Embracing DevOps as a Security Professional

Astha Singhal
Engineering Manager, Application Security
Netflix

Swiss Cyber Storm 2018

#netflixeverywhere

How do you change your approach in a different engineering culture to achieve the same security goals?

Freedom and Responsibility

Context not Control*

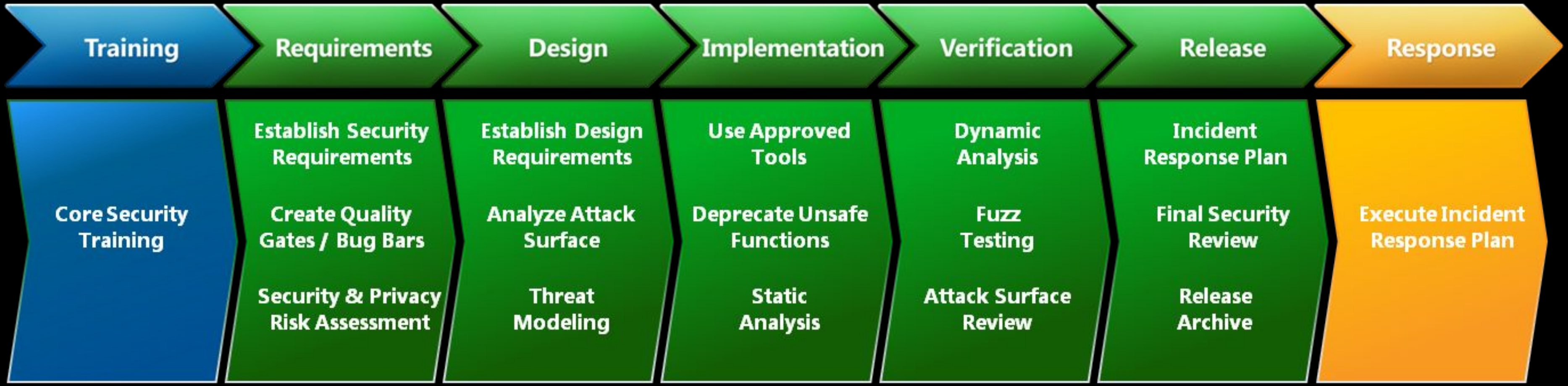
Security @ Netflix

“Guardrails not Gates”

Product Security aka The Defenders

- Finding, Fixing and Preventing Vulnerabilities
- Threat modeling, Code Reviews, Penetration Testing
- Static and Dynamic analysis
- Security Consulting, Developer Training

Security Development Lifecycle



Training
- Core Security Training

Requirements
- Establish Security Requirements
- Create Quality Gates / Bug Bars
- Security & Privacy Risk Assessment

Design
- Establish Design Requirements
- Analyze Attack Surface
- Threat Modeling

Implementation
- Use Approved Tools
- Deprecate Unsafe Functions
- Static Analysis

Verification
- Dynamic Analysis
- Fuzz Testing
- Attack Surface Review

Release
- Incident Response Plan
- Final Security Review
- Release Archive

Response
- Execute Incident Response Plan

No way to know everything that’s being released

Not enough time and resources to review everything

Manual security approvals would slow everything down

Code analysis in a microservice, polyglot environment is really hard

Advantages of the Continuous Delivery model

- Centralized CI/CD to hook in security automation

Advantages of the Continuous Delivery model

- Centralized CI/CD to hook in security automation
- **Cloud Infrastructure primitives to automatically derive asset inventory**

