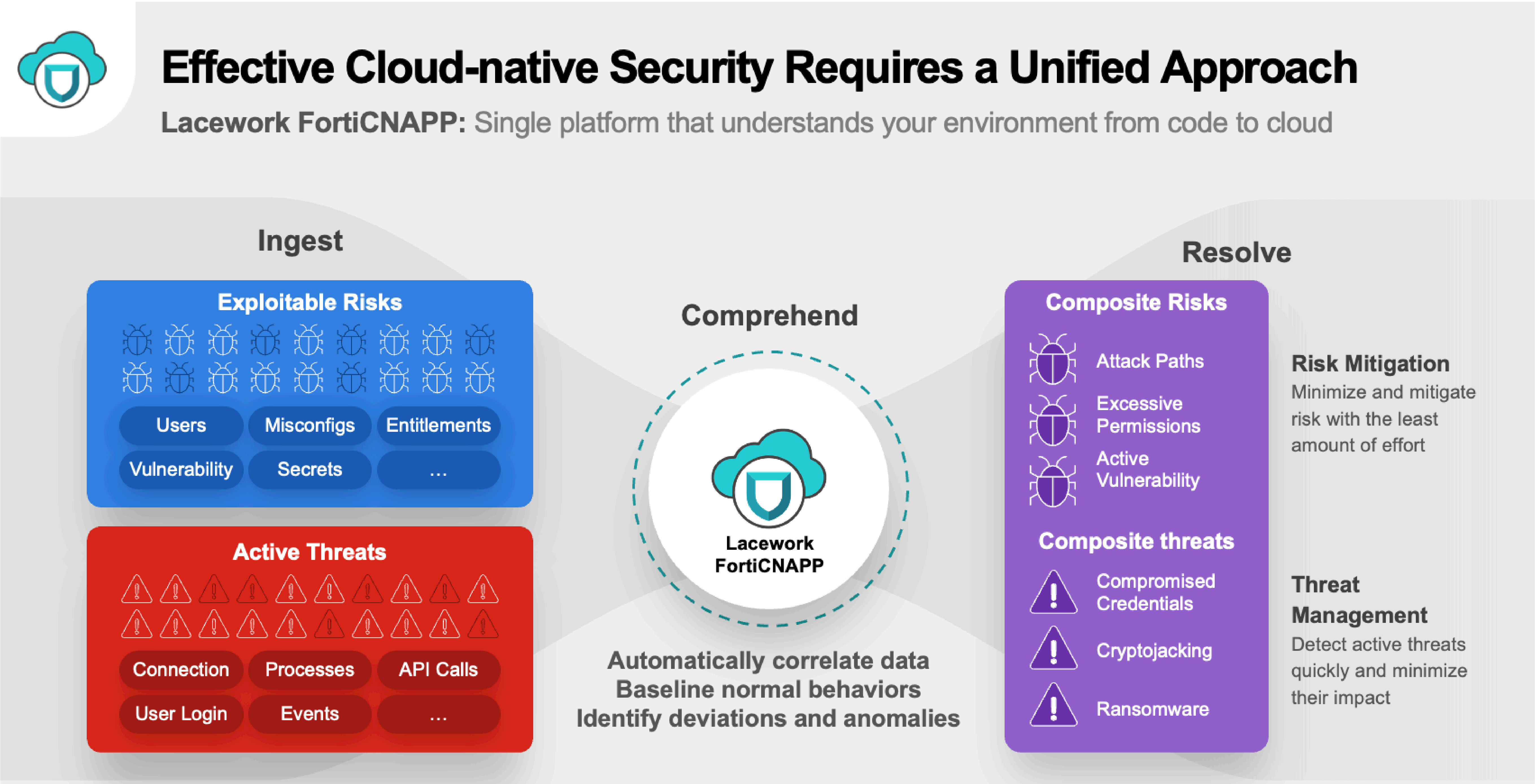
Assessment Report

Report created for ACME

Thursday April 24, 2025

> Generated by Fortinet
> AWS Accounts Analyzed: 1, Azure Subscriptions Analyzed: 1, GCP Projects Analyzed: 1, Hosts Scanned: 11, Containers Scanned: 16



Effective Cloud-native Security Requires a Unified Approach

Lacework FortiCNAPP: Single platform that understands your environment from code to cloud

Executive Summary

The purpose of this report is to highlight the assessment findings for ACME. The findings below are representative of the cloud accounts and hosts that were in scope of the engagement and cover cloud compliance and vulnerability findings leveraging FortiCNAPP agentless scanning capabilities. This report provides a detailed summary of each identified area of interest and how it pertains to your overall cloud security and risk.

Below is a summary of findings. Additional detail is provided on subsequent pages:

Total Containers with Critical Vulnerabilities	Hosts with Critical Vulnerabilities	Total Critical AWS Compliance Findings	Total Critical Azure Compliance Findings	Total Critical GCP Compliance Findings	Total High / Critical Behaviors Detected	Number of Secrets Detected
8	2	0	0	40	2	1

This assessment offers a glimpse into the value that FortiCNAPP provides customers, including:

- Reduce alerts 100:1
- Speed up security investigations by 80%
- Decrease SIEM ingestion costs by 50%
- Improve detections of anomalous behaviors in cloud accounts and workloads
- Accelerate security throughout development with less effort

Recommendations

Based on the findings of this assessment, Fortinet recommends the following action plan and next steps:

- Engage with your Fortinet account team and partner to review services offerings to prioritize and remediate the findings
- Complete a recurring Cloud Security Assessment once a wider FortiCNAPP deployment has been completed to baseline and trend improvements to your cloud security posture.

Exposed SSH Keys

Using FortiCNAPP agentless workload scanning the following SSH Keys have been found on your workloads:

Hostname	File Path	SSH Key Type
ip-172-16-1-45.us-east-2.compute.internal	home/ubuntu/.ssh/id_frontend	ssh-rsa

