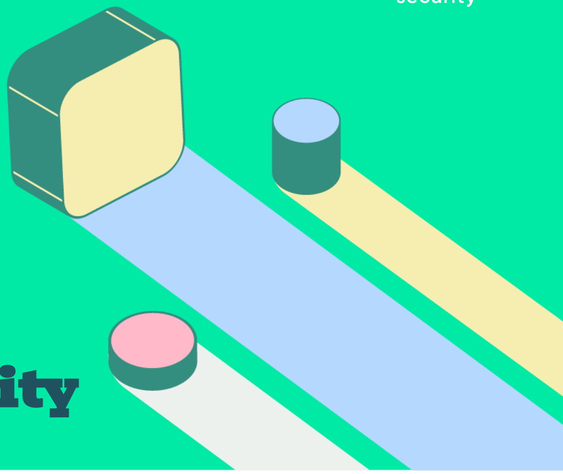


Solution brief

Vulcan Cyber and Orca Security

The challenge

Cloud infrastructure exposes organizations to external risks stemming from different types of vulnerabilities and misconfigurations. In today's complex multi-cloud environments, the abundance of assets can create overwhelming noise, making it challenging to focus on the right security issues and address them quickly. Furthermore, rapid deployment and updating of applications with new container images add to the complexity, requiring streamlined processes to ensure security measures are maintained.

- **75%** of security professionals pinpoint cloud security as their top concern
- **Only 20%** of organizations assess their overall cloud security posture in real-time
- **45%** of data breaches happen on the cloud

Vulcan Cyber and Orca security – better together

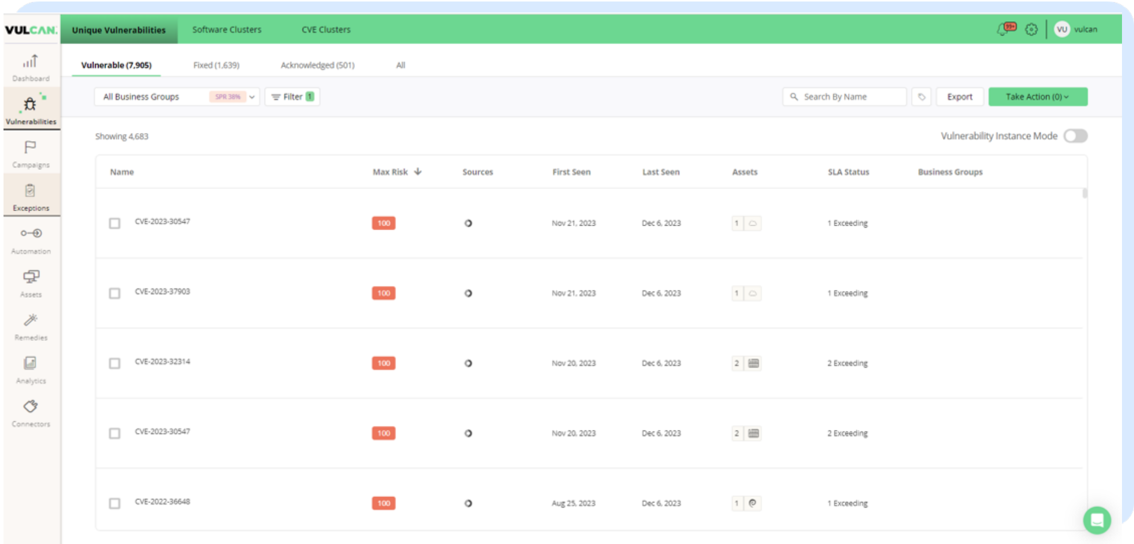
With Vulcan Cyber and Orca Security, teams can effectively manage cloud risks in one centralized platform at scale. The Orca Cloud Security Posture Management (CSPM) platform detects risks across all layers of the cloud, including misconfigurations, vulnerabilities, malware, overprivileged identities, and unsecured sensitive data. The Vulcan Cyber exposure operating system (ExposureOS) provides visibility into multi-cloud environments by aggregating these findings to gain a comprehensive view of organizational cloud risk. This integration allows for better prioritization and enables effective communication between security and DevOps teams, resulting in faster mitigation processes.

