Smarter Code Shifting Everywhere

In an era of Application Security Testing where ‘everything as code’ dominates, AppSec is no longer just about shifting left but ‘shifting everywhere’

Jon Taylor
Worldwide Vice President - Fortify

Fortify by opentext

OpenText ©2023 All rights reserved

Agenda

Why Application Security?

- Opportunities & Challenges
- Emerging Use Cases

AppSec Programs

- Objectives
- Maturity Journey
- Persona Challenges

FoD Govtech Demo

Q&A

OpenText ©2023 All rights reserved

Why Application Security?

OpenText ©2023 All rights reserved

Just imagine how great it will be in the future…

…when we get that Secure Code stuff right!

AEROFLOT
SKY PRIORITY

opentext™ | Cybersecurity

Fortify by opentext™

We are getting there….

SPEED TO MARKET
REVENUE GROWTH
RISK STRATEGY
DEFCON 18

Forbidden items -
not allowed on the aircraft:
ACID
POISON
Acids
Poisons
Flammable liquids
Explosives
Compressed gas
Bleach
over 100ml
Water, drinks,
make-up &
toiletries
Hand baggage:
Check your bag
size with your
airline
Accept and continue >

The AppSec Problem (Opportunity!)

OpenText ©2023 All rights reserved

opentext™ | Cybersecurity

2001
SOX

2008
MAJOR CYBER ATTACKS

2020
COVID DRIVING DX

COMPLY

ERA OF COMPLIANCE
2001 - 2008

DE-RISK

ERA OF THREAT MANAGEMENT
2008 - 2014

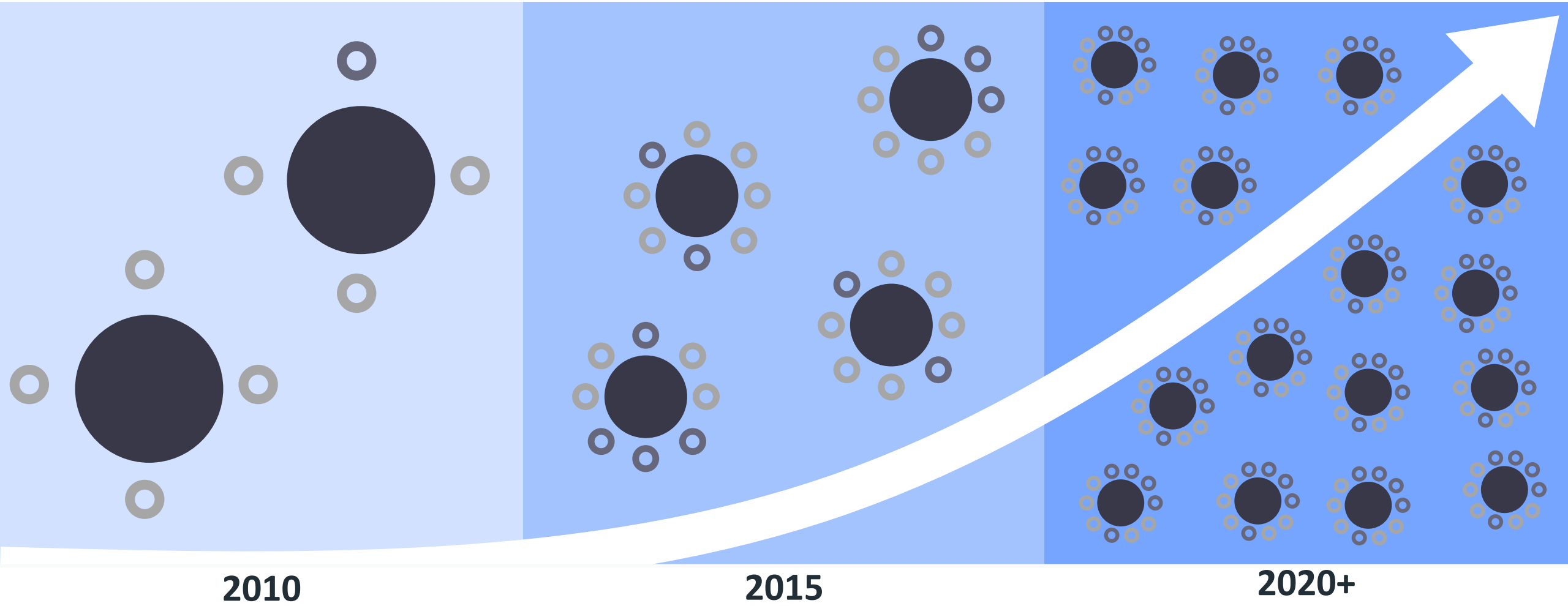
ENABLE

ERA OF DX TRANSFORM
2014 - 2020

RESILIENT

ERA OF GROWTH
2021+

Business needs faster innovation…
… but faster innovation increases risk



opentext™ | Cybersecurity

OpenText ©2023 All rights reserved

Fortify by opentext™

2022 AppSec Trend Report

The application security industry continues to evolve at pace as organizations recognize that software security risks need to balance with business imperatives that accelerate digital innovation.