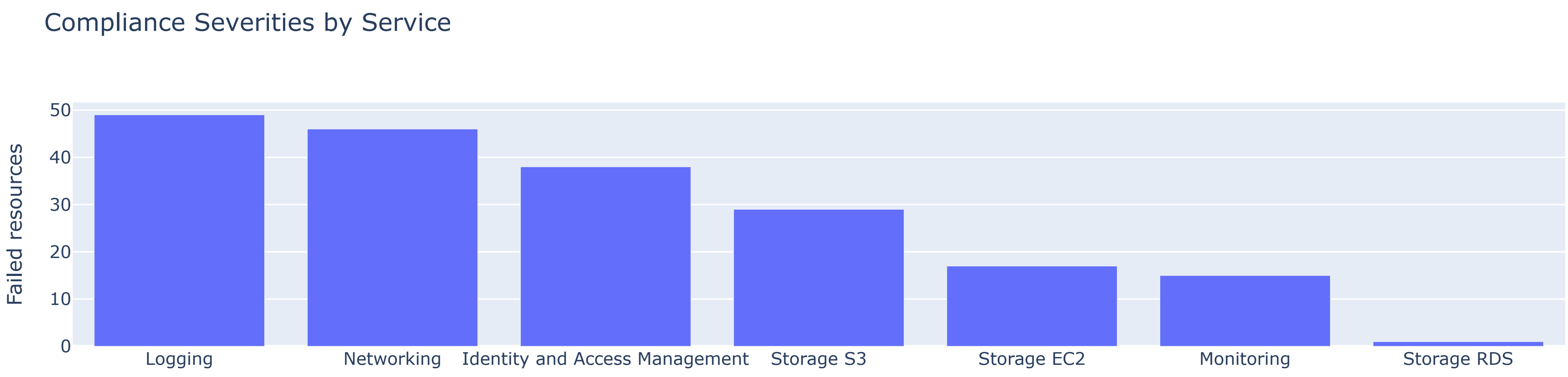
Compliance Findings

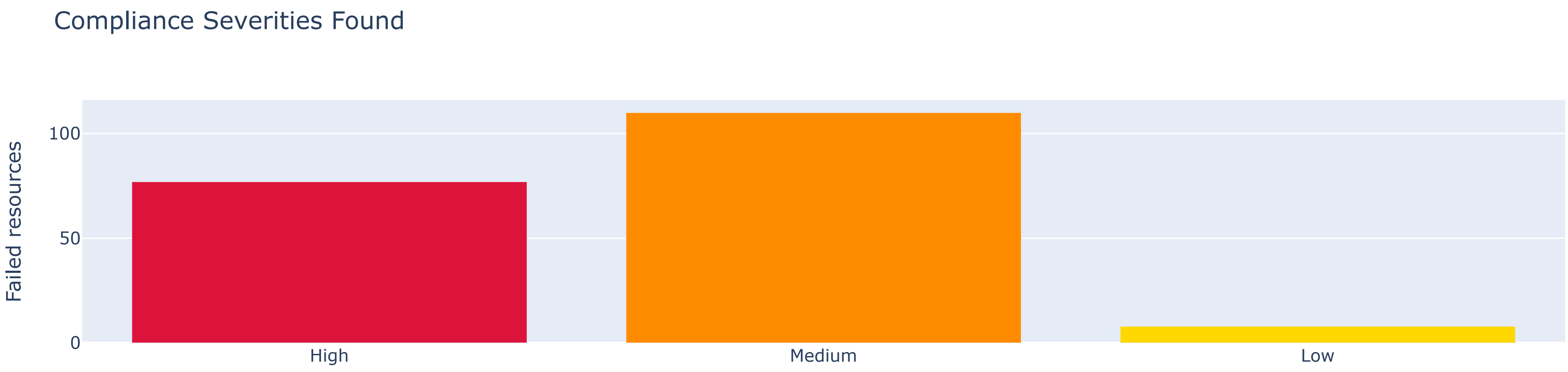
Using FortiCNAPP agentless compliance functionality, we've assessed the current security posture against best practices, policies, and compliance frameworks. FortiCNAPP identified the following:

AWS Compliance Findings

`Total AWS Accounts Analyzed: 1`

Account ID	Severity Count	Non-compliant Resources	Total Assessed Resources
583683056848	High: 8	77	192

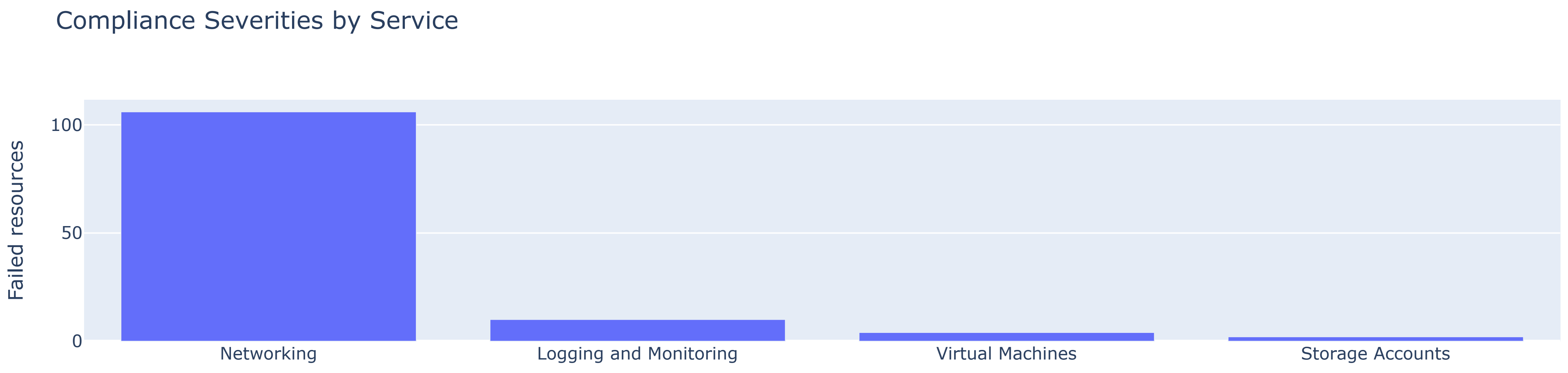


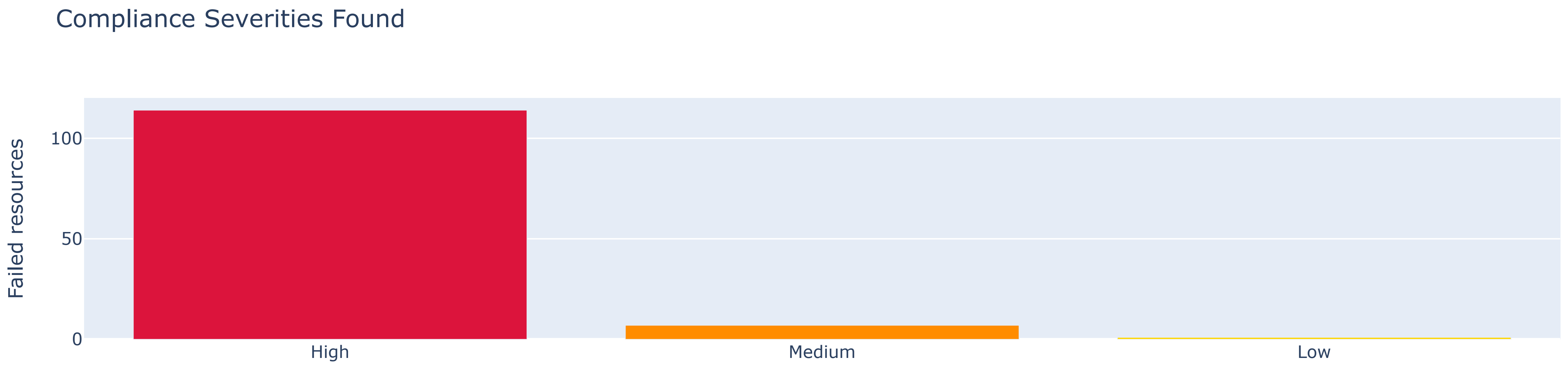


Azure Compliance Findings

`Total Azure Subscriptions Analyzed: 1`

Tenant ID	Severity Count	Non-compliant Resources	Total Assessed Resources
a329d4bf-4557-4ccf-b132-84e7025ea22d	High: 15	114	144

