Effective Application Security Testing at High Velocity: Keeping up with Agile / DevOps

February 28, 2017

Today's Speaker:

Cindy Blake CISSP
Product Marketing Manager
Hewlett Packard Enterprise

Hewlett Packard Enterprise

The webinar will begin shortly.

vivit

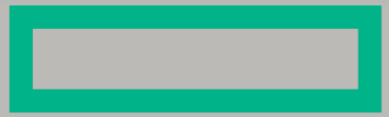
vivit

Discover the independent HPE software user community where you can share, collaborate, exchange, and grow

Effective Application Security Testing at High Velocity: Keeping up with Agile / DevOps

February 28, 2017

Brought to you by



Hewlett Packard
Enterprise

YOUR INDEPENDENT HPE SOFTWARE USER COMMUNITY

vivit

Hosted By

Richard Howe
Account Manger
Results Positive

Today's Speaker

Cindy Blake CISSP
Product Marketing Manager
Hewlett Packard Enterprise

Webinar Housekeeping

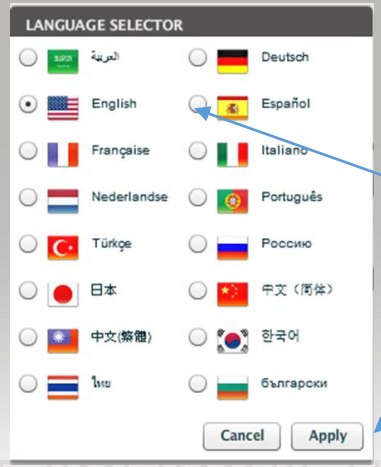
- This “LIVE” session is being recorded
- Recordings are available to all Vivit members
- To enlarge the presentation screen, click on the rectangle in the upper right hand corner of the Presentation pane

vivit

Webinar Control Panel

- Session Q&A:

  Please type questions in the Q&A pane
  and click on "Ask"
- Choose the language in which you would like to ask your questions



Feb 28 2017

Hewlett Packard Enterprise

Effective Application Security Testing at High Velocity:

Keeping up with DevOps

Cindy Blake – Fortify Product Marketing Manager
Cindy.blake@hpe.com
Linkedin.com/in/cblake2000

Agenda

Effective Application Security at High Velocity (DevOps)

- What problem are we solving? Level set on the challenge

- How to integrate application security throughout your software development lifecycle
  - Development: How to eliminate security flaws right at the source
  - Test: Application Security Testing Automation and the DevOps tool chain of automation
  - Production: How to gain visibility into production application behavior and exploits and protect security flaws to buy time for true remediation

- How to make static and dynamic analysis more efficient and effective

Polling Questions

1. What percentage of your application portfolio is developed in-house? (can include open source, but not purchased software pkg)

2. What percentage of your in-house portfolio uses a DevOps methodology?

3. Have you integrated application security testing into your overall test automation?

What Problem Are We Solving?

The DevOps Challenge

DevOps

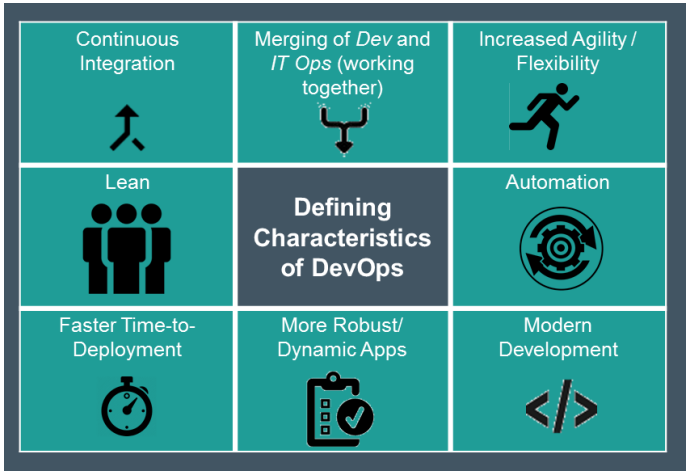
DevOps- A practice that emphasizes the collaboration and communication between software developers and IT professionals, with the goal of automating the process of software delivery and infrastructure changes.

Principles

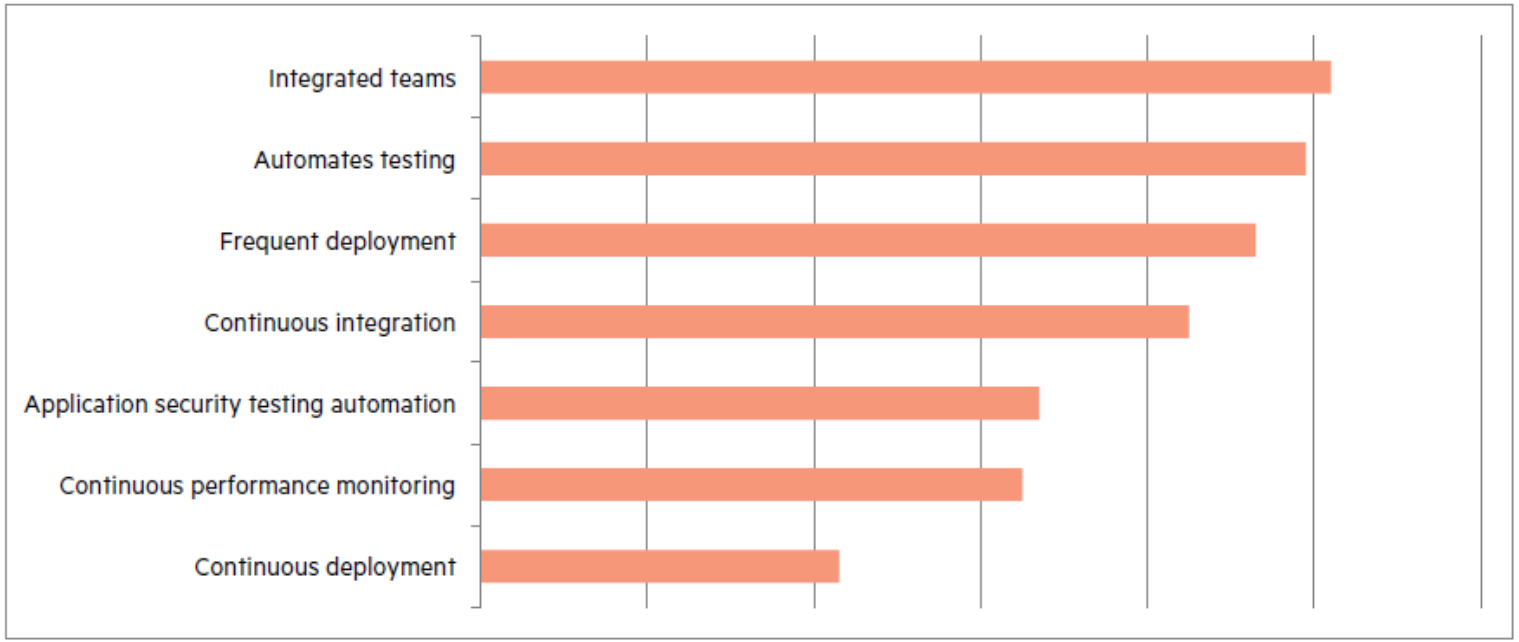
- Develop and test in an environment similar to production
- Deploy builds frequently
- Automate the process of delivering software
- Validate quality continuously

