Software Security Assurance for DevOps

Mike Pittenger, VP Security Strategy, Black Duck Software
Lucas v. Stockhausen, Sr. Product Manager HPE Fortify

Agenda

- Challenges impacting application security in DevOps
- Strategies for overcoming these challenges
- 5 Things you can do tomorrow

BLACKDUCK

Hewlett Packard Enterprise

Why We Partnered

- Organizations today manage application security for both custom and open source code
- HPE Security Fortify is a market leader in the application security space for customer code; Black Duck is a market leader in the application security space for open source
- Together, we allow customers to manage security risk in custom and open source code, through a single interface

Application Security Challenges

GROWING ATTACK SURFACE

Web, Mobile, Cloud, IoT

- Which apps are people using?
- How do I set internal policy requirements for app security?
- Is my private / sensitive data exposed by apps?
- Who is developing the apps?

NEW DEPLOYMENT MODELS

Containers, IT and Small Security Teams

- How do we prioritize the work for the resources I have?
- What do we test and how do we test it?
- How do we staff and improve skills and awareness?

OPEN SOURCE

Increasing Portion of Code Base

- What policies are in place for open source use?
- How are those policies enforced?
- Who is tracking usage for new vulnerabilities

Changing Attack Surface

- Web applications
- Cloud applications and services
- IoT

IoT Units Installed Base by Category (Millions of Units)

Category	2014	2015	2016	2020
Consumer	2,277	3,023	4,024	13,509
Business: Cross-Industry	632	815	1,092	4,408
Business: Vertical-Specific	898	1,065	1,276	2,880
Grand Total	3,807	4,902	6,392	20,797

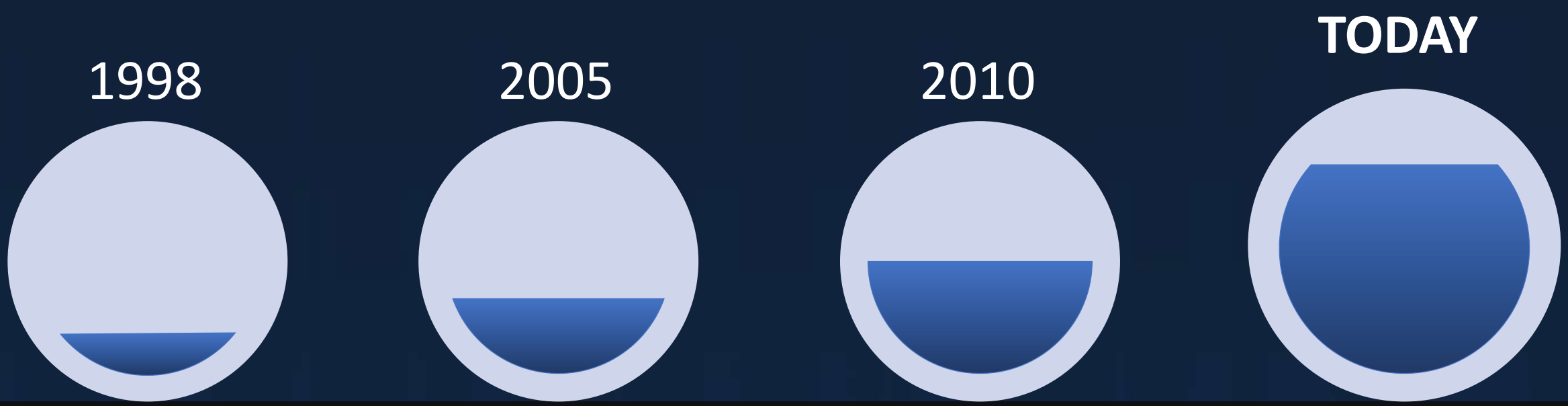
Source: Gartner (November 2015)

"If perimeter control is to remain the paradigm of cybersecurity, then the number of perimeters to defend in the Internet of Things is doubling every 17 months."

Dan Geer
In-Q-Tel
RSA 2016

BLACKDUCK

Open Source is the Foundation of Modern Applications



10%
Open Source

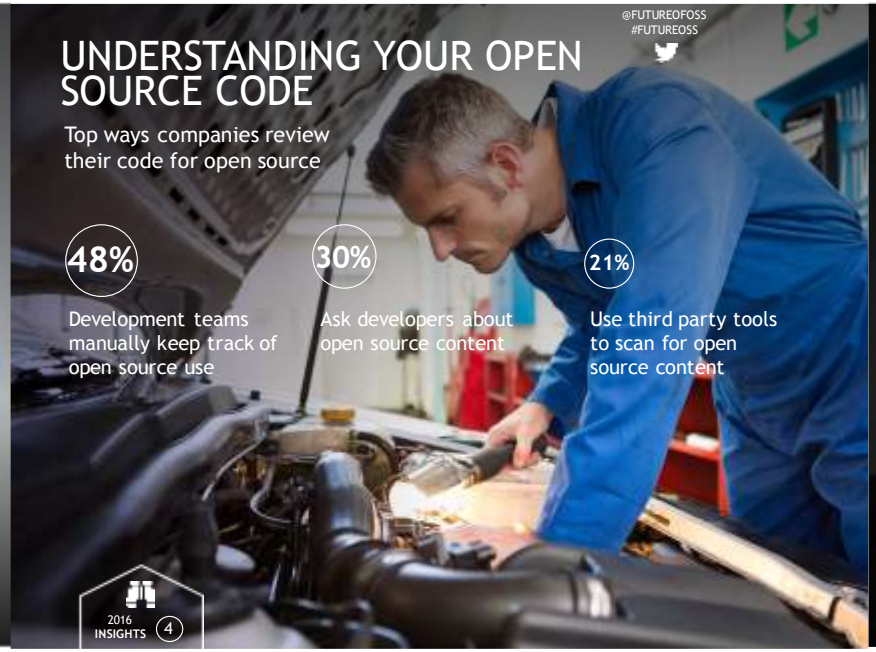
20%
Open Source

50%
Open Source

Up to 90%
Open Source

Open source Use has Outpaced Process Maturity

Everybody is using open source, but many organizations still do not have adequate processes or tools in place to manage it.

