ACCUKNOX®

Application Security Posture Management Report (ASPM)

Report Period **30 Days - Jul 01, 2025** to **Jul 31, 2025**

Prepared for

Product

Prepared by

AccuKnox

support@accuknox.com

About the Report

This report provides an in-depth analysis of the current application security posture, highlighting critical vulnerabilities, compliance gaps, and risk factors across our cloud infrastructure. Leveraging advanced ASPM tools, we have identified areas for improvement, recommended actionable strategies, and outlined a roadmap to strengthen our cloud security framework. This comprehensive assessment is designed to support informed decision-making, enhance risk management, and align with our organization’s security and regulatory requirements.

SAST Findings

Jul 01, 2025
to Jul 31, 2025

Report Summary

The SAST scan detected **3,438 potential security vulnerabilities** in the source code, categorized into **215 Critical**, **436 High**, **1,390 Medium**, **1,394 Low** and **3 Others** severity issues across **3 repositories.https://gitlab.com/project/repo2** was identified as the most vulnerable, contributing **584 findings** alone.These issues pose a significant security risk if not remediated in a timely manner.

SAST Findings by Severity

215
Critical Findings

436
High Findings

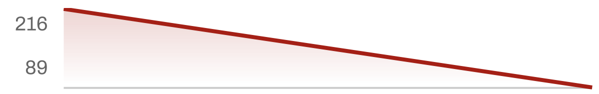
1390
Medium Findings

1394
Low Findings

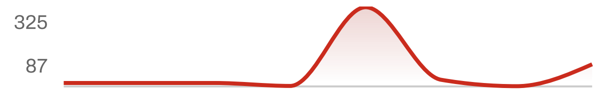
Displays the total number of findings along with their severity distribution, helping users identify and prioritize security risks.

SAST Findings Trend by Severity

Critical ↓ -170 % **45**



High ↑ 89 % **92**



Displays static code analysis findings over time, categorized by severity, helping users monitor risk trends and remediation progress.

Top 5 SAST Findings

Category	Severity	Findings
Add curly braces around the nested statement(s).	Critical	18
Refactor this method to reduce its Cognitive Complexity from 16 to the 15 ...	Critical	15
Unexpected var, use let or const instead.	Critical	14
Refactor this method to reduce its Cognitive Complexity from 23 to the 15 ...	Critical	12
Add a "case default" clause to this "switch" statement.	Critical	9

Displays the top 5 static code analysis findings, sorted first by criticality and then by occurrence count, helping users focus on the most impactful issues.

Top 5 SAST Findings by Count

Category	Severity	Findings
Improper_Exception_Handling	Medium	857
Broken_or_Risky_Hashing_Function	Low	187
Parameter_Tampering	Low	157
Relative_Path_Traversal	Low	146
CSRF	Low	118

Displays the top 5 static code analysis findings sorted by occurrence count, helping users identify the most frequent issues.

SAST Findings by Types

Findings Type	Findings					Severity
Code_smell	726	209 C	271 H	0 M	204 L	42 I
Security_hotspot	61	4 C	0 H	12 M	45 L	0 I
Vulnerability	105	2 C	103 H	0 M	0 L	0 I
Bug	54	0 C	42 H	0 M	12 L	0 I

Displays static code analysis findings categorized by type, along with their severity distribution, helping users prioritize remediation.

Top Vulnerable Repos – SAST

Repository	Findings					Severity
project/repo2	584	80 C	236 H	10 M	253 L	5 I
safeer-accuknox/use-cases	13	0 C	4 H	4 M	2 L	0 I
example/repo1	6	0 C	1 H	2 M	3 L	0 I

Displays the top 5 repositories with the highest number of SAST findings, categorized by severity to highlight risk distribution.

SAST Findings by Security Category

Category	Severity	Findings
auth	Critical	2
sql-injection	Critical	2
permission	Medium	4
rce	Medium	2
weak-cryptography	Medium	6

Displays static code analysis findings categorized by security category, along with their severity distribution, helping users prioritize remediation.

DAST Findings

Jul 01, 2025
to Jul 31, 2025

Report Summary

The DAST scan uncovered **197 findings** across **3 domains**, categorized into **60 Medium** and **137 Low** severity issues.The domain **https://juice-shop.herokuapp.com** was identified as the most impacted, contributing **188 findings**.These vulnerabilities may expose systems to real-time threats such as insecure endpoints, authentication bypasses, and injection attacks, requiring prompt investigation and remediation.

