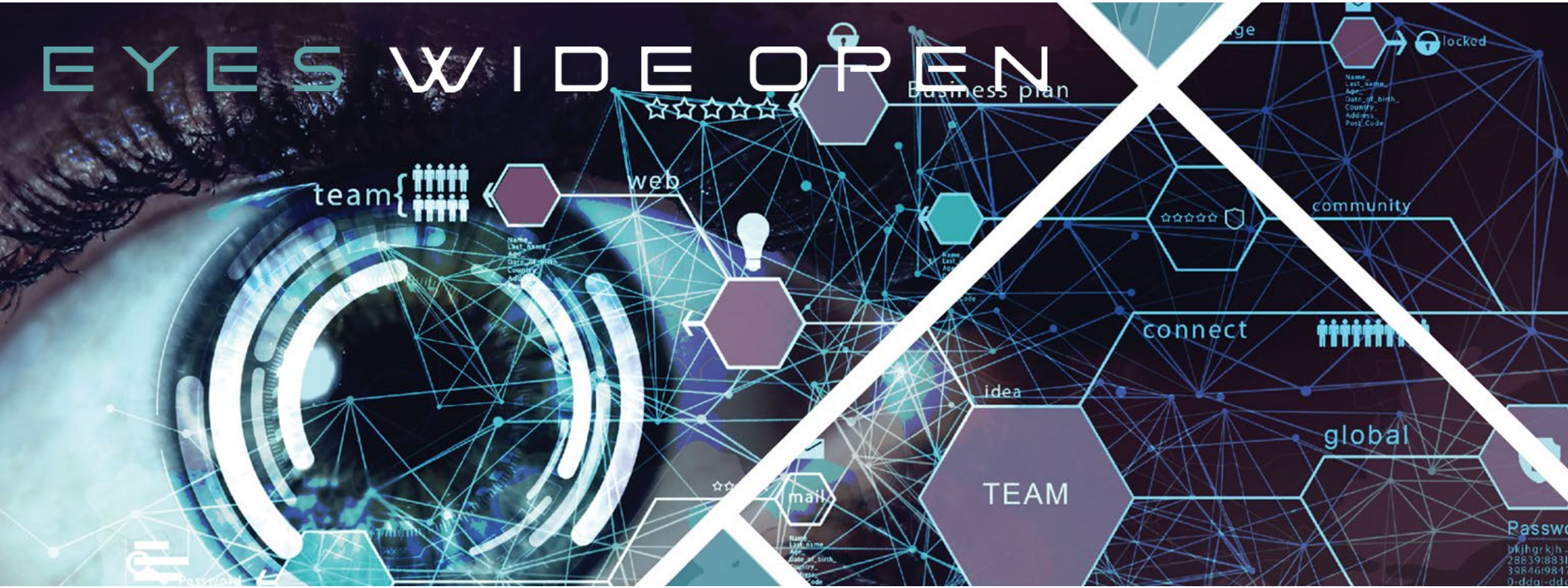
12TH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

TITLE SPONSOR

Island



DevSecOps: Shifting Security Left

The future of application security is here and it is called DevSecOps. Security can no longer be a “thing” you do at the end of a project and only if you have time. Security cannot be optional but integrated organically throughout the lifecycle from the start. Shifting security left is more than a process, it’s a shift in culture, mindset, development practices and project management.

Introduction

Drew Koenig

- Principal Security Architect, Federal Reserve 9th District
- 20 years in IT and cybersecurity
- Financial, healthcare and consulting industries
- Daily Podcast host, Security In Five

Security, Why Do We Care?

- Simply, breaches are expensive
  - Decrease/Loss Customer Confidence
  - Loss of profits
  - Fines, lawsuits, additional operational costs
  - Remediation, forensics, personnel

- It’s our job!