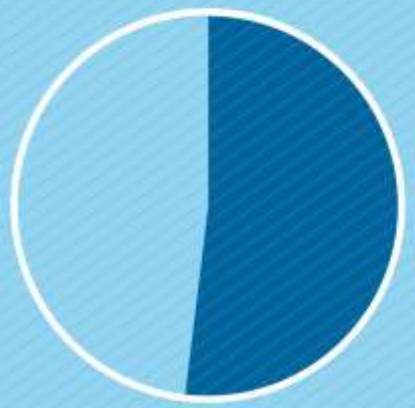


How Well Do Manual Processes Work?

2017 Open Source Security and Risk Analysis

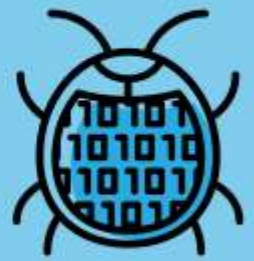
67%
Applications that contained known open source vulnerabilities

52%
Known open source vulnerabilities in each application that were rated as 'severe'

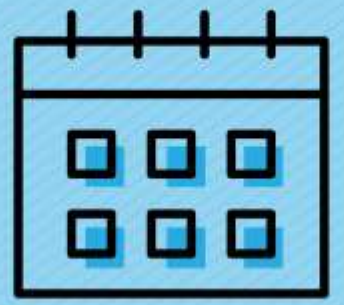


7%
Applications that still contained Heartbleed, Poodle, Freak, or Drown vulnerabilities

