



BLACKDUCK

Black Duck Hub

Presentation and Demonstration

Peter Andersson Solution Architect Nordics

pandersson@blackducksoftware.com

Primary OSS License Categories

- Permissive Licenses

- Licensee can use, copy, modify and distribute the software.
- Licensee is allowed to combine the source with open source or proprietary software.
- Licensee is NOT obligated to distribute the source code of derivative works.

• BSD

• MIT

- Copyleft Licenses

- Any Licensee modifications to the software (derivative works) must be **distributed** under the same reciprocal license.
- Copyleft licenses are substantially more complex than permissive licenses.

• GPL

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



Heartbleed

OpenSSL
Introduction: 2011
Discovery: 2014



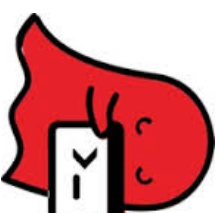
Shellshock

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

Discovering vulnerabilities is time critical



OPENSSL RELEASE DATES AND VULNERABILITIES:

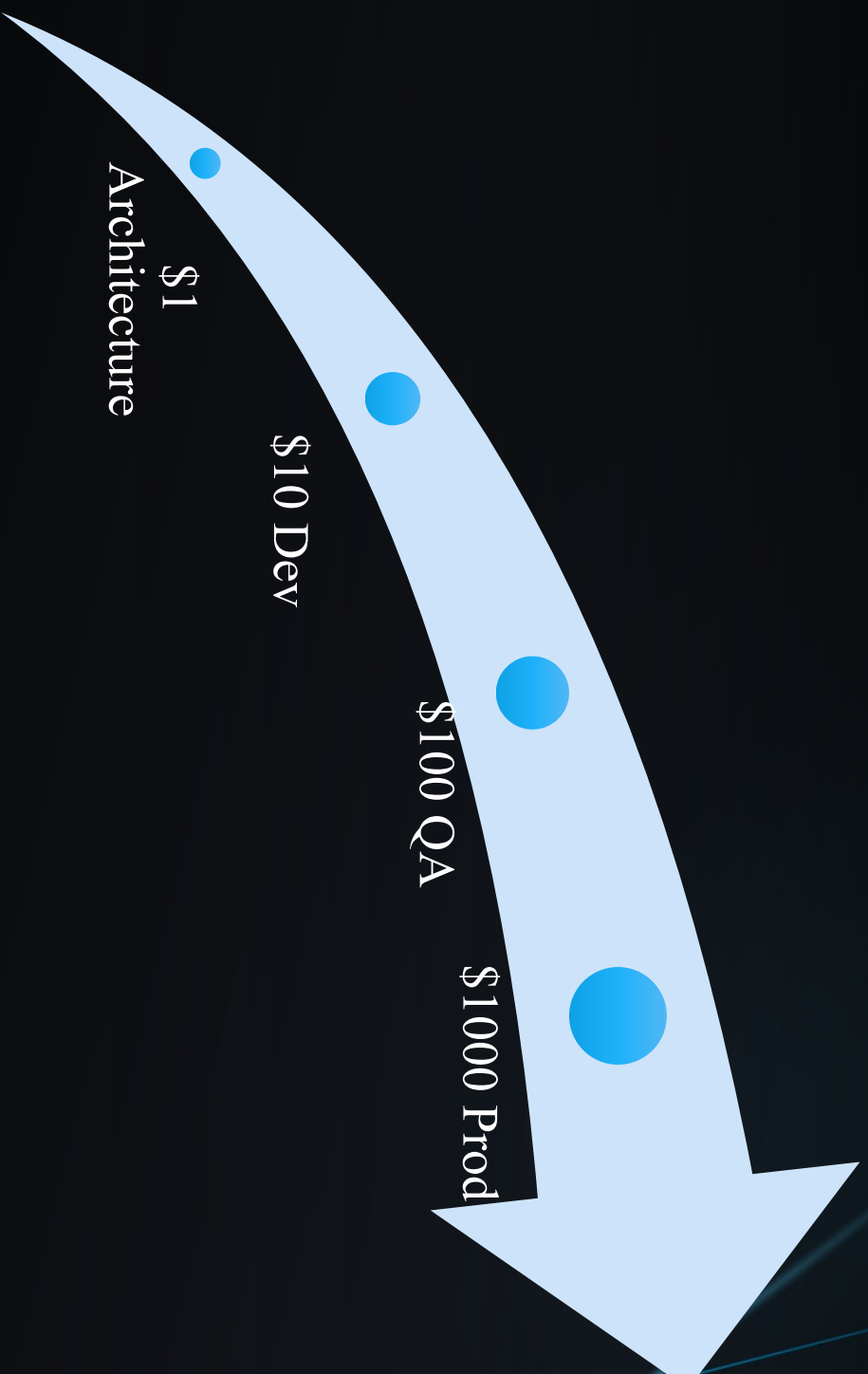
Version	Date	# Vulns Fixed
1.0.1s	1 Mar 2016	6
1.0.1r	28 Jan 2016	1
1.0.1q	3 Dec 2015	2
1.0.1p	9 Jul 2015	2
1.0.1o	12 Jun 2015	
1.0.1n	11 Jun 2015	
1.0.1m	10 Jun 2015	6
1.0.1l	24 Apr 2015	0
1.0.1k	8 Jan 2015	8
1.0.1j	15 Oct 2014	4
1.0.1i	6 Aug 2014	9
1.0.1h	5 Jun 2014	6
1.0.1g	7 Apr 2014	2 HEARTBLED!
1.0.1f	6 Jan 2014	3
1.0.1e	11 Feb 2013	1
1.0.1d	5 Feb 2013	3
1.0.1c	10 May 2012	1
1.0.1b	26 Apr 2012	0
1.0.1a	19 Apr 2012	1