Joint solution key features

- **Unified cloud risk calculation:** Get a single view of all cloud assets and vulnerabilities and risk scores.
- **Prioritize and mitigate across clouds:** Identify and address risks based on business impact across multiple cloud environments.
- **Accelerate cloud security with AI:** Orca's AI-driven approach simplifies investigations and speeds up remediation, saving time and effort.
- **Manage container security at scale:** Monitor and remediate container risks efficiently, reducing overall security exposure.

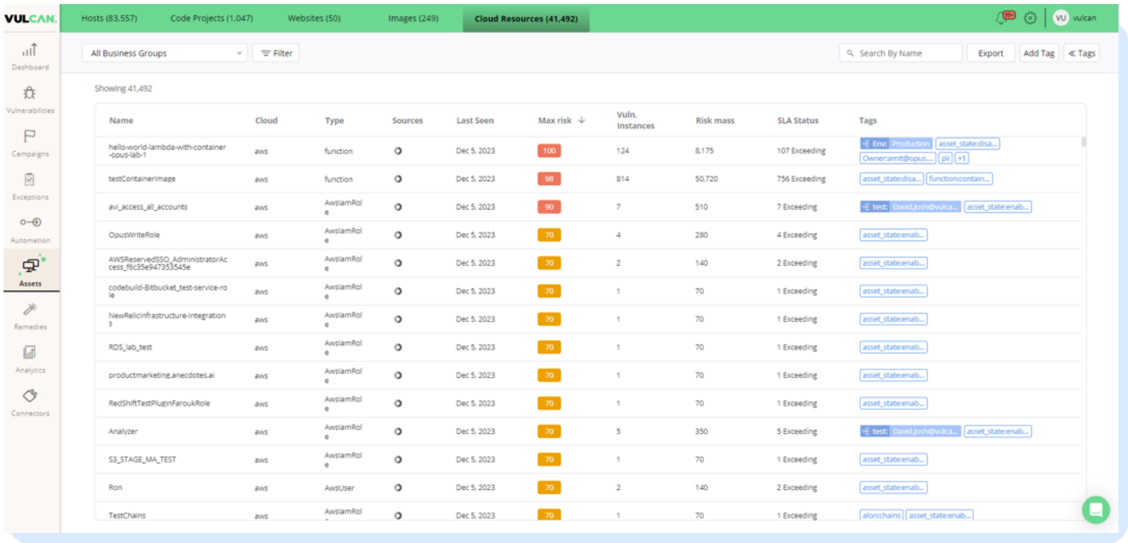
Use cases

- **Cloud (and multi-cloud) migration:** By offering centralized cloud exposure management, the integration facilitates streamlined cloud migration processes.
- **Ensure compliance:** Organizations can maintain compliance with industry standards and regulations by continuously monitoring cloud environments and receiving actionable insights to remediate detected issues.
- **Improving CI/CD lifecycle security:** Security measures are ensured throughout the software development process, preventing security vulnerabilities from being introduced into production cloud environments.
- **Stakeholder alignment and communication:** The integration enables security, DevOps, and management to align their efforts and gain visibility into the security posture of the organization's cloud infrastructure.



