BAE SYSTEMS
INSPIRED WORK

Incident response

[Recovering from a targeted cyber attack]

Real and growing threat

Cyber attacks are a global phenomenon that affects every major business sector. 93% of large corporations and 87% of small business reported a cyber breach in the past year according to information published by the UK Government. Terrorists, rogue states and cyber criminals are among those targeting computer systems in the UK.

Many of the attack groups use highly advanced techniques, attempt persist in networks without detection while remaining covert, and pose a substantial threat to company and customer information – the term used to describe this is Advanced Persistent Threat (APT).

UK security strategy

In 2013, the UK issued a policy on Keeping the UK Safe in Cyberspace. The Government recognised that with great openness, interconnection and dependency comes greater vulnerability. The National Security Strategy categorises cyber attacks as a Tier One threat to our national security, alongside international terrorism.

To make the UK more resilient to cyber attacks, actions were set out including the creation of a new Cyber Incident Response Scheme by GCHQ to help organisations respond safely and effectively to advanced cyber attacks.

Backed by leading cyber capabilities

As a founding member of the pilot scheme, we worked closely with CESG and industry partners to define best practice and acceptance criteria for suppliers. The scheme was launched as a full service to victims of cyber attacks in September 2013.

Our capability is built on a proven methodology with over 10 years experience specialising in advanced targeted attacks. It is complemented by our Threat Analytics platform to conduct behavioural analytics which are developed to detect advanced unknown malware typical of advanced cyber attacks. Our in-house Threat Intelligence team monitor advanced and organised threat groups; tracking the latest tactics and trends as well as working to understand the identities of these actors. We work closely with this team to provide specific insight for incident response.

Combining these capabilities – industry leading in their own right – builds a service which offers cyber attack victims a world leading incident response service.

Certified by UK Government to deliver cyber incident response.

Cyber incident response

- Global, world-class responders for advanced and targeted cyber-attacks, including cyber espionage, cyber crime, 'hactivism'.
- Proven method of attack investigation to lead you from an initial meeting to full recovery.
- Rapid safe remediation by using our expertise to focus on the most relevant data and tasks.
- Recommendations that not only remediate the current threat but help you protect yourselves against future threats.
- Business and technical expertise to ensure we help you recover both from a technical and business perspective.

Technical services

- Core incident response services offered as standalone capability:
  - Digital forensics.
  - Malware reverse engineering.
  - Log and network data analysis.
  - Decryption and de-obfuscation.

Consultancy services

- Incident response experts offered as flexible resourcing, including:
  - Lead investigators.
  - Data capture, inc. evidential capture.
  - Incident management and reporting.
  - Incident response readiness planning.

Flexible service offerings

When an incident occurs, time is of the essence. The actions taken during those first few hours can be critical to mitigating business impact and risks.

We offer a 24/7 hotline as well as retained services which ensure that we can respond to an incident rapidly.

Emergency

- World-class cyber incident response team
- Rapid response with no previous contract in place
- Contain and remediate attacks

Prepared

- Framework contact in place
- Experts on standby
- Defined rate card and terms
- React faster when it matters most

Retained

- Retained service contract
- Priority response
- Service level agreement for response times
- Preferential rates for response

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, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK
UK: +44 (0) 1483 816000
E: learn@baesystems.com | W: baesystems.com/businessdefence

linkedin.com/company/baesystemsai
twitter.com/baesystems_ai

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

Copyright © BAE Systems plc 2015. All rights reserved. BAE SYSTEMS, the BAE SYSTEMS Logo and the product names referenced herein are trademarks of BAE Systems plc. BAE Systems Applied Intelligence Limited registered in England & Wales (No.1337451) with its registered office at Surrey Research Park, Guildford, England, GU2 7RQ. No part of this document may be copied, reproduced, adapted or redistributed in any form or by any means without the express prior written consent of BAE Systems Applied Intelligence.