Benefits

- Faster time to value
- Faster time to market with higher quality
- Stay ahead in a competitive environment



DevOps Characteristics

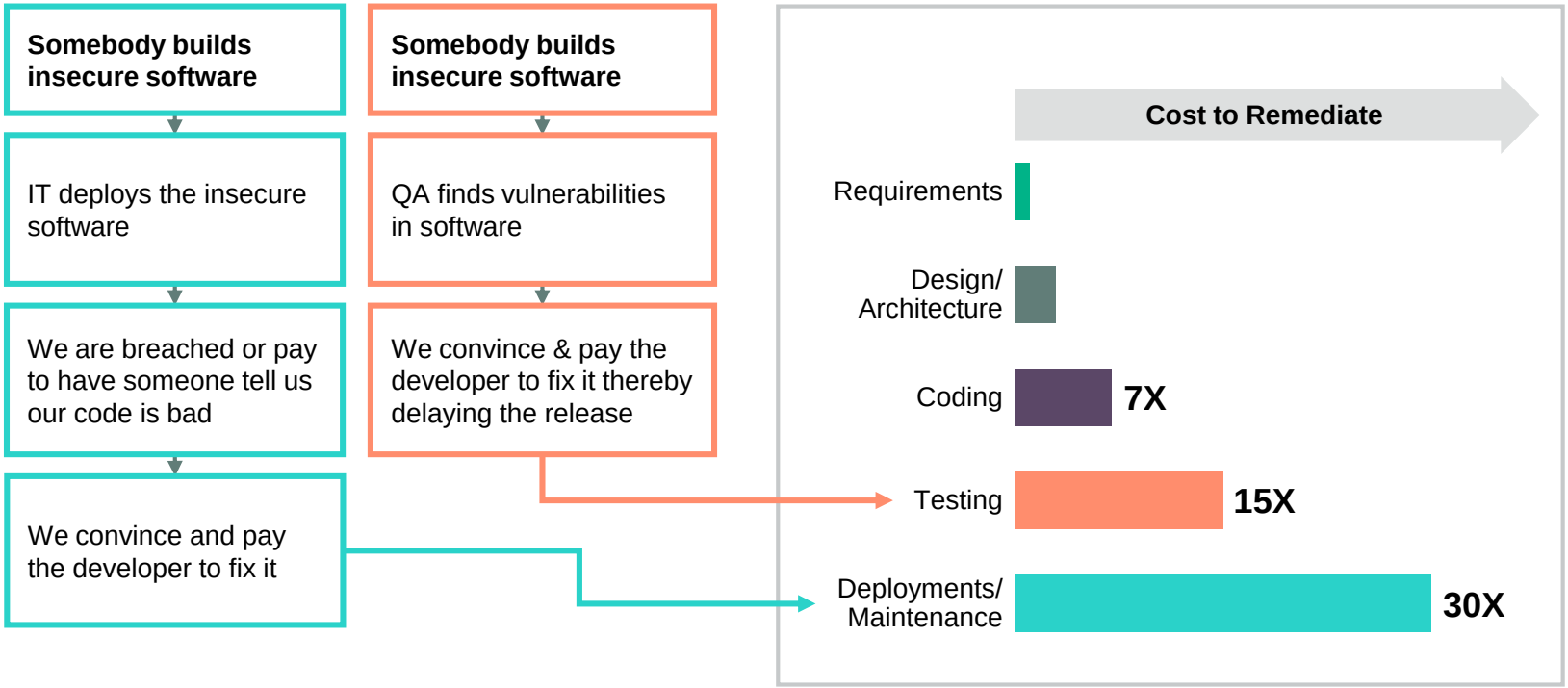


Source: Application Security and DevOps: What is the true state of security in DevOps? Sept 2016

Traditional vs. Modern (DevOps) Delivery Processes

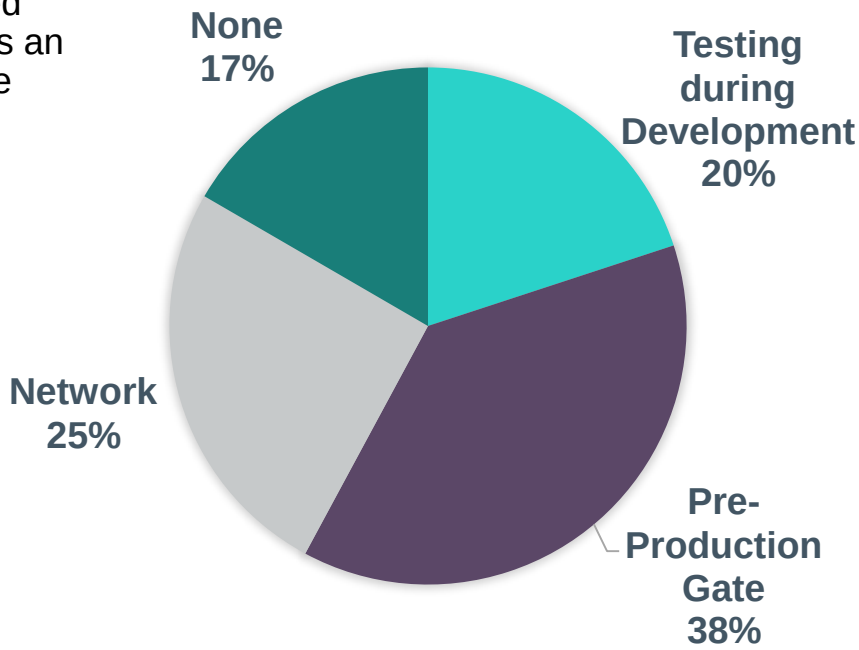
	Traditional	Modern (DevOps)
Release Frequency	• 1-2 versions a year • Service pack every 3 months • Customer upgrades that include downtime and planning	• Version every 3 months • Weekly updates • Quick process with no downtime
Continuous Integration	• Teams working independently; Integration performed every 2 weeks	• Continuous Integration running every 30 minutes
Sanity Automation	• Limited coverage of automated tests • Manual effort required from Dev to deliver build to QA	• Fully automated Acceptance Test • 72% coverage of test automation
Technology Adoption	• Significant overhead from technology changes	• Rapid technology changes and adoption
Operation & Support	• Production environment owned by customer. • Support via Support org.	• Full responsibility for production environment.