Threat/Response Are Misaligned

- Approximately 50% of cyberattacks are at the application layer
- Yet less than 1% of security spending in on the app. layer
- The problem is traditional security focuses on the ‘networks’ and ‘systems’ not the applications
- In the world of DevSecOps security cannot be an afterthought

Application Development

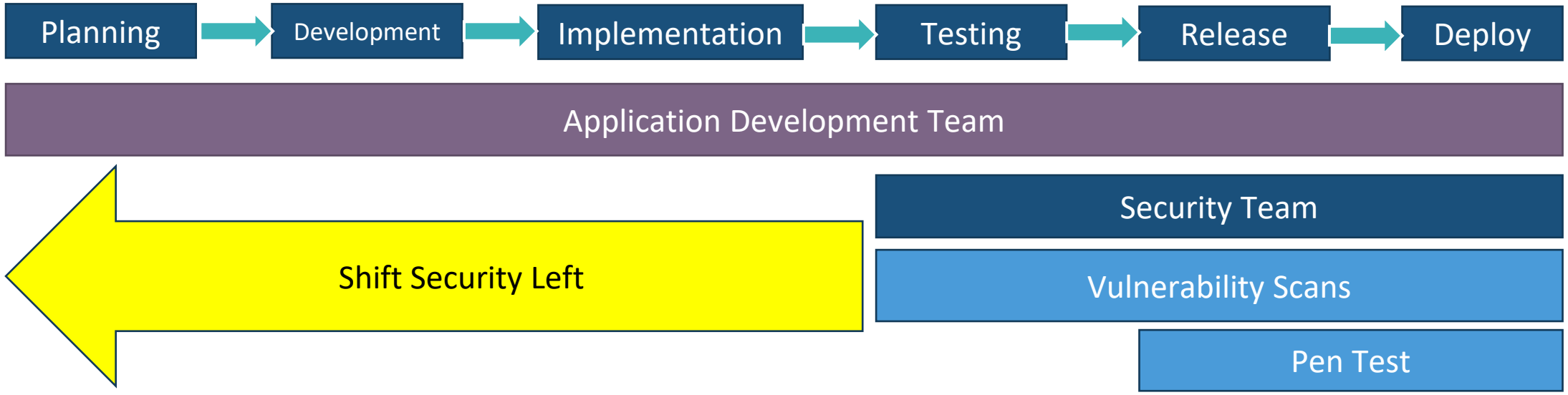
- The cloud evolution has changed application development forever
- Small, fast, component based development
- Several releases more frequently
- Compressed timelines
- The traditional methods of security don't fit this model

Attitudes

- Traditional security practitioners ‘measure’ and ‘control’ – *They Audit*

- Traditional application developers ‘develop’ and ‘build’ – *They Create*

The Old Security Mentality Is Outdated



- Traditionally release schedules dictate remediation efforts
- Security findings, flaws, vulnerabilities are “accepted” and pushed to the next release
- The next release may be months later, increasing risk
- Time to shift security left

DevOps

- Development Operations (DevOps) focuses on getting an application to market as fast as possible
- Like the traditional model, security testing is separate, at the end of development prior to deployment

DevSecOps

- Development Security Operations (DevSecOps) includes security into the SDLC-CI/CD process
- Security practitioners are at the planning table
- Security stories are added Sprint 1
- Security test cases are built alongside development
- Most security vulnerabilities are design flaws, not bugs, and won't be found through traditional scanning

How?

- There is no silver bullet, no formula, no clear roadmap

- It comes from training
- It comes from process
- It comes from thinking about security like –
  - QA & Change Control

Organic Inclusion

The trick to security in DevSecOps is combining the security controls into the creative process

Cultivate a security attitude with everyone

DevSecOps - Security Everywhere (To The Left)

- Secure Application Development
  - How are the apps built regardless of hosting site
- Deployment Security
  - How is the app deployed and executed
- Environment Security
  - Where does the app 'live'
- Operational Security
  - Scanning, testing, reviews, compliance, remediation

Security Is A Specialty Not A Singular Role

- Assess and Profile
  - What are you building, what are the security risks
- Prioritize and Plan
  - The balance between security protections and business functionality
- Enable and Enhance
  - Enable developers with security tools to enhance your security visibility
- Educate and Operationalize
  - Awareness, contextual reports, automation
  - Always answer – *"So What?"*

DevSecOps Control Areas

Security Architecture	Authentication / Authorization	Application Code & Environment
Design	User ID and Onboarding	Input Validation
Security Configurations	Account Provisioning	Cryptography
Secure Development	Passwords	Secure Communications
Security Operations	Authentication	Data Confidentiality
Security Policy and Regulations	Multi-Factor Auth	Information Leakage
Threat/Data Modeling	Session Management	Logging and Auditing
Compliance	Authorization	Code Reviews
	Zero Trust	Secure Repos
		Vulnerability Mgmt.

