OpenSouthCode Málaga – 9 June 2023

Jorge Hidalgo
@deors314
in/deors

DevSecOps Mythbusters

Detecting security vulnerabilities in and beyond CI/CD pipelines – "Open-Source Edition"

ABOUT ME

JORGE HIDALGO

@deors314

in/deors

Associate Director – Software Engineering Group – Accenture Spain

Global Java Community of Practice co-lead

Spain Cloud First DevOps lead

Spain Adv. Tech. Center Cloud First Architecture & DevOps & Cloud lead

Communities matter: ***MálagaJUG*** */* ***Málaga Scala Developers*** */* ***BoquerónSec co-lead***

Co-organizer: ***OpenSouthCode Málaga***

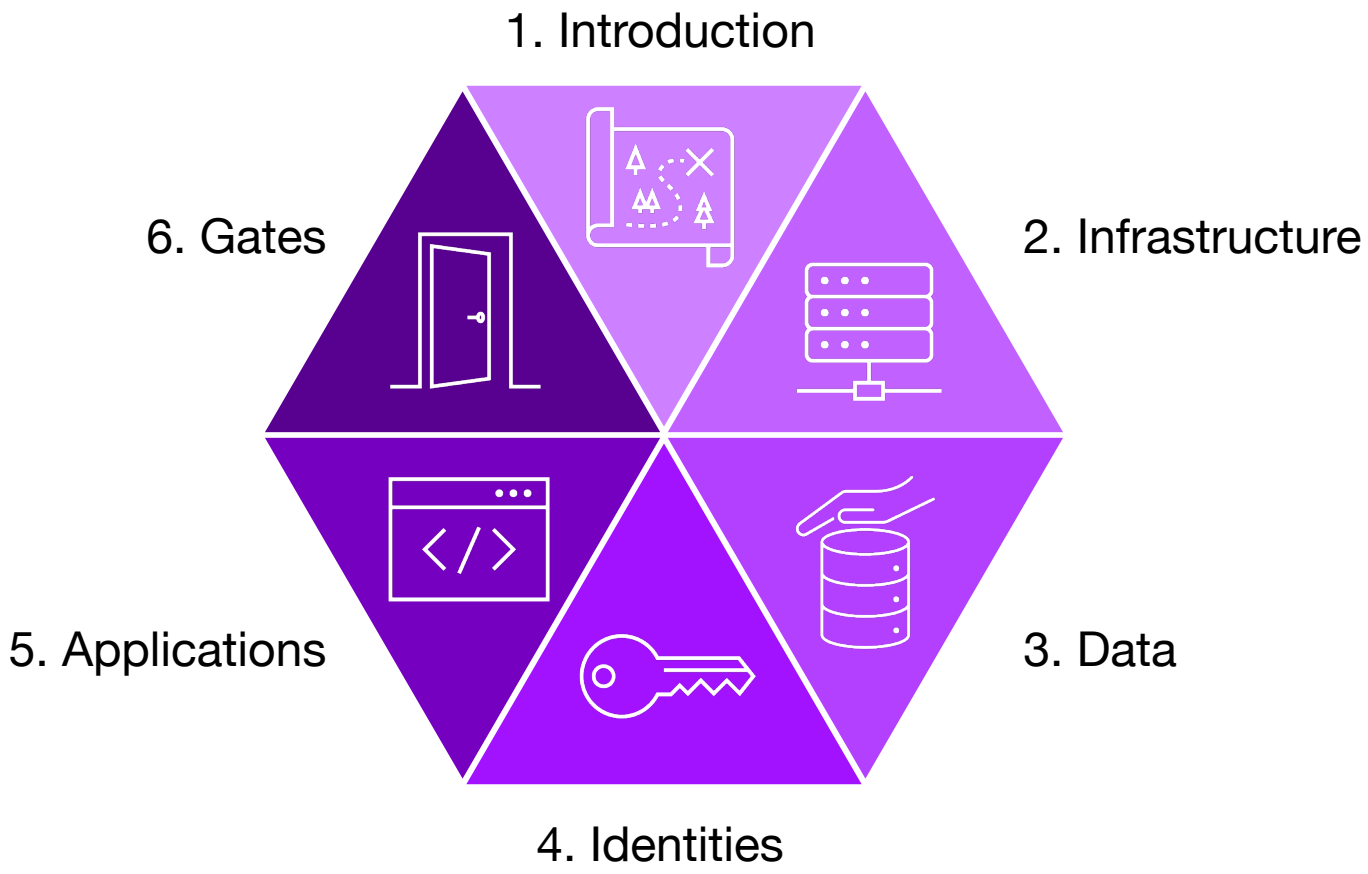
*Father of two, husband, whistle player, video gamer, sci-fi *.*, Lego, Raspberry Pi,*
Star Wars, Star Trek, LOTR, Halo, Borderlands, Watch Dogs, Diablo, StarCraft, Black Desert,… LLAP!

MÁLAGAJUG JAVA USER GROUP

Málaga Scala Developers

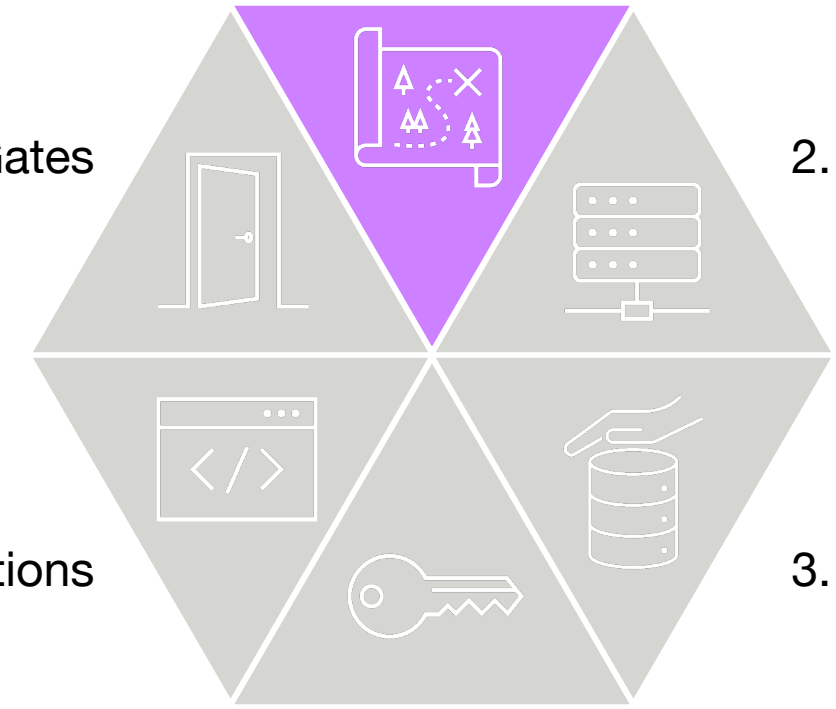
open south code

AGENDA


1. Introduction
2. Infrastructure
3. Data
4. Identities
5. Applications
6. Gates

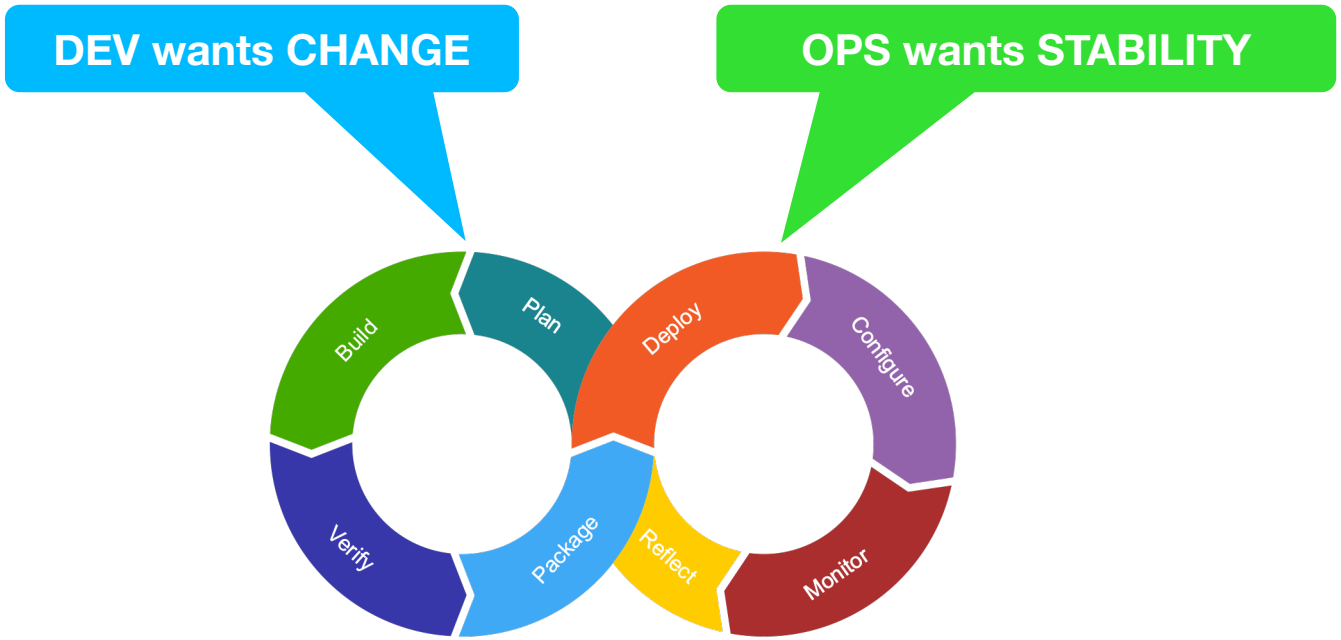
AGENDA

1. Introduction
2. Infrastructure
3. Data
4. Identities
5. Applications
6. Gates



DevSecOps == DevOps

<< DevOps is not possible unless security practices are adopted >>



But…, what does SECURITY want?

(let's not promote stereotypes ☺)


LUMINOUS BEINGS ARE WE

DEV(SEC)OPS "DRAMATIS PERSONAE"

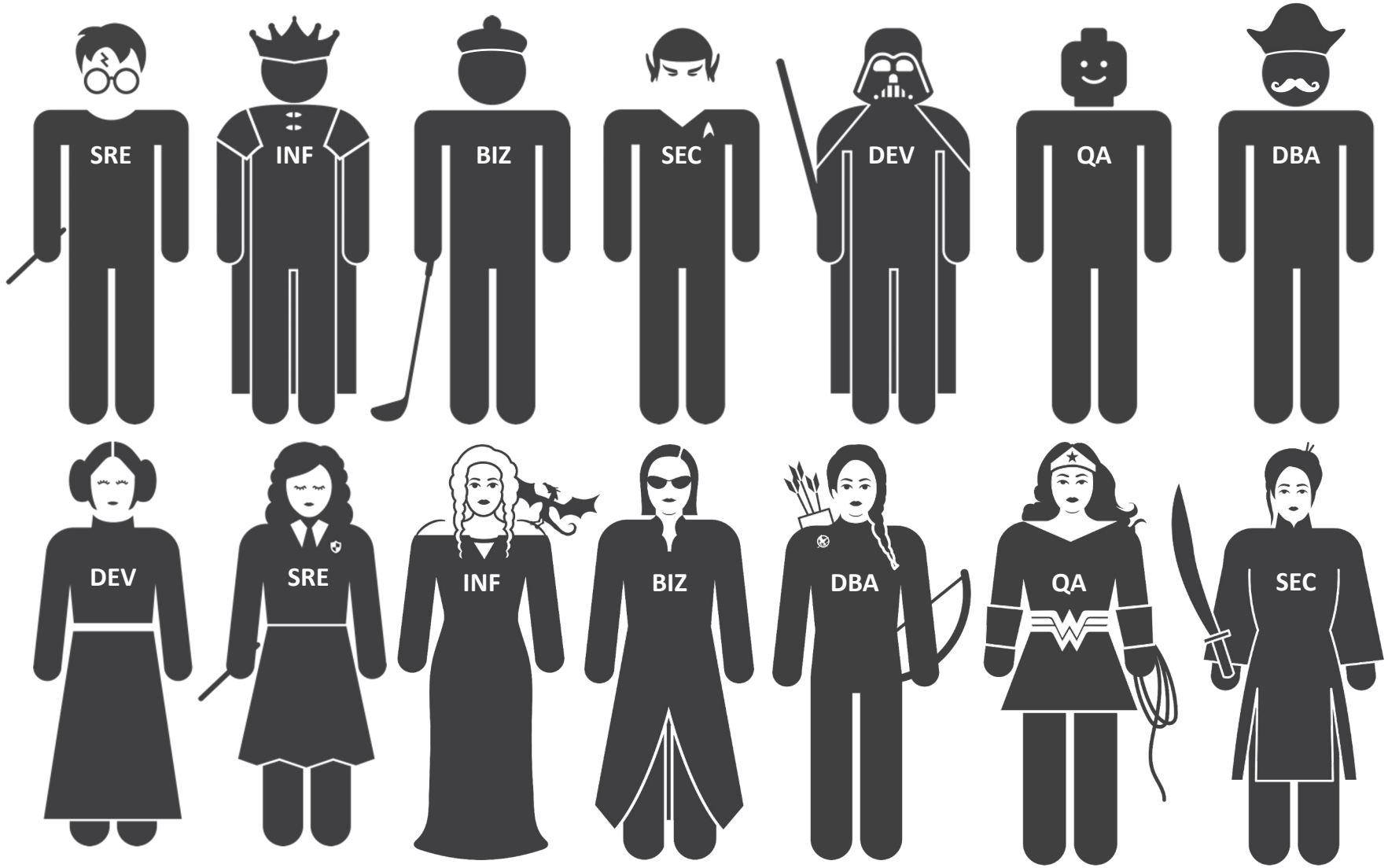
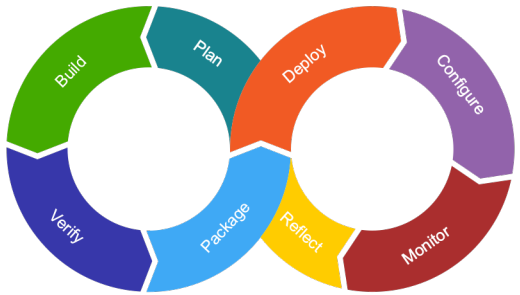
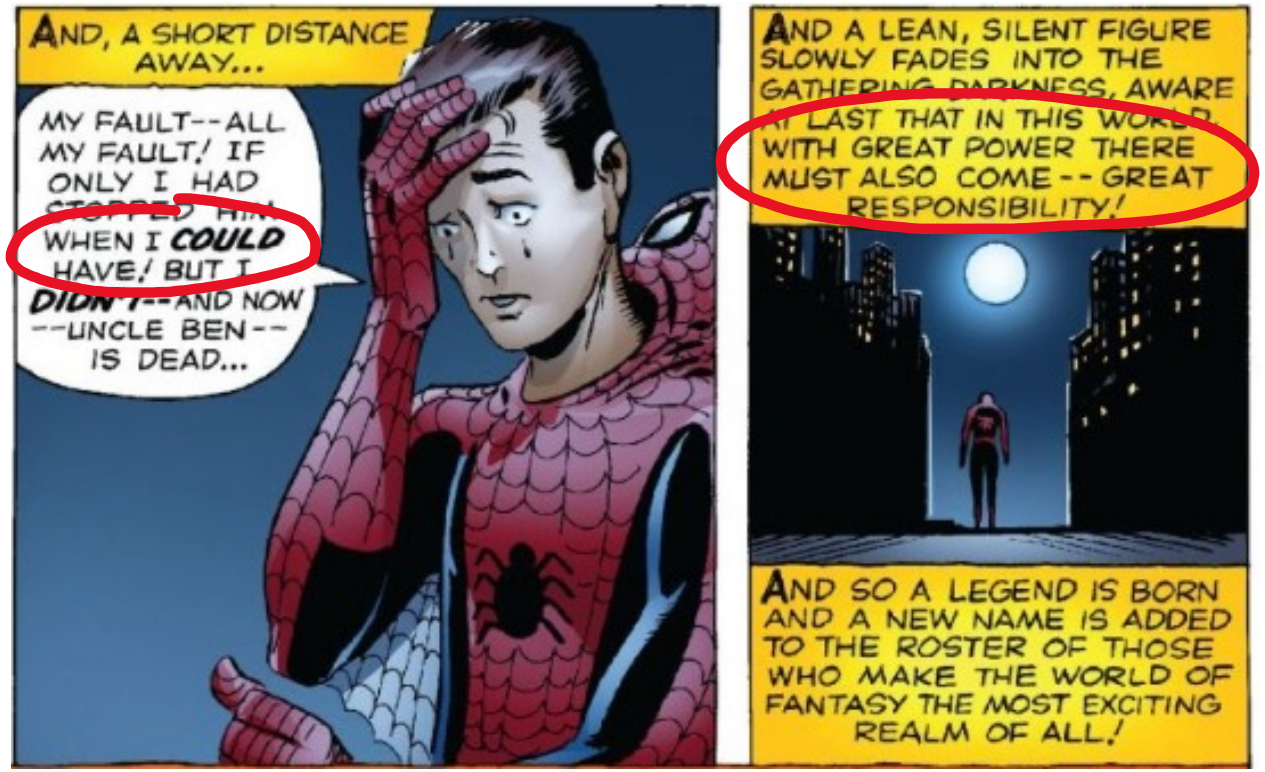


