Digital Intelligence

BAE SYSTEMS

Incident Response
Proactive Services

BAE Systems' experts are at the frontline of cyber security, helping our customers prepare for, contain and recover from even the most sophisticated cyber attacks.

Be ready to respond

It is a consequence of our interconnected world that nearly every organisation today faces a real possibility of cyber attack. Governments around the world now recognise that cyber attacks are a Tier One threat to national security.

Many cyber attacks can be defeated by rigorous and well-maintained defences. However some attacks, particularly those launched by a determined adversary, will eventually evade such safeguards and have a business impact.

Managing the response to a cyber incident is a complex undertaking that involves the coordination of many decisions, resources, tasks and information. Events and threats must be understood. Decisions must be taken. Technical measures must be deployed. Further damage must be avoided. Stakeholders must be updated. Evidence must be preserved. All under intense time pressure and scrutiny.

A further complication of targeted cyber attacks is that there is an intelligent adversary focused on your estate; any actions you take may alert them and cause them to change tactics, potentially worsening the attack if you are not prepared and able to react. Without a well planned and rehearsed Incident Response (IR) plan, such incidents can quickly develop into unmanageable, unpredictable and even chaotic situations.

When your business is the target of a significant cyber threat

- 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?
- Do you have the appropriate resources and skills to ensure a swift and efficient response to an incident?

Why BAE Systems?

For more than a decade, BAE Systems' experts have been at the frontline of cyber security - helping our customers prepare for, contain and recover from even the most sophisticated cyber attacks.

Our expertise in combatting state-sponsored, criminal and other highly motivated attackers is recognised by our status as a founding member of the UK NCSC Cyber Incident Response Scheme.

We understand that when a cyber incident occurs, however serious, time is of the essence. The remedial actions taken in the first few hours will critically influence the eventual outcome. The right decisions are needed at the right times and can only be achieved with proper preparation and planning.

Our services

We understand the need to improve organisations' IR maturity, so have developed a set of proactive service offerings. These services are delivered by our skilled consultants who have real-world experience of responding to large cyber security incidents and breaches across different sectors.

Incident Response Tabletop Exercise

Interactive bespoke exercises designed to test your responses to a relevant and sophisticated cyber attack and identify potential issues/problems which can be remediated in a 'safe environment' before a real-life incident occurs.

Incident Response Readiness Assessment

Expert assessment of every aspect of your incident management capability across people, process and technology and your preparedness for each phase of the incident response lifecycle.

Incident Response Processes and Playbooks

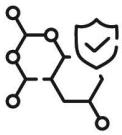
Custom incident response processes and playbooks created by experts with real life experience in responding to sophisticated cyber attacks, tailored for the organisation based on existing team structures, processes and technology.

Threat Response Training

Training for your information security teams available in three different tracks: Cyber Incident Response, Threat Hunting and Linux Incident Response.

First Responder Workshop

Comprehensive workshops tailored for your first responder and incident management teams, providing insights into the dynamics of IR and equipping them with the skills to manage initial incident response efforts.



Compromise Assessment

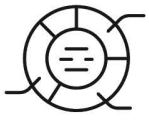
Lightweight cyber incident investigations that target your high priority systems to establish whether any current or historic breach has evaded detection, and identify high-risk behaviour and potential policy breaches.

Threat Hunt

An enterprise-wide hunt for current or historic compromises and for threats that may have evaded the current security stack in the target environment.

PII Data Search

Identifying Personally Identifiable Information within your largest datasets. Find out if a system contains information that could cause serious harm to your company if it was stolen before threat actors get access to it.



Post Incident Review

A detailed review of an incident and your team's response to understand areas of response that were effective, those that need improvement and what can be done to prevent future recurrence of such incidents.

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

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

linkedin.com/company/baesystemsdigital @BAESystemsDigi

Assured Service Provider

in association with National Cyber Security Centre

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

UK & International: +44 330 158 5263
Email: cyberresponse@baesystems.com