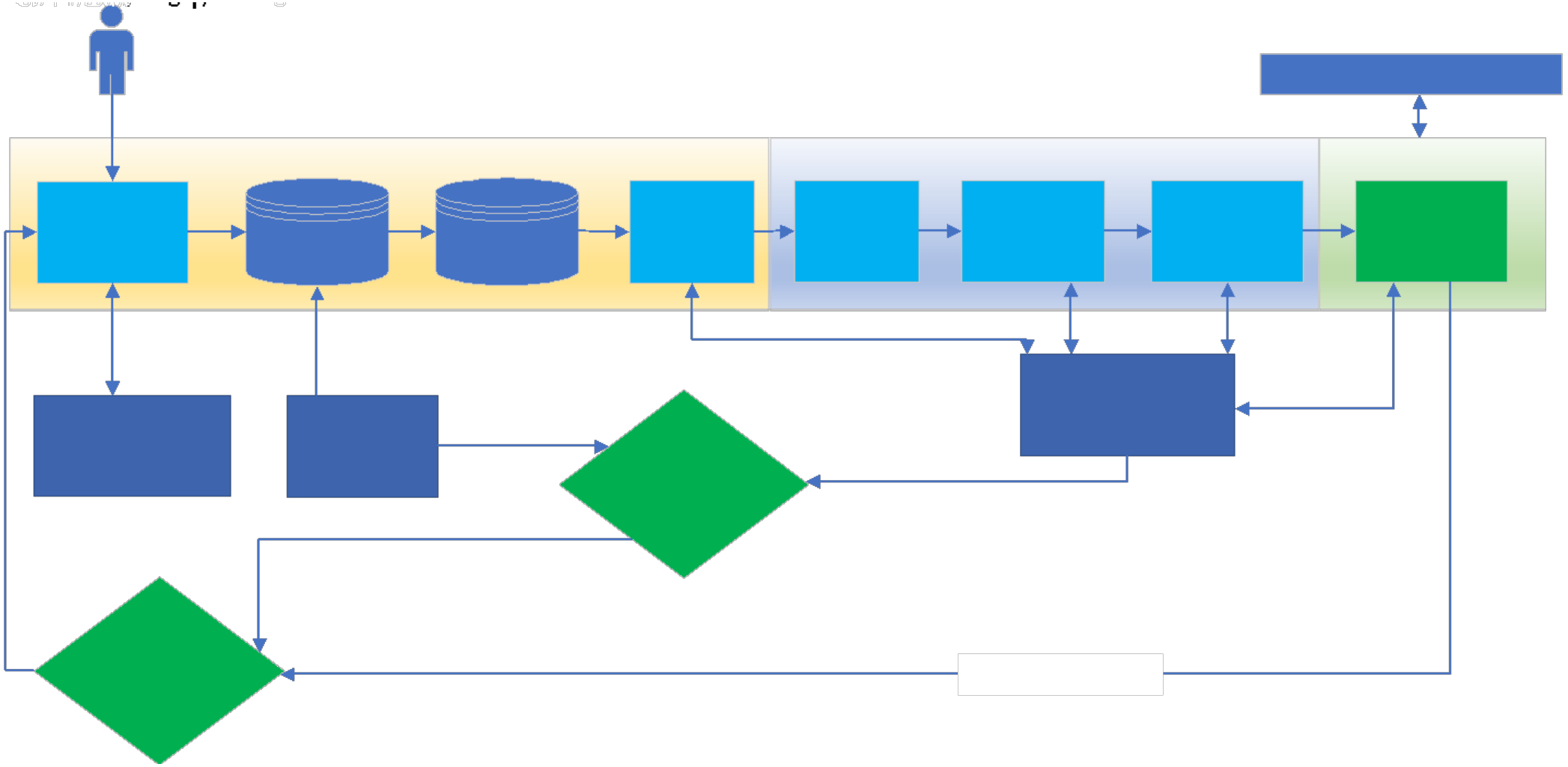
DevSecOps Cloud Control Areas

Cloud Security Control Areas To Consider		
Encryption	Key Management	Multi-Factor
SSO / IAM (cloud portal and app integration)	Log Collection	Incident Management
Geo-location	Anti-virus / Patching / Vulnerability Scanning / End point protection	Server/VM/Container deployments
Security Testing	WAFs	Firewalls
Tenancy	On-Prem Connectivity	Scaling