Image adapted from Burr Sutter's "8 Steps to Becoming Awesome with Kubernetes"

SPIDER-MAN "INVENTED" DEV(SEC)OPS ☺





DEV(SEC)OPS TEAMS

- Take decisions
- Take ownership
- Measure and improve continuously
- Never asume that someone else with take care

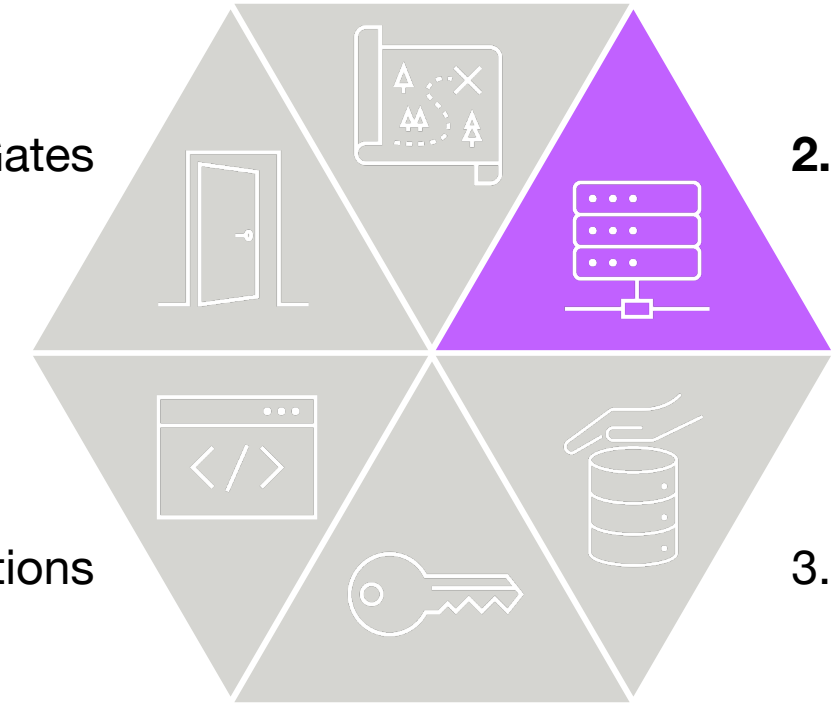
DECISIONS AND OWNERSHIP, BUT, ABOUT WHAT?

- Infrestructure & platform
- Data protection
- Identity and access management
- Application security
- Quality gates

AGENDA

1. Introduction

6. Gates



2. Infrastructure

5. Applications

3. Data

4. Identities

INFRASTRUCTURE & PLATFORM SECURITY

- Hardening
- Periodic patch/upgrade cycles (special attention to EOLs)
- Vulnerability detection powered by tools (vs. manually reviewing the CVE catalog)
- Cloud-native vulnerabilities
- Infrastructure as code vulnerabilities
- Zero-day vulnerabilities

INFRASTRUCTURE & PLATFORM SECURITY

- Of course, end-user computing/infrastructure
  - Access from unsupported/untrusted operating system
  - Access from old browsers (maybe 2-3 version tolerance)
  - Access from rooted/compromised devices

https://www.cve.org/

About | Partner Information | Program Organization | Downloads | Resources & Support | Report/Request

Enter CVE ID (CVE-YYYY-NNNN) Find

Site Search

Find CVE Records by keyword on cve.mitre.org

Welcome to the new CVE Beta website! CVE List keyword search & downloads will be temporarily hosted on the old cve.mitre.org website until we complete the transition. Please use our web form for any comments or concerns.

CVE® Program Mission

Identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

Currently, there are **165,386** CVE Records accessible via **Download** or **Search**

The CVE Program partners with community members worldwide to grow CVE content and expand its usage. Click below to learn more about the role of **CVE Numbering Authorities (CNAs)** and **Roots**.

Learn More | Become a Partner

Access

- List of Partners
- CNA Rules
- CVE Record Information
- CVEProject on Github for Development

Learn

- About CVE
- Process
- Program Organization
- Related Efforts
- Terminology

Report/Request

- Report vulnerability/Request CVE ID
- Request CVE Record be published/updated
- Report the use of a reserved CVE ID

News

- Welcome to the New CVE Program Web Address and Website!
- TeamViewer Added as CVE Numbering Authority (CNA)
- Profelis Added as CVE Numbering Authority (CNA)
- "CVE Global Summit – Fall 2021"

NEWS ICONS

MORE NEWS

Events

CVE Outreach and Communications Working Group (OCWG) Meeting

TOTAL CVE Records: 165419

NOTICE: Transition to the all-new CVE website at www.cve.org is underway and will last up to one year. (details)

Search Results

There are **222** CVE Records that match your search.

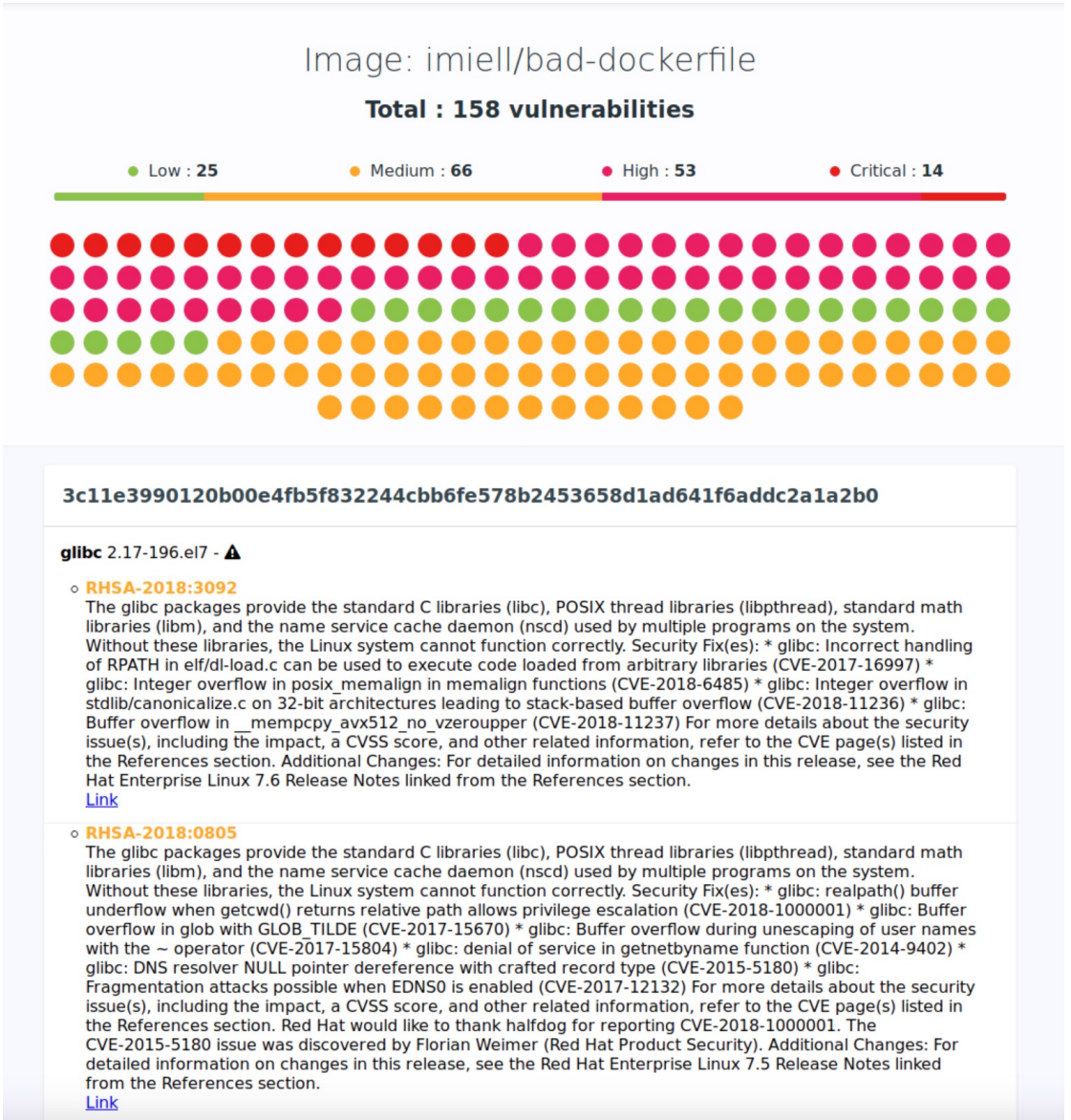
Name	Description
CVE-2021-43800	Wiki.js is a wiki app built on Node.js. Prior to version 2.5.254, directory traversal outside of Wiki.js context is possible when a storage module with local asset cache fetching is enabled on a Windows host. A malicious user can potentially read any file on the file system by crafting a special URL that allows for directory traversal. This is only possible on a Wiki.js server running on Windows, when a storage module implementing local asset cache (e.g Local File System or Git) is enabled and that no web application firewall solution (e.g. cloudflare) strips potentially malicious URLs. Commit number 414033de9dff66a327e3f3243234852f468a9d85 fixes this vulnerability by sanitizing the path before it is passed on to the storage module. The sanitization step removes any windows directory traversal sequences from the path. As a workaround, disable any storage module with local asset caching capabilities (Local File System, Git).
CVE-2021-43788	Nodebb is an open source Node.js based forum software. Prior to v1.18.5, a path traversal vulnerability was present that allowed users to access JSON files outside of the expected `languages/` directory. The vulnerability has been patched as of v1.18.5. Users are advised to upgrade as soon as possible.
CVE-2021-43787	Nodebb is an open source Node.js based forum software. In affected versions a prototype pollution vulnerability in the uploader module allowed a malicious user to inject arbitrary data (i.e. javascript) into the DOM, theoretically allowing for an account takeover when used in conjunction with a path traversal vulnerability disclosed at the same time as this report. The vulnerability has been patched as of v1.18.5. Users are advised to upgrade as soon as possible.
CVE-2021-43786	Nodebb is an open source Node.js based forum software. In affected versions incorrect logic present in the token verification step unintentionally allowed master token access to the API. The vulnerability has been patch as of v1.18.5. Users are advised to upgrade as soon as possible.
CVE-2021-43571	The verify function in the Stark Bank Node.js ECDSA library (ecdsa-node) 1.1.2 fails to check that the signature is non-zero, which allows attackers to forge signatures on arbitrary messages.
CVE-2021-42740	The shell-quote package before 1.7.3 for Node.js allows command injection. An attacker can inject unescaped shell metacharacters through a regex designed to support Windows drive letters. If the output of this package is passed to a real shell as a quoted argument to a command with exec(), an attacker can inject arbitrary commands. This is because the Windows drive letter regex character class is {A-z] instead of the correct {A-Za-z]. Several shell metacharacters exist in the space between capital letter Z and lower case letter a, such as the backtick character.
CVE-2021-41580	** DISPUTED ** The passport-oauth2 package before 1.6.1 for Node.js mishandles the error condition of failure to obtain an access token. This is exploitable in certain use cases where an OAuth identity provider uses an HTTP 200 status code for authentication-failure error reports, and an application grants authorization upon simply receiving the access token (i.e., does not try to use the token). NOTE: the passport-oauth2 vendor does not consider this a passport-oauth2 vulnerability.
CVE-2021-41109	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to version 4.10.4, for regular (non-LiveQuery) queries, the session token is removed from the response, but for LiveQuery payloads it is currently not. If a user has a LiveQuery subscription on the `Parse.User` class, all session tokens created during user sign-ups will be broadcast as part of the LiveQuery payload. A patch in version 4.10.4 removes session tokens from the LiveQuery payload. As a workaround, set `user.acl(new Parse.ACL())` in a beforeSave trigger to make the user private already on sign-up.
CVE-2021-40831	The AWS IoT Device SDK v2 for Java, Python, C++ and Node.js appends a user supplied Certificate Authority (CA) to the root CAs instead of overriding it on macOS systems. Additionally, SNI validation is also not enabled when the CA has been “overridden”. TLS handshakes will thus succeed if the peer can be verified either from the user-supplied CA or the system’s default trust-store. Attackers with access to a host’s trust stores or are able to compromise a certificate authority already in the host's trust store (note: the attacker must also be able to spoof DNS in this case) may be able to use this issue to bypass CA pinning. An attacker could then spoof the MQTT broker, and either drop traffic and/or respond with the attacker's data, but they would not be able to forward this data on to the MQTT broker because the attacker would still need the user's private keys to authenticate against the MQTT broker. The 'aws_tls_ctx_options_override_default_trust_store_*' function within the aws-c-io submodule has been updated to address this behavior. This issue affects: Amazon Web Services AWS IoT Device SDK v2 for Java versions prior to 1.5.0 on macOS. Amazon Web Services AWS IoT Device SDK v2 for Python versions prior to 1.7.0 on macOS. Amazon Web Services AWS IoT Device SDK v2 for C++ versions prior to 1.14.0 on macOS. Amazon Web Services AWS IoT Device SDK v2 for Node.js versions prior to 1.6.0 on macOS. Amazon Web Services AWS-C-IO 0.10.7 on macOS.