Advantages of the Continuous Delivery model

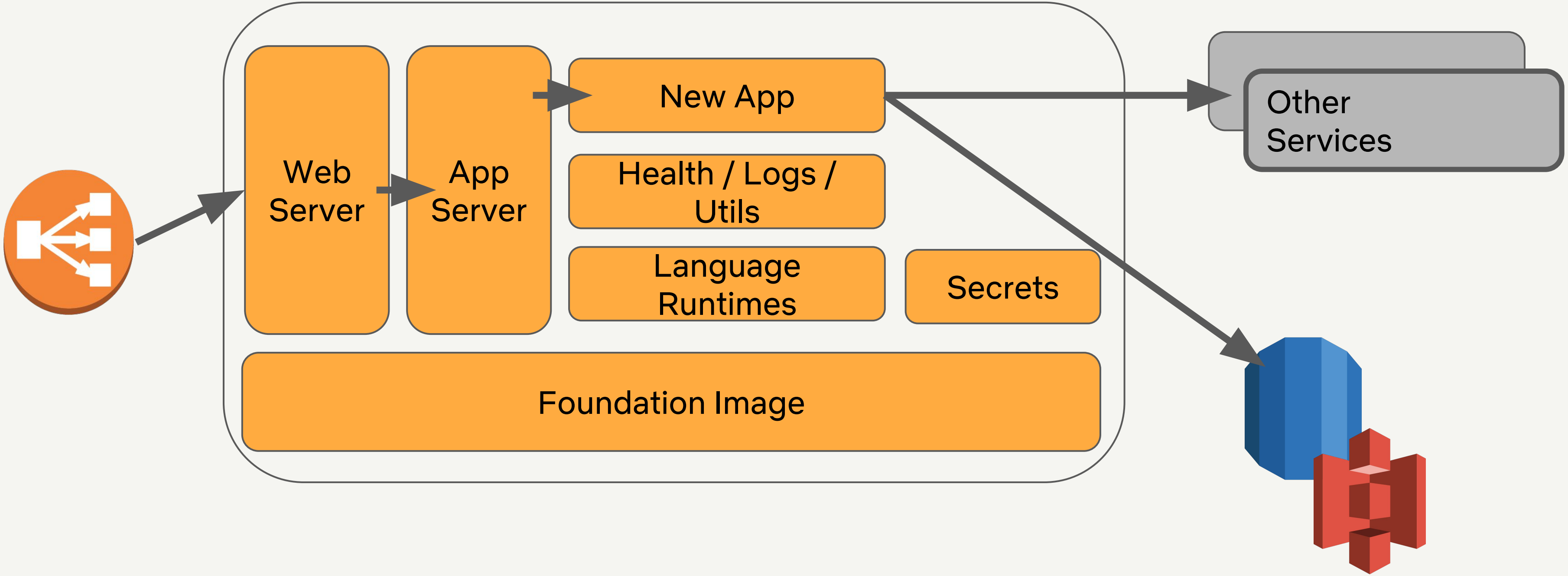
- Centralized CI/CD to hook in security automation
- Cloud Infrastructure primitives to automatically derive asset inventory
- **On-call to handle interrupt driven work**

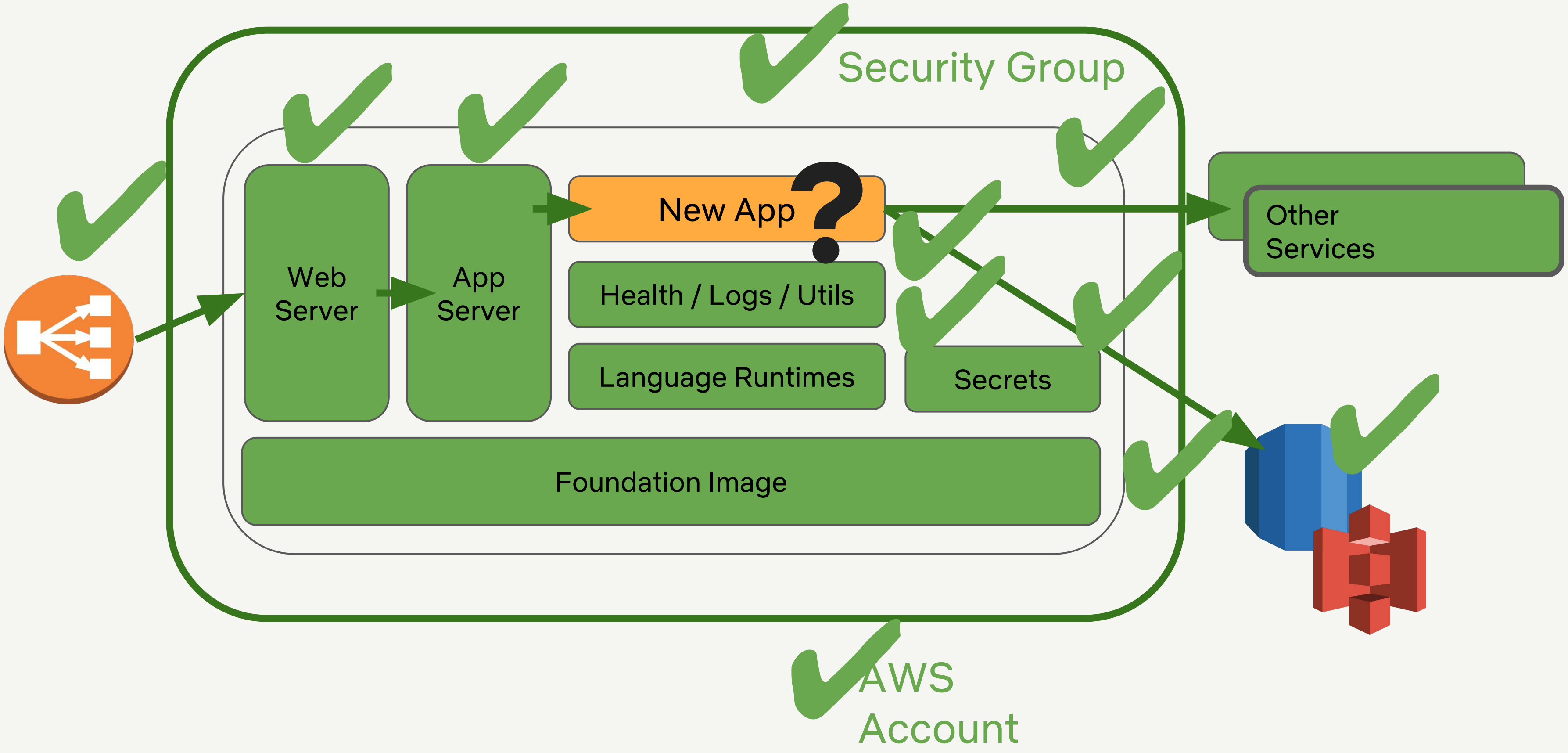
Advantages of the Continuous Delivery model

