

TOP CLOUD RISKS & INCIDENTS REPORT

POWERED BY COMMAND CENTER

July 18, 2022 at 8:44:53 PM UTC

Prepared for PANW-dev

ACCOUNT GROUPS

n/a

TIME RANGE

Past 7 Days

Table of Contents

00

Executive Summary	4
Top Open Alerts	5
Total Urgent Alerts	5
Top Policy Violations	5
Top Violations by Assets	5

01

Incidents	6
Top Open Alerts	7
Top Incident Violations	7
Top Incident Assets	7

02

Misconfigurations	8
Top Open Alerts	9
Top Misconfiguration Violations	9
Top Misconfigured Assets	9

03

Exposures	10
Top Open Alerts	11
Top Exposure Violations	11
Top Exposure Assets	11

04

Identity	12
Top Open Alerts	13
Top Identity Risk Violations	13
Top Identity Risk Assets	13

Executive Summary

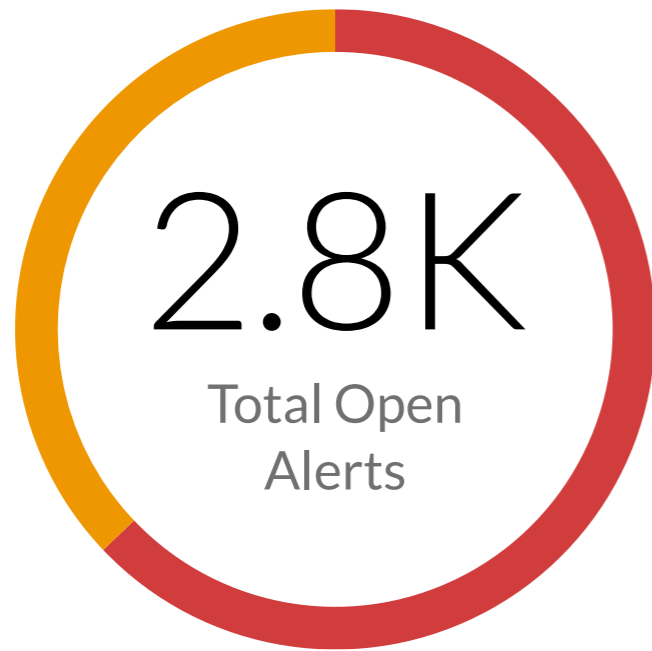
Top Open Alerts

Total Urgent Alerts

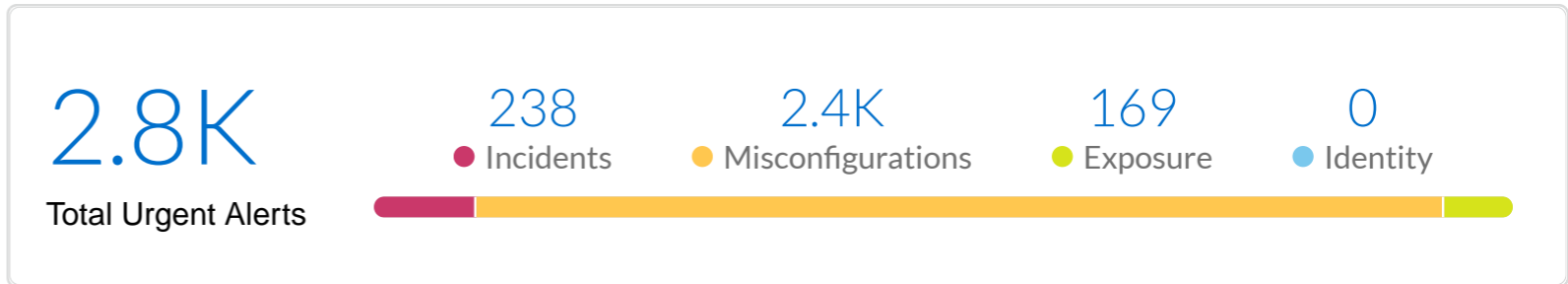
Top Policy Violations

Top Violations by Assets

Executive Summary



Total Open Alerts by Severity



Top Policy Violations

Policies	Alerts	Severity
SC-AWS S3 Buckets Block public access setting disabled	819	●●●●
Prb Azure VM instance in running state that is internet reachable with	35	●●●●
SavedSearch_contract_f1d815	35	●●●●
[BETA] [CNS] Ajay AWS ELB exposed to internet over HTTP	32	●●●●
app-stage test	17	●●●●

