SAND2022-6887C

CVE®

Common Vulnerabilities and Exposures

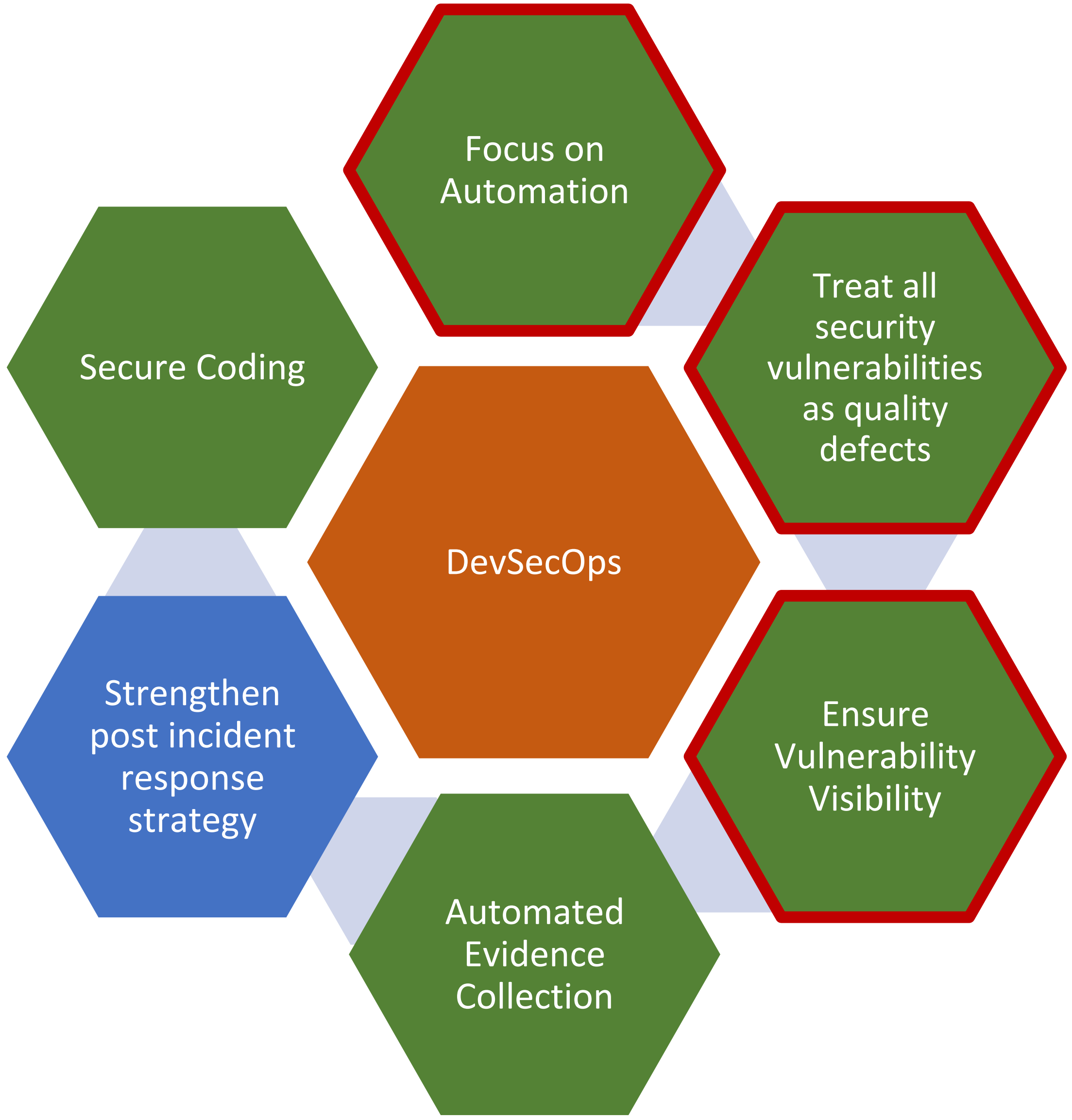
LOG4J

DON'T
PANIC
AND
CARRY A
TOWEL

Through the use of a software Bill-of-Materials and third-party library tracking, it is possible to leverage the CI/CD system to quickly address CVEs that occur in the software supply-chain.

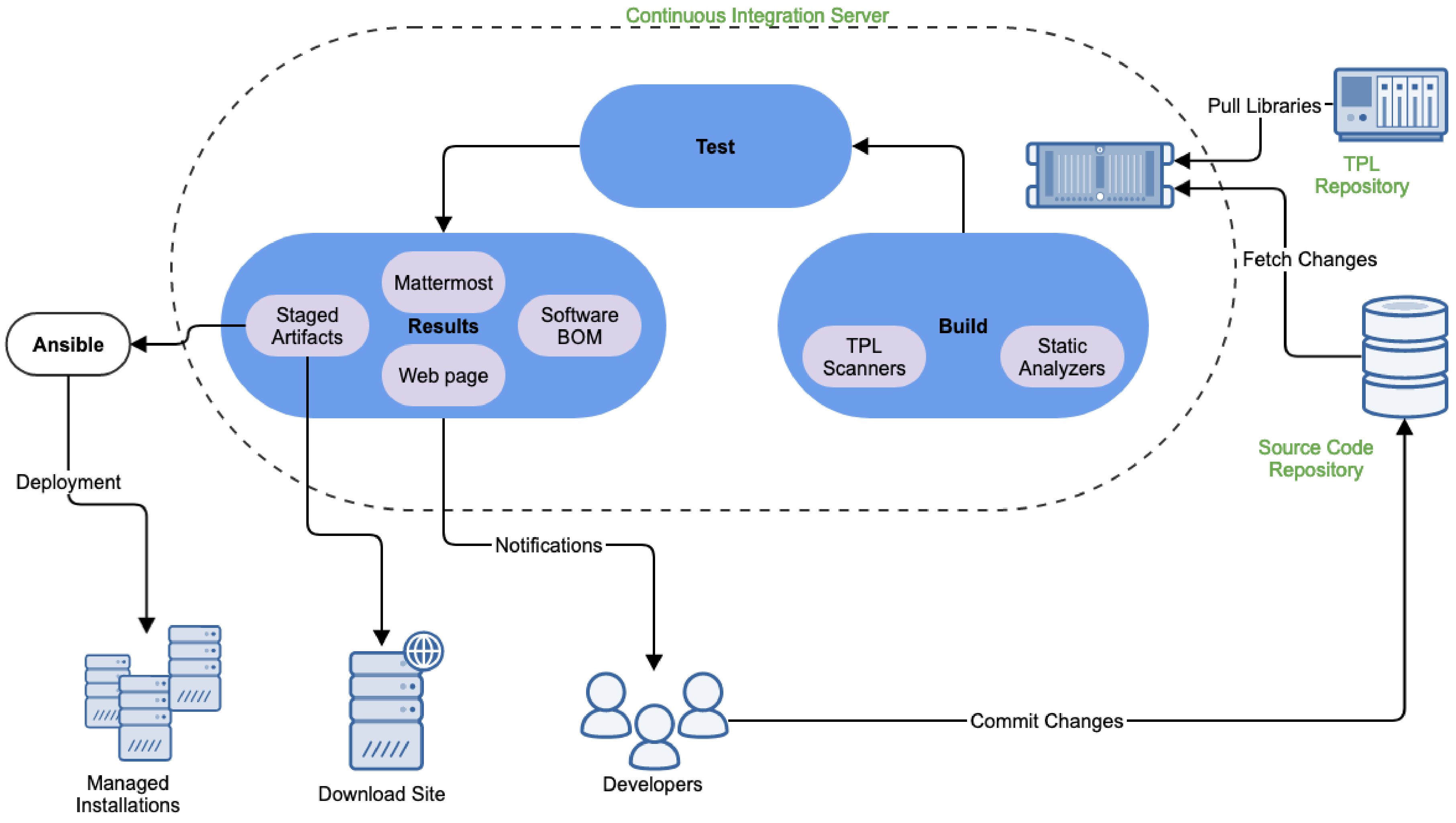
- Software BOM
- CI/CD
- Third Party Library Repository
- Third Party Library Scanning