A reactive approach to AppSec is inefficient and expensive



Promise vs Reality of Security in DevOps

99% of those surveyed agreed that DevOps is an opportunity to improve application security



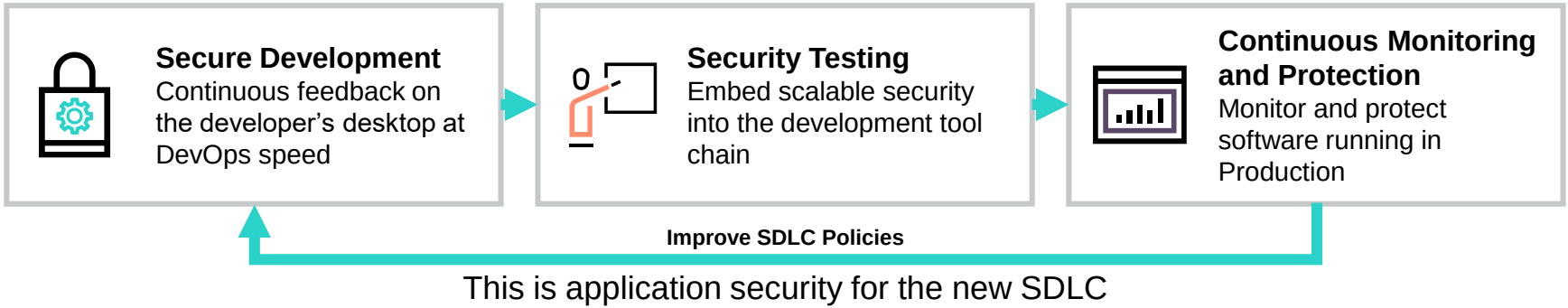
But only 20% perform application security testing during development. Most wait until late in the SDLC – or not at all!

Source: Application Security and DevOps: What is the true state of security in DevOps? Sept 2016

Hewlett Packard Enterprise

How to integrate app sec into your SDLC

The right approach for the new SDLC – Build it in



This is application security for the new SDLC

1. Shift left to eliminate vulnerabilities early
2. Build app sec into automated testing
3. Monitor and protect production apps

The right approach for the new SDLC – Build it in
Eliminate security flaws right at the source

This is application security for the new SDLC

Building in security as you code

Fortify security assistant

Identify weaknesses as developers write code in real-time

Spell check security scanning

Identify issues earlier in the SDLC

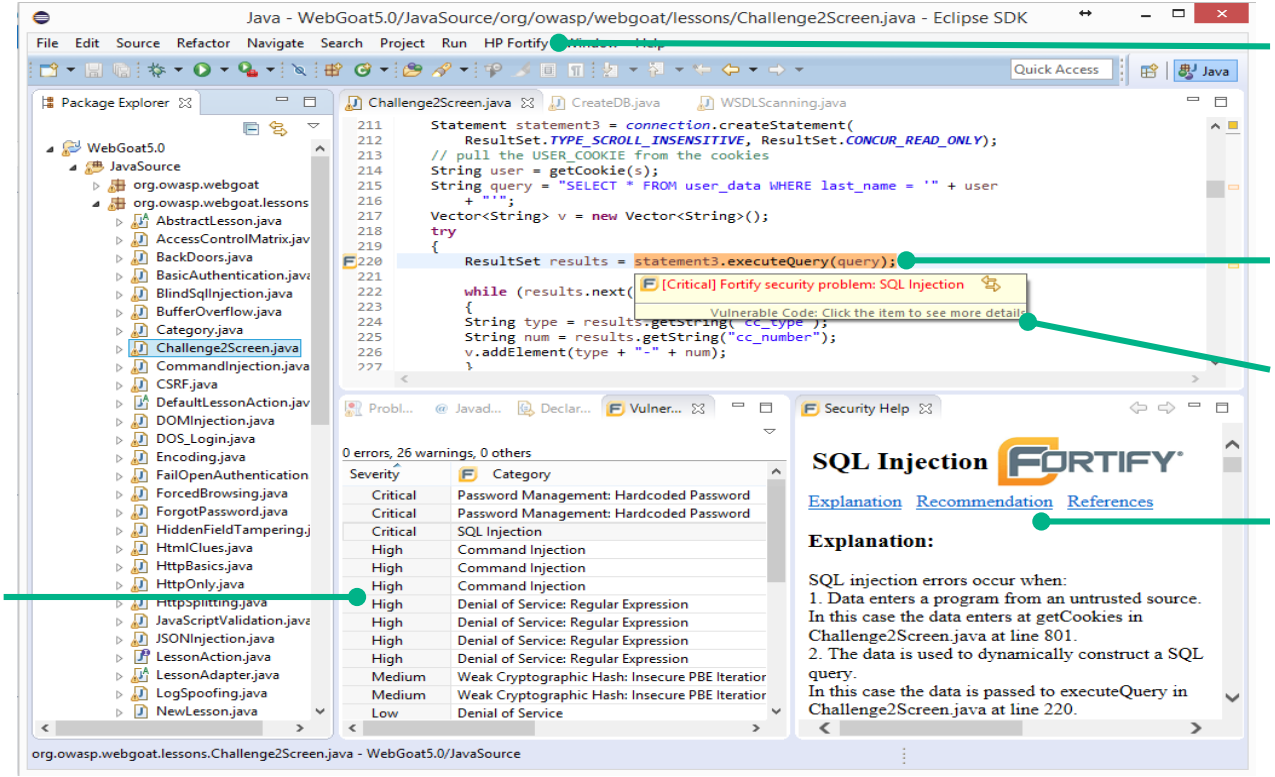
Educate developer about security

Accelerate appsec program (increase productivity & efficiency)

Hewlett Packard Enterprise

Fortify security assistant feature

Real-time lightweight analysis of the source code



Fortify menu for additional options

Vulnerable line of code is highlighted as developer code & provides tips for additional information