49 NEW OPENSSL VULNERABILITIES SINCE HEARTBLED

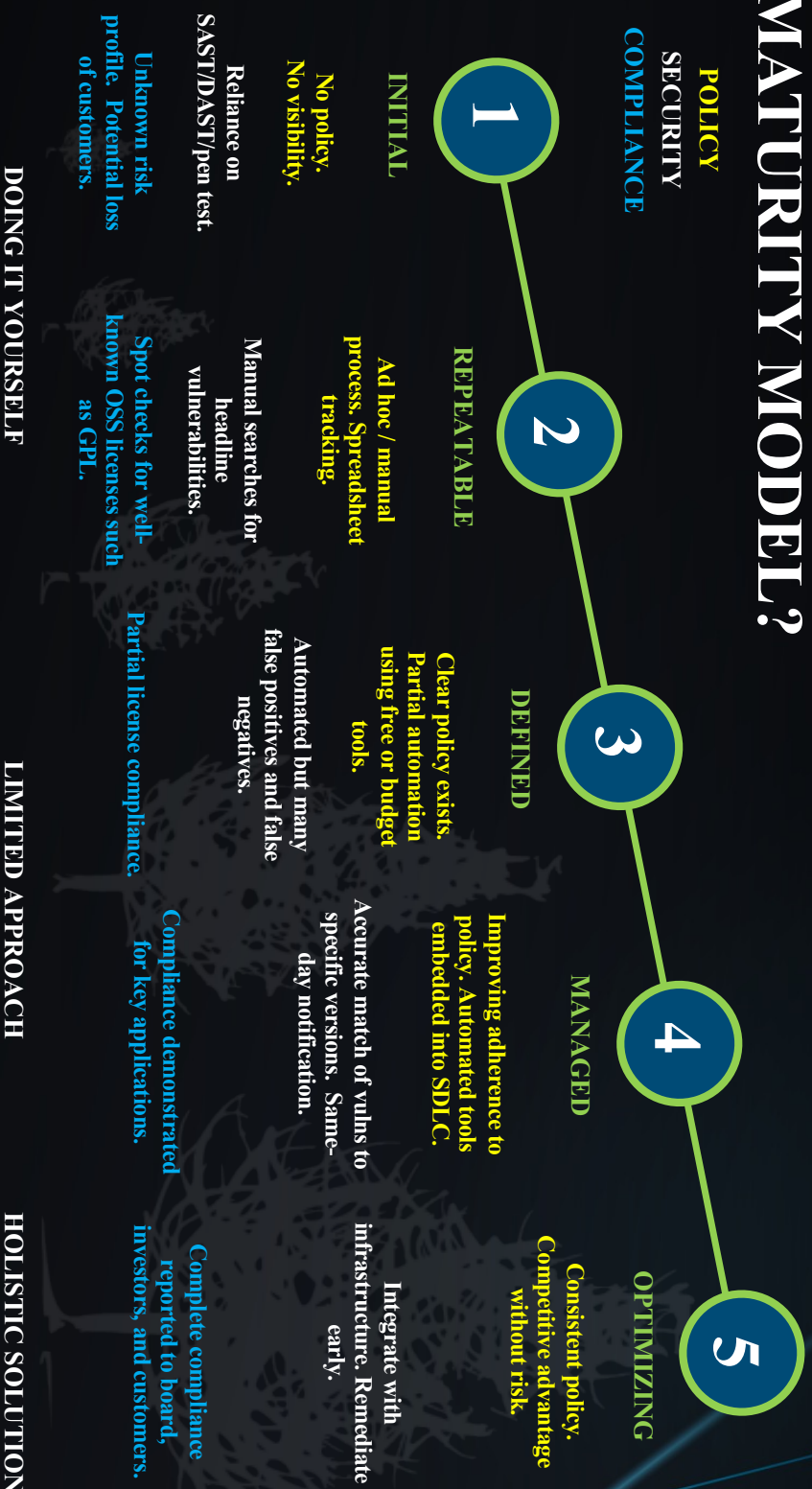


CONTINUOUS MONITORING OF NEW VULNERABILITIES IN YOUR APPLICATIONS

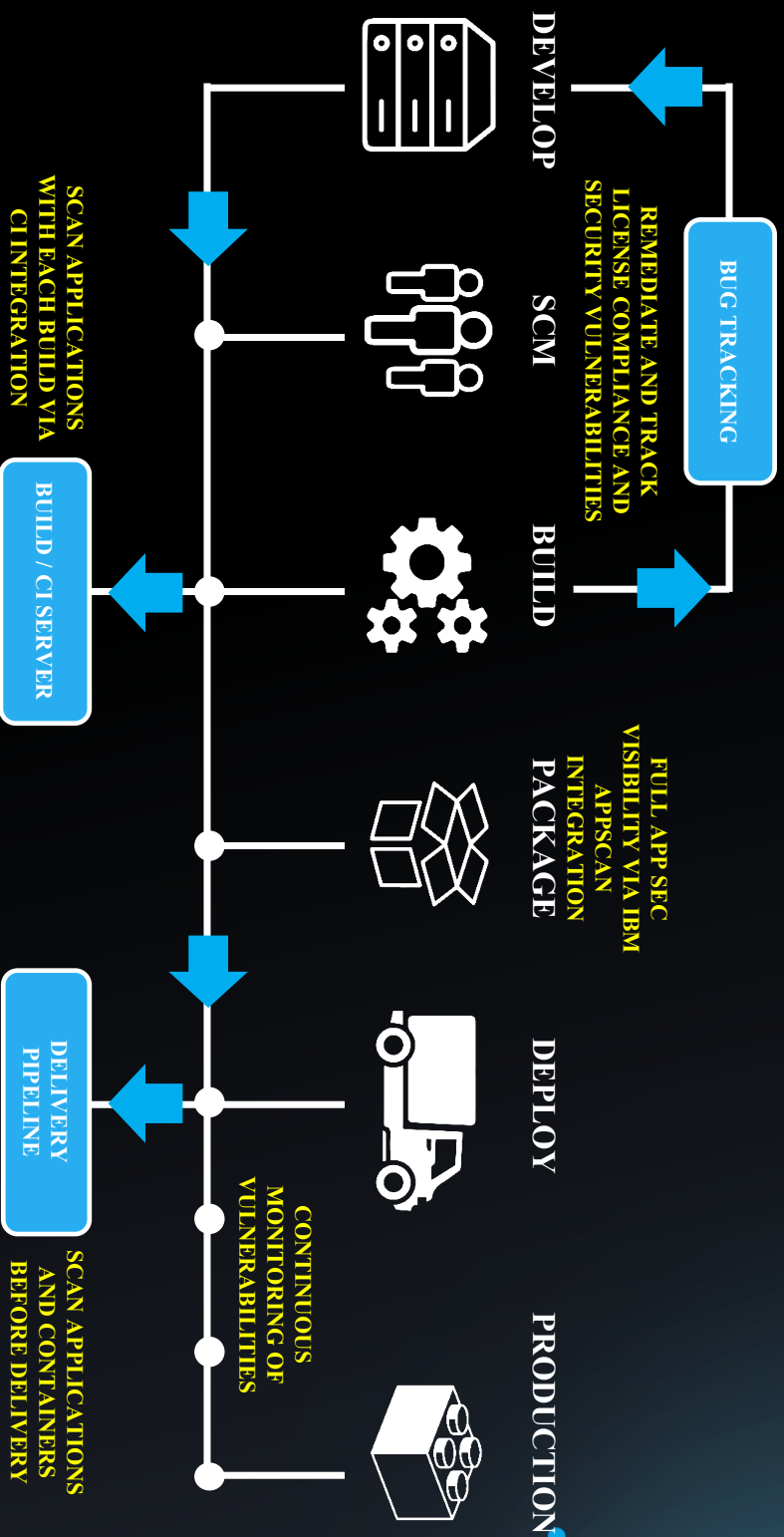
Costs to remediate a vulnerability



WHERE ARE YOU ON THE MATURITY MODEL?



Integrating into your development environment





INVENTORY

to Search and
Monitor Open
Source



MAP

Known Security,
License and
Operational Risk



IDENTIFY

Automatically
the Open Source
In Use



TRACK

Policy Violations
and Remediation
Priorities



ALERT

New
Vulnerabilities
and Policy
Violations

Hub Architecture

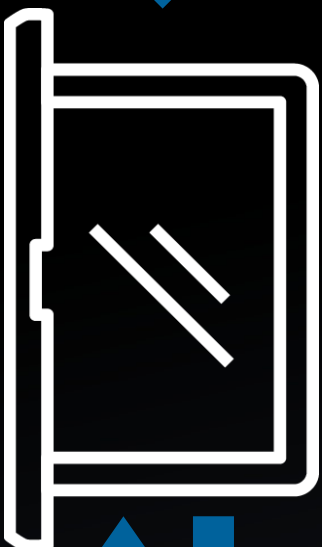
1 Hub Scan



2 File & Directory Signatures



Hub Web Application



3 Open Source is Identified



Black Duck
KnowledgeBase

On Premises

Black Duck Data Center

Hub Architecture Details



Scan Optimizations

JAVA, C, C++, C#, JAVASCRIPT, RUBY, PYTHON, SCALA, PHP, OBJ-C, SWIFT, GO, R, PERL

DEBIAN, FEDORA, RHEL, ALPINE



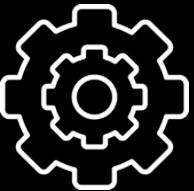
Hub Web Application



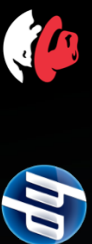
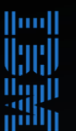
Weekly project updates

Hourly vulnerability updates

KnowledgeBase
Registration
Updates
Docs



Integrations



Black Duck KnowledgeBase

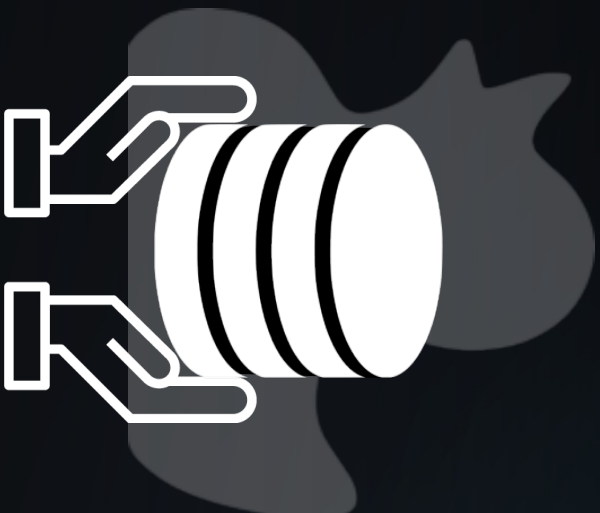
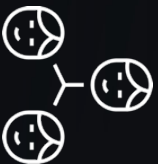
1.5



Million Projects
(+5M Releases)

300,000

OpenHub.com Users
(per month)



KB Team

31 Dedicated Members

3 Teams

8,500

Websites



140,000

Vulnerabilities
(Includes NVD & VulnDB)





DEMO

1. Find most vulnerable application
2. Look at risks
 1. Security
 2. License
 3. Operational risks
3. Policy Management
4. Use the Black Duck Knowledgebase proactively



Summary

- Inventory of OSS components
- Risks associated with the found components
 - Security risks
 - License risks
 - Operational risks
- Keep up the speed of innovation with policies
- Use the Black Duck Knowledgebase proactively

*No scanning solution
is 100% accurate.*

*The Black Duck Hub
is designed to provide
the best results
possible.*



Hub Scanning & Identification

Why?

- Open Source uses Open Source
- Many Languages and Environments

How?

- Evidence-based; multi-factor
- Usability
- Knowledge Base Team
- Roadmap

***We recommend joint review of scan results during your POC*

Search Results

Search Types

- Projects **0**
- Components **9,382**
- Vulnerabilities **2,309**

</> Primary Language

Primary Language

Commit Activity

- Stable **125**
- Decreasing **34**
- Increasing **18**

Tags

web (209)

github.com
Apache HTTP Server

Versions: 302

The Apache HTTP Server Project is a collaborative software development effort aimed at creating a robust, commercial-grade, feature-rich, and freely-available source code implementation of an HTTP (Web) server. The project is jointly managed by a groa€!

- gateway
- dav
- httpd
- dynamic_content
- xml
- isapi
- ssl
- authorization
- ftp
- plugin
- apache
- modular
- intranet
- webdav
- ldap
- cgi
- ftpservlet
- http_server
- http
- webservers
- cgi
- web
- server
- scgi
- fastcgi
- https
- sni
- authentication
- tls
- html
- internet

github.com
jetty - java based HTTP / Servlet / SPDY / WebSocket Server

Versions: 730

Jetty is an Open Source HTTP Servlet Server written in Java. It is a full featured HTTP/1.1 server and a Servlet container. It is designed to be small, fast, embeddable and extensible. It supports HTTP/1.1, servlets 2.3, and JSP 1.2.

- web
- dynamic_content
- web_server
- java
- servlet
- application_server
- embedded
- jsp
- ajax
- usability
- servlet_container
- http_server
- http
- j2ee

pancakehttp.net
Pancake HTTP Server

Versions: 0

Pancake is a fast and lightweight HTTP Server written in C and PHP. It comes with its own PHP SAPI and features support for FastCGI and AJP13. Stay tuned for great new features in the future!

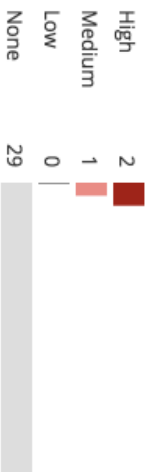
- gateway
- web
- codecache
- http
- fastcgi
- ajp13
- webservers
- php

rack.github.com
Rack





Security Risks



Filter components...