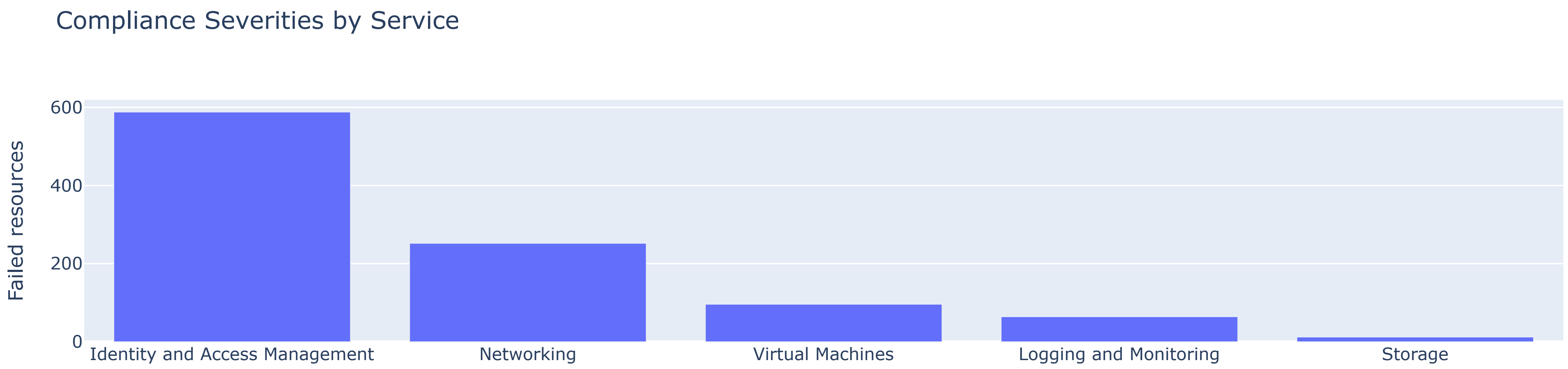


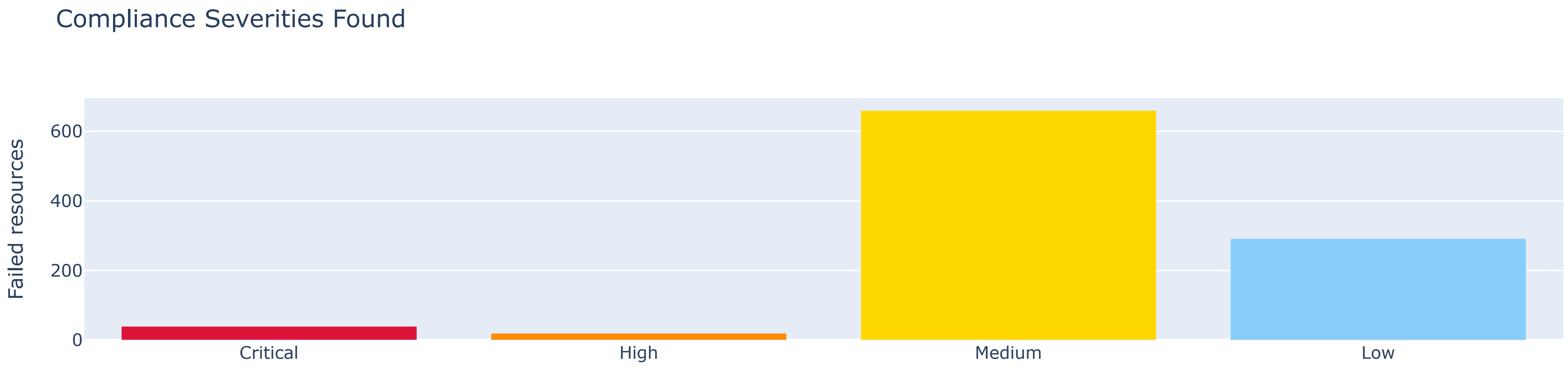


GCP Compliance Findings

Total GCP Subscriptions Analyzed: 1

Project ID	Severity Count	Non-compliant Resources	Total Assessed Resources
lacework-demo-dev	Critical: 4 High: 2	60	116





Behavioral & Known-Bad Alerts - Polygraph Anomalies (last 7 days / top 25)

Using the FortiCNAPP agentless Cloud Log behavioral assessment & any behavioral data from any agents you may have deployed, we've identified the following anomalous or policy-based activity for further investigation.

Alert ID	Severity	Alert Time	Alert Name	Description
478601	High	March 29, 2025 09:41PM	Potentially Compromised Host	Host machines may have been compromised. The following entities are suspected. Hosts: ip-10-0-2-5.us-east-2.compute.internal, ip-10-0-1-186.us-east-2.compute.internal.
442601	High	March 22, 2025 09:17PM	Potentially Compromised Host	Host machines may have been compromised. The following entities are suspected. Hosts: ip-10-0-1-186.us-east-2.compute.internal, ip-10-0-2-5.us-east-2.compute.internal.

Workload Vulnerability Assessment

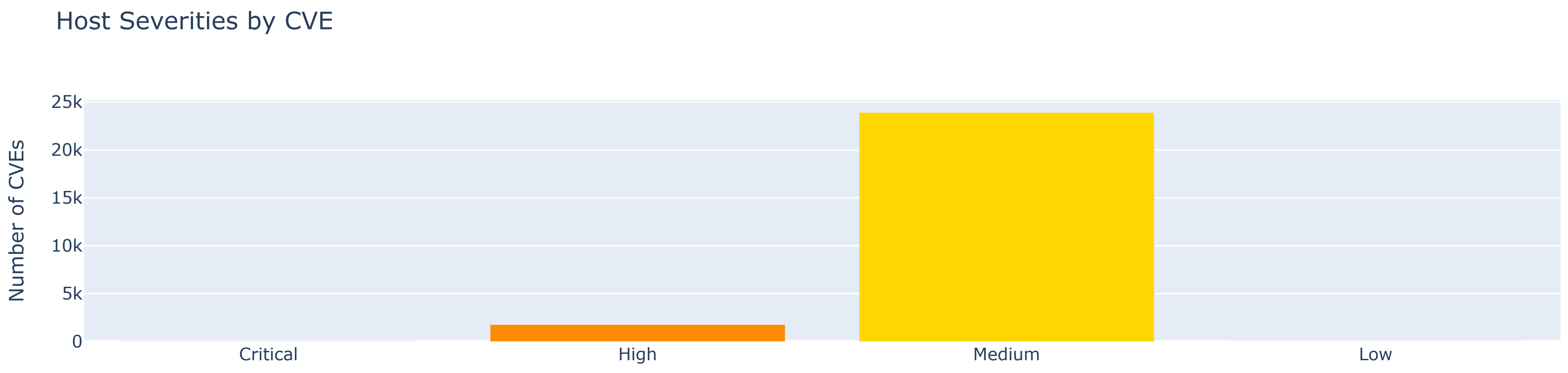
FortiCNAPP has scanned and identified vulnerable container images and/or hosts and associated risk of the vulnerabilities present. If the FortiCNAPP agent was not installed as part of this assessment it may be installed later to highlight observed behavior, communication paths, and context.