Level of criticality

Type of vulnerability, explanation and detailed remediation guidance

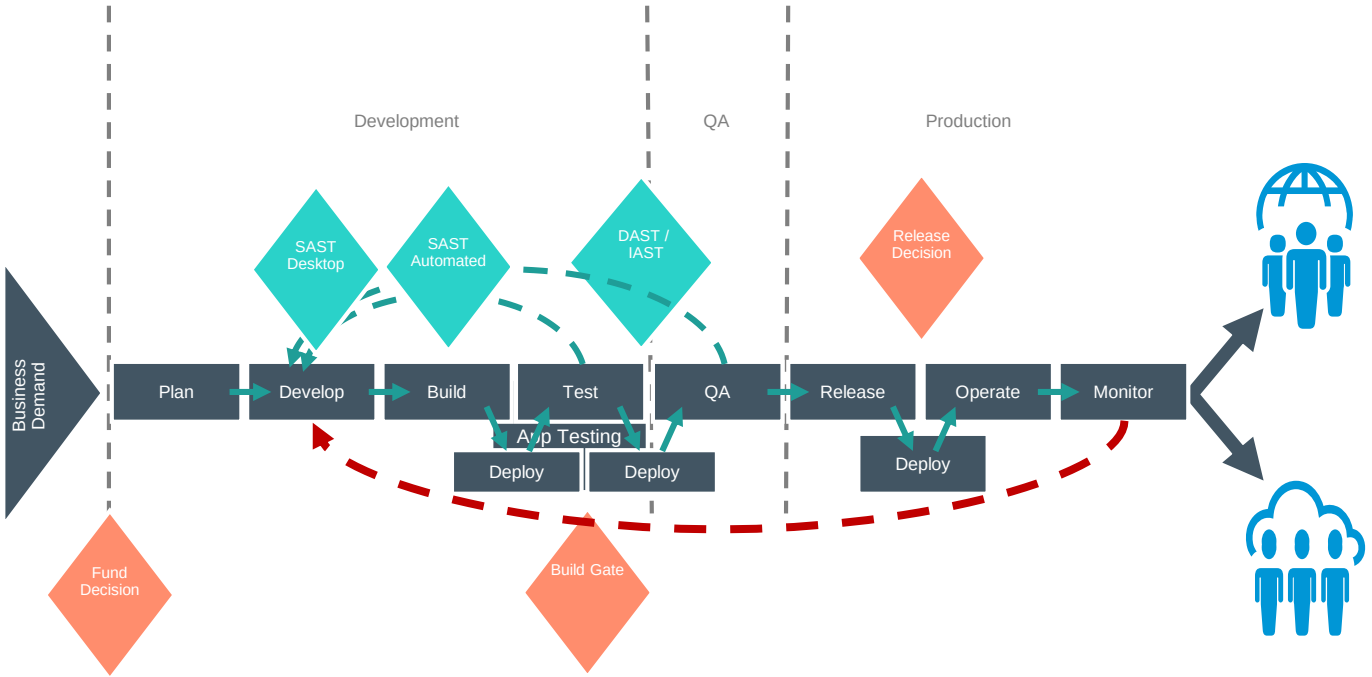
All issues detected in the project

Hewlett Packard Enterprise

The right approach for the new SDLC – Build it
App Sec Testing Automation and the DevOps tool chain of automation

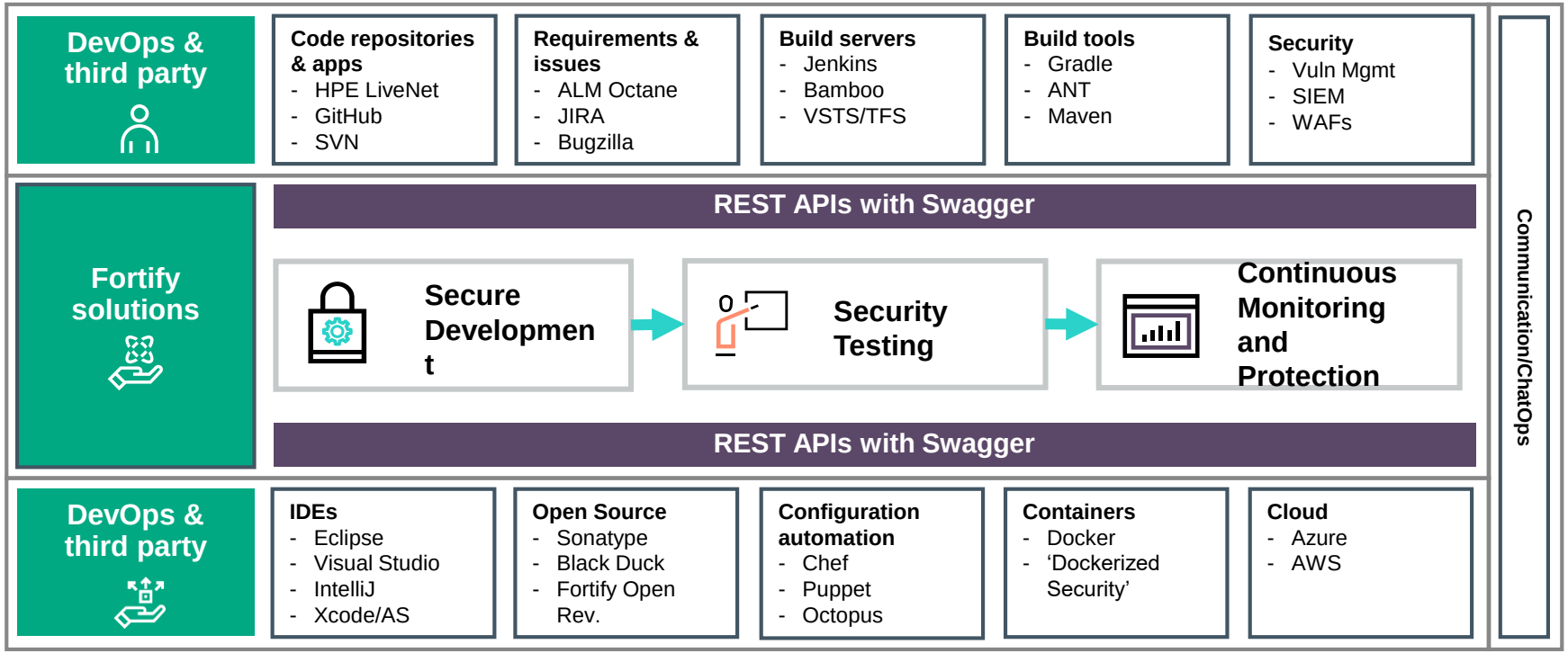
This is application security for the new SDLC

App Journey – How to build it in



Automation – DevOp Tool Chain

HPE Security Fortify Ecosystem



The right approach for the new SDLC – Build it in
Visibility into production application exploits and protect security flaws

This is application security for the new SDLC

Compensating Controls

Application Defender

Identify vulnerabilities in test

Deploy (with security flaws) and remediate in future sprint

Use Application Defender to monitor and protect application vulnerabilities

Send events and application logs to SOC for greater visibility

Fortify Application Defender

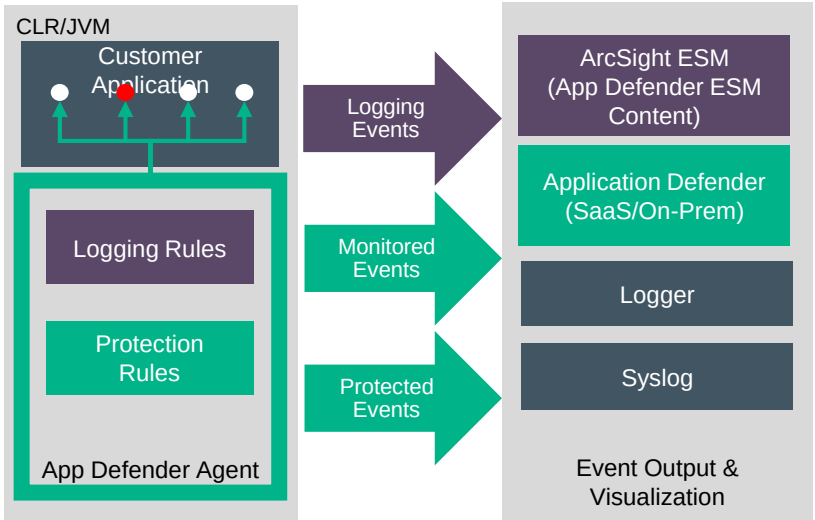
Monitor and protect software vulnerabilities

Application Logging

- Consistent out-of-the-box logging for any application
- 60 Logging categories
  - e.g. File Read/Write; HTTP Session Start/Stop; Login Succeed/Fail
- Send CEF events to ESM or Syslog

Application Protection

- Vulnerability exploit attempts and other security violations
- 29 Vulnerability categories
  - e.g. SQLi; XSS; Privacy Violation
- Monitor & Protect actions



