

# SECURITY WITHOUT HEADACHES

A background image of a person's face, heavily shadowed and dimmed, with their hands pressed against their temples, conveying a sense of stress or a headache.

# CONTINUOUS SECURITY INSIGHTS

 FULL PORTFOLIO SCANNING

 DEEP DIVE ANALYSIS

 GUIDANCE TO FIX

Secure the whole application landscape by enabling you to mitigate risks and vulnerabilities across the breadth and depth of your organization.

- ✓ Ranks and benchmarks the identified security risks
- ✓ Exposes them in full transparency
- ✓ Help communicate the urgencies
- ✓ Presents a clear control overview of your software fixing needs

# 1 PLATFORM



**1 SINGLE VERSION OF THE TRUTH**



**PRIORITIZED RECOMMENDATIONS**



**CLEAR & EASY TO USE FOR ALL TEAMS**

Unified and role-based perspective:

**Security Specialists:** One platform to support me with:

- ✓ Overall software scanning
- ✓ Deep dives per category
- ✓ Prioritization and guidance to fix
- ✓ One version of the truth helps communicate the action to take and coach the teams

**Developers:** Quickly identify the most pressing security issues in the system and code they are working on.

**Managers:** Focus on business management without worrying about the performance and security of software.

Sigrid® | Software Security provides careful curation & benchmarking of your software security situation in three steps:

# SCAN

the code for **vulnerabilities**

# RANK

for **compliance**

# RECOMMEND

for **risk mitigation**

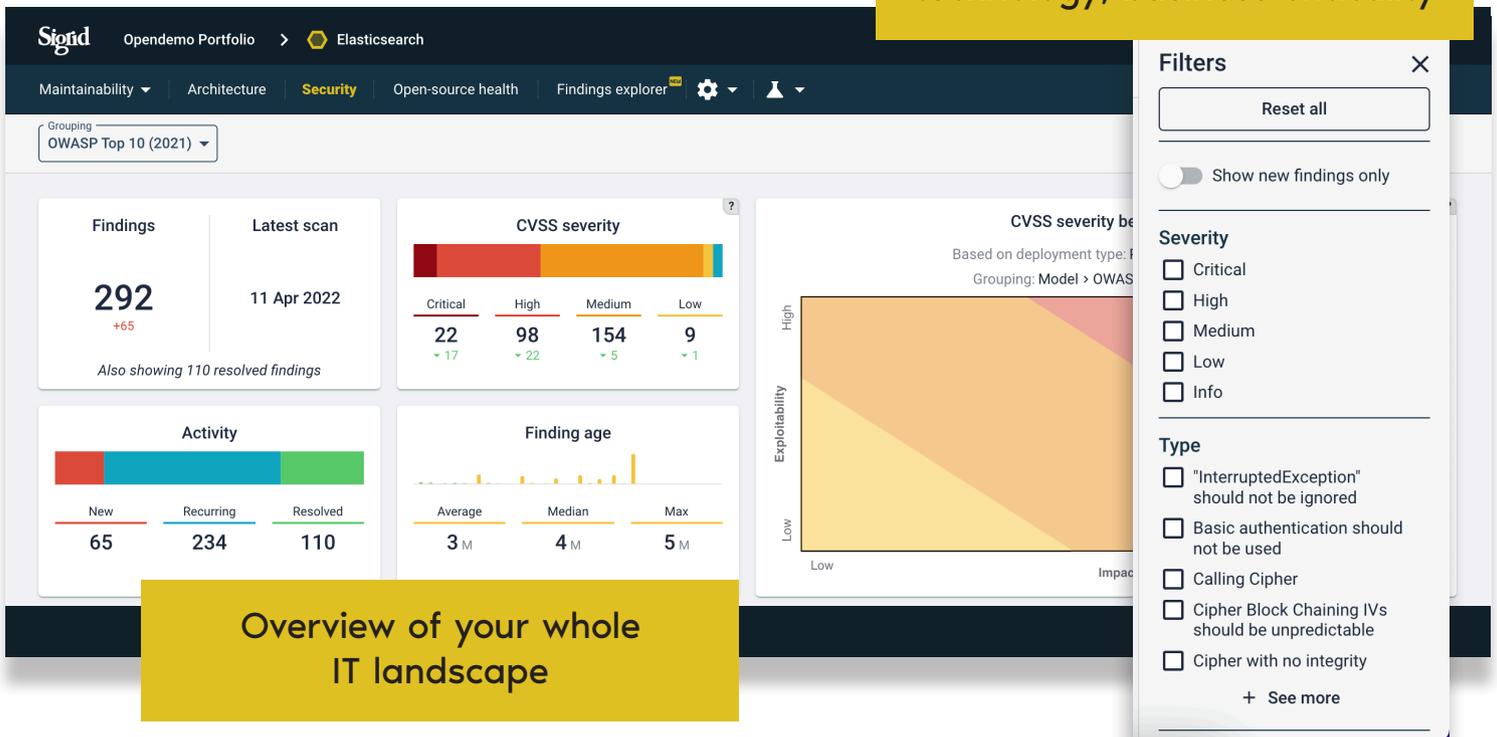
It helps reducing the noise with one platform, one single version of the truth, clear prioritization of issues, and is easy to use for all teams.