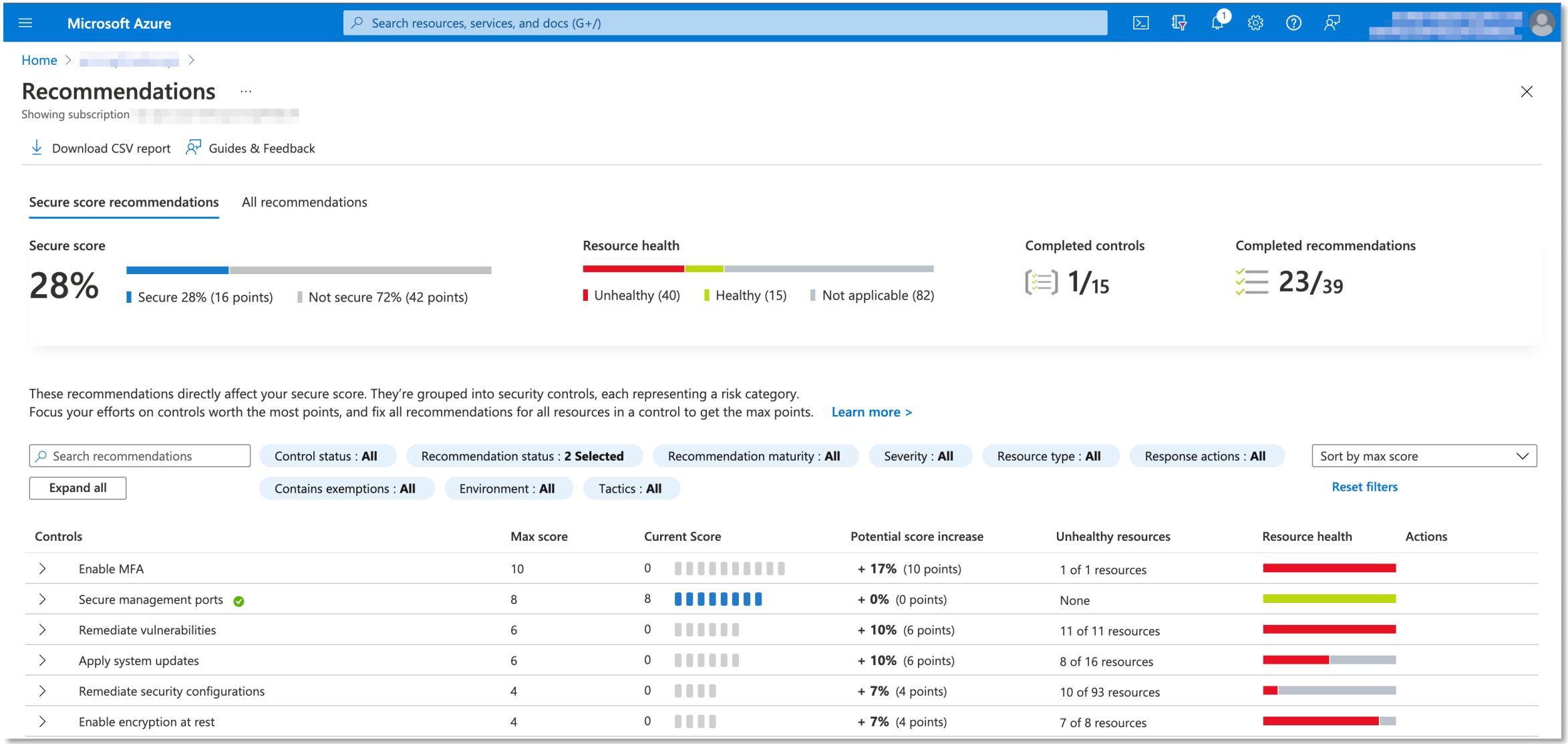
```
james@ilmiontdesktop:~$ ./trivy image php:latest
2021-06-15T20:55:42.134+0100    INFO    Need to update DB
2021-06-15T20:55:42.134+0100    INFO    Downloading DB...
21.97 MiB / 21.97 MiB [----------------------] 100.00% 19.88 MiB p/s 1s
2021-06-15T20:55:52.726+0100    INFO    Detected OS: debian
2021-06-15T20:55:52.726+0100    INFO    Detecting Debian vulnerabilities...
2021-06-15T20:55:52.742+0100    INFO    Number of PL dependency files: 0

php:latest (debian 10.9)
========================
Total: 584 (UNKNOWN: 2, LOW: 425, MEDIUM: 60, HIGH: 90, CRITICAL: 7)

+---------------------------+--------------------+----------+-----------------------+----------------
|          LIBRARY          |  VULNERABILITY ID  | SEVERITY |   INSTALLED VERSION   |  FIXED VERSION
+---------------------------+--------------------+----------+-----------------------+----------------
| apt                       | CVE-2011-3374      | LOW      | 1.8.2.3               |
|                           |                    |          |                       |
|                           |                    |          |                       |
+---------------------------+--------------------+          +---------
| bash                      | CVE-2019-18276     |          | 5.0-4
|                           |                    |          |
|                           |                    |          |
+                           +--------------------+          +
|                           | TEMP-0841856-B18BAF |          |
```

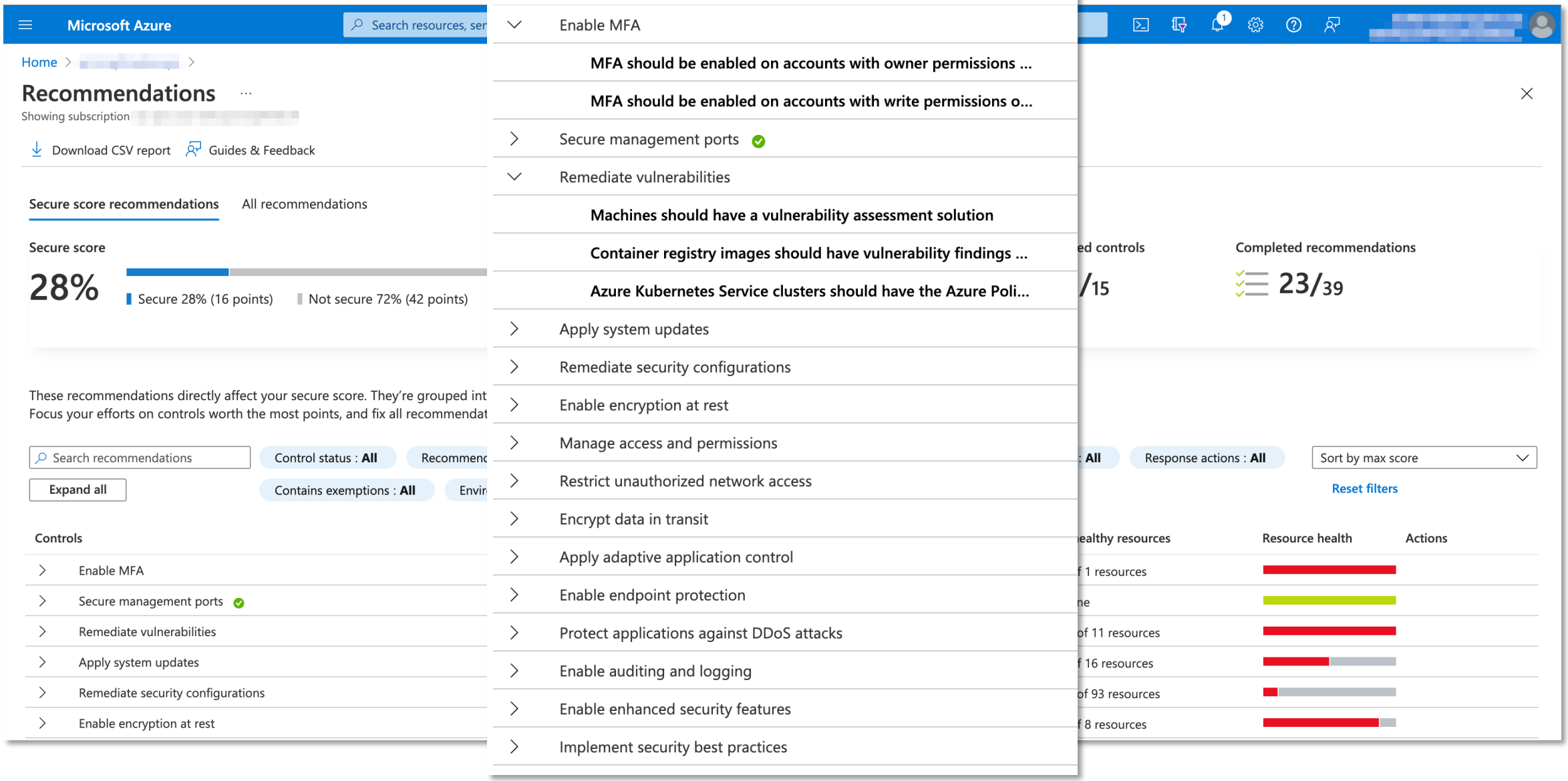
php:latest (debian 10.9) - Trivy Report - 2021-06-16T15:42:30.167294693Z

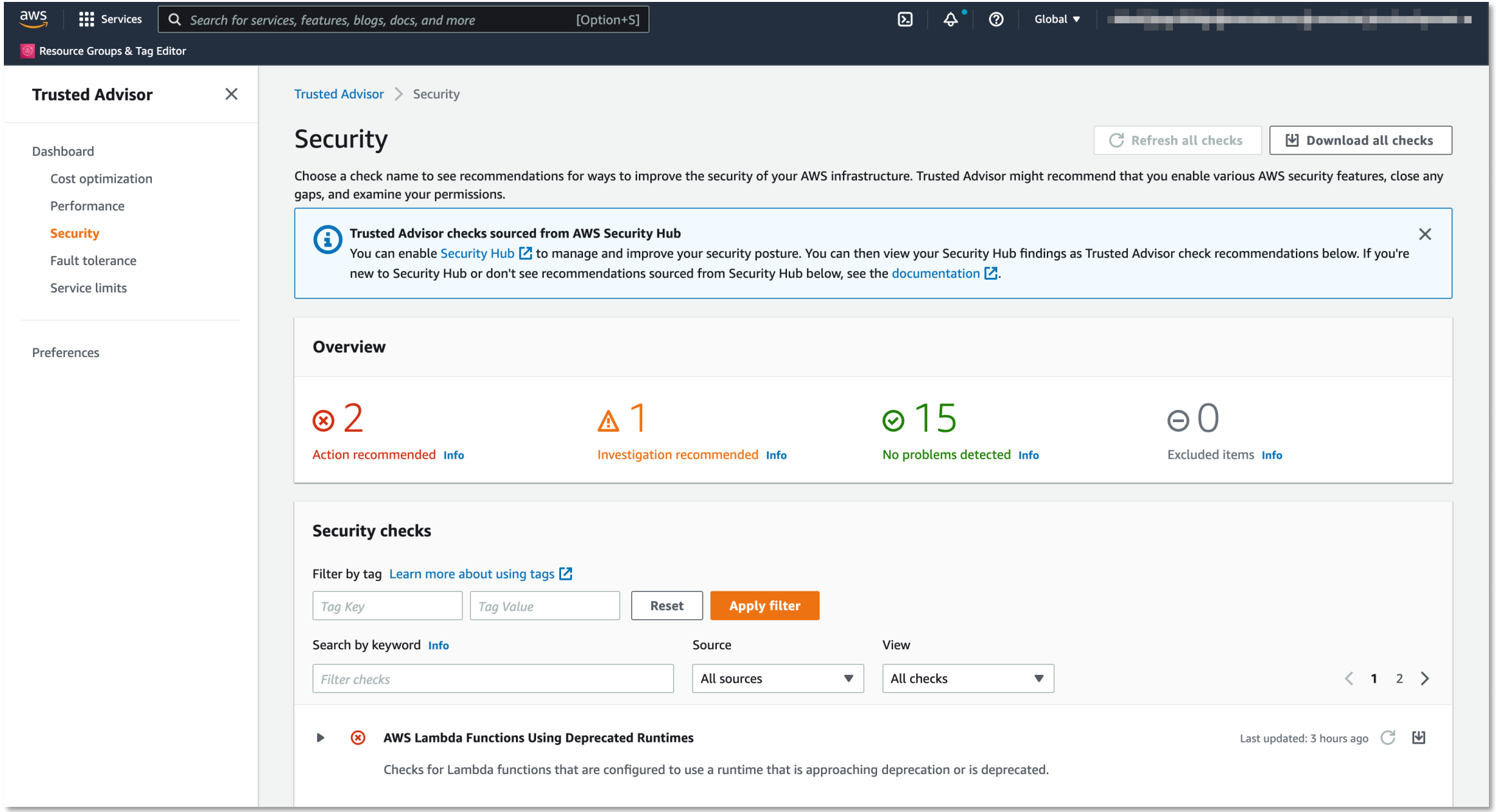
					debian
Package	**Vulnerability ID**	**Severity**	**Installed Version**	**Fixed Version**	
apt	CVE-2011-3374	LOW	1.8.2.3		https://access.redhat.com/security/cve/cve-2011-337 https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=64 https://people.canonical.com/~ubuntu-security/cve/20 Toggle more links
bash	CVE-2019-18276	LOW	5.0-4		http://packetstormsecurity.com/files/155498/Bash-5.0 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE https://github.com/bminor/bash/commit/951bdaad7a1 Toggle more links
bash	TEMP-0841856-B18BAF	LOW	5.0-4		
binutils	CVE-2017-13716	LOW	2.31.1-16		https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE https://sourceware.org/bugzilla/show_bug.cgi?id=220
binutils	CVE-2018-1000876	LOW	2.31.1-16		http://lists.opensuse.org/opensuse-security-announce http://lists.opensuse.org/opensuse-security-announce http://www.securityfocus.com/bid/106304 Toggle more links
binutils	CVE-2018-12697	LOW	2.31.1-16		http://www.securityfocus.com/bid/104538 https://access.redhat.com/errata/RHSA-2019:2075 https://bugs.launchpad.net/ubuntu/+source/binutils/+ Toggle more links
binutils	CVE-2018-12698	LOW	2.31.1-16		http://www.securityfocus.com/bid/104539 https://bugs.launchpad.net/ubuntu/+source/binutils/+