`Total Hosts Scanned: 11`

`Total Container Images Scanned: 16`

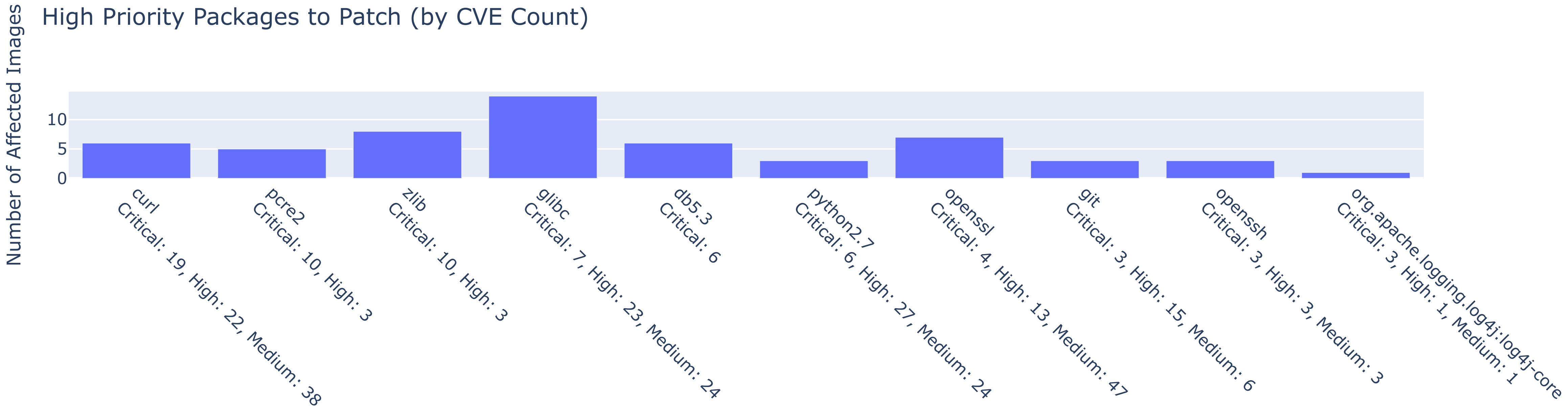
Host Vulnerability Summary

Severity	Total CVEs	Hosts Affected
Critical	7	2
High	1795	9
Medium	23929	11
Low	0	0



Container Vulnerability Summary

Severity	Total CVEs	Images Affected
Critical	104	8
High	484	10
Medium	630	16
Low	0	0



High Priority Packages to Patch (by CVE Count)

Appendix of Detailed Findings

This section contains additional details on the findings that were summarized above:

Detailed CVE Breakdown

Hosts With Critical, Fixable Vulnerabilities

This table lists all hosts with "critical" vulnerabilities that have fixes available. Additional vulnerability information for other severity levels can be found in the FortiCNAPP UI.

	Hostname	CVE	Severity	Package Name	Installed Version	Fixed Version(s)
0	ip-172-16-1-217.us-east-2.compute.internal	CVE-2023-45133	Critical	babel-traverse	6.26.0	7.23.2
1	ip-172-16-1-217.us-east-2.compute.internal	CVE-2021-44906	Critical	minimist	1.2.5	1.2.6
2	ip-172-16-1-45.us-east-2.compute.internal	CVE-2023-45133	Critical	babel-traverse	6.26.0	7.23.2
3	ip-172-16-1-45.us-east-2.compute.internal	CVE-2021-44906	Critical	minimist	1.2.5	1.2.6
4	ip-172-16-1-45.us-east-2.compute.internal	CVE-2021-44228	Critical	org.apache.logging.log4j:log4j-core	2.6.1	2.15.0
5	ip-172-16-1-45.us-east-2.compute.internal	CVE-2021-45046	Critical	org.apache.logging.log4j:log4j-core	2.6.1	2.16.0
6	ip-172-16-1-45.us-east-2.compute.internal	CVE-2017-5645	Critical	org.apache.logging.log4j:log4j-core	2.6.1	2.8.2

Containers With Critical, Fixable Vulnerabilities

This table lists all containers with "critical" vulnerabilities that have fixes available. Additional vulnerability information can be found in the FortiCNAPP UI.

	Repository	Image ID	CVE	Severity	Package Name	Installed Version	Fixed Version(s)
0	detcaccounts/ecommerce-inventory	sha256:e01e3ff828c30b87203fbcf381272e6c505dcfaa436d585fba5b04aec7ab9bd0	CVE-2024-32002	Critical	git	1:2.20.1-2+deb10u8	1:2.20.1-2+deb10u9
1	detcaccounts/ecommerce-inventory	sha256:e01e3ff828c30b87203fbcf381272e6c505dcfaa436d585fba5b04aec7ab9bd0	CVE-2023-38408	Critical	openssh	1:7.9p1-10+deb10u2	1:7.9p1-10+deb10u3
2	detcaccounts/ecommerce-inventory	sha256:e01e3ff828c30b87203fbcf381272e6c505dcfaa436d585fba5b04aec7ab9bd0	CVE-2022-1586, CVE-2022-1587	Critical	pcre2	10.32-5	10.32-5+deb10u1
3	detcaccounts/ecommerce-inventory	sha256:e01e3ff828c30b87203fbcf381272e6c505dcfaa436d585fba5b04aec7ab9bd0	CVE-2021-3177	Critical	python2.7	2.7.16-2+deb10u1	2.7.16-2+deb10u2
4	detcaccounts/ecommerce-inventory	sha256:e01e3ff828c30b87203fbcf381272e6c505dcfaa436d585fba5b04aec7ab9bd0	CVE-2022-48565	Critical	python2.7	2.7.16-2+deb10u1	2.7.16-2+deb10u3
5	detcaccounts/ecommerce-inventory	sha256:e01e3ff828c30b87203fbcf381272e6c505dcfaa436d585fba5b04aec7ab9bd0	CVE-2022-48565	Critical	python3.7	3.7.3-2+deb10u4	3.7.3-2+deb10u6
6	detcaccounts/ecommerce-login	sha256:53955dfb22799ff8c62067e429ceba9856864a48c66fad6c591f4f4316b538cf	CVE-2024-32002	Critical	git	1:2.20.1-2+deb10u8	1:2.20.1-2+deb10u9
7	detcaccounts/ecommerce-login	sha256:53955dfb22799ff8c62067e429ceba9856864a48c66fad6c591f4f4316b538cf	CVE-2023-38408	Critical	openssh	1:7.9p1-10+deb10u2	1:7.9p1-10+deb10u3
8	detcaccounts/ecommerce-login	sha256:53955dfb22799ff8c62067e429ceba9856864a48c66fad6c591f4f4316b538cf	CVE-2022-1586, CVE-2022-1587	Critical	pcre2	10.32-5	10.32-5+deb10u1