OpenText ©2023 All rights reserved

Top Application Security Trends

Fortify by opentext™

Securing the Software Supply Chain

98% of all code bases relied on open source components

API Security Needs Growing Ever Larger

By the end of 2023 over 50% of all B2B transactions will be performed via real-time APIs (Gartner)

AppSec is evolving from Shift-Left to Shift Everywhere

Only 20% of organizations have automated most (>75%) of their security testing and fewer than half (44%) have included security testing into their dev workflows

Next-Generation DAST

AppSec Orchestration & Correlation

When increasing the speed and frequency of scans and prioritizing SCA tickets, we found enterprises that tightly integrate security testing within their CI/CD pipelines fix over 90% of new issues

Machine Learning and AI are Key to the Next Evolution of Automation

Cloud-Native AppSec

More than half of organizations use three or more cloud platforms

OpenText ©2023 All rights reserved

Equifax

Leading global data, analytics, and technology company protects client data with Fortify

Challenges

- Drive AppSec modernization to deliver actionable, data-driven results
- Evolve AppSec from being a centralized to a decentralized function where developers are responsible for ensuring their own code is secure

Solution

Fortify on Demand

- Static
- Dynamic
- Opensource

Results

✓ Adopted a shift-left culture and secure DevOps practices utilizing FoD when transforming development to the cloud

Learn how Equifax adopted a shift-left culture and secure DevOps practices utilizing Fortify on Demand when transforming development to the cloud

