



NTT DATA

**Open Source Governance for a full
and proper DevSecOps process**

**AGILE/
DEVOPS
GLOBAL
CONFERENCE**

Marco Iusi

Manager - NTT DATA Italia

Marco Iusi



Manager
Digital Architecture
NTT DATA Italia

I'm passionate about **innovation** and in recent years I deal with **Open Source**, in which I strongly believes as a lever for innovation, but at the same time I strives to spread a culture of greater awareness of related risks, addressing a way to prevent and govern them adequately.

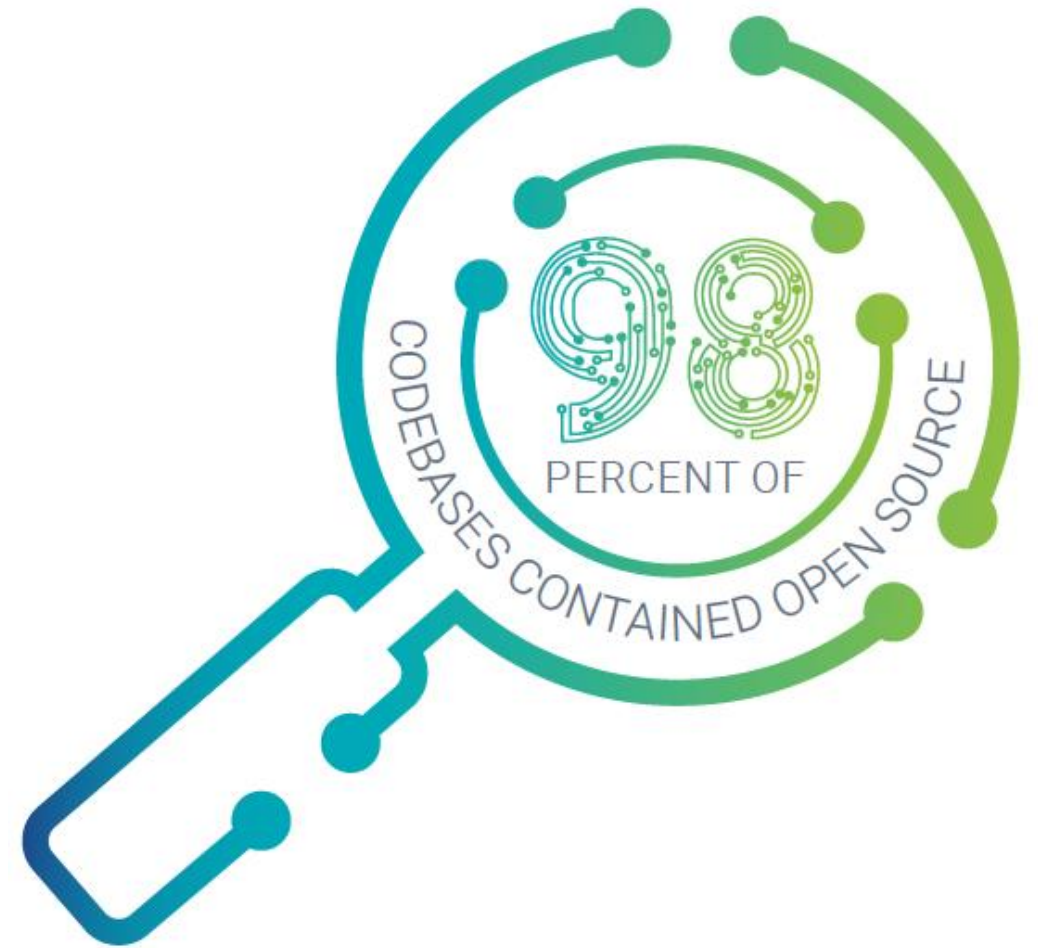
I also lead the **Google Cloud Competence Centre** inside the **Digital Architecture** area.

Outside work, I love to travel, I love nature and I like being part of voluntary and social associations.

I also enjoy doing and seeing sport, especially football, and I appreciate good food ... I'm Italian, you know!

Open Source

Open Source is a foundation for innovation and is everywhere!

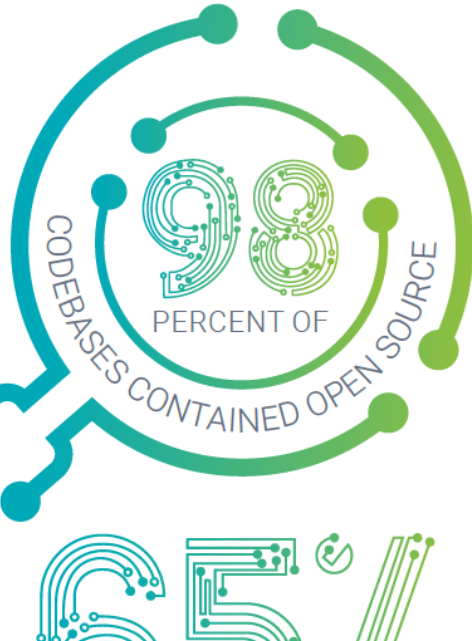


Open Source Governance

1546
CODEBASES
AUDITED IN 2020



17 INDUSTRIES REPRESENTED



65%
OF CODEBASES
HAD LICENSE
CONFLICTS

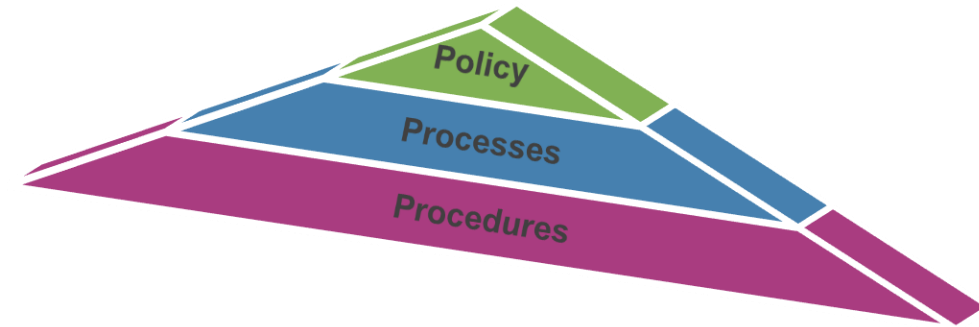
84%
OF CODEBASES
HAD AT LEAST ONE
VULNERABILITY
WITH AN AVERAGE OF
158
PER CODEBASE



75%
OF ALL CODEBASES WERE
COMPOSED OF OPEN SOURCE

What's behind Open Source?

Open Source Software Adds Complexity



Open Source Software Can Involve Risks

**Open Source Governance
is a MUST!**

Log4J case

Logging Services <http://logging.apache.org>

LOG4J

Last Published: 2021-12-28 | Version: 2.17.1

Apache Log4j Security Vulnerabilities

This page lists all the security vulnerabilities fixed in released versions of Apache Log4j 2. Each vulnerability is given a security impact rating by the Apache Logging security team. Please note that this rating may vary from platform to platform. We also list the versions of Apache Log4j the flaw is known to affect, and where a flaw has not been verified list the version with a question mark.