- Centralized CI/CD to hook in security automation
- Cloud Infrastructure primitives to automatically derive asset inventory
- On-call to handle interrupt driven work
- **Security is not “special”**

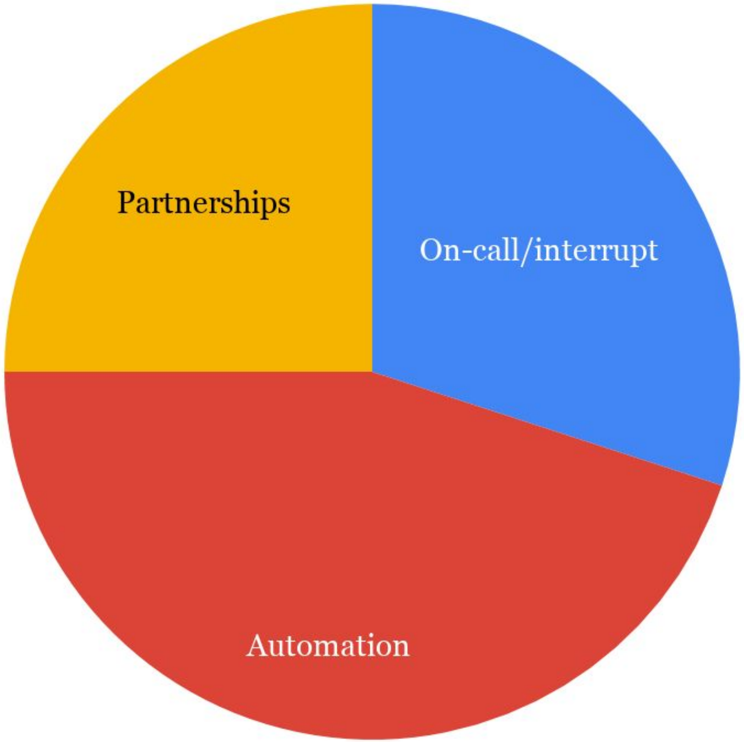
Advantages of the Continuous Delivery model

- Centralized CI/CD to hook in security automation
- Cloud Infrastructure primitives to automatically derive asset inventory
- On-call to handle interrupt driven work
- Security is not “special”
- **“Paved Road” to incorporate security controls**


Web Server
App Server
New App
Health / Logs / Utils
Language Runtimes
Secrets
Foundation Image
Other Services


Security Group
Web Server
App Server
New App ?
Health / Logs / Utils
Language Runtimes
Secrets
Foundation Image
Other Services
AWS Account

Appsec Team Composition



What needs to change

- Enable your developers via security self-service
- Integrate with the developer workflows
- Build secure by default platforms
- Scale product security resources via automation
- Better automated visibility & action for developers

What needs to change

- Enable your developers via security self-service
- Integrate with the developer workflows
- Build secure by default platforms
- Scale product security resources via automation
- Better automated visibility & action for developers

What stays the same

- **Building relationships with your customers across the org is still important**
- **Security work continues to be driven by Enterprise Risk**
- **Strategic partnerships with high risk areas**
- **Developer training where relevant**
- **Pentesting and bug finding**

Thank you