DAST Findings by Severity

0
Critical Findings

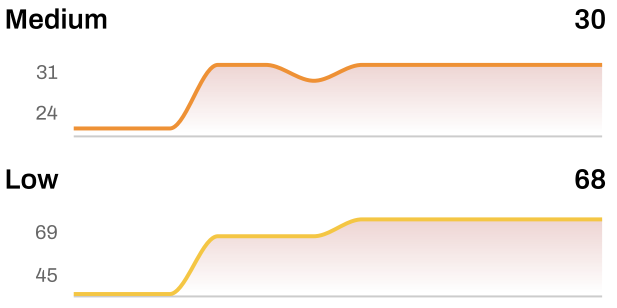
0
High Findings

60
Medium Findings

137
Low Findings

Displays the total number of findings along with their severity distribution, helping users identify and prioritize security risks.

DAST Findings Trend by Severity



Displays DAST findings over time, categorized by severity, helping users monitor risk trends and remediation progress.

Top 5 DAST Findings

Findings	Severity	Assets
Content Security Policy (CSP) Header Not Set	Medium	26
Cross-Domain Misconfiguration	Medium	22
Missing Anti-clickjacking Header	Medium	4
Sub Resource Integrity Attribute Missing	Medium	4
CSP: Failure to Define Directive with No Fallback	Medium	2

Displays the top 5 DAST findings, sorted first by criticality and then by occurrence count, helping users focus on the most impactful issues.

Top 5 DAST Findings by Count

Findings	Severity	Assets
Strict-Transport-Security Header Not Set	Low	38
Re-examine Cache-control Directives	Informational	32
Modern Web Application	Informational	28
Insufficient Site Isolation Against Spectre Vulnerability	Low	27
Content Security Policy (CSP) Header Not Set	Medium	26

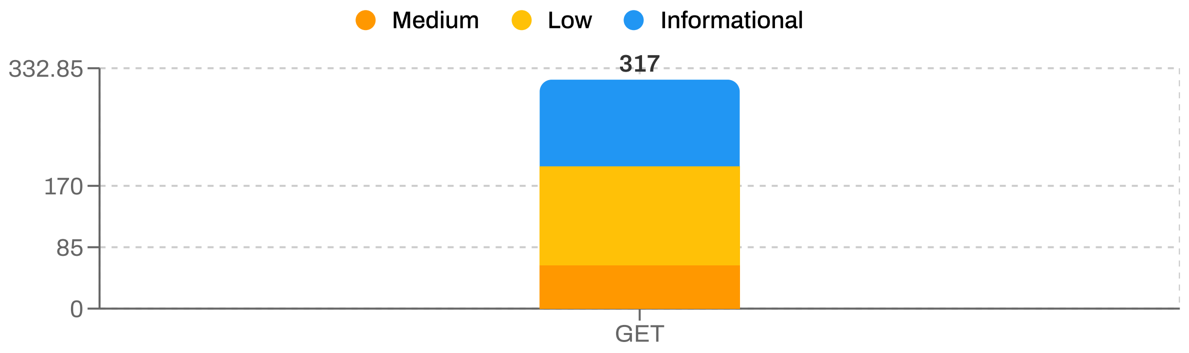
Displays the top 5 DAST findings sorted by occurrence count, helping users identify the most frequent security issues.

Top 5 Vulnerable Endpoints

Endpoints	Count					Severity
https://prabhavdev.me/	20	0 C	0 H	6 M	8 L	6 I
https://prabhavdev.me/sitemap.xml	20	0 C	0 H	6 M	8 L	6 I
https://juice-shop.herokuapp.com	20	0 C	0 H	4 M	10 L	6 I
https://juice-shop.herokuapp.com/sitema...	20	0 C	0 H	4 M	10 L	6 I
https://juice-shop.herokuapp.com/	18	0 C	0 H	4 M	8 L	6 I

Displays the top 5 endpoints with the highest number of findings, sorted by total count. Also shows the severity distribution for each endpoint, helping users assess risk exposure.

Findings by HTTP Methods



Displays findings categorized by HTTP methods (GET, POST, etc.), showing the distribution of findings by severity to highlight potential risks across different request types.