Hewlett Packard Enterprise

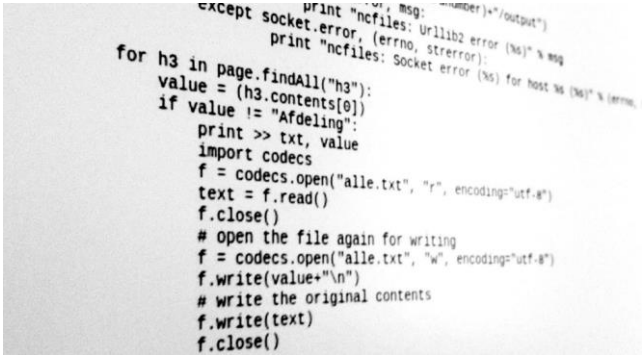
Let’s Talk AppSec

Process, Challenges, Auditing, Remediation

How development organizations have made static and dynamic analysis more efficient and effective

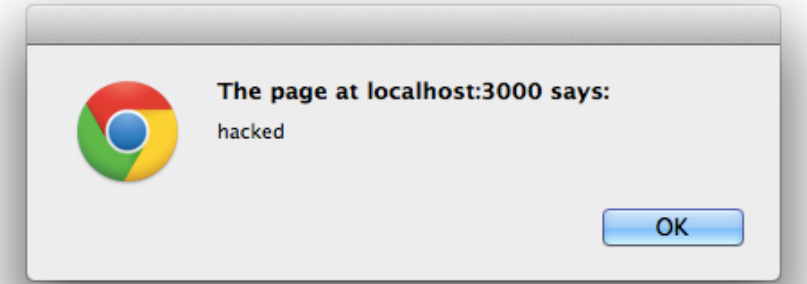
Application Security Testing

Static Analysis



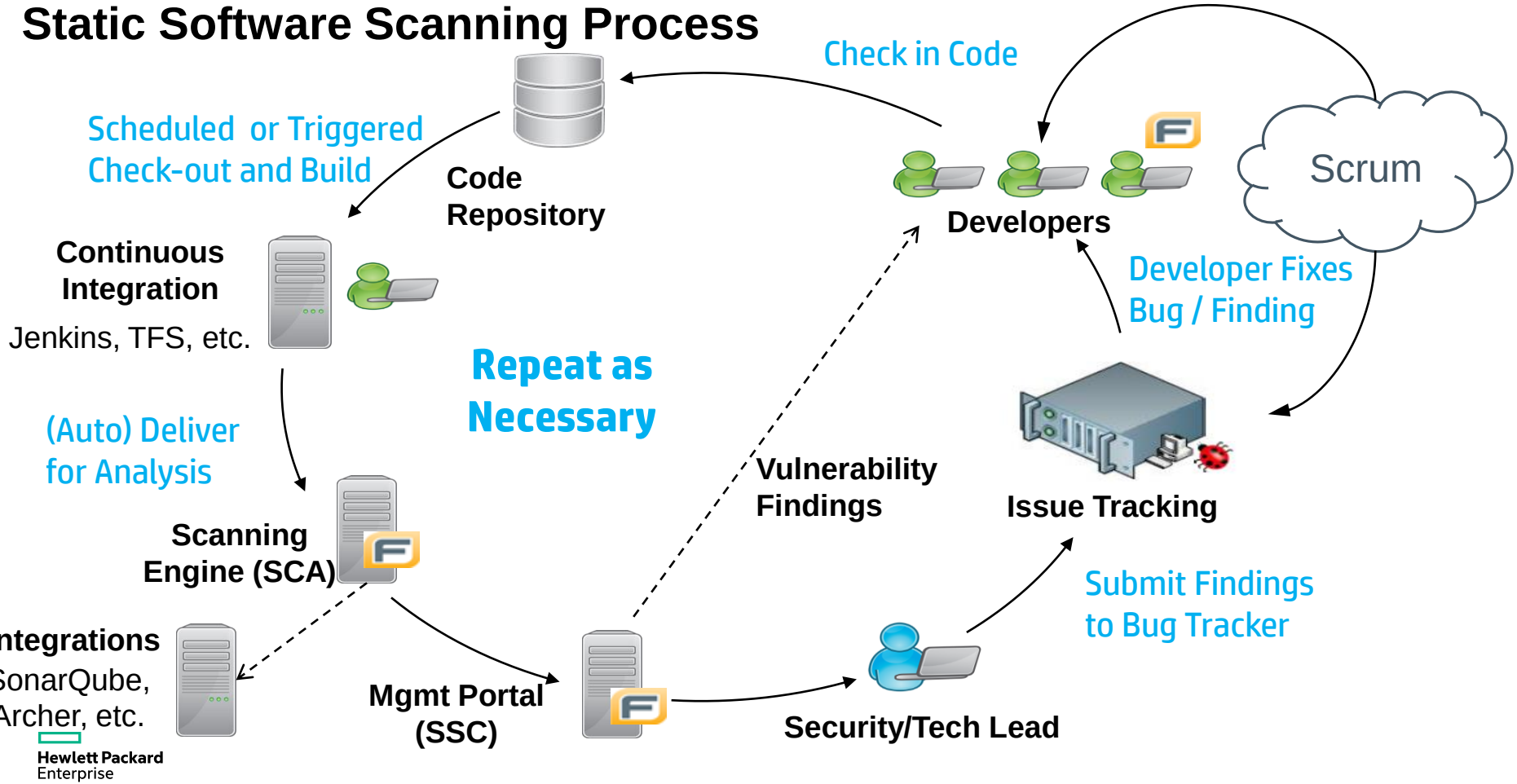
Analyzes source, bytecode or binary code

Dynamic Analysis



Analyzes a running application

Static Software Scanning Process



Hewlett Packard
Enterprise

Static Analysis - AppSec Testing Challenges

Scale

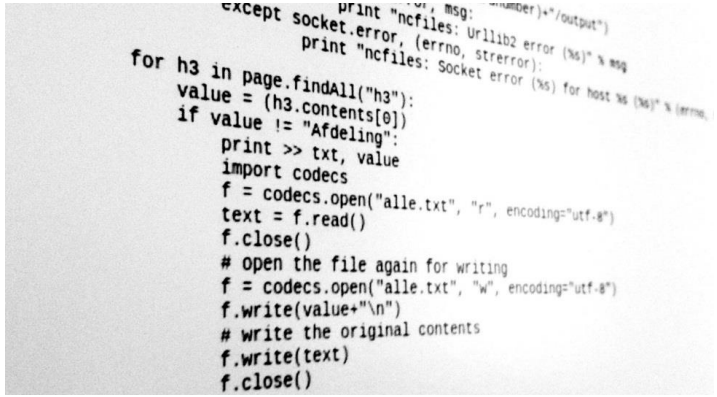
- Volume of static findings requiring human auditing to validate
- Remediate validated findings
- Lengthy / Memory intensive scans
- Communicate findings to developers and metrics/KPIs to mgmt

Application complexity

- Complex build processes, frequency of builds, difficult security integrations
- Modular builds / micro services present dataflow challenges