	Repository	Image ID	CVE	Severity	Package Name	Installed Version	Fixed Version(s)
9	detcaccounts/ecommerce-login	sha256:53955dfb22799ff8c62067e429ceba9856864a48c66fad6c591f4f4316b538cf	CVE-2021-3177	Critical	python2.7	2.7.16-2+deb10u1	2.7.16-2+deb10u2
10	detcaccounts/ecommerce-login	sha256:53955dfb22799ff8c62067e429ceba9856864a48c66fad6c591f4f4316b538cf	CVE-2022-48565	Critical	python2.7	2.7.16-2+deb10u1	2.7.16-2+deb10u3
11	detcaccounts/ecommerce-login	sha256:53955dfb22799ff8c62067e429ceba9856864a48c66fad6c591f4f4316b538cf	CVE-2022-48565	Critical	python3.7	3.7.3-2+deb10u4	3.7.3-2+deb10u6
12	detcaccounts/ecommerce-order	sha256:39294e42ebc94c2a3ac0da99d351f90a5878d97b20e050bcfea134f5ff77df0d	CVE-2024-32002	Critical	git	1:2.20.1-2+deb10u8	1:2.20.1-2+deb10u9
13	detcaccounts/ecommerce-order	sha256:39294e42ebc94c2a3ac0da99d351f90a5878d97b20e050bcfea134f5ff77df0d	CVE-2024-21508	Critical	mysql2	2.3.3	3.9.4
14	detcaccounts/ecommerce-order	sha256:39294e42ebc94c2a3ac0da99d351f90a5878d97b20e050bcfea134f5ff77df0d	CVE-2024-21511	Critical	mysql2	2.3.3	3.9.7
15	detcaccounts/ecommerce-order	sha256:39294e42ebc94c2a3ac0da99d351f90a5878d97b20e050bcfea134f5ff77df0d	CVE-2023-38408	Critical	openssh	1:7.9p1-10+deb10u2	1:7.9p1-10+deb10u3
16	detcaccounts/ecommerce-order	sha256:39294e42ebc94c2a3ac0da99d351f90a5878d97b20e050bcfea134f5ff77df0d	CVE-2022-1586, CVE-2022-1587	Critical	pcre2	10.32-5	10.32-5+deb10u1
17	detcaccounts/ecommerce-order	sha256:39294e42ebc94c2a3ac0da99d351f90a5878d97b20e050bcfea134f5ff77df0d	CVE-2021-3177	Critical	python2.7	2.7.16-2+deb10u1	2.7.16-2+deb10u2

	Repository	Image ID	CVE	Severity	Package Name	Installed Version	Fixed Version(s)
18	detcaccounts/ecommerce-order	sha256:39294e42ebc94c2a3ac0da99d351f90a5878d97b20e050bcfea134f5ff77df0d	CVE-2022-48565	Critical	python2.7	2.7.16-2+deb10u1	2.7.16-2+deb10u3
19	detcaccounts/ecommerce-order	sha256:39294e42ebc94c2a3ac0da99d351f90a5878d97b20e050bcfea134f5ff77df0d	CVE-2022-48565	Critical	python3.7	3.7.3-2+deb10u4	3.7.3-2+deb10u6
20	detcaccounts/ecommerce-website	sha256:7aba286656dc7d4b7529ec75090a117f1454fbf28bd8195848da6a69c74338fa	CVE-2017-1000257	Critical	curl	7.52.1-r2	7.56.1-r0
21	detcaccounts/ecommerce-website	sha256:7aba286656dc7d4b7529ec75090a117f1454fbf28bd8195848da6a69c74338fa	CVE-2017-8816, CVE-2017-8817, CVE-2017-8818	Critical	curl	7.52.1-r2	7.57.0-r0
22	detcaccounts/ecommerce-website	sha256:7aba286656dc7d4b7529ec75090a117f1454fbf28bd8195848da6a69c74338fa	CVE-2018-1000005	Critical	curl	7.52.1-r2	7.58.0-r0
23	detcaccounts/ecommerce-website	sha256:7aba286656dc7d4b7529ec75090a117f1454fbf28bd8195848da6a69c74338fa	CVE-2018-1000120, CVE-2018-1000122	Critical	curl	7.52.1-r2	7.59.0-r0
24	detcaccounts/ecommerce-website	sha256:7aba286656dc7d4b7529ec75090a117f1454fbf28bd8195848da6a69c74338fa	CVE-2018-1000300, CVE-2018-1000301	Critical	curl	7.52.1-r2	7.60.0-r0
25	detcaccounts/ecommerce-website	sha256:7aba286656dc7d4b7529ec75090a117f1454fbf28bd8195848da6a69c74338fa	CVE-2018-0500	Critical	curl	7.52.1-r2	7.61.0-r0
26	detcaccounts/ecommerce-website	sha256:7aba286656dc7d4b7529ec75090a117f1454fbf28bd8195848da6a69c74338fa	CVE-2018-14618	Critical	curl	7.52.1-r2	7.61.1-r0

	Repository	Image ID	CVE	Severity	Package Name	Installed Version	Fixed Version(s)
27	detcaccounts/ecommerce-website	sha256:7aba286656dc7d4b7529ec75090a117f1454fbf28bd8195848da6a69c74338fa	CVE-2018-16839, CVE-2018-16840, CVE-2018-16842	Critical	curl	7.52.1-r2	7.61.1-r1
28	detcaccounts/ecommerce-website	sha256:7aba286656dc7d4b7529ec75090a117f1454fbf28bd8195848da6a69c74338fa	CVE-2017-8105, CVE-2017-8287	Critical	freetype	2.7-r0	2.7.1-r1
29	detcaccounts/ecommerce-website	sha256:7aba286656dc7d4b7529ec75090a117f1454fbf28bd8195848da6a69c74338fa	CVE-2018-14599, CVE-2018-14600	Critical	libx11	1.6.4-r0	1.6.6-r0
30	detcaccounts/ecommerce-website	sha256:7aba286656dc7d4b7529ec75090a117f1454fbf28bd8195848da6a69c74338fa	CVE-2018-2938	Critical	openjdk8	8.121.13-r0	8.181.13-r0
31	detcaccounts/ecommerce-website	sha256:7aba286656dc7d4b7529ec75090a117f1454fbf28bd8195848da6a69c74338fa	CVE-2018-3183	Critical	openjdk8	8.121.13-r0	8.191.12-r0
32	detcaccounts/ecommerce-website	sha256:7aba286656dc7d4b7529ec75090a117f1454fbf28bd8195848da6a69c74338fa	CVE-2021-44228	Critical	org.apache.logging.log4j:log4j-core	2.6.1	2.15.0
33	detcaccounts/ecommerce-website	sha256:7aba286656dc7d4b7529ec75090a117f1454fbf28bd8195848da6a69c74338fa	CVE-2021-45046	Critical	org.apache.logging.log4j:log4j-core	2.6.1	2.16.0
34	detcaccounts/ecommerce-website	sha256:7aba286656dc7d4b7529ec75090a117f1454fbf28bd8195848da6a69c74338fa	CVE-2017-5645	Critical	org.apache.logging.log4j:log4j-core	2.6.1	2.8.2
35	detcaccounts/ecommerce-website	sha256:7aba286656dc7d4b7529ec75090a117f1454fbf28bd8195848da6a69c74338fa	CVE-2022-22963	Critical	org.springframework.cloud:spring-cloud-function-context	3.2.2	3.2.3