Top Vulnerable Domains – DAST

Domain	Count					Severity
https://juice-shop.herokuapp.com	188	0 C	0 H	44 M	74 L	70 I
https://prabhavdev.me	91	0 C	0 H	12 M	49 L	30 I
https://cloud.tenable.com	38	0 C	0 H	4 M	14 L	20 I

Displays the domains with the highest number of DAST findings, helping security teams identify and prioritize externally exposed assets with the most critical vulnerabilities.

Container Image Findings

Jul 01, 2025
to Jul 31, 2025

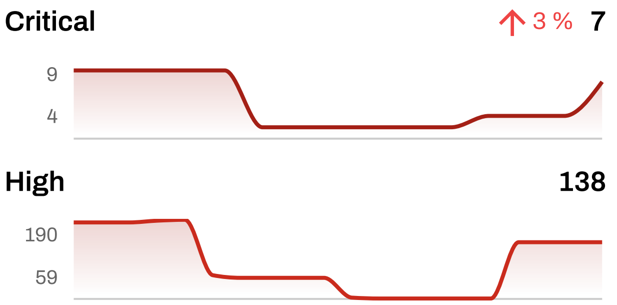
Report Summary

The container image scan detected **9,074 findings** across **11** container images, categorized into **18 Critical**, **346 High**, **7,111 Medium**, **1,582 Low** and **17 Others** severity issues.The image **harbor.do.accuknox.com/chola_ms/956994857092.dkr.ecr.us-east-2.amazonaws.com/soarcast/redis:latest** was identified as the most vulnerable, contributing **2,849 findings**.These vulnerabilities are commonly associated with outdated base images, unpatched packages, and misconfigurations—posing a significant threat to workload security if not addressed promptly.

Container Image Findings by Severity

18	Critical Findings
346	High Findings
7111	Medium Findings
1582	Low Findings

Container Image Findings Trend



Critical

High

Displays Container Image Findings over time, categorized by severity, helping users track risk trends and remediation progress.

Top Vulnerable Packages

Cloud Provider	Findings					Severity
libxml2	62	7 C	11 H	30 M	14 L	0 I
stdlib	84	3 C	12 H	65 M	0 L	0 I
zlib1g	7	3 C	0 H	4 M	0 L	0 I
libaom3	4	2 C	2 H	0 M	0 L	0 I
boost-license1_66_0	1	1 C	0 H	0 M	0 L	0 I

This widget displays the top 10 container images with the highest number of known vulnerabilities, assisting in identifying and prioritizing remediation efforts for the most at-risk images in your environment.

Top 10 Container Images by Vulnerabilities

Image	Findings
harbor.do.accuknox.com/chola_ms/9...	2.85K
harbor.do.accuknox.com/test_airgapp...	2.85K
harbor.do.accuknox.com/npci/kubear...	2.80K
harbor.do.accuknox.com/test_airgapp...	157
harbor.do.accuknox.com/chola_ms/ng...	152

Displays the top 10 container images with the highest number of associated vulnerabilities, helping teams quickly identify and prioritize remediation efforts for the most impacted images.

Top CVEs by Severity and Affected Images

CVE ID	Severity	Findings
CVE-2023-45853	Critical	3
CVE-2023-6879	Critical	2
CVE-2024-24790	Critical	3
CVE-2025-49794	Critical	3
CVE-2025-49795	Critical	1

This widget displays the top 10 CVEs ranked by severity and the number of container images affected. It helps prioritize remediation efforts by highlighting vulnerabilities that pose the greatest risk and have the widest impact across container images.

Top 20 CVEs with CVSS Baseline vs Severity

CVE	Severity	CVSS Score	Count
CVE-2023-45853	Critical	9.8	3
CVE-2024-24790	Critical	9.8	3
CVE-2025-49794	Critical	0	3
CVE-2025-49796	Critical	0	3
CVE-2023-6879	Critical	9.8	2

This widget highlights the Top 20 CVEs by prioritizing those with the highest CVSS scores, followed by severity level, and then by the number of affected instances. It enables teams to focus on vulnerabilities that pose the greatest risk due to their criticality and widespread presence.

