Shift Left Compliance & Security

Jim Doran, IBM
What’s at Stake

Brand reputation
25%
company value attributed to reputation

Client trust
69%
of consumers believe companies are vulnerable to cyberattacks

Financial fines
$425M
Fines levied on Equifax to help people affected by the data breach

Skills shortage
1.8 million
unfulfilled cybersecurity jobs by 2022 facing CISO

Compliance
$31M
Average cost for Financial Services Company

Complexity
94%
of organizations have multiple clouds

Industry Pain points
We have integrated the IBM Cloud hosted in data centers dedicated to the bank. We will also strengthen our Hybrid Cloud ‘As a Service’ capabilities using IBM solutions offered via its public Cloud to support the development of new services, including Continuous Delivery, Tekton pipelines, test and applications environments.

- IBM Banking Client
I need to ensure that my organization workloads comply with regulations and security best practices by setting guardrails around what application teams can do, by continuously monitoring the security and compliance posture and identifying violations, and by collecting evidence for audit without disrupting agile development processes or application availability.

- IBM Financial Services Client
Securely Develop at the Speed of Cloud

- **Agile** transformation *requires Cloud* to maximize benefits
- **SecDevOps** is the way to develop *securely and efficiently* for Cloud

Need both **Speed and Control**:
- **Deploy** >20 times per day with **quality**
- **Automate** toolchain with quality & security gates
- **Use** Templates
Need both **Speed** and **Control**:

- Deploy >20 times per day with quality
- Automate toolchain with quality & security gates

**SecDevOps** is the way to develop securely and efficiently for Cloud.

---

**Cloud Native Apps require increased scope**

**Pre Cloud Era**

- Open Source Libraries
- Application Code
- IT Apps
- Virtual Machine Config
- DataCenter / Network
- Hypervisor
- Hardware

**Cloud Native Era**

- Open Source Libraries
- Application Code
- Cloud Services
- Containers
- Network Mesh
- Kubernetes
- Cloud

*DevOps drives infrastructure to be part of the application*
Anatomy of a modern cloud application

*conf configmaps secrets

Vulnerability Checks  Network  Bill-of-Material / Evidence  OpenSource Licenses  Third-party Service  CIS Checks  Cloud Services
Pipeline Integration
- **PR Pipeline** – Trigger checks on every pull request
- **CI Pipeline** – Trigger checks in every build pipeline
- **CD Pipeline** – Trigger checks before every deployment

Developer Feedback
- **PR Comments**: All findings are reported as comments to PR in PR pipeline
- **Issues**: In CI/CD pipeline, any failures are reported as issues

OPA-based Policy Control
- Policy configuration are defined out-of-band of pipeline
- **Pipeline Gates**: Control PR merge through policy gates
Code Risk Analyzer

Automate security and compliance checks and remediation based on static assets in git repository, leveraging threat intelligence from Snyk and Clair.

Vulnerability Scans
- Discover vulnerabilities in your Application (python, node, java, golang) and OS stack (base image) based on curated threat intelligence from Snyk and Red Hat Clair
- Recommendation to fix vulnerabilities
- Auto-remediations for some available fixes via pull requests
- Continuous monitoring against new vulnerabilities and automated notifications

Deployment Analysis
- Discover misconfigurations in your deployment *.yaml against CIS Standards

Bill-of-Materials
- Generate Bill-of-Materials accounting for all the build dependencies and their sources for your application
- BoM-Diff to allow comparing diffs in any dependency w.r.t. base branch

Network Policy Analysis
- Built-in Checks to identify any redundancy or gaps in network policies

Terraform Configuration Analysis
- Parsing terraform templates for different cloud services (IAM, COS, CIS, LogDNA-AT) to discover any security mis-configurations
- Implements 20+ policy checks, all anchored around NIST controls
CI pipeline

**CODE**
- Detect secrets in code
  - Code reviews
  - Unit tests
  - Open source scan
  - Static code scan

**BUILD**
- Build deployable artifacts
  - Sign deployable artifacts
  - Run vulnerability scan
  - Open source scans
  - Dev deployment

**Setup**
- Code extract
  - Toolchain CRN
  - Fetch credentials
  - Fetch evidence locker
  - Fetch code

**Code Reviews**
- Build DOI publish
  - BuildRecord

**Unit Tests**
- Code unit tests
  - Create issue
  - Create evidence

**Static Code Scan**
- Code vulnerability scan uploader
  - Code vulnerability scan
  - Create issue
  - Create evidence

** Completion**
- Build pipeline evaluator
Traditional agile approach

- Siloed roles and level of expertise
- Fragmented / bypassed security checks
- Lack audit readiness
- Lack of visibility into development process
- Reactive and time-consuming security remediation
- Runtime Probes required

Continuous Dev + Sec + Ops

- Auto-Remediation fix vulnerabilities / config
- Consistent security patterns (pipelines)
- Immutable runtime platform
- Continuous threat intelligence model
- Proactive Audit readiness
- Security checks scale with Development process
Backup slides