



BCDevExchange

DevOps and Cloud Services

Preparing your Organization for DevSecOps

Product Owner: Olena Mitovska

Security Architect: Nick Corcoran

A decorative graphic on the left side of the slide, consisting of a solid blue triangle pointing downwards and to the right, partially overlapping a larger, outlined white triangle that also points downwards and to the right.

Q1: How did you tackle the idea of making BC Gov's Private Cloud SaaS the best security platform in the public sector?



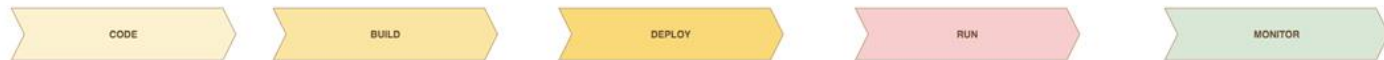
Q1: How did you tackle the idea of making BC Gov's Private Cloud SaaS the best security platform in the public sector?

"Divide and Conquer"

- **Network Security** with Zero-Trust Model
- Container and Image **Vulnerability Scanning**
- **Secrets Management**
- **Logging/Monitoring**
- **Security Awareness**

What we have in store for you...

BCGOV DevOps Security Toolkit Map



DEVOPS SECURITY TOOLS

Version Control System

GitHub

- Open-source collaboration
- Gov-specific compliance and governance
- Write Access control (BCGov org members only)
- Private reports for closed-source code

Dev Best Practice and Compliance Enforcement

Repo-mountain

- Custom developed "robot"
- Dev best practices and good ethics enforcement
- Email notifications for violators
- Continuous STRA and PIA completion check

Automated CI/CD Pipeline

Jenkins

- Pipeline Governance
- Integration support

CircleCI

Azure DevOps

Singer Actions

Argo

Static Code Analysis

SonarQube

- Code bugs and vulnerabilities discovery
- Code scan at each commit

Trusted image repository

Artifactory

- Secure artifact management for images and libraries
- Inherent audit trail

Container Technology

RedHat Containers

- Minimized attack through OS segmentation
- Security Enhanced Linux kernel model
- Multi tenant separation
- Enforced non-root access

Kubernetes

Docker

Secret Management

Vault

- Secure vault for application credentials

Production Deployment GateKeeper

Aqua

- Enforced integration with mandatory security tools for production deployments

SSO and Access Mgmt

Keycloak

- Openshift platform authentication
- Application authentication
- Federated identity from IDIR, GitHub, BC Services Card and BCeID

Zero-Trust Network Enforcement

Kubernetes

- Application-identity based network security policies (OCI Levels 2 to 7)
- "Default Deny" base policy
- Developer-controlled at application level

Platform Built-in Security

OpenShift Container Platform

- Multi level High Availability (HA)
 - Application HA
 - Openshift Cluster HA
 - Data Center HA (DR Site in Calgary)
- Regular platform vulnerability scans and penetration testing
- Red-Hat Certified Image Catalog

Platform Built-In Resiliency

- Virtualization
- Load Balancing
- Dynamic Elasticity

Security Hardware and Software

F5 Firewall

Container Scanning and Monitoring

Aqua

- Container image vulnerability alerts
- Dynamic scanning of running applications

Network Security Monitoring

Network Security Monitoring

- Dashboard for MISOs and ISBs to monitor application network security policies

Platform Services Monitoring

sysdig

- Platform Capacity Monitoring
- Platform Service Availability and Performance Monitoring
- Application Monitoring

Intrusion Detection

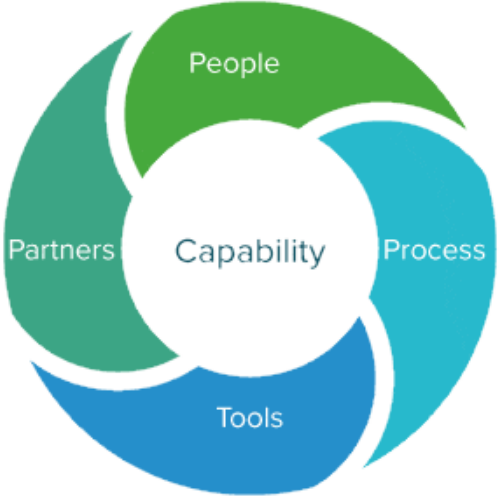
Tripwire

LEGEND:

Work in progress

ENTERPRISE SECURITY TOOLS

Improving Security Capabilities in DevOps





Q2: How do you keep your community engaged with you and one another?