OpenText ©2023 All rights reserved

Let’s think about AppSec Initiatives & Programs

OpenText ©2023 All rights reserved

The mitigation of application security risks is not a one time exercise

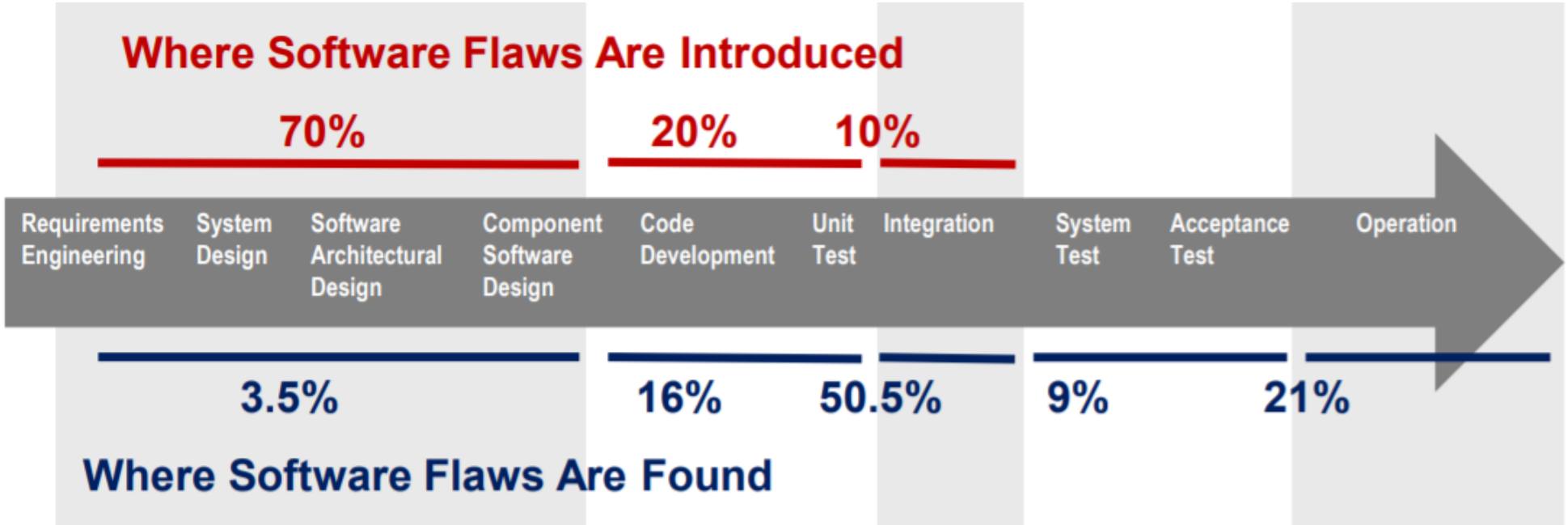
Rather it is an ongoing activity that requires paying close attention to emerging threats and planning ahead for the deployment of new security measures to mitigate these new threats.

This includes the planning for the adoption of new application security activities, processes, controls and training