Top 25 CWEs

Rank	CWE ID	Name	Findings
1	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7
2	CWE-787	Out-of-bounds Write	356
3	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	4
4	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	35
5	CWE-125	Out-of-bounds Read	260

This widget displays the Top 25 most dangerous Common Weakness Enumerations (CWEs) based on the MITRE 2024 list. These represent the most critical and prevalent software vulnerabilities that attackers commonly exploit.Use this insight to identify common vulnerability patterns and strengthen security posture.

IaC Findings

Jul 01, 2025
to Jul 31, 2025

Report Summary

The Infrastructure as Code (IaC) scan identified **232 findings** across **1 repository** , categorized into **21 High**, **68 Medium**, **139 Low** and **4 Others** severity issues.The repository **https://github.com/collabnix/terraform** was flagged as the most vulnerable, contributing **130 findings**. These issues highlight common configuration weaknesses that could impact the security and reliability of infrastructure if not addressed in a timely manner.

IaC Findings by Severity

0
Critical Findings

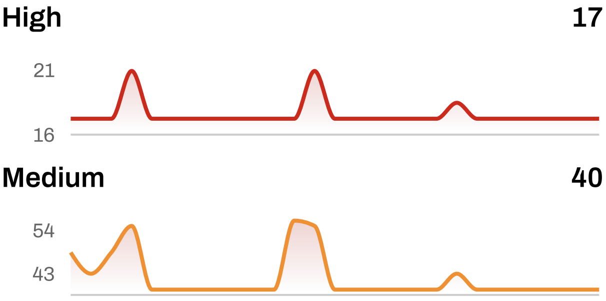
21
High Findings

68
Medium Findings

139
Low Findings

Displays the total number of findings along with their severity distribution, helping users identify and prioritize security risks.

IaC Findings Trend by Severity



Displays IaC findings over time, categorized by severity, helping users track risk trends and remediation progress.

Top 5 IaC Findings

Finding	Severity	Assets
Ensure all data stored in the Launch configuration or instance Elastic Bloc...	High	4
Ensure linux VM enables SSH with keys for secure communication	High	2
Ensure RDS Performance Insights are encrypted using KMS CMKs	High	2
Ensure Terraform module sources use a commit hash	High	2
Missing User Instruction	High	2

Displays the top 5 IaC findings, sorted first by severity and then by occurrence count, helping users focus on the most impactful issues.

Top 5 IaC Findings by Count

Finding	Severity	Findings
Unpinned Actions Full Length Commit SHA	Low	45
Chown Flag Exists	Low	11
Apt Get Install Pin Version Not Defined	Medium	9
Healthcheck Instruction Missing	Low	9
Healthcheck Not Set	Medium	6

Displays the top 5 IaC findings sorted by occurrence count, helping users identify the most frequent issues.

Top 5 Vulnerable IaC Repositories

Repository	Findings	Severity				
collabnix/terraform	130	0 C	17 H	40 M	66 L	3 I

Displays the top 5 repositories with the highest number of IaC security findings, categorized by severity to highlight risk distribution.

IaC Findings by Framework

Framework	Findings
terraform	130

Displays the number of IaC findings categorized by framework, providing insight into which frameworks have the most issues.

Secret Scan Findings

Jul 01, 2025
to Jul 31, 2025

Report Summary

The Secret scan revealed **20 hardcoded or exposed secrets**, categorized into **5 Critical** and **15 High** severity issues across **5 repositories. https://github.com/pishone-accuknox/juice-shop** had the highest exposure with **7 findings**. These issues pose a critical risk of unauthorized access to sensitive systems and services if not remediated promptly.

Secret Scan Findings

5
Critical Findings

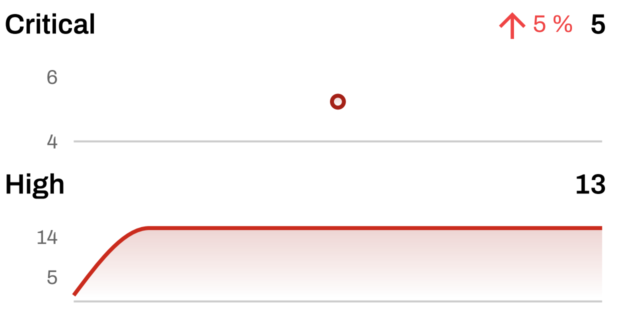
15
High Findings

0
Medium Findings

0
Low Findings

Displays the number of exposed secrets categorized by severity, helping teams assess risk levels and prioritize remediation efforts effectively.