## Step 1:

# SCAN

the code for **vulnerabilities**

Categorize your IT systems based on division, supplier, technology, business criticality



Overview of your whole IT landscape

# Step 2: RANK

for compliance

Grouping  
OWASP Top 10 (2021)

None

Latest scan

Finding

Location

Model

Also show

SIG Security

SIG Code Reliability Top 10

ISO 5055 - Security

ISO 5055 - Reliability

ISO 5055 - Performance Efficiency

CWE Top 25 Most Dangerous Softwar...

PCI DSS v3.2.1 - Requirement 6.5 (201...

PCI DSS v4.0 - Control Objectives (202...

New

65

Finding age

Average Median Max

3 M 4 M 5 M

Exploitability

Low Impact High

Easily rank your findings to specific and industry standards such as OWASP Top 10, ISO 5055, CWE Top 25, PCI DSS, and more

Findings

292

Latest scan

11 Apr 2022

CVSS severity

Critical	High	Medium	Low
22	98	154	9
-17	-22	-5	-1

Activity

New	Recurring	Resolved
65	234	110

Finding age

Average Median Max

3 M 4 M 5 M

CVSS severity benchmark

Based on deployment type: Public-facing

Grouping Model: OWASP Top 10 (2021)

Exploitability

Low Impact High

Ranking is based on both impact and exploitability

Description

Findings

- A1 Broken Access Control
- A2 Cryptographic Failures
- A3 Insecure Deserialization
- A4 Insecure Default Permissions
- A5 Sensitive System Configuration
- A6 Vulnerable Components
- A7 Weak and Obscure Credentials

See which new findings Sigrid® has found

## Step 3:

# RECOMMEND

for  
risk  
mitigation

Check for the newest security findings

Type	Location	Severity	Impact	Exploitability	Age	Raw
Gradle dependency h2 contains 6 vulnerabilities	.../build.gradle:1	9.4 C	4 M	High	4 M	Raw
Jar dependency google-oauth-client contains 1 vulnerability	.../google-oauth-client-1.23.0.jar.sha1:1	9.1 C	3 M	High	3 M	Raw
Gradle dependency xmlsec contains 1 vulnerability	.../build.gradle:1	7.5 H	4 M	High	4 M	Raw
Jar dependency xmlsec contains 1 vulnerability	.../xmlsec-2.1.4.jar.sha1:1	7.5 H	4 M	High	4 M	Raw
Gradle dependency xmlsec contains 1 vulnerability	.../build.gradle:1	7.5 H	4 M	High	4 M	Raw
Jar dependency xmlsec contains 1 vulnerability	.../xmlsec-2.1.4.jar.sha1:1	7.5 H	4 M	High	4 M	Raw
Potential Path Traversal (file read)	.../SslConfig.java:135	6.9 M	1 M	High	1 M	Raw

See the recommendation from Sigrid® and SIG's certified security experts

```
x-pack/plugin/sql/sql-client/src/main/java/org/elasticsearch/xpack/sql/client/SslConfig.java  
120  
121- private KeyManager[] loadKeyManagers() throws GeneralSecurityException, IOException {  
122-     if (StringUtil.hasText(keystoreLocation) == false) {  
123-         return null;  
124-     }  
125-  
126-     char[] pass = (StringUtil.hasText(keystorePass) ? keystorePass.trim().toCharArray() : null);  
127-     KeyStore keyStore = loadKeyStore(keystoreLocation, pass, keystoreType);  
128-     KeyManagerFactory kmFactory = KeyManagerFactory.getInstance(KeyManagerFactory.getDefaultAlgorithm());  
129-     kmFactory.init(keyStore, pass);  
130-     return kmFactory.getKeyManagers();  
131- }  
132-  
133- private KeyStore loadKeyStore(String source, char[] pass, String keystoreType) throws GeneralSecurityException, IOException {  
134-     KeyStore keyStore = KeyStore.getInstance(keystoreType);  
135-     Path path = Paths.get(source);  
136-  
137-     if (Files.exists(path) == false) {  
138-         throw new ClientException(  
139-             "Expected to find keystore file at [" + source + "] but was unable to. Make sure you have specified a valid URI."  
140-         );  
141-     }  
142-  
143-     try (InputStream in = Files.newInputStream(Paths.get(source), StandardOpenOption.READ)) {  
144-         keyStore.load(in, pass);  
145-     }  
146- }
```