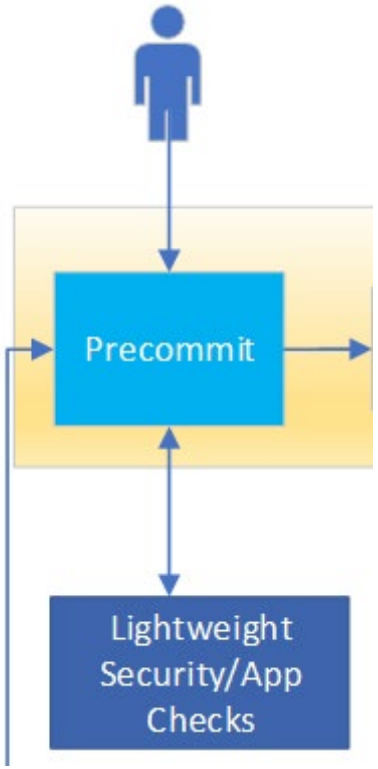
It Is No Longer Just The Security Team

- In the evolving application world, leaving security solely with the security teams will ultimately fail
- Security people are very smart, but not globally knowledgeable
- Expertise in each control/business area is needed
- It is far easier to include security concepts into existing expertise than attempting to make security experts be experts in everything

DevSecOps Maturity Model

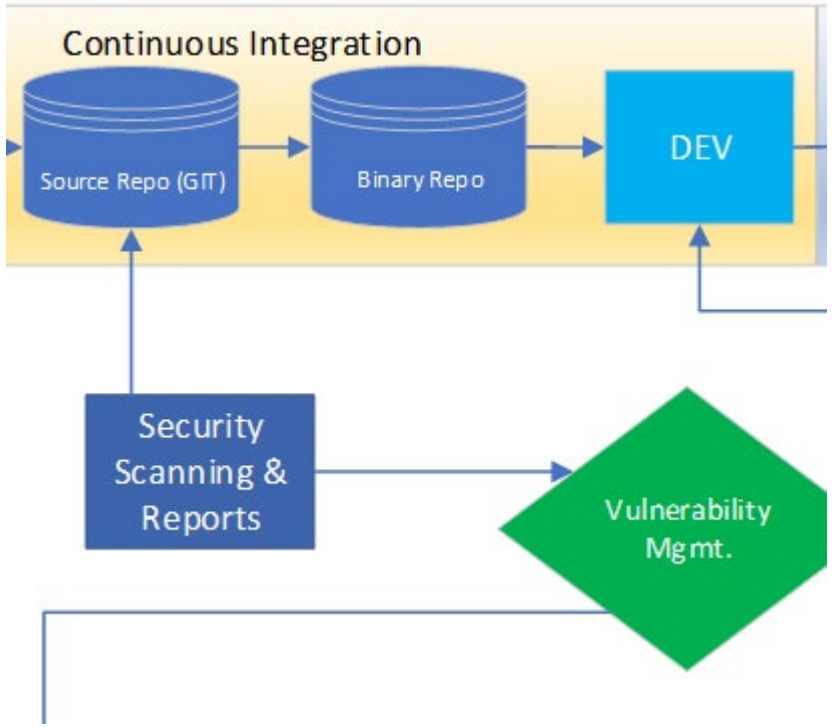


Precommit



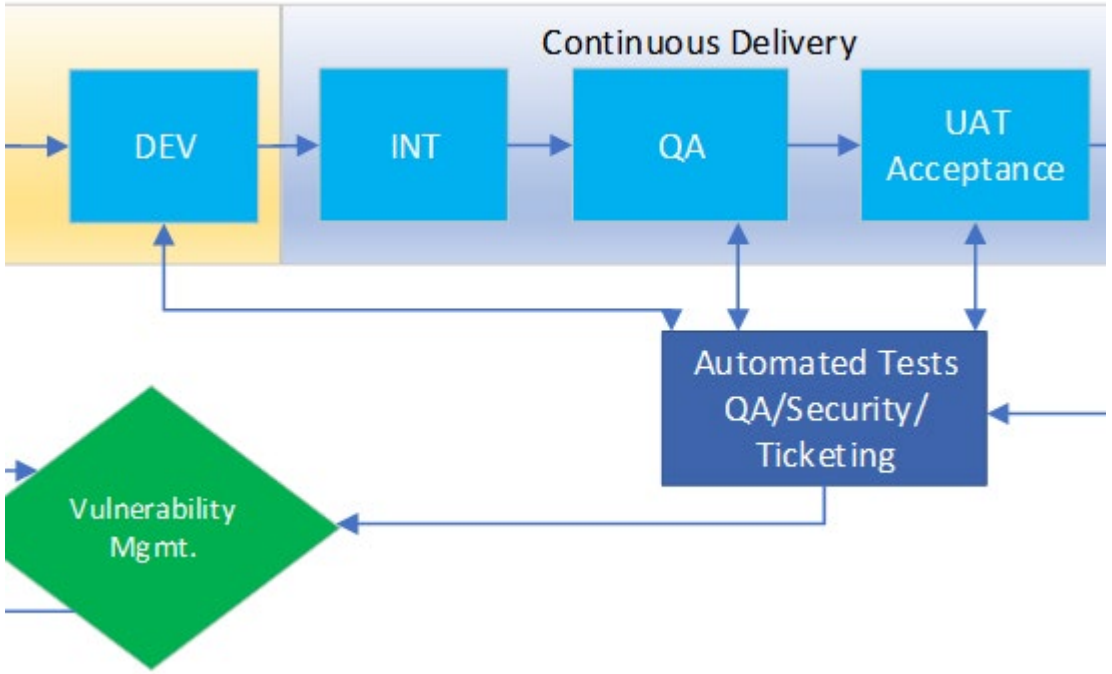
- Lightweight checks *(Enablement)*
  - Peer Code reviews
  - Risk Assessments, if required
  - IDE plug-ins for ‘real time’ security scans
  - Developer driven security