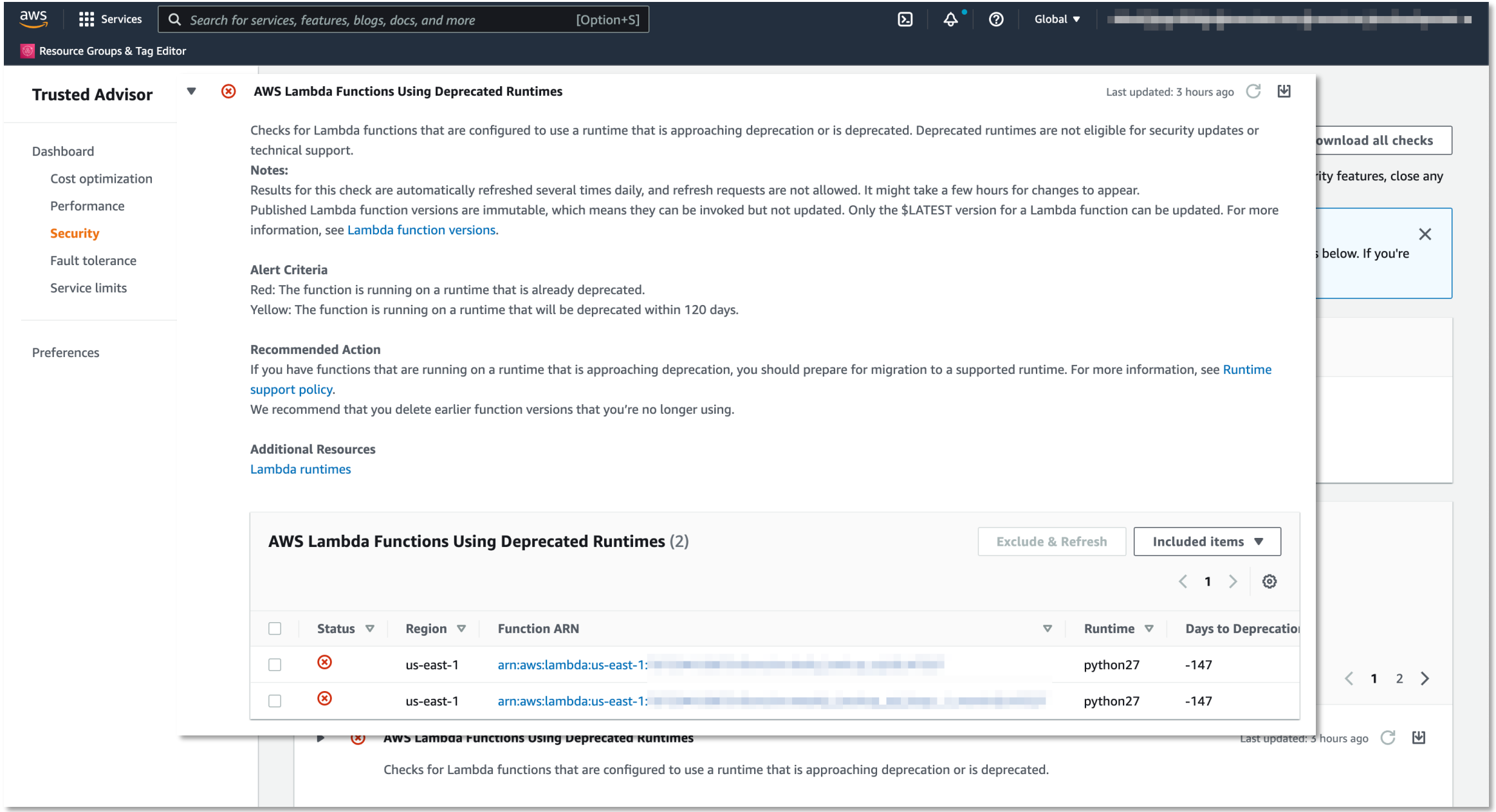
```
Starting: Image scan by Clair
==============================================================================
Task         : Command line
Description  : Run a command line script using Bash on Linux and macOS and cmd.exe on Windows
Version      : 2.182.0
Author       : Microsoft Corporation
Help         : https://docs.microsoft.com/azure/devops/pipelines/tasks/utility/command-line
==============================================================================
Generating script.
========================== Starting Command Output ===========================
/usr/bin/bash --noprofile --norc /azp/agent/_work/_temp/7d680b3a-6d4e-43f1-b74f-a96a7f7ad543.sh
5e7e0abf239da06696ccc88431b8c6a2f0f7b58a610e4a56e4939b0efbcb4480
9ad3636fd6ab9cb2065ab4c863f85c52120d82049285437ec1585eab5e0e37ab
2021/05/24 05:42:06 [INFO] ▶ Start clair-scanner
2021/05/24 05:42:34 [INFO] ▶ Server listening on port 9279
2021/05/24 05:42:34 [INFO] ▶ Analyzing aceeadd97fac6c40d656deb08b28cde40a8c54bd15b64802f3bf18472e0011e1
2021/05/24 05:42:38 [INFO] ▶ Analyzing c22869270d9242b45e85384fc8b42ffa0821490494e1a4bfc71c9094bdcdbd29
2021/05/24 05:42:38 [INFO] ▶ Analyzing 9fad01cfb28daca25afc2b18617b3e70ef192bdd1ccc8fe531540b69a8c04643
2021/05/24 05:42:39 [WARN] ▶ Image [openjdk:17-jdk-slim] contains 60 total vulnerabilities
2021/05/24 05:42:39 [ERRO] ▶ Image [openjdk:17-jdk-slim] contains 1 unapproved vulnerabilities
+------------+-------------------+--------------+-----------------+-----------------------------------------------------------------------------+
| STATUS     | CVE SEVERITY      | PACKAGE NAME | PACKAGE VERSION | CVE DESCRIPTION                                                             |
+------------+-------------------+--------------+-----------------+-----------------------------------------------------------------------------+
| Unapproved | High CVE-2019-25013 | glibc        | 2.28-10         | The iconv feature in the GNU C Library (aka                                 |
|            |                   |              |                 | glibc or libc6) through 2.32, when processing                               |
|            |                   |              |                 | invalid multi-byte input sequences in the                                   |
|            |                   |              |                 | EUC-KR encoding, may have a buffer over-read.                               |
|            |                   |              |                 | https://security-tracker.debian.org/tracker/CVE-2019-25013                  |
+------------+-------------------+--------------+-----------------+-----------------------------------------------------------------------------+
clair
clair
clair-db
clair-db
Finishing: Image scan by Clair
```



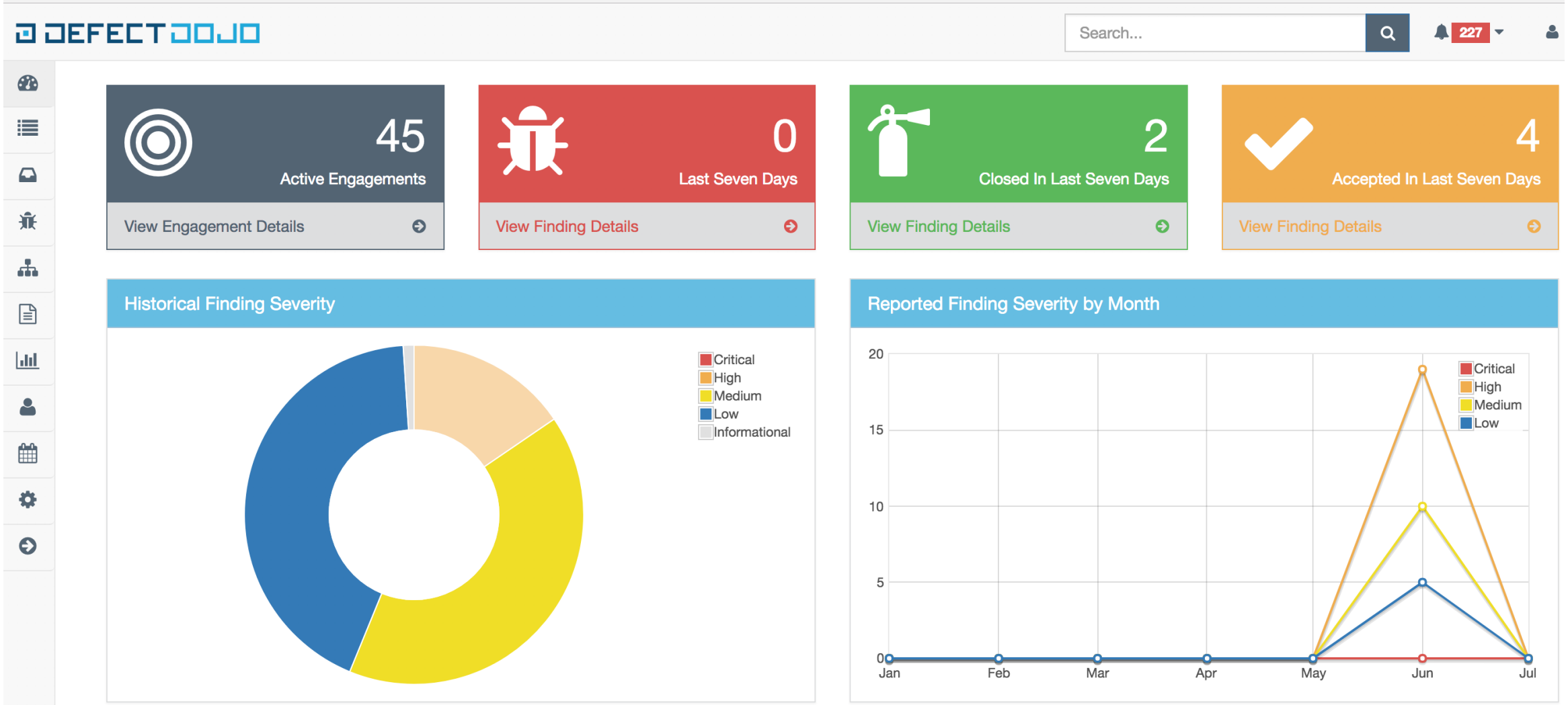

Microsoft Azure
Search resources, services, and docs (G+/)
Home
Recommendations
Showing subscription
Download CSV report
Guides & Feedback
Secure score recommendations
All recommendations
Secure score
28%
Secure 28% (16 points)
Not secure 72% (42 points)
Resource health
Unhealthy (40)
Healthy (15)
Not applicable (82)
Completed controls
1/15
Completed recommendations
23/39
These recommendations directly affect your secure score. They're grouped into security controls, each representing a risk category.
Focus your efforts on controls worth the most points, and fix all recommendations for all resources in a control to get the max points.
Learn more >
Search recommendations
Control status : All
Recommendation status : 2 Selected
Recommendation maturity : All
Severity : All
Resource type : All
Response actions : All
Sort by max score
Expand all
Contains exemptions : All
Environment : All
Tactics : All
Reset filters
Controls
Max score
Current Score
Potential score increase
Unhealthy resources
Resource health
Actions
Enable MFA
10
0
+ 17% (10 points)
1 of 1 resources
Secure management ports
8
8
+ 0% (0 points)
None
Remediate vulnerabilities
6
0
+ 10% (6 points)
11 of 11 resources
Apply system updates
6
0
+ 10% (6 points)
8 of 16 resources
Remediate security configurations
4
0
+ 7% (4 points)
10 of 93 resources
Enable encryption at rest
4
0
+ 7% (4 points)
7 of 8 resources


