Case study

MOD

BT's eCND solution enables the MOD to deter, protect from, react to, and recover from a computer network attack or exploitation

> "With eCND we can successfully complete work that previously took around two weeks in less than 30 seconds. It makes a real difference."

Member
Information Systems and Service
MOD

Challenge

Keeping the UK safe from attack in an era of heightened international threats requires Ministry of Defence (MOD) ICT infrastructures to continuously adapt to emerging threat sources and attack vectors. These include disaffected staff, foreign intelligence services, terrorist organisations, investigative journalists, computer hackers, and criminals (including organised criminal groups). Each may attempt to breach MOD security using a range of mechanisms and methods, potentially compromising UK defence capabilities.

Such attempts are becoming more complex, co-ordinated, and difficult to detect. Defence against them needs to focus on, and be capable of countering, several attack vectors at once.

With different ICT systems, the MOD lacked a cohesive response to actual or attempted network intrusion or disruption. An additional layer of protection was required to bring together an already formidable armoury of security mechanisms. The need was to integrate existing system security information sources to create a centralised security capacity and expand its situational awareness. Detection and protection, as well as monitoring and analysis, were all equally crucial.

Solution

BT designed and deployed a COTS (commercial off the shelf) based cyber-defence solution called eCND (enhanced computer network defence). A fully accredited solution, it delivers round-the-clock support to users.

The use of COTS technology improves interoperability and can enable government departments to improve efficiency and provide increased functionality. Yet its open nature means COTS technology can be vulnerable to the unique risks faced by defence systems. A close relationship with the MOD means that BT is ideally positioned to maximise the advantages of a COTS-based approach, while ensuring that all components meet exacting national and MOD security and safety criteria.

BT worked closely with all stakeholders including the MOD user community, service providers, and delivery partners to assure integration with existing MOD systems. Spanning multiple security domains, eCND maintains separation which allows it to be security accredited up to IL5.

Delivering a holistic view of the configuration and security postures of multiple ICT infrastructures, eCND enables management of threats and threat sources, including a combined multi-domain view where appropriate. This is realised through centralised monitoring and correlation of security event feeds from many different systems, including known vulnerabilities, to identify anomalous behaviour.

All the information is collated and presented to the user to enable a real time view of the MOD ICT estate. Risk analysis and modelling is used to evaluate identified vulnerabilities within ICT systems, and the likely ability of threats to exploit them.

By providing an incident archive, eCND helps the MOD to learn from previous cases. Events can be replayed to better understand risk management decisions and actions taken during the mitigation process, enabling decision-making to evolve. In addition, such data can be searched and linked to new cases exhibiting similar characteristics.

"This proactive problem management approach is one of the most powerful features of eCND," says a member of the MOD Information Systems and Service organisation. "It means we no longer have to waste time fire-fighting because we're always continuously learning."

The BT Differentiators

- Long term, in-depth experience supporting UK national defence, in a close working relationship with the MOD
- Exceptional expertise in the selection and implementation of COTS products, including any necessary integration, customisation and standardisation
- The ability to lead joint design and development teams using established systems engineering frameworks and processes
- Strength and depth of resources to offer comprehensive support including a 24/7 user help desk

Case study

MOD

> “This proactive problem management approach is one of the most powerful features of eCND. It means we no longer have to waste time fire-fighting because we’re always continuously learning.”

Member
Information Systems and Service
MOD

Value

BT has integrated a range of approved COTS products and combined security information feeds into a coherent overarching environment. Information from all MOD security systems is now integrated, correlated, and accessible from a centralised control centre. The centre provides users with the functionality to exploit live and historic data via a common user interface. It also enables risk management-based and fully informed decision-making; ensuring responses are based on comprehensive situational awareness.

Proactive planning and scenario modelling is now widely used to reduce MOD operational risk. The MOD is able to identify vulnerabilities within its ICT estate far more effectively. It can react more accurately and quickly to reduce the window of exploitation open to threat sources. Meanwhile, decisions are based on a comprehensive up-to-date view. Mitigation strategies can be planned and rehearsed in advance – reducing or eliminating the need for reactive responses.

“With eCND we can successfully complete work that previously took around two weeks in less than 30 seconds. It makes a real difference,” concludes the member of the MOD Information Systems and Service (ISS) organisation.

Core BT services

- COTS and CESG-approved products where applicable (not named for security reasons)

Offices worldwide

Registered office: 81 Newgate Street, London EC1A 7AJ
Registered in England No: 1800000

06/11