MINDLINK

CASE STUDY

ECI SUB-COMPARTMENT INTELLIGENCE SHARING

Company
MindLink Software Ltd.

Industry
National Security & Defence

Website
mindlinksoft.com

CONTENTS

Overview

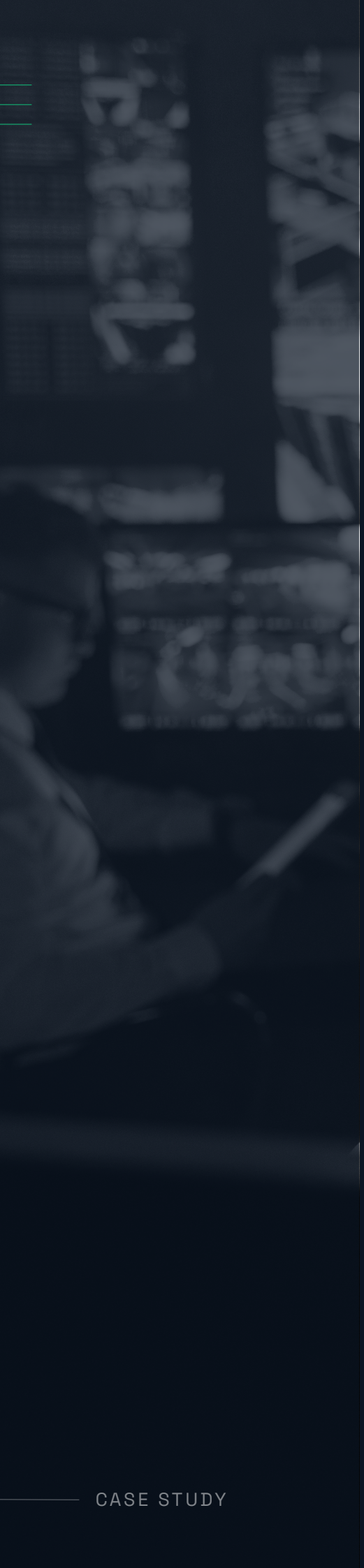
MindLink was deployed by a National Security agency to enable secure intelligence sharing and analysis at exceptionally classified mission levels. MindLink's information assurance capabilities and compartmentalized security model allowed accreditation for above exceptionally classified working and delivered an unprecedented collaboration environment for the nation and its intelligence partners.

Problem

The most critical and sensitive National Security operations occur at the highest classification levels. Referred to as "exceptionally classified information" (ECI), there is a continuous and prevalent risk of such information being compromised by internal or external threat actors, leading to potentially catastrophic consequences for the UK and its coalition nations.

Over the last 70 years, the intelligence community has developed information handling practices for dealing with such classified data and mission activities. The strict application and enforcement of "need-to-know" boundaries ("sub compartments") – with clearly defined ownership and individually managed risk profiles – enables such highly sensitive information and associated operations to be closely protected within minimal, supervised groups.

However, timely intelligence collection and analysis is vital in achieving decision advantage and ensuring positive operational outcomes. The need to protect sensitive data directly impedes the ability for mission participants to share and collaborate at the speed of relevance.



IT tools are typically deployed to facilitate such secure information sharing, but in the customer agency, lack of sufficiently assured products meant that only email was approved for ECI working. Email itself was identified by the customer as inappropriate and in-secure for such sensitive classified operations:

- The email paradigm of branched replies is unsuited to collaborative intelligence analysis: real-time collaboration between many individuals using email is difficult and often leads to fragmented discussions across multiple threads, inhibiting decision clarity and mission outcomes with no single source of truth.
- Email is impossible to secure using sub-compartmented risk-management techniques: the physical location of classified data is duplicated between servers and email clients, multiplying attack surfaces.
- The “need-to-know” is dependent on correct manual user behaviors (i.e. ensuring the right users are copied into each email): day-zero effectiveness of new users is inhibited by the difficulty of locating existing classified data when they are “read on” to a sub compartment; inboxes of users that have been “read off” from a sub compartment remain a perpetual attack as data is not automatically removed.

In light of world events, the customer agency was under pressure to provide a more secure and more effective technology platform for ECI intelligence sharing. Mission operatives demanded a more collaborative and real-time environment, whilst risk-owners and partner nations sought a tool with an elevated and more appropriate high-grade security posture.

Solution

The customer agency deployed MindLink into their classified on-premises air-gapped infrastructure as a secure platform for ECI intelligence analysis and mission collaboration. The system was configured to allow users from partner national and international organizations to access the MindLink web interface over secure network links to support close real-time coalition working.

MindLink’s sophisticated data-centric security engine was used to enforce strict access to sub-compartmented mission data.

The system labels and controls “need-to-know” dissemination of all collaboration information and activities automatically in real-time, with data only residing at-rest in the encrypted backend databases.

MindLink was integrated into existing National Security infrastructure through pluggable integration points to deliver the assurance and accreditation needed for ECI-level working. User identities, encryption keys, and entitlements (attributes) are synchronized from trusted National Security directory servers, and multiple real-time auditing data streams are sent to accredited monitoring and high-grade compliance vault systems.

MindLink’s multi-layered data spillage and data loss prevention controls are configured to provide strong protection for ECI intelligence as automated always-on mechanisms. Such controls are configured on a per-sub-compartment basis, allowing sub-compartment data owners to precisely satisfy their risk profiles on an individual basis.

MindLink’s information assurance USPs combine to deliver a fully-fledged ECI-compatible collaboration platform:

- The data-centric security engine automates data access based on sub-compartment information architecture and additional powerful entitlement-based controls.
- The integration to National Security directory infrastructure automatically synchronizes updates to user clearances and the “need-to-know”.
- The data architecture of stateless web client and column-encrypted backend databases minimizes data-loss attack surfaces.
- The granular, multi-layered, and expressive data-spillage prevention controls allow accreditation for individual sub-compartments with different risk profiles.
- The encrypted data-export controls deliver an accredited path to share intelligence analysis to downstream mission systems.
- The immutable event-based data model delivers a high-definition audit trail of all user activities to meet demanding compliance regulations.

To deliver this project, MindLink worked in close partnership with the customer agency technical program team to design and implement an incremental service rollout to ambitious deadlines. MindLink undertook engineering activities to build plugin components to customer IDAM, PKI and audit infrastructure, and to enhance various data-spillage capabilities to satisfy the demanding and complex needs of individual sub-compartment risk owners.

Outcomes

Deployment of MindLink has delivered a step-change capability for National Security operations at ECI-levels for the nation and its coalition partners. MindLink's automated data-centric security and assurance systems balance the "need-to-know" with the "need-to-share", enabling users to perform more rapid and more collaborative intelligence analysis with a heightened security posture.

The migration from email-based work has mitigated major security vulnerabilities in the use of legacy and inappropriate tools. MindLink's chat room-based collaboration technology delivers a more productive and expedient user experience for intelligence analysis, dissemination, and mission execution.

The MindLink system has enabled and encouraged closer working between operatives from multiple national and coalition agencies. The high-grade accreditation capabilities have given many risk owners and international partner organizations confidence to on-board their ECI working to a shared digital platform for the first time.

The MindLink service has rapidly enhanced the quality and timeliness of the intelligence cycle for the most vital parts of National Security mission operations. Decisions facilitated by MindLink have already contributed operationally to direct avoiding action, resulting in the saving of mission operatives' lives in the face of active enemy threat.

Conclusion

MindLink's high-grade information assurance collaboration platform was deployed to enhance and secure critical operations in National Security. The MindLink security architecture provides operators with an autonomous and capable real-time intelligence sharing capability, whilst meeting the demanding accreditation needs for ECI-level sub compartment information.