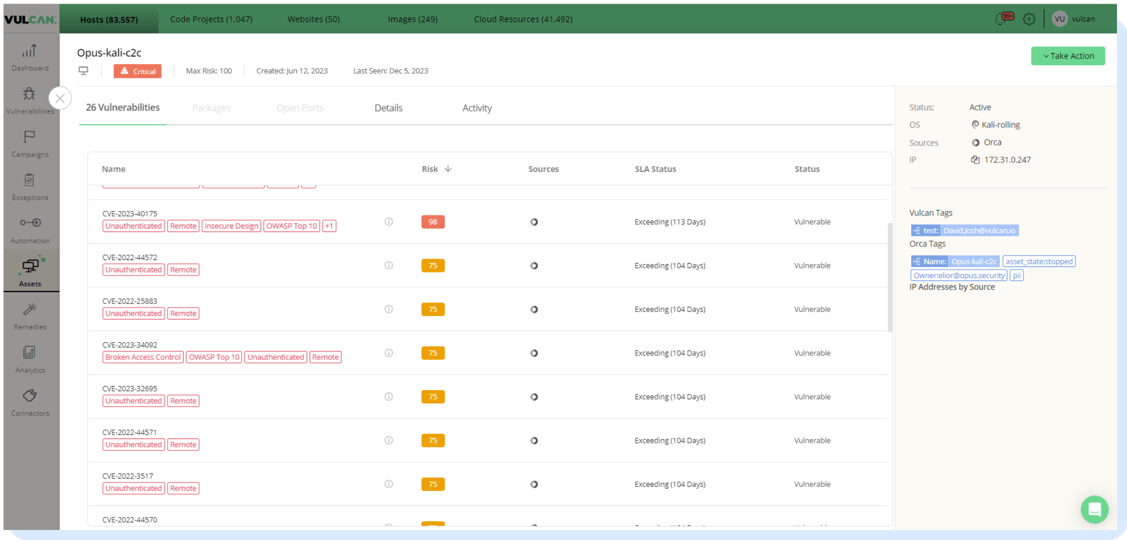
Showing 4,683

	Name	Max Risk ↓	Sources	First Seen	Last Seen	Assets	SLA Status	Business Groups
□	CVE-2023-30547	100	●	Nov 21, 2023	Dec 6, 2023	1	1 Exceeding	
□	CVE-2023-37903	100	●	Nov 21, 2023	Dec 6, 2023	1	1 Exceeding	
□	CVE-2023-32314	100	●	Nov 20, 2023	Dec 6, 2023	2	2 Exceeding	
□	CVE-2023-30547	100	●	Nov 20, 2023	Dec 6, 2023	2	2 Exceeding	
□	CVE-2022-36648	100	●	Aug 25, 2023	Dec 6, 2023	1	1 Exceeding	



Showing 41,492

Name	Cloud	Type	Sources	Last Seen	Max risk ↓	Vuln. Instances	Risk mass	SLA Status	Tags
hello-world-lambda-with-container-opus-lab-1	aws	function	●	Dec 5, 2023	100	124	8,175	107 Exceeding	Env: Production asset_state:disa... Owner:amit@opus.... pii +1
testContainerImage	aws	function	●	Dec 5, 2023	98	814	50,720	756 Exceeding	asset_state:disa... function:contain...
avi_access_all_accounts	aws	AwsIamRole	●	Dec 5, 2023	90	7	510	7 Exceeding	test: David.Josh@vulca... asset_state:enab...
OpusWriteRole	aws	AwsIamRole	●	Dec 5, 2023	70	4	280	4 Exceeding	asset_state:enab...
AWSReservedSSO_AdministratorAccess_f6c35e947353545e	aws	AwsIamRole	●	Dec 5, 2023	70	2	140	2 Exceeding	asset_state:enab...
codebuild-Bitbucket_test-service-role	aws	AwsIamRole	●	Dec 5, 2023	70	1	70	1 Exceeding	asset_state:enab...
NewRelicInfrastructure-Integrations	aws	AwsIamRole	●	Dec 5, 2023	70	1	70	1 Exceeding	asset_state:enab...
RDS_lab_test	aws	AwsIamRole	●	Dec 5, 2023	70	1	70	1 Exceeding	asset_state:enab...
productmarketing.anecdotes.ai	aws	AwsIamRole	●	Dec 5, 2023	70	1	70	1 Exceeding	asset_state:enab...
RedShiftTestPluginFaroukRole	aws	AwsIamRole	●	Dec 5, 2023	70	1	70	1 Exceeding	asset_state:enab...
Analyzer	aws	AwsIamRole	●	Dec 5, 2023	70	5	350	5 Exceeding	test: David.Josh@vulca... asset_state:enab...
S3_STAGE_MA_TEST	aws	AwsIamRole	●	Dec 5, 2023	70	1	70	1 Exceeding	asset_state:enab...
Ron	aws	AwsUser	●	Dec 5, 2023	70	2	140	2 Exceeding	asset_state:enab...
TestChains	aws	AwsIamRol	●	Dec 5, 2023	70	1	70	1 Exceeding	alon:chains asset_state:enab...



