Cyber Security Analytics

G-Cloud 15

January 2026

Cyber Security Analytics

About this service

BMT provides cybersecurity and data analytical services that help organizations assess the cyber threat landscape and develop analytical solutions. BMT design, build, test, deploy, and run big data detective and predictive cyber analytics solutions. Our expertise cover vulnerabilities, threat intelligence, analysing attack patterns, and understanding the behaviours of threat actors.

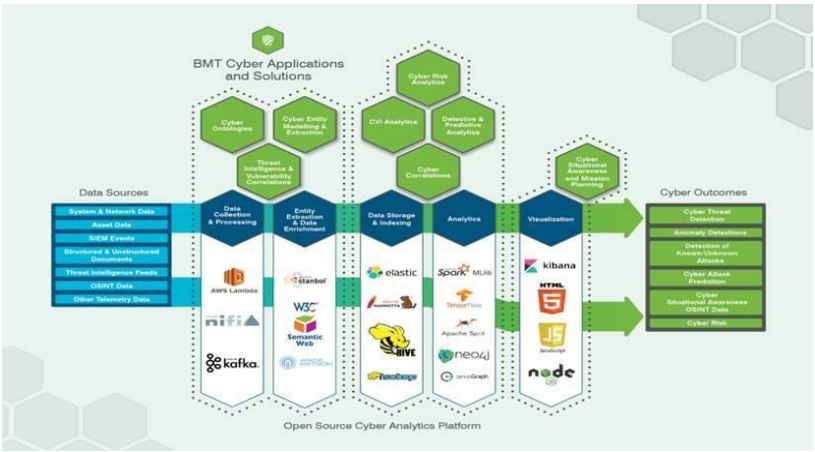
Leveraging appropriate data sources, BMT provides an end-to-end service to design, build, test, deploy, and run big data detective and predictive cyber analytics solutions. This helps our clients in staying ahead of potential threats and enhancing cybersecurity strategies.

What we deliver

- Detective cyber analytics: baselining, anomaly detection, empirical rules, etc.
- Predictive cyber analytics: Bayesian networks, Markov chains, etc.
- Big Data Cyber Platforms: Requirements, Design, Architecture, Data Modelling, Analytics
- Real-time streaming data, log processing: NiFi, Kafka, Spark Streaming
- Analytical engines on top of Apache Spark, Elastic Search, Hadoop
- Fusion of structured/unstructured data, threat intelligence feeds. Data enrichment.
- Advanced Big Data Analytics for forensic attack analysis, threat hunting
- Data sources: DNS (Domain Name System) logs, web proxy logs, netflow (network traffic), Active Directory (AD) logs, system/user event logs
- Artificial Intelligence, Machine Learning: Supervised and unsupervised techniques
- Advanced AI techniques: Deep Neural Networks (DNN), Natural Language Processing (NLP), Particle Filters (PF)

What benefits we provide

- Advanced detection of known/unknown cyber threats
- Advanced Analytics to inform security decision making and reduce risk
- AI and Machine Learning tailored to analyse vulnerabilities, threats, incidents
- Cyber analytics strategy to inform business case and cost-effective solutions
- Scalable, resilient open-source analytical platforms/ solutions
- Anticipating and predicting attack behaviour and driving mitigation efforts
- Targeted collection and processing of meaningful data sets/logs for analytics
- Adoption of open-source tools, ML/AI technologies for cyber analytics
- Reducing alert fatigue by increasing true positive alert rates



Example design and implementation of a BMT analytics platform

How we deliver this service

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

As cyber-attacks become more targeted, more persistent, and more damaging, BMT's Cyber Security Analytics Service ensures that threat environment and attack patterns can be effectively analysed and assessed and are used to enable detective and preventive measures for known/unknown threats and attacks. We deliver this service by:

(1) leveraging our expertise on relevant structured and unstructured data sets and logs to enable effective cyber analytics for threat detection. This includes collection, enrichment, and storage of data at scale.
(2) leveraging our deep expertise on cyber-attacks patterns and knowledge of tactics, techniques and procedures (TTPs) to identify, develop and deploy advanced cyber analytics, which use open-source analytics platforms, latest AI/ML tools, visualisation. An example of a BMT analytics platform is shown in the above image. In addition, we utilise our experience within the defence and commercial sectors 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

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.

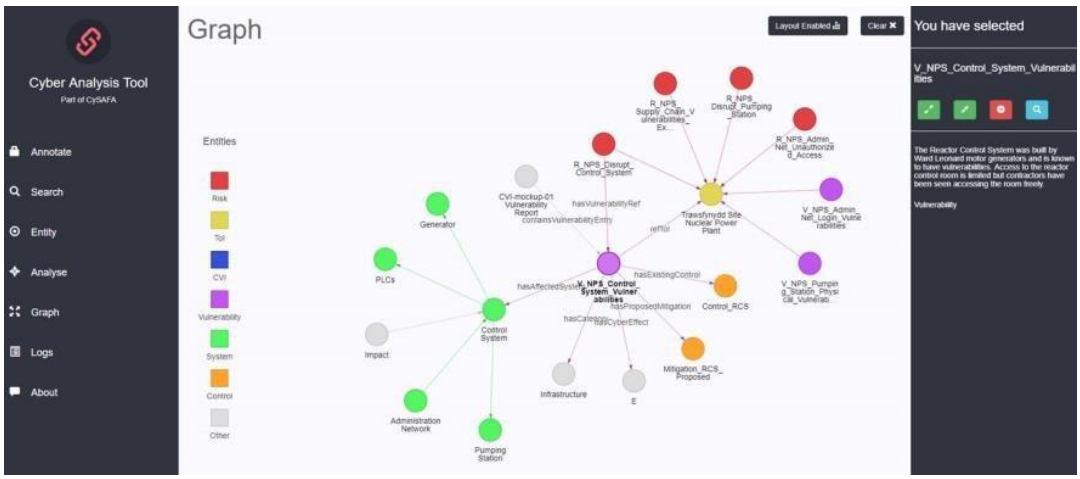
We have provided advice and guidance on emerging and developing standards including STIX v1.0 to STIX v2.0 for normalised Threat Intelligence sharing.

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