DevSecOps

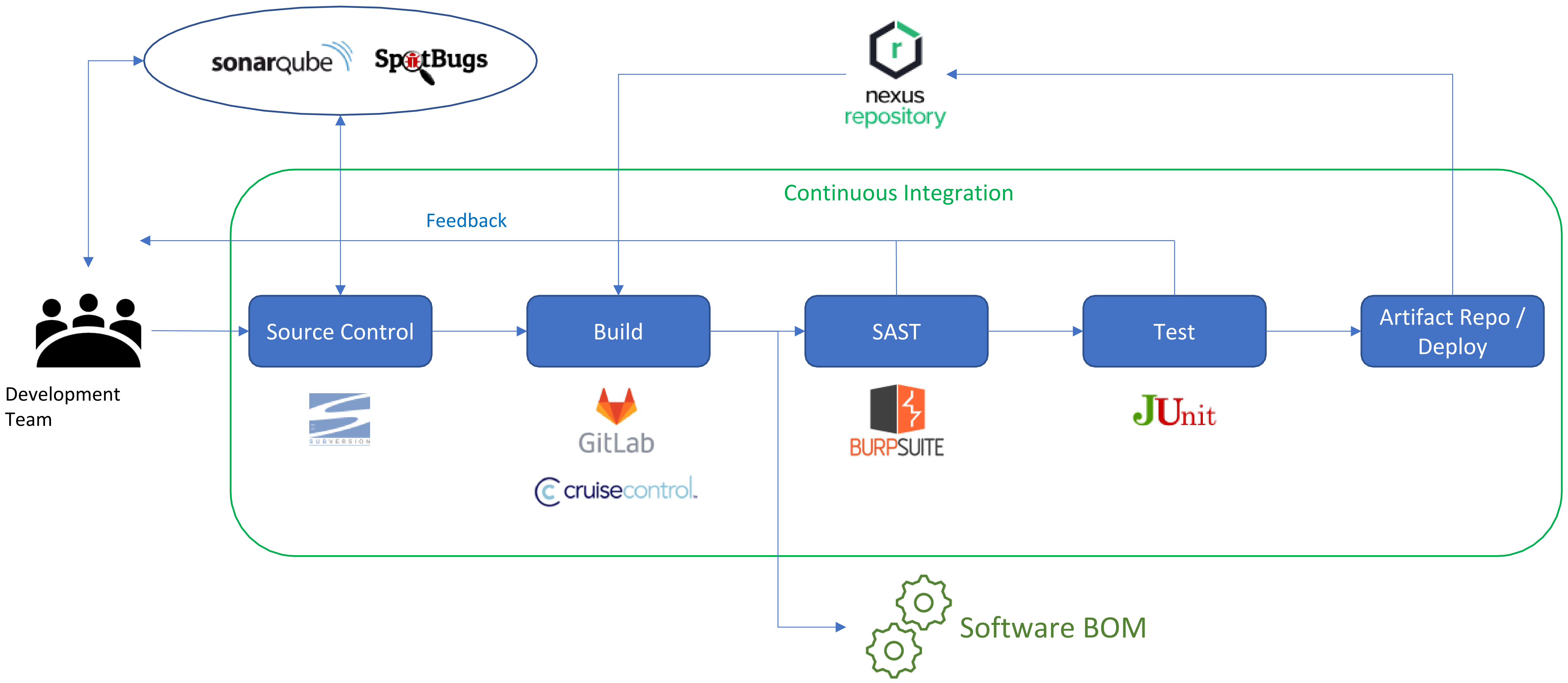

Focus on Automation
Secure Coding
Treat all security vulnerabilities as quality defects
DevSecOps
Strengthen post incident response strategy
Ensure Vulnerability Visibility
Automated Evidence Collection

Adapted from N. Radzuan (2022), *From DevOps to DevSecOps*

Basic SAW CI/CD

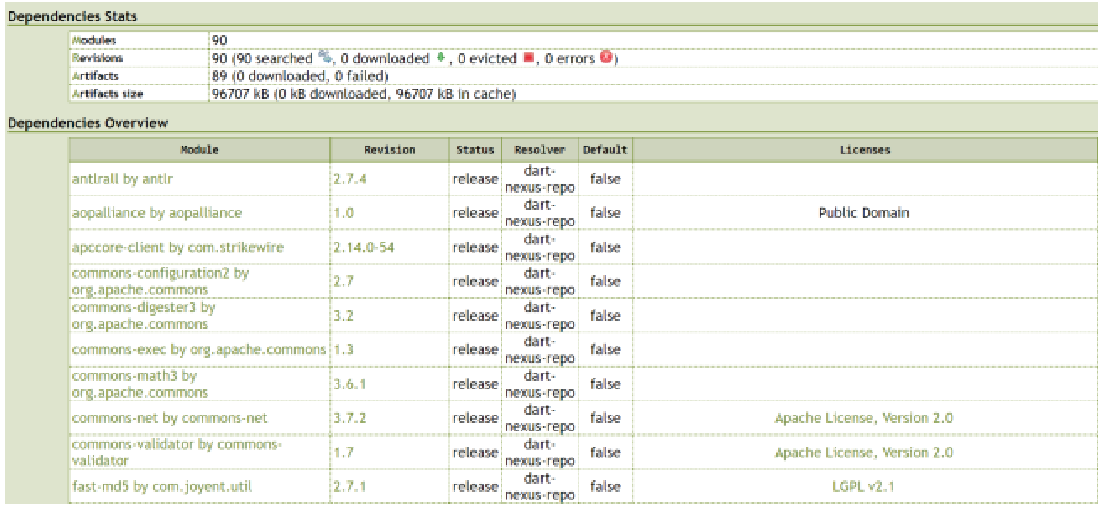


Pipeline View



An SBOM is a complete inventory of a codebase including the open source components, the license and version information for those open source components, and whether there are any known vulnerabilities in those components.