Microsoft Azure
Search resources, ser
Home
Recommendations
Showing subscription
Download CSV report
Guides & Feedback
Secure score recommendations
All recommendations
Secure score
28%
Secure 28% (16 points)
Not secure 72% (42 points)
These recommendations directly affect your secure score. They're grouped int
Focus your efforts on controls worth the most points, and fix all recommendat
Search recommendations
Control status : All
Recommenc
Expand all
Contains exemptions : All
Envir
Controls
Enable MFA
Secure management ports
Remediate vulnerabilities
Apply system updates
Remediate security configurations
Enable encryption at rest
ed controls
/15
Completed recommendations
23/39
: All
Response actions : All
Sort by max score
Reset filters
ealthy resources
Resource health
Actions
f 1 resources
ne
of 11 resources
f 16 resources
of 93 resources
f 8 resources
Controls
Enable MFA
MFA should be enabled on accounts with owner permissions ...
MFA should be enabled on accounts with write permissions o...
Secure management ports
Remediate vulnerabilities
Machines should have a vulnerability assessment solution
Container registry images should have vulnerability findings ...
Azure Kubernetes Service clusters should have the Azure Poli...
Apply system updates
Remediate security configurations
Enable encryption at rest
Manage access and permissions
Restrict unauthorized network access
Encrypt data in transit
Apply adaptive application control
Enable endpoint protection
Protect applications against DDoS attacks
Enable auditing and logging
Enable enhanced security features
Implement security best practices

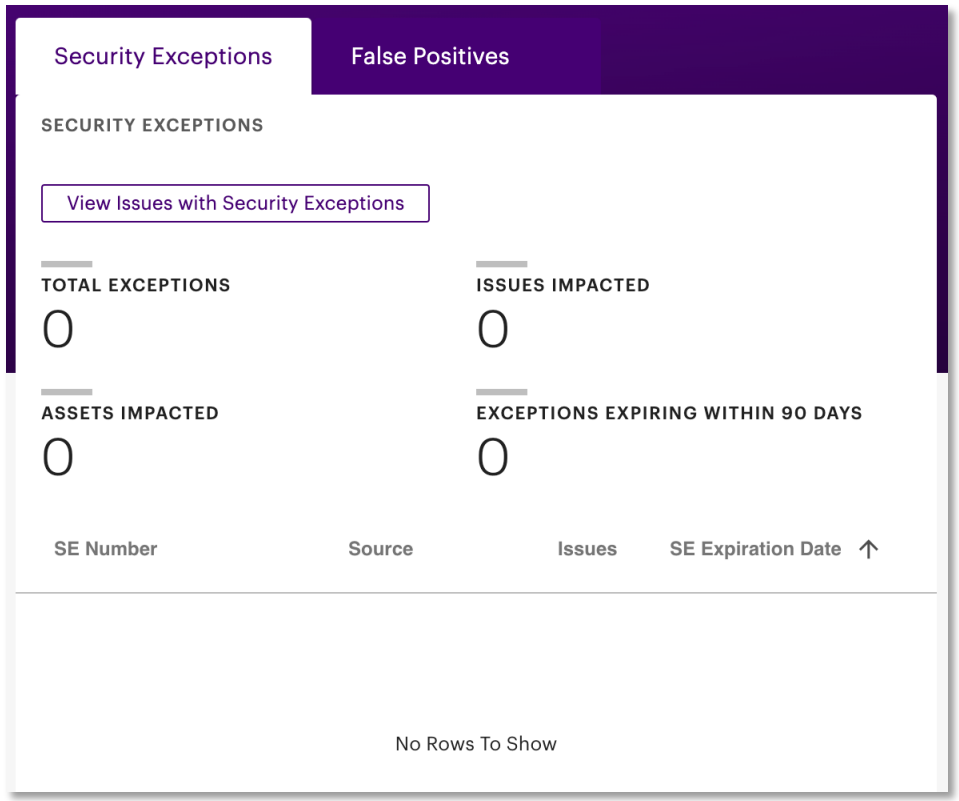

aws
Services
Search for services, features, blogs, docs, and more
[Option+S]
Global
Resource Groups & Tag Editor
Trusted Advisor
Dashboard
Cost optimization
Performance
Security
Fault tolerance
Service limits
Preferences
Trusted Advisor > Security
Security
Refresh all checks
Download all checks
Choose a check name to see recommendations for ways to improve the security of your AWS infrastructure. Trusted Advisor might recommend that you enable various AWS security features, close any gaps, and examine your permissions.
Trusted Advisor checks sourced from AWS Security Hub
You can enable Security Hub to manage and improve your security posture. You can then view your Security Hub findings as Trusted Advisor check recommendations below. If you're new to Security Hub or don't see recommendations sourced from Security Hub below, see the documentation.
Overview
2
Action recommended Info
1
Investigation recommended Info
15
No problems detected Info
0
Excluded items Info
Security checks
Filter by tag Learn more about using tags
Tag Key
Tag Value
Reset
Apply filter
Search by keyword Info
Filter checks
Source
All sources
View
All checks
1 2
AWS Lambda Functions Using Deprecated Runtimes
Last updated: 3 hours ago
Checks for Lambda functions that are configured to use a runtime that is approaching deprecation or is deprecated.


aws
Services
Search for services, features, blogs, docs, and more
[Option+S]
Global
Resource Groups & Tag Editor
Trusted Advisor
Dashboard
Cost optimization
Performance
Security
Fault tolerance
Service limits
Preferences
AWS Lambda Functions Using Deprecated Runtimes
Last updated: 3 hours ago
Checks for Lambda functions that are configured to use a runtime that is approaching deprecation or is deprecated. Deprecated runtimes are not eligible for security updates or technical support.
Notes:
Results for this check are automatically refreshed several times daily, and refresh requests are not allowed. It might take a few hours for changes to appear.
Published Lambda function versions are immutable, which means they can be invoked but not updated. Only the $LATEST version for a Lambda function can be updated. For more information, see Lambda function versions.
Alert Criteria
Red: The function is running on a runtime that is already deprecated.
Yellow: The function is running on a runtime that will be deprecated within 120 days.
Recommended Action
If you have functions that are running on a runtime that is approaching deprecation, you should prepare for migration to a supported runtime. For more information, see Runtime support policy.
We recommend that you delete earlier function versions that you're no longer using.
Additional Resources
Lambda runtimes
AWS Lambda Functions Using Deprecated Runtimes (2)
Exclude & Refresh
Included items
Status
Region
Function ARN
Runtime
Days to Deprecatio
us-east-1
arn:aws:lambda:us-east-1:
python27
-147
us-east-1
arn:aws:lambda:us-east-1:
python27
-147
ownload all checks
ity features, close any
s below. If you're
AWS Lambda Functions Using Deprecated Runtimes
Last updated: 3 hours ago
Checks for Lambda functions that are configured to use a runtime that is approaching deprecation or is deprecated.

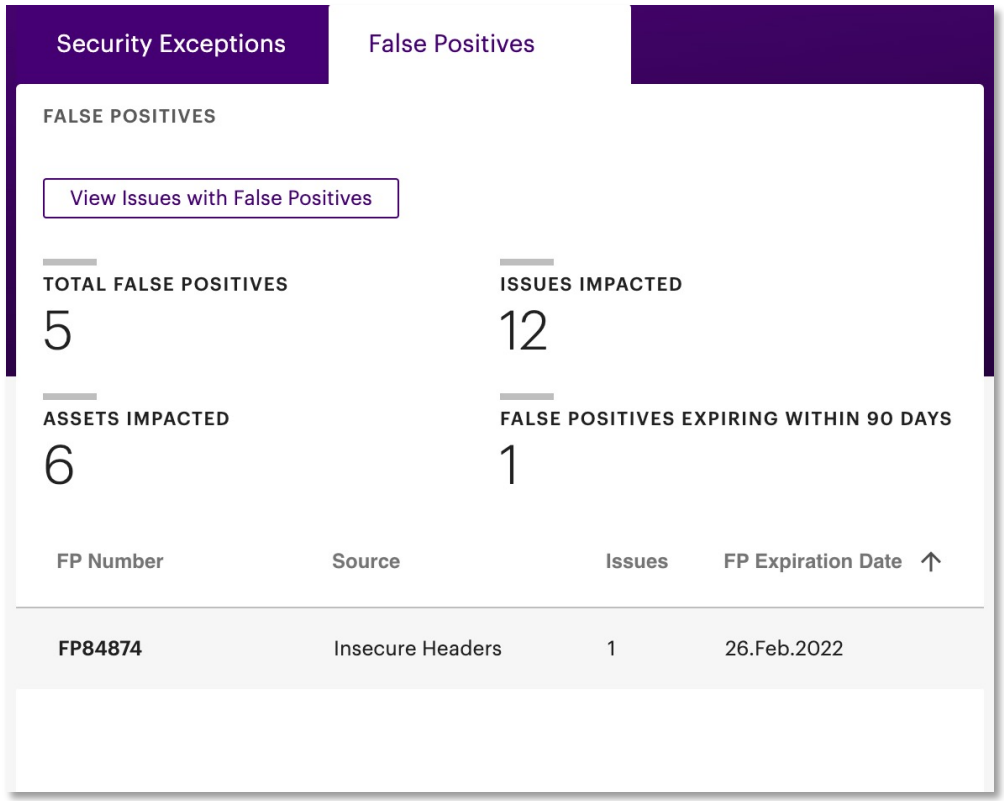
AGGREGATING EVENTS FROM MULTIPLE SOURCES



NO PROCESS OR TOOL IS PERFECT



Identify and manage policy exceptions

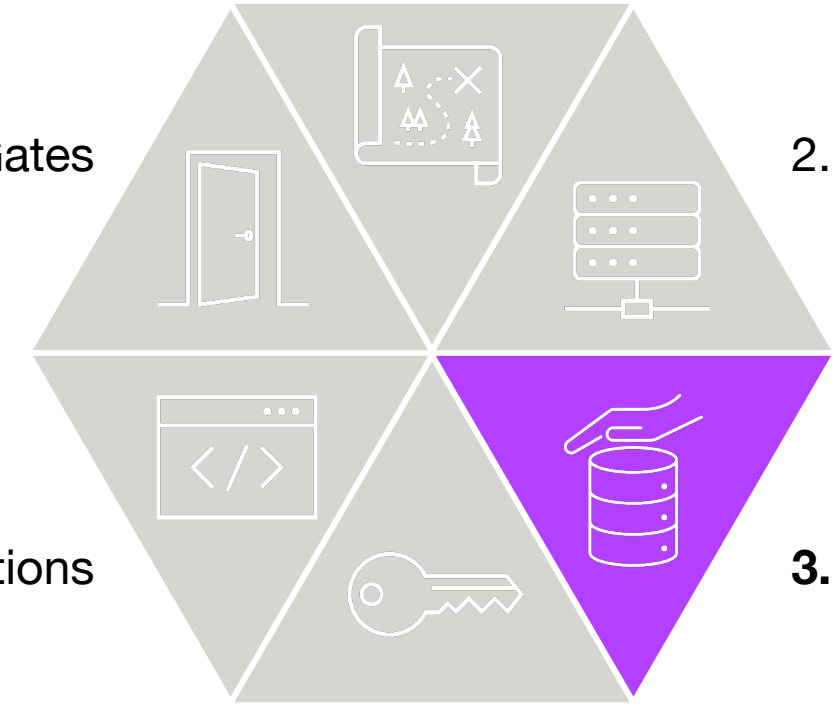


Identify and manage false positives

EXEMPLAR TOOLS

- Falco
- Clair Scanner
- Trivy
- TFLint
- Checkov
- Defect Dojo

AGENDA

1. Introduction
6. Gates
2. Infrastructure

5. Applications
3. Data
4. Identities

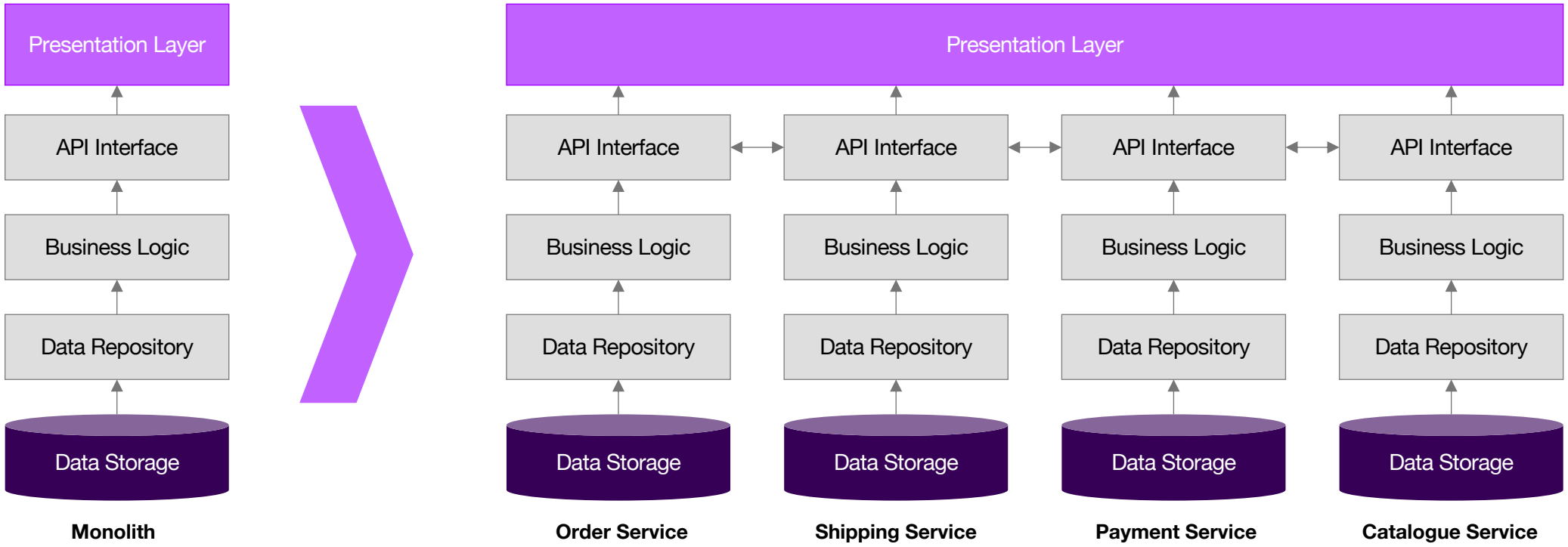
DATA SECURITY

- Encryption in transit and at rest
- Data classification and GDPR
- Retention and deletion policies
- Data access modeling, as per data classification
  - Access per functional role (e.g. user belongs to marketing dept.)
  - Information blocks in user interfaces (e.g. employee economic profile)
  - Report catalogue per role (e.g. report only available to insider list)

DATA SECURITY

- Classification leads to compartment and isolation
- Microservice-oriented architectures can be of help for that
- More difficult in monolithic databases or data lakes, where a huge amount of company information is stored and made available
- Mitigate with segmented access and RBAC, e.g. no direct access to data lake but through a data mart with a business intelligence tool