147
Average number of unique open source components per application

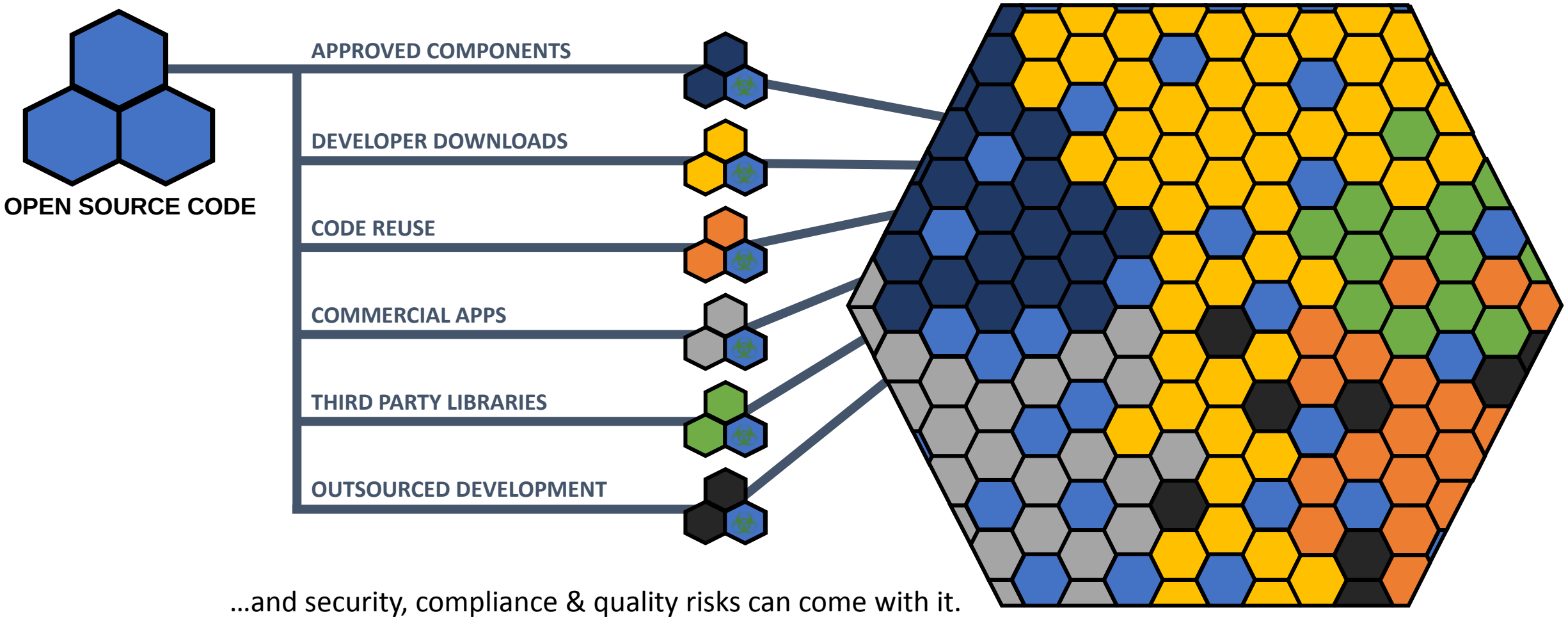


27
Average number of known open source vulnerabilities in per application



4 YEARS
Average age of vulnerabilities found in each application

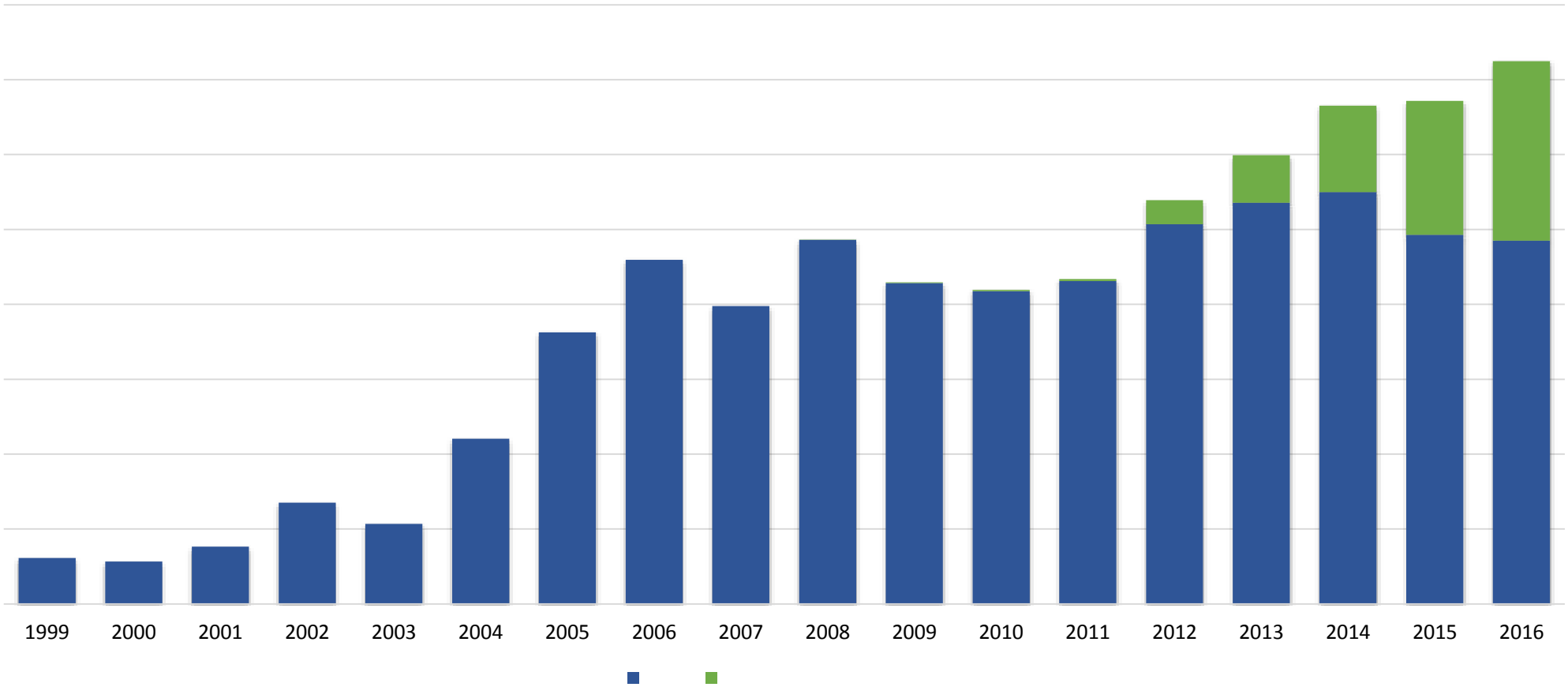
Open Source Enters Your Code in Many Ways…



…and security, compliance & quality risks can come with it.

BLACKDUCK

Open Source Vulnerabilities are Increasing



FREAK!
SSL, TLS Vulnerability

Reference: Black Duck Software knowledgebase, NVD, VulnDB

Static Analysis Does Not Help With Open Source

- Automated testing finds common vulnerabilities in the code you write
  - They are good, not perfect
  - Different tools work better on different classes of bugs
  - Many types of bugs are undetectable except by trained security researchers

Four Factors That Make Open Source Different

Used Everywhere

Easy access to code

GitHub

nuget

Vulnerabilities are public

Exploits readily available

Who's Responsible for Open Source Security?

Commercial Code

- Dedicated security researchers
- Alerting and notification infrastructure
- Regular patch updates

Dedicated support team with SLA

Open Source Code

- "Community"-based code analysis
- Monitor newsfeeds yourself
- No standard patching mechanism

Ultimately, you are responsible

Bad Guys Have Quotas Too (Non-Targeted Attacks)