Source: "Application Security Guide for CISOs," OWASP

OpenText ©2023 All rights reserved

It’s extremely difficult to develop vulnerability-free software



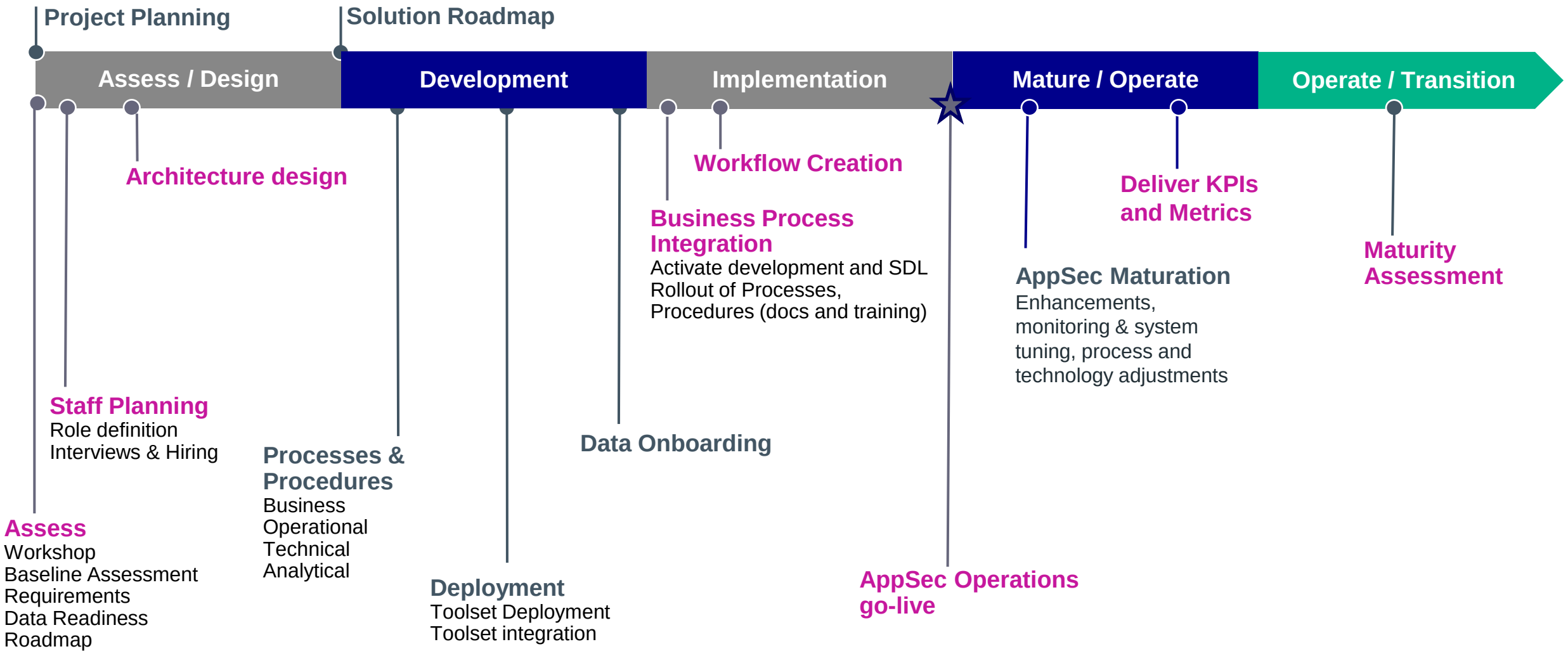
- Good levels of defects in software would be 600 - 1,000 defects per MLOC
- Exceptional levels would be below 600 defects per MLOC
- Thus, software can’t always function perfectly as intended
- 5% of defects should be categorized as security vulnerabilities

