BLACKDUCK OSS SCANNING

DevOps Training

OPEN SOURCE HYGIENE MANTRA

Open source hygiene –

Mitigating Security Risks from Development, Integration,

Distribution and Deployment of Open Source Software

WHY BD SCANNING IS REQUIRED?

Across the landscape of IT, Open Source Software (OSS) is pervasive and ubiquitous. From the cloud and web to data centers; from the desktop to mobile devices; and across a range of embedded and IoT applications, OSS commands an ever-increasing, dominant share of the system software stack and provides equally substantial swathes of enabling application middleware, applications themselves, and tooling.

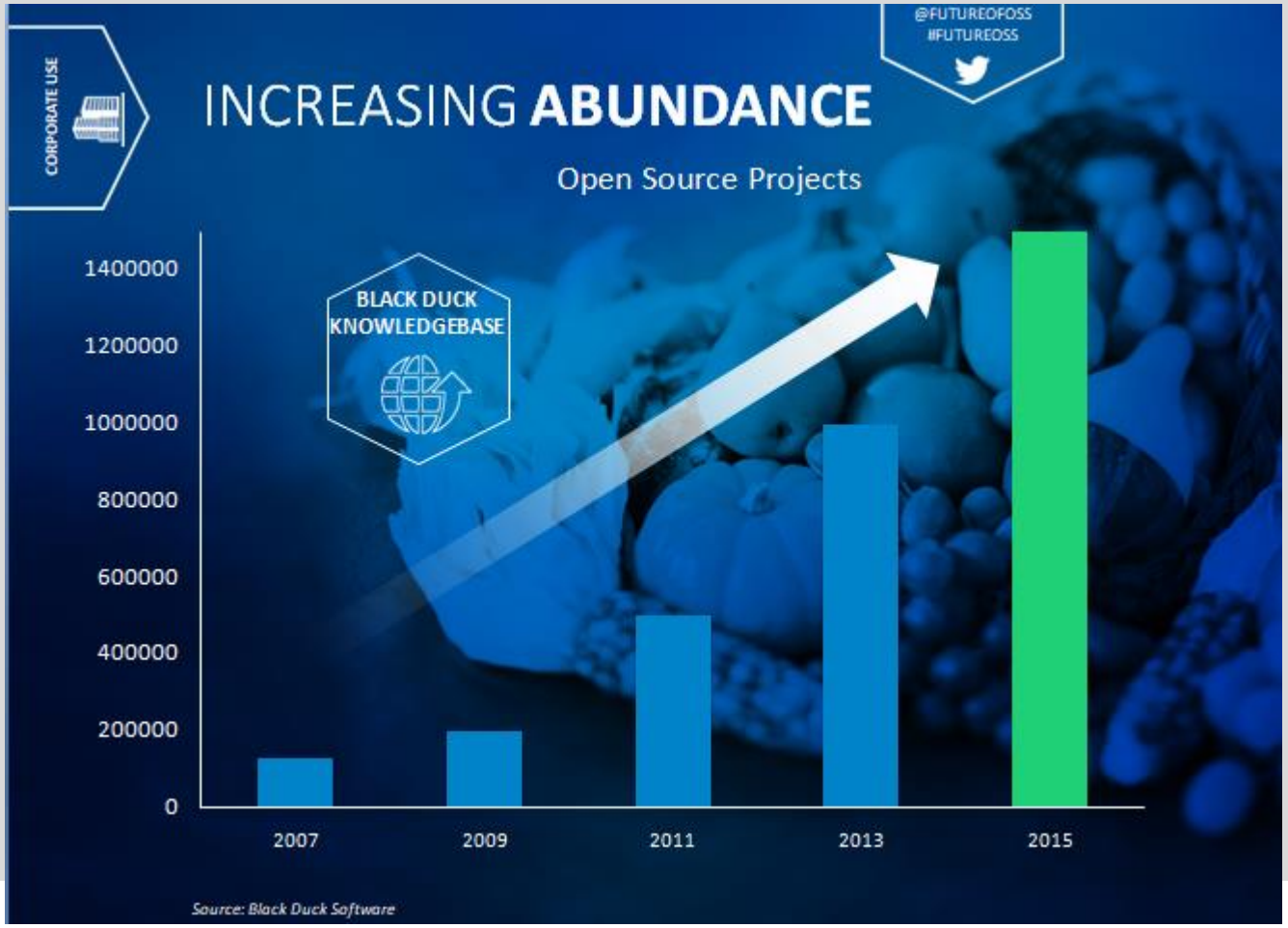
While rapid adoption of OSS demonstrably offers a range of advantages, the community development model presents developers, integrators and deployers with a set of accompanying challenges related to security, operational, and legal risk. Historically, foremost among these concerns stood license compliance and IP protection; however, with recent highly publicized threats to OSS, security has joined these concerns and today dominates the OSS adoption conversation.

This presentation will explore the role of and requirements for secure development of and deployment with OSS.

OPEN SOURCE IS UNSTOPPABLE

Usage became 2X

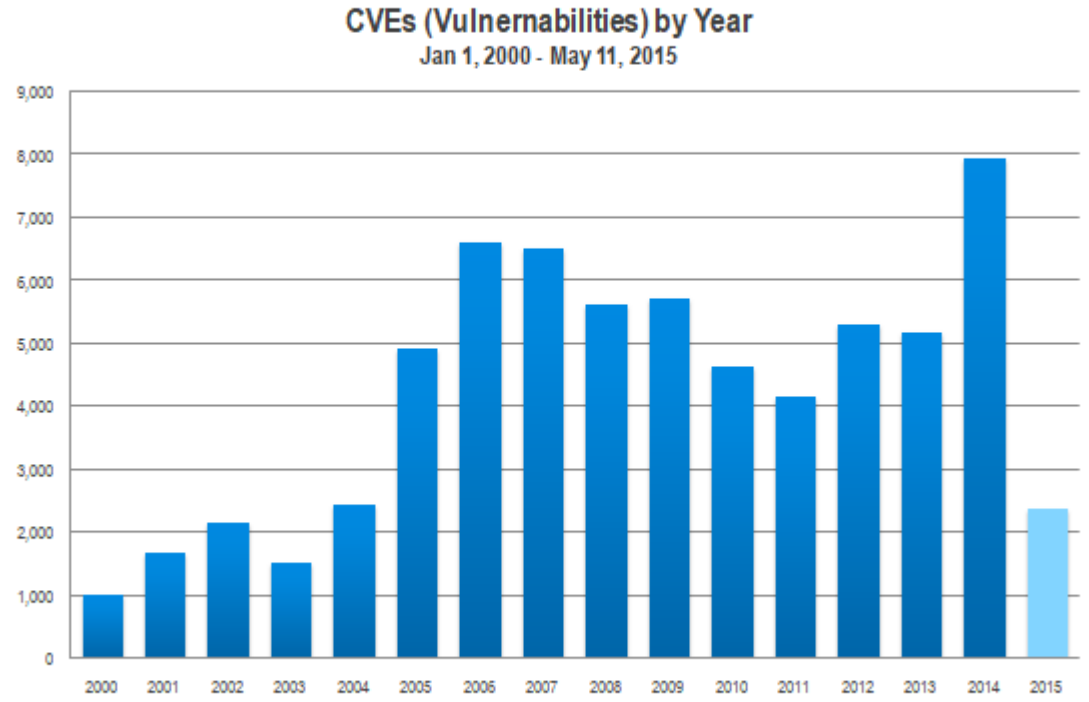
Per Blackduck Knowledge Base



TECHNOLOGY IMPACT

VULNARABILITY COUNT INCREASE

THE GROWTH IN SECURITY VULNERABILITIES



Based on the National Vulnerability Database published by the National Institute of Standards and Technology (a repository by the U.S. government)

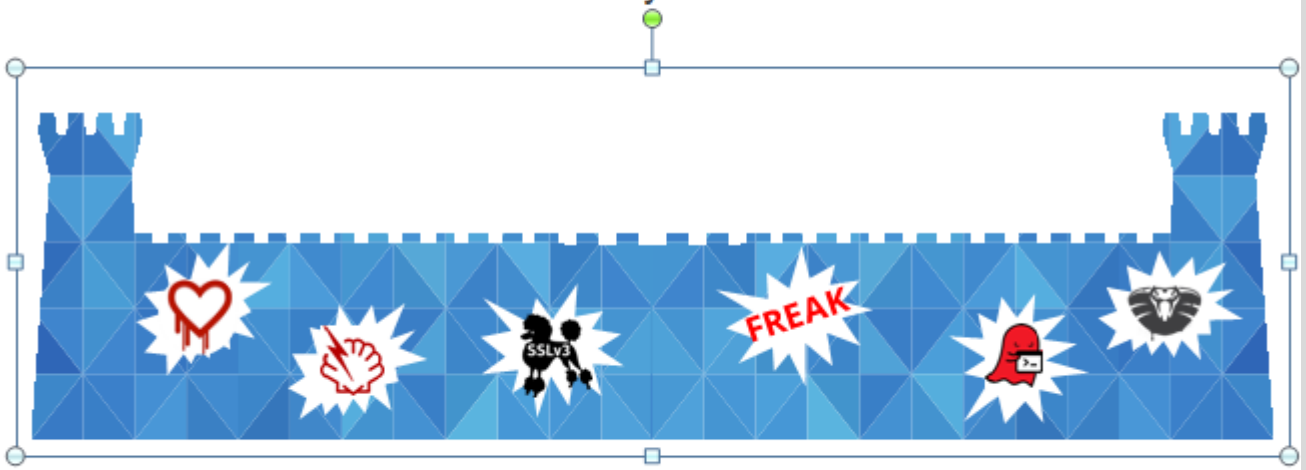
13

BLACKDUCK

NATIONAL VULNERABILITY DATABASE

Of 9,200 security vulnerabilities reported in 2014, 4,000 affected open source code.

– National Vulnerability Database & IBM X-Force



14

BLACKDUCK

CHAIN TRANSPARENCY AND REMEDIATION ACT ("THE ROYCE BILL")

3 Key Provisions:

- Vendors must provide a Bill of Materials of 3rd-Party and Open Source Components (including versions)
- Vendors cannot use known vulnerable components if there is a less vulnerable component available
- Software must be patchable/updateable (to address new vulnerabilities when they are discovered)

H. R. 5793

To ensure the integrity of any software, firmware, or product developed for or purchased by the United States Government that uses a third party or open source component, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

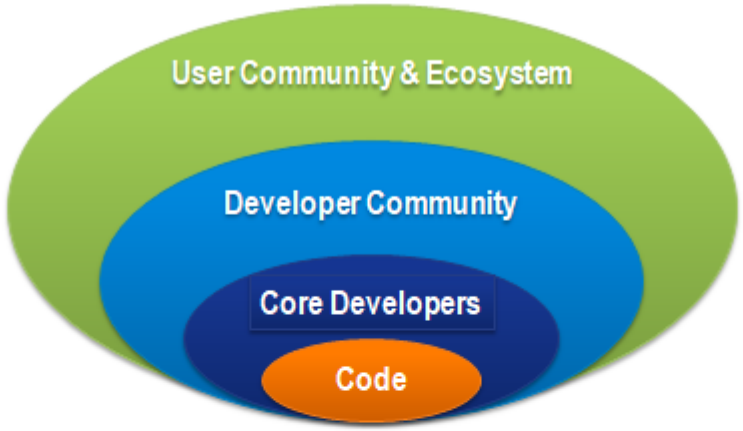
A BILL

To ensure the integrity of any software, firmware, or product developed for or purchased by the United States Government that uses a third party or open source component, and for other purposes.

16

BLACKDUCK

OPEN SOURCE DEVELOPMENT MODEL

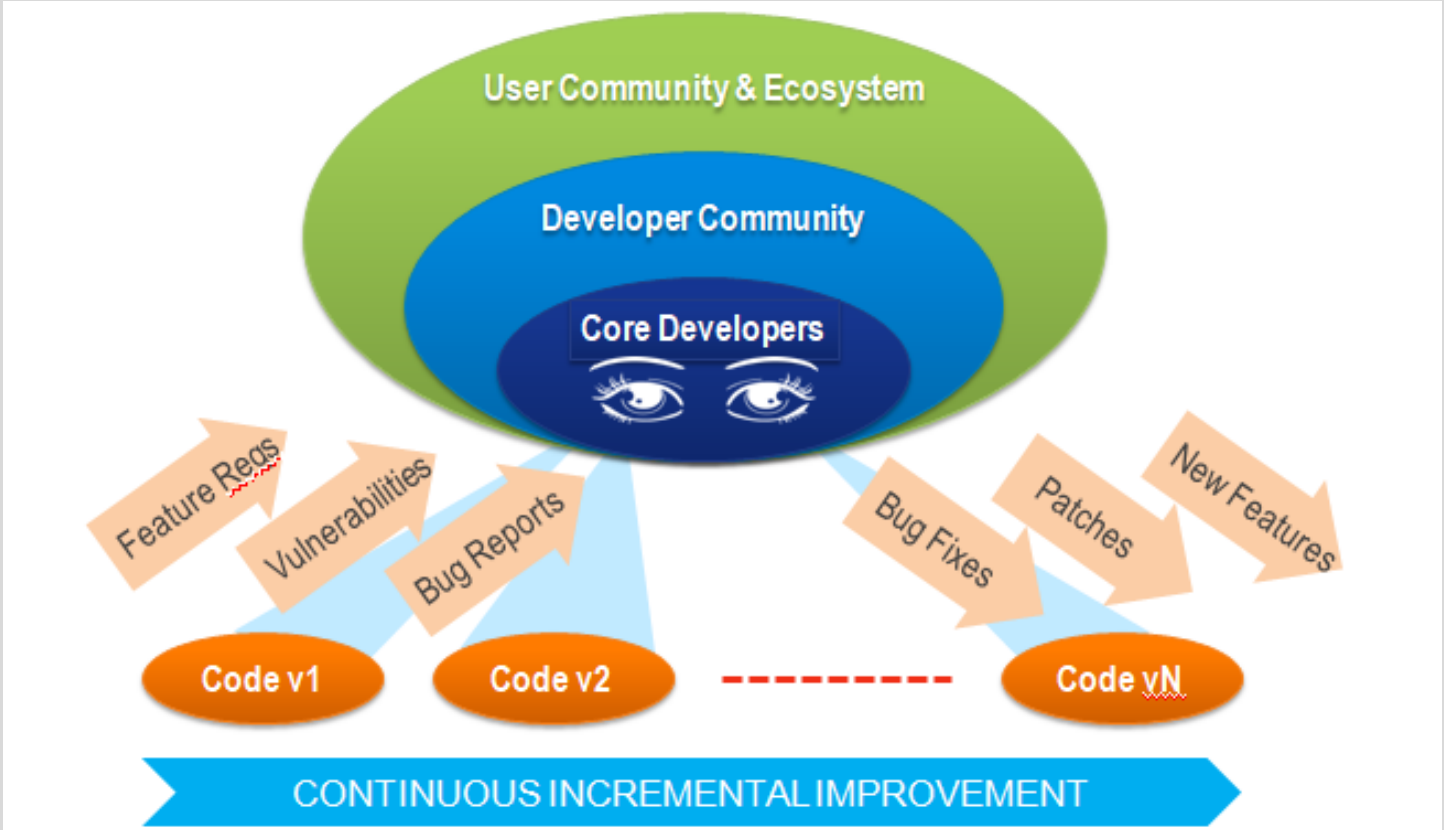


- Core project developers create, maintain, curate code base
- Vet contributions from larger communities
- Focus on project goals – features, performance, etc.

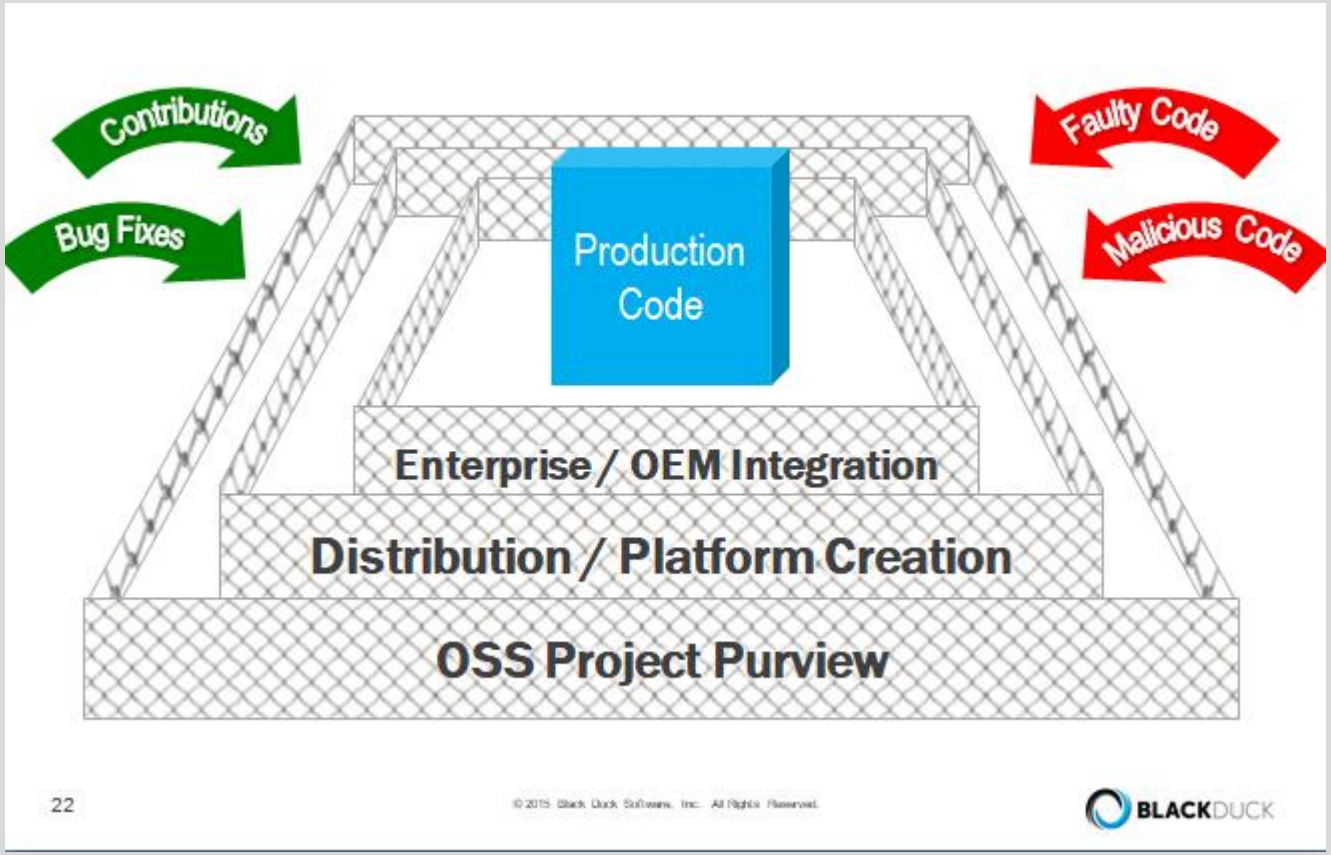
19

BLACKDUCK

OPEN SOURCE CODE CURATION MODEL



THEORETICAL "TRIPLE FENCE" OF OSS SECURITY



THREATS RESISTANT TO COMMUNITY OVERSIGHT

- Use-case specific errors
- Local misconfiguration
- LAN-based vulnerabilities
- Deployed deprecated s/w versions
- Weak encryption
- Bad authentication
- Stolen credentials
- Viruses, Trojans & other malware
- Denial of service attacks
- Weak passwords
- Unenforced security policy
- Phishing
- Man-in-the-middle attacks
- Forged certificates
- Spoofed MACs and IP addresses
- Latent zero-day exploits
- Brute force decryption

24

BLACKDUCK

COMPONENT-LEVEL BEST PRACTICES FOR SECURING OPEN SOURCE SOFTWARE

WHAT IS OPEN SOURCE HYGIENE

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.

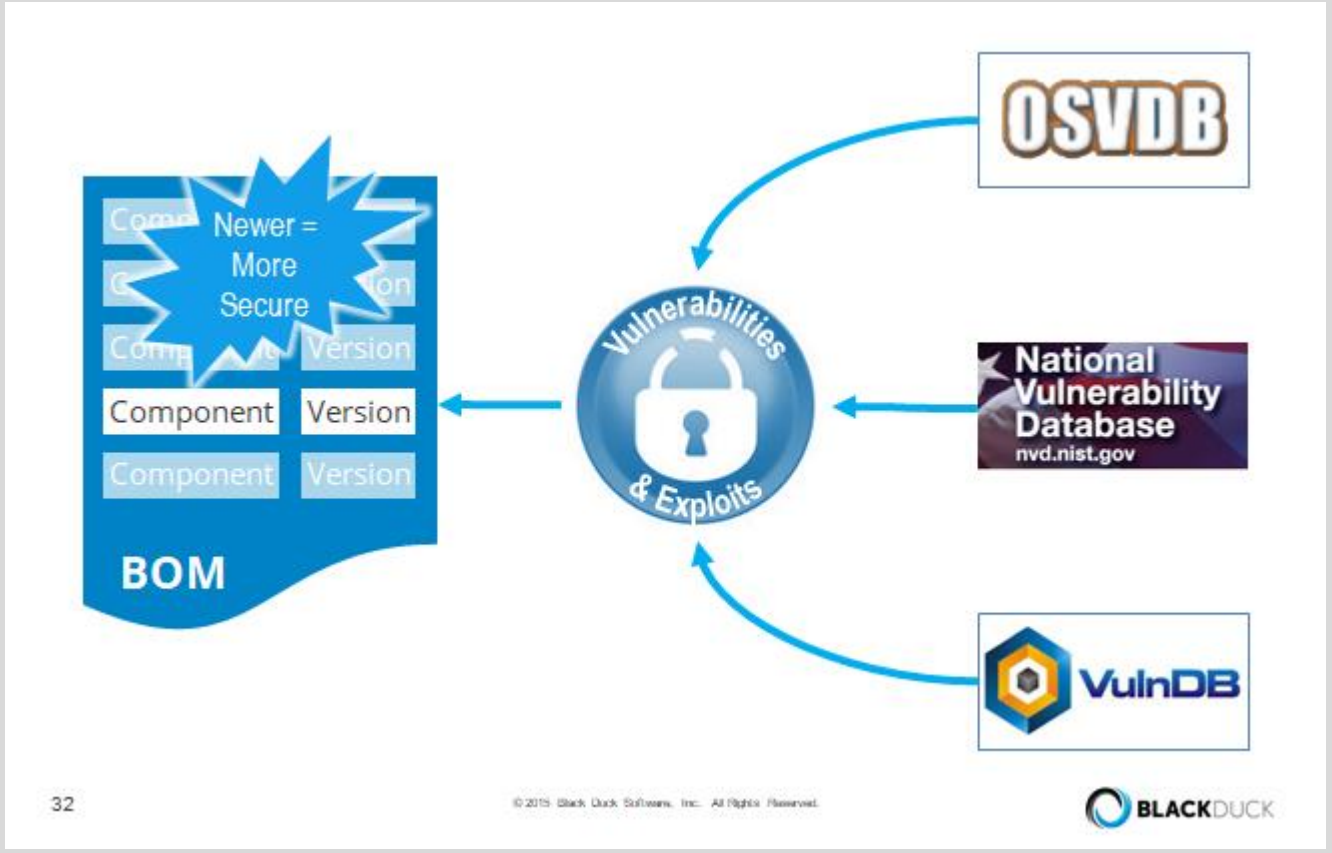
28

BLACKDUCK

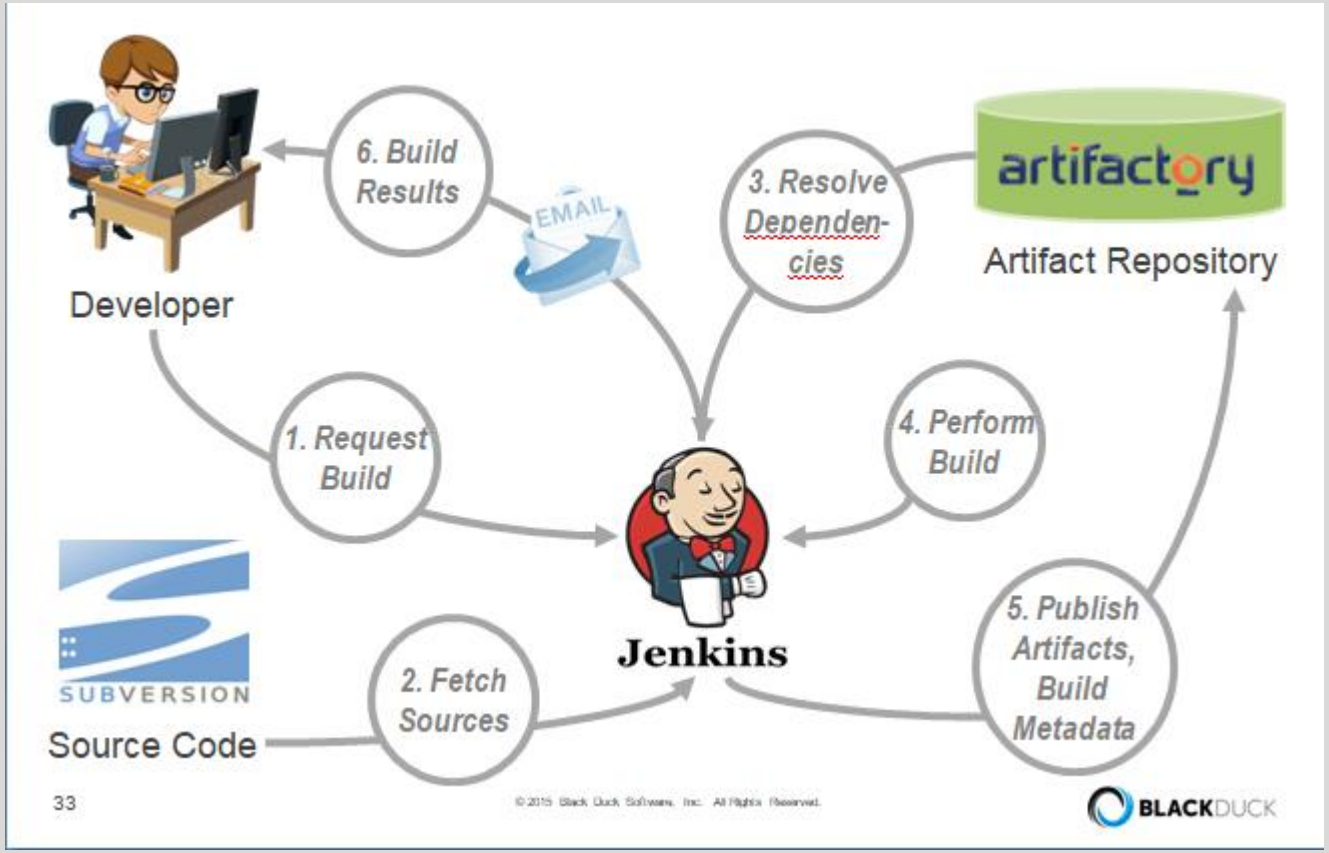
SECURITY TECHNOLOGIES – WHERE DOES OSS HYGIENE FIT?

Intrusion Detection	Authentication	Network Security	Encryption
End-point Security	Code Quality Tools	Patch/Update Management	Auditing & Logging
Hardware Mechanisms	Configuration Management	Policy Enforcement	Physical Security
Formal Verification	Certifiable Systems	Capabilities & Access Control	Binary Obfuscation

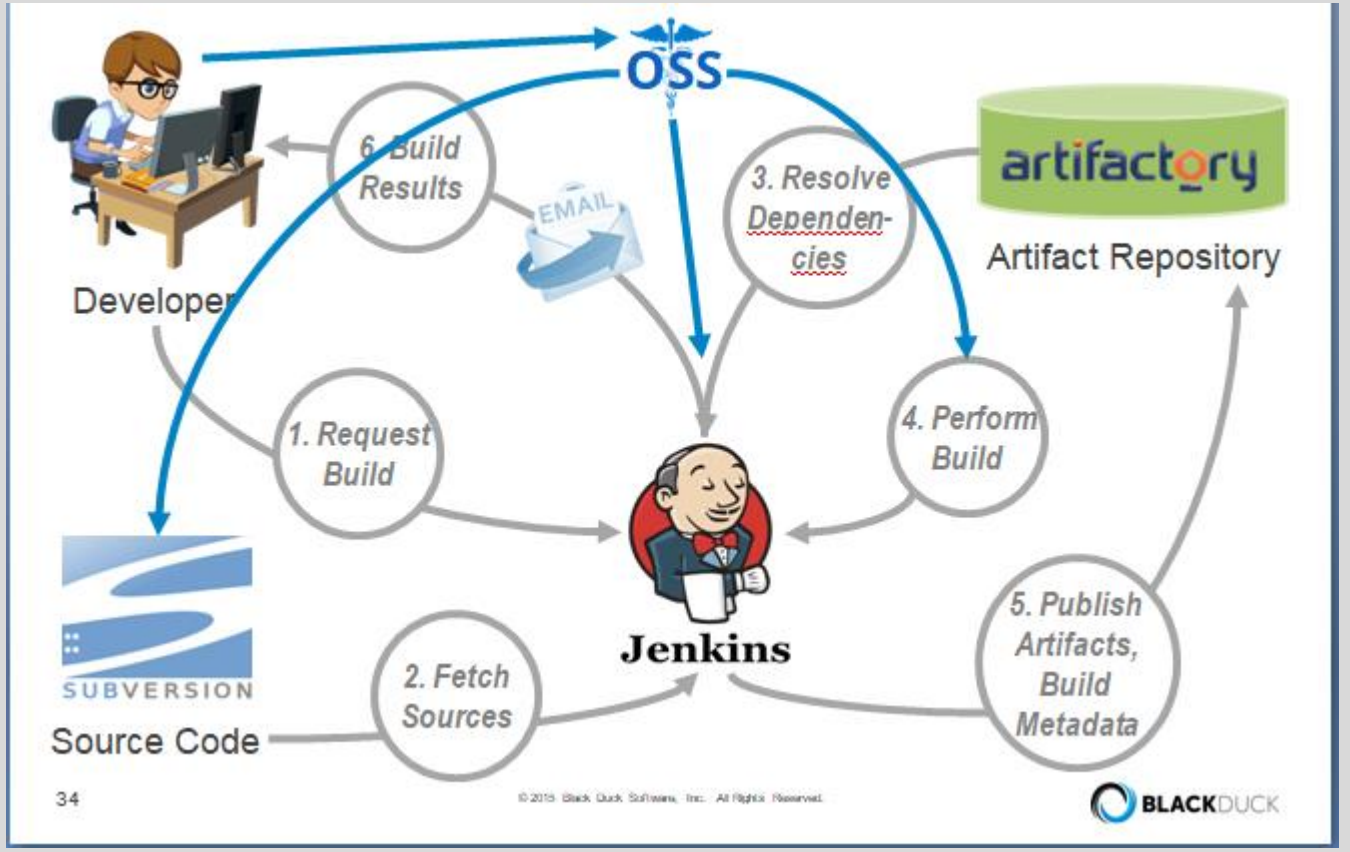
VERSIONS AND VULNERABILITIES



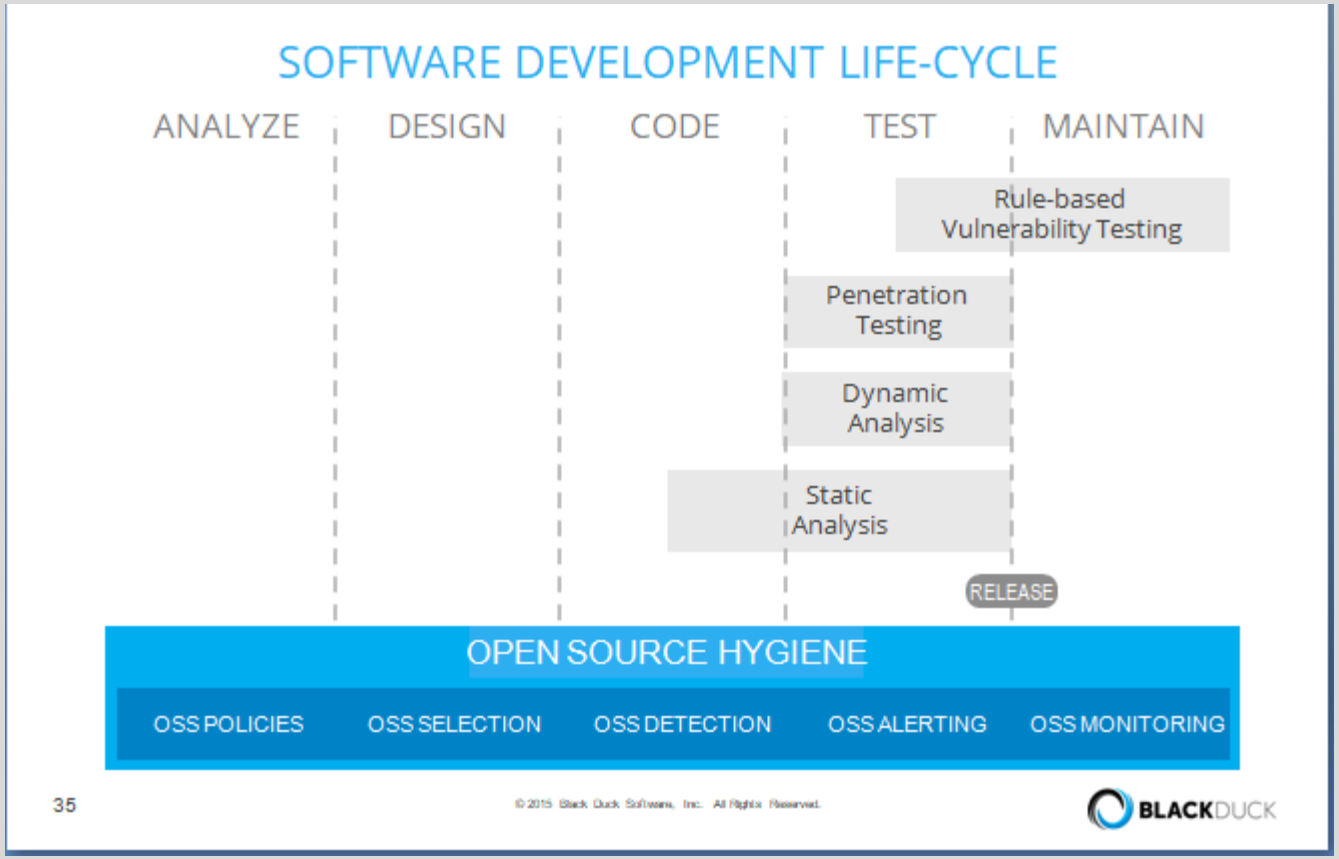
EXAMPLE ENTERPRISE SOFTWARE BUILD (CI) WORKFLOW



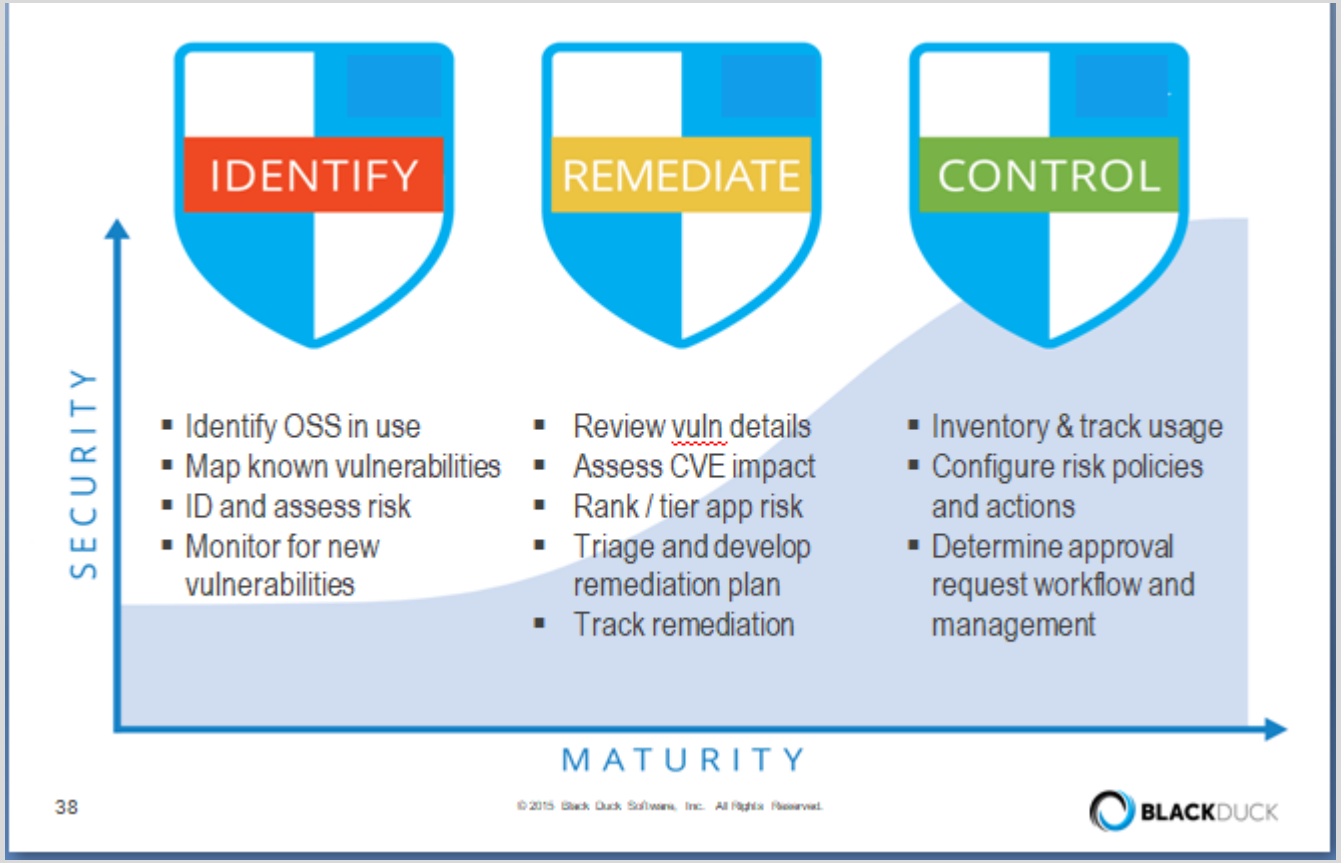
OSS KEY AREAS IN A CI



OSS HYGIENE COMPLEMENTS SECURITY TESTING



THE ROAD TO SECURE OSS USE – BEST PRACTICES



OSS REMEDIATION / TRIAGE CONSIDERATIONS

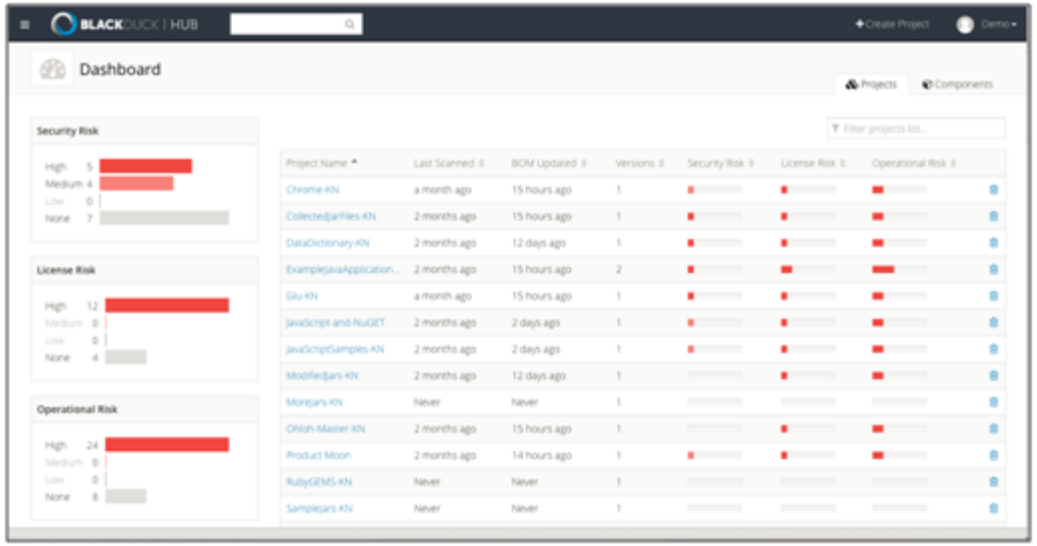
Comparable to other types of software

- Severity of vulnerability (CVSS and other rankings)
- Number of vulnerabilities / component
- Existence/availability of exploits (if known)
- Context of vulnerability (internet/customer facing vs. internal)
- Availability of patches or other remediation
- Existence of comparable functionality in alternate OSS tech
- Willingness / capability to patch / maintain OSS forks

39

BLACKDUCK

IDENTIFY VULNERABILITIES IN OSS SOFTWARE PORTFOLIOS



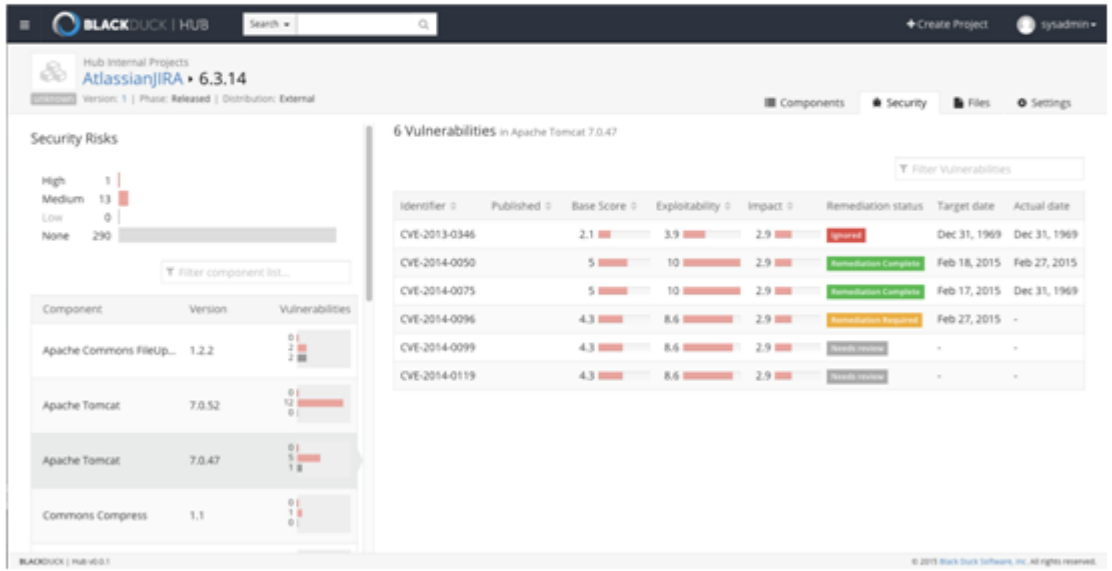
- Scan code to automatically identify open source in use
- Map known security vulnerabilities
- Assess licenses, versions, community activity (operational risk)
- Identify open source in use with potential high-risk

41

BLACKDUCK

REMEDIATION DASHBOARDS

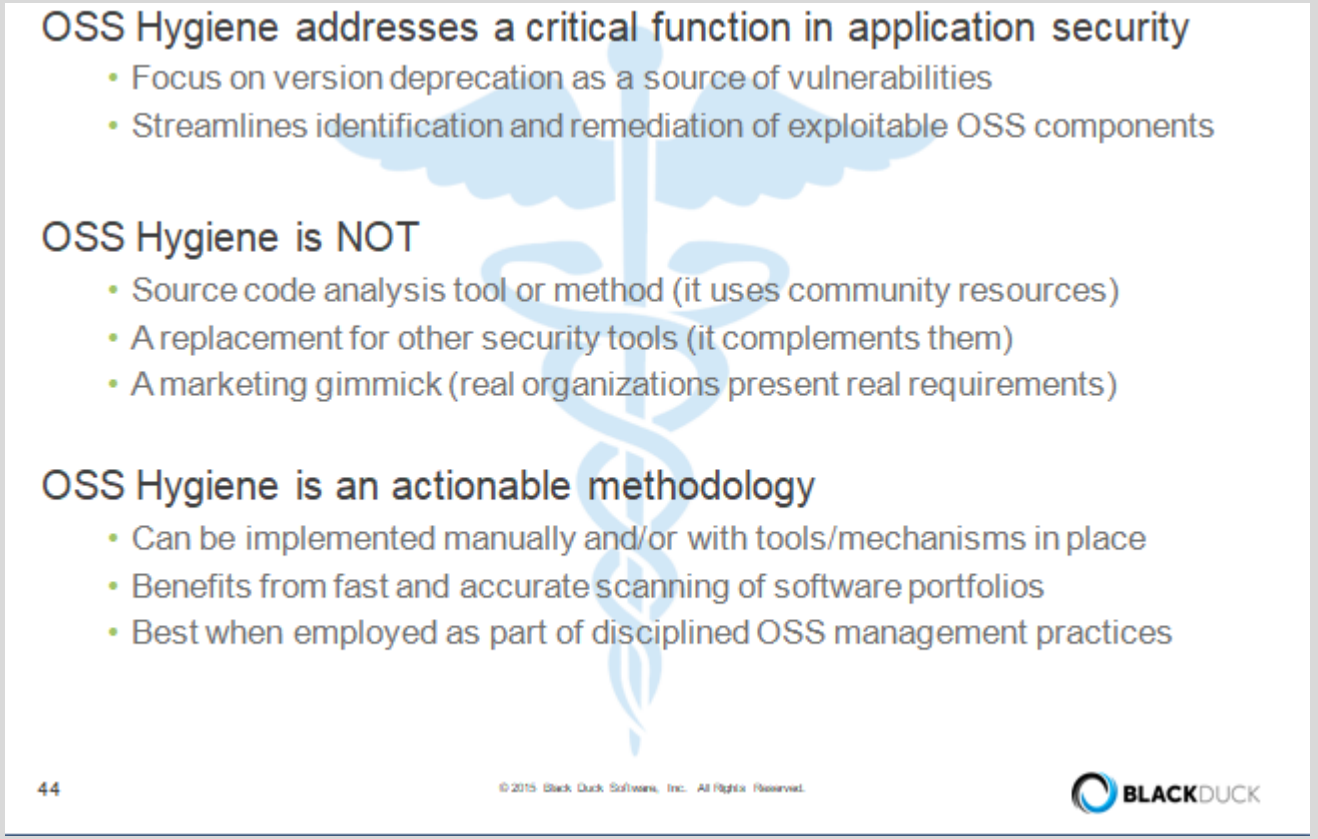
- Review CVSS and its impact on each project
- Assess, triage and prioritize vulnerabilities
- Schedule and track planned and actual remediation dates



42

BLACKDUCK

CONCLUSION


OSS Hygiene addresses a critical function in application security
• Focus on version deprecation as a source of vulnerabilities
• Streamlines identification and remediation of exploitable OSS components
OSS Hygiene is NOT
• Source code analysis tool or method (it uses community resources)
• A replacement for other security tools (it complements them)
• A marketing gimmick (real organizations present real requirements)
OSS Hygiene is an actionable methodology
• Can be implemented manually and/or with tools/mechanisms in place
• Benefits from fast and accurate scanning of software portfolios
• Best when employed as part of disciplined OSS management practices
44
BLACKDUCK

THANK YOU!

training@laksans.com