Severity	Impact	Exploitability
6.9 M	Medium	High

Status
Raw

Finding age	Date first seen	Date last seen
1 M	7 Mar 2022	11 Apr 2022

Origin
FindSecBugs

Location
.../SslConfig.java:135

Remark

The exact vulnerability is within each finding

# BENEFITS

- ✓ Part of the **SIGRID® | SOFTWARE ASSURANCE** platform - Go beyond security - and measurably improve software reliability, architecture quality, maintainability, and more.
- ✓ **ACTIONABLE ADVICE** with its unique risk-based analysis. This analysis originates from a large benchmark of software weaknesses and consequences. It rates the probability and exploitability of findings within the business context.
- ✓ Delivers a **TAILORED SECURITY SOLUTION** - the appropriate level of security insights for each application within your portfolio.
- ✓ **NO CONFIGURATION NEEDED** - runs on your entire portfolio.
- ✓ **FOCUS** on what matters most, with **CURATED RESULTS.**
- ✓ Advisory **SERVICES** from SIG's certified security experts - help you coach your organization, triage findings, and perform code reviews.
- ✓ Applies a wide range of **BEST IN CLASS SCAN TECHNOLOGIES.**

# SECURITY MODULE

of Sigrid® | Software Assurance-with-a-Service

Sigrid provides a holistic view of your software application landscape. Surface insights from bits-to-boardroom that brings everyone together.

Teams can review the condition of the entire IT portfolio, and specialists can quickly dive into code-level violations or review the architecture. CIOs, CISOs, product owners, developers, and every stakeholder get relevant insights via personalized dashboards with actionable recommendations.



## Our clients



# **COMPLETE TRANSPARENCY**

Visibility into your entire software application landscape

# **BUSINESS CONTEXT**

Bridge the gap between the business and IT. Track progress against both technical and business objectives.

# **BETTER COLLABORATION**

A single point of reference empowers teams to communicate more efficiently and work better together.

# **REDUCE WASTAGE**

Fact-based analysis generates actionable recommendations within the code. Eliminate the noise, reduce costs, and optimize the software development lifecycle.

# **BUSINESS RESILIENCE**

Customized views enable the workforce to build an agile, secure, and compliant software application landscape.

# LEARN MORE

Click here:

Get  
your  
live demo

More  
on  
SIG

Subscribe  
for  
news

Request a live demo: [www.softwareimprovementgroup.com/sigrid-demo](http://www.softwareimprovementgroup.com/sigrid-demo)

More on SIG: [www.softwareimprovementgroup.com/SecureMySoftware](http://www.softwareimprovementgroup.com/SecureMySoftware)

Want to stay updated? Subscribe to SIG newsletter: [www.softwareimprovementgroup.com](http://www.softwareimprovementgroup.com)

## About Software Improvement Group

Software Improvement Group (SIG) helps organizations trust the technology they depend on. We've made it our mission to get software right for a healthier digital world by combining our intelligent technology with our human expertise to dig deep into the build quality of enterprise software and architecture - measuring, monitoring, and benchmarking it against the world's largest software analysis database.

With SIG software assurance, organizations can surface the factors driving software total cost of ownership and make fact-based decisions to cut costs, reduce risk, speed time to market, and accelerate digital transformation.

Software Improvement Group is the first fully certified laboratory in the world to measure against the ISO 25010 standard. We make this lab accessible to our clients through our SaaS software assurance platform - Sigrid - which enables them to take a risk-based approach to improving the health of their IT landscapes.

We serve clients spanning the globe in every industry, including DHL, Philips, ING, KLM, BTPN, Weltbild, KPN, as well as leading European governmental organizations.

SIG was founded in 2000 as an independent technology company with embedded consulting services. SIG is headquartered in Amsterdam, with offices in New York, Copenhagen, Antwerp and Frankfurt.

Learn more at [www.softwareimprovementgroup.com](http://www.softwareimprovementgroup.com).



Fred. Roeskestraat 115  
1076 EE Amsterdam  
The Netherlands

[www.softwareimprovementgroup.com](http://www.softwareimprovementgroup.com)  
[marketing@softwareimprovementgroup.com](mailto:marketing@softwareimprovementgroup.com)

### Legal Notice

This document may be part of a written agreement between Software Improvement Group (SIG) and its customer, in which case the terms and conditions of that agreement apply hereto. In the event that this document was provided by SIG without any reference to a written agreement with SIG, to the maximum extent permitted by applicable law this document and its contents are provided as general information 'as-is' only, which may not be accurate, correct and/or complete and SIG shall not be responsible for any damage or loss of any nature related thereto. All rights are reserved. Unauthorized use, disclosure or copying of this document or any part thereof is prohibited.