This would be 30 security vulns per MLOC even in exceptional code!

OpenText ©2023 All rights reserved

Establishing AppSec Programs can be hard!

Building an AppSec Program – Major Milestones



OpenText ©2023 All rights reserved

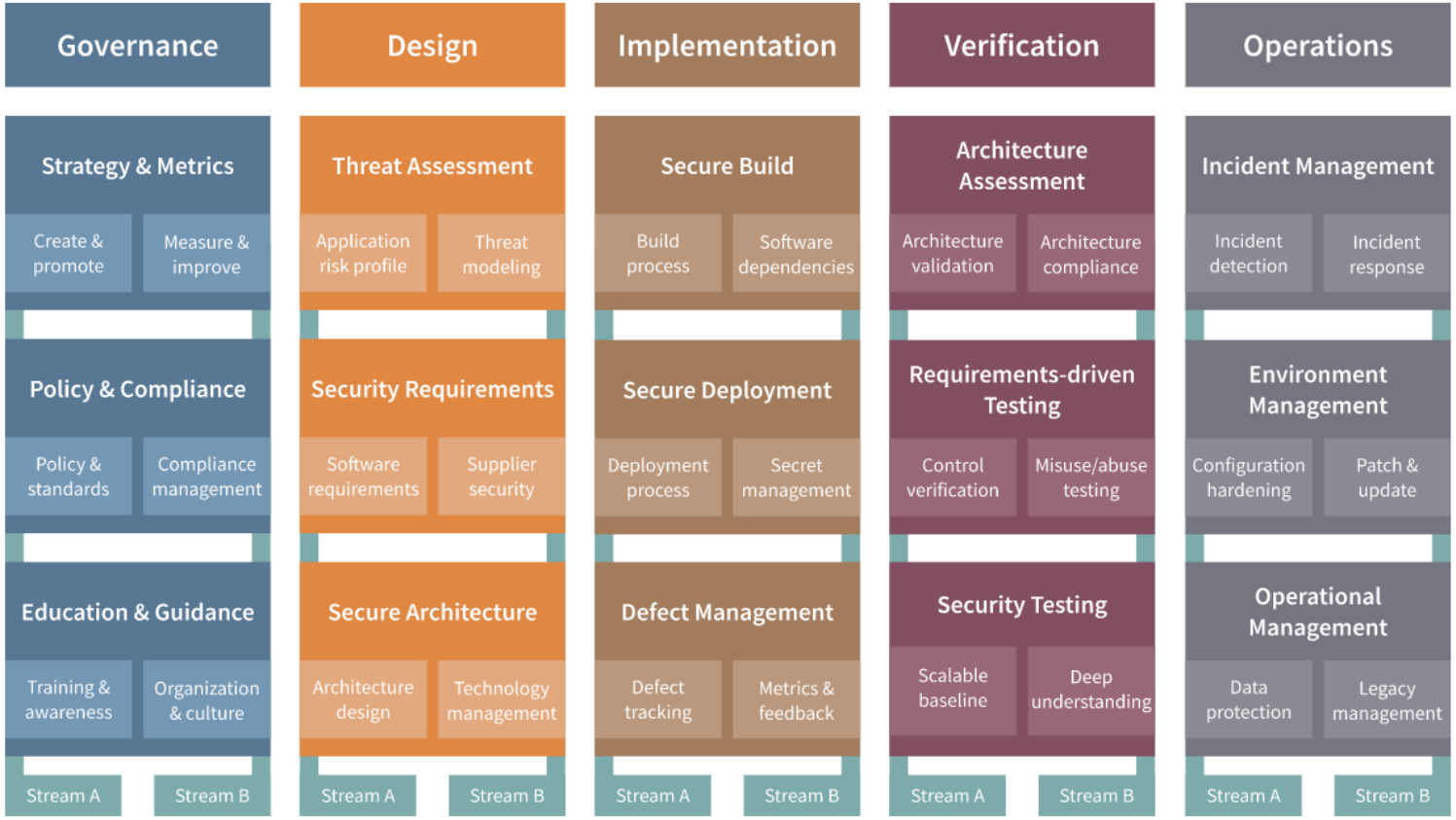
Measure to demonstrate success

- % of security defects identified by sprint/phase
- % of security defects whose risk has been accepted vs. % fixed
- % of security defects per project over time (ex. quarter to quarter)
- Vulnerability density (security defects/LOC)
- Average time required to fix/close security defects during design, coding and testing
- Average time to fix security defects by defect type
- Average time to fix security defects by app size / code complexity

OpenText ©2023 All rights reserved

OWASP Software Assurance Maturity Model (SAMM)

An open framework created by industry leaders (including Fortify's SRG!) to help customers measure where they are and where they'd like to be and what maturity looks like for each area



OpenText ©2023 All rights reserved

Successful AppSec programs needs to…

- Establish AppSec standards that can guide developers and set agreed-to expectations on how to remediate the findings from security tests
- Seamlessly integrate testing into development processes and tool chains
- Only be recognised as effective at reducing risk if flaws are actually fixed once they're identified!

OpenText ©2023 All rights reserved

Effective AppSec Programs Rely on Partnerships

…also think about how this works with outsourced development

OpenText ©2023 All rights reserved

CISO Challenge:

Regulatory Compliance, Governance & Risk

Visibility into Application Security Risks
Through Comprehensive Testing

MAS Monetary Authority of Singapore

GDPR

loss of shareholder (stakeholder) value & confidence

OpenText ©2023 All rights reserved

Developer Director Challenge:

Integrating security testing into
development toolchains with low friction

Intelligent automation using Cloud DevSecOps

Automate and manage
Secure Build and release checkpoints from SCM to CI

Orchestrate secure deployments across all application environments

Automated security certification without any manual intervention

Leverage out of the box extensive library of plugins that integrate across the build and deployment pipeline

OpenText ©2023 All rights reserved

Using a combination of Application Security Testing methods is essential to assess Application Risk