Third-Party Library SBOM Examples



Dependencies Stats

Modules	90
Revisions	90 (90 searched, 0 downloaded, 0 evicted, 0 errors)
Artifacts	89 (0 downloaded, 0 failed)
Artifacts size	96707 kB (0 kB downloaded, 96707 kB in cache)

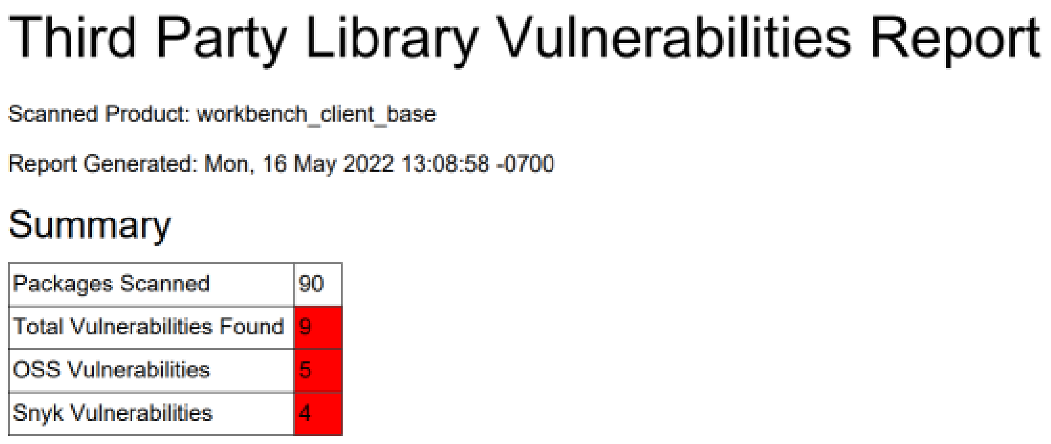
Dependencies Overview

Module	Revision	Status	Resolver	Default	Licenses
antlrall by antlr	2.7.4	release	dart-nexus-repo	false	
aopalliance by aopalliance	1.0	release	dart-nexus-repo	false	Public Domain
apccore-client by com.strikewire	2.14.0-54	release	dart-nexus-repo	false	
commons-configuration2 by org.apache.commons	2.7	release	dart-nexus-repo	false	
commons-digester3 by org.apache.commons	3.2	release	dart-nexus-repo	false	
commons-exec by org.apache.commons	1.3	release	dart-nexus-repo	false	
commons-math3 by org.apache.commons	3.6.1	release	dart-nexus-repo	false	
commons-net by commons-net	3.7.2	release	dart-nexus-repo	false	Apache License, Version 2.0
commons-validator by commons-validator	1.7	release	dart-nexus-repo	false	Apache License, Version 2.0
fast-md5 by com.joyent.util	2.7.1	release	dart-nexus-repo	false	LGPL v2.1

```
+--- com.google.code.gson:gson:2.8.7
+--- org.apache.commons:commons-lang3:3.12.0
+--- org.apache.commons:commons-math3:3.6.1
+--- org.springframework.boot:spring-boot-starter-web -> 2.6.1
|    +--- org.springframework.boot:spring-boot-starter:2.6.1
|    |    +--- org.springframework.boot:spring-boot:2.6.1
|    |    |    +--- org.springframework:spring-core:5.3.13
|    |    |    |    \--- org.springframework:spring-jcl:5.3.13
|    |    |    |    \--- org.springframework:spring-context:5.3.13
|    |    |         +--- org.springframework:spring-aop:5.3.13
|    |    |         |    +--- org.springframework:spring-beans:5.3.13
|    |    |         |    |    \--- org.springframework:spring-core:5.3.13 (*)
|    |    |         |    \--- org.springframework:spring-core:5.3.13 (*)
|    |    |         +--- org.springframework:spring-beans:5.3.13 (*)
|    |    |         +--- org.springframework:spring-core:5.3.13 (*)
|    |    |         \--- org.springframework:spring-expression:5.3.13
|    |    |              \--- org.springframework:spring-core:5.3.13 (*)
|    |    +--- org.springframework.boot:spring-boot-autoconfigure:2.6.1
|    |    |    \--- org.springframework.boot:spring-boot:2.6.1 (*)
|    |    +--- org.springframework.boot:spring-boot-starter-logging:2.6.1
|    |    |    +--- ch.qos.logback:logback-classic:1.2.7
|    |    |    |    +--- ch.qos.logback:logback-core:1.2.7
|    |    |    |    \--- org.slf4j:slf4j-api:1.7.32
|    |    |    +--- org.apache.logging.log4j:log4j-to-slf4j:2.14.1
|    |    |    |    +--- org.slf4j:slf4j-api:1.7.25 -> 1.7.32
|    |    |    |    \--- org.apache.logging.log4j:log4j-api:2.14.1
|    |    |    \--- org.slf4j:jul-to-slf4j:1.7.32
|    |    |         \--- org.slf4j:slf4j-api:1.7.32
|    |    +--- jakarta.annotation:jakarta.annotation-api:1.3.5
|    |    +--- org.springframework:spring-core:5.3.13 (*)
|    |    \--- org.yaml:snakeyaml:1.29

…
```

Third Party Library Visibility Reporting

PDF Report



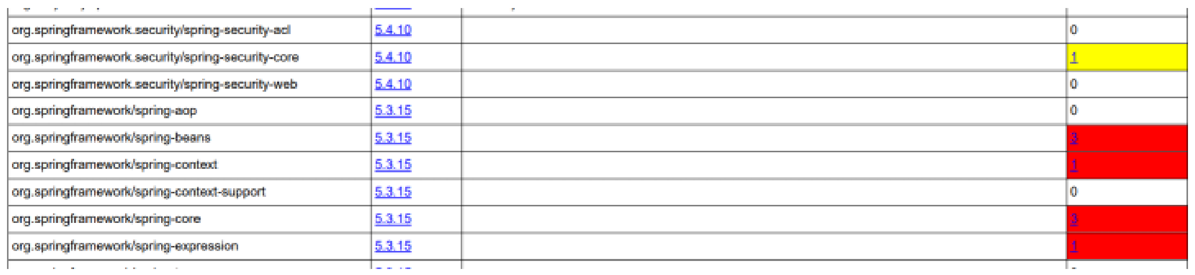
Third Party Library Vulnerabilities Report

Scanned Product: workbench_client_base

Report Generated: Mon, 16 May 2022 13:08:58 -0700

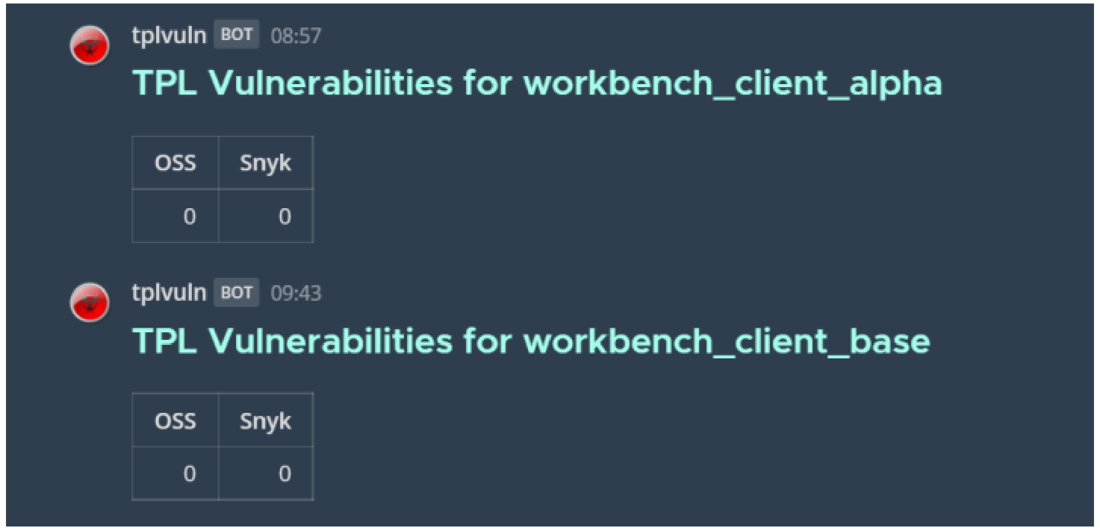
Summary

Packages Scanned	90
Total Vulnerabilities Found	9
OSS Vulnerabilities	5
Snyk Vulnerabilities	4



