cds Defence & Security

Tackling Insider Threat

Reducing the risk of cyber security threat from insiders

A matter of global security

High-profile incidents of leaked top-secret documents, including those perpetrated by Jeffrey Delisle in 2007, Chelsea (then Bradley) Manning in 2010 and Edward Snowden in 2013, have shaken the confidence of many governments to share information.

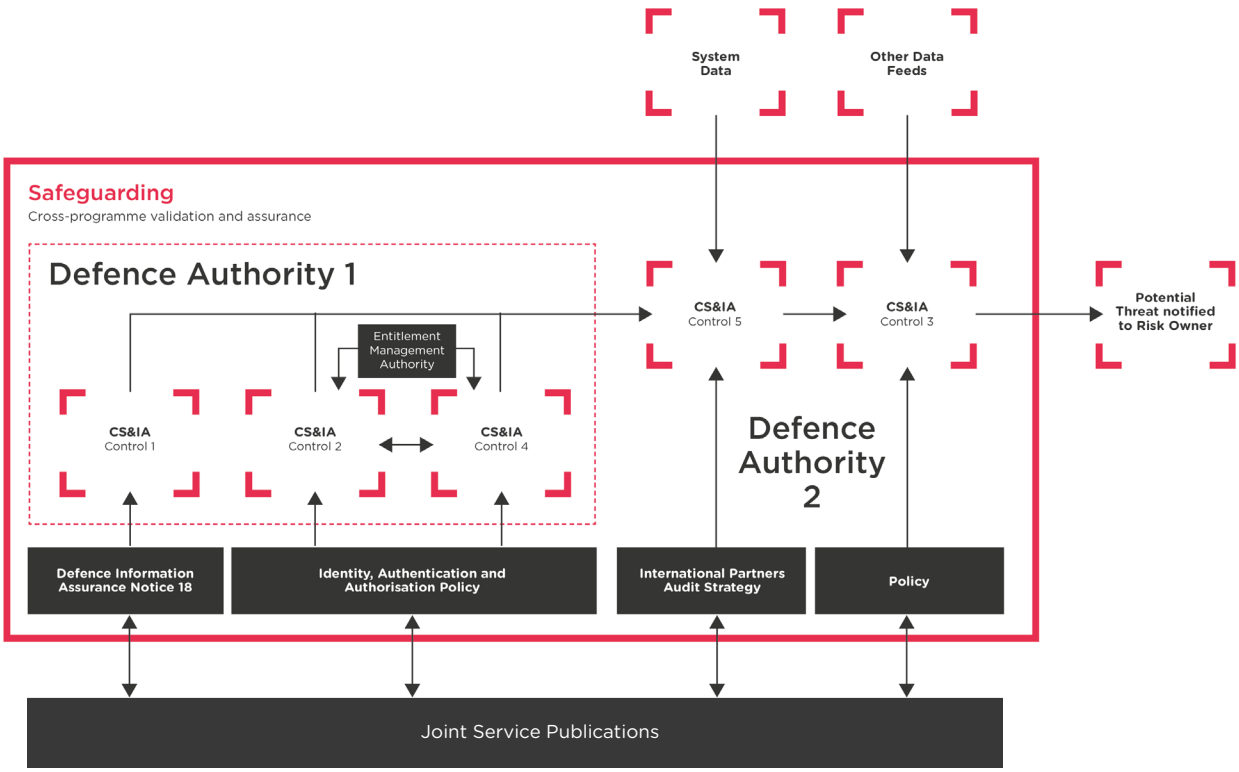
Project achievements

- All requirements met
- Up to 21 embedded experts
- On time delivery
- Whole Force Approach

According to intelligence officials, Snowden downloaded and exposed up to 1.5 million files. To this day, it remains the largest ever leak of classified material containing information concerning the US and its Five Eyes partner nations.

Minimising the threat that 'insiders' pose to national security had never been so pressing. Reducing the malicious, deliberate and unintentional security risks associated would reinstall the confidence of governments to share information.

The Ministry of Defence (MOD) sought to demonstrate the maturity of its insider threat cyber security and information assurance controls by evidencing alignment with US driven compliance standards by an agreed completion date of 31st January 2017.