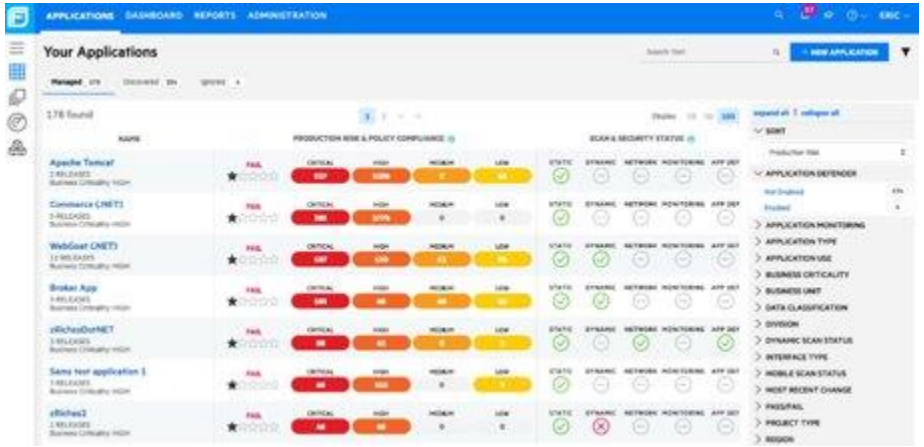
OpenText ©2023 All rights reserved

FoD – Static Assessment (SAST)

Find critical security weaknesses during development

Why Fortify on Demand SAST?

- ✓ 27 coding languages
- ✓ 810+unique vulnerability categories
- ✓ 85% automated audit scans in <1 hour
- ✓ No file or code size restrictions
- ✓ Comprehensive IDE plugins
- ✓ Integration with build / CI tools



Static Assessments include:

- Fortify Static Code Analyzer evaluation of source, binary or bytecode
- Automated audit of results by Fortify Scan Analytics*
- Real-time identification with Security Assistant**

Static+ Assessments include:

- Security expert review of prioritized results for all scans

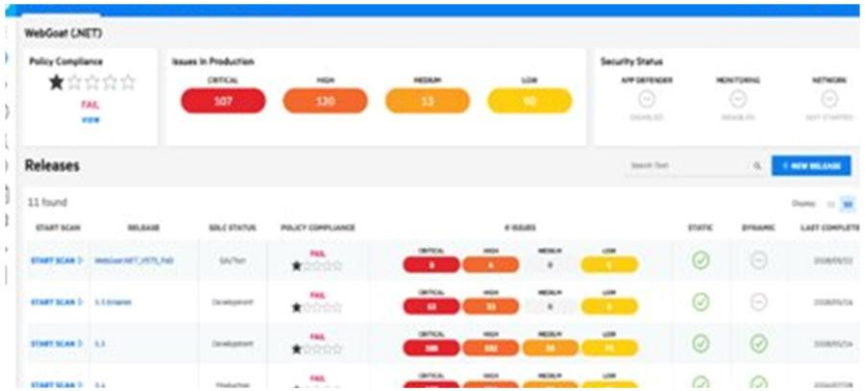
Resource: FoD SAST Brochure

OpenText ©2023 All rights reserved

FoD – Dynamic Assessments (DAST)

Why Fortify on Demand DAST?

- ✓ 250+ unique vulnerability categories
- ✓ Test in QA, staging & production
- ✓ Assess single page applications (SPAs)
- ✓ Built-in support for scan blackout periods
- ✓ Virtual patches for all top WAFs
- ✓ External or internal network applications
- ✓ Includes IAST for accuracy & coverage



Dynamic Assessments include:

- WebInspect analysis of website
- Generated authentication macro
- Security expert review of prioritized results

Dynamic + Assessments include:

- Manual testing of website

  or

- Manual testing of web services**

Resource: FoD DAST Brochure

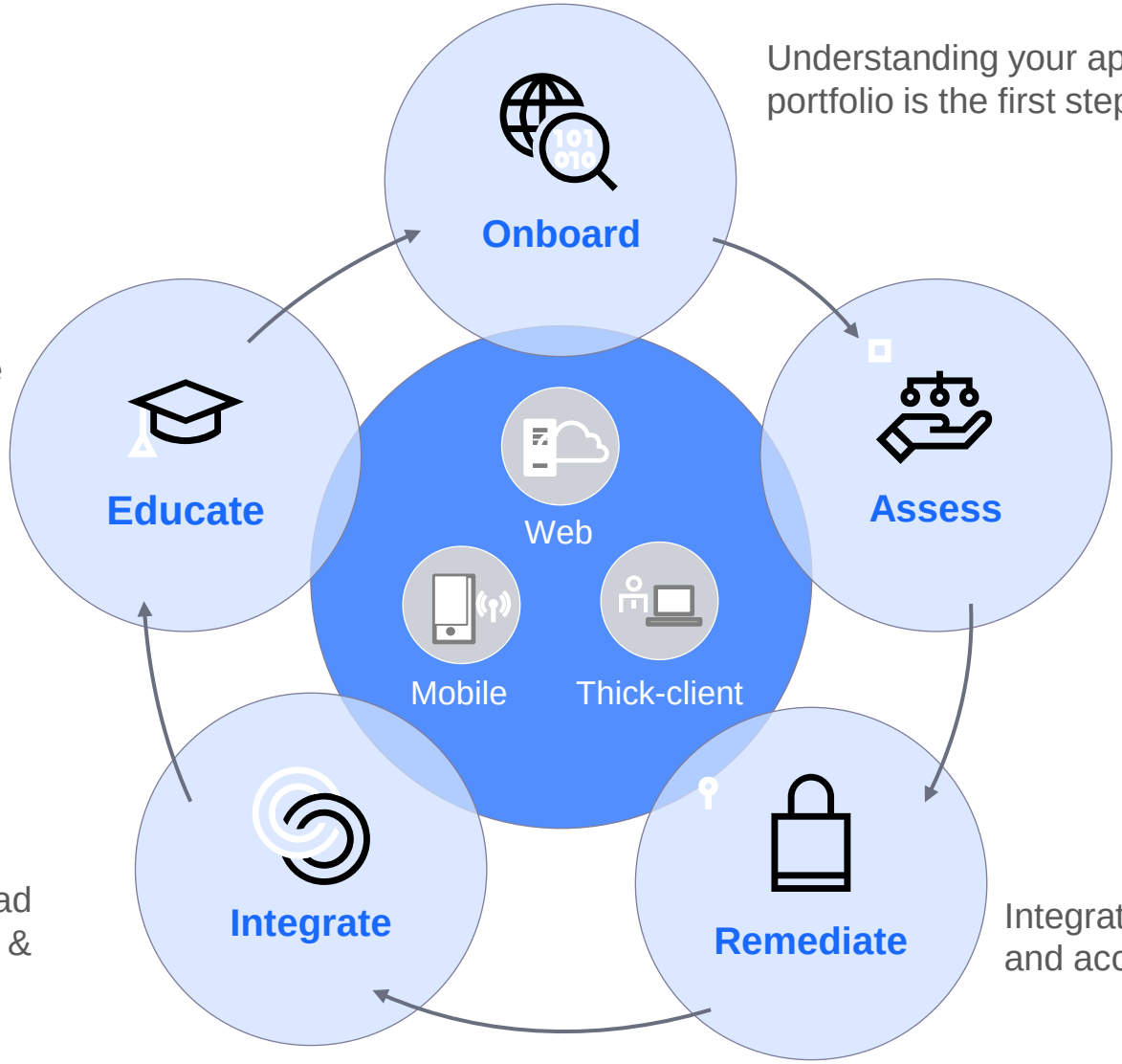
OpenText ©2023 All rights reserved

Fortify on Demand Accelerates AppSec Programs

Fortify on Demand Process

Understanding your application portfolio is the first step to securing it

Leading-edge developer training for secure coding best practices and prevent vulnerabilities before check-in



Industry's most comprehensive static, software composition analysis dynamic/interactive appsec testing delivered at the speed of development

Securing DevOps through broad Fortify Ecosystem integrations & automation tools

Integrated workflows to fix vulnerabilities faster and accelerate & mature AppSec programs

OpenText ©2023 All rights reserved

Demos

GitLab integration with FoD – Jie Han, GovTech
FoD Walkthrough – Jeremy Chua, OpenText

Summary

Discovery Questions for Key Stakeholders

CISO

- How do you manage overall app security risk?
- From the oversight perspective, who conducts applications security testing?
- Do your staff have the skills to implement the AppSec program you need?
- What percent of the app inventory are covered with your AppSec program?
- Are you concerned about missing risks in apps?
- How are you demonstrating compliance to auditors?

