Cyber Security Support

G-Cloud 15

January 2026

Cyber Security Support

About this service

BMT provides expertise to help organisations understand the cyber threat landscape, providing insight into digital risks, and resources to implement business resilience in systems, people, and processes. We help optimise your security controls and policies, adhering to best practice guidance and complying with regulatory standards and frameworks.

What we deliver

- Cyber Vulnerability Investigations (System/Enterprise) to determine business impact
- Threat Intelligence Services: assessment of requirements for threat intelligence platforms and vendor threat intelligence feeds through proof of value trials
- General Data Protection Regulation Compliance organisational modelling and actionable reporting
- Human Factors Assessment methodology/tools to assess/mitigate human error
- Assurance Services (System, Platform and Enterprise) tailored to customer needs, including support to Secure by Design principles and processes.
- Risk Assessment Process methodology/tools to assess/improve risk profile
- Advanced Data Analytics for attack and behaviour analysis and threat hunting
- Cyber Analytics Platforms and bespoke cyber solutions based on open source platforms
- Strategy/Architecture system engineering and evidence-based modelling business change
- Artificial Intelligence and Machine Learning resilience for high performance systems
- TEMPEST Services (emanation security); policy, process, and installation requirement

What benefits we provide

- Understanding of security risks
- Optimised Security Controls to mitigate unacceptable impacts to your business
- Threat Intelligence insights to protect people, assets, operations and organisation
- GDPR expert guidance to understanding, achieving and maintaining enterprise compliance
- Human Factor risk reduction and avoidance actions identified and prioritised
- Assurance expertise to achieve and maintain system and enterprise compliance
- Risk Assessment Process objectively assesses/monitors organisational cyber security risk profile
- Advanced Analytics to inform security decision making and reduce risk
- Delivery of cyber analytics for alerting, threat analysis and detection

- Unbiased recommendations about best cyber security practices
- Assessment of security controls and commercial cyber security vendor solutions (e.g. Threat Intelligence Platforms, Vulnerability Scanning Solutions, SIEM, IDAM, etc).
- Strategy and Architecture to inform business case and cost-effective solutions
- AI and Machine Learning to forensically analyse vulnerabilities and threats
- TEMPEST Policy provision; protective measures to mitigate risk to emanation security

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. As cyberattacks become more targeted, more persistent, and more damaging, BMT's Cyber Security Service provides mission assurance to detect and prevent attacks and to respond when they occur.

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-to-face 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

DCC 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 DCC 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 derisk product selection.

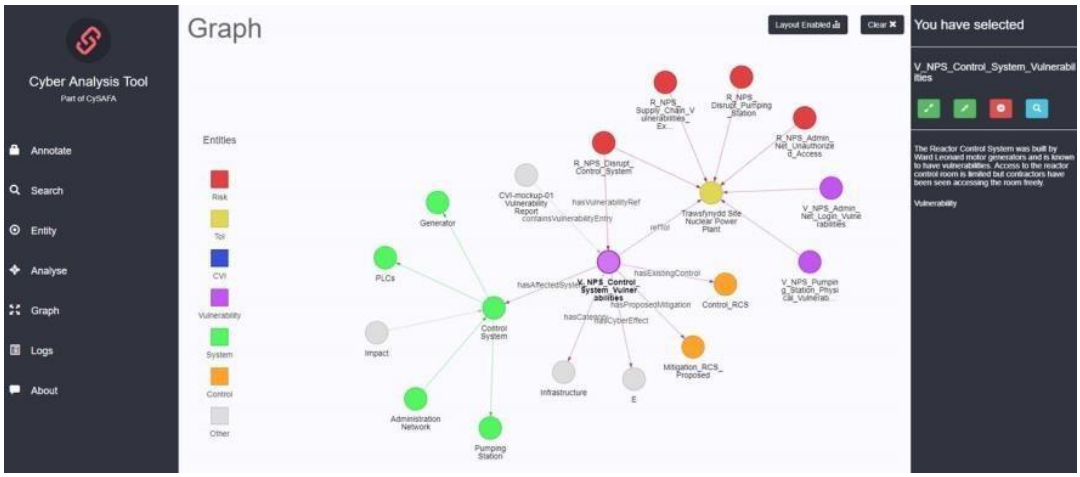
We have provided advice and guidance on emerging and developing standards including STIX v1.0 to STIX v2.0 for normalised Threat Intelligence sharing.

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