org.springframework.security/spring-security-acl	5.4.10		0
org.springframework.security/spring-security-core	5.4.10		1
org.springframework.security/spring-security-web	5.4.10		0
org.springframework/spring-aop	5.3.15		0
org.springframework/spring-beans	5.3.15		3
org.springframework/spring-context	5.3.15		1
org.springframework/spring-context-support	5.3.15		0
org.springframework/spring-core	5.3.15		3
org.springframework/spring-expression	5.3.15		1

Mattermost Postings



tplvuln BOT 08:57

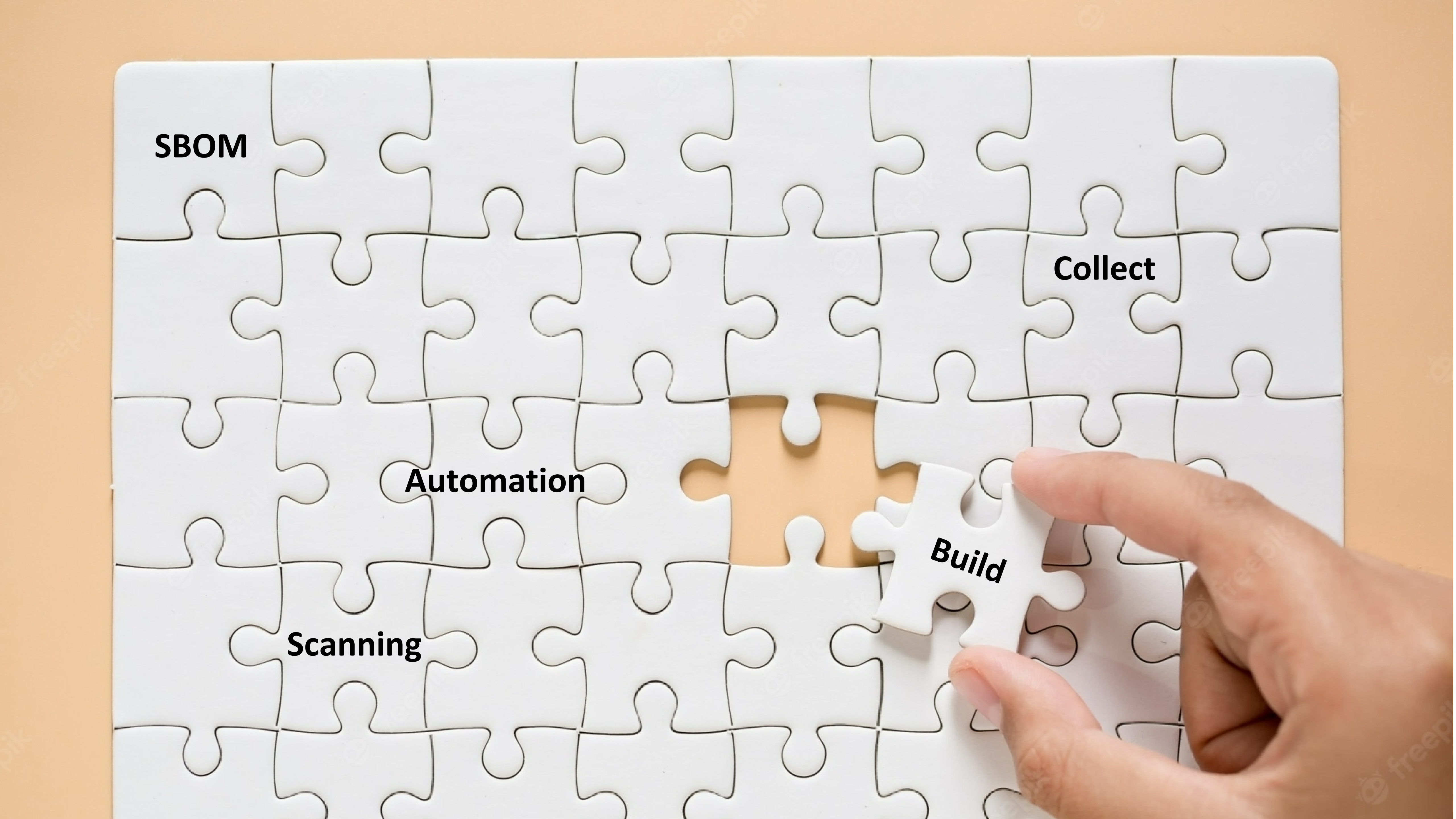
TPL Vulnerabilities for workbench_client_alpha