	Repository	Image ID	CVE	Severity	Package Name	Installed Version	Fixed Version(s)
36	detcaccounts/ecommerce-website	sha256:7aba286656dc7d4b7529ec75090a117f1454fbf28bd8195848da6a69c74338fa	CVE-2022-22963	Critical	org.springframework.cloud:spring-cloud-function-core	3.2.2	3.2.3
37	detcaccounts/ecommerce-website	sha256:7aba286656dc7d4b7529ec75090a117f1454fbf28bd8195848da6a69c74338fa	CVE-2016-9841, CVE-2016-9843	Critical	zlib	1.2.8-r2	1.2.11-r0
38	detcaccounts/voteapp-results-site	sha256:1c27e07fb052c879bf0237ad0d6bc84ce4084d0a3fa7377fb13f325e95798e80	CVE-2022-1664	Critical	dpkg	1.18.25	1.18.26
39	detcaccounts/voteapp-results-site	sha256:1c27e07fb052c879bf0237ad0d6bc84ce4084d0a3fa7377fb13f325e95798e80	CVE-2021-3918	Critical	json-schema	0.2.3	0.4.0
40	detcaccounts/voteapp-results-site	sha256:1c27e07fb052c879bf0237ad0d6bc84ce4084d0a3fa7377fb13f325e95798e80	CVE-2021-3520	Critical	lz4	0.0~r131-2	0.0~r131-2+deb9u1
41	detcaccounts/voteapp-results-site	sha256:1c27e07fb052c879bf0237ad0d6bc84ce4084d0a3fa7377fb13f325e95798e80	CVE-2021-44906	Critical	minimist	1.2.5	1.2.6
42	detcaccounts/voteapp-results-site	sha256:1c27e07fb052c879bf0237ad0d6bc84ce4084d0a3fa7377fb13f325e95798e80	CVE-2022-29155	Critical	openldap	2.4.44+dfsg-5+deb9u8	2.4.44+dfsg-5+deb9u9
43	detcaccounts/voteapp-results-site	sha256:1c27e07fb052c879bf0237ad0d6bc84ce4084d0a3fa7377fb13f325e95798e80	CVE-2022-2421	Critical	socket.io-parser	3.3.2	3.3.3
44	detcaccounts/voteapp-results-site	sha256:1c27e07fb052c879bf0237ad0d6bc84ce4084d0a3fa7377fb13f325e95798e80	CVE-2022-2421	Critical	socket.io-parser	3.4.1	3.4.2

	Repository	Image ID	CVE	Severity	Package Name	Installed Version	Fixed Version(s)
45	detcaccounts/voteapp-results-site	sha256:1c27e07fb052c879bf0237ad0d6bc84ce4084d0a3fa7377fb13f325e95798e80	CVE-2021-31597	Critical	xmlhttprequest-ssl	1.5.5	1.6.1
46	detcaccounts/voteapp-results-site	sha256:1c27e07fb052c879bf0237ad0d6bc84ce4084d0a3fa7377fb13f325e95798e80	CVE-2020-28502	Critical	xmlhttprequest-ssl	1.5.5	1.6.2
47	detcaccounts/voteapp-website	sha256:a94d80f1fd196a58a99957a2c7b6f6b387fe88a32b76d1a0b696219bc7e5ac14	CVE-2023-38545	Critical	curl	7.74.0-1.3+deb11u1	7.74.0-1.3+deb11u10
48	detcaccounts/voteapp-website	sha256:a94d80f1fd196a58a99957a2c7b6f6b387fe88a32b76d1a0b696219bc7e5ac14	CVE-2021-22945, CVE-2022-32207	Critical	curl	7.74.0-1.3+deb11u1	7.74.0-1.3+deb11u2
49	detcaccounts/voteapp-website	sha256:a94d80f1fd196a58a99957a2c7b6f6b387fe88a32b76d1a0b696219bc7e5ac14	CVE-2022-32221	Critical	curl	7.74.0-1.3+deb11u1	7.74.0-1.3+deb11u5
50	detcaccounts/voteapp-website	sha256:a94d80f1fd196a58a99957a2c7b6f6b387fe88a32b76d1a0b696219bc7e5ac14	CVE-2022-1664	Critical	dpkg	1.20.9	1.20.10
51	detcaccounts/voteapp-website	sha256:a94d80f1fd196a58a99957a2c7b6f6b387fe88a32b76d1a0b696219bc7e5ac14	CVE-2024-45491, CVE-2024-45492	Critical	expat	2.2.10-2+deb11u3	2.2.10-2+deb11u6
52	detcaccounts/voteapp-website	sha256:a94d80f1fd196a58a99957a2c7b6f6b387fe88a32b76d1a0b696219bc7e5ac14	CVE-2024-37371	Critical	krb5	1.18.3-6+deb11u1	1.18.3-6+deb11u5
53	detcaccounts/voteapp-website	sha256:a94d80f1fd196a58a99957a2c7b6f6b387fe88a32b76d1a0b696219bc7e5ac14	CVE-2021-46848	Critical	libtasn1-6	4.16.0-2	4.16.0-2+deb11u1

	Repository	Image ID	CVE	Severity	Package Name	Installed Version	Fixed Version(s)
54	detcaccounts/voteapp-website	sha256:a94d80f1fd196a58a99957a2c7b6f6b387fe88a32b76d1a0b696219bc7e5ac14	CVE-2022-29155	Critical	openldap	2.4.57+dfsg-3	2.4.57+dfsg-3+deb11u1
55	detcaccounts/voteapp-website	sha256:a94d80f1fd196a58a99957a2c7b6f6b387fe88a32b76d1a0b696219bc7e5ac14	CVE-2022-1292	Critical	openssl	1.1.1n-0+deb11u1	1.1.1n-0+deb11u2
56	detcaccounts/voteapp-website	sha256:a94d80f1fd196a58a99957a2c7b6f6b387fe88a32b76d1a0b696219bc7e5ac14	CVE-2022-2068	Critical	openssl	1.1.1n-0+deb11u1	1.1.1n-0+deb11u3
57	detcaccounts/voteapp-website	sha256:a94d80f1fd196a58a99957a2c7b6f6b387fe88a32b76d1a0b696219bc7e5ac14	CVE-2024-5535	Critical	openssl	1.1.1n-0+deb11u1	1.1.1w-0+deb11u2
58	detcaccounts/voteapp-website	sha256:a94d80f1fd196a58a99957a2c7b6f6b387fe88a32b76d1a0b696219bc7e5ac14	CVE-2022-1586, CVE-2022-1587	Critical	pcre2	10.36-2	10.36-2+deb11u1
59	detcaccounts/voteapp-website	sha256:a94d80f1fd196a58a99957a2c7b6f6b387fe88a32b76d1a0b696219bc7e5ac14	CVE-2022-37434	Critical	zlib	1:1.2.11.dfsg-2+deb11u1	1:1.2.11.dfsg-2+deb11u2
60	library/postgres	sha256:e09e90144645e02137d087f0dc059f4d2e3c6356ef8f9e40eeb15d1c901dbc73	CVE-2022-23806	Critical	go-compiler	1.16.7	1.16.14
61	library/postgres	sha256:e09e90144645e02137d087f0dc059f4d2e3c6356ef8f9e40eeb15d1c901dbc73	CVE-2024-37371	Critical	krb5	1.18.3-6+deb11u1	1.18.3-6+deb11u5
62	library/postgres	sha256:e09e90144645e02137d087f0dc059f4d2e3c6356ef8f9e40eeb15d1c901dbc73	CVE-2022-3515	Critical	libksba	1.5.0-3	1.5.0-3+deb11u1