Source Repository



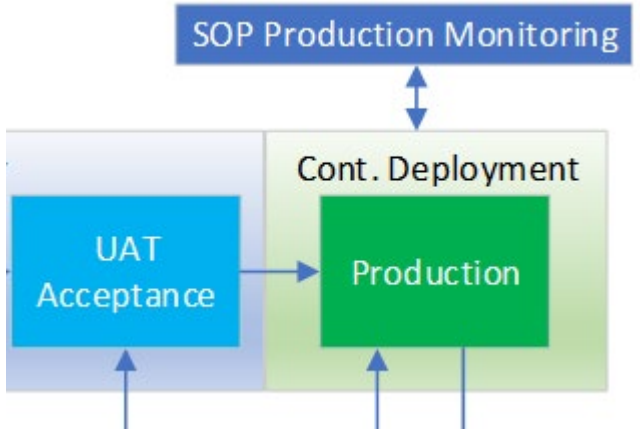
- Code Check-In *(Automation)*
  - Static Code Analysis (SAST)
  - Open Source Analysis
  - Bulk Scanning before leaving Dev.
  - Security/Logic gates to prevent vulnerabilities from moving forward

QA



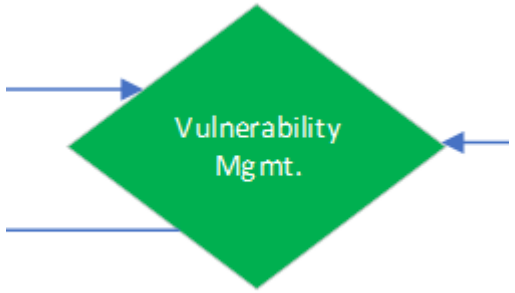
- QA/UAT
  - Automate, automate, automate
  - Security functional testing (DAST)
  - Application security scans
  - Environment scans, configuration verifications
  - Validate security requirements and model verifications
  - Fuzz testing, injection attacks, XSS, session mgmt. testing, Auth/Az, etc…

Production



- In Prod, clone of prod, pen tests
- Continuous Monitoring
  - SIEM
  - IDS/IPS monitoring
  - Regular vulnerability scanning