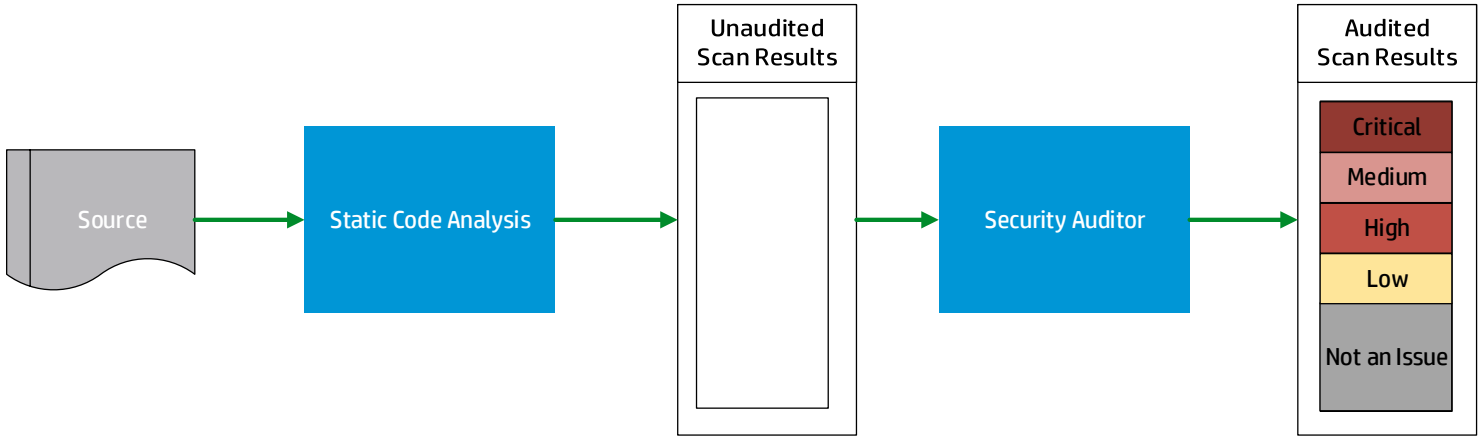
Judgement/expertise

- Risk tolerance to validated findings
- Managed service findings require prioritization



Static analysis workflow

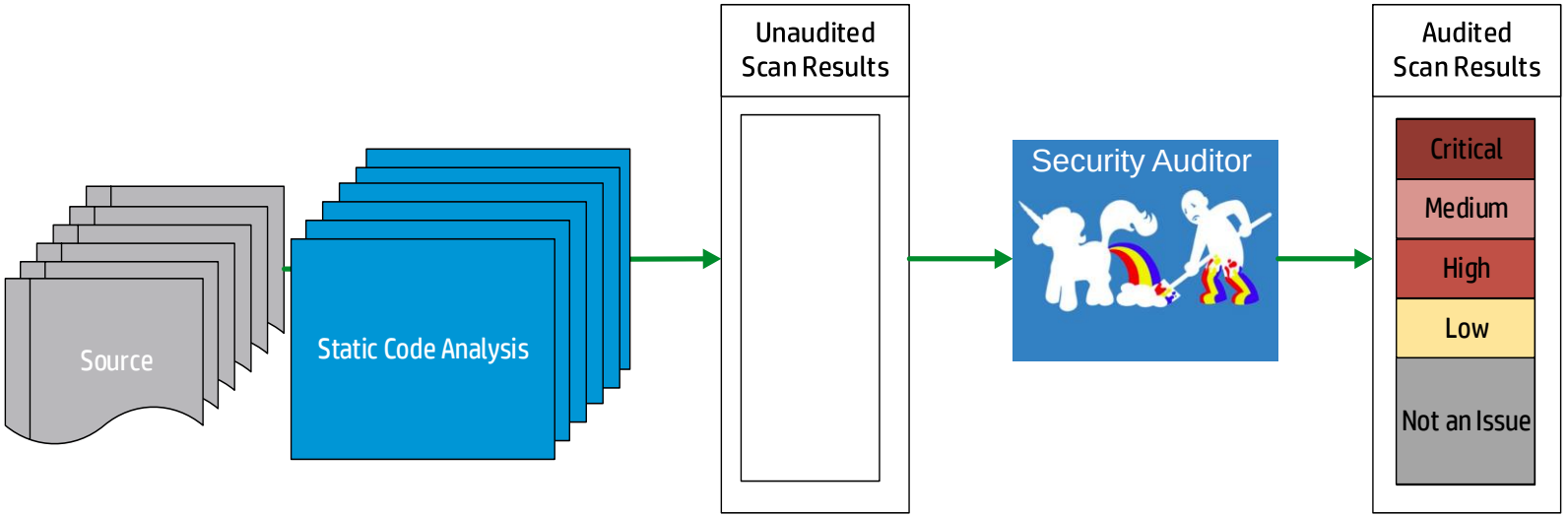
Or: How I scan a singe application



Finding relevant scan results is expensive and hard to scale because it requires:

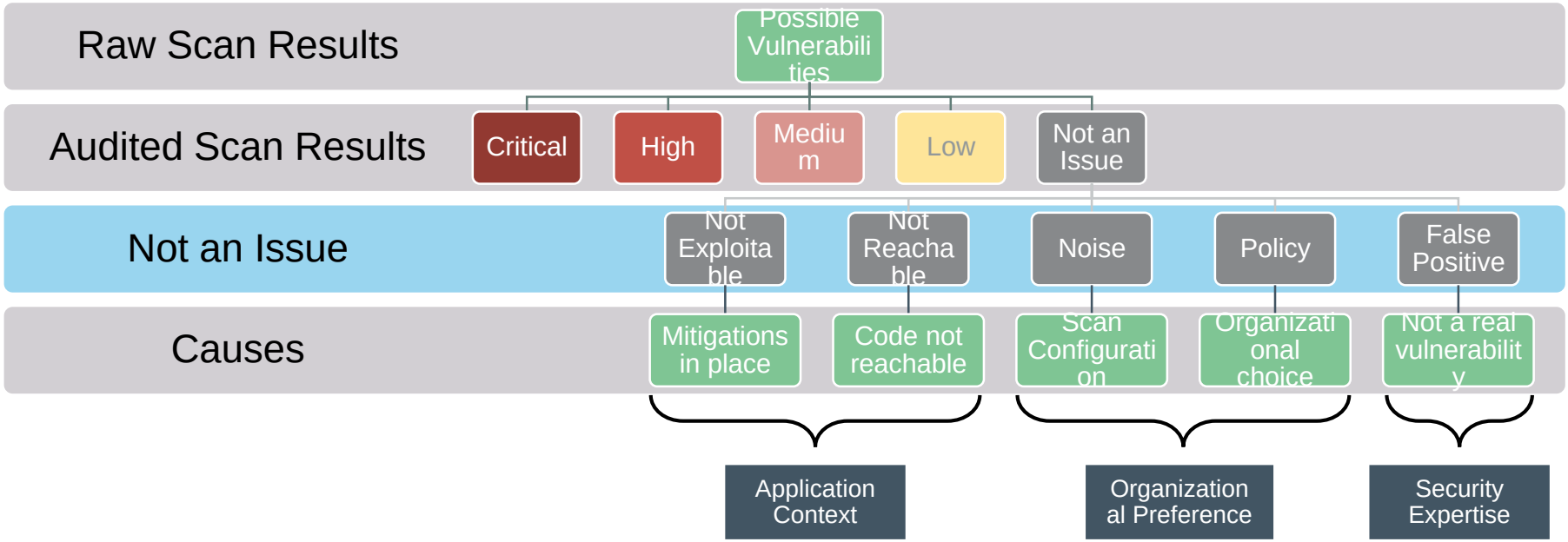
- Security expertise
- Knowledge of scanned application's context

