PRISMA® CLOUD
BY PALO ALTO NETWORKS

# 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

# Executive Summary

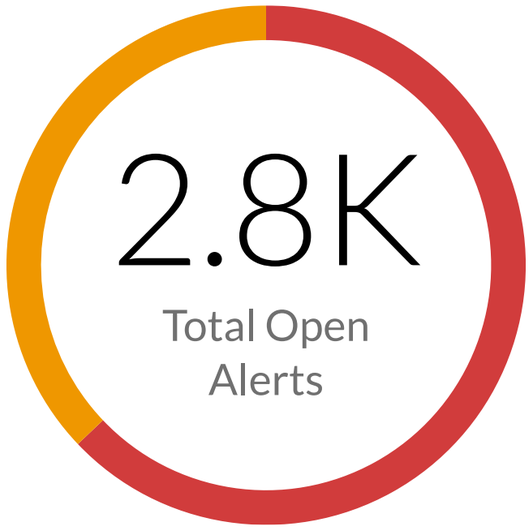
Top Open Alerts

Total Urgent Alerts

Top Policy Violations

Top Violations by Assets

# Executive Summary




Total Open Alerts by Severity

| 1.7K | 1K |
|---|---|
| High | Medium |

**2.8K** Total Urgent Alerts

| 238 | 2.4K | 169 | 0 |
|---|---|---|---|
| Incidents | Misconfigurations | Exposure | Identity |

## 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

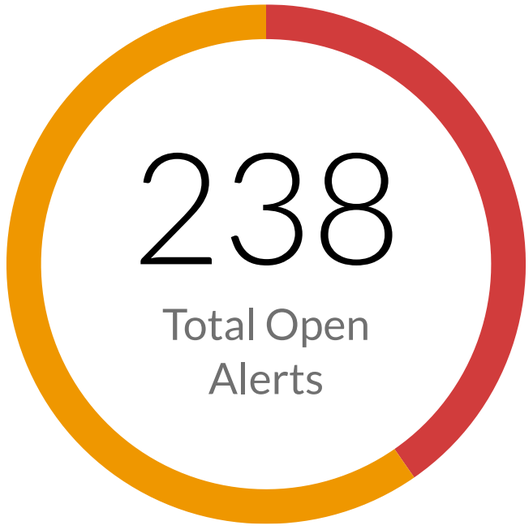
Top Open Alerts

Top Incident Violations

Top Incident Assets

COMMAND CENTER / INCIDENTS

# Incidents




Total Open Alerts by Severity

96 High

142 Medium

## 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 | ●●● |
| AWS EC2 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

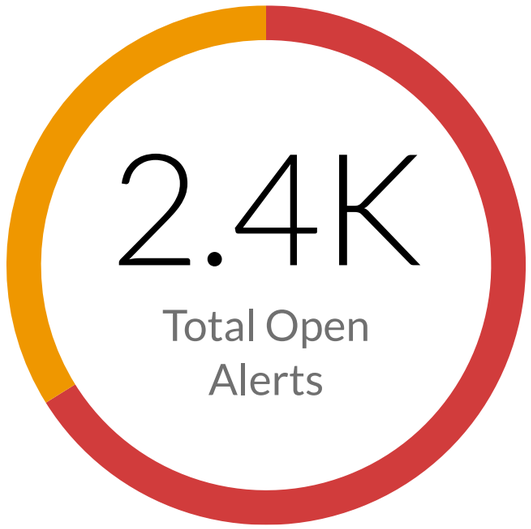
# Misconfigurations

Top Open Alerts

Top Misconfiguration Violations

Top Misconfigured Assets

# Misconfigurations




Total Open Alerts by Severity

| 1.6K | 802 |
|---|---|
| High | Medium |

## 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_qrozig | 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

84 High

85 Medium

## 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 | ●●● |
| AWS EC2 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-i3z | 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 | |

4

# 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