DATA SECURITY

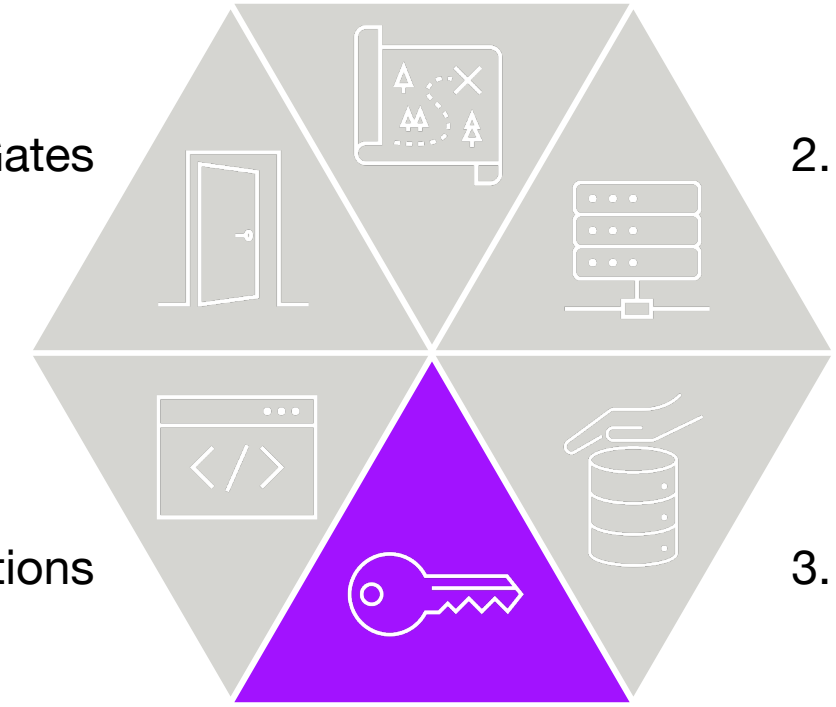


DATA SECURITY

- Create test cases to validate all of the previous
- Made them part of acceptance criteria and regression
- Run them in CI/CD pipelines

```
given
as a user from Human Resources group
when
I’m authenticated into the system
then
I have access to employee payroll data
```

AGENDA

1. Introduction
6. Gates
2. Infrastructure

5. Applications
3. Data
4. Identities

IDENTITY AND ACCESS MANAGEMENT

- Authentication and authorization
- Differentiate end users from internal users (admins, devs…)
- Multi-factor authentication (MFA)
- Privileged access management (PAM)
- Machine-to-machine access (M2M) a.k.a. “application IDs”
  - Workload identities
  - Service principal / service account
- Certificate management (HTTPS)
- Role-based access control (RBAC)
  - Low-level granularity, key for multi-tenant (shared) platforms

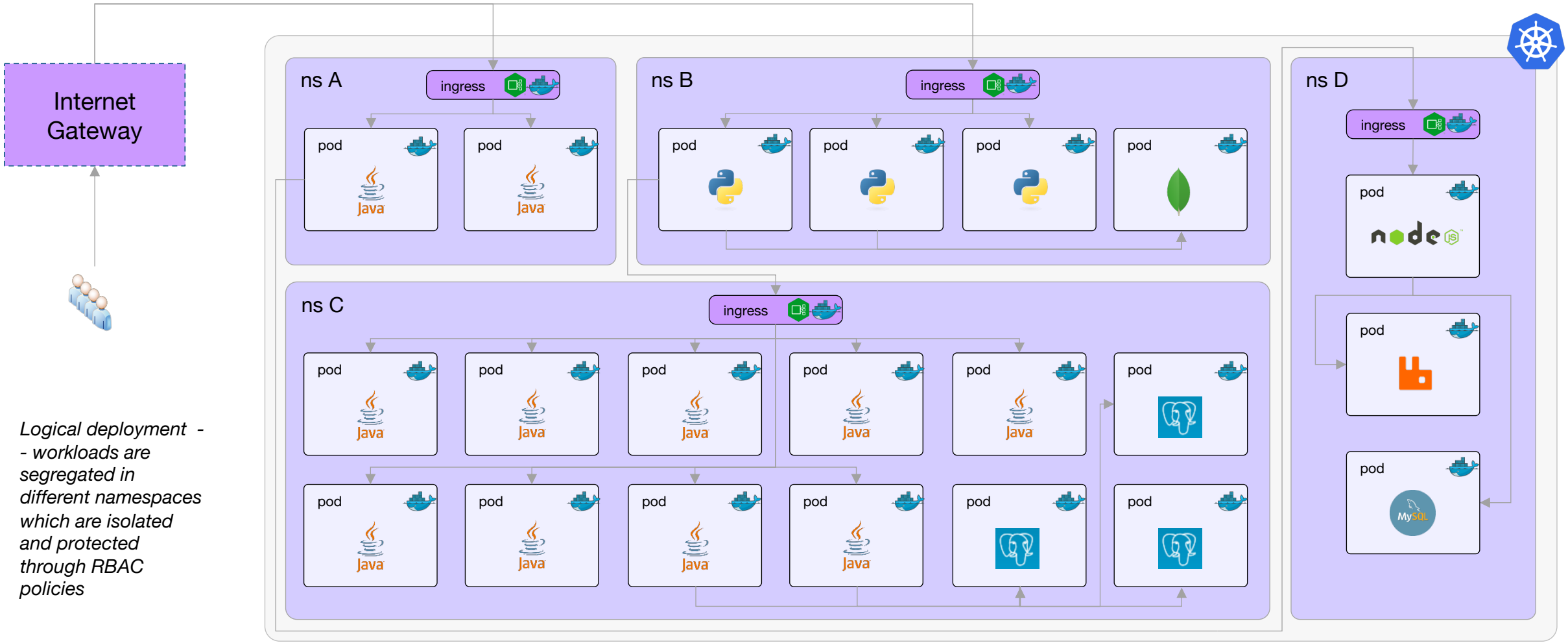
CERTIFICATE MANAGEMENT

- Easy in small environments, e.g., a dozen of nodes
  - Easily solved using wildcard certificates and internal DNS to route access to individual tenants/applications
- More complex in medium or large environments, e.g. a Kubernetes cluster with hundreds of nodes provisioned elastically – automation is key to escale the solution
  - **cert-manager** integrated with a certificate manager such as **Let's Encrypt**
  - A service mesh such as **Istio**, capable to manage intra-cluster communication through mTLS and ingress/egress traffic

ROLE-BASED ACCESS CONTROL

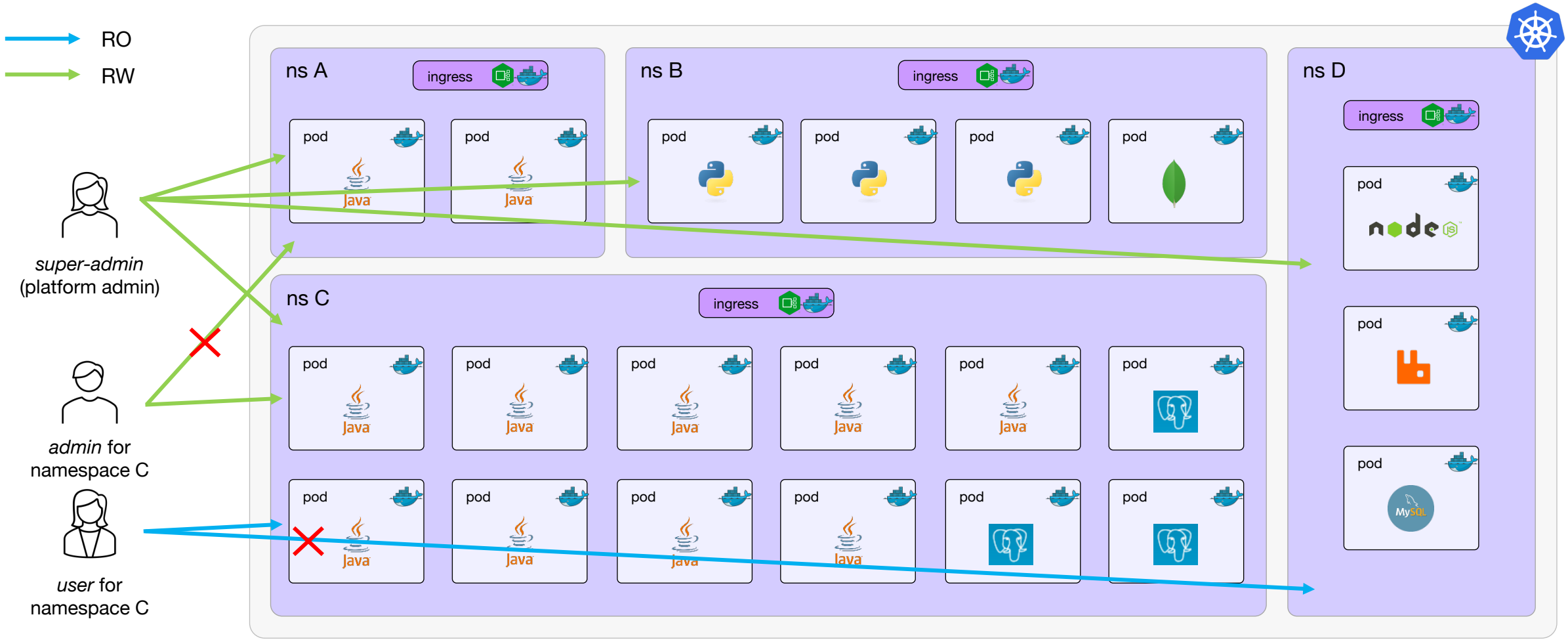
Physical deployment in a container platform – not related workloads share computing resources from the common infrastructure (through hypervisor)

ROLE-BASED ACCESS CONTROL



Logical deployment -- workloads are segregated in different namespaces which are isolated and protected through RBAC policies

ROLE-BASED ACCESS CONTROL



ROLE-BASED ACCESS CONTROL

```
18  resource "kubernetes_role" "admin_roles" {
19    for_each = {for org in local.resourcesToCreate: org.shortName => org}
20    metadata {
21      name      = format("%s-namespace-admin-role", each.key)
22      namespace = format("org-%s", each.value.name)
23    }
24
25    rule {
26      api_groups = ["*"]
27      resources  = ["*"]
28      verbs      = ["*"]
29    }
30  }
```

```
33  resource "kubernetes_role" "user_roles" {
34    for_each = {for org in local.resourcesToCreate: org.shortName => org}
35    metadata {
36      name      = format("%s-namespace-user-role", each.key)
37      namespace = format("org-%s", each.value.name)
38    }
39
40    rule {
41      api_groups = ["*"]
42      resources  = ["*"]
43      verbs      = ["get", "list", "watch"]
44    }
45  }
```

```
67  resource "kubernetes_role_binding" "admin_role_binding" {
68    for_each = {for org in local.resourcesToCreate: org.shortName => org}
69    metadata {
70      name      = format("%s-admin-role-binding", each.key)
71      namespace = format("org-%s", each.value.name)
72    }
73    role_ref {
74      api_group = "rbac.authorization.k8s.io"
75      kind      = "Role"
76      name      = format("%s-namespace-admin-role", each.key)
77    }
78    subject {
79      kind      = "Group"
80      name      = data.azuread_group.admin_groups[each.key].id
81      api_group = "rbac.authorization.k8s.io"
82      namespace = format("org-%s", each.value.name)
83    }
84  }
```

ROLE-BASED ACCESS CONTROL

- Extend the model to protect from supply-chain attacks
  - Container registry or binary artefact management
  - Who/what can push, who/what can pull

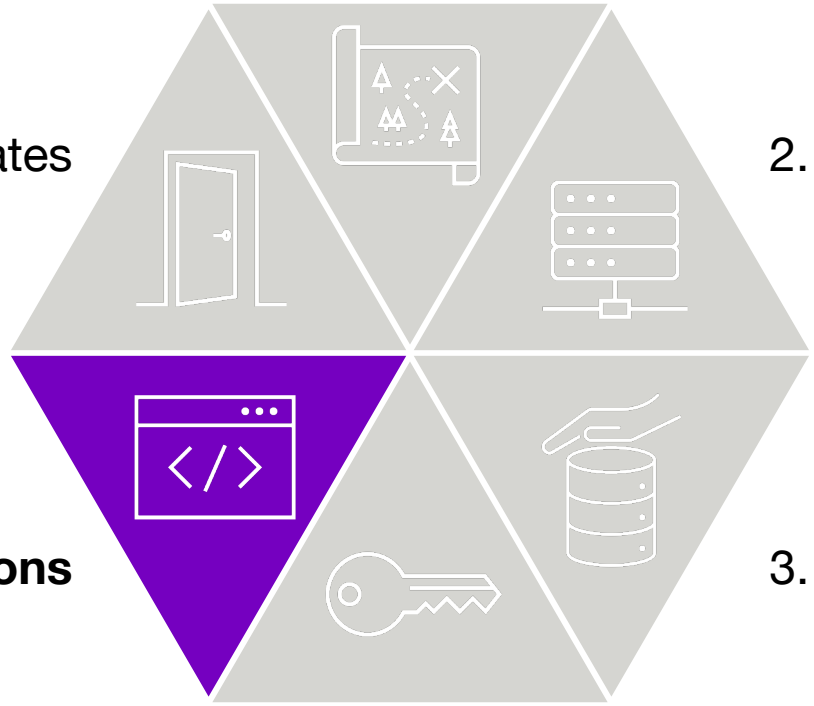
- Extend the model to secret management
  - Isolate and segment access
  - Who/what can create or change a secret
  - Who/what can access or use a secret

EXEMPLAR TOOLS

- cert-manager
- Let’s Encrypt
- Envoy
- Linkerd
- Istio
- Open Service Mesh
- Helm Secrets
- Conjur

