

Cyber Threat Intelligence

Unique insight into the threats that matter most

BAE Systems Cyber Threat Intelligence provides mature intelligence and security teams with high-confidence intelligence on the world's most capable cyber adversaries.

Built upon years of intelligence tradecraft development and informed by frontline experience responding to serious cyber incidents, our intelligence delivers unique insights into threat actor intent, capability and activity, helping organisations make informed decisions and strengthen their cyber resilience.

The Challenge

Today's threat intelligence teams face an overwhelming volume of information. While access to intelligence has increased, identifying the insights that genuinely matter has become more challenging.

For organisations facing nation-state and strategically significant cyber threats, understanding the motivations, capabilities and behaviours of sophisticated adversaries is critical. Security teams require intelligence that goes beyond indicators and headlines to provide actionable insight that supports strategic, operational and technical decision making.

BAE Systems Cyber Threat Intelligence helps organisations cut through the noise by focusing on the threats that matter most.

Service Overview

BAE Systems Cyber Threat Intelligence delivers focused intelligence on the most capable threat actors and emerging threats relevant to government, defence, financial services and critical national infrastructure organisations.

The service combines expert analysis, technical intelligence, direct analyst engagement and a modern Threat Intelligence Portal, enabling customers to understand evolving threats, prioritise defensive activity and enhance threat-informed decision making.

Our approach is centred on quality over quantity, delivering intelligence that provides meaningful insight rather than overwhelming customers with reporting volume.

Key Benefits

Understand High-Priority Threats - Gain deeper insight into the actors, campaigns and technologies most likely to impact the communities you protect.

Improve Decision Making - Access intelligence that provides context and understanding, enabling more effective threat prioritisation.

Strengthen Threat-Informed Defence - Support detection, threat hunting, vulnerability management and incident response activities with actionable intelligence.

Enhance Internal Intelligence Capability - Collaborate directly with experienced intelligence analysts to develop a richer understanding of the threat landscape.

Integrate with Existing Investments - Enrich existing threat intelligence platforms, security tooling and operational workflows without creating additional complexity.

"BAE Systems provide the most insightful threat intelligence product and analysis that we buy. The product focuses on high value threats and always seems to be ahead of other vendors. The people we meet come from unique backgrounds, approach their work with humility and are clearly experts in their field."

A European National Cyber Security Centre

Threat Intelligence Service Components

Actor-Focused Intelligence - Detailed intelligence reporting focused on significant threat actor campaigns, targeting activity and emerging developments. Reporting provides insight into adversary objectives, tradecraft, infrastructure and operational behaviour, helping organisations understand both current and future threats.

Technology-Focused Intelligence - In-depth analysis of threats, vulnerabilities, and emerging risks across critical technology domains. Coverage includes Operational Technology (OT), cloud platforms and services, supply chains, critical enterprise technologies, and emerging technology trends. This intelligence enables organisations to understand how evolving technologies influence cyber risk and create opportunities for adversaries.

Signatures and Detection Content - Technical intelligence derived from investigations, threat research and operational experience delivered through our MISP instance. This includes: Indicators of Compromise (IOCs), detection rules and signatures, adversary infrastructure intelligence.

Analyst Access and Intelligence Briefings - Direct engagement with experienced intelligence professionals provides customers with valuable context and expert insight.

Threat Intelligence Portal

Customers access intelligence through the BAE Systems Threat Intelligence Portal, providing a central location for reporting, technical intelligence, research and supporting analysis.

The portal enables analysts to quickly discover relevant intelligence, track developments across threat actors and technologies, and access years of accumulated research.

AI-Assisted Search

The Threat Intelligence Portal includes AI-assisted search capabilities, allowing analysts to query the intelligence using natural language questions.

Rather than relying solely on keywords, users can interrogate years of intelligence reporting through more intuitive queries, helping them rapidly locate relevant research, identify relationships between campaigns and gain deeper insights from existing intelligence holdings.

Why BAE Systems Threat Intelligence?

Unique Insights on the Most Capable Threat Actors - We maintain a deliberate focus on the actors most likely to impact governments, critical national infrastructure operators and defence organisations.

Tradecraft-Driven Intelligence - Our intelligence capability is built upon years of intelligence tradecraft development and continuous tracking of the world's most capable cyber adversaries.

Quality Over Quantity - Our customers consistently highlight the quality, relevance and uniqueness of our intelligence. Rather than generating large volumes of reporting, we focus on delivering meaningful insights that improve understanding of the threats that matter most.

Trusted During the Most Serious Incidents - BAE Systems is an NCSC Assured Cyber Incident Response provider, trusted to support organisations through some of the most significant cyber incidents.

Develop Your Teams

Alongside our Cyber Threat Intelligence service, we offer specialist training designed to strengthen cyber security and intelligence capabilities, including:

- Threat Intelligence Training
- Malware Analysis Training
- Cyber Threat Hunting Training
- Cyber Incident Response Training
- Linux Incident Response Training

Delivered by experienced practitioners, our courses provide practical skills and real-world techniques to help teams identify, investigate and respond to advanced cyber threats with confidence.

To discuss our Cyber Threat Intelligence services or training offerings, contact us at -

government.tenders@baesystems.com.



Assured Service Provider



in association with
National Cyber
Security Centre

Cyber Incident Response: Enhanced Level



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



[@BAESystemsDigi](https://twitter.com/BAESystemsDigi)

Copyright © BAE Systems plc 2026. 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 Digital Intelligence.