OSS	Snyk
0	0

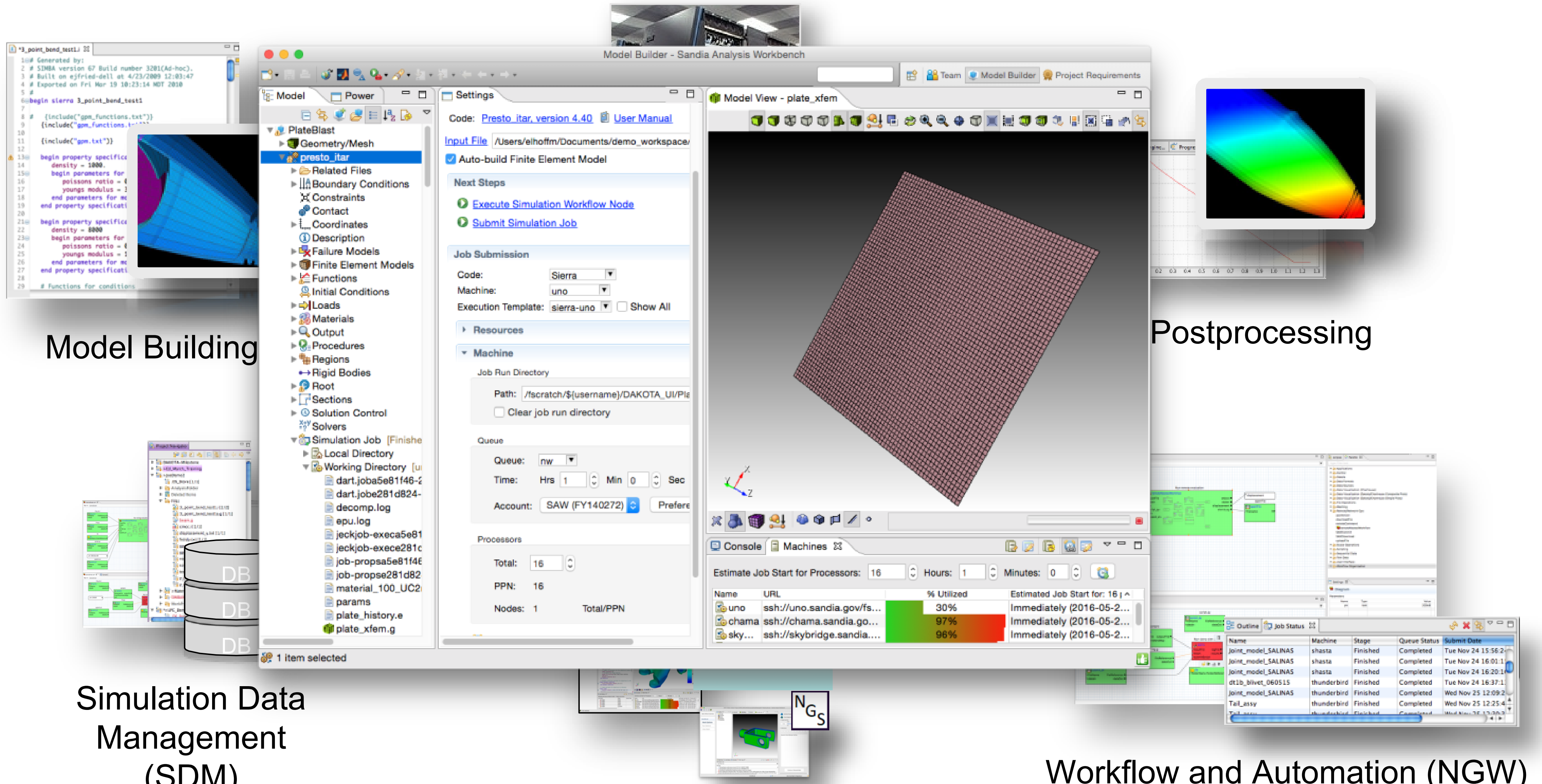
tplvuln BOT 09:43

TPL Vulnerabilities for workbench_client_base

OSS	Snyk
0	0


SBOM
Collect
Automation
Build
Scanning

SAW: A Comprehensive Toolkit for Modeling and Simulation



Model Builder - Sandia Analysis Workbench

Team | Model Builder | Project Requirements

Model | Power

- PlateBlast
  - Geometry/Mesh
  - presto_itar
    - Related Files
    - Boundary Conditions
    - Constraints
    - Contact
    - Coordinates
    - Description
    - Failure Models
    - Finite Element Models
    - Functions
    - Initial Conditions
    - Loads
    - Materials
    - Output
    - Procedures
    - Regions
    - Rigid Bodies
    - Root
    - Sections
    - Solution Control
    - Solvers
    - Simulation Job [Finishe
      - Local Directory
      - Working Directory [u
        - dart.jobaa5e81f46-2
        - dart.jobe281d824-
        - decomp.log
        - epu.log
        - jeckjob-execa5e81
        - jeckjob-exece281c
        - job-propsa5e81f4€
        - job-propse281d82
        - material_100_UC2
        - params
        - plate_history.e
        - plate_xfem.g

Settings

Code: Presto_itar, version 4.40 | User Manual

Input File: /Users/elhoffm/Documents/demo_workspace/

Auto-build Finite Element Model

Next Steps

- Execute Simulation Workflow Node
- Submit Simulation Job

Job Submission

Code: Sierra

Machine: uno

Execution Template: sierra-uno | Show All

Resources

Machine

Job Run Directory

Path: /fscratch/${username}/DAKOTA_UI/Pla

Clear job run directory

Queue

Queue: nw

Time: Hrs 1 Min 0 Sec

Account: SAW (FY140272) | Prefere

Processors

Total: 16

PPN: 16

Nodes: 1 Total/PPN

Model View - plate_xfem

Console | Machines

Estimate Job Start for Processors: 16 Hours: 1 Minutes: 0

Name	URL	% Utilized	Estimated Job Start for: 16
uno	ssh://uno.sandia.gov/fs...	30%	Immediately (2016-05-2...
chama	ssh://chama.sandia.go...	97%	Immediately (2016-05-2...
sky...	ssh://skybridge.sandia....	96%	Immediately (2016-05-2...

1 item selected

Model Building

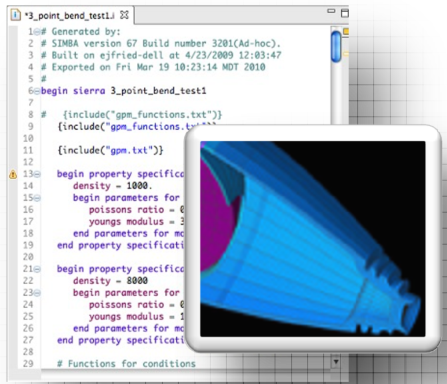
Postprocessing

Simulation Data Management (SDM)

Integration Platform

Workflow and Automation (NGW)

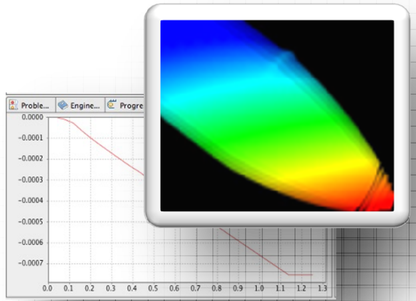
SAW: A Comprehensive Toolkit for Modeling and Simulation



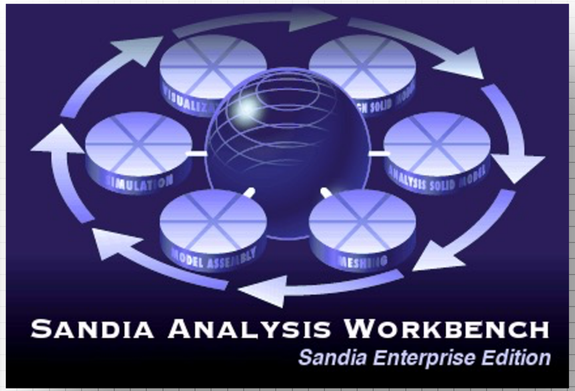
```
*3_point_bend_test1.i
# Generated by:
# SIMBA version 67 Build number 3201(Ad-hoc).
# Built on ejfried-dell at 4/23/2009 12:03:47
# Exported on Fri Mar 19 10:23:14 MDT 2010
#
begin sierra 3_point_bend_test1

#   {include("gpm_functions.txt")}
   {include("gpm_functions.t

   {include("gpm.txt")}

   begin property specifica
      density = 1000.
      begin parameters for
         poissons ratio = 0
         youngs modulus = 3
      end parameters for mo
   end property specificati

   begin property specifica
      density = 8000
      begin parameters for
         poissons ratio = 0
         youngs modulus = 1
      end parameters for mo
   end property specificati

   # Functions for conditions
```