AGENDA

1. Introduction
2. Infrastructure
3. Data
4. Identities
5. Applications
6. Gates

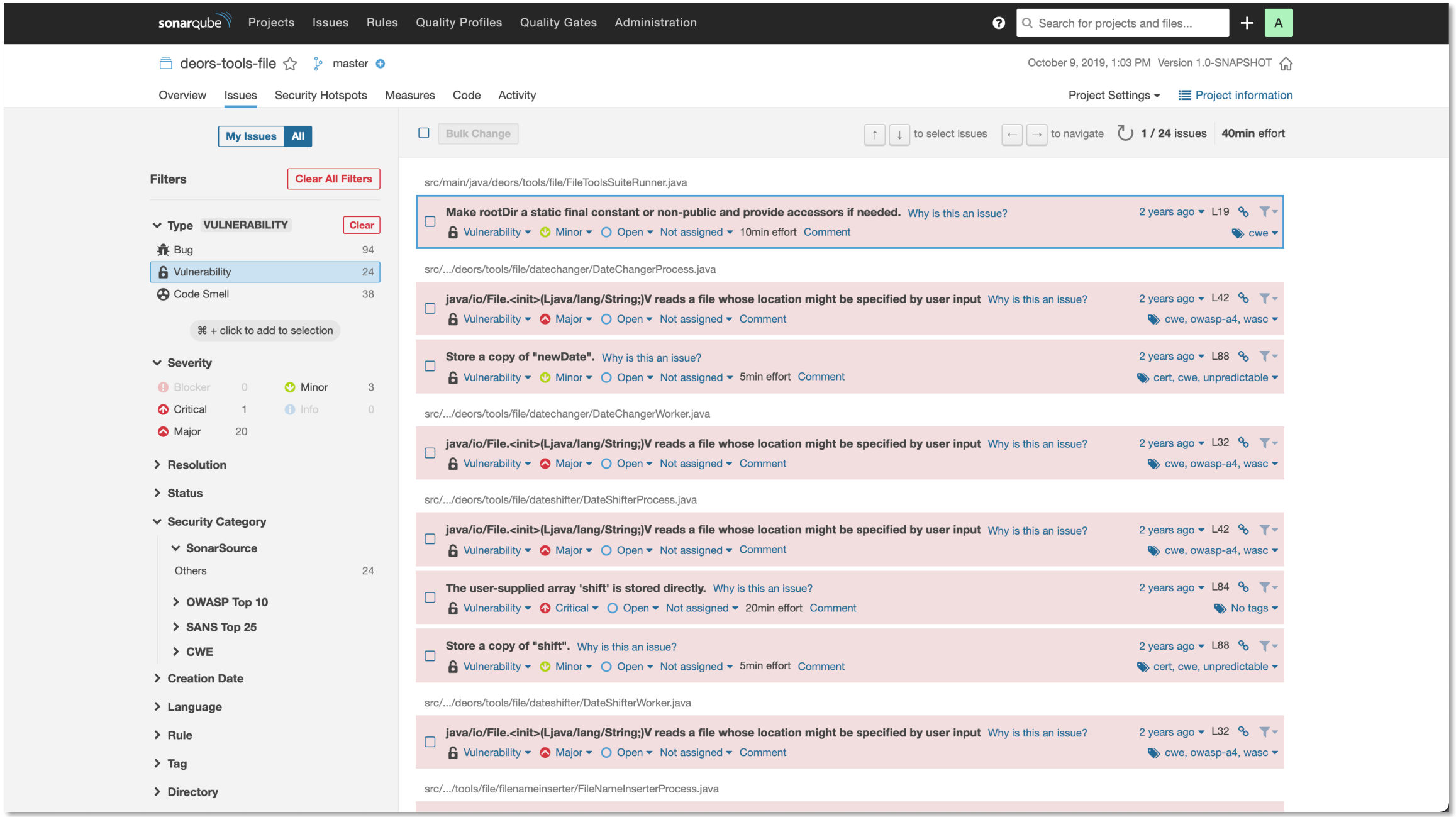


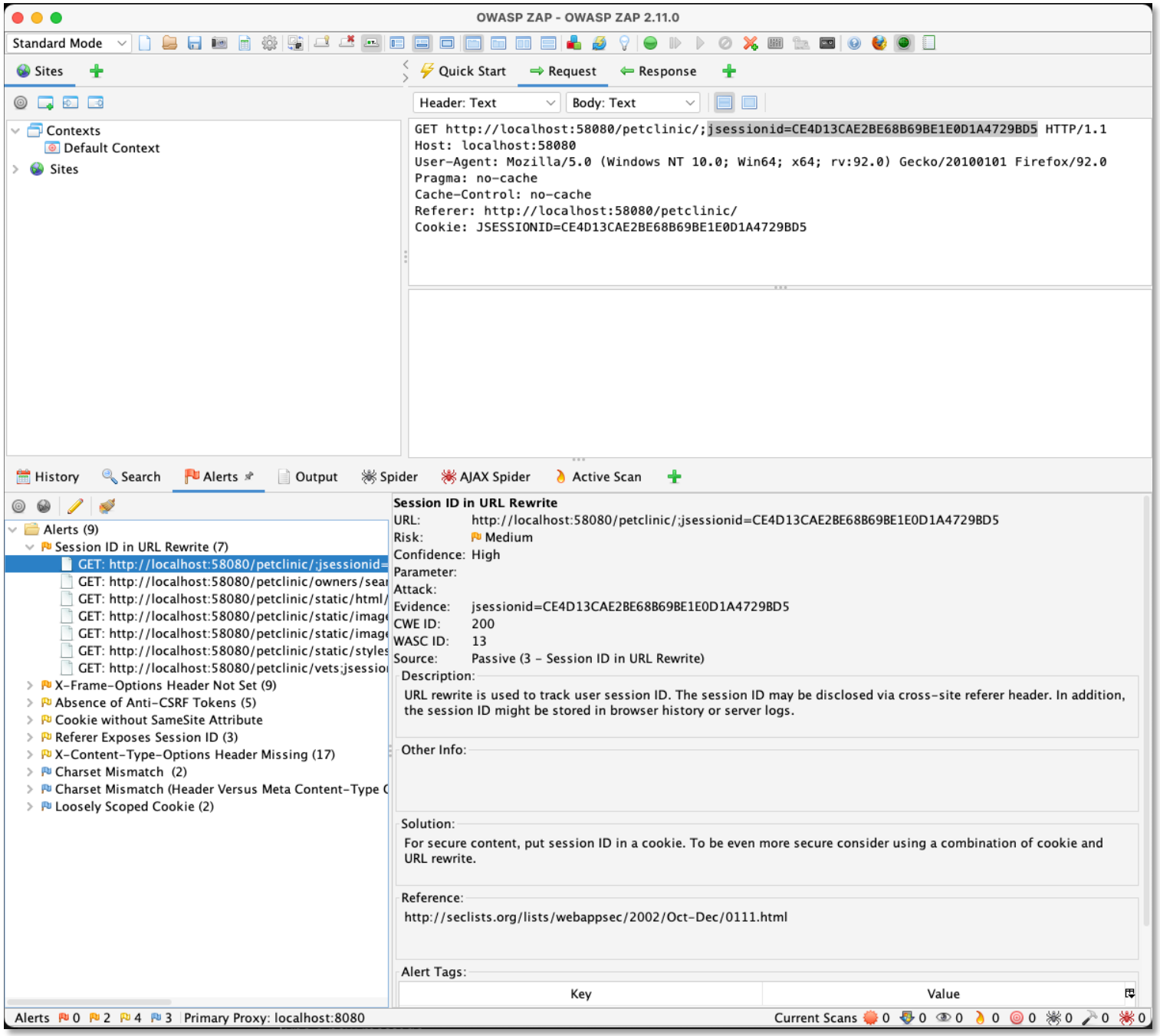
APPLICATION SECURITY

- Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST)
  - Passive (web proxy)
  - Active (web spider/crawler)
- Software Composition Analysis (SCA)
- Secrets and sensitive configuration (leak protection)

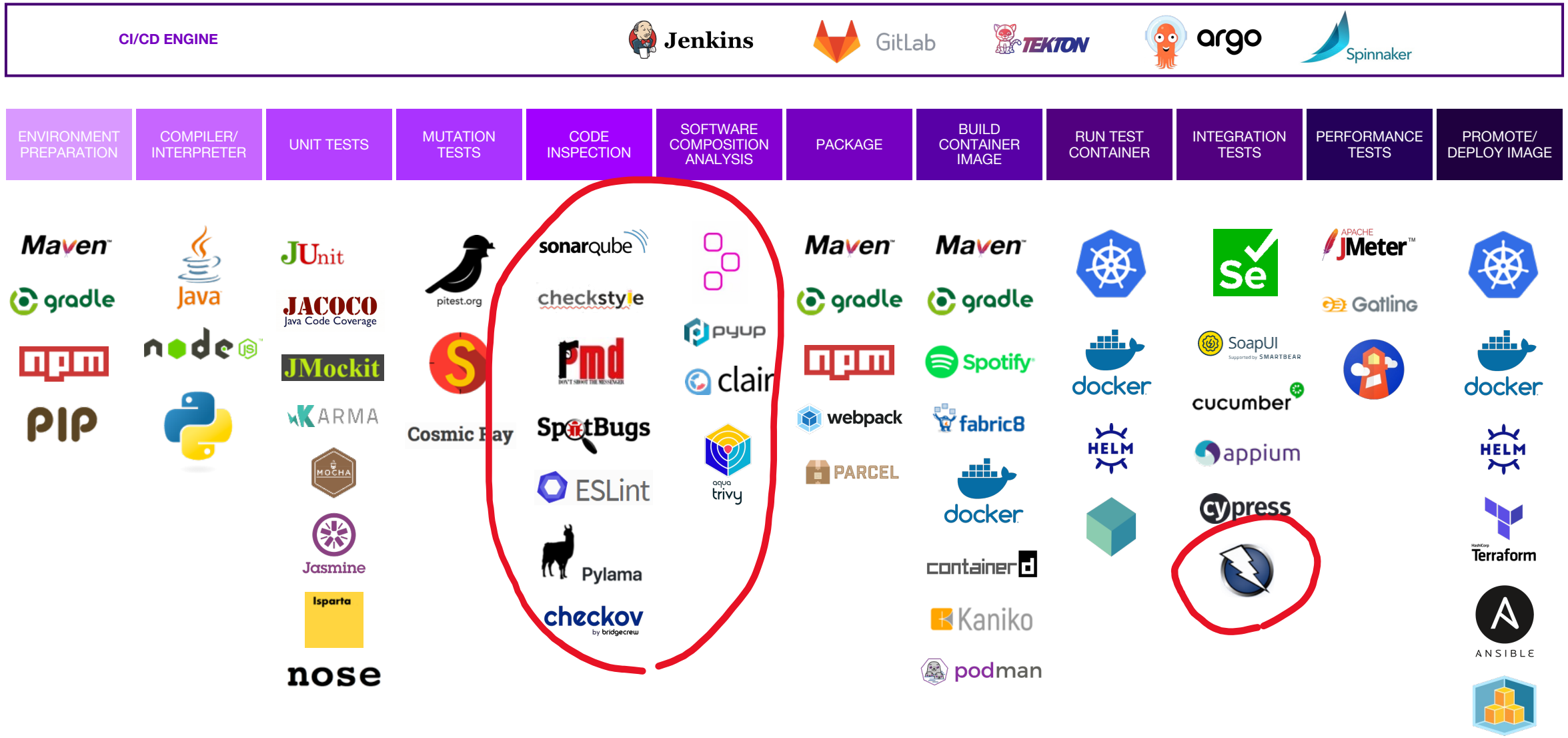
DETECTOR TYPES

- SQL injection
- File path injection
- XPath injection
- Regular expression injection
- Command injection
- Code injection
- Object injection (serialization)
- Log injection (e.g. log4j)
- Data leaks
- Cross-Site Scripting (XSS)
- Server-Side Request Forgery (SSRF)
- Open redirection
- Wrong authentication
- Wrong access control
- Hard-coded credentials
- Weak crypto ciphers
- Buffer overflows


sonarqube
Projects
Issues
Rules
Quality Profiles
Quality Gates
Administration
Search for projects and files...
A
deors-tools-file
master
October 9, 2019, 1:03 PM Version 1.0-SNAPSHOT
Overview
Issues
Security Hotspots
Measures
Code
Activity
Project Settings
Project information
My Issues
All
Bulk Change
to select issues
to navigate
1 / 24 issues
40min effort
Filters
Clear All Filters
Type VULNERABILITY
Clear
Bug 94
Vulnerability 24
Code Smell 38
⌘ + click to add to selection
Severity
Blocker 0
Minor 3
Critical 1
Info 0
Major 20
Resolution
Status
Security Category
SonarSource
Others 24
OWASP Top 10
SANS Top 25
CWE
Creation Date
Language
Rule
Tag
Directory
src/main/java/deors/tools/file/FileToolsSuiteRunner.java
Make rootDir a static final constant or non-public and provide accessors if needed. Why is this an issue?
2 years ago L19
Vulnerability Minor Open Not assigned 10min effort Comment
cwe
src/.../deors/tools/file/datechanger/DateChangerProcess.java
java/io/File.<init>(Ljava/lang/String;)V reads a file whose location might be specified by user input Why is this an issue?
2 years ago L42
Vulnerability Major Open Not assigned Comment
cwe, owasp-a4, wasc
Store a copy of "newDate". Why is this an issue?
2 years ago L88
Vulnerability Minor Open Not assigned 5min effort Comment
cert, cwe, unpredictable
src/.../deors/tools/file/datechanger/DateChangerWorker.java
java/io/File.<init>(Ljava/lang/String;)V reads a file whose location might be specified by user input Why is this an issue?
2 years ago L32
Vulnerability Major Open Not assigned Comment
cwe, owasp-a4, wasc
src/.../deors/tools/file/dateshifter/DateShifterProcess.java
java/io/File.<init>(Ljava/lang/String;)V reads a file whose location might be specified by user input Why is this an issue?
2 years ago L42
Vulnerability Major Open Not assigned Comment
cwe, owasp-a4, wasc
The user-supplied array 'shift' is stored directly. Why is this an issue?
2 years ago L84
Vulnerability Critical Open Not assigned 20min effort Comment
No tags
Store a copy of "shift". Why is this an issue?
2 years ago L88
Vulnerability Minor Open Not assigned 5min effort Comment
cert, cwe, unpredictable
src/.../deors/tools/file/dateshifter/DateShifterWorker.java
java/io/File.<init>(Ljava/lang/String;)V reads a file whose location might be specified by user input Why is this an issue?
2 years ago L32
Vulnerability Major Open Not assigned Comment
cwe, owasp-a4, wasc
src/.../tools/file/filenameinserter/FileNameInserterProcess.java

