BLACKDUCK

DOES OPEN MEAN VULNERABLE?

GENIVI All Members Meeting, Seoul Korea - October 2015

Bill Weinberg, Senior Director, Open Source Strategy
Black Duck Software

AGENDA

- Introduction
- Security by Obscurity
- Security through Openness
- Open Source Hygiene
- Conclusion and Q&A

INTRODUCTION

BLACKDUCK

YOUR SPEAKER

Bill Weinberg, Senior Director, Open Source Strategy – Black Duck Software

Bill helps Fortune 1000 clients create secure approaches to enable, build, and deploy software for intelligent devices, IoT, automotive systems, enterprise data centers, and cloud infrastructure.

Working with FOSS since 1997, Bill also boasts more than thirty years of experience in embedded and open systems, telecommunications, and enterprise software. As a founding team-member at MontaVista Software, Bill pioneered Linux as leading platform for intelligent and mobile devices. During his tenure as Senior Analyst at OSDL (today, the Linux Foundation), Bill ran Carrier Grade and Mobile Linux initiatives and worked closely with foundation members, analyst firms, and the press. As General Manager of the Linux Phone Standards Forum, he worked tireless to establish standards for mobile telephony middleware.

Bill is also a prolific author and busy speaker on topics spanning global FOSS adoption to real-time computing, IoT, legacy migration, licensing, standardization, telecoms infrastructure, and mobile applications. Learn more at http://www.linuxpundit.com/.

BLACKDUCK

BLACK DUCK – SECURING AND MANAGING OPEN SOURCE

24
Countries

185+
Employees

1,600
Customers

27 of the Fortune 100

7 of the top 10 Software companies, and 44% of the top 100

6 of the top 8 Mobile handset vendors

6 of the top 10 Investment Banks

Four Years in the "Software 500" Largest Software Companies

Six Years in a row for Innovation

Gartner Group "Cool Vendor"

Award for Innovation

"Top Place to Work," The Boston Globe

BLACKDUCK

TWO COMPETING NARRATIVES

Security by Obscurity

Security through Openness

BLACKDUCK

SECURITY BY OBSCURITY

The Traditional Approach

BLACKDUCK

SECURITY BY OBSCURITY

Classified

Non-disclosure

Obfuscation

Need to know

Least Privilege

Role-based

Encryption

Eyes Only

Mandatory Access Control

Triple Fence

Top Secret

Hardened

BLACKDUCK

SECURITY BY OBSCURITY

Practical Definition for Developers

- Minimize/eliminate access to source code
- Small teams create, review, maintain systems and apps
- No purview by or sharing with third parties
- Restrictions enforced by technical and statutory means

The practical antithesis of open source

OBSCURITY FALLACY

Hacking tools and malware don't require source code

- Root kits, RATs, fuzzing, etc.
- Viruses, worms, DDoS, MitM, etc.

Fewer eyes mean less purview, potentially more bugs

- Closed favors black hats over white

Secrecy affects vendor behavior

- False sense of security
- Slower, less aggressive remediation

BLACKDUCK

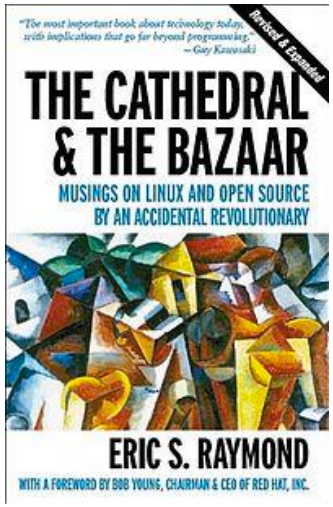
SECURITY THROUGH OPENNESS

Community-based security

BLACKDUCK

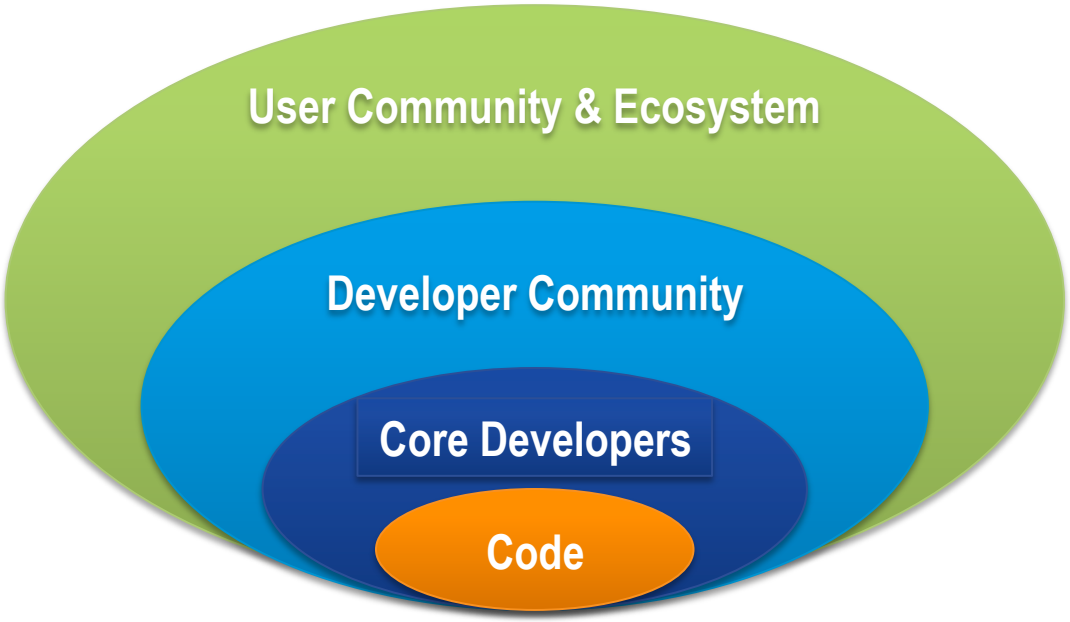
LINUS' LAW

Given enough eyeballs, all bugs are shallow



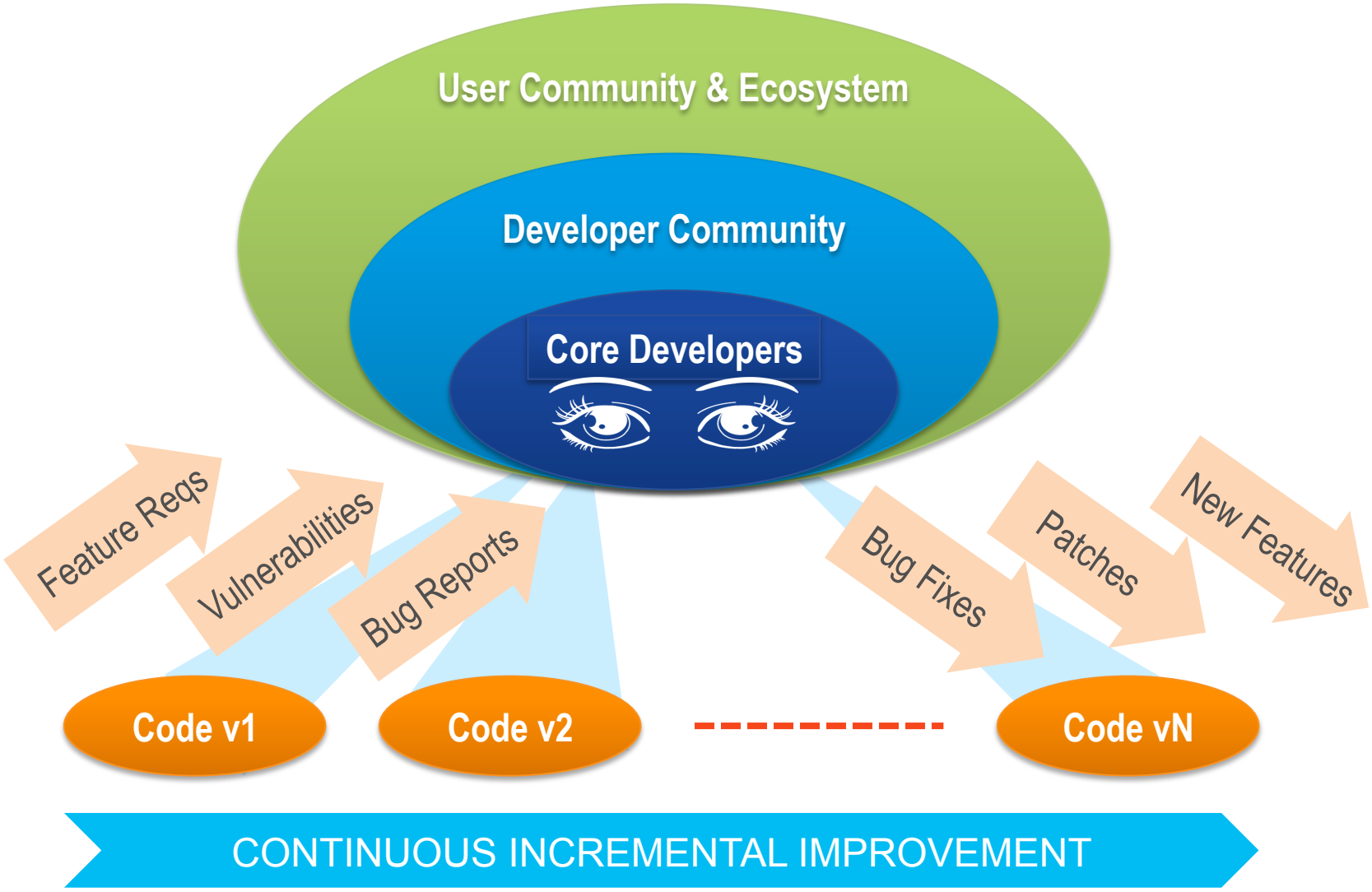
BLACKDUCK

OPEN SOURCE DEVELOPMENT MODEL



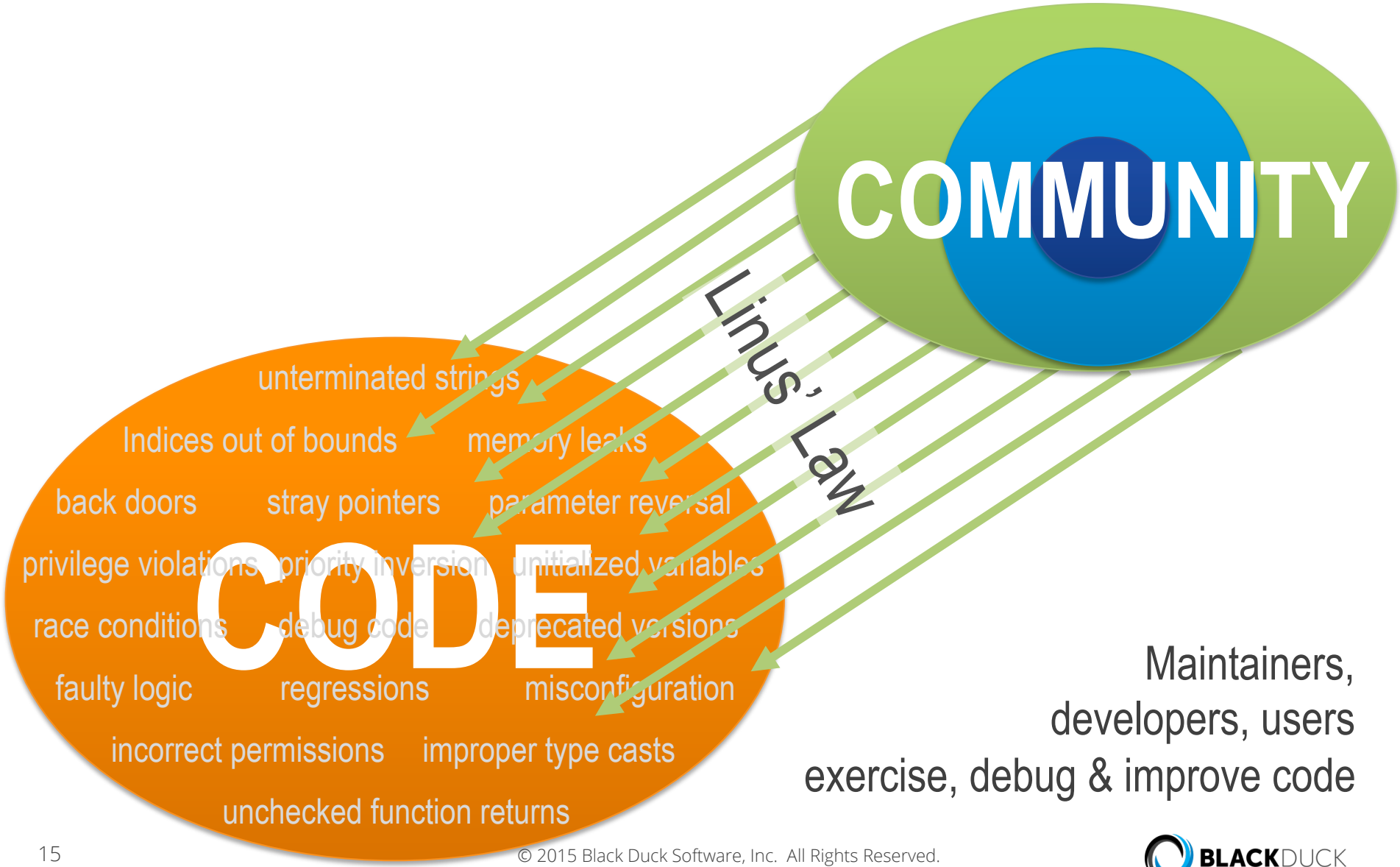
- Core project developers create, maintain, curate code base
- Vet contributions from larger communities
- Focus on project goals – features, performance, etc.

OPEN SOURCE CODE CURATION MODEL



BLACKDUCK

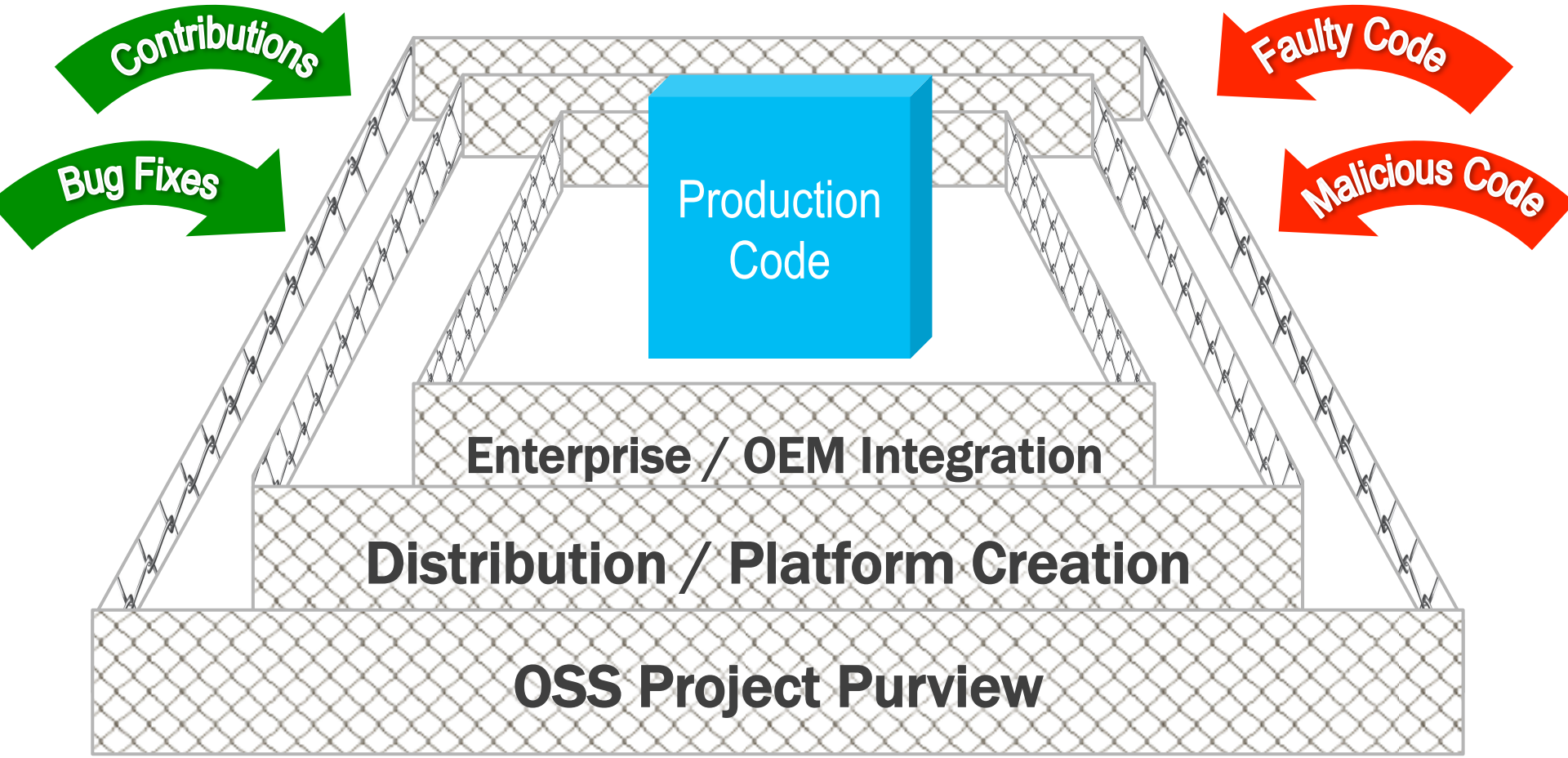
OPEN SOURCE CODE QUALITY ASSURANCE



Maintainers,
developers, users
exercise, debug & improve code

BLACKDUCK

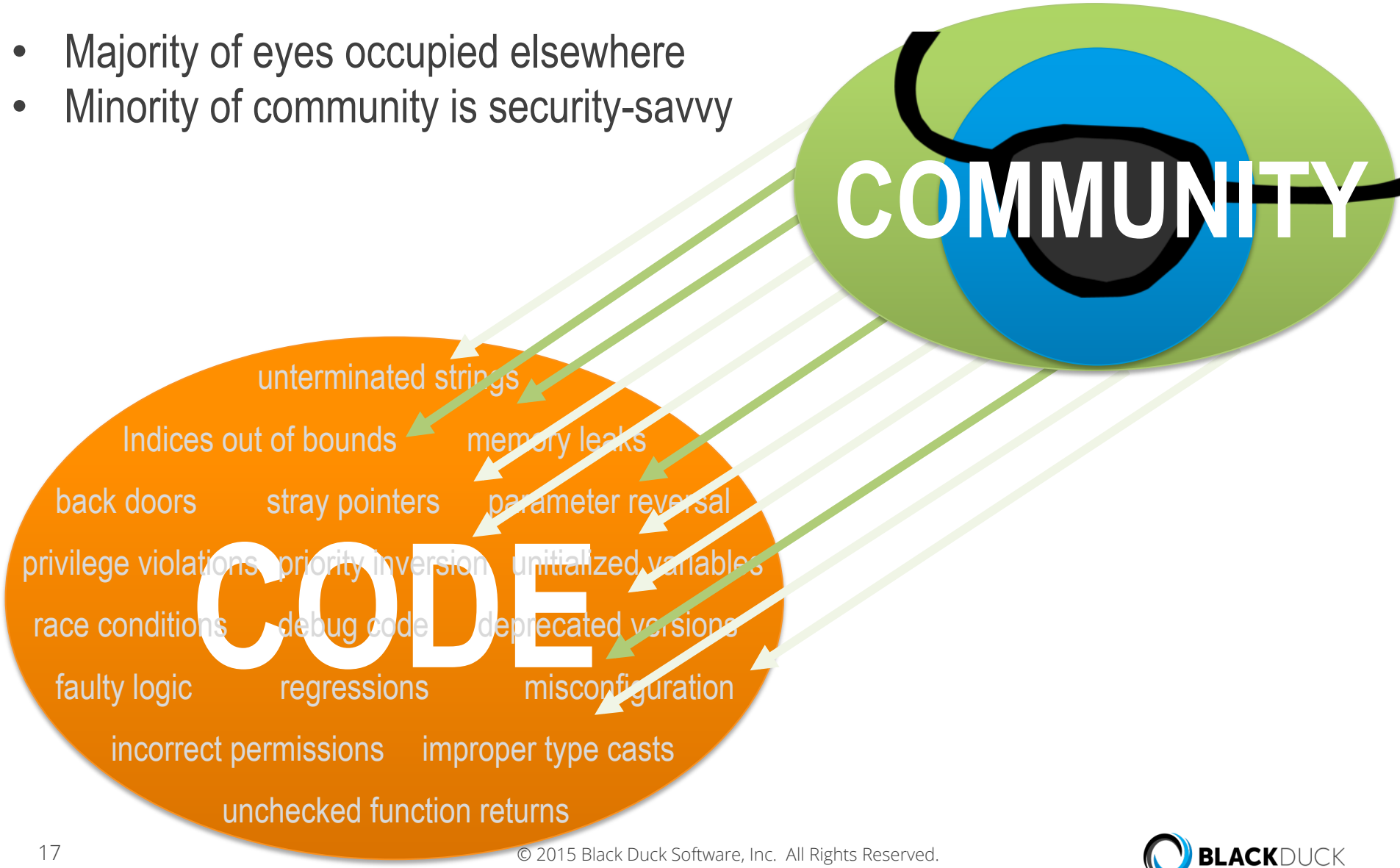
THEORETICAL "TRIPLE FENCE" OF OSS SECURITY



BLACKDUCK

OPEN SOURCE CODE SECURITY GAP

- Majority of eyes occupied elsewhere
- Minority of community is security-savvy



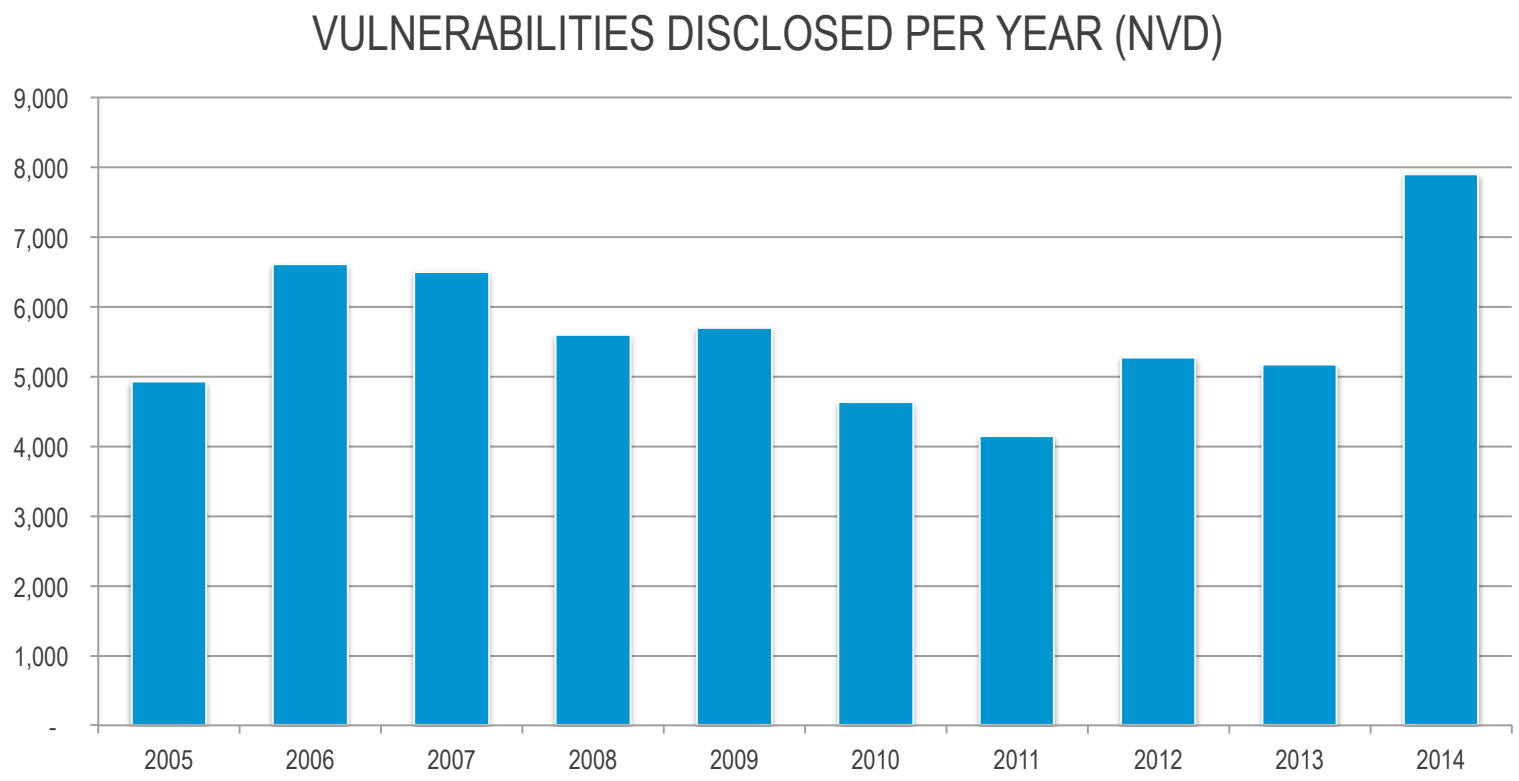
BLACKDUCK

WHAT DO THESE VULNERABILITIES HAVE IN COMMON?

	Heartbleed	Shellshock	Freak	Ghost	Venom
Since:	2011	1989	1990's	2000	2004
Discovered:	2014	2014	2015	2015	2015
Discovered by:	Riku, Antti, Matti, Mehta	Chazelas	Beurdouche	Qualys researchers	Geffner
Component:	OpenSSL	Bash	OpenSSL	GNU C library	QEMU

BLACKDUCK

INCREASING VULNERABILITIES



In 2014:

- Over 7,900 new vulnerabilities disclosed & catalogued
- ~4,300 in Open Source, ~3,600 in commercial software

Reference: Black Duck Software knowledgebase, NVD

THE BROADER IT INDUSTRY IS CONCERNED

"Through 2020, security and quality defects publicly attributed to OSS projects will increase significantly, driven by a growing presence within high-profile, mission-critical and mainstream IT workloads."

Gartner

Gartner, Road Map for Open-Source Success: Understanding Quality and Security, Mark Driver, 3 March 2014.

BLACKDUCK

OPEN SOURCE HYGIENE

Securing and Managing Open Source S/W

BLACKDUCK

Open Source Hygiene is the practice of cross referencing the open source content of a company or product software stack, module by module, version by version, with databases of known vulnerabilities of those software components.

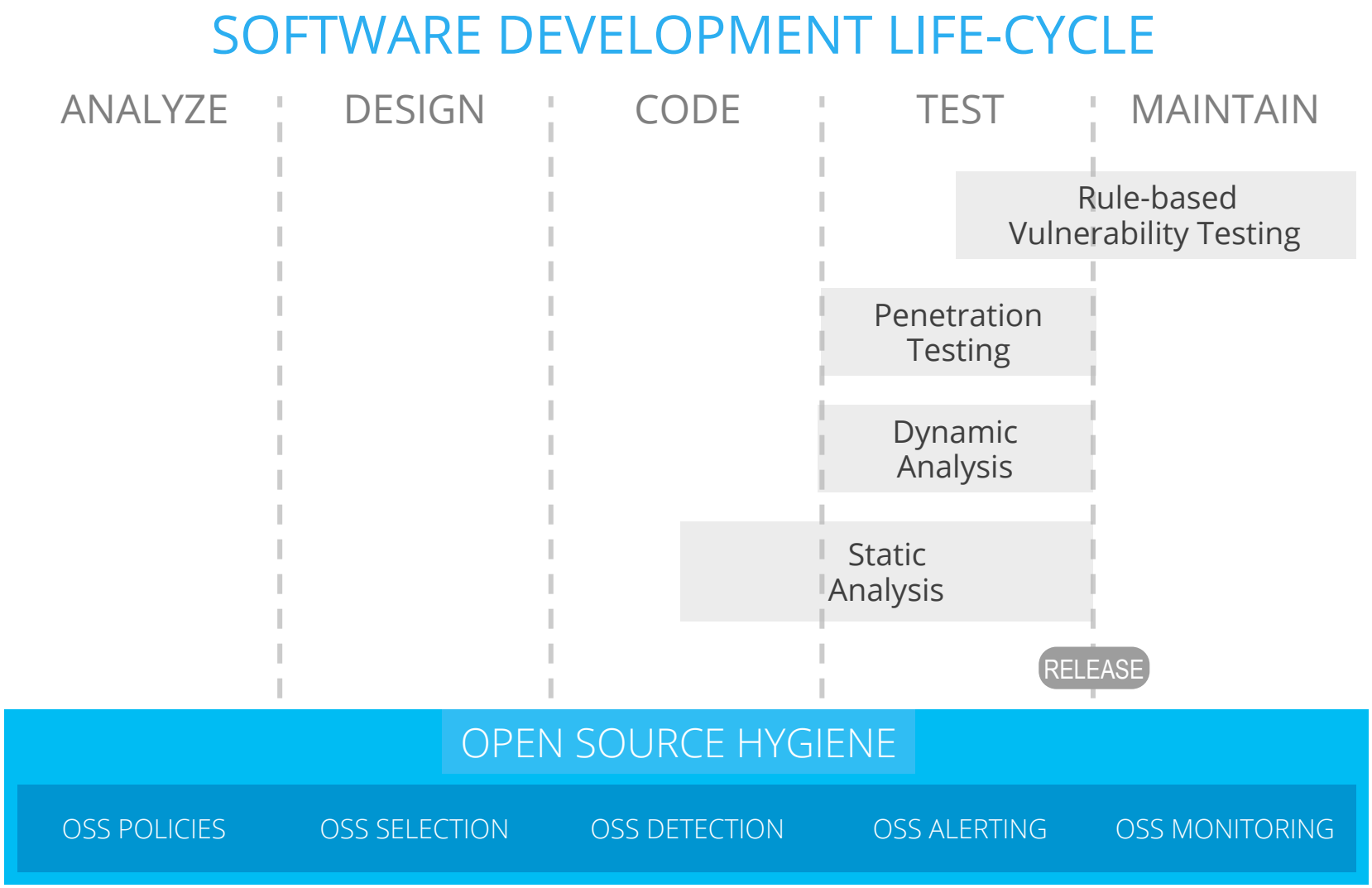
BLACKDUCK

YET ANOTHER SECURITY TECHNOLOGY TERM

Software Composition Analysis (SCA)

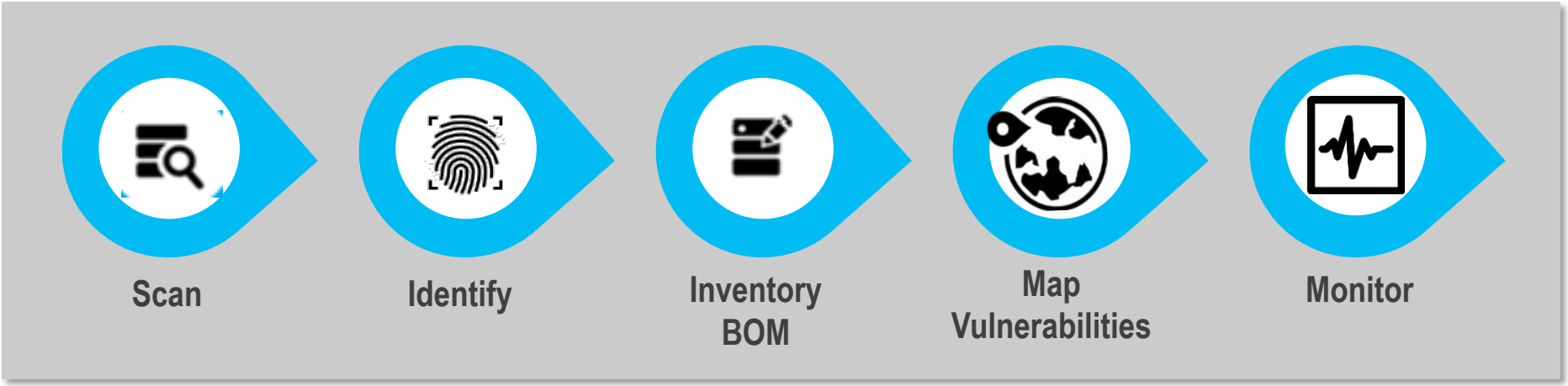
BLACKDUCK

OSS HYGIENE COMPLEMENTS SECURITY TESTING



BLACKDUCK

DUE DILIGENCE ACROSS THE DEVELOPMENT LIFE-CYCLE



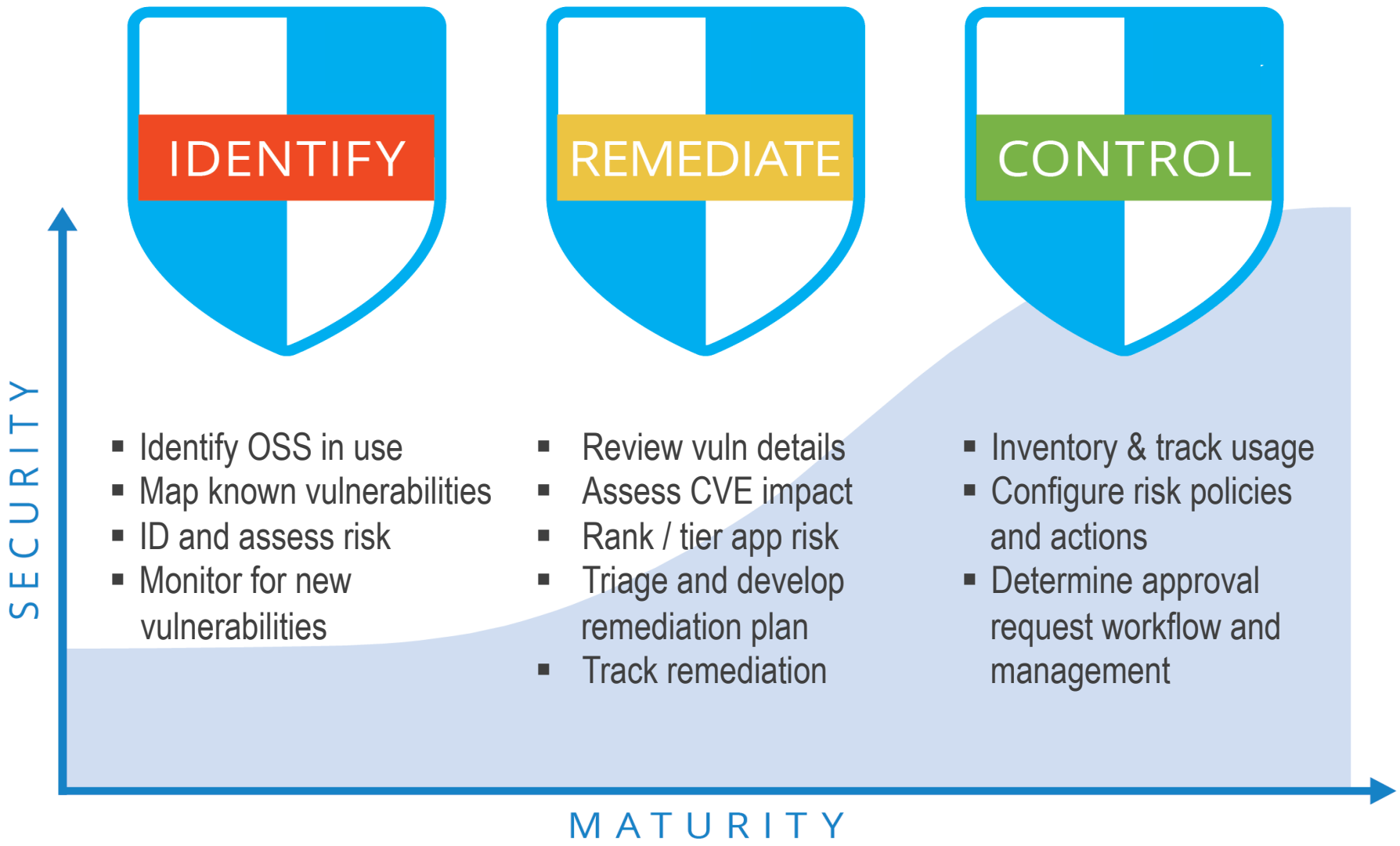
Accurate list of open source components automatically created for any application at any point in the SDL

Identify vulns during development

Alert new vulns in production apps

BLACKDUCK

THE ROAD TO SECURE OSS USE – BEST PRACTICES



- Identify OSS in use
- Map known vulnerabilities
- ID and assess risk
- Monitor for new vulnerabilities

- Review vuln details
- Assess CVE impact
- Rank / tier app risk
- Triage and develop remediation plan
- Track remediation

- Inventory & track usage
- Configure risk policies and actions
- Determine approval request workflow and management

BLACKDUCK

DOES OPEN MEAN VULNERABLE? IT DEPENDS . . .

1. Under ideal conditions, open is more secure than closed
2. Conditions are never ideal
3. Integrators and end-users need to supplement community

Choose Your Hat

BLACKDUCK


Q&A
BLACKDUCK