Challenge: Identifying Issues at scale can be painstaking



There are many types of findings which are not issues

Contextual awareness and expertise is required to validate findings



Hewlett Packard Enterprise

Return value-added time to auditors & developers

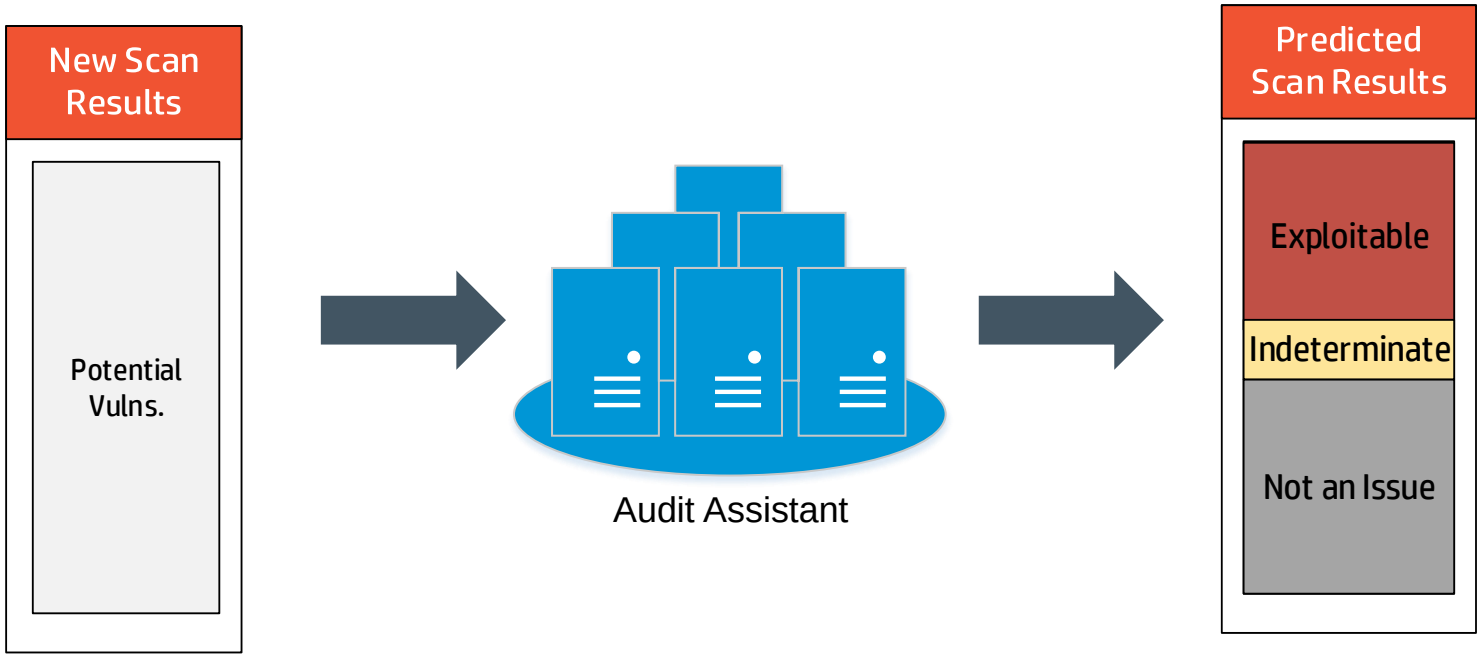
Without sacrificing scan integrity

Non-Issue Reduction	Accuracy	False Negative
25% – 90%	80%-98%	<1%

Results obtained are based on real world applications and scenarios.
Results vary based on training and customization. They are not guarantees of future performance.

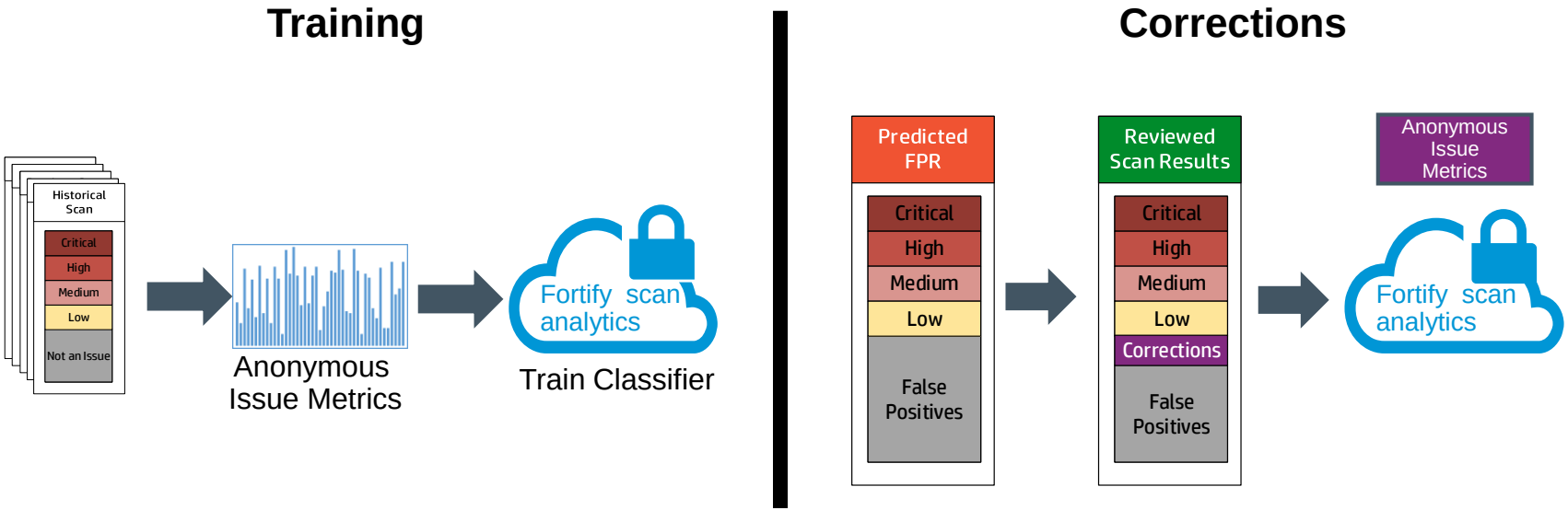
Software Security Center (SSC) - Audit assistant