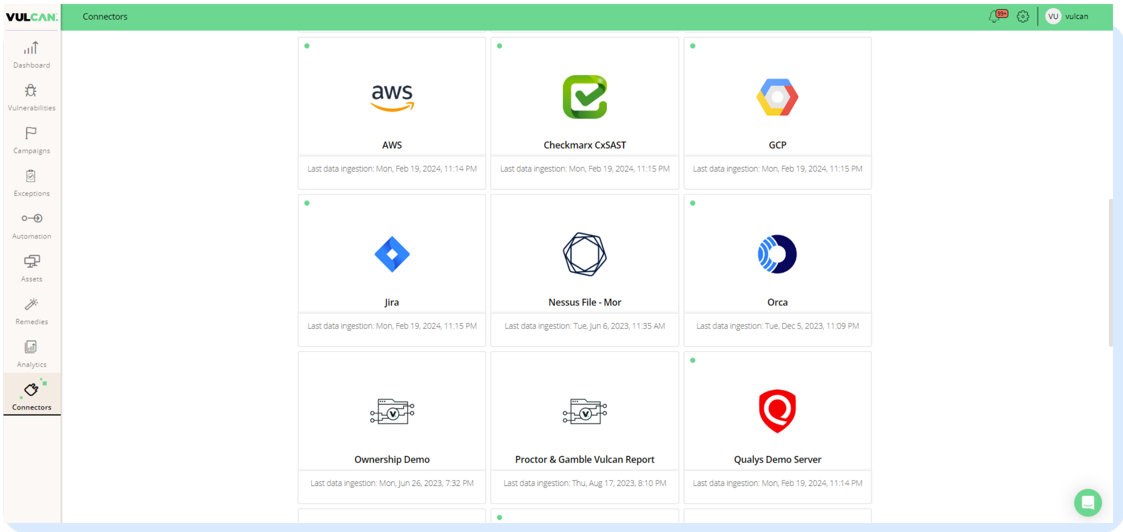
Opus-kali-c2c

Critical | Max Risk: 100 | Created: Jun 12, 2023 | Last Seen: Dec 5, 2023

Name	Risk ↓	Sources	SLA Status	Status
CVE-2023-40175 Unauthenticated Remote Insecure Design OWASP Top 10 +1	98	●	Exceeding (113 Days)	Vulnerable
CVE-2022-44572 Unauthenticated Remote	75	●	Exceeding (104 Days)	Vulnerable
CVE-2022-25883 Unauthenticated Remote	75	●	Exceeding (104 Days)	Vulnerable
CVE-2023-34092 Broken Access Control OWASP Top 10 Unauthenticated Remote	75	●	Exceeding (104 Days)	Vulnerable
CVE-2023-32695 Unauthenticated Remote	75	●	Exceeding (104 Days)	Vulnerable
CVE-2022-44571 Unauthenticated Remote	75	●	Exceeding (104 Days)	Vulnerable
CVE-2022-3517 Unauthenticated Remote	75	●	Exceeding (104 Days)	Vulnerable
CVE-2022-44570				

Status: Active
OS Kali-rolling
Sources Orca
IP 172.31.0.247

Vulcan Tags
test: David.Josh@vulcan.io
Orca Tags
Name: Opus-kali-c2c | asset_state:stopped | Owner:elior@opus.security | pii
IP Addresses by Source



AWS
Last data ingestion: Mon, Feb 19, 2024, 11:14 PM

Checkmarx CxSAST
Last data ingestion: Mon, Feb 19, 2024, 11:15 PM

GCP
Last data ingestion: Mon, Feb 19, 2024, 11:15 PM

Jira
Last data ingestion: Mon, Feb 19, 2024, 11:15 PM

Nessus File - Mor
Last data ingestion: Tue, Jun 6, 2023, 11:35 AM

Orca
Last data ingestion: Tue, Dec 5, 2023, 11:09 PM

Ownership Demo
Last data ingestion: Mon, Jun 26, 2023, 7:32 PM

Proctor & Gamble Vulcan Report
Last data ingestion: Thu, Aug 17, 2023, 8:10 PM

Qualys Demo Server
Last data ingestion: Mon, Feb 19, 2024, 11:14 PM

About Orca

Orca Security is the cloud security innovation leader, providing deeper visibility into AWS, Azure, and GCP without the operational costs of agents. With Orca Security, there are no overlooked assets, no DevOps headaches, and no performance hits on live environments.

About Vulcan Cyber

Vulcan Cyber has developed the market-leading Exposure operating system (ExposureOS) to provide information security teams with one platform to prioritize, orchestrate, and mitigate exposure risk at scale throughout the entire attack surface.