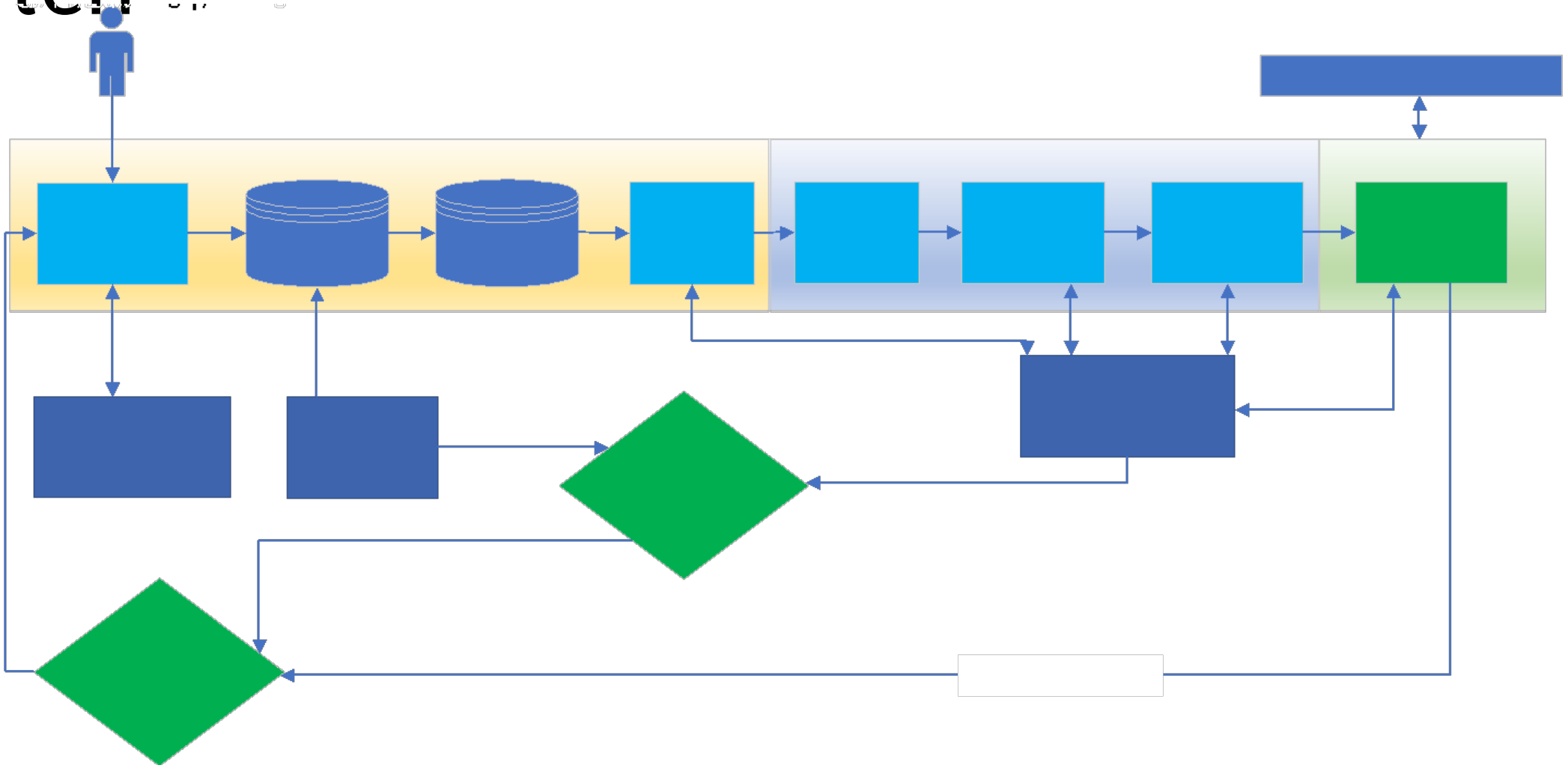
Vulnerability Feedback Cycle



All areas of testing security or otherwise will use a central vulnerability management solution to track and help prioritize remediation

- May be the Agile manager tool, a separate enterprise vuln mgmt. solution
- Vulnerabilities and findings need to be reviewed and backlogged properly
- Policies and logic gates need to be created to define promotion criteria as a release moves toward production

DevSecOps Model – Shift Left, Early & Often



Empower Security In Everyone

- Security is everyone's responsibility
- Security Champions, from the CISSP, helps extend security empowerment to non-traditional security resources
  - Developers
  - Architects
  - Business Analysts

- When everyone is thinking about security, your coverage expands

DevSecOps Is A Journey

- Security is subjective, optional
- You can choose to apply security concepts or not
- Security also has to be adopted by the end users
  - Overwhelming & complicated controls will push people to go around them or not build them

DevSecOps Is A Journey

- Know your team, know your business and start with what you can do today

- If you don't have a security resource on your dev teams, get one

- Small steps over time will achieve more progress than waiting until all the pieces are in place

This journey never ends, be ready to adjust, culture of change

Thank You

Drew Koenig
securityinfive@binaryblogger.com
https://securityinfive.com
Podcast (available everywhere) – Security In Five
@SecurityInFive