Cyber Threat Intelligence
As cyberspace evolves, so do the threats that seek to exploit users for financial, political, or nation state objectives. Understanding the nature of these threats has rapidly become a key part of a mature cyber security program.

As a result, the field of cyber threat intelligence has emerged to support both tactical network defence and to help communicate operational and strategic risks to stakeholders.

BAE Systems offers a leading cyber threat intelligence service, providing actionable information on threats facing organisations globally, enabling our customers to act with confidence.
The Use Cases for **Threat Intelligence**

**Incident Management**
Use threat intelligence to inform incident response and help shut down attacks quickly. Expert knowledge of particular adversary groups can allow teams to better detect or mitigate attacker actions.

**Situational Awareness**
Keep up to date with the threat landscape relevant to your organisation and region. Understand who is conducting attacks: their methods, tools, infrastructure, and motivations.

**Network Defence**
Ensure the networks you defend are maintained with signatures and rules designed to detect the most sophisticated cyber attacks.

Make the most informed decisions for your organisation by using cyber threat intelligence and the benefits it offers.
## Our Service

The BAE Systems Cyber Threat Intelligence Service is made up of several components:

<table>
<thead>
<tr>
<th><strong>Threat Intelligence Portal Access</strong></th>
<th>All our subscription customers have access to our Threat Intelligence Portal. Through this users can access our monthly operations summary, regional threat reporting, and other services.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Threat Intelligence Research Reports</strong></td>
<td>For customers requiring deep insights into past, current, and emerging threats we offer access to our Research Reports. This provides users with both historical reporting as well as the latest research, released every couple of days. Our Research Reports contain detailed breakdowns of malware, campaigns, attribution, etc., and are intended for intelligence teams tasked with tracking the threat landscape.</td>
</tr>
<tr>
<td><strong>Threat Intelligence Signature Feeds</strong></td>
<td>Threat data acquired by our team during investigations is turned into IOCs and Rules delivered via our Signatures Feed. We use a dedicated MISP instance for this, offering both web and API access. Typical indicators include C&amp;C domains and malicious IP addresses. All are tagged with a Confidence and Priority score to help investigators. We also include attribution details where possible. Customers receiving our Research Reports can also access these through the MISP API, along with associated MITRE ATT&amp;CK TTPs. Our feed is compatible with STIX, and integrations are available for third-party platforms such as EclecticIQ, ThreatConnect, and Anomali.</td>
</tr>
</tbody>
</table>
| **Threat Intelligence Analyst Access** | On-demand subject matter expert analysis of threats. For example, customers may request analyst support services to:  
  - Provide insights on recent attacks  
  - Analyse or reverse-engineer malware  
  - Examine suspicious websites, IP addresses, emails  
  - Attribute threats |
| **Threat Intelligence Briefings** | We provide customers with briefings on the latest threat landscape, delivered by one of our subject matter experts. These can be provided to end-users of the portal, or other stakeholders such as senior management. Briefings can be provided in-person or via WebEx, depending on customer availability and requirements. |
Our Sources and Methods

There are many good sources of information about common place threats. We focus on subtly-executed attacks that traditional cyber defences miss. Our view of the threat landscape is informed by the threat actors that cause the most impact - not the ones that make the most noise.

We leverage a unique mix of sources to deliver original insights in our services. These include intelligence from customer engagement, such as incident response, as well as a range of premium commercial data sources. We also boast a wide network of trusted community contacts who provide insight and enrichment on the latest attacks.

Our team uses a range of analytical methods, such as malware reverse engineering, infrastructure pivoting, as well as attribution analysis.

We are data-driven and make heavy use of graphs when investigating and delivering our intelligence products. Our evidence based approach allows customers to have confidence in our findings and enable the benefits to be realised.
Our Team

The BAE Systems Threat Intelligence team is comprised of industry experts, with decades of combined experience.

We are specialists in investigating nation state and serious organised crime activity, tracking the most prolific groups using our unique mix of sources and methods.

Many of our team hold high calibre professional accreditations, such as:

- CREST Certified Threat Intelligence Manager (CCTIM)
- CREST Certified Malware Reverse Engineer (CCMRE)
- CREST Certified Incident Manager (CCIM)
- CREST Certified Host Intrusion Analyst (CCHIA)

Our analysts are part of a global team, working alongside our incident response and other cyber security specialists, helping customers with challenging cyber defence needs.

We operate globally, but act locally, gaining close trusted working relationships with our customers.
Our Customers

Customer Sectors

We are experts in providing cyber threat intel to intel teams. Our customers are made up of specialists across the following sectors:

- National Security
- Banking
- Telecoms
- Government
- Insurance
- Manufacturing
- Oil & Gas

Customer Feedback

BAE Systems’ Cyber Threat Intelligence offering serves mature threat intelligence data through an easily integratable service. Comprehensive reports and a low false-positive rate provide a good base for advanced security operations.

Provided reports are versatile, targeted at different audiences and provide comprehensive intelligence.

Of the APT-related network indicators that overlapped with other threat intelligence providers, over 75% were reported first (or simultaneously) by BAE Systems.

Due to the MISP-based data exchange, BAE Systems provided the indicators in a very consistent way and covered all common indicator types. The indicators were provided with additional information and could be correlated through the supplied MISP events.
Our Portfolio

Our Threat Intelligence Service is part of a broader portfolio of specialist services. For more information on these, please speak to one of our account managers.

- Threat Intelligence Service
- Threat Advisory
- Threat Intelligence Training
- Incident Readiness
- Incident Response Retainer
- Incident Response Emergency
Our Culture and Mission

We exist to support our customers and business with insights into threats.

We are part of BAE Systems Applied Intelligence which exists to protect and enhance the connected world.

We support our customers through close working relationships and deep understanding of their intelligence needs.

We derive original insights from our unique mix of sources and tradecraft, blending technical and non-technical expert analysis.

We track high-end criminals and nation state actors, helping customers mitigate the most serious cyber threats.

130+ Advanced Persistent Threat Groups Tracked.

Our customer base stretches across 30 countries and 4 continents.

We focus on high-end threats that target large enterprises and other networks of national importance.

We are the leading global certified provider of cyber threat intelligence to intelligence teams.
We are BAE Systems

At BAE Systems, we provide some of the world’s most advanced technology, defence, aerospace and security solutions.

We employ a skilled workforce of 82,500 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, protect people and national security, and keep critical information and infrastructure secure.

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

UK:  0808 168 6647
US:  1 (800) 417-2155
Australia:  1800 825 411
International: +44 (0) 1483 816000
Email:  cyberresponse@baesystems.com

Global Headquarters
BAE Systems
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
8000 Towers Crescent Drive
13th Floor
Vienna, VA 22182
USA
T: +1 720 696 9830

BAE Systems
Level 12
20 Bridge Street
Sydney NSW 2000
Australia
T: +61 2 9240 4600

BAE Systems
1 Raffles Place #42-01, Tower 1
Singapore 048616
Singapore
T: +65 6499 5000

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

Copyright © BAE Systems plc 2020. 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.