

Ian Mungovan Boarding



2023-01-20 | Ian Mungovan | Boarding Rolls-Royce

Boarding Packet

Ian Mungovan is a DevSecOps Engineer that specializes in Cloud Native Development, Agile Methodology, and Digital Transformation. Ian also is a Cybersecurity Officer in the Army National Guard and holds an interim Top Secret Security Clearance. He has experience with multiple programming languages, DevSecOps, and Cybersecurity. Holding a degree in Mechanical Engineering with a specialization in unmanned robotic systems, Ian has a passion for learning, efficiency, and leadership.

- **Ian T. Mungovan**
- **Role:** Digital transformational Specialist
- **Education:** Embry-Riddle Aeronautical University, BS Mechanical Engineering
- **Professional Origination:** Cyber Security Officer Army National Guard, OWASP Member
- **Clearance:** DOD Top Secret Security Clearance
- **Time in Role:** 2 years in Digital Transformation Role
- **Certifications:** CompTIA Security+, VHL, Udacity Cloud Native Developer, Udacity Azure Cloud Developer,

Software Factory

The Software Factory is the group of people working to build applications from within Rolls-Royce. It is attempting to organize both formal full-time app developers and part-time developers working on small to medium-group-level software. There is a push to not only develop more applications in-house but to have regular people work on them. Ideally, it will foster a large group of people throughout the business working 10-20% of their time on small applications, which will help their groups and Rolls-Royce as a whole.

Stakeholders

A stakeholder map has been created by Josh Haines to support both the digital transformation team and the Software Factory. This map can be accessed using 2nd level F5 and will highlight the teams that Ian supports in the Software Factory and as part of Project Catalyst, as seen below. Stakeholder Map

<http://docs.uscdz.local/files/customers.html>

Tasks

- **Maintainer:** Ian is one of the two Maintainers in the Software Factory. He helps support 60+ citizen developers (part-time programmers) and over 30 different web applications. Deploying both on-premise and into the Azure Gov Cloud, using industry best practices.
- **Frontend Development:** Frontend developer that uses JavaScript/Typescript with Vue framework to develop web applications. I conduct testing using Jest and Cypress. Applications are built into static web apps for deployment or are containerized to be deployed.
- **Backend Development:** Backends are built using python with fast API and typeORM. Node backends are built using Node and Prisma. Ian has built both GraphQL Apis and RestAPI's both have been implemented with authentication.
- **Database Administration:** Ian has Deployed and Managed PostgreSQL, Azure SQL, and MongoDB, database systems using both on-premise using the Controls Collaboration Zone and off-network using Azure Gov Cloud.
- **DevOps:** Has written Automated Pipelines in GitHub Actions and GitLab Pipelines to conduct approval to operate standards. Containerized Applications and deployed them using Docker into both Collaboration Zone and Azure Gov Cloud. Has built logging to monitor deployed applications
- **Cloud Security:** Manages allocated ports and firewall access to applications deployed in the Azure Gov Cloud. Has also configured networking for docker containers in the Collaboration Zone.
- **Technical Writer:** Documented best practices for deploying applications and securing firewalls in accordance with industry best practices, while also documenting web apps that are developed in the Software Factory.

Catalyst

Catalyst is implementing modern DevSecOps in line with the DOD. Moving forward outside the standard IA & IT Security processes with an accepted risk profile in order to forge a fresh path of continuous compliance with automated testing, in line with the DOD DevSecOps 2.0 Playbook and industry best practices. Catalyst uses GitHub Enterprise to store our source code, a platform used by 65 million developers and more than 3 million organizations. This platform represents the future of source code managers for Microsoft and the most used and capable source code platform which exists today. Catalyst also uses the Azure commercial and government clouds as appropriate as well as on-premise servers if necessary. As well as using compliant pipelines and continuous Authority/Approval to Operate (ATO) models as recommended by the DOD.

Stakeholder

Josh Haines has created a stakeholder map to support both the digital transformation team and the Software Factory. One can access this map using 2nd level F5 and will highlight the teams that Ian supports in the Software Factory and as part of Project Catalyst, as seen below. Stakeholder Map <http://docs.uscdz.local/files/customers.html> Currently helping to deliver the Safety Assurance framework application recently tasked by Gareth Jones to the Software Factory. I will be taking the lead with cloud deployments, security, and user authentication and authorization for the application. This application will be the first to use real data in the Gov Cloud for the software factory and will enable future delivery of real applications into the Gov cloud. Building ATO and cATO tool called OGRE to allow Rolls-Royce to have an automated cATO system in place. This will be leading for both Rolls-Royce and the aerospace industry and will allow for stronger security while also enabling faster delivery of digital activities.

Tasks

- **Coach:** Ian helped coach and develop four GDP's assisting in the development of Catalyst from Aug - Dec 2022, using modern cloud-native architecture.
- **Gap Analysis:** Has written several gap analyses that highlight where the DOD requires us to be from a Digital Standpoint, and how Rolls-Royce compares. This includes the DOD, E-Series, and CMMC Gap Analysis.
- **DevOps Documentation:** Ian is helping to write the output of Catalyst which will be documentation that highlights the guard rails that one must stay inside for the new approval to operate when developing software.
- **Purchasing:** As part of Catalyst, Ian has been involved in the purchasing of GitHub Enterprise, the world's largest git repository. He also assisted in the purchasing of Snyk a static/container scanning security tool, that is used in automated security scanning of all codes developed in GitHub.
- **Branding:** Ian has been involved in the rebranding of Software Factory as part of Catalyst. This has been in coordination with Midwest Studios.

Army Cyber Officer

Ian is a Cybersecurity Officer in the Indiana National Guard. As part of this, he has his interim Top Secret Clearance and will have his Top Secret Clearance by the end of 2022. They accepted Ian into the US Army Cyber school at Fort Gordon, Georgia. He will spend 37 weeks training with US cyber command on a variety of cybersecurity concepts and will graduate with over 30 industry-recognized cyber certifications. Ian will be attending Army Cyber School in 2023. In the meantime, he will be actively training and working with the Army Cyber Command.

Stakeholder

Supports Cyber defense for the state of Indiana as well as supporting the cyber defense for the United States Army, Homeland Security, and the whole of the United States.

Tasks

- **Leads:** Ian leads a ten-person cybersecurity team that supports cybersecurity for the State of Indiana and the US Army. This involves both leading soldiers directly under his command and working with other leaders across the US to secure the nation's cyber infrastructure.
- **Secures:** Works with networking and serves as an InfoSec specialist, securing applications as an Application Security specialist, and working as a cybersecurity leader.
- **Trains:** In charge of training and developing soldiers under his command. Making sure they are certified to industry standards in cybersecurity and equipped to get the mission done.
- **Operates:** Ian runs several projects in coordination with other teams around the country supporting the nation's cyber-security.

Future Goals

Ian's future goals include becoming the lead platform and application security engineer for the Software Factory. This includes being responsible for future cloud operations and security for the Software Factory and the teams that it supports. He also plans to increase his work with Liberty Works by leveraging his Top Secret Clearance support past and future clearance programs. He also plans to continue to work with the Army Cyber Command and the Indiana National Guard to secure the nation's cyber infrastructure.