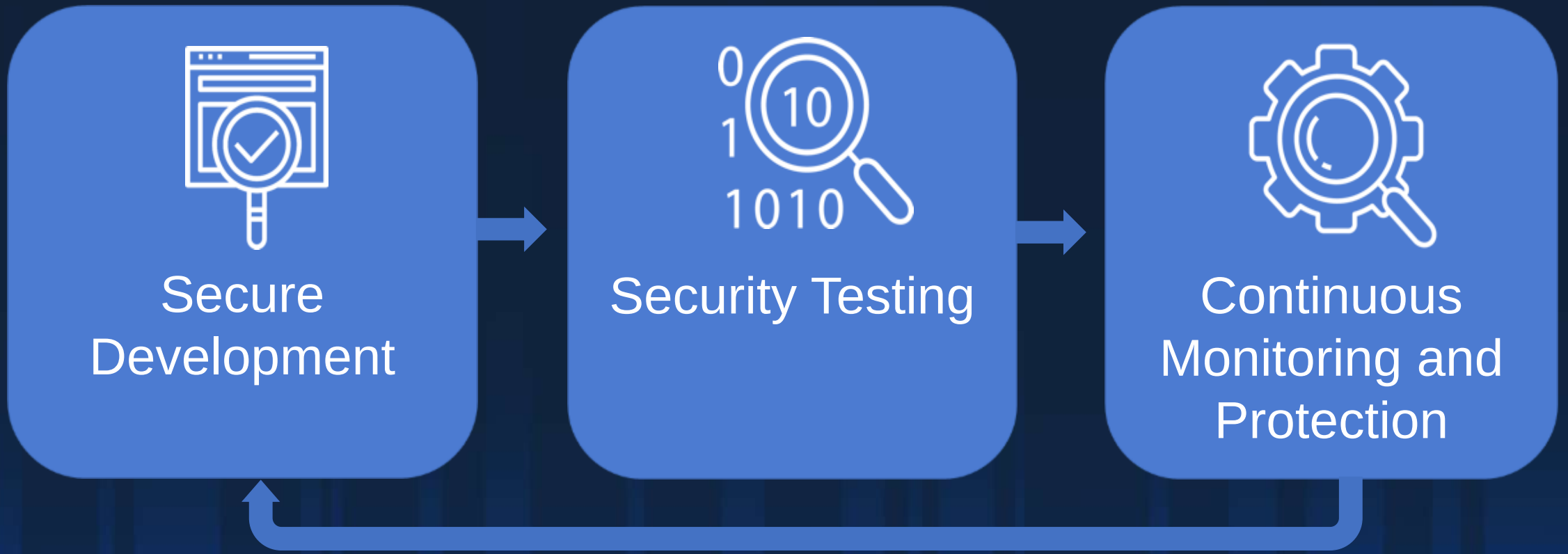
Rational Choice Theory

- Criminals make a conscious, rational choice to commit crimes
- Behavior is a personal choice made after weighing costs and benefits of available alternatives
- The path of least resistance will be taken

Integrating Application Security in DevOps

BLACKDUCK

Application Security Testing for the New SDLC



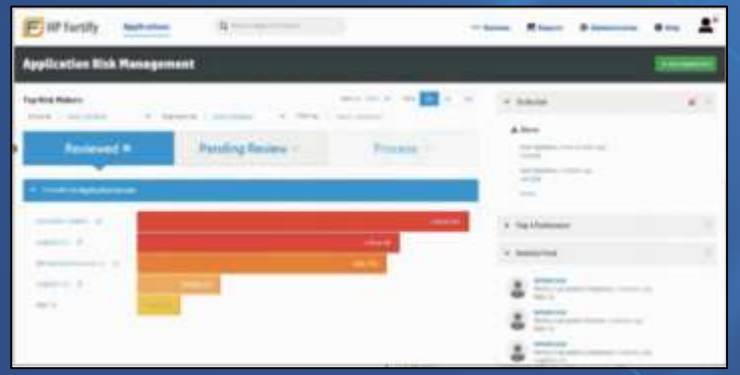
HPE Security Fortify and Black Duck Integration

BLACKDUCK

Black Duck Integration with HPE Security Fortify SSC

- HPE Security Fortify + Black Duck Technology Alliance Partnership
- Address pervasive, rapidly-growing Security & Compliance risks with Open Source
- Gain visibility on risks across Custom Code and Open Source Code
- Integrate governance and remediation as part of Software Security Assurance

Manage Risks in Open Source as part of HPE Security Fortify SSC



Hewlett Packard Enterprise

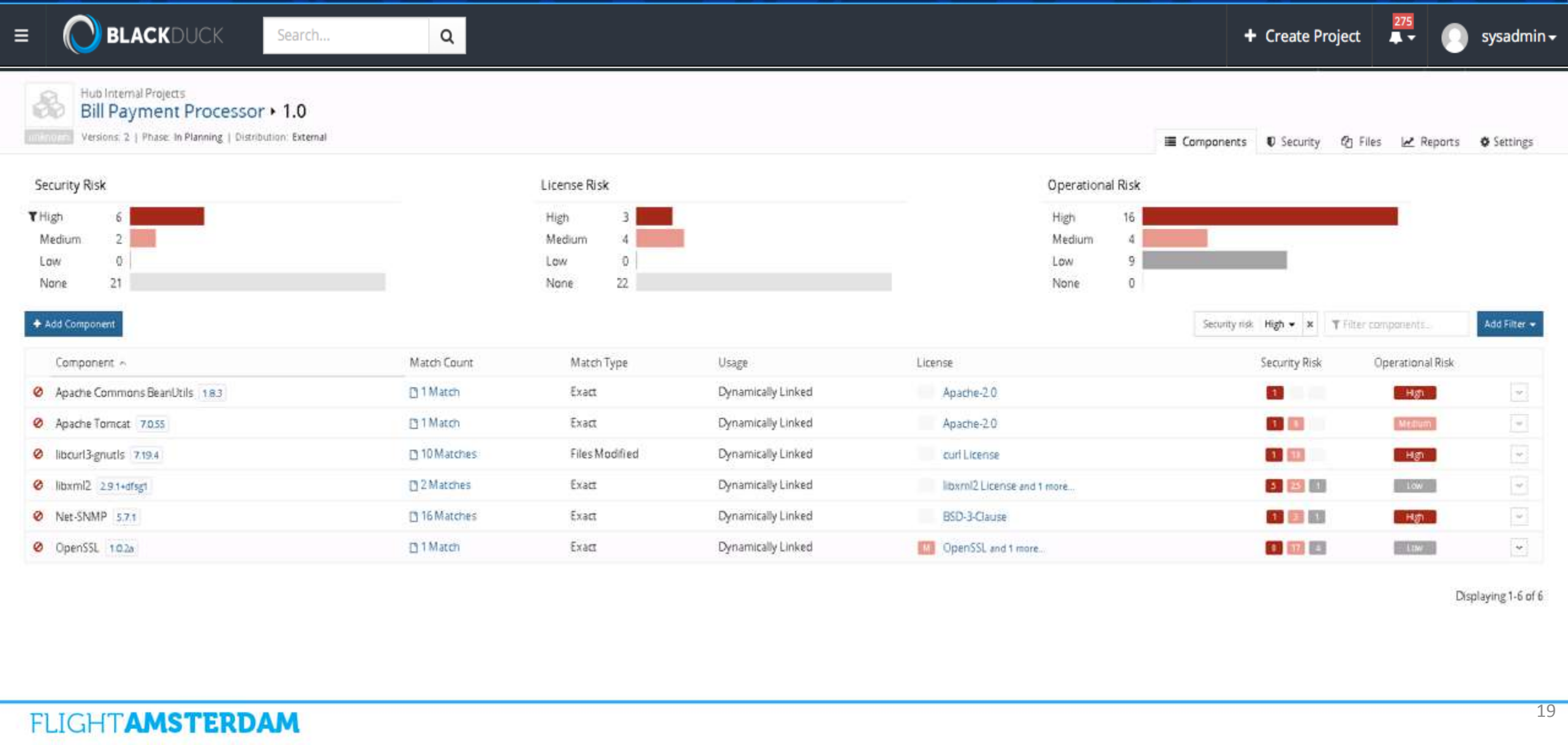
Risks in **Custom Code** with SAST, DAST, & RASP

