CASE STUDY

Defence Digital: Secure by Design Implementation for E-Discovery Capability

Strategic Command
Defence Digital

Overview

Defence Digital (UK Ministry of Defence) urgently required expert security support to enable the deployment of a secure e-discovery capability on an environment classified as SECRET. This platform, used to manage, process, and review highly sensitive digital information, formed a critical component of operations for a sensitive project.

To meet operational deadlines and security obligations, the client needed assurance that the solution would comply with Secure by Design (SbD) principles and the MOD's Joint Service Publication (JSP) 604 requirements, which together ensure robust protection of sensitive information throughout the entire system lifecycle. Unusually, this had to be achieved in a very short space of time.

The Challenge

i3Secure was engaged to provide immediate, expert security support to facilitate the secure deployment and security assurance of the e-discovery capability within a fixed three-month timeframe.

This included progressing the solution through the formal MOD assurance process, achieving Authority to Test (AtT) and Initial Authority to Operate (IAtO). These project milestones have strict requirements which must be approved by specialist boards.

Key objectives included:

- Embedding Secure by Design principles into the system's architecture and delivery.
- Ensuring full compliance with JSP 604 and supporting MOD security artefacts.
- Engaging key stakeholders across Defence Digital, supplier teams, and project delivery functions.
- Establishing effective Governance, Risk and Compliance (GRC) controls for ongoing secure operations.

© 2025 i3Secure Ltd

Our Solution

i3Secure rapidly deployed a Highly Security Cleared Consultant from its pool of professionals already vetted to the highest levels of UK government clearance. This allowed for immediate integration into the delivery environment, ensuring no delay in mobilisation or security coverage.

Operating under the direction of the Senior Responsible Owner (SRO) at Defence Digital, the i3Secure Security SME worked closely with internal MOD stakeholders, the technology supplier, and project management teams to embed security at every stage of the delivery lifecycle.

Crucially, our consultant brought extensive experience from both the military and the UK Civil Service reflecting the backgrounds of many i3Secure team members. This enabled rapid cultural alignment and instant credibility, by already having a deep understanding of Defence ways of working.

As a result, the consultant was able to embed quickly and add immediate value, navigating complex stakeholder relationships and MOD protocols with ease. This is a level of effectiveness that more traditional consultancy models often struggle to achieve.

Key outputs included:

- Conducting robust threat modelling and risk assessments to shape security design and prioritise controls.
- Developing a full suite of security documentation, including:
  - Security Risk Management Plan
  - Incident Response Plan
  - Forensic Readiness Plan
  - Protective Monitoring Strategy
- Ensuring continuous alignment with SbD principles and MOD accreditation requirements.
- Embedding security practices into the Operational Service Model, ensuring resilience, visibility, and capacity for continuous improvement.

Security was fully integrated into the project's core delivery processes, enabling fast-paced, risk-aware decision-making and sustained operational alignment.

The Result

The capability was successfully deployed and accredited within the defined three-month period, meeting all MOD security and operational expectations.

Outcomes included:

- **Accelerated accreditation:** Successful navigation of JSP 604 stage gates (AtT and IAtO) within the fixed delivery window.
- **Immediate mobilisation:** Deployment of a Highly Cleared Consultant ensured no delay in meeting security demands.
- **Operational effectiveness:** Enhanced discovery capabilities improved data retrieval speeds, reduced case durations, and increased document review throughput.
- **Cost efficiency:** Automation within the platform reduced reliance on manual paralegal effort, delivering measurable cost savings.
- **Sustained assurance:** Security governance structures were embedded to support ongoing compliance, monitoring, and readiness.

© 2025 i3Secure Ltd