Component Vulnerabilities



Displaying 1-3 of 3

Displaying 21 Vulnerabilities for Apache Struts 2.3.7

maven / org.apache.struts:struts2-core:2.3.7

Filter Vulnerabilities

Add Filter

Identifier	Published	Base Score	Exploitability	Impact	Status	Target date	Actual date
> NVD CVE-2016-3082	May 17, 2016	10	10	10	New	Never	Never
> NVD CVE-2013-4316	Oct 1, 2013	10	10	10	New	Never	Never
> NVD CVE-2016-0785	Apr 12, 2016	10	10	10	New	Never	Never
> VulnDB 103918	Mar 3, 2014	10	10	10	New	Never	Never
> NVD CVE-2016-3081	Jun 1, 2016	9.3	8.6	10	New	Never	Never
> NVD CVE-2013-2251	Mar 31, 2016	9.3	8.6	10	New	Never	Never

Description

Apache Struts 2.0.0 through 2.3.15 allows remote attackers to execute arbitrary OGNL expressions via a parameter with a crafted (1) action, (2) redirect, or (3) redirectAction: prefix.

[View full record](#)

Base Score Metrics

AV NETWORK A COMPLETE
 AC MEDIUM C COMPLETE
 AU NONE I COMPLETE

Published on Mar 31, 2016 Updated on Mar 31, 2016 Updated by default-authenticated-user on Jul 1, 2016

Remediation

Status New

Target date

Actual date





C Demo Project 1.0

unknown Versions: 1 | Owner: Dave Meurer | Tier: 1 | Phase: In Development | Distribution: External

- Components
- Security
- Files
- Reports
- Settings

Security Risk



License Risk



Operational Risk



+ Add Component

Filter components...

Add Filter

Component	Match Count	Match Type	Usage	License	Security Risk	Operational Risk
Linux Kernel 4.3.3	Manually Added	Dynamically Linked	GPL-2.0	40 86 22	Low	
Open Office 2.0.4	43 Matches	Files Modified, Files Added/Deleted	Dynamically Linked	LGPL-2.1+	24 2	High
OpenSSL 1.0.1d	1 Match	Exact	Dynamically Linked	OpenSSL and 1 more...	16 56 6	Medium
LibreOffice 3.4.5.2	431 Matches	Files Modified, Exact, Files Added/Deleted	Dynamically Linked	LGPL-3.0+	3 3	High
Python programming language 3.4.1	Manually Added	Dynamically Linked	Python-2.0	1 4 1	Medium	
Vim Python 7.4.488	1 Match	Exact	Dynamically Linked	GPL-2.0+ and 1 more...	1 2 1	High
ActionBarSherlock 4.1.0	1 Match	Files Modified	Dynamically Linked	Apache-2.0		High
PortableApps.com OpenOffice.org 3.2.1 Source	3 Matches	Files Modified, Files Added/Deleted	Dynamically Linked	MIT and 4 more...		High
tiger 3.2.3	1 Match	Exact	Dynamically Linked	GPL-1.0+		
LabPlot 1.3.1	1 Match	Files Added/Deleted	Dynamically Linked	GPL-2.0+		High
libpam-ldap 184	1 Match	Exact	Dynamically Linked	GPL-2.0+ and 1 more...		
Adobe Source Libraries 2	Manually Added	Dynamically Linked	Unknown License			High





Security Risk



+ Add Component

Component

Linux Kernel	4.3.3	Manually Added	Dynamically Linked	H	GPL-2.0	40	86	22	Low
Open Office	2.0.4	43 Matches	Files Modified, Files Added/Deleted	M	LGPL-2.1+	24	2		High
OpenSSL	1.0.1d	1 Match	Exact	M	OpenSSL and 1 more...	16	56	6	Medium
LibreOffice	3.4.5.2	431 Matches	Files Modified, Exact, Files Added/Deleted	M	LGPL-3.0+	3	3		High
Python programming language	3.4.1	Manually Added	Dynamically Linked		Python-2.0	1	4	1	Medium
Vim Python	7.4.488	1 Match	Exact		GPL-2.0+ and 1 more...	1	2	1	High
ActionBarSherlock	4.1.0	1 Match	Files Modified		Apache-2.0				High
PortableApps.com	OpenOffice.org 3.2.1 Source	3 Matches	Files Modified, Files Added/Deleted	H	MIT and 4 more...				High
tiger	3.2.3	1 Match	Exact	M	GPL-1.0+				High
LabPlot	1.3.1	1 Match	Files Added/Deleted	H	GPL-2.0+				High
libpam-ldap	184	1 Match	Exact	M	GPL-2.0+ and 1 more...				High
Adobe Source Libraries	2	Manually Added	Dynamically Linked	H	Unknown License				High

Policy Violations

Here is the list of policies this component violates. By overriding this component it will no longer be in violation.