	Repository	Image ID	CVE	Severity	Package Name	Installed Version	Fixed Version(s)
63	library/postgres	sha256:e09e90144645e02137d087f0dc059f4d2e3c6356ef8f9e40eeb15d1c901dbc73	CVE-2022-47629	Critical	libksba	1.5.0-3	1.5.0-3+deb11u2
64	library/postgres	sha256:e09e90144645e02137d087f0dc059f4d2e3c6356ef8f9e40eeb15d1c901dbc73	CVE-2021-46848	Critical	libtasn1-6	4.16.0-2	4.16.0-2+deb11u1
65	library/postgres	sha256:e09e90144645e02137d087f0dc059f4d2e3c6356ef8f9e40eeb15d1c901dbc73	CVE-2024-5535	Critical	openssl	1.1.1n-0+deb11u3	1.1.1w-0+deb11u2
66	library/postgres	sha256:e09e90144645e02137d087f0dc059f4d2e3c6356ef8f9e40eeb15d1c901dbc73	CVE-2022-1586, CVE-2022-1587	Critical	pcre2	10.36-2	10.36-2+deb11u1
67	library/postgres	sha256:e09e90144645e02137d087f0dc059f4d2e3c6356ef8f9e40eeb15d1c901dbc73	CVE-2022-37434	Critical	zlib	1:1.2.11.dfsg-2+deb11u1	1:1.2.11.dfsg-2+deb11u2

Detailed Cloud Compliance Findings

AWS - Top High/Critical Compliance Findings

	Account ID	Category	Title	Severity	Resources
0	583683056848	Networking	Ensure no Network Access Control Lists (ACL) allow ingress from 0.0.0.0/0 to remote server administration ports	High	21 / 26
1	583683056848	Networking	Ensure the default security group of every Virtual Private Cloud (VPC) restricts all traffic	High	21 / 42
2	583683056848	Logging	Enable AWS Config in all regions	High	17 / 17

	Account ID	Category	Title	Severity	Resources
3	583683056848	Identity and Access Management	Ensure Identity and Access Management (IAM) policies that allow full "*:*" administrative privileges are not attached to roles	High	10 / 60
4	583683056848	Networking	Ensure no security groups allow ingress from 0.0.0.0/0 to remote server administration ports	High	4 / 42
5	583683056848	Identity and Access Management	Ensure Identity and Access Management (IAM) policies that allow full "*:*" administrative privileges are not attached to users	High	2 / 3
6	583683056848	Storage RDS	Enable encryption for Relational Database Service (RDS) Instances	High	1 / 1
7	583683056848	Logging	Ensure AWS Config is recording Global Resources in at least one region	High	1 / 1

Azure - Top High/Critical Compliance Findings

Tenant ID	Category	Title	Severity	Resources
a329d4bf-4557-4ccf-b132-84e7025ea22d	Networking	Ensure that Network Watcher is 'Enabled' (includes Reserved access regions)	High	55 / 58
a329d4bf-4557-4ccf-b132-84e7025ea22d	Networking	Ensure that Network Watcher is 'Enabled' (excludes Reserved access regions)	High	41 / 58
a329d4bf-4557-4ccf-b132-84e7025ea22d	Virtual Machines	Encrypt 'OS and Data' disks with Customer Managed Key (CMK)	High	4 / 4
a329d4bf-4557-4ccf-b132-84e7025ea22d	Networking	Evaluate and restrict SSH access from the Internet	High	2 / 5
a329d4bf-4557-4ccf-b132-84e7025ea22d	Networking	Evaluate and restrict HTTP(S) access from the Internet	High	2 / 5

Tenant ID	Category	Title	Severity	Resources
a329d4bf-4557-4ccf-b132-84e7025ea22d	Storage Accounts	Set Default Network Access Rule for Storage Accounts to Deny	High	1 / 1
a329d4bf-4557-4ccf-b132-84e7025ea22d	Logging and Monitoring	Ensure that Activity Log Alert exists for Create or Update Network Security Group	High	1 / 1
a329d4bf-4557-4ccf-b132-84e7025ea22d	Logging and Monitoring	Ensure that Activity Log Alert exists for Delete Network Security Group	High	1 / 1
a329d4bf-4557-4ccf-b132-84e7025ea22d	Logging and Monitoring	Ensure that Activity Log Alert exists for Create or Update Security Solution	High	1 / 1
a329d4bf-4557-4ccf-b132-84e7025ea22d	Logging and Monitoring	Ensure that Activity Log Alert exists for Delete Security Solution	High	1 / 1
a329d4bf-4557-4ccf-b132-84e7025ea22d	Logging and Monitoring	Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule	High	1 / 1
a329d4bf-4557-4ccf-b132-84e7025ea22d	Logging and Monitoring	Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule	High	1 / 1
a329d4bf-4557-4ccf-b132-84e7025ea22d	Logging and Monitoring	Ensure that Activity Log Alert exists for Create or Update Public IP Address rule	High	1 / 1
a329d4bf-4557-4ccf-b132-84e7025ea22d	Logging and Monitoring	Ensure that Activity Log Alert exists for Delete Public IP Address rule	High	1 / 1
a329d4bf-4557-4ccf-b132-84e7025ea22d	Networking	Evaluate and restrict Remote Desktop Protocol (RDP) access from the Internet	High	1 / 5

GCP - Top High/Critical Compliance Findings

Project ID	Category	Title	Severity	Resources
lacework-demo-dev	Virtual Machines	Encrypt VM Disks for Critical VMs With Customer-Supplied Encryption Keys (CSEK)	Critical	18 / 18

Project ID	Category	Title	Severity	Resources
lacework-demo-dev	Virtual Machines	Encrypt VM Disks for Critical VMs With Customer-Supplied Encryption Keys (CSEK)	Critical	18 / 18
lacework-demo-dev	Networking	Restrict Remote Desktop Protocol (RDP) Access From the Internet	Critical	2 / 24
lacework-demo-dev	Networking	Restrict Remote Desktop Protocol (RDP) Access From the Internet	Critical	2 / 24
lacework-demo-dev	Virtual Machines	Ensure That Compute Instances Do Not Have Public IP Addresses	High	10 / 16
lacework-demo-dev	Virtual Machines	Ensure That Compute Instances Do Not Have Public IP Addresses	High	10 / 16

GCP - Critical Findings with Details

This table contains CIS compliance findings with a severity of "Critical". Other severity levels can be reviewed in the FortiCNAPP UI.

