Sign in

elastic / detection-rules Public

Notifications Fork 498 Star 2k

Code Issues 145 Pull requests 19 Actions Security Insights

[New Rule] GCP Kubernetes Rolebindings Created or Patched #1267

New issue

Merged

w0rk3r merged 45 commits into `elastic:main` from `austinsonger:credential_access_gcp_kubernetes_rolebindings_creation.toml` on Oct 15, 2021

Conversation 12 Commits 45 Checks 0 Files changed

austinsonger commented on Jun 6, 2021 Contributor ···

Issues

Resolves #1191

Summary

Contributor checklist

- Have you signed the contributor license agreement?
- Have you followed the contributor guidelines?

austinsonger and others added 27 commits 3 years ago

`Update impact_iam_deactivate_mfa_device.toml` … 13b7a2c

Reviewers

brokensound77 ✓

w0rk3r ✓

Assignees

w0rk3r

Labels

backport: auto community Domain: Cloud Integration: GCP Rule: New

Projects

None yet

Milestone

No milestone

Update impact_iam_deactivate_mfa_device.toml da7d230

Update discovery_post_exploitation_external_ip_lookup.toml … b57fd60

Merge branch 'main' into main b0bddce

Merge branch 'main' into main 178baaf

Update rules/aws/impact_iam_deactivate_mfa_device.toml … 475a132

Revert "Update discovery_post_exploitation_external_ip_lookup.toml" … ef40cc2

Merge pull request #1 from elastic/main … 3c9fed2

Merge pull request #2 from elastic/main … 76344b7

Merge pull request #3 from elastic/main … 1f4723e

Merge pull request #4 from elastic/main … e60c7fe

Merge branch 'elastic:main' into main 71b7597

Merge branch 'elastic:main' into main 80d1035

Merge branch 'elastic:main' into main bdf860d

Merge branch 'elastic:main' into main d5dda87

Update 6833d0b

New Rule: Okta User Attempted Unauthorized Access 006e02e

Update privilege_escalation_okta_user_attempted_unauthorized_access.toml 1297aac

Update privilege_escalation_okta_user_attempted_unauthorized_access.toml 7d6357a

Delete privilege_escalation_okta_user_attempted_unauthorized_access.toml 72ffc88

Development

Successfully merging this pull request may close these issues.

[New Rule] Kubernetes Creation/Patching ...

4 participants

`Create persistence_new-or-modified-federation-domain.toml` 037d240

`Delete persistence_new-or-modified-federation-domain.toml` 5bb487b

`Merge branch 'elastic:main' into main` 0be9c10

`Merge branch 'elastic:main' into main` deb69c5

`Create credential_access_gcp_kubernetes_rolebindings_creation.toml` 361766f

`Update credential_access_gcp_kubernetes_rolebindings_creation.toml` 00ff87d

`Update credential_access_gcp_kubernetes_rolebindings_creation.toml` 73452bc

github-actions bot added the **backport: auto** label on Jun 6, 2021

austinsonger added 2 commits 3 years ago

`Update credential_access_gcp_kubernetes_rolebindings_creation.toml` 31b6109

`Update credential_access_gcp_kubernetes_rolebindings_creation.toml` 25a947c

7 hidden items

Load more...

botelastic bot added the **stale** label on Sep 21, 2021

`Merge branch 'main' into credential_access_gcp_kubernetes_rolebinding…` b9dad55

…

botelastic bot added Domain: Cloud Integration: GCP and removed stale labels on Sep 22, 2021

`Merge branch 'main' into credential_access_gcp_kubernetes_rolebinding…` … 4406913

w0rk3r self-assigned this on Oct 12, 2021

w0rk3r requested changes on Oct 13, 2021 View reviewed changes

w0rk3r left a comment Contributor •••

Left some points we need to clarify, thanks!

`rules/integrations/gcp/credential_access_gcp_kubernetes_rolebindings_creation.toml` Outdated Show resolved

`.gitignore` Outdated Show resolved

`rules/integrations/gcp/credential_access_gcp_kubernetes_rolebindings_creation.toml` Outdated Show resolved

`rules/integrations/gcp/credential_access_gcp_kubernetes_rolebindings_creation.toml` Outdated Show resolved

`rules/integrations/gcp/credential_access_gcp_kubernetes_rolebindings_creation.toml` Outdated Show resolved `rules/integrations/gcp/credential_access_gcp_kubernetes_rolebindings_creation.toml` Outdated Show resolved

`rules/integrations/gcp/credential_access_gcp_kubernetes_rolebindings_creation.toml` Outdated Show resolved

austinsonger and others added 8 commits 3 years ago

- `Update .gitignore` … a14dcd9
- `Update rules/integrations/gcp/credential_access_gcp_kubernetes_rolebi…` … 13ef800
- `Update credential_access_gcp_kubernetes_rolebindings_creation.toml` 88e9920
- `Update credential_access_gcp_kubernetes_rolebindings_creation.toml` 944ac9d
- `Update and rename credential_access_gcp_kubernetes_rolebindings_creat…` … bf530a5
- `Update credential_access_gcp_kubernetes_rolebindings_created_or_patch…` … 35b2ccd
- `Update credential_access_gcp_kubernetes_rolebindings_created_or_patch…` … 3f6c159
- `Merge branch 'main' into credential_access_gcp_kubernetes_rolebinding…` … c1ab047

w0rk3r approved these changes on Oct 14, 2021 View reviewed changes

w0rk3r left a comment Contributor …

LGTM after renaming to privilege_escalation_*

`Rename credential_access_gcp_kubernetes_rolebindings_created_or_patch…` … a964f7e

austinsonger changed the title ~~[New Rule] GCP Kubernetes Rolebindings Creation~~ [New Rule] GCP Kubernetes Rolebindings Created or Patched on Oct 14, 2021

w0rk3r requested a review from **brokensound77** 3 years ago

brokensound77 reviewed on Oct 15, 2021

View reviewed changes

`rules/integrations/gcp/privilege_escalation_gcp_kubernetes_rolebindings_created_or_patched.toml` Outdated Show resolved

`remove space from query` 65f799a

brokensound77 approved these changes on Oct 15, 2021

View reviewed changes

w0rk3r merged commit **27ba204** into `elastic:main` on Oct 15, 2021

protectionsmachine pushed a commit that referenced this pull request on Oct 15, 2021

`[New Rule] GCP Kubernetes Rolebindings Created or Patched (#1267)` … bd3adfd

protectionsmachine pushed a commit that referenced this pull request on Oct 15, 2021

`[New Rule] GCP Kubernetes Rolebindings Created or Patched (#1267)` … 8bb2d27

protectionsmachine pushed a commit that referenced this pull request on Oct 15, 2021

`[New Rule] GCP Kubernetes Rolebindings Created or Patched (#1267)` … