SECURITY IN THE AGE OF OPEN SOURCE

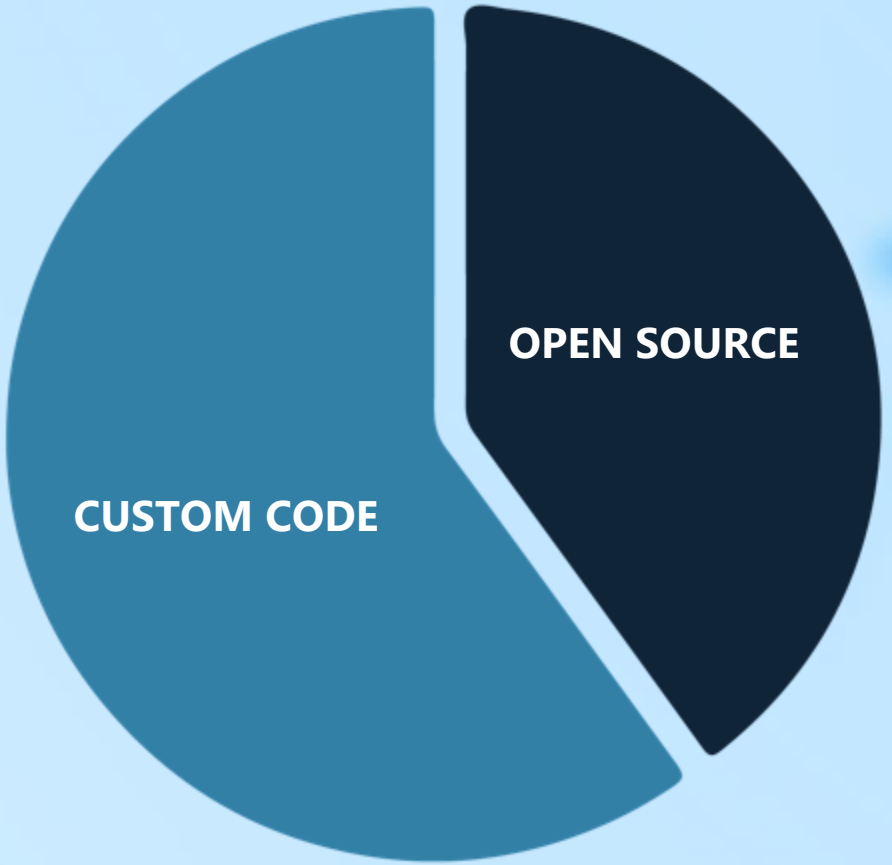
Mike Pittenger
VP, Security Strategy

BLACKDUCK

Applications Are Include Custom and 3rd Party Code

CUSTOM CODE

- Proprietary functionality
- Core enterprise IP
- Competitive differentiation

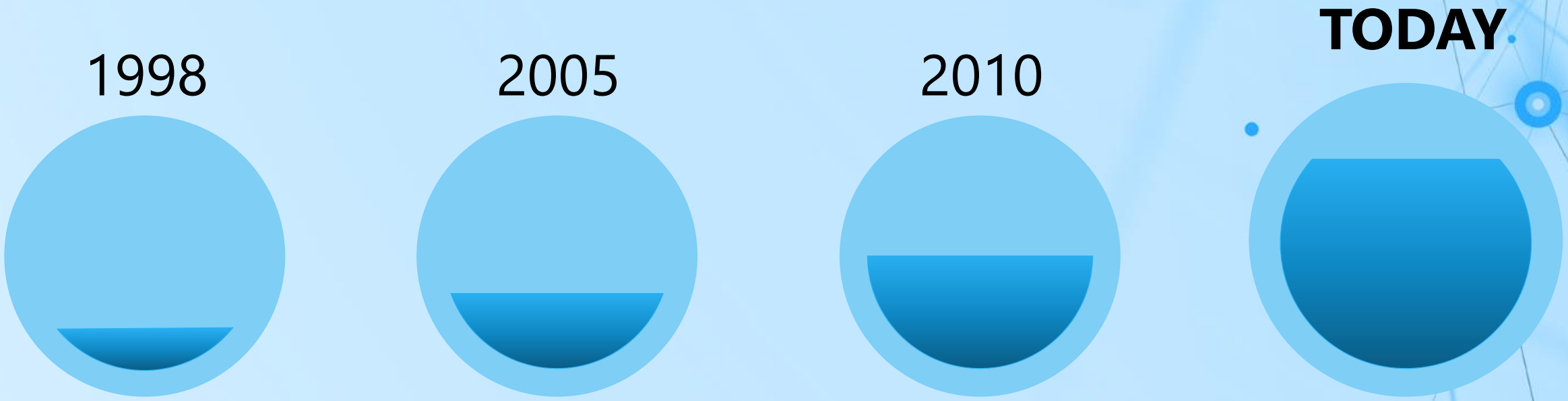


OPEN SOURCE

- Needed functionality without acquisition costs
- Faster time to market
- Lower development costs
- Broad support from communities

BLACKDUCK

Open Source Changed the Way Applications are Built



Custom & Commercial Code

Open Source Software

Open Source is the modern architecture

BLACKDUCK

Consequences Can Be Costly When You Can't Control What You Can't See

Heartbleed

OpenSSL
Introduction: 2011
Discovery: 2014

Shellshock

Bash
Introduction: 1989
Discovery: 2014

FREAK!

Freak

OpenSSL
Introduction: 1990's
Discovery: 2015

Ghost

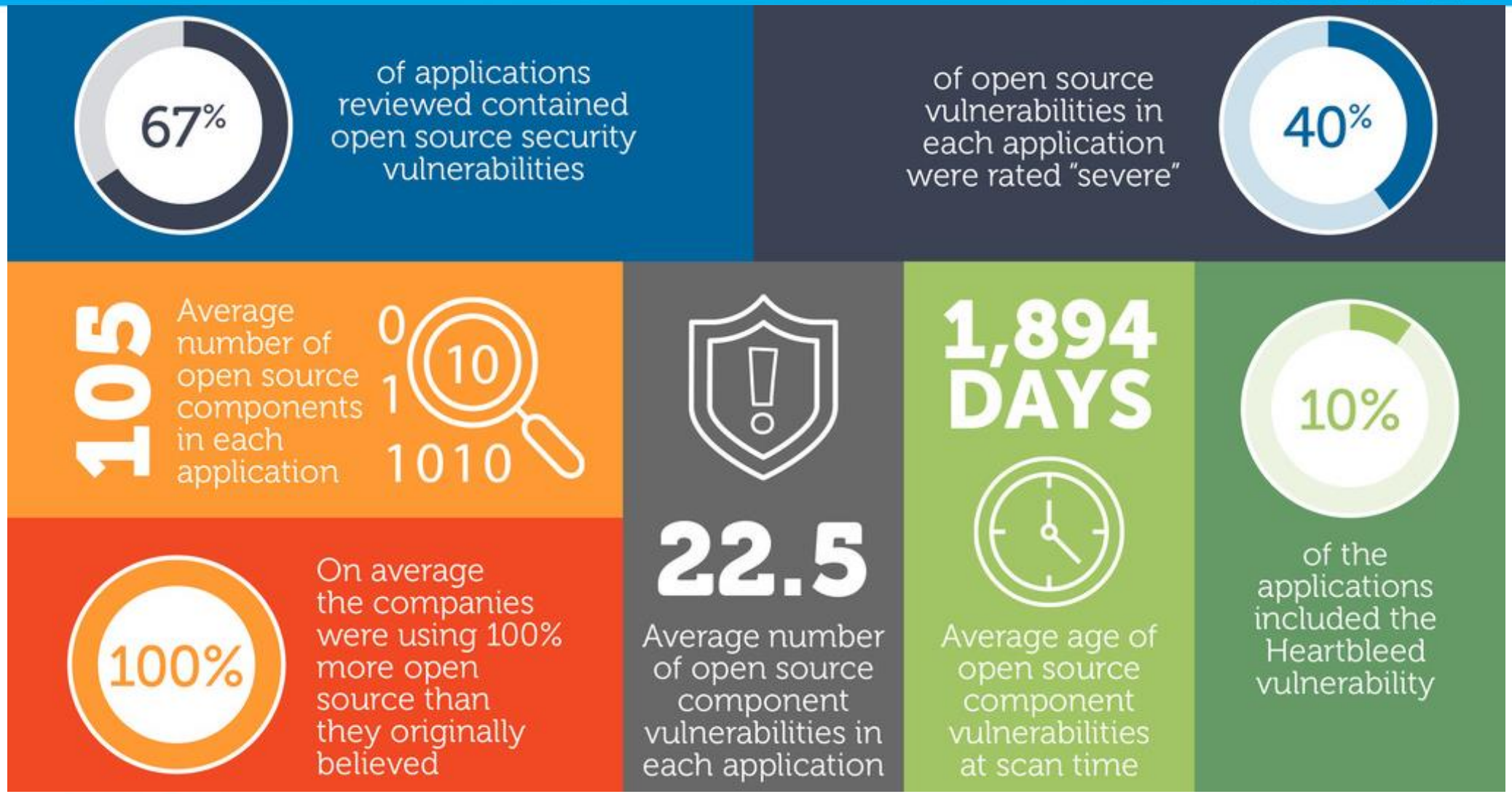
GNU C Library
Introduction: 2000
Discovery: 2015

Venom

QEMU
Introduction: 2004
Discovery: 2015

BLACKDUCK

Black Duck Open Source Security Audit Report Highlights Security & Management Challenges



BLACKDUCK

Why Aren't We Finding These in Testing?

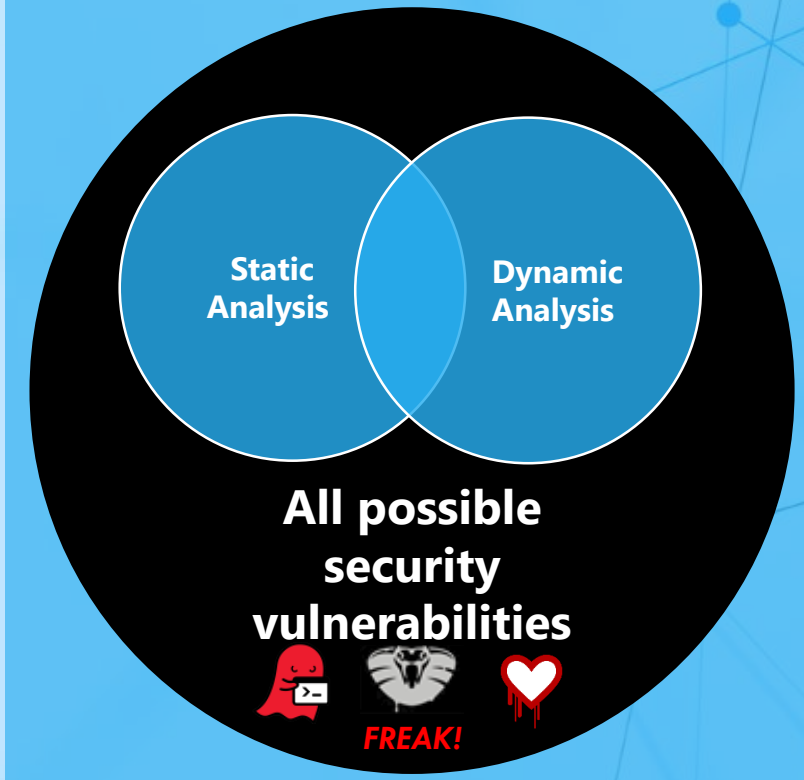
- Static analysis
  - Testing of source code or binaries for unknown security vulnerabilities in custom code
  - Advantages in buffer overflow, some types of SQL injection
  - Provides results in source code
- Dynamic analysis
  - Testing of compiled application in a staging environment to detect unknown security vulnerabilities in custom code
  - Advantages in injection errors, XSS
  - Provides results by URL, must be traced to source

- *What's Missing?*

BLACKDUCK

There Are No Silver Bullets

- 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



BLACKDUCK

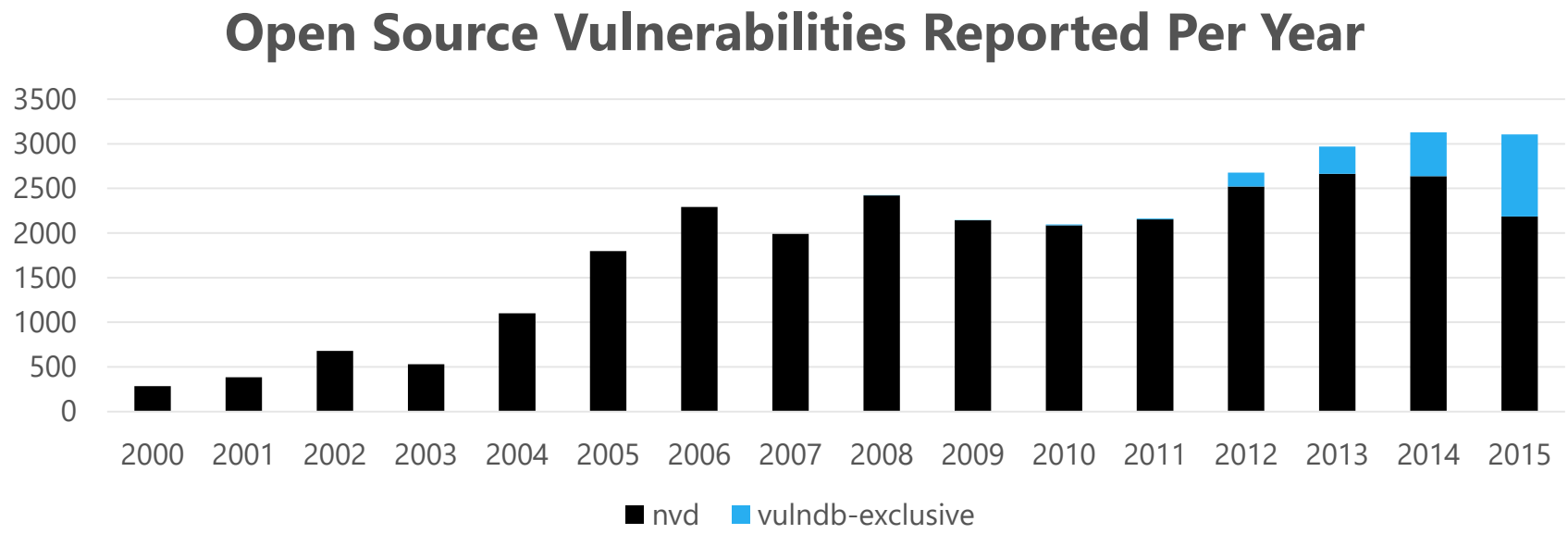
What Do Security Testing Tools Miss?

- Static Analysis Tools and Dynamic Analysis Tools can be ***very effective*** in finding bugs in the code written by internal developers.
- HOWEVER…
  - They are ***ineffective*** in finding known vulnerabilities in Open Source components
  - They provide a **point-in-time** snapshot of security

What happens when the threat landscape changes?

BLACKDUCK

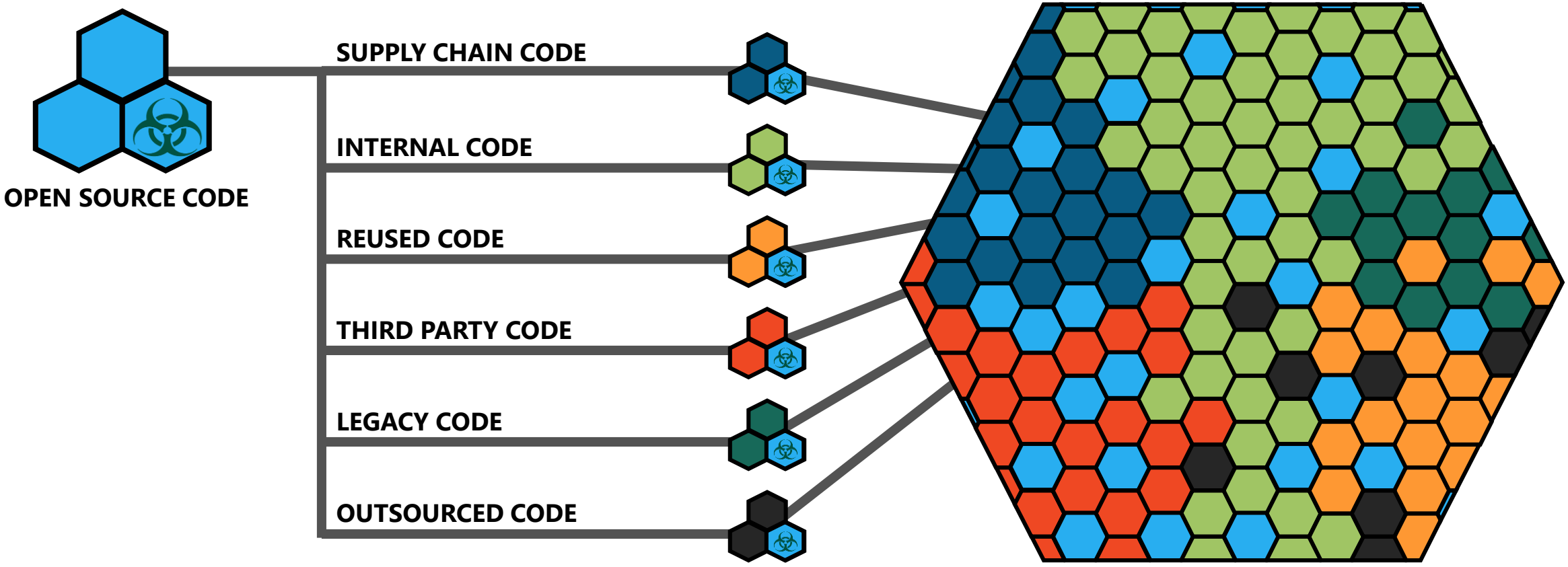
The Threat Landscape Constantly Changes



- VulnDB (Open Source Vulnerability Database)
  - In 2015, over 3,000 new vulnerabilities in open source
- Since 2004, over 74,000 vulnerabilities have been disclosed by NVD.
  - 63 reference automated tools
  - 50 of those are for vulnerabilities reported in the tools
  - 13 are for vulnerabilities that could be identified by a fuzzer

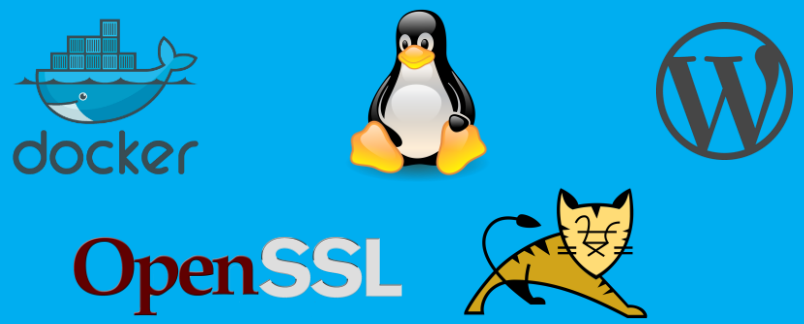
BLACKDUCK

We Have Little Control Over How Open Source Enters The Code Base



BLACKDUCK

Open Source is an Attractive Target



OPEN SOURCE IS USED EVERYWHERE

STEPS TO EXPLOIT READILY AVAILABLE

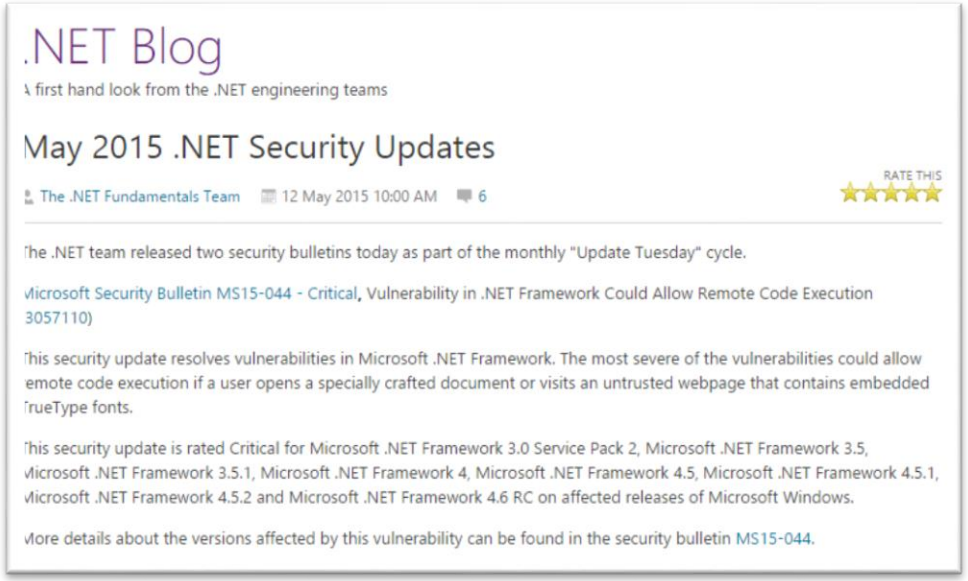
EASY ACCESS TO SOURCE CODE

VULNERABILITIES ARE PUBLICIZED

BLACKDUCK

Who's Responsible For Security?

Commercial Code



.NET Blog

A first hand look from the .NET engineering teams

May 2015 .NET Security Updates

The .NET Fundamentals Team | 12 May 2015 10:00 AM | 6

RATE THIS

The .NET team released two security bulletins today as part of the monthly "Update Tuesday" cycle.

Microsoft Security Bulletin MS15-044 - Critical, Vulnerability in .NET Framework Could Allow Remote Code Execution (3057110)

This security update resolves vulnerabilities in Microsoft .NET Framework. The most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted document or visits an untrusted webpage that contains embedded TrueType fonts.

This security update is rated Critical for Microsoft .NET Framework 3.0 Service Pack 2, Microsoft .NET Framework 3.5, Microsoft .NET Framework 3.5.1, Microsoft .NET Framework 4, Microsoft .NET Framework 4.5, Microsoft .NET Framework 4.5.1, Microsoft .NET Framework 4.5.2 and Microsoft .NET Framework 4.6 RC on affected releases of Microsoft Windows.

More details about the versions affected by this vulnerability can be found in the security bulletin MS15-044.

- Dedicated security researchers
- Alerting and notification infrastructure
- Regular patch updates
- **Dedicated support team with SLA**

Open Source Code

[MediaWiki-announce] MediaWiki Security and Maintenance Releases: 1.25.2, 1.24.3, 1.23.10

Chad innocentkiller at gmail.com
Mon Aug 10 21:54:44 UTC 2015

- **Messages sorted by:** [date] [thread] [subject] [author]

would like to announce the release of MediaWiki 1.25.2, 1.24.3, and
.23.10.
These releases fix three security issues in core, in addition to other bug
fixes. Several extensions have also had security issues fixed. Download
links
are given at the end of this email

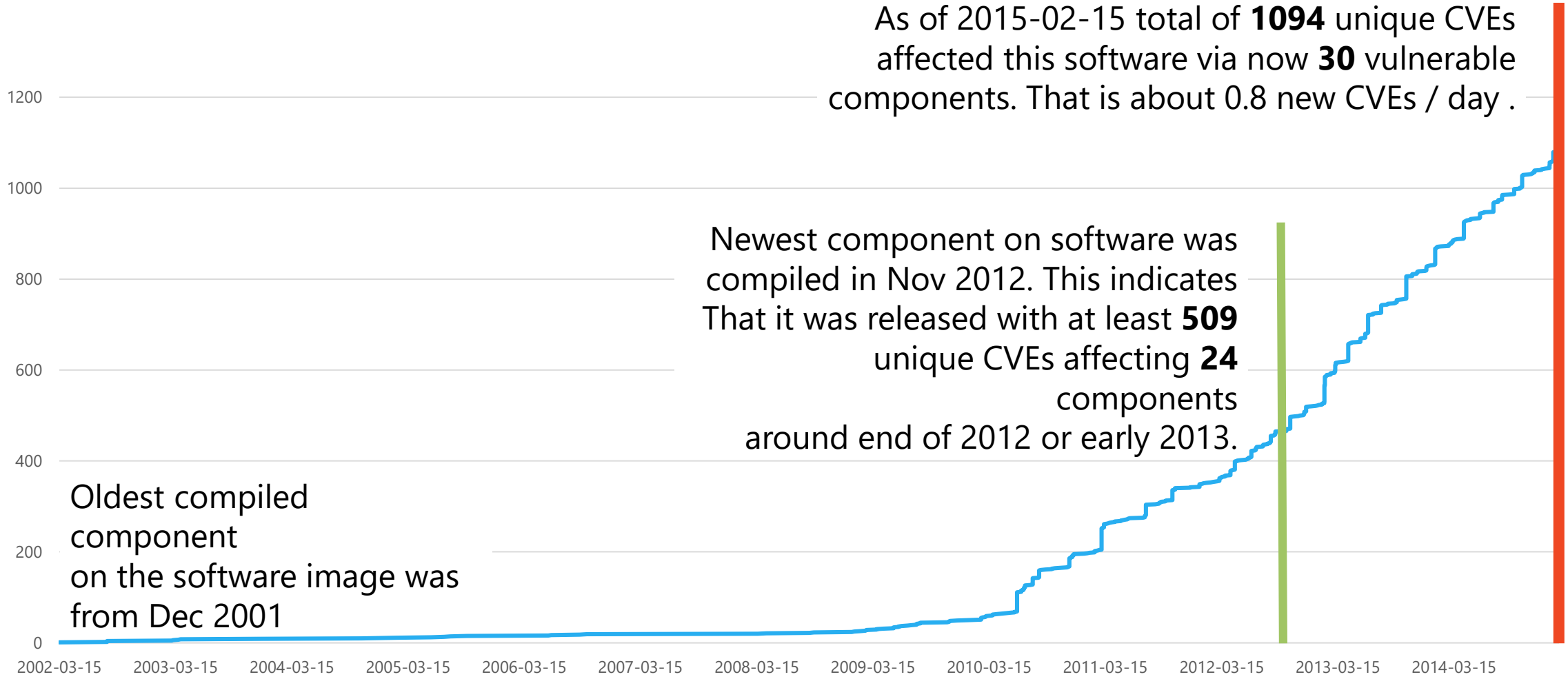
== Security fixes ==

* Internal review discovered that Special:DeletedContributions did not
properly
protect the IP of autoblocked users. This fix makes the functionality of
Special:DeletedContributions consistent with Special:Contributions and
Special:BlockList.
<https://phabricator.wikimedia.org/T106893>

- "community"-based code analysis
- Monitor newsfeeds yourself
- No standard patching mechanism
- **Ultimately, you are responsible**

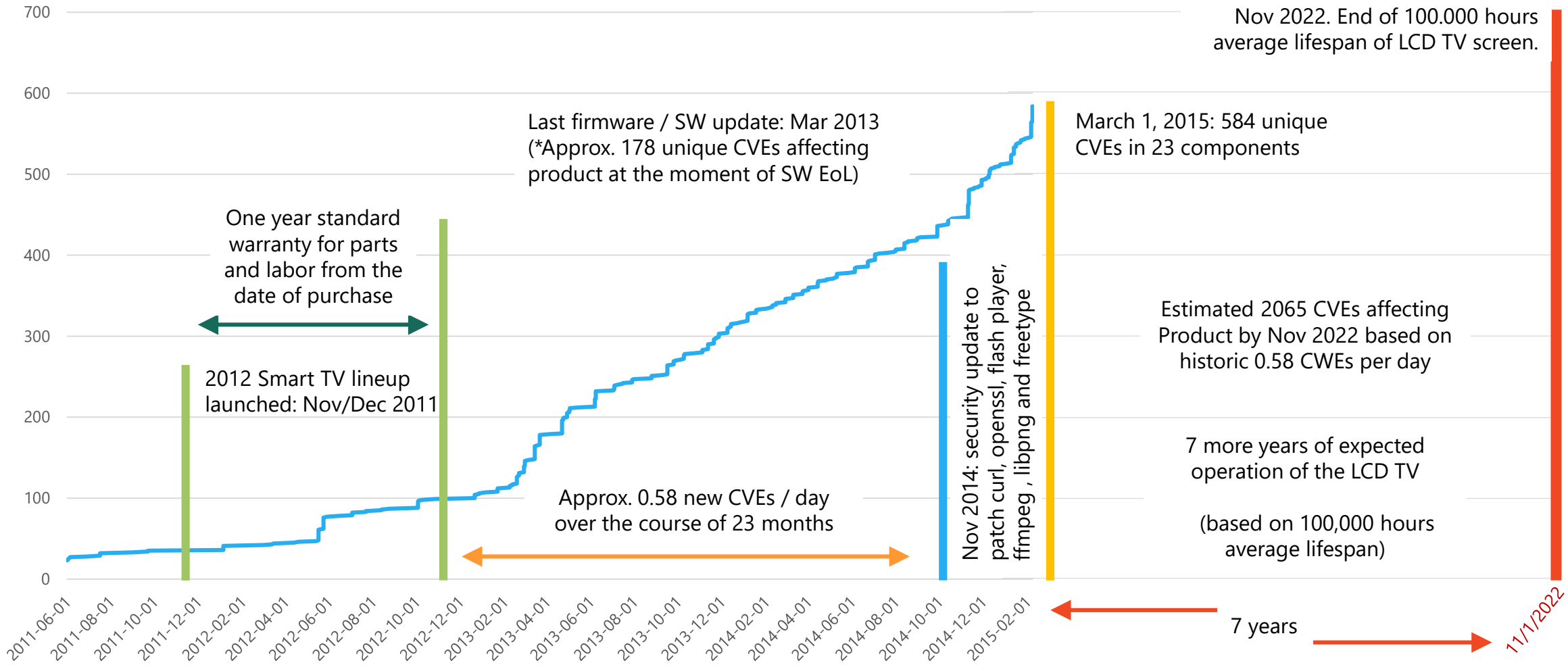
BLACKDUCK

Hospital Monitoring System



BLACKDUCK

Smart TV Set



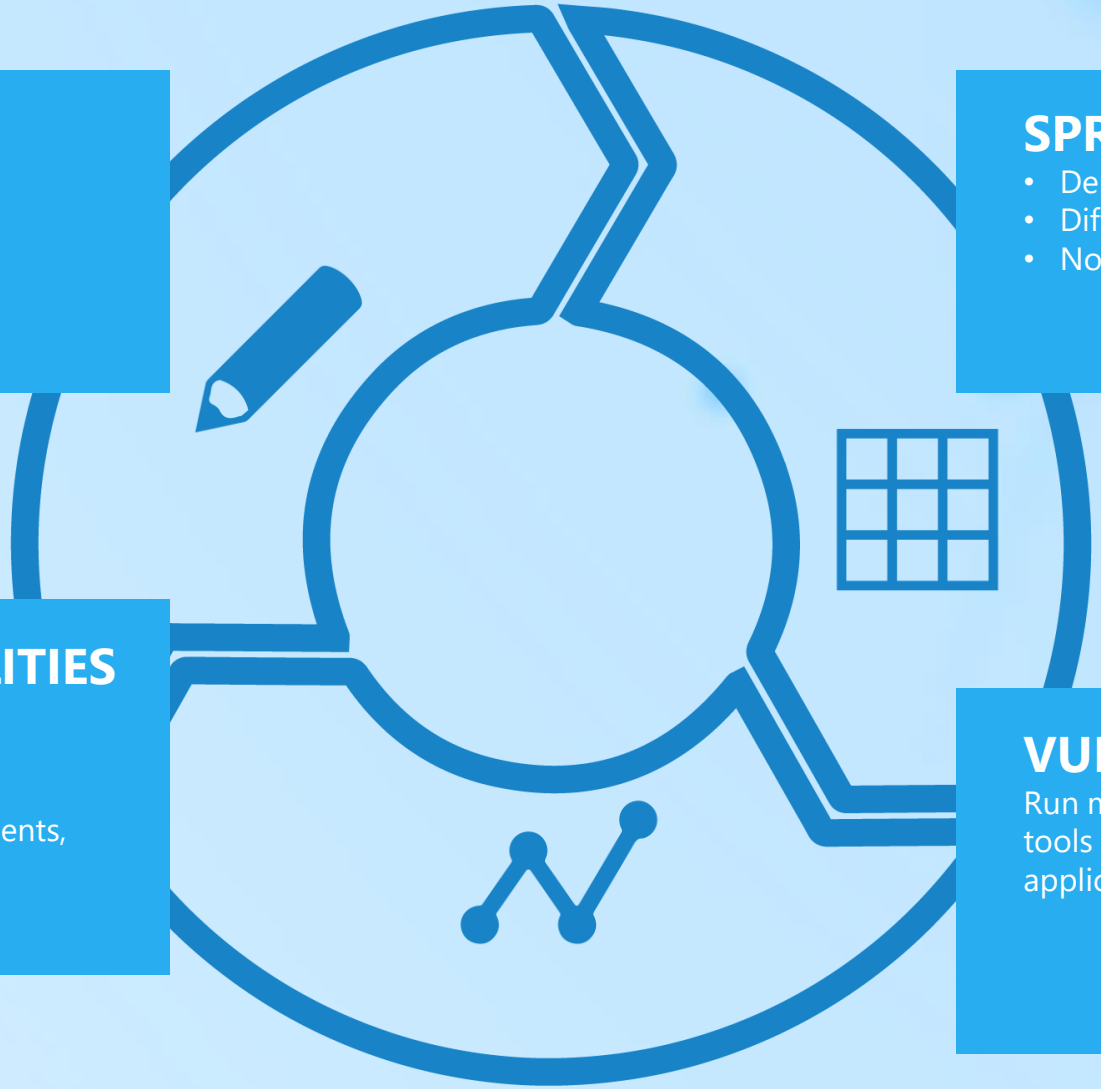
BLACKDUCK

(* date may not be fully accurate, as e.g. partial OTA updates may have been delivered after this date as well (see sec. update on Nov 2014)

How are Companies Managing Open Source Today? Not Well.

MANUAL TABULATION
- Architectural Review Board
- Occurs at end of SDLC
- High effort and low accuracy
- No controls

SPREADSHEET INVENTORY
- Depends on developer best effort or memory
- Difficult maintenance
- Not source of truth



TRACKING VULNERABILITIES
- No single responsible entity
- Manual effort and labor intensive
- Unmanageable (11/day)
- Match applications, versions, components, vulnerabilities

VULNERABILITY DETECTION
Run monthly/quarterly vulnerability assessment tools (e.g., Nessus, Nexpose) against all applications to identify exploitable instances

BLACKDUCK

Automating Five Critical Tasks and Having a Bill of Materials Provide Distinct Advantage

Visibility *AND* Control

INVENTORY
Open Source Software

1

MAP
Known Security Vulnerabilities

2

IDENTIFTY
License Compliance Risks

3

TRACK
Remediation Priorities & Progress

4

ALERT
New Vulnerabilities Affecting You

5

BLACKDUCK

Best Practices For Open Source

- Build and *automatically enforce* OSS policies
- Identify OSS components early in the SDLC
- Automatically create and maintain bills of material
- Continuously monitor threat environment for new vulnerabilities

Reqs	Design	Code	Test	Release
• **OSS Policies** • Application Criticality Ranking • OSS Risk Parameters • License Risk • Security Risk • Operational Risk	• **OSS Selection** • Design Review • License Risk • Security Risk • Operational Risk	• **OSS Detection** • Automatically detect and alert on non-conforming components • Correlation with Bills of Material	• **OSS Enforcement** • Detect and alert on non-conforming components • Correlation with Bills of Material	• **OSS Monitoring** • Timely OSS Vulnerability Identification & Reporting • Bug Severity • Remediation Advice

BLACKDUCK

Key Takeaways

- Open source is here to stay (and growing)
  - Open source saves development costs and accelerates time to market
- Open Source Security isn't covered by traditional tools
  - Static analysis is good, but doesn't help with open source vulnerabilities
  - Identify open source with known vulnerabilities, early in the SDL
- New paradigm requires new methodologies
  - Visibility to open source and continuous monitoring is required.

BLACKDUCK

What Can You Do Tomorrow?

Speak with your head of application development and find out:

- What policies exist?
- Is there a list of components?
- 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?

About Black Duck

24
Countries

250+
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"

"Top Place to Work," The Boston Globe

SBANE
Award for Innovation

BLACKDUCK

BLACKDUCK