

# Incident Response

## You can't stop every cyber attack, but you can have the best response

When cyber-attacks occur, your goal is to regain control. Not every cyber-attack is a sensational, headline-grabbing news story, but each needs to be investigated, prioritized, responded to and mitigated. Thankfully, resources are available so you don't have to respond alone.

Depending on the extent, sophistication and risk potential of an attack your response may be a combination of a variety of resources, whether that means technical investigation, containment or recovery. Sometimes you want someone to validate your course of action or provide threat intelligence. In other cases, you may want highly skilled resources to guide or physically assist you in your response, either over the phone, online, or onsite.

## Immediate help when you need it most

Every minute counts, so one call to our 24/7 hotline and we deploy expert Incident Response teams to your site. Supported by BAE Systems Centers of Excellence and infrastructure around the globe we move fast to mitigate the effects of the attack.

Our teams use proven tools, proprietary analytics, and unique knowledge of the tactics employed by over 170 of the world's most advanced threat groups to uncover the critical facts fast. We offer strategic guidance to ensure your organisation makes the right decisions at the right time. We help manage internal and external stakeholders, customers, the press and regulators. We support you every step of the way so you can get back to your business.

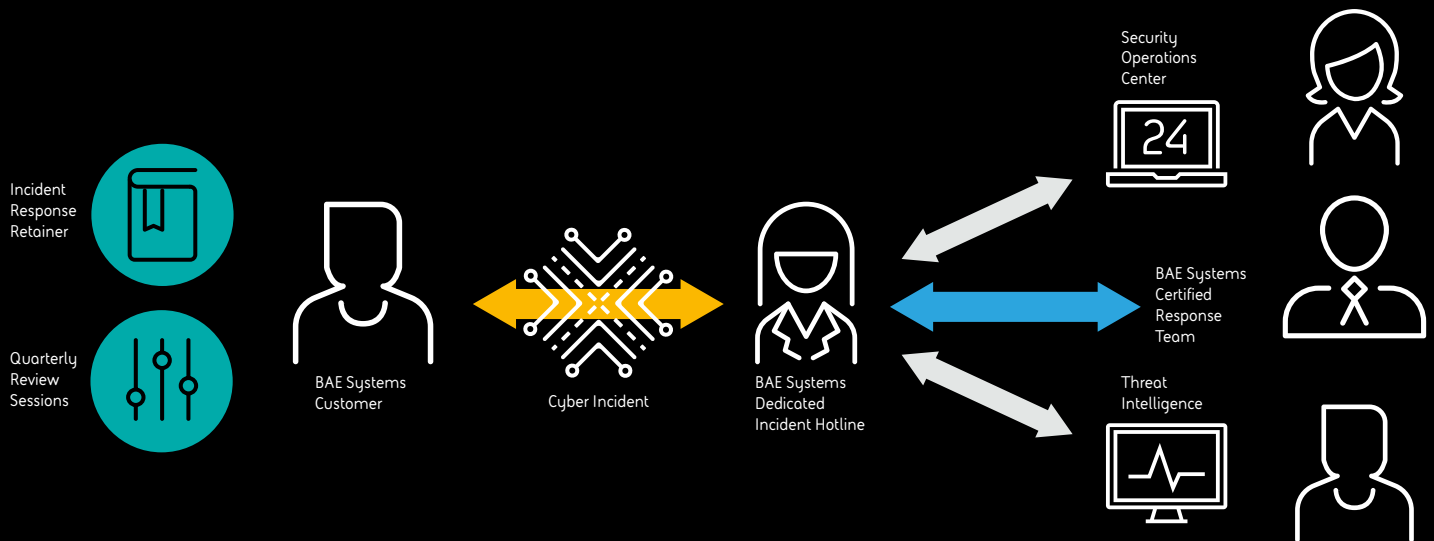
## A retained relationship

An incident response retainer with BAE Systems guarantees you are our priority and we are available for you whenever your crisis occurs. We spend time in your organization, understanding you, your team and your operation. This ensures no additional pain in your moment of need. It also eliminates costly delays due to procurement processes and required contract approvals. During our quarterly review sessions we help you identify root causes and security improvements and review, update and improve your response plan.

## Benefits

- World-class cyber incident response team
- On-boarding assessment of your incident response capability - people, process, and technology
- Contain and remediate attacks
- Retained service contract
- Service level agreement for response times

# BAE Systems Incident Response



## BAE Systems Difference

- Endorsed by NCSC to handle serious cyber-attacks
- Certified by CREST
- Unique Threat Intelligence, based on the activity of 170+ threat actor groups we track
- Operational Intelligence from over 2,500 managed security customers
- Over 40 years experience defending critical business and government activities
- Global Coverage from teams in the US, UK and Australia around the clock.

Our Incident Response experts can also be offered as flexible resourcing, including:

- Lead investigators
- Data capture, including evidential capture
- Incident management and reporting
- Incident response readiness planning



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

**Contact Details:** US: +1 (703)848 7000 | UK: +44 (0) 1483 816000 | AUS: +612 9240 4600

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK  
 E: learn@baesystems.com | W: baesystems.com/cyberreveal

[linkedin.com/company/baesystemsai](https://www.linkedin.com/company/baesystemsai)

[twitter.com/baesystems\\_ai](https://twitter.com/baesystems_ai)

Copyright © BAE Systems plc 2019. 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, adopted or redistributed in any form or by any means without the express prior written consent of BAE Systems Applied Intelligence.