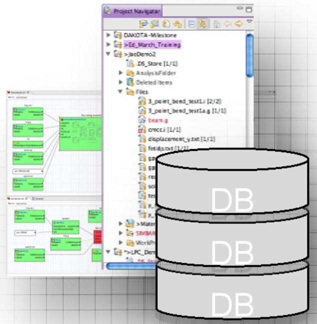
Model Building

Job Submission

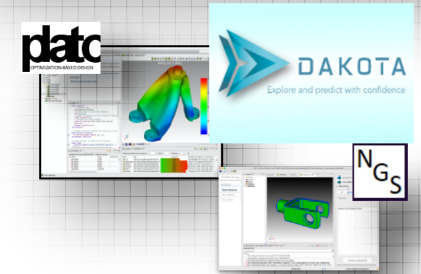


Postprocessing

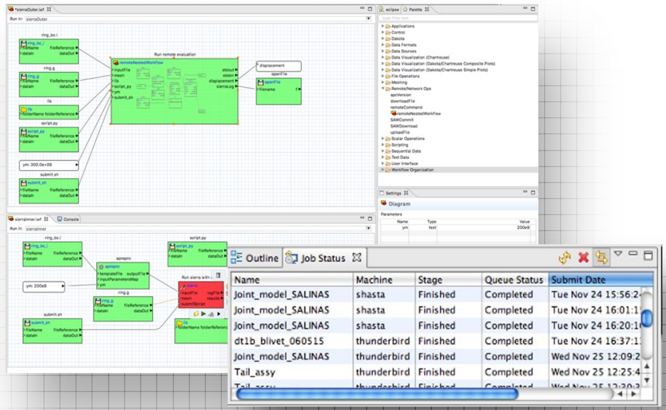




Data and Process Management (SDM)



Integration Platform



Outline | Job Status

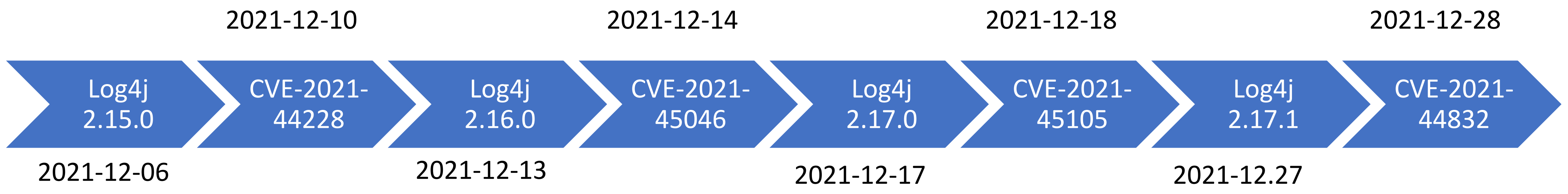
Name	Machine	Stage	Queue Status	Submit Date
Joint_model_SALINAS	shasta	Finished	Completed	Tue Nov 24 15:56:2
Joint_model_SALINAS	shasta	Finished	Completed	Tue Nov 24 16:01:1
Joint_model_SALINAS	shasta	Finished	Completed	Tue Nov 24 16:20:1
dt1b_blivet_060515	thunderbird	Finished	Completed	Tue Nov 24 16:37:1
Joint_model_SALINAS	thunderbird	Finished	Completed	Wed Nov 25 12:09:2
Tail_assy	thunderbird	Finished	Completed	Wed Nov 25 12:25:4

Workflow and Automation (NGW)

What is CVE-2021-44228

- Essentially, an injection-based attack that allowed for remote code execution
- At its base, allowed exploiting JNDI to load arbitrary code, and the recursive resolution of the formatting strings enabled the exploit
- Though it clearly occurred in the supply-chain, it was **not** a supply-chain attack
- Within just 24 hours, almost 200,000 attempted attacks; 72 hours, 800,000 attacks

Public Timeline log4j Updates



Identify the Products

With the SBOM, easy to identify the particular products.

In theory.

Though the SBOM had the information, there was not a central search for the SBOM contents.

But find and grep are our friends.

Build (and rebuild) and Publish

For the identified products, execute the standard approach.

Update the library version reference & commit.

Allow branch to build and scan.

Merge, build, and release.

Easy-peasy.

Except for high-side networks, COVID Restrictions, and the multiple log4j updates…

