Cyber Threat Intelligence

G-Cloud 15

January 2026

Cyber Threat Intelligence

About this service

BMT provide threat intelligence expertise to help organisations understand, prepare and respond to threats seen in the cyber threat landscape. The services provided range from assessment of threat intelligence requirements, advice on threat intelligence driven processes, to guidelines for commercial threat intelligence platform and feed selection and technical integration aspects.

BMT's digital offerings cover four core areas of expertise to our customers: Code, Visualisation, Data and Cyber. Within our Cyber capability, we support organisations to help them understand the cyber landscape, providing insight into threats and risks and secure design across development and enterprise systems. We combine skills from threat intelligence, security architecture, data science and mission planning, to deliver enterprise resilience for high performance and critical information systems.

BMT has a proven track record in designing, developing and delivering applications that provide access to information in a secure environment. This information includes threat intelligence and cyber related data stored in databases, technical documents of various formats, graphics, dynamic reports, etc.

The company has recognised professional development schemes with several professional institutes and is recognised by the UK Department of Trade and Industry as an "Investor in People". All BMT consultants, analysts, software developers and testers are professional members of the British Computer Society (BCS), including staff members with Chartered status. In addition, the software team includes PRINCE2 Practitioners and we seek to utilise PRINCE2 project management where applicable.

BMT is certified to ISO 9001/27001 and TickITplus. Security Clearance: UK Security-cleared staff; Facility Security Clearance (FSC).

What we deliver

- Gather and assess threat intelligence requirements
- Assist in defining threat intelligence feed selection criteria
- Support proof of value trials of threat intelligence feeds
- Work with vendors such as Crowdstrike, FireEye, Recorded Future, Intel471
- Support selection and assessment of threat intelligence platforms
- Work with platform vendors such as EclecticIQ, Anomali, ThreatConnect
- Assist with custom integration, orchestration, configuration and automation
- Support transition and transformation to threat Intelligence driven cyber operations
- Support intelligence driven threat hunting and integration with SIEM solutions

- Assessment of OSINT requirements and solutions

What benefits we provide

- Enabling strategic discussions that impact an organisation's threat and risk priorities
- Service tailored to an organisation's specific threat landscape, industry/market
- Information and process management to extract holistic, evidence-based insights
- Ability to respond quickly, decisively and effectively to emerging threats
- Informing cyber security defence operations, decision making and reducing risk
- Robust operational framework to proactively adapt to changing threat landscape
- Adherence to open standards such as STIX and TAXII and NIST guidelines
- Shared intelligence across threat hunting, security operations and incident response
- Increased integration/automation across operations, alerting, signatures and reporting
- Advanced open-source early warning capability

How we deliver this service

Our team combines skills from cyber security, threat intelligence, security architecture, data science, and mission planning to deliver enterprise resilience for high performance and critical information systems.

Our cyber security professionals possess a range of qualification including Certified Cyber Professional (CCP) in Risk Management and Security Architecture; ISC2 (CISSP, CCSP); ISACA CISM; Chartered Cyber Security Professional (ChCSP); other

As cyber-attacks become more targeted, more persistent and more damaging, BMT's Threat Intelligence Service ensures that threat environment and attack patterns can be effectively analysed and assessed and are used to enable detective and preventive measure. In addition, we utilise our experience within the defence sector and our adherence to our ISO27001 accreditation to investigate and advise on security considerations and data classification, which can be essential when assessing cloud hosting options.

Experience

Our experience includes the full end-to-end delivery of the following projects:

Cyber Professional Services

MOD's Defensive Cyber Capability (DCC) Customer Friend

DCC moves defensive Cyber to a loosely coupled big data architecture. Big Data Architectures were new to the MOD and the Cyber Delivery Team (CDT) required technical expertise in finding the best supplier to deliver DCC.

In our role of Customer Friend we delivered the ITQ for DCC; this included mapping the tender questions to the procurement framework's evaluation areas. The ITQ enabled the authority to differentiate between the potential suppliers in terms of their likelihood of being able to meet the Authority's needs for the DCC service capability.

BMT supported the CDT to adopt and follow the GDS development lifecycle in the delivery of DCC. We actively led the transition to a User Story based approach. We collected User Stories from the majority of MoD project Stakeholders using workshops and face-toface meetings, providing guidance on how to capture stories that centred on the user's needs, their Acceptance Criteria and Definition of Done.

We have supported the DCC Product Owner (PO) at sprint review and planning sessions and supported the PO in organising and prioritising the product backlog and providing problem specific advice from a Cyber and big data technologies and techniques perspective.

We have captured and de-conflicted requirements at both the strategic (CSOC) layer and tactical (application) layer to inform decision making at the short (Sprint review fortnightly), medium (phase 6 monthly) and longer term timelines. We have helped the CDT and supplier to assist in project delivery against accelerated timelines, and expanding scope, via an Agile methodology

CySAFA Specialist Technical Support -

We have provided technical specialist Big Data and Cyber Expertise to the Cyber Delivery Team (CDT). We have engaged with many project stakeholders including: Internal Stakeholders (MOD Stakeholders), System suppliers (facilitating Discovery, Alpha and Beta delivery) and Vendors.