BLACKDUCK

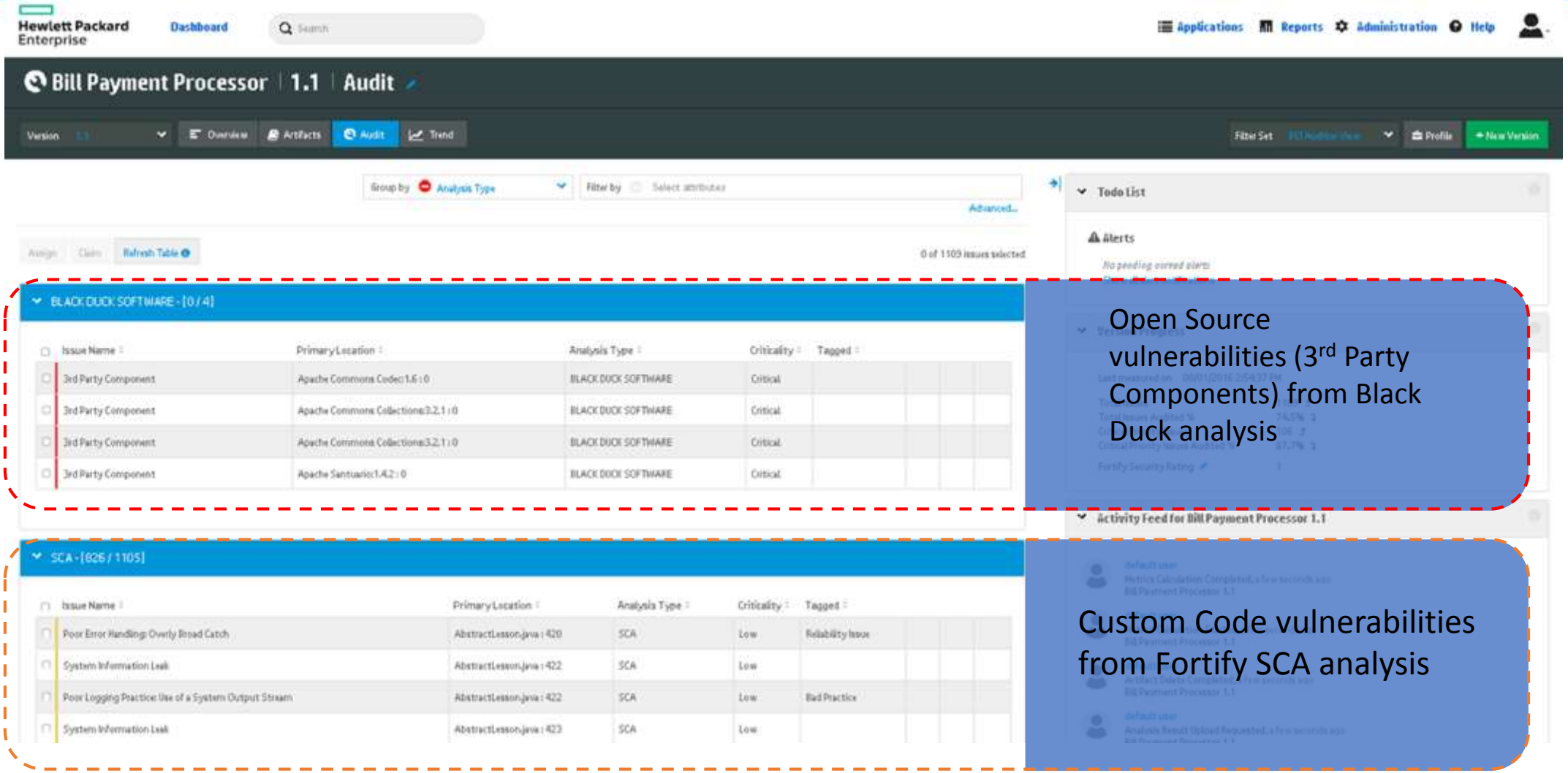
Risks in **Open Source Code** (Black Duck Hub)

BLACKDUCK

Open Source Vulnerabilities – Black Duck



Overview Shows Black Duck Results Within HPE Security Fortify

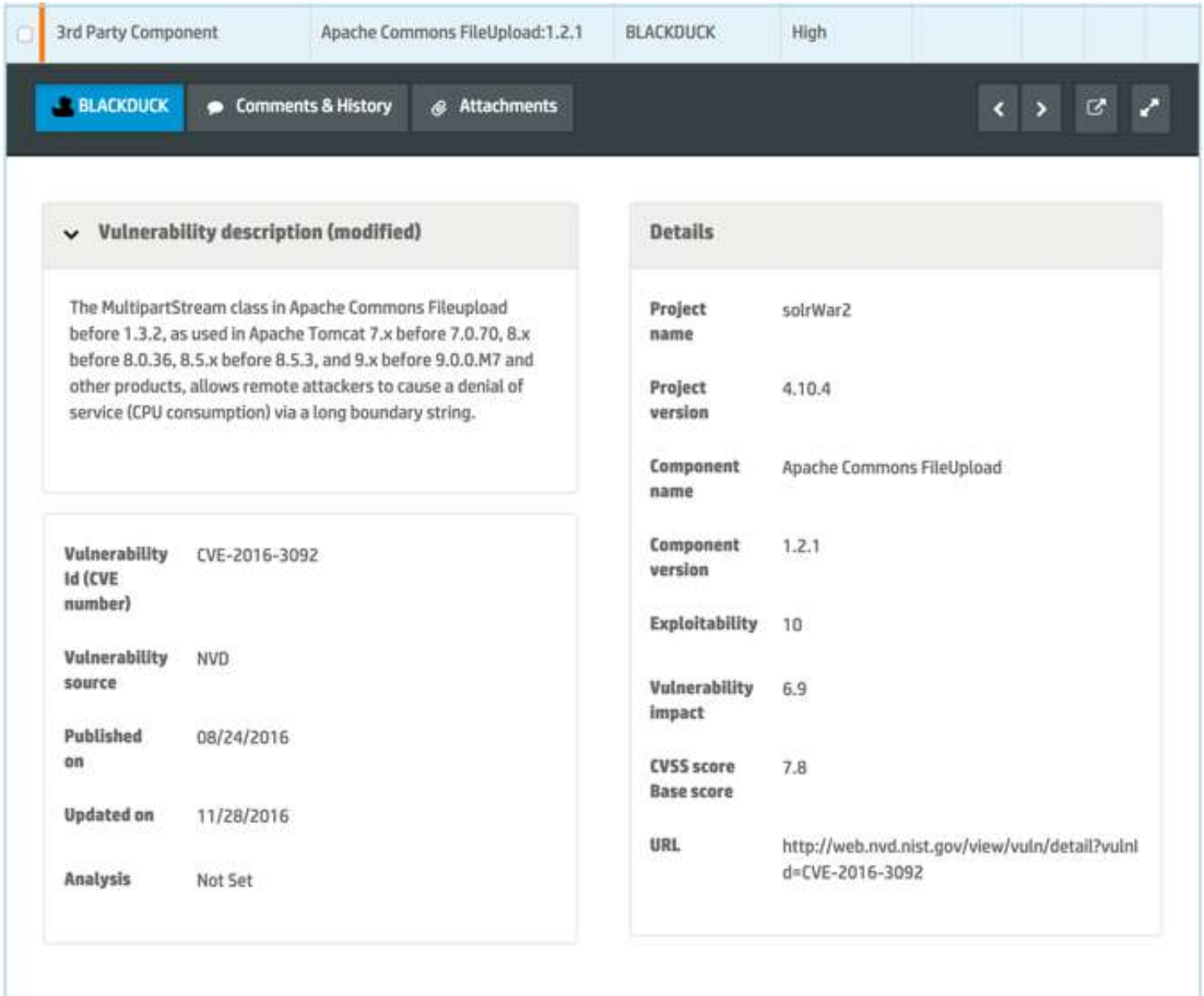


Open Source vulnerabilities (3rd Party Components) from Black Duck analysis

Custom Code vulnerabilities from Fortify SCA analysis

BLACKDUCK

Detailed View of Black Duck Results Within HPE Security Fortify

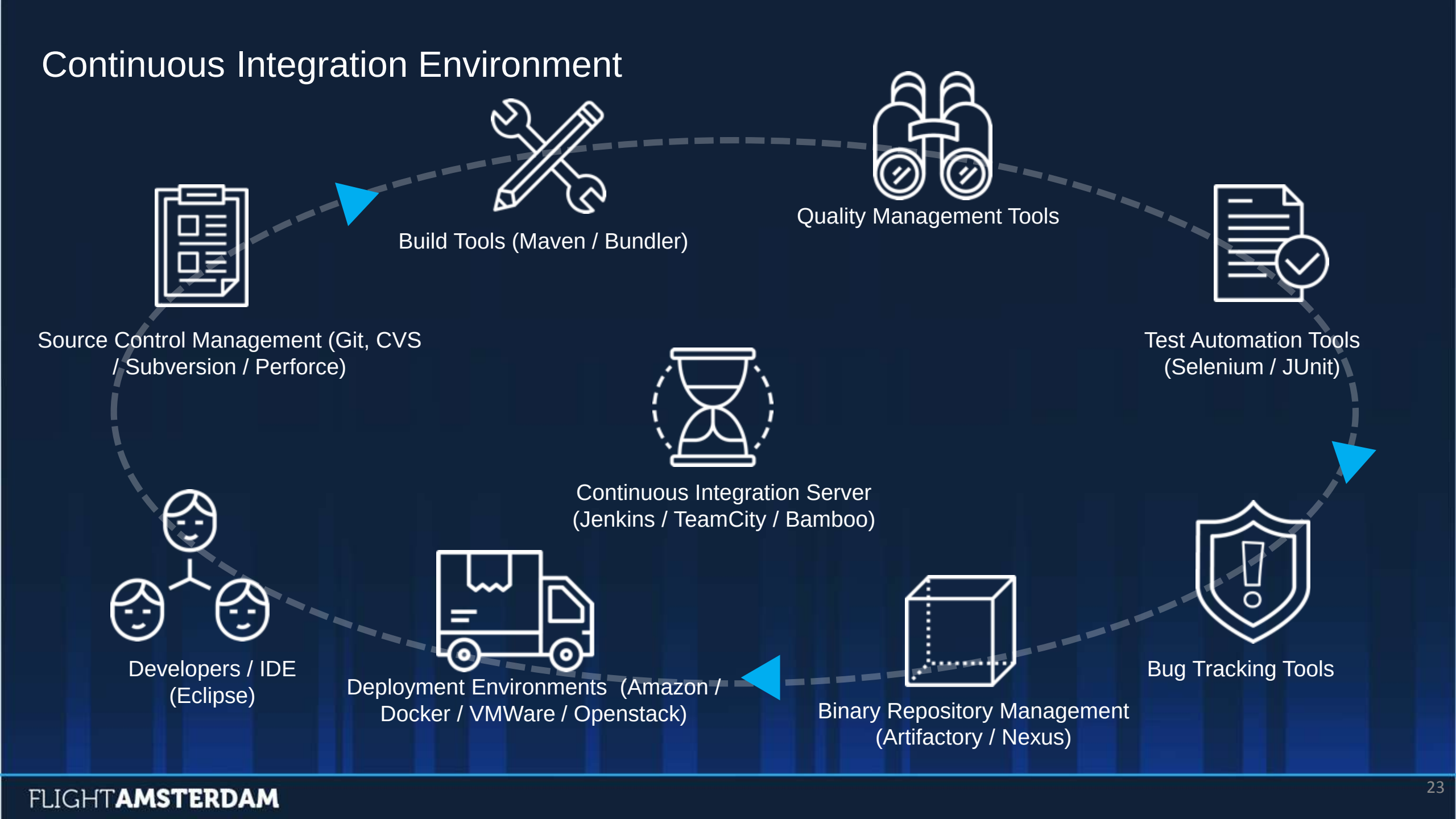


BLACKDUCK

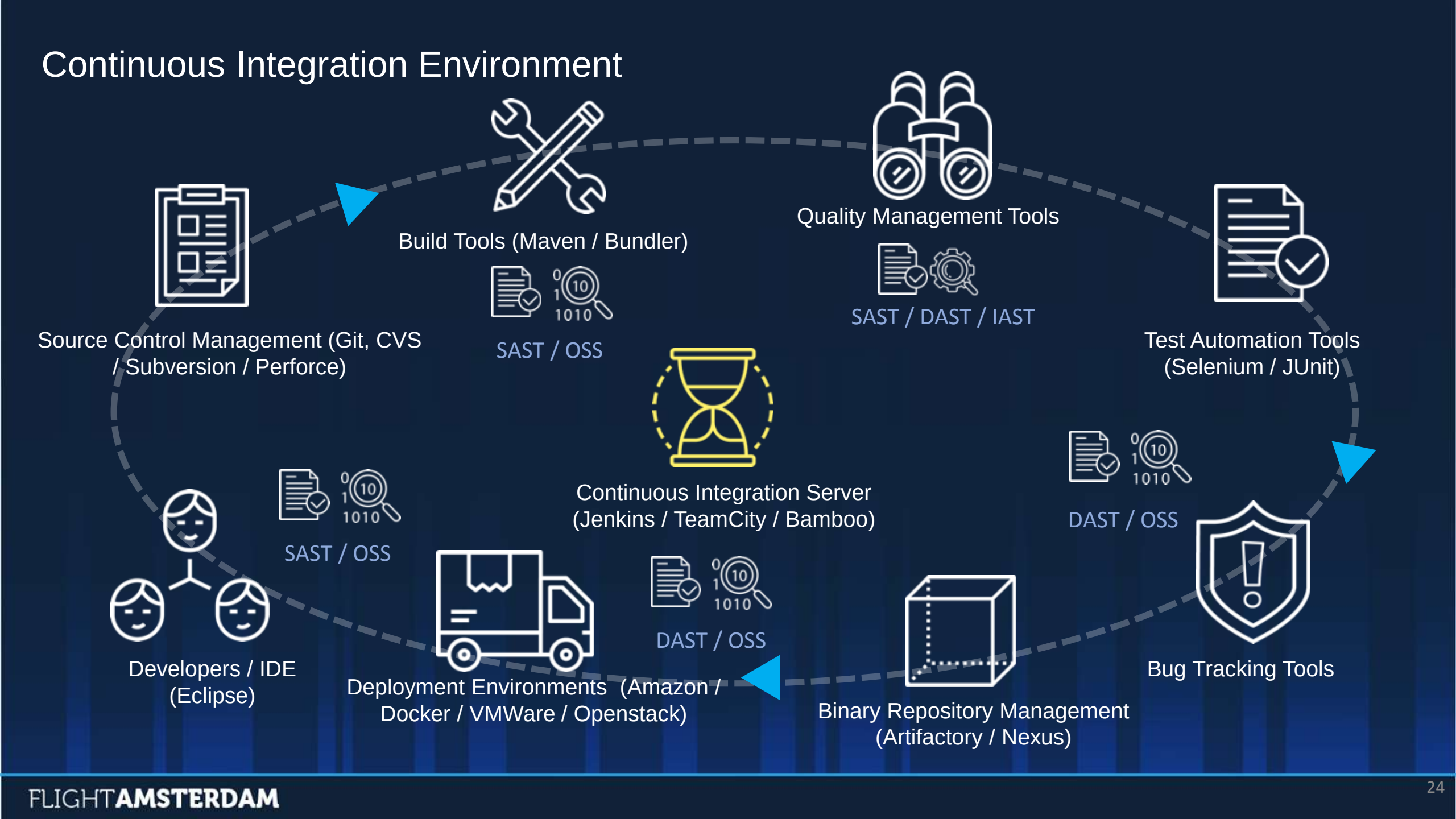
Automating Security Testing in a DevOps Environment