Note: Vulnerabilities that are not Log4j vulnerabilities but have either been incorrectly reported against Log4j or where Log4j provides a workaround are listed at the end of this page.

Please note that Log4j 1.x has reached End of Life in 2015 and is no longer supported and will not be fixed. Users should upgrade to Log4j 2 to obtain security fixes.

Please note that binary patches are never provided. If you need to apply a source code patch, please refer to the instructions in the root subdirectory of the source code. For Log4j 2 this is BUILDING.md. This file can be found in the root subdirectory.

If you need help on building or configuring Log4j or other help on following the instructions, please refer to the Log4j Users mailing list.

If you have encountered an unlisted security vulnerability or other unexpected behaviour, please report it to the Apache Logging security team.

National Cyber Security Centre

Home Information for... Advice & guidance Education & skills Products & services News, blogs, events...

THE CONVERSATION

Academic rigor. Journalism. Fair.

LOG4J

What is Log4j? A cybersecurity expert explains the latest internet vulnerability, how bad it is and what's at stake

Log4j vulnerability - what everyone needs to know

Information about the critical vulnerability and what steps you can take to reduce risk

CONTRAST SECURITY

DEVELOPERS THE PLATFORM SOLUTIONS WHY CONTRAST? PARTNERS COMPANY RESOURCES



NEWS INSIGHTS: THE LOG4J DISASTER

By Journal of Cyber Policy | Dec 17, 2021 12:09:05 AM | Contrast News

The Log4j cyber threat is being compared to the notorious Equifax hack of 2017, which affected 147 million Americans. However, the Log4j exploit has far greater reach due to the software component's widespread adoption. It was recently recognized as critical with reactive guidance for organizations to follow from CISA, the federal government's cybersecurity arm.

Jeff Williams, Co-Founder and CTO at Contrast Security, does not believe that CISA's reactive recommendations for organizations to protect themselves go far enough. He said, "There are a wide range of methods hackers can use to access personal information through Log4j's vulnerability."

RESEARCH & INTELLIGENCE

Log4j Vulnerability FAQs

FRIDAY, DECEMBER 17, 2021
BY: COUNTER THREAT UNIT RESEARCH TEAM

Twitter LinkedIn Facebook Email

OPEN SOURCE / SECURITY / WHAT IS DEVOPS? / SPONSORED / CONTRIBUTED

Learning from the Unfolding Log4j Emergency

22 Dec 2021 4:00am, by Charlotte Freeman



Log4j Zero-Day Vulnerability Response

→ Last Updated: January 7, 2022

Contents

The 'most serious' security breach ever is unfolding right now. Here's what you need to know.

Much of the Internet, from Amazon's cloud to connected TVs, is riddled with the log4j vulnerability, and has been for years



Log4J case – the real world

Your next task is to figure out which applications in your org use log4j



Log4J case – the imaginary world

- You know all the projects that are using the library
- You know the precise version you are using in each project
- You know the path where you can find the library in each project
- Before the news goes public and it is known by all, you have received an email addressed only to you, as the owner of a project in which the Log4j library is present, with the details of the new vulnerability and the indications to remedy immediately.

Let's build this word!

Bill of Materials and OSS related Risks



Open Source License Compliance: OpenChain ISO/IEC 5230

OpenChain ISO/IEC 5230 is the **International Standard** for open source license compliance.

It is simple, effective and suitable for **companies of all sizes in all markets**.

This standard is **openly developed** by a **vibrant user community** and **freely available** to all.