Top Violations by Assets

Assets	Service	Account	Alerts	Severity
auto-ii-ec2-qualys-i3z4	Amazon EC2	AWS_Red...	7	●●●● 4 ●●●● 3
auto-ii-ec2-qualys-i3z4	Amazon EC2	AWS_Red...	7	●●●● 4 ●●●● 3
i-0d0a6e8050a596e9	Amazon EC2	AWS_Red...	5	●●●● 3 ●●●● 2
i-0d0a6e8050a596e9	Amazon EC2	AWS_Red...	5	●●●● 3 ●●●● 2
appsec-poc2-appsec-n	Amazon EC2	AWS Sand...	4	●●●● 2 ●●●● 2

1

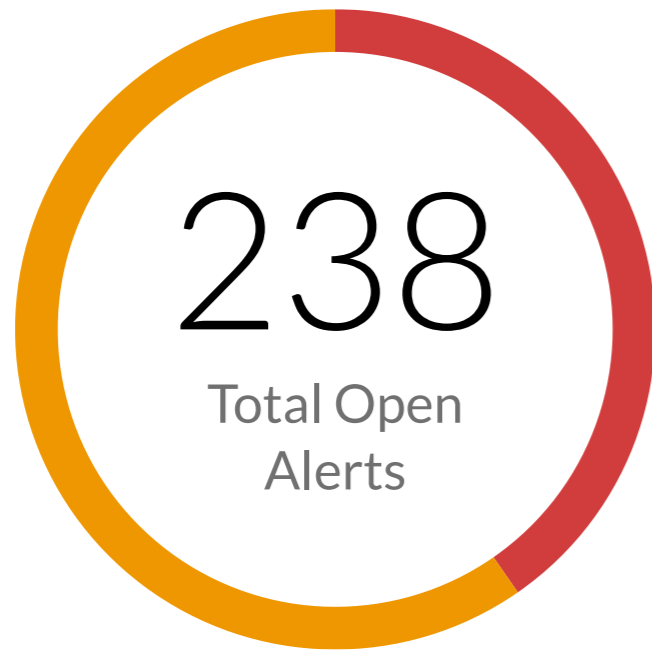
Incidents

Top Open Alerts

Top Incident Violations

Top Incident Assets

Incidents



Total Open Alerts by Severity



Top Incident Violations

Policies	Alerts	Severity
Prb Azure VM instance in running state that is internet reachable with	35	●●●●
[BETA] [CNS] Ajay AWS ELB exposed to internet over HTTP	32	●●●●
network-config-policy-without-saved-rql	11	●●●●
Instances exposed to network traffic from the internet	7	●●●●
AWSEC2 instance that is internet reachable with unrestricted access	4	●●●●

Top Incident Assets

Assets	Service	Account	Alerts	Severity
auto-ii-ec2-qualys-i3z4	Amazon EC2	AWS_Red...	7	●●●● 4 ●●●● 3
i-0d0a6e8050a596e9	Amazon EC2	AWS_Red...	5	●●●● 3 ●●●● 2
appsec-poc2-appsec-n	Amazon EC2	AWS_Sand...	4	●●●● 2 ●●●● 2
i-02de5c747734d1ca	Amazon EC2	AWS_Red...	3	●●●● 2 ●●●● 1
eni-003556190997d4	Amazon EC2	AWS_Evi...	1	●●●● 1

2

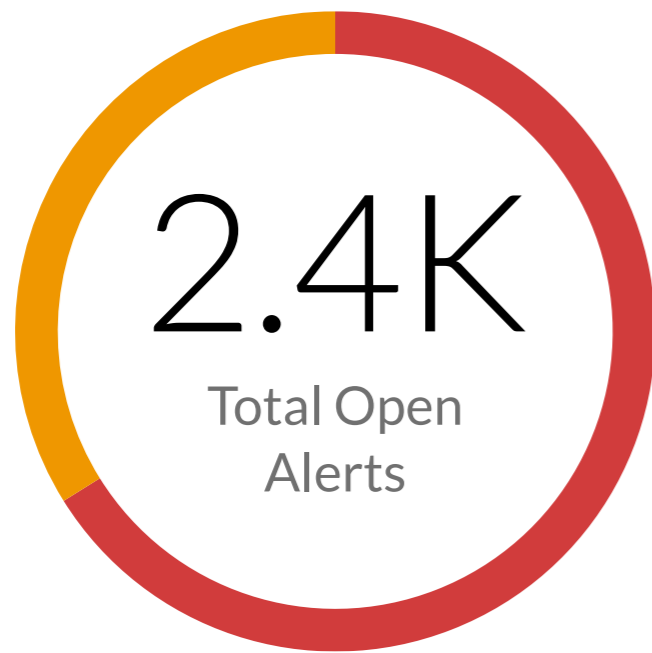
Misconfigurations

Top Open Alerts

Top Misconfiguration Violations

Top Misconfigured Assets

Misconfigurations



Total Open Alerts by Severity



Top Misconfiguration Violations

Policies	Alerts	Severity
SC-AWS S3 Buckets Block public access setting disabled	819	●●●●
SavedSearch_contract_f1d815	35	●●●●
app-stage test	17	●●●●
OCI IAM local (non-federated) user account does not have a valid and	14	●●●●
OCI MFA is disabled for IAM users	14	●●●●

Top Misconfigured Assets

Assets	Service	Account	Alerts	Severity
Terraform_user_qroziğ	OCI IAM	pris...	3	●●●● 2 ●●●● 1
Terraform_user_aare..	OCI IAM	pris...	3	●●●● 2 ●●●● 1
Ter...	OCI IAM	pris...	3	●●●● 2 ●●●● 1
Terraform_user_cdnjh>	OCI IAM	pris...	3	●●●● 2 ●●●● 1
Ter...	OCI IAM	pris...	3	●●●● 2 ●●●● 1

3

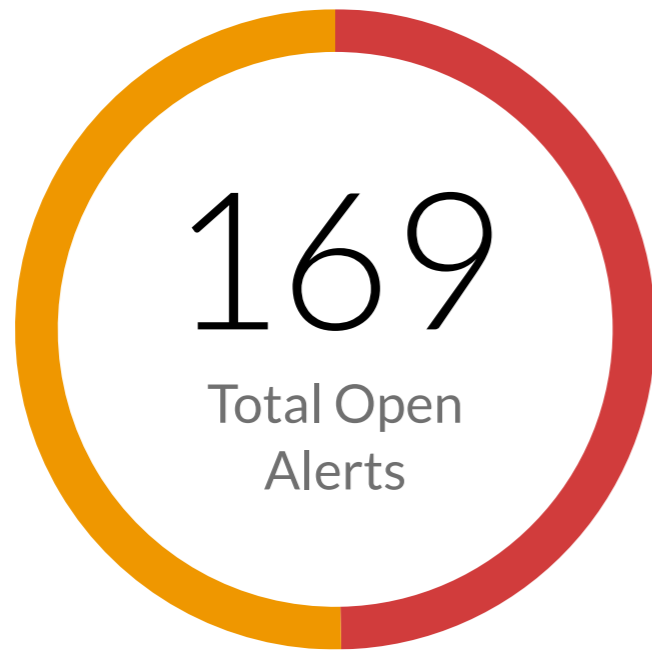
Exposures

Top Open Alerts

Top Exposure Violations

Top Exposure Assets

Exposures



Total Open Alerts by Severity

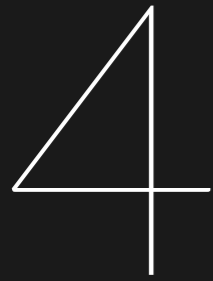


Top Exposure Violations

Policies	Alerts	Severity
Prb Azure VM instance in running state that is internet reachable with	35	●●●●
[BETA] [CNS] Ajay AWS ELB exposed to internet over HTTP	32	●●●●
network-config-policy-without-saved-rql	11	●●●●
AWSEC2 instance that is internet reachable with unrestricted access	4	●●●●
Prb Azure MySQL (PaaS) instance that is internet reachable with unre	2	●●●●

Top Exposure Assets

Assets	Service	Account	Alerts	Severity
auto-ii-ec2-qualys-i3z4	Amazon EC2	AWS_Red...	7	●●●● 4 ●●●● 3
i-0d0a6e8050a596e9	Amazon EC2	AWS_Red...	5	●●●● 3 ●●●● 2
appsec-poc2-appsec-n	Amazon EC2	AWS_Sand...	4	●●●● 2 ●●●● 2
i-02de5c747734d1ca	Amazon EC2	AWS_Red...	3	●●●● 2 ●●●● 1
eni-003556190997d4	Amazon EC2	AWS_Evi...	1	●●●● 1



Identity

Top Open Alerts

Top Identity Risk Violations

Top Identity Risk Assets

Identity

0
Total Open Alerts

Total Open Alerts by Severity

0 High 0 Medium

Top Identity Risk Violations

Policies	Alerts	Severity
----------	--------	----------

Top Identity Risk Assets

Assets	Service	Account	Alerts	Severity
--------	---------	---------	--------	----------

Thank You For Using Prisma Cloud