BLACKDUCK

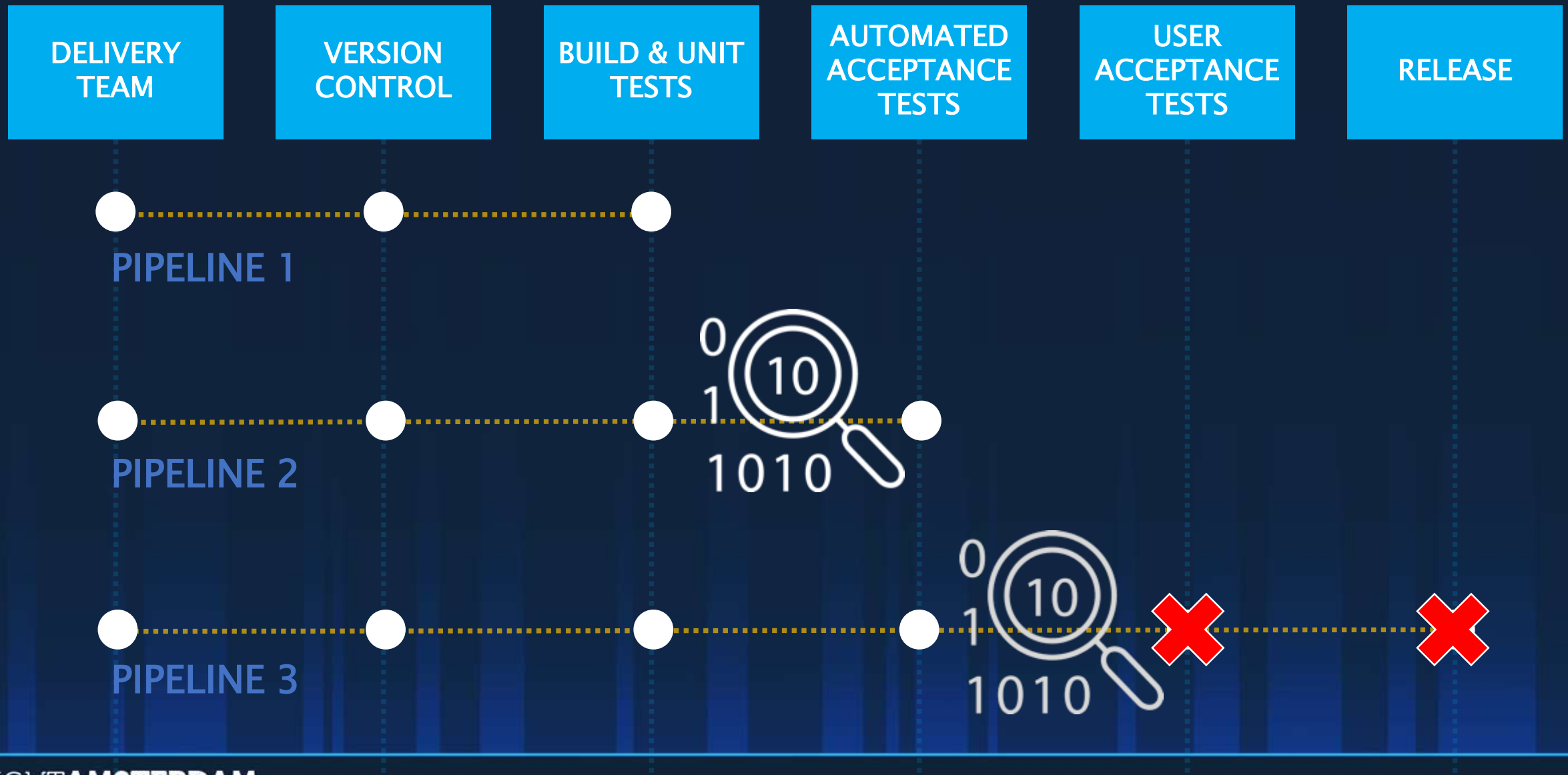
Continuous Integration Environment



Continuous Integration Environment



Automation Differs Between Apps



What Can You Do Tomorrow?

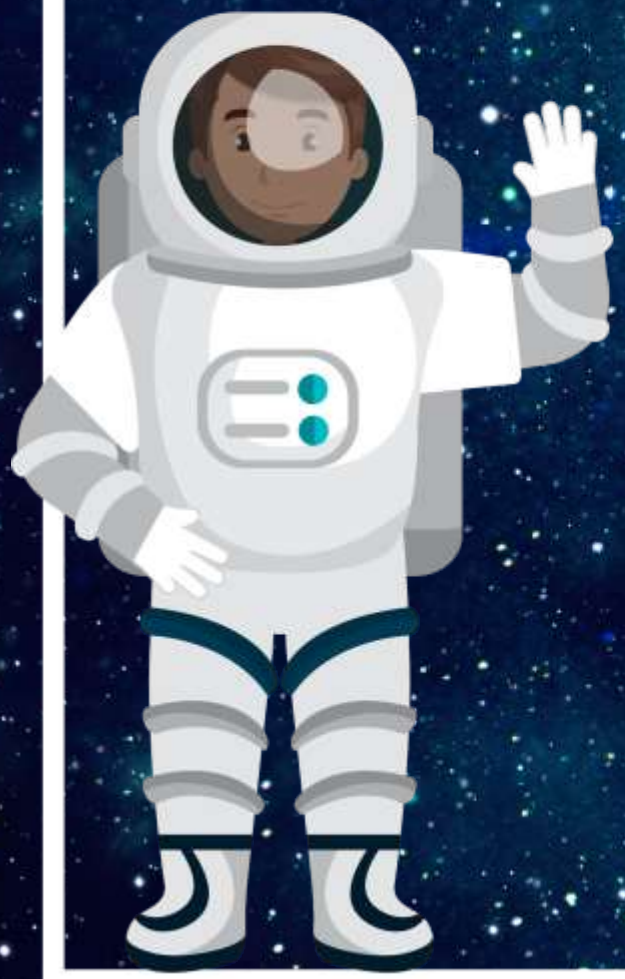
- Speak with your heads of application security and software development and find out…
  - What policies exist for managing open source?
  - Is there a list of components used in all applications?
  - How are they creating the list?
  - What controls do they have to ensure nothing gets through?
  - How are they tracking vulnerabilities for all components over time?
  - How do they account for the different testing requirements for custom code v. open source?
  - What is the best security automation strategy for your organization?

Questions

Contact: hpe@blackducksoftware.com

Visit: http://www.blackducksoftware.com/hpe

BLACKDUCK



BLACKDUCK 2017 FLIGHT

November 7-9, 2017 | Boston, MA

Join us in Boston

REGISTER NOW

Or Click Here: http://blkduk.io/2vnikhH