No Copy-left licenses in external applications

- Project Distribution Type EQUALS EXTERNAL
- License Family EQUALS RECIPROCAL

No High Vulnerabilities for high priority external applications

- High Severity Vulnerability Count GREATER THAN 0
- Project Tier EQUALS 1
- Project Distribution Type IN EXTERNAL SAAS

Cancel

Override

Operational Risk

Filter components...

Add Filter

+ Create Project



Dave

Notifications

All notifications

Show Removed Notifications

1 new vulnerability on Apache Commons FileUpload 1.2.2 New: CVE-2016-5992	Jul 8, 2016
Vulnerabilities updated on Apache Struts 2.3.7 New:	Jun 9, 2016
6 new policy violations Duck Hub Demo 2.0	Jul 14, 2016
1 new policy violation Slub Component Demo 6.0.1	Jul 14, 2016
10 new policy violations (BDS00820)debian 7.11	Jul 14, 2016
6 new policy violations C Demo Project 1.0	Jul 14, 2016
3 new policy violations DweTest 1.0	Jul 14, 2016
5 new policy violations rheif7-atomic-scan Friday, 24Jun-16 19:48:45 UTC	Jul 14, 2016
3 new policy violations Duck Hub Bamboo 3.0	Jul 14, 2016

JIRA Dashboards - Projects - Boards - Create

Search

Sales Demo Project / SDP-9

Black Duck Policy Violation detected on Hub Project 'Duck Hub Demo' / '2.0', component 'Transaction 1.1 API' / '1.0.1.Final' [Rule: 'No Copy-left licenses in external applications']

Details

Type: Task

Status: **To Do** (View Workflow)

Resolution: Unresolved

Labels: None

Description

The Black Duck Hub has detected a Policy Violation on Hub Project 'Duck Hub Demo' / '2.0', component '1.0.1.Final'. The rule violated is: 'No Copy-left licenses in external applications'

Attachments

Activity

All Comments Work Log History

There are no comments yet on this issue.

Comment

People

Assignee: Unassigned

Reporter: Sales Engineering

Watchers: 1 Stop watching this issue

Jenkins

Back to Dashboard

Status

Changes

Workspaces

Build Now

Delete Maven project

Configure

Modules

Build History

Build	Time
#109	Jul 7, 2016 4:16 PM
#108	Jul 7, 2016 4:13 PM
#107	Jul 5, 2016 3:33 PM
#106	Jul 5, 2016 2:18 PM
#105	Jul 1, 2016 12:30 PM

SSS for all SSS for failures

Maven project name: Duck Hub Demo

Description

Post-build Actions

Black Duck Hub Integration

Project Name: Duck Hub Demo

This Project exists on the Hub Server: https://saleshub.blackducksoftware.com/

Project Version: 3.0

This Version exists in the Project: Duck Hub Demo

Phase: In Development

Distribution: SASS

Scan target: /sd/duckhubtarget/duckhub-3.0.war

Delete Scan target

Add another Scan target

Black Duck Hub Failure Conditions

Fail the Build for Hub Policy violations

Create Project/Version

Advanced...

Delete

Delete

Done Meurer | log out





BLACKDUCK

Organizations worldwide use Black Duck Software's industry-leading products to automate the processes of securing and managing open source software, eliminating the pain related to security vulnerabilities, open source license compliance and operational risk. Black Duck is headquartered in Burlington, MA, and has offices in San Jose, CA, London, Frankfurt, Hong Kong, Tokyo, Seoul and Beijing. For more information, visit www.blackducksoftware.com