Application Security Director

- How confident are you that your AppSec team can adapt and scale to keep up with rapid application development?
- Who is responsible for AppSec Testing?
- Do you want to offload resource requirements for security testing?
- What is your standard for testing applications produced by 3rd parties, including open source?
- Are you scanning APIs for security weaknesses?
- How much time is spent triaging scan results?
- Who ensures that identified security defects are remediated?

Development Director

- What languages are used in the applications you are building?
- Which development methodologies are you using? DevOps? Is security testing integrated in?
- What are your expectations for application security testing tool integration into your DevOps tool chains?
- Are you developers aware of secure coding best practices?
- How much time is spent remediating security vulnerabilities? Do they need assistance with remediation?
- What steps are you taking to secure open-source software components used in your applications?

FedRAMP Case Study

Leveraging FoD for Compliance in US Government

FedRAMP™

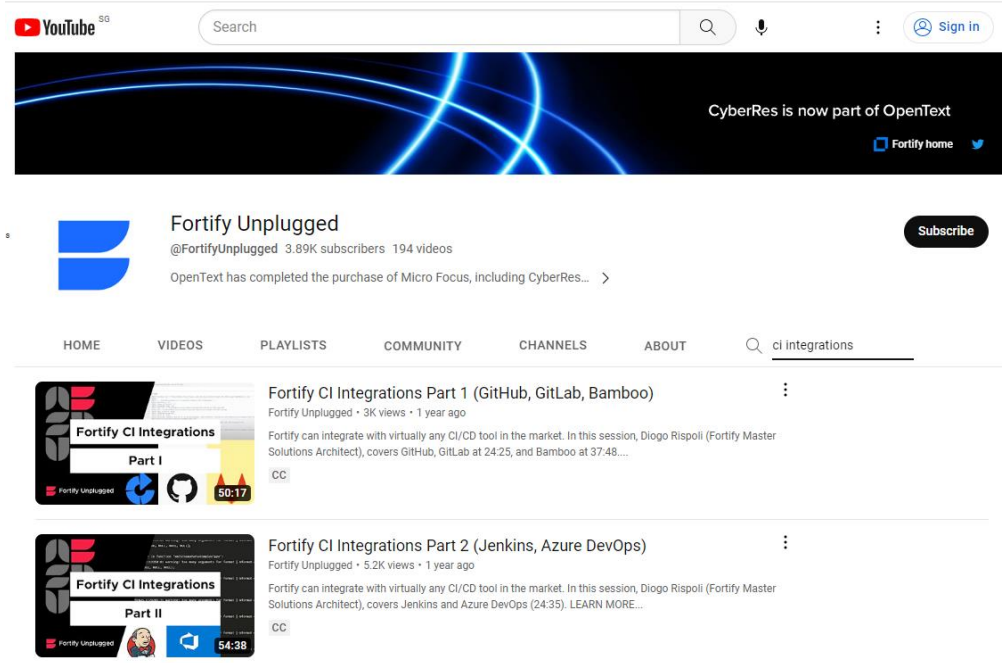
Learn how the US Federal Government uses Fortify on Demand to deliver assurance to apps developed for an by Federal Agencies

OpenText ©2023 All rights reserved

Resources for further reading

Insights to latest **State of Code Security Report**
[Watch on demand]

Subscribe to Fortify Unplugged for demo videos
http://www.youtube.com/c/FortifyUnplugged



Jeremy Chua
jeremy.chua@microfocus.com

Clarence Ho
clarence.ho@microfocus.com

Jon Taylor
jont@microfocus.com

Chin Yan
chinhwang.yan@microfocus.com

OpenText ©2023 All rights reserved

Great Code Demands Great Security

Fortify
by opentext™