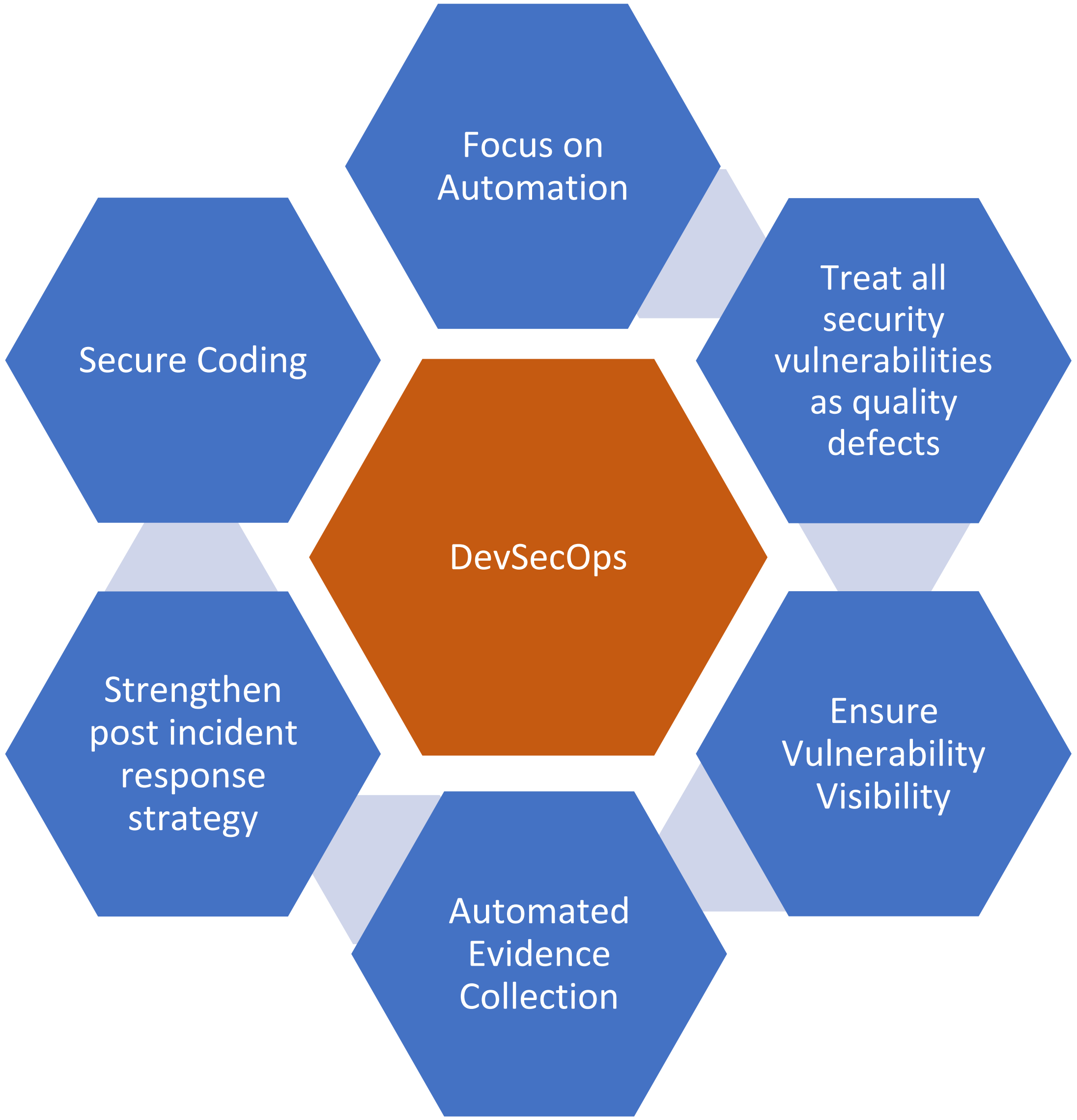
Work with Others

Communicate with and update platform partners.

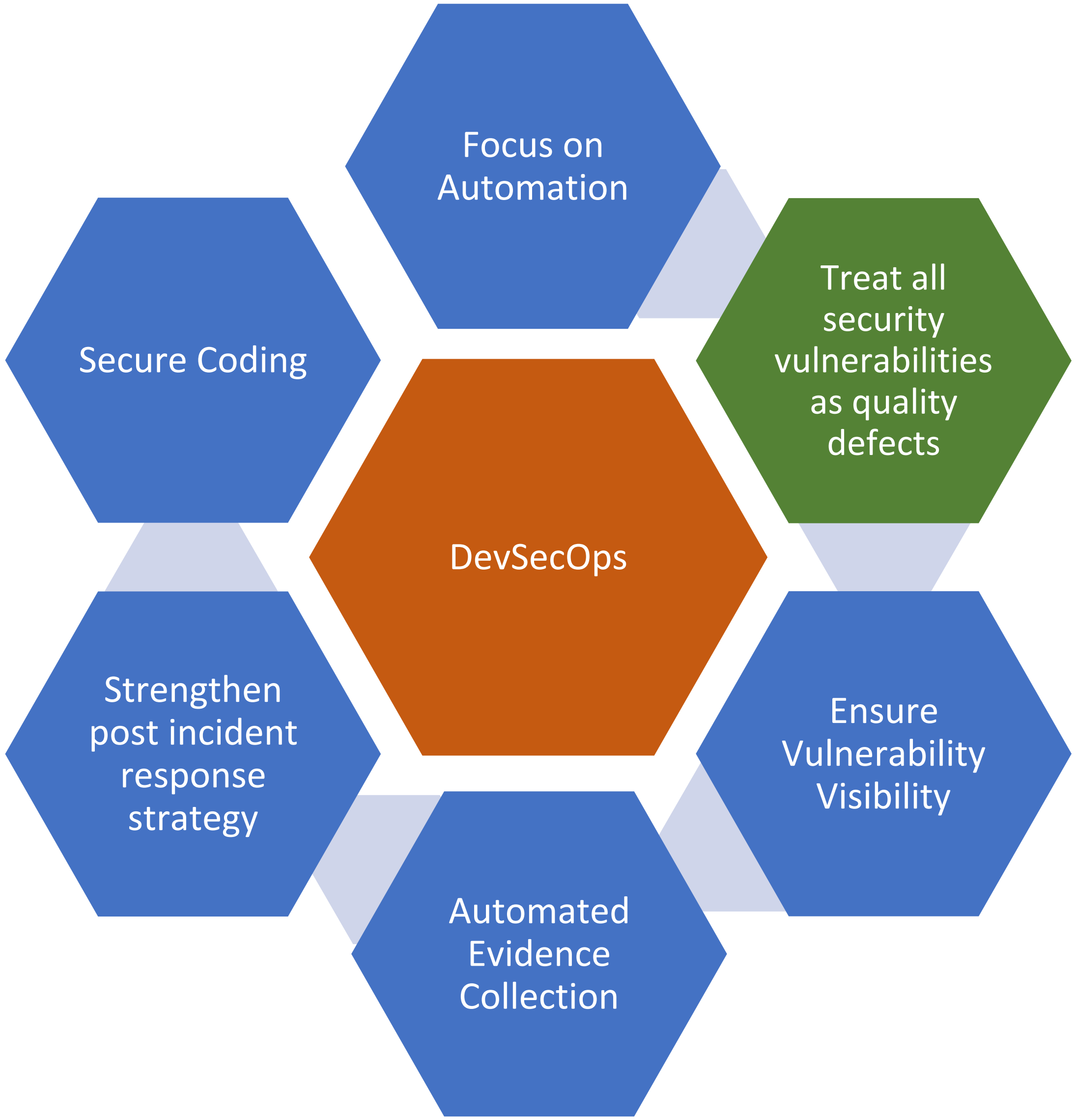
Coordinate with external customers.

Pro-active identification and releases allowed zero -friction between our DevOps and security scanning.