	Project ID	Category	Control	Violations
42	lacework-demo-dev	Networking	Restrict Remote Desktop Protocol (RDP) Access From the Internet	Region:global Resource: //compute.googleapis.com/projects/lacework-demo-dev/global/firewalls/default-allow-rdp Reasons: ['RDPAccessAllowed'] Region:global Resource: //compute.googleapis.com/projects/lacework-demo-dev/global/firewalls/default-allow-rdp Reasons: ['RDPAccessAllowed']
54	lacework-demo-dev	Virtual Machines	Encrypt VM Disks for Critical VMs With Customer-Supplied Encryption Keys (CSEK)	Region:us-central1-c Resource: //compute.googleapis.com/projects/lacework-demo-dev/zones/us-central1-c/disks/disk-clone-xaccount Reasons: ['DiskNotEncryptedWithCSEK'] Region:us-central1-c Resource: //compute.googleapis.com/projects/lacework-demo-dev/zones/us-central1-c/disks/disk-clone-

Project ID	Category	Control	Violations

			xaccount
			Reasons: ['DiskNotEncryptedWithCSEK']
			
			Region:us-east1-b
			Resource:
			//compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-b/disks/activity-generator
			Reasons: ['DiskNotEncryptedWithCSEK']
			
			Region:us-east1-b
			Resource:
			//compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-b/disks/activity-generator
			Reasons: ['DiskNotEncryptedWithCSEK']
			
			Region:us-east1-b
			Resource:
			//compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-b/disks/datalayer0
			Reasons: ['DiskNotEncryptedWithCSEK']
			
			Region:us-east1-b
			Resource:
			//compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-b/disks/datalayer0
			Reasons: ['DiskNotEncryptedWithCSEK']
			
			Region:us-east1-b
			Resource:
			//compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-b/disks/datalayer1
			Reasons: ['DiskNotEncryptedWithCSEK']
			
			Region:us-east1-b
			Resource:
			//compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-b/disks/datalayer1
			Reasons: ['DiskNotEncryptedWithCSEK']
			
			Region:us-east1-b
			Resource:
			//compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-b/disks/gke-sharedgke-default-node-pool-f1d63e9e-pqrt
			Reasons: ['DiskNotEncryptedWithCSEK']
			
			Region:us-east1-b
			Resource:
			//compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-b/disks/gke-sharedgke-default-node-pool-f1d63e9e-pqrt
			Reasons: ['DiskNotEncryptedWithCSEK']
			
			Region:us-east1-b
			Resource:
			//compute.googleapis.com/projects/lacework-

	Project ID	Category	Control	Violations

				demo-dev/zones/us-east1-b/disks/mongodb
				Reasons: ['DiskNotEncryptedWithCSEK']
				Region:us-east1-b
				Resource:
				//compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-b/disks/mongodb
				Reasons: ['DiskNotEncryptedWithCSEK']
				Region:us-east1-b
				Resource:
				//compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-b/disks/ticketing-utilty
				Reasons: ['DiskNotEncryptedWithCSEK']
				Region:us-east1-b
				Resource:
				//compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-b/disks/ticketing-utilty
				Reasons: ['DiskNotEncryptedWithCSEK']
				Region:us-east1-c
				Resource:
				//compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-c/disks/gke-sharedgke-default-node-pool-da487fab-1wjx
				Reasons: ['DiskNotEncryptedWithCSEK']
				Region:us-east1-c
				Resource:
				//compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-c/disks/gke-sharedgke-default-node-pool-da487fab-1wjx
				Reasons: ['DiskNotEncryptedWithCSEK']
				Region:us-east1-d
				Resource:
				//compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-d/disks/gke-sharedgke-default-node-pool-0899760d-hjvn
				Reasons: ['DiskNotEncryptedWithCSEK']
				Region:us-east1-d
				Resource:
				//compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-d/disks/gke-sharedgke-default-node-pool-0899760d-hjvn
				Reasons: ['DiskNotEncryptedWithCSEK']

130	lacework-demo-dev	Networking	Restrict Remote Desktop Protocol (RDP) Access From the Internet	Region:global Resource: //compute.googleapis.com/projects/lacework-demo-dev/global/firewalls/default-allow-rdp Reasons: ['RDPAccessAllowed']

	Project ID	Category	Control	Violations
				Region:global Resource: //compute.googleapis.com/projects/lacework-demo-dev/global/firewalls/default-allow-rdp Reasons: ['RDPAccessAllowed']
142	lacework-demo-dev	Virtual Machines	Encrypt VM Disks for Critical VMs With Customer-Supplied Encryption Keys (CSEK)	Region:us-central1-c Resource: //compute.googleapis.com/projects/lacework-demo-dev/zones/us-central1-c/disks/disk-clone-xaccount Reasons: ['DiskNotEncryptedWithCSEK'] Region:us-central1-c Resource: //compute.googleapis.com/projects/lacework-demo-dev/zones/us-central1-c/disks/disk-clone-xaccount Reasons: ['DiskNotEncryptedWithCSEK'] Region:us-east1-b Resource: //compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-b/disks/activity-generator Reasons: ['DiskNotEncryptedWithCSEK'] Region:us-east1-b Resource: //compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-b/disks/activity-generator Reasons: ['DiskNotEncryptedWithCSEK'] Region:us-east1-b Resource: //compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-b/disks/datalayer0 Reasons: ['DiskNotEncryptedWithCSEK'] Region:us-east1-b Resource: //compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-b/disks/datalayer0 Reasons: ['DiskNotEncryptedWithCSEK'] Region:us-east1-b Resource: //compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-b/disks/datalayer1 Reasons: ['DiskNotEncryptedWithCSEK'] Region:us-east1-b Resource: //compute.googleapis.com/projects/lacework-

Project ID	Category	Control	Violations

			demo-dev/zones/us-east1-b/disks/datalayer1
			Reasons: ['DiskNotEncryptedWithCSEK']
			
			Region:us-east1-b
			Resource:
			//compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-b/disks/gke-sharedgke-default-node-pool-f1d63e9e-pqrt
			Reasons: ['DiskNotEncryptedWithCSEK']
			
			Region:us-east1-b
			Resource:
			//compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-b/disks/gke-sharedgke-default-node-pool-f1d63e9e-pqrt
			Reasons: ['DiskNotEncryptedWithCSEK']
			
			Region:us-east1-b
			Resource:
			//compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-b/disks/mongodb
			Reasons: ['DiskNotEncryptedWithCSEK']
			
			Region:us-east1-b
			Resource:
			//compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-b/disks/mongodb
			Reasons: ['DiskNotEncryptedWithCSEK']
			
			Region:us-east1-b
			Resource:
			//compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-b/disks/ticketing-utilty
			Reasons: ['DiskNotEncryptedWithCSEK']
			
			Region:us-east1-b
			Resource:
			//compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-b/disks/ticketing-utilty
			Reasons: ['DiskNotEncryptedWithCSEK']
			
			Region:us-east1-c
			Resource:
			//compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-c/disks/gke-sharedgke-default-node-pool-da487fab-1wjx
			Reasons: ['DiskNotEncryptedWithCSEK']
			
			Region:us-east1-c
			Resource:
			//compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-c/disks/gke-sharedgke-default-node-pool-da487fab-1wjx
			Reasons: ['DiskNotEncryptedWithCSEK']
			
			Region:us-east1-d

Project ID	Category	Control	Violations
			Resource: //compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-d/disks/gke-sharedgke-default-node-pool-0899760d-hjvn Reasons: ['DiskNotEncryptedWithCSEK'] Region:us-east1-d Resource: //compute.googleapis.com/projects/lacework-demo-dev/zones/us-east1-d/disks/gke-sharedgke-default-node-pool-0899760d-hjvn Reasons: ['DiskNotEncryptedWithCSEK']