Secret Exposure Trend by Severity



Displays the trend of detected secrets over time, categorized by severity, helping users track and prioritize secret exposures.

Top 5 Repositories with Secrets

Repository	Count	Severity				
pishone-accuknox/juice-shop	7	5 C	2 H	0 M	0 L	0 I
health_data.csv	6	0 C	6 H	0 M	0 L	0 I
commit/c488915b614e5f7995a0b9e4ee3...	3	0 C	3 H	0 M	0 L	0 I
commit/7470ee39170c834c878705e53d...	2	0 C	2 H	0 M	0 L	0 I
commit/adc24c5a18f4b77e1ae849e1636...	2	0 C	2 H	0 M	0 L	0 I

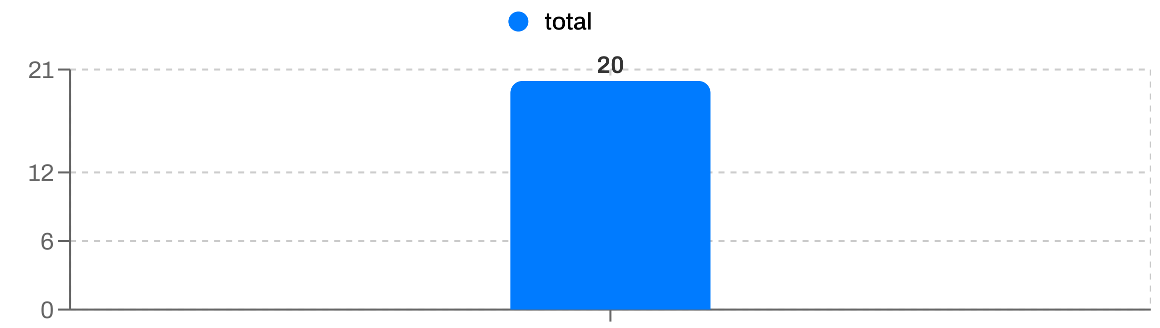
Displays the repositories with the highest number of detected secrets, helping users identify where sensitive data exposure is most prevalent.

Top 5 Contributors with Exposed Secrets

Name	Total
rishabhkeshan@gmail.com	3
bjoern.kimminich@owasp.org	2
tghosth@users.noreply.github.com	2

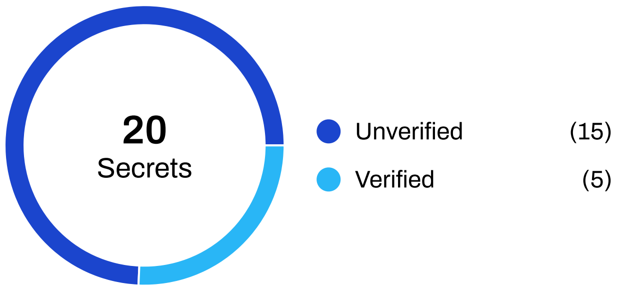
Displays the top 5 contributors responsible for exposed secrets in the codebase, showing the number of detected secrets per contributor. Helps teams enforce better security practices among developers.

Secrets by Decoder Type



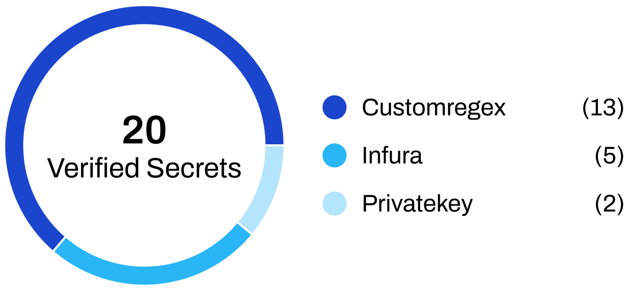
Displays verified and unverified secrets for each decoder type, helping users understand the distribution of detected secrets across different decoders.

Verified vs Unverified Secrets



Displays the number of verified and unverified secrets, helping users prioritize verified secrets for immediate attention.

Verified Secrets Breakdown



Displays the number of verified secrets categorized by the detector type, helping users understand the distribution of exposed secrets across different sources.