Software BOM Benefits Summary

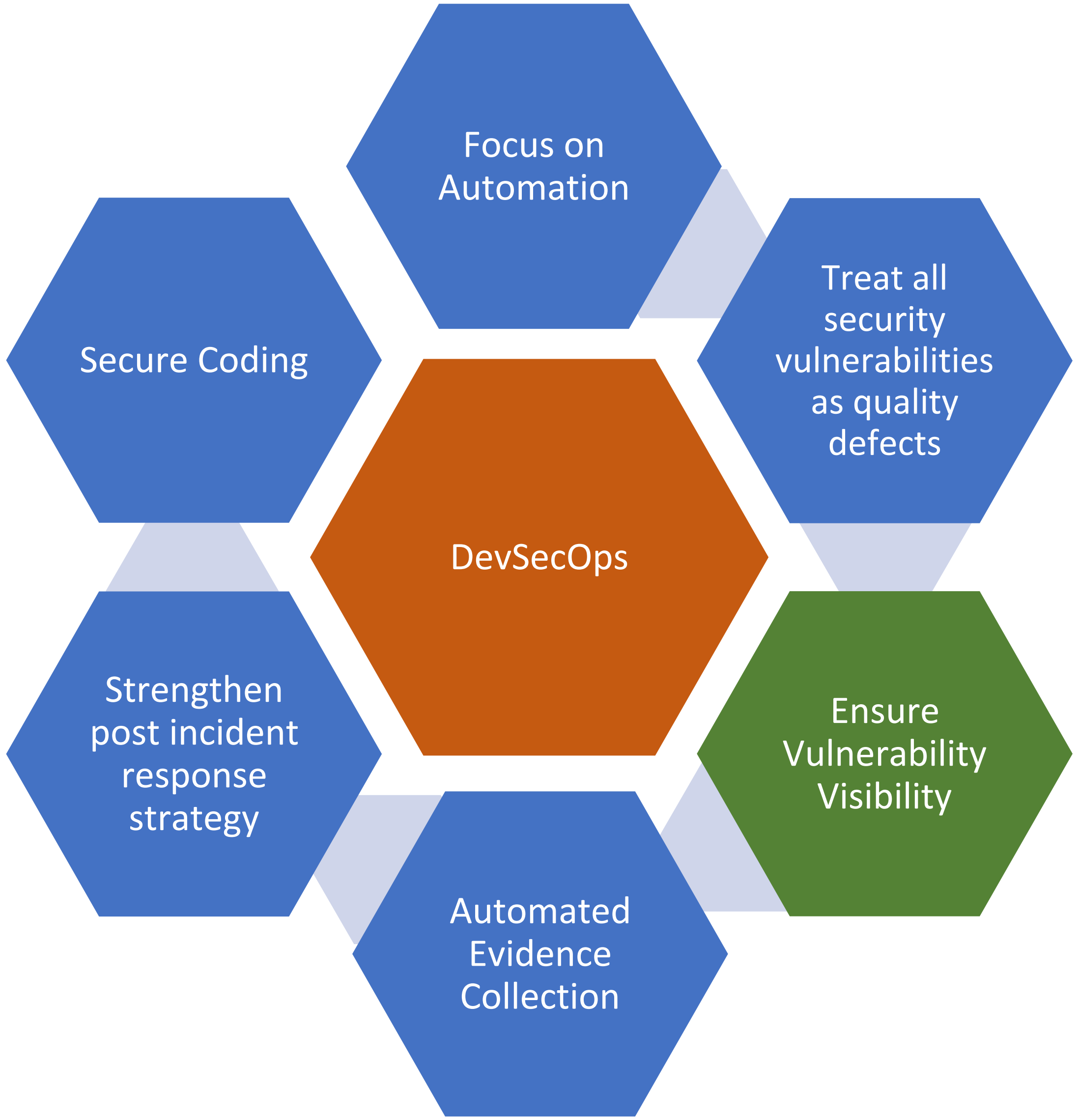

Focus on Automation
Secure Coding
Treat all security vulnerabilities as quality defects
DevSecOps
Strengthen post incident response strategy
Ensure Vulnerability Visibility
Automated Evidence Collection

Software BOM Benefits Summary


Focus on Automation
Secure Coding
Treat all security vulnerabilities as quality defects
DevSecOps
Strengthen post incident response strategy
Ensure Vulnerability Visibility
Automated Evidence Collection

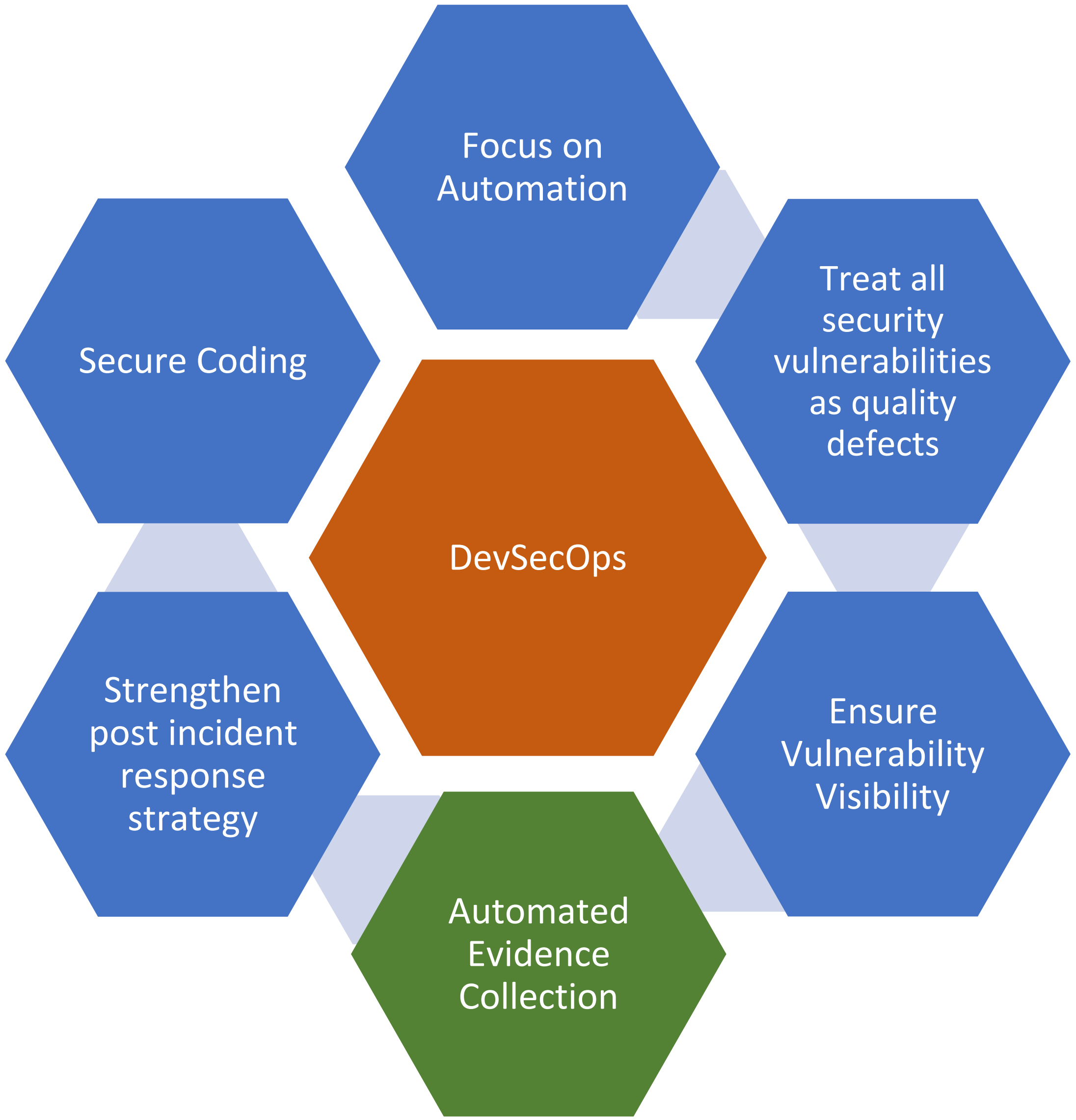
The SBOM allows for build system to flag Third-party library issues and fail builds.

Software BOM Benefits Summary


Focus on Automation
Secure Coding
Treat all security vulnerabilities as quality defects
DevSecOps
Strengthen post incident response strategy
Ensure Vulnerability Visibility
Automated Evidence Collection

The SBOM supports visibility by integrating with multiple alerting systems.

Software BOM Benefits Summary


Focus on Automation
Secure Coding
Treat all security vulnerabilities as quality defects
DevSecOps
Strengthen post incident response strategy
Ensure Vulnerability Visibility
Automated Evidence Collection

The SBOM provides evidence of the as-built configuration with versions, licensing, and vulnerability reporting.

Lessons Learned

Vulnerable installations from pre -SBOM days can keep popping up

Messaging about vulnerabilities demands care

Elasticsearch or similar would be helpful

Having an SBOM helps you reduce attack surface by consolidating usage of similar libraries in different parts of a large codebase

Fixing bugs found by static analysis demands the same care as fixing any other bugs