A decorative graphic on the left side of the slide consists of two overlapping triangles. The top triangle is white with a thin grey outline, and the bottom triangle is a solid blue color. They overlap in the middle, creating a blue-shaded area.

Q2: How do you keep your community engaged with you and one another?

Purpose/Vision - shared every time we meet

- To **build** a constantly **improving** application platform for delivery of **modern** government services
- To **inspire** a DevOps **culture shift**, which values **open-source, collaboration, communication & speed**
- To **create** a community that **takes care of each other** and works together to solve the unsolvable



Q2: How do you keep your community engaged with you and one another?

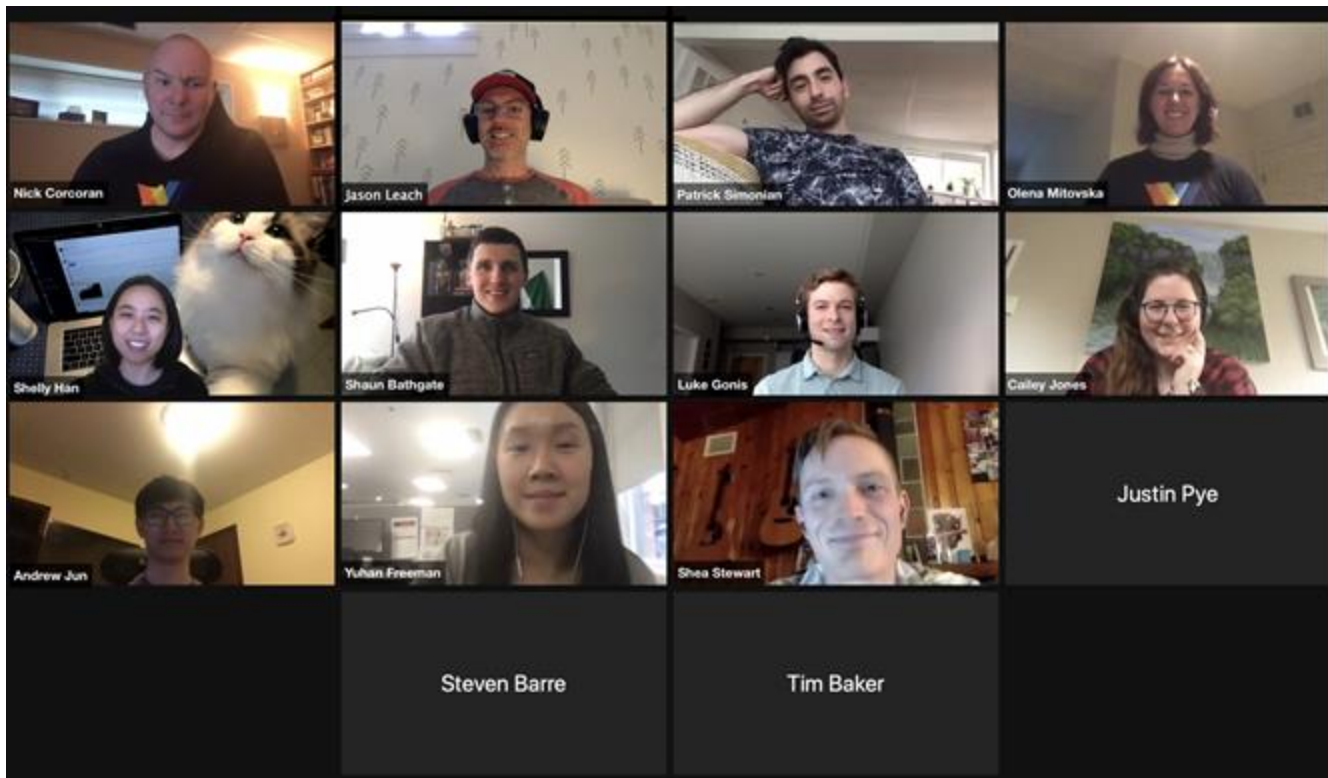
Purpose/Vision - shared every time we meet

- To **build** a constantly **improving** application platform for delivery of **modern** government services
- To **inspire** a DevOps **culture shift**, which values **open-source, collaboration, communication & speed**
- To **create** a community that **takes care of each other** and works together to solve the unsolvable

And...