BMT has excellent understanding of CySAFA's underlying Big Data technology, Cyber Tools and End User operating procedures. Applying this knowledge we have advised the Cyber Delivery Team on case management, orchestration, Threat Intelligence (TI) and SIEM tools with respect to the Big Data solution.

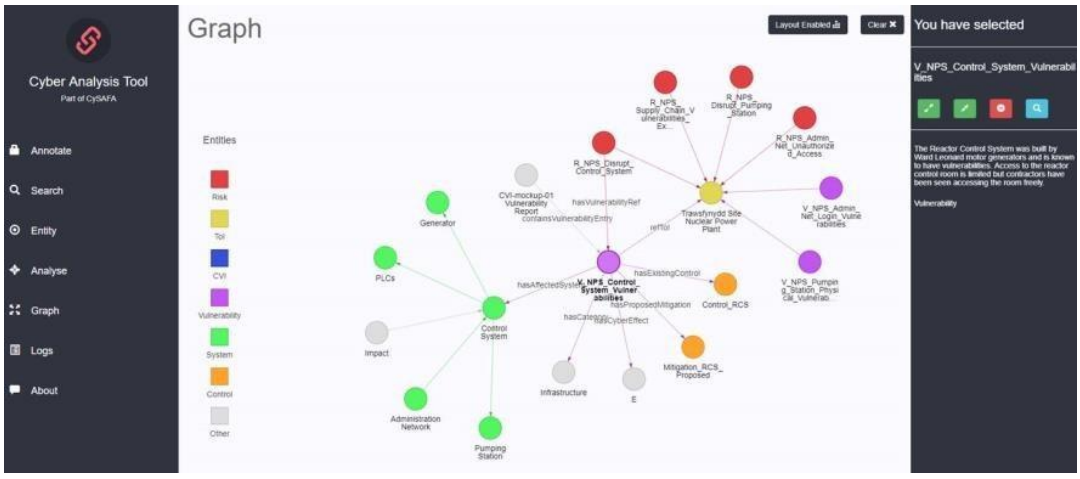
On behalf of the Customer we have engaged with vendors and internal stakeholders to support the customer in technology reviews and technology down-selection. This has included SIEM, TI and Vulnerability Scanning tooling. We have also run proof of concept demonstrators to de-risk product selection.

We have provided advice and guidance on emerging and developing standards including STIX v1.0 to STIX v2.0 for normalised Threat Intelligence sharing.

Advanced Cyber Data Analytics

BMT have a strong pedigree in Advanced Cyber Data Analytics Tools for information fusion and visualisation. Experienced in index store and graph engineering for query performance, effective data ETL pipelines, data indexing, natural language analysers, knowledge graph manipulation, graph algorithm. Experience of index data stores, such as Elastic Search, Solr, as well as graph databases and RDF-based triple stores such as Neo4J, OrientDB, Apache Jena, Blazegraph, Grakn, and JanusGraph.

Cyber Intelligence Analysis - BMT have developed systems to query semantic rules that are been automatically extracted from unstructured text (e.g. case intelligence reports). We have produced a web application that ingests entity and relationships outputs into an RDF Triplestore (Blazegraph). We also developed a web application with a REST API to allow the user to discover and search the entities and relationships. BMT tested the tool by processing a portion of Wikipedia using Baleen. In addition, we have further expanded the system for Cyber Vulnerability Investigation (CVI) processing and analysis;



Implementation of a graph database to enhance cyber intelligence analysis

NCA Cyber Data Platform

BMT provided a core team to develop the Cyber Data Platform (CDP) for the National Crime Agency, a single infrastructure platform for hosting and analysing cybercrime-related data (both investigation-specific and OSINT). BMT delivered a data and analytics platform that provides the National Cyber Crime Unit (NCCU) with the ability to: search more easily,

analyse better, and share existing data and intelligence information across NCCU and from industry partners; deliver insights across multiple data sources; manage access and control measures to support compliance with business, legal, and security constraints; and trace data provenance to enable end-to-end traceability of data and intelligence for identifying the origin of gathered information.

Mission Planning

Joint User Mission Planning (JUMP) - BMT have developed a system on behalf of the UK MOD to integrate cyber threat analysis and mission planning with traditional land sea and air planning. We combine geographic intelligence integrated with Intelligence, Surveillance & Reconnaissance Systems and seamless linkage of physical terrain to cyber terrain. JUMP allows the cyber analyst to understand cyber assets within the wider context of the mission.

Contact details

Edyta Redfern

Global Head of Bidding

E: bidding.uk-europe@uk.bmt.org

T: +44 (0) 1225 473 727

www.bmt.org