Machine learning assisted identification of relevant scan results



Hewlett Packard Enterprise

Train audit assistant based on your organizational preferences



Machine Learning - scan analytics & audit assistant

Do more with your AppSec data

Streamline appsec program by making the auditing process more efficient

Increase the relevancy and consistency of findings unique to your organization preferences

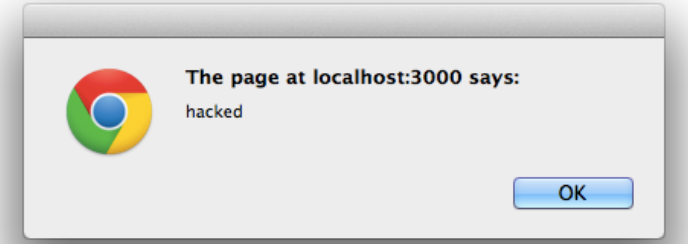
Identify relevant issues earlier in the SDLC

Scale and accelerate your AppSec program with existing resources

Hewlett Packard Enterprise

Dynamic Analysis - AppSec Testing Challenges

- *Loooong* scan times
- Testing can have persistent consequences
- Manual crawl often necessary to ensure coverage
- Additional manual security tests necessary to ensure vulnerabilities are identified
- Security findings in a running application will need to be linked to source

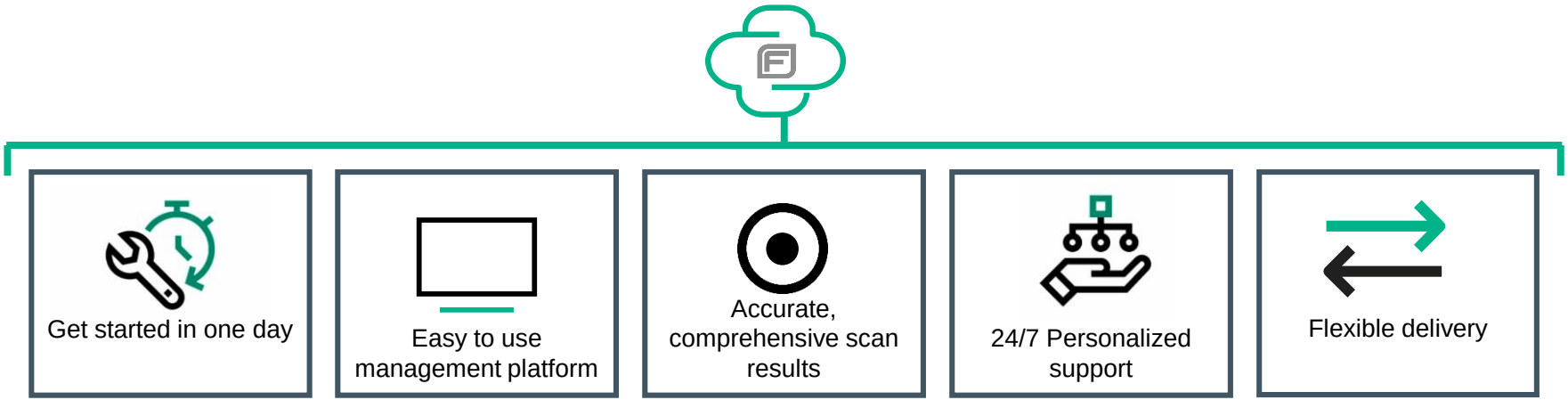


Recommendations

– Not sure where to start?	➔	Application Security Assessment
– DIY app sec?	➔	Attend a Fortify workshop near you
– Short on Security expertise?	➔	Fortify on Demand: software security as a service

HPE Security Fortify on Demand

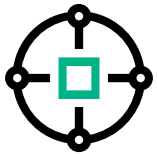
Managed Service that is Easy, Quick, Flexible and Scalable



Hewlett Packard Enterprise

HPE Security Fortify key advantages

Comprehensive



Only app sec provider to cover SAST, DAST, IAST and RASP

Proven

Over a decade of successful deployments backed by the largest security research team

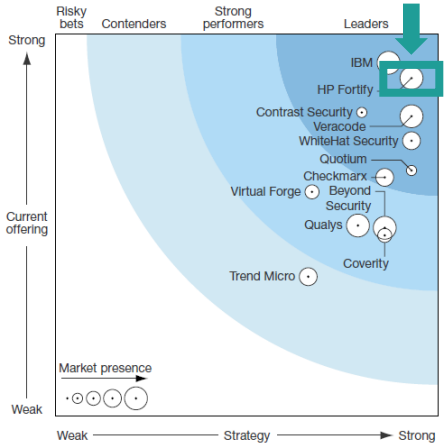
Flexible

Available on premise and on demand

HPE Security Fortify Leadership

Over a decade of successful deployments backed by the largest security research team

- 10 out of 10 of the largest information technology companies
- 9 out of 10 of the largest banks
- 4 out of 5 of the largest pharmaceutical companies
- 3 out of 3 of the largest independent software vendors
- 5 out of 5 of the largest telecommunication companies



Questions?

HPE Security Fortify WebInspect agent

IAST (Interactive AppSec Testing)

Find More

- Runtime level insight into application behavior
- Discover new vulnerability categories
- Identify and assess hidden areas of the site

Find Faster

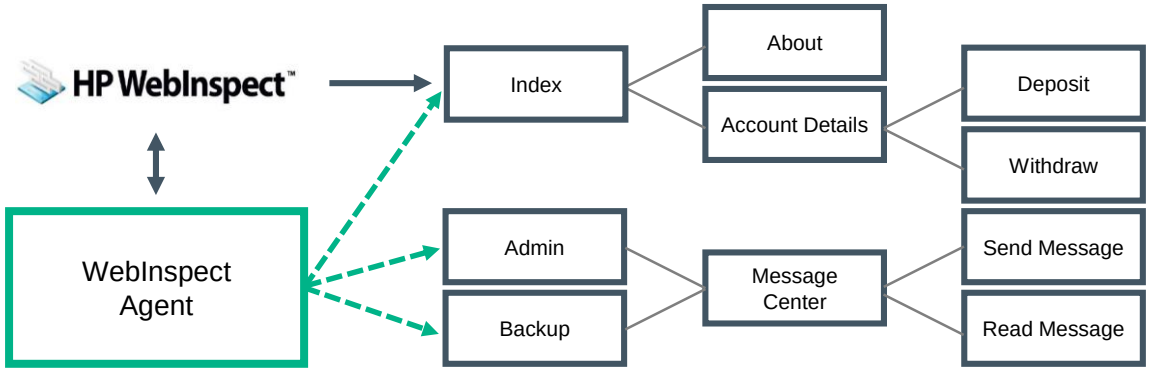
- Decrease scan time with active mode
- Avoid retesting reused code

Fix Faster

- Stack trace gives line of code accuracy to tell developers where to start
- Reduce false positives

IAST

- Supports Java and .Net applications

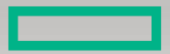


Thank you

- Complete the short survey and opt-in for more information from Hewlett Packard Enterprise.

www.hpe.com/software/fortify

www.vivit-worldwide.org



Hewlett Packard
Enterprise

YOUR INDEPENDENT HPE SOFTWARE USER COMMUNITY

vivit

vivit

Thank You

vivit-worldwide.org