- Teams are invited to demo their work in our sprint reviews
- Common Components
- Feedback for features/products
- Comms platform

The BC Gov's Platform Services Team welcomes you to the Community!



Watch our [Team Introduction Video](#)!!!!





Q3: How do you ensure the platform and hosted apps are available when you need them?

Q3: How do you ensure the platform and hosted apps are available when you need them?

- **High Availability** is built into the **OpenShift Platform** itself
 - Multi-node

Q3: How do you ensure the platform and hosted apps are available when you need them?

- **High Availability** is built into the **OpenShift Platform** itself
 - Multi-node
- **Tools** available to app teams to **make apps highly available**
 - Multi-node
 - HA database solutions
 - DR site

Final State: OCP 4 cluster services

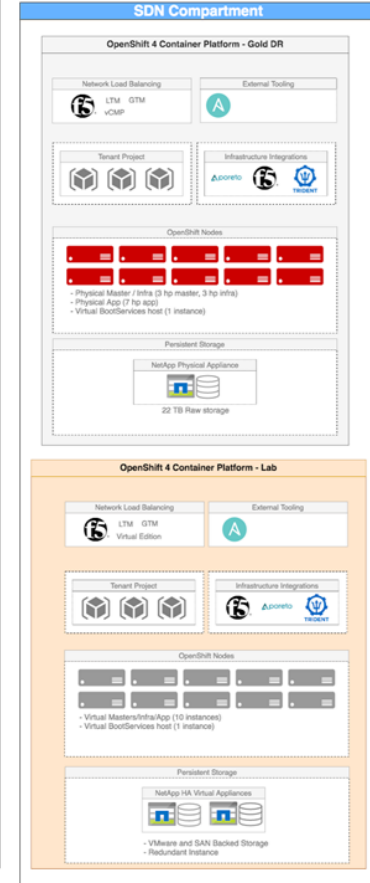
Azure



Data Centre A



Data Centre B





Q4: How do you empower others
implement security?



Q4: How do you empower others implement security?

- Give developers **self-serve tools that are easy to use!**
- Zero-Trust Model
- Image and Vulnerability Scanning (coming soon)
- **Pipeline templates** (coming soon)



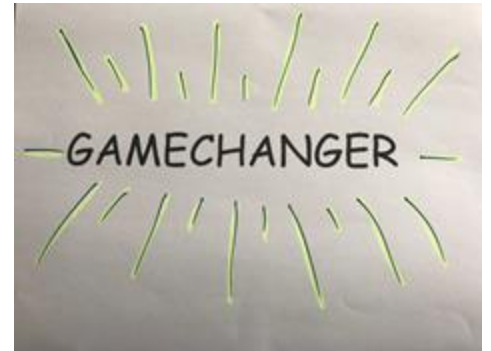
Q5: What does it take (resource-wise)
to run a platform like this?



Q5: What does it take (resource-wise) to run a platform like this?

- We started as a **Pathfinder project** with limited staff and invited experienced teams who loved experimenting with new tech
- To become more enterprise ready, we needed to **educate community and onboard more staff** to support
 - ~10 gov staff, 5 contractors, data centre support staff (4) all working together
 - Product **teams rely on each other for support** and only reaching to Platform Services Team if they cannot get help from the Community
 - Most cluster and tool management as well as project provisioning is **automated through GitOps and infrastructure as a code**

We're Better Together!



Thank you



PS: Remember -> Try. Experiment. Iterate.
Fail. Try again. Change the world, together!