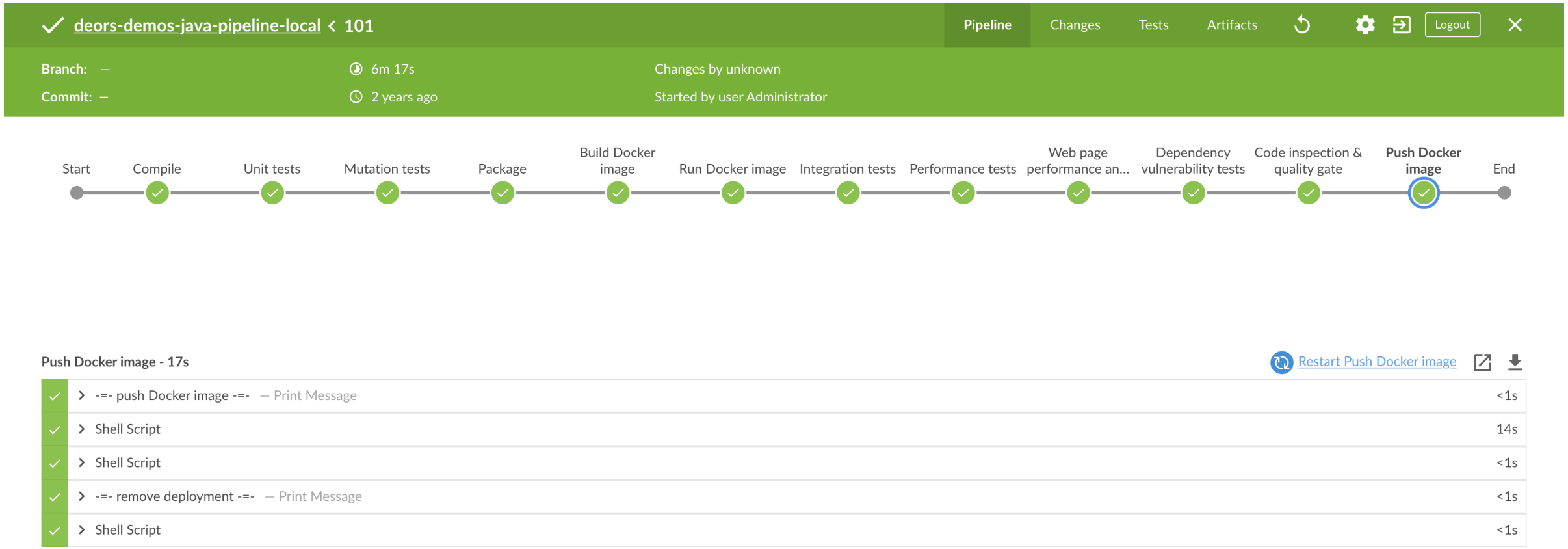

OWASP ZAP - OWASP ZAP 2.11.0
Standard Mode
Sites
Quick Start
Request
Response
Header: Text
Body: Text
Contexts
Default Context
Sites
GET http://localhost:58080/petclinic/;jsessionid=CE4D13CAE2BE68B69BE1E0D1A4729BD5 HTTP/1.1
Host: localhost:58080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
Pragma: no-cache
Cache-Control: no-cache
Referer: http://localhost:58080/petclinic/
Cookie: JSESSIONID=CE4D13CAE2BE68B69BE1E0D1A4729BD5
History
Search
Alerts
Output
Spider
AJAX Spider
Active Scan
Alerts (9)
Session ID in URL Rewrite (7)
GET: http://localhost:58080/petclinic/;jsessionid=
GET: http://localhost:58080/petclinic/owners/sea
GET: http://localhost:58080/petclinic/static/html/
GET: http://localhost:58080/petclinic/static/image
GET: http://localhost:58080/petclinic/static/image
GET: http://localhost:58080/petclinic/static/styles
GET: http://localhost:58080/petclinic/vets;jsessio
X-Frame-Options Header Not Set (9)
Absence of Anti-CSRF Tokens (5)
Cookie without SameSite Attribute
Referer Exposes Session ID (3)
X-Content-Type-Options Header Missing (17)
Charset Mismatch (2)
Charset Mismatch (Header Versus Meta Content-Type C
Loosely Scoped Cookie (2)
Session ID in URL Rewrite
URL: http://localhost:58080/petclinic/;jsessionid=CE4D13CAE2BE68B69BE1E0D1A4729BD5
Risk: Medium
Confidence: High
Parameter:
Attack:
Evidence: jsessionid=CE4D13CAE2BE68B69BE1E0D1A4729BD5
CWE ID: 200
WASC ID: 13
Source: Passive (3 - Session ID in URL Rewrite)
Description:
URL rewrite is used to track user session ID. The session ID may be disclosed via cross-site referer header. In addition, the session ID might be stored in browser history or server logs.
Other Info:
Solution:
For secure content, put session ID in a cookie. To be even more secure consider using a combination of cookie and URL rewrite.
Reference:
http://seclists.org/lists/webappsec/2002/Oct-Dec/0111.html
Alert Tags:
Key
Value
Alerts 0 2 4 3
Primary Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0

APPLICATION SECURITY TOOLS IN CI/CD PIPELINES



This map is not exhaustive of every available option, but representative of common tools used by projects

APPLICATION SECURITY TOOLS IN CI/CD PIPELINES

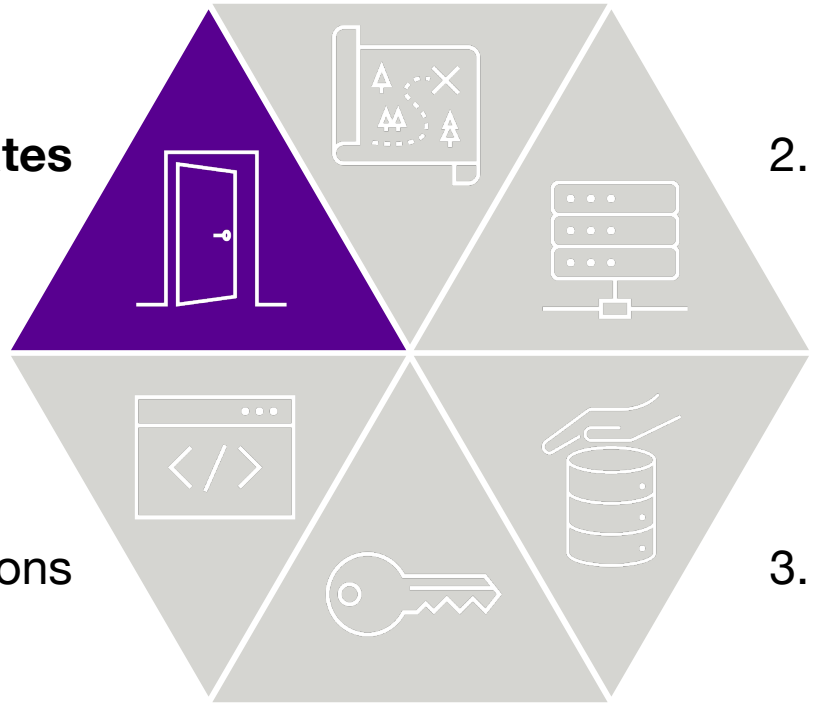


EXEMPLAR TOOLS

- SonarQube
- SpotBugs (FindSecBugs)
- PMD
- ESLint
- Pylama
- checkov
- Nikto
- OWASP ZAP
- OWASP Dependency Tracker
- Detectify

AGENDA

1. Introduction
2. Infrastructure
3. Data
4. Identities
5. Applications
6. Gates



QUALITY GATES

- For every control validating something it should exist the corresponding quality gate
- Gates must be enforced in the CI/CD pipeline not allowing to continue when a threshold is not met
- For infrastructure and platform, define clear policies and vulnerability resolution times
  - E.g., 30 days for non-critical vulnerabilities, 2 days for critical
  - Do not allow deployments after the resolution threshold is exceeded
  - For stuff already running, eliminate the deployment or preferably quarantine the stack (e.g., eliminate network routes but do not remove for forensics)
  - Make the process aware of exceptions and false positives

QUALITY GATES FAQ

- Should we have global gates at the organization level, or gates per domain or application?
  - DevSecOps promotes the second: Independence and responsibility of product-oriented teams
  - To make it viable at the organization level, govern them with transparency and traceability
- Some tools already have their own project-level quality gate functionality, e.g., SonarQube. Should we use them?
  - It is possible, but may be of limited applicability (only partial measures, evaluation at inconvenient times along the pipeline)
  - It is generally better to set up gates per stage or even per tool
- Should we hard-code thresholds in the pipelines?
  - A threshold in a pipeline should be a clear and traceable specification
  - It is better to externalize gate thresholds, for transparency and for clarity about who set what and why (e.g., do not “dilute” threshold values in long pipelines)

QUALITY GATES EXTERNALIZATION

```
104         stage('Dependency vulnerability tests') {
105             steps {
106                 echo "-=- run dependency vulnerability tests -=-"
107                 sh "./mvnw dependency-check:check"
108                 dependencyCheckPublisher
109                     failedTotalHigh: 2,
110                     unstableTotalHigh: 2,
111                     failedTotalMedium: 5,
112                     unstableTotalMedium: 5
113             }
114         }
```

GOOD

```
23      stages {
24          stage('Prepare Environment') {
25              qualityGates = readYaml(file: "quality-gates.yaml")
26          }
```

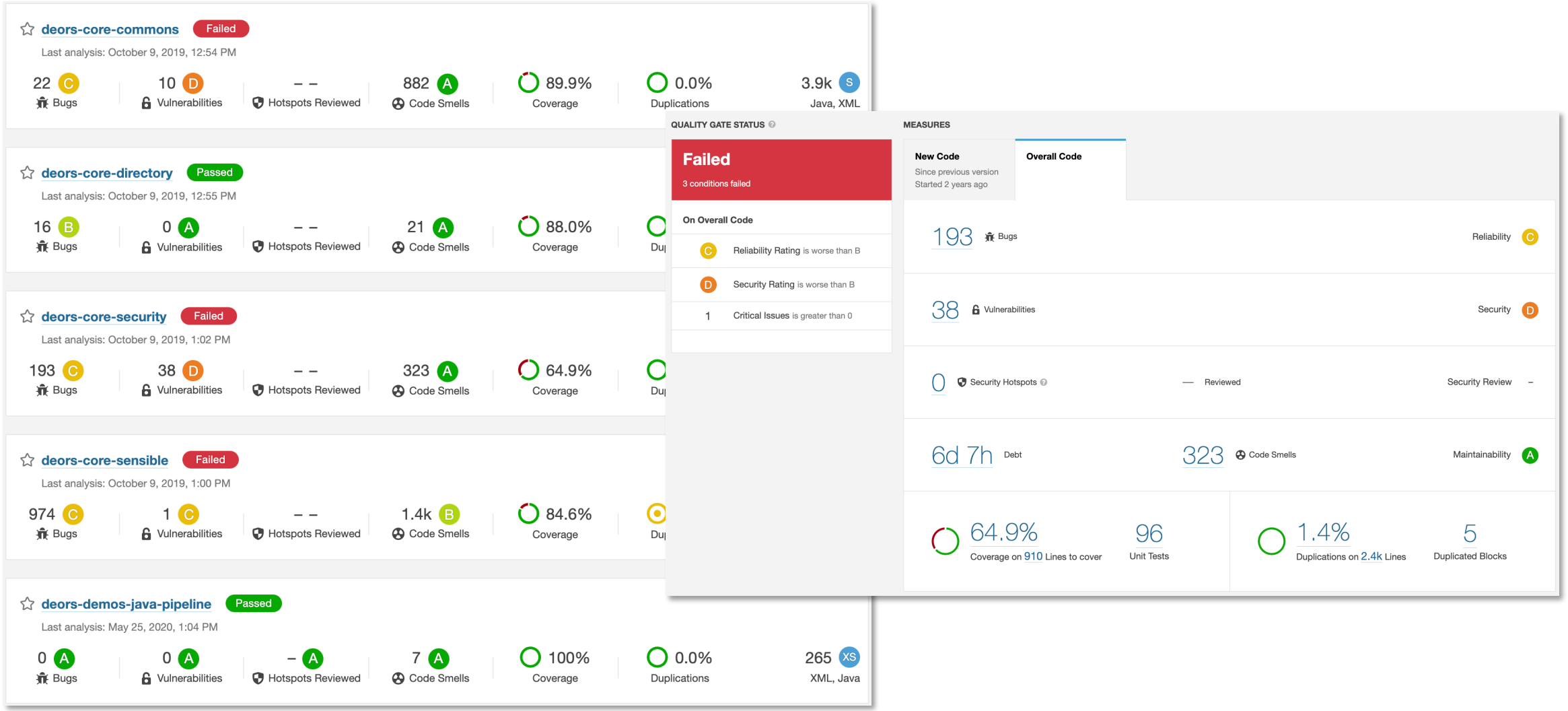
BETTER!

```
110         stage('Dependency vulnerability tests') {
111             steps {
112                 echo "-=- run dependency vulnerability tests -=-"
113                 sh "./mvnw dependency-check:check"
114                 dependencyCheckPublisher
115                     failedTotalHigh: qualityGates.security.dependencies.high.failed,
116                     unstableTotalHigh: qualityGates.security.dependencies.high.unstable,
117                     failedTotalMedium: qualityGates.security.dependencies.medium.failed,
118                     unstableTotalMedium: qualityGates.security.dependencies.medium.unstable
119             }
120         }
```

quality-gates.yaml

```
1  security:
2    static:
3      high:
4        unstable: 0
5        failed: 0
6      medium:
7        unstable: 0
8        failed: 5
9    dynamic:
10     high:
11       unstable: 0
12       failed: 0
13     medium:
14       unstable: 0
15       failed: 5
16   dependencies:
17     high:
18       unstable: 2
19       failed: 2
20     medium:
21       unstable: 5
22       failed: 5
```

QUALITY GATES MANAGED BY TOOLS



ANY QUESTIONS?