult situation. Understanding the plan and team member roles and responsibilities is critical. Hence the team must routinely execute the plan against a variety of scenarios to develop the 'muscle memory' required to perform well in potential crisis situation.

Whether tabletop exercise or mock attack, our experts lead the exercise that brings together all resources involved in the incident response plan including senior management. Our incident exercises are tailored to your organization, business sector and specific internal teams and skill sets. We provide a way for all relevant teams to experience the reality of a cyber attack and prepare themselves to ensure they can respond successfully when it matters.

Responding to an incident

When facing a major cyber incident your organization must be prepared and staffed to respond effectively. The appropriate resources must be pre-arranged and readily available to ensure a swift and successful response without unnecessary delay and potential chaos.

Our incident response and management service provides the skilled resources and procedures to ensure successful containment, remediation and recovery of a data breach. Our incident management process addresses requirements for investigation, communications, briefings and stakeholder engagement activities.

Service model

Retained
Retained service contract with priority response
Prepared
Framework contact in place with experts on standby
Emergency
Rapid response with no previous contract in place

Managed incident readiness service

The Managed Incident Readiness Service (MIRS) combines the incident planning and preparing components into an annual service that ensures your incident response plan and capabilities are reviewed and improved annually. Routine reviews and updates are essential to keep pace with cyber threat landscape and organizational dynamics. The MIRS service provides additional benefits to include a prearranged incident response framework and the comfort of knowing that our talented and experience incident responders are available for the organization at a discounted rate.

We are BAE Systems

We help nations, governments and businesses around the world defend themselves against cyber crime, reduce their risk in the connected world, comply with regulation, and transform their operations.

We do this using our unique set of solutions, systems, experience and processes - often collecting and analyzing huge volumes of data. These, combined with our cyber special forces - some of the most skilled people in the world, enable us to defend against cyber attacks, fraud and financial crime, enable intelligence-led policing and solve complex data problems.

We employ over 4,000 people across 18 countries in the Americas, APAC, UK and EMEA.

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

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

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