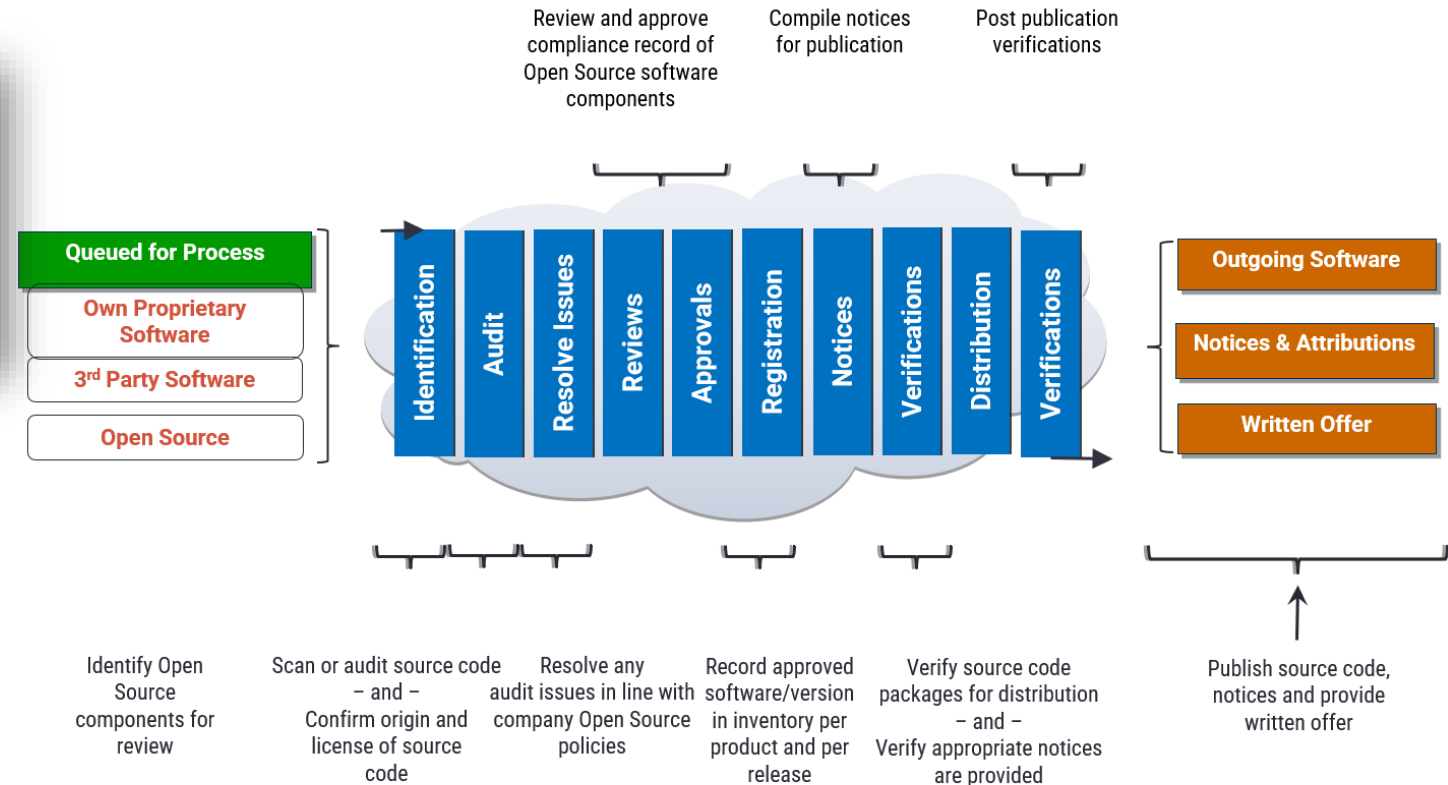


NTT DATA Italy collaborates with OpenChain project to build trust in open source

By Shane Coughlan | February 5, 2020 | Featured, News



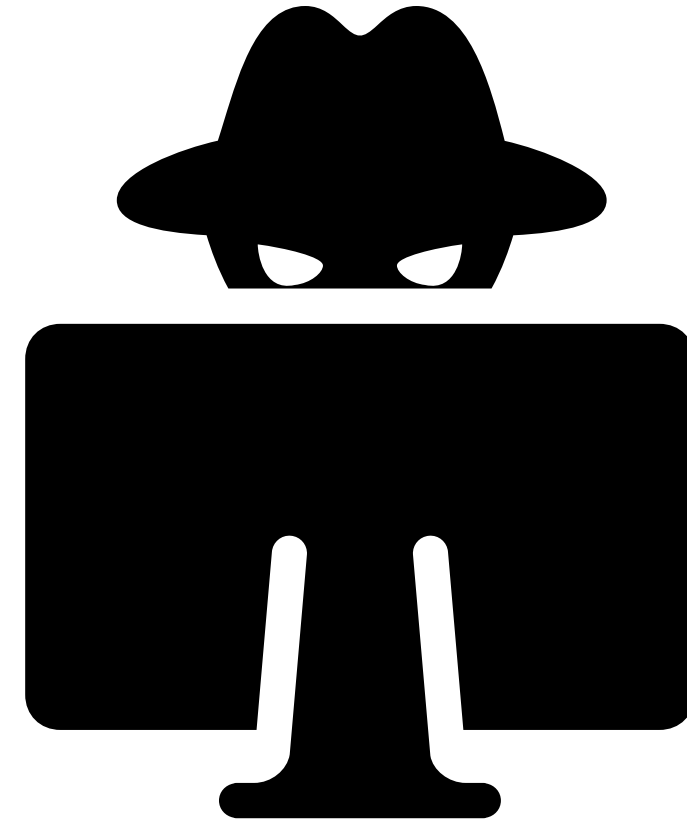
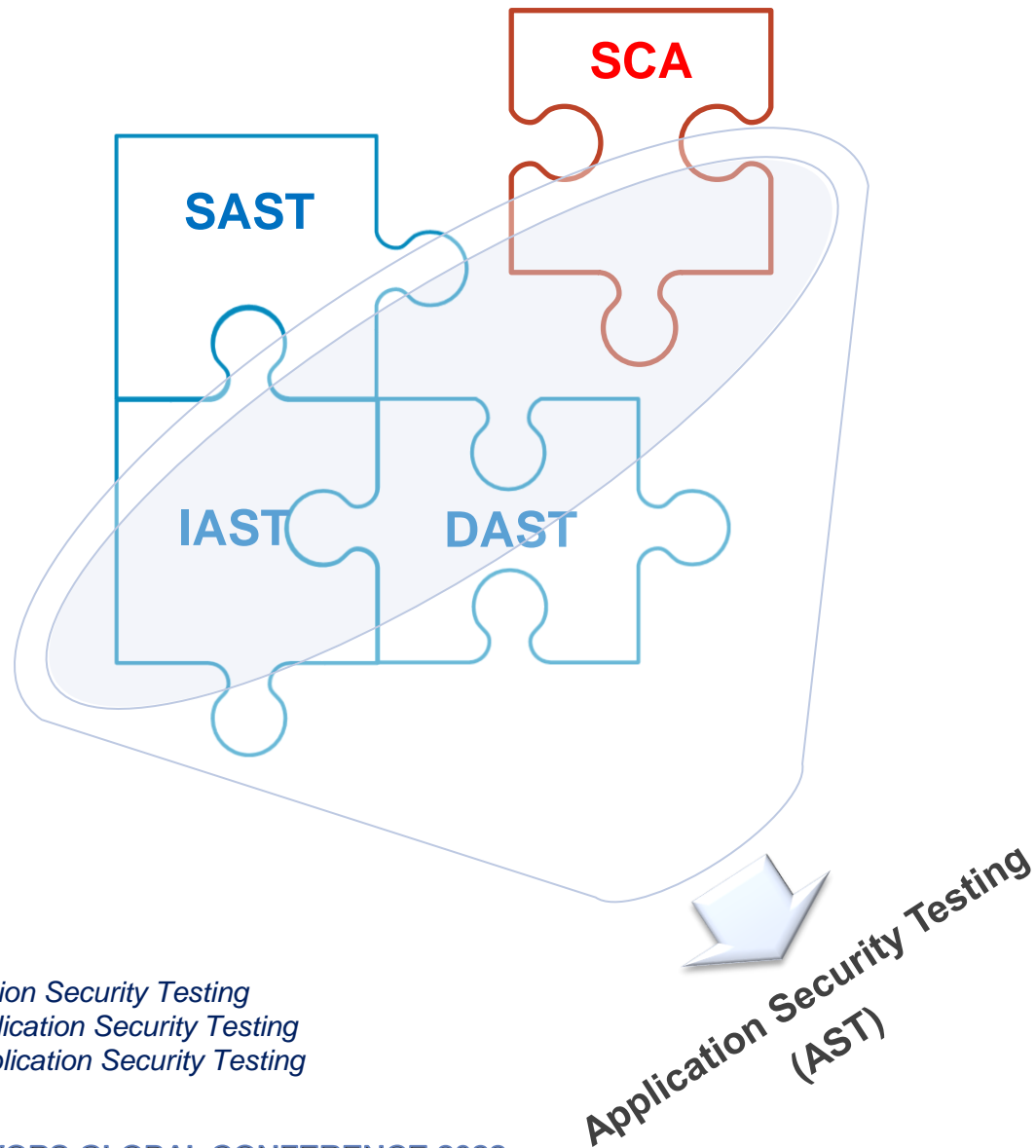
AGILE/DEVOPS GLOBAL CONFERENCE 2022



Example of Compliance Management End-to-End Process

**<https://www.openchainproject.org/resources>*

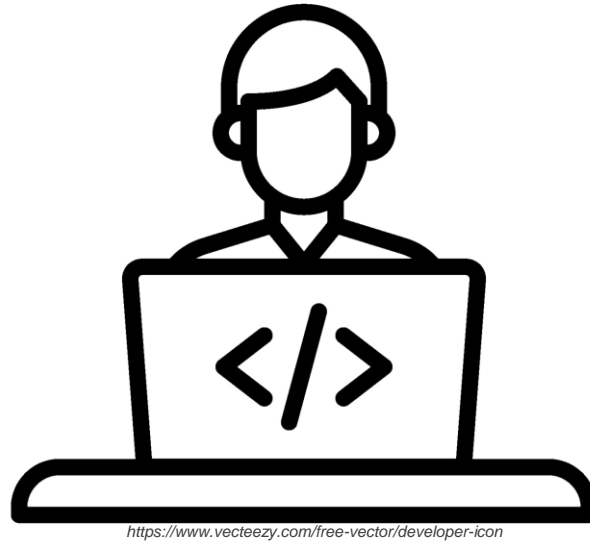
SCA: Software Composition Analysis



<https://www.visualpharm.com/free-icons/hacker-595b40b75ba036ed117d616b>

SAST: Static Application Security Testing
DAST: Dynamic Application Security Testing
IAST: Interactive Application Security Testing

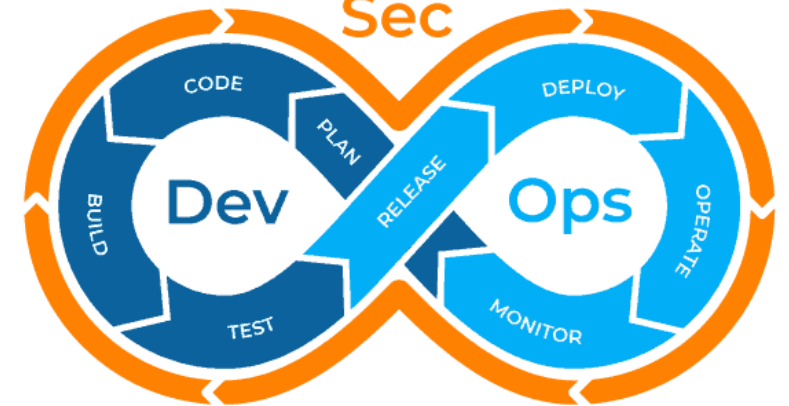
Open Source Audit



Final assessment

VS

Sec



DevSecOps

Synopsys Black Duck

Synopsys named a Leader in the 2021 Gartner Magic Quadrant for Application Security Testing for the fifth year

Posted by [Jason Schmitt](#) on Tuesday, June 1, 2021

In the 2021 Gartner Magic Quadrant for Application Security Testing, Synopsys placed highest and furthest for the third consecutive year for our ability to execute and our completeness of vision.

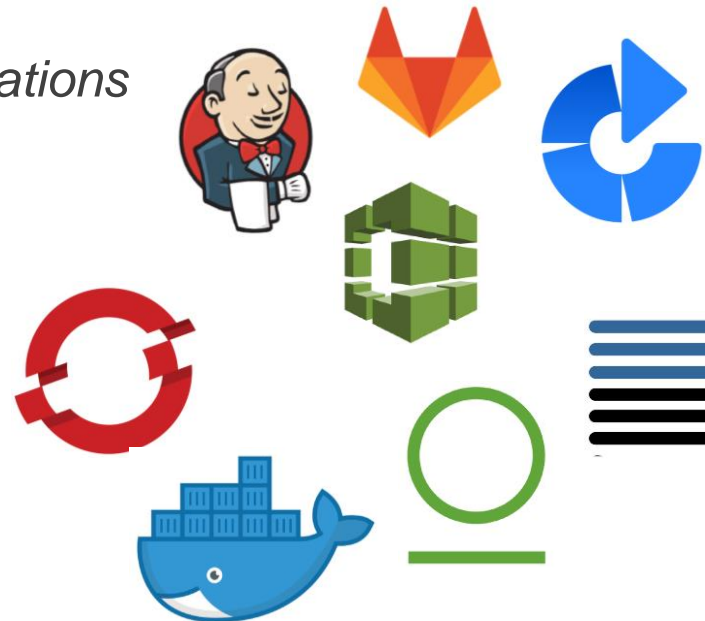
**<https://www.synopsys.com/blogs/software-security/gartner-mq-ast/>*

BLACKDUCK

BY **SYNOPSYS**[®]

Black Duck DevOps Integrations

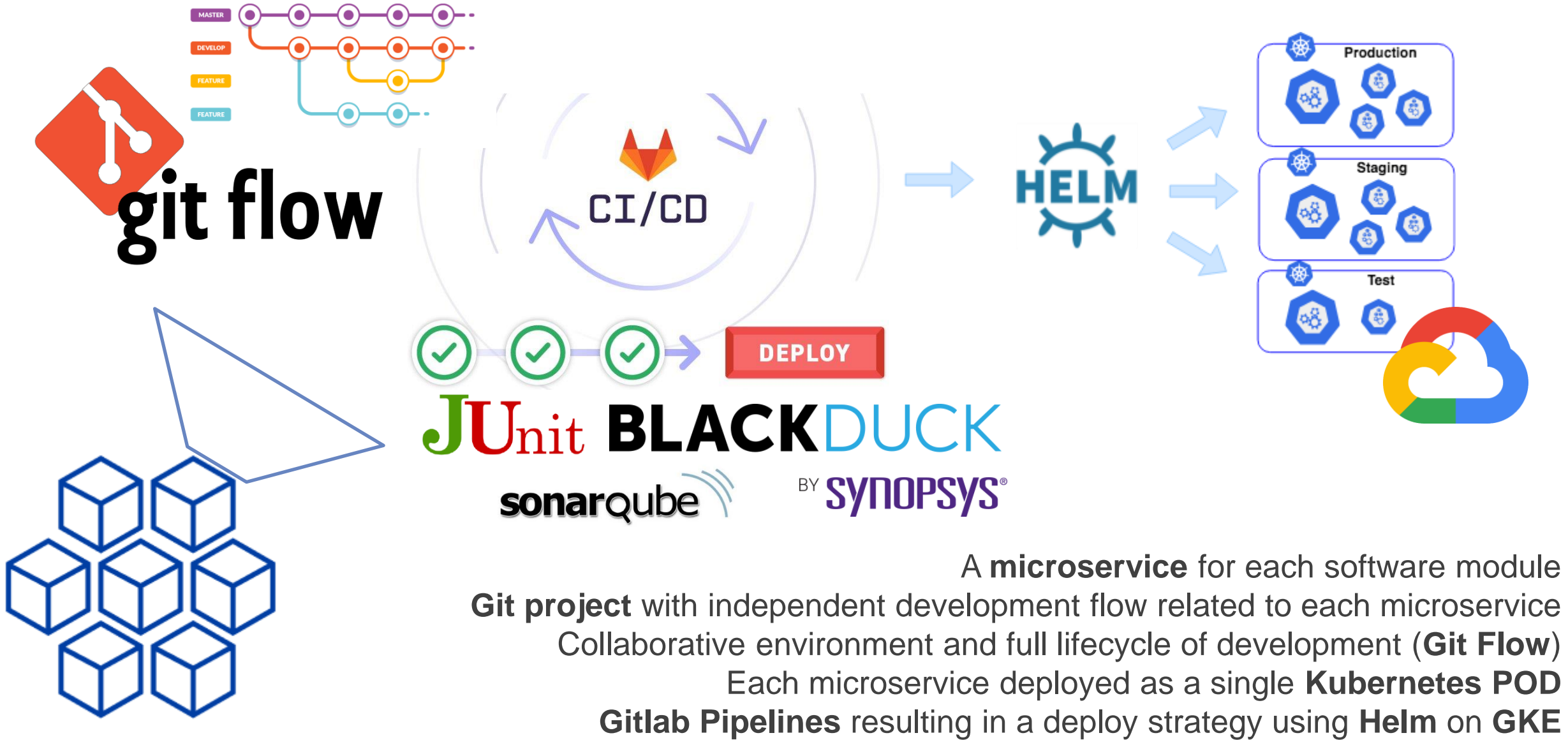
- *IDE integrations*
- *Continuous integration (CI) tool integrations*
- *Package managers and build tools*
- *Bug and issue tracking integrations*
- *Binary repository integrations*
- *Application security suite integrations*
- *Container platform integrations*



Black Duck CLI
Black Duck API
SPDX integration

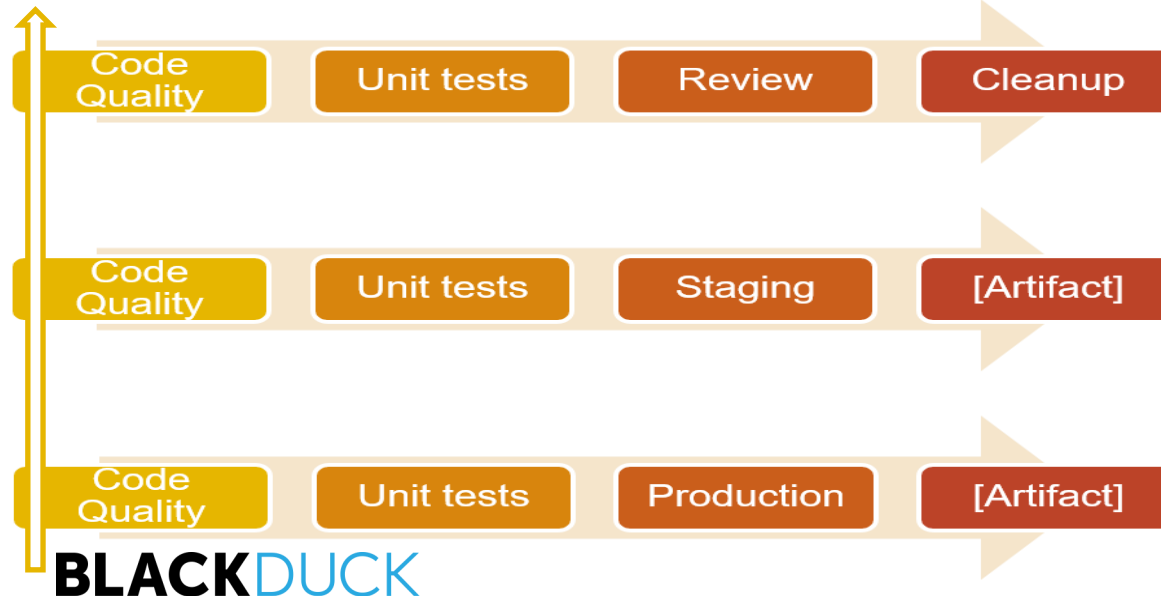
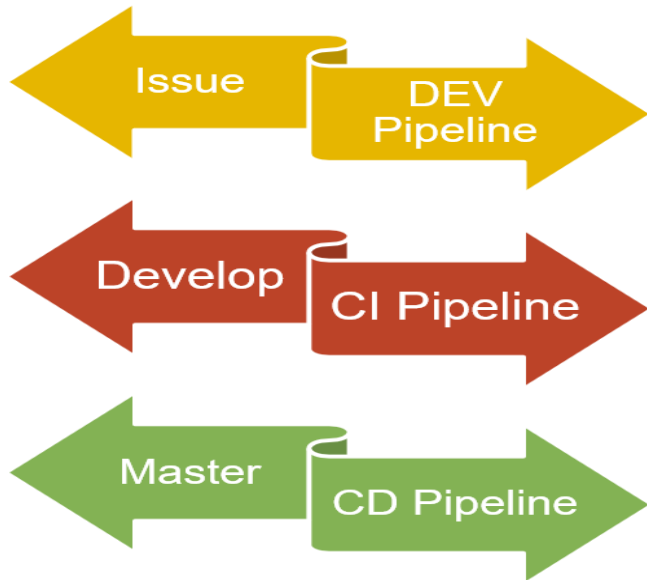
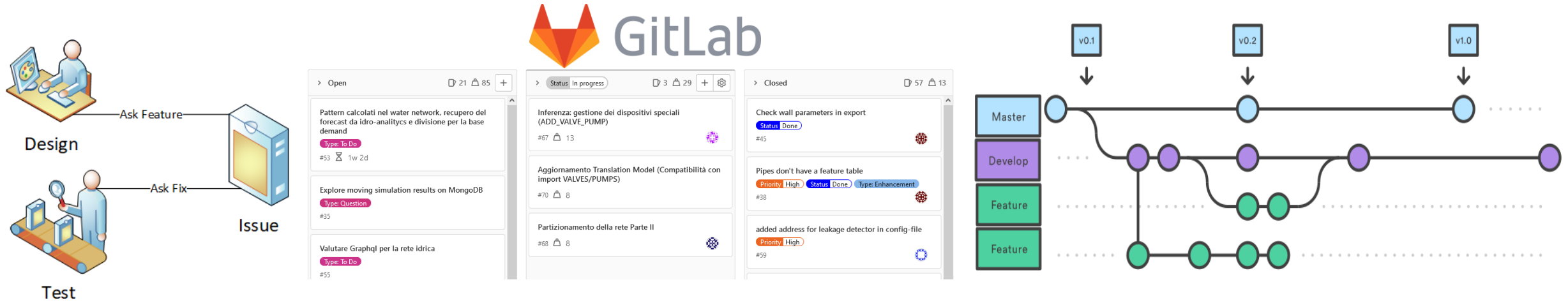
Most Black Duck integrations are provided as open source integrations under the Apache 2.0 open source license.

DevSecOps environment for Cloud Native Projects

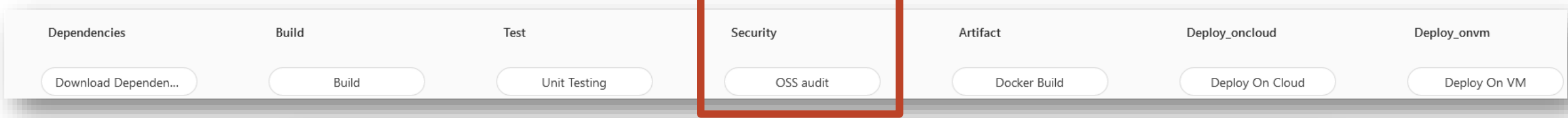


A **microservice** for each software module
Git project with independent development flow related to each microservice
Collaborative environment and full lifecycle of development (**Git Flow**)
Each microservice deployed as a single **Kubernetes POD**
Gitlab Pipelines resulting in a deploy strategy using **Helm** on **GKE**

DEMO environment



GitLab Pipeline Configuration



NTT DATA Menu Search GitLab

✓ This GitLab CI configuration is valid. [Learn more](#)

Edit Visualize **Lint** View merged YAML

🟢 Status:
Syntax is correct. CI configuration validated, including all configuration added with the `includes` keyword. [More information](#)

Parameter	Value
Dependencies Job - Download Dependencies	<pre>mvn dependency:go-offline mvn dependency:copy-dependencies -Dmdep.useRepositoryLayout=true -Dmdep.copyPom=true -DoutputDirectory=.m2/repository</pre> <p>Only policy: branches, tags When: on_success</p>
Build Job - Build	<pre>mvn package -Dmaven.test.skip=true</pre> <p>Only policy: branches, tags When: on_success</p>
Test Job - Unit Testing	<pre>mvn verify</pre> <p>Only policy: branches, tags When: on_success</p>
Security Job - OSS audit	<pre>bash <(curl -s -L https://detect.synopsys.com/detect.sh) --blackduck.url="{HUB_URL}" --blackduck.api.token="{HUB_TOKEN}" --blackduck.trust.cert=true --detect.policy.check.fail.on.severities=CRITICAL --detect.impact.analysis.enabled=true</pre> <p>Only policy: branches, tags When: on_success</p>
Artifact Job - Docker Build	<pre>docker login -u \$CI_REGISTRY_USER -p \$CI_REGISTRY_PASSWORD \$CI_REGISTRY</pre> <pre>echo "Building Docker image:" \$DOCKER_IMAGE_NAME docker build --pull -t \$DOCKER_IMAGE_NAME . docker push \$DOCKER_IMAGE_NAME</pre> <p>Only policy: branches, tags When: on_success</p>

Gitlab for NTT Data EMEA projects - All rights reserved ©

BlackDuck Policy Configuration

The screenshot shows the BlackDuck Policy Management interface. On the left is a navigation sidebar with options: Dashboard, Find, Scans, Reports, Manage (Component Management, Custom Fields Management, License Management, Policy Management, Project Group Management), and Admin. The main area is titled 'Policy Management' and contains a table of policy rules. At the top of the table are buttons for '+ Create Policy Rule', 'Delete', and 'Add Filter'. The table has columns for Policy Rule, Description, Severity, Scan Modes, and Category. The 'High Risk Vulnerabilities' rule is highlighted.

Policy Rule	Description	Severity	Scan Modes	Category
Reciprocal		Critical	Full	License
Old versions		Minor	Full	Operational
High Risk Vulnerabilities		Blocker	Full	Security
		Major	Full	Uncategorized



The 'Edit Policy Rule' dialog box shows the configuration for the 'High Risk Vulnerabilities' rule. The fields are: Name (High Risk Vulnerabilities), Category (Security), Description (Block any component with High Risk Vulnerability), and Severity (Blocker).

The dropdown menu for 'Component Release Date' lists several conditions under three categories: Operational, Vulnerabilities, and Licenses.

- Operational**
 - Component Release Date
 - Commits in the past year
 - Contributors in the past year
- Vulnerabilities**
 - Critical Severity Vulnerability Count
 - High Severity Vulnerability Count
 - Medium Severity Vulnerability Count
 - Low Severity Vulnerability Count
 - Highest Vulnerability Score
- Licenses**
 - Unfulfilled License Terms
 - License Conflict with Project Version

The 'Component Conditions' panel shows a list of conditions for the policy rule. Each condition has a dropdown for the condition name, a dropdown for the operator, and a text input for the value. There are also buttons to add and delete conditions.

- Component Release Date: less than, 01/01/2020
- Critical Severity Vulnerability Count: greater than, 1
- License Family (Declared): equals, Reciprocal
- + Component Condition
- Vulnerability Conditions
 - RCE (Remote Code Execution): equals, Yes
 - Overall Score: greater than or equal to, 7,0
 - Exploit Available: equals, Yes

GitLab Pipeline execution



GitLab

failed Pipeline #87189 triggered 7 minutes ago by Melina, Antonio

Update .gitlab-ci.yml file

5 jobs for **master** in 6 minutes and 13 seconds (queued for 8 seconds)

latest

dbd9d86e

No related merge requests found.

Pipeline Needs Jobs 5 Failed Jobs 1 Tests 0

Dependencies	Build	Test	Security	Deploy_onvm
Download Dependencies	Build	Unit Testing	Security Scan	Deploy On VM

```
202 2022-01-21 16:00:14 UTC INFO [main] --- ===== Detect Status =====
203 2022-01-21 16:00:14 UTC INFO [main] ---
204 2022-01-21 16:00:14 UTC INFO [main] --- GIT: SUCCESS
205 2022-01-21 16:00:14 UTC INFO [main] --- MAVEN: SUCCESS
206 2022-01-21 16:00:14 UTC INFO [main] ---
207 2022-01-21 16:00:14 UTC INFO [main] --- Signature scan / Snippet scan on /builds/D5sZHx3R/0/italy/solution-services/open-
208 2022-01-21 16:00:14 UTC INFO [main] ---
209 2022-01-21 16:00:14 UTC INFO [main] --- IMPACT_ANALYSIS: SUCCESS
210 2022-01-21 16:00:14 UTC INFO [main] --- Overall Status: FAILURE_POLICY_VIOLATION - Detect found policy violations.
211 2022-01-21 16:00:14 UTC INFO [main] ---
212 2022-01-21 16:00:14 UTC INFO [main] --- =====
213 2022-01-21 16:00:14 UTC INFO [main] ---
214 2022-01-21 16:00:14 UTC INFO [main] --- Detect duration: 00h 03m 58s 146ms
215 2022-01-21 16:00:14 UTC ERROR [main] --- Exiting with code 3 - FAILURE_POLICY_VIOLATION
216 Result code of 3, exiting
218 Cleaning up project directory and file based variables
220 ERROR: Job failed: command terminated with exit code 1
```

passed Pipeline #87189 triggered 12 minutes ago by Melina, Antonio

Update .gitlab-ci.yml file

6 jobs for **master** in 5 minutes and 16 seconds (queued for 8 seconds)

latest

dbd9d86e

No related merge requests found.

Pipeline Needs Jobs 6 Tests 0

Dependencies	Build	Test	Security	Deploy_onvm
Download Dependencies	Build	Unit Testing	Security Scan	Deploy On VM

```
194 2022-01-21 16:05:06 UTC INFO [main] --- ===== Detect Status =====
195 2022-01-21 16:05:06 UTC INFO [main] ---
196 2022-01-21 16:05:06 UTC INFO [main] --- GIT: SUCCESS
197 2022-01-21 16:05:06 UTC INFO [main] --- MAVEN: SUCCESS
198 2022-01-21 16:05:06 UTC INFO [main] ---
199 2022-01-21 16:05:06 UTC INFO [main] --- Signature scan / Snippet scan on /builds/D5sZHx3R/0/italy/solution-services/open-
200 2022-01-21 16:05:06 UTC INFO [main] ---
201 2022-01-21 16:05:06 UTC INFO [main] --- IMPACT_ANALYSIS: SUCCESS
202 2022-01-21 16:05:06 UTC INFO [main] --- Overall Status: SUCCESS - Detect exited successfully.
203 2022-01-21 16:05:06 UTC INFO [main] ---
204 2022-01-21 16:05:06 UTC INFO [main] --- =====
205 2022-01-21 16:05:06 UTC INFO [main] ---
206 2022-01-21 16:05:06 UTC INFO [main] --- Detect duration: 00h 02m 58s 983ms
207 Result code of 0, exiting
209 Saving cache for successful job
210 Not uploading cache 79cb8c7724b0361248b5cfdce29690a4fdea46a2 due to policy
212 Cleaning up project directory and file based variables
214 Job succeeded
```

Black Duck DEMO

SYNOPSYS Search... + Create Project 259 ? System

Black Duck Projects devops.lab.postgres > 1.0.0-SNAPSHOT
 Project ☆ | Phase: In Development | Scans: Up to Date | Status: Up to Date

Components Security Source Reports Details Settings

Security Risk

Number of Components

Critical 0
 High 0
 Medium 7
 Low 4
 None 116

License Risk

Number of Components

High 5
 Medium 20
 Low 0
 None 102

Operational Risk

Number of Components

High 15
 Medium 12
 Low 72
 None 28

Add Bulk Actions Compare to... Print...

Match ignore Not ignored Match Status Confirmed Ignore Not ignored Filter Components... Add Filter

Component	Source	Match Type	Usage	License	Security Risk	Operational Risk
antr 2.7.7	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	ANTLR-PD	High	High
Apache Commons FileUpload 1.4	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	Apache-2.0	Low	Low
Apache Commons Lang 3.12.0	2 Matches	Direct Dependency, Exact Directory	Dynamically Linked	Apache-2.0	Low	Low
Apache Geronimo Annotation Spec 1.3 1.2	1 Match	Exact Directory	Dynamically Linked	Apache-2.0	Low	Low
Apache HttpClient 4.5.13	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	Apache-2.0	High	High
Apache HttpComponents Core 4.4.14	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	Apache-2.0	High	High
Apache Log4j 2.14.1	Manually Added	Manually Added	Dynamically Linked	Apache-2.0	2 2	Low
Apache Log4j to SLF4J Adapter 2.14.1	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	Apache-2.0	Low	Low
Apache Tomcat 9.0.53	26 Matches	Exact Directory	Dynamically Linked	Apache-2.0	1	Low
Apache Tomcat Embed 9.0.53	6 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	Apache-2.0	1	Low
ASM 9.1	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	BSD-3-Clause	High	High
ASM based accessors helper used by json-smart 2.4.7	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	Apache-2.0	Low	Low
AspectJ Runtime 1.9.7	4 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	EPL-2.0	Low	Low
AspectJ weaver 1.9.7	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	EPL-2.0	Low	Low
AssertJ fluent assertions 3.19.0	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	Apache-2.0	Low	Low
Bean Validation API 2.0.2	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	Apache-2.0	Medium	Medium
Bouncy Castle 1.68	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	MIT	1	Low
Bouncy Castle PKIX, CMS, EAC, TSP, PKCS, OCSP, CMP, and CRMF APIs 1.68	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	MIT	Low	Low
Byte Buddy byte-buddy-1.10.22	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	Apache-2.0	Low	Low
byte-buddy-agent 1.10.22	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	Apache-2.0	Low	Low
Checker Qual 3.5.0	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	MIT	Low	Low

Black Duck DEMO

SYNOPSIS Black Duck Projects devops.lab.postgres ▸ 1.0.0-SNAPSHOT

Phase: In Development | Scans: Up to Date | Status: Up to Date

Components Security Source Reports Details Settings

Security Risk
Number of Components

Critical 0
High 0
Medium 7
Low 4
None 116

License Risk
Number of Components

High 5
Medium 20
Low 0
None 102

Operational Risk
Number of Components

High 15
Medium 12
Low 72
None 28

Add Bulk Actions Compare to... Print...

Component	Source	Match Type	Usage	License	Security Risk	Operational Risk
com.guicedee.services.bouncycastle 1.2.0.3-jre17-rc1	11 Matches	Exact Directory	Dynamically Linked	GPL-3.0+	Low	Low
Dataflow 3.1.1	1 Match	Exact Directory	Dynamically Linked	GPL-2.0-with-classpath-exception and 1 more...	Low	Low
h2 1.0.14.0-RC1-jre8	15 Matches	Exact Directory	Dynamically Linked	GPL-3.0+	Low	Low

License Risk | High | Match Ignore | Not Ignored | Match Status | Confirmed | Ignore | Not Ignored | Filter Components... Add Filter

SYNOPSIS Black Duck Projects devops.lab.postgres ▸ 1.0.0-SNAPSHOT

Phase: In Development | Scans: Up to Date | Status: Up to Date

Components Security Source Reports Details Settings

Security Risk
Number of Components

Critical 0
High 0
Medium 7
Low 4
None 116

License Risk
Number of Components

High 5
Medium 20
Low 0
None 102

Operational Risk
Number of Components

High 15
Medium 12
Low 72
None 28

Add Bulk Actions Compare to... Print...

Component	Source	Match Type	Usage	License	Operational Risk
antlr 2.7.7	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	ANTLR-PD	High
Apache HttpClient 4.5.13	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	Apache-2.0	High
Apache HttpComponents Core 4.4.14	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	Apache-2.0	High
ASM 9.1	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	BSD-3-Clause	High

Operational Risk | High | Match Ignore | Not Ignored | Match Status | Confirmed | Ignore | Not Ignored | Filter Components... Add Filter

Operational Risk Factors

- This version was released on Sep 6, 2006 (5,625 days ago)
- 116 Newer project versions available.
- There is increasing commit activity.
- 667 Commits over the last 12 months.
- 62 Contributors over the last 12 months.

Black Duck DEMO

SYNOPSYS Search... + Create Project 259 ? System

Black Duck Projects
devops.lab.postgres > 1.0.0-SNAPSHOT
Project ☆ | Phase: In Development | Scans: Up to Date | Status: Up to Date

Components Security Source Reports Details Settings

Security Risk

Number of Components

Critical 0
High 0
Medium 7
Low 4
None 116

License Risk

Number of Components

High 5
Medium 20
Low 0
None 102

Operational Risk

Number of Components

High 15
Medium 12
Low 72
None 28

Add Bulk Actions Compare to... Print...

Match ignore Not ignored x Match Status Confirmed x Ignore Not ignored x Filter Components... Add Filter

Component	Source	Match Type	Usage	License	Security Risk	Operational Risk
antr 2.7.7	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	ANTLR-PD	High	High
Apache Commons FileUpload 1.4	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	Apache-2.0		
Apache Commons Lang 3.12.0	2 Matches	Direct Dependency, Exact Directory	Dynamically Linked	Apache-2.0		Low
Apache Geronimo Annotation Spec 1.3 1.2	1 Match	Exact Directory	Dynamically Linked	Apache-2.0		
Apache HttpClient 4.5.13	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	Apache-2.0		High
Apache HttpComponents Core 4.4.14	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	Apache-2.0		High
Apache Log4j 2.14.1		Manually Added	Dynamically Linked	Apache-2.0	2 2	Low
Apache Log4j to SLF4J Adapter 2.14.1	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	Apache-2.0		Low
Apache Tomcat 9.0.53	26 Matches	Exact Directory	Dynamically Linked	Apache-2.0	1	Low
Apache Tomcat Embed 9.0.53	6 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	Apache-2.0	1	Low
ASM 9.1	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	BSD-3-Clause		High
ASM based accessors helper used by json-smart 2.4.7	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	Apache-2.0		
AspectJ Runtime 1.9.7	4 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	EPL-2.0		Low
AspectJ weaver 1.9.7	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	EPL-2.0		Low
AssertJ fluent assertions 3.19.0	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	Apache-2.0		Low
Bean Validation API 2.0.2	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	Apache-2.0		Medium
Bouncy Castle 1.68	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	MIT	1	Low
Bouncy Castle PKIX, CMS, EAC, TSP, PKCS, OCSP, CMP, and CRMF APIs 1.68	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	MIT		Low
Byte Buddy byte-buddy-1.10.22	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	Apache-2.0		Low
byte-buddy-agent 1.10.22	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	Apache-2.0		Low
Checker Qual 3.5.0	2 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	MIT		Low

Black Duck DEMO

SYNOPSYS Search... + Create Project [Notifications] [Help] [System]

Black Duck Projects
devops.lab.postgres ▸ 1.0.0-SNAPSHOT
 Project ☆ | Phase: In Development | Scans: Up to Date | Status: Up to Date

Security Risk
 Number of Unique Component Origins
 Critical 0 High 0 Medium 16 Low

Components

- Apache Log4j 2.14.1
 github: apache/logging-log4j2:rel/2.14.1
 Vulnerabilities 2

Apache Log4j 2.14.1
 github: apache/logging-log4j2:rel/2.14.1
 4 Known Vulnerabilities

Displaying 1-1 of 1

Identifier	Overall Score	Status	CWE	Exploit	Workaround	Solution
> BDSA BDSA-2021-3731 (CVE-2021-44228) ⚠ RCE	6.5 Medium	New	CWE-502	✓	✓	✓
> NVD CVE-2021-45046	5.1 Medium	New	CWE-502	-	-	-
> BDSA BDSA-2021-3817 (CVE-2021-45105)	3.9 Low	New	CWE-835	✓	✓	✓

4 new vulnerabilities found in Apache Log4j 2.14.1 affecting devops.lab.postgres 1.0.0-SNAPSHOT 7:30 AM

Vulnerabilities updated in Spring Framework 5.3.10 affecting devops.lab.postgres 1.0.0-SNAPSHOT Jan 25, 2022


Vulnerabilities updated in Spring Framework 5.3.10 affecting devops.lab.postgres 1.0.0-SNAPSHOT Jan 25, 2022

Vulnerabilities updated in Spring Framework 5.3.10 affecting devops.lab.postgres 1.0.0-SNAPSHOT Jan 25, 2022

See All Notifications

https://10.166.16.8:30443/api/projects/7e7186bc-a2cb-488b-98e4-1de873b298d3/versions/252201d8-8888-412f-9719-4347332337d9/vulnerability-bom?selectedItem=6b7ce8de-63f4-42a0-b8be-973711d4ead6&q=Apache Log4j#erved.

Black Duck DEMO

 + Create Project 73 System

Black Duck Projects
devops.lab.postgres ▸ 1.0.0-SNAPSHOT

Project ☆ | Phase: In Development | Scans: Up to Date | Status: Up to Date

Components Security Source Reports Details Settings

Security Risk

Number of Unique Component Origins

Critical 0 High 0 Medium 16 Low 6

Apache Log4j × Add Filter

Components

Apache Log4j 2.14.1
github: apache/logging-log4j2:rel/2.14.1

Vulnerabilities 2 2

Apache Log4j 2.14.1

github: apache/logging-log4j2:rel/2.14.1

4 Known Vulnerabilities

Short Term Upgrade Recommendation 2.17.1
Long Term Upgrade Recommendation 2.17.1

Identifier	Overall Score	Status	CWE	Exploit	Workaround	Solution
> BDSA BDSA-2021-3731 (CVE-2021-44228) ⚠️ RCE	6.5 Medium	New	CWE-502	✓	✓	✓
> NVD CVE-2021-45046	5.1 Medium	New	CWE-502	-	-	-
> BDSA BDSA-2021-3817 (CVE-2021-45105)	3.9 Low	New	CWE-835	✓	✓	✓

Displaying 1-1 of 1

BLACK DUCK v2021.10.0 | Notices

© 2021 Synopsys, Inc. All rights reserved.

Black Duck DEMO

SYNOPSYS

Search...

+ Create Project



System

Dashboard

Find

Scans

Reports

Manage

Admin



logging.apache.org
Apache Log4j ▾ 2.14.1

java Versions: 194

Security

Copyrights

Details

Settings

Filter Vulnerabilities...

Remote Code Execution

This vulnerability allows an attacker to remotely execute arbitrary code.

Identifier

Published

Overall Score ▾

▼ **BDSA** BDSA-2021-3731 (CVE-2021-44228) ⚠ **RCE**

Dec 10, 2021

6.5 Medium

Description

Apache Log4j, as used in many popular services, is vulnerable to improperly allowing lightweight directory access protocol (LDAP) access via Java naming and directory interface (JNDI). A remote attacker able to supply the end application with specially crafted input that is then processed by the Log4j subcomponent could cause the execution of arbitrary Java code.

Note

- log4j-api packages by themselves do not contain the vulnerable functionality and are therefore unaffected. log4j-core packages and the upstream overarching source repository are affected.
- A previously suggested mitigation of setting environment

Base Score Metrics (CVSS v2 Metrics)

AV NETWORK	A PARTIAL
AC LOW	C PARTIAL
Au NONE	I PARTIAL

Published on Dec 10, 2021

Last Modified Jan 12, 2022

Black Duck DEMO

SYNOPSYS

Search...

+ Create Project

259

System

logging.apache.org

Apache Log4j ▾ 2.14.1

java Versions: 194

Security Copyrights Details Settings

Description
No description.

Released	Newer Versions	Approval Status	Updated
Mar 7, 2021	24	Unreviewed	Jan 27, 2022

Activity
Last 12 Months: **1092 commits** ↑ increasing
Last Commit: Jan 27, 2022

Community
Last 12 Months: **53 contributors**

Where Used

Project	Version	Released	Phase
devops.lab.postgres	1.0.0-SNAPSHOT	Never	In Development
Mobile	1.0	Never	Deprecated
profiles	v2.0.0.2	Never	In Development
Reconciliation	1.0	Never	In Planning

Displaying 1-4 of 4

4 Vulnerabilities

Licenses
Apache License 2.0

Open Hub
<https://www.openhub.net/p/598518>

Component Links
<http://logging.apache.org/log4j/>

Tags
analysis apache java log log4j logging

Dashboard

Find

Scans

Reports

Manage

Admin

Is this world really imaginary?

- You know all the projects that are using the library
- You know the precise version you are using in each project
- You know the path where you can find the library in each project
- Before the news goes public and it is known by all, you have received an email addressed only to you, as the owner of a project in which the Log4j library is present, with the details of the new vulnerability and the indications to remedy immediately.

We just need to make it happen!

NTT DATA

THANK YOU

**AGILE/
DEVOPS
GLOBAL
CONFERENCE**