The perfect mix of experience

CDS Defence & Security (CDS DS) were selected to provide vital support to the MOD Insider Threat Programme; providing an expert team to enable a complex insider threat monitoring and detection capability.

From programme and project management, decision and change support, right through to technical services, enterprise audit, analysis and permissions management, our embedded team became a valued partner in the successful delivery of the MOD's wider SAFEGUARDING programme.

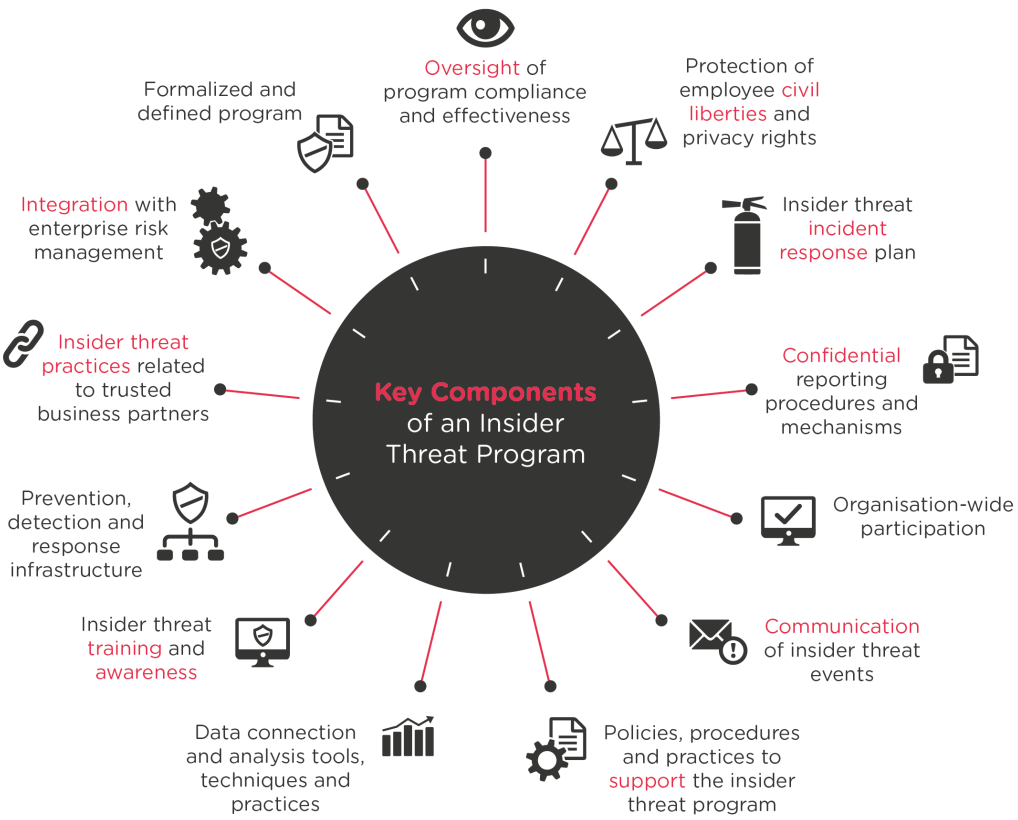
Placing CDS DS experts alongside serving military personnel and MOD civil servants supported the aims of the Whole Force Approach. Our consistent presence and expertise have provided much-needed continuity, which allows for continued progress even when military personnel change over.

The team combines its in-depth defence and cyber security knowledge to consider risks in the context of the complex operational and political environment. Our grounding in behavioural psychology and experience in developing security and data protection training programmes meant that the MOD could be sure of our human-centred approach to mitigating the risks.

100% solution, on time

Our team enabled the MOD to demonstrate its full alignment with US insider threat compliance standards by 31 January 2017, underlining its proactive approach to minimising cyber security risk.

CDS DS continues to support the SAFEGUARDING programme, ensuring our standards and processes



Our approach to mitigating Insider Threat is wholistic, grounded in the US-CERT model, originally developed by Carnegie Mellon University.