Milestone 1.

Mission - Establish a secure (high side) production cluster capable of running the 3 workloads currently on the C4ISR Platform and a sandbox cluster suitable for testing target workloads.

T**arget Outcomes:**

The ASEC and data science applications that are currently running on C4ISR are deployed to the new production cluster.

The C4ISR platform can be decommissioned and is replaced by the new, air gapped (high side) production only cluster.

There is a single, transparent, real time view of the threat level posted by applications running on the High side cluster.

The KPN team have experienced new ways of working; e.g., GitOps. The KPN team are confident they can operate the cluster going forward and have a blueprint to deploy future applications to the cluster.

Acceptance criteria/ measured by:

Bart and Gideon agree to shut off the C4ISR platform, having moved their applications to production on the new platform.

Impact: The C4ISR cluster can be decommissioned.

Milestone 2.

Mission - Deploy and configure a high side Non-Production Cluster. Deploys with Trusted Software Supply Chain (TSSC) features and Dev spaces. Implement a way to track cATO, RMF and sTIGs security requirements making it ready for assessment.

Target Outcomes:

Application development and test environments are deployed High side, there is a working CI/CD (trusted software supply chain) that enables an understanding of risk and the ability to promote a basic application from development to production.

There is a single, transparent, real time view of the threat level posted by applications running on the High side cluster. The solution will enable a shift left to security that supports development teams.

The KPN team has experienced new ways of working to understand and develop the solution. They feel confident they can manage and create policies within the Trusted Software Supply Chain (TSSC) that increases security and reduces developer cognitive load.

Acceptance criteria/ measured by:

A single, transparent, real time view of the threat level posed by applications running on the non-production cluster.

A secure, scalable container image registry.

The ability to securely sign and verify software artefacts throughout their lifecycle.

The ability to track security states of single components, track source code provenance and attestations and provide recommended fixes.

Platform is ready for an assessment against cATO standards

Impact: A single, transparent, real time view of the threat level posed by applications running on the cluster and a step change in security standards. Discussion can commence with the US military regarding access and storage of protected data.

Milestone 3.

Mission - Deploy and configure a low side Sandbox, Non-production, Trusted Software Supply Chain features and Dev spaces in line with cATO standards and the RMF so it is ready for assessment.

Target Outcomes:

Non-Production Cluster with application development and test environments are deployed low side, and there is a working CI/ CD (trusted software supply chain) enabling an understanding of risk and the ability to develop and promote a basic application through the entire development lifecycle until it is ready for transfer to the high side production cluster.

There is a single, transparent, real time view of the threat level posted by applications running on the low side cluster. The solution will enable a shift left to security that supports development teams working Low-Side..

The KPN team have experienced new ways of working to understand and develop the solution. They feel confident they can manage and provide a trusted software supply chain that increases security and reduces developer cognitive load and have a path to promote artefacts from low-side to high side.

Acceptance criteria/ measured by:

A single, transparent, real time view of the threat level posed by applications running on the cluster.

A secure, scalable container image registry.

The ability to securely sign and verify software artefacts throughout their lifecycle.

The ability to isolate components, track source code provenance and attestations and provide recommended fixes.

Platform is ready for an assessment against cATO standards

Impact: A single, transparent, real time view of the threat level posed by applications running on the cluster and a step change in security standards. The resulting cluster and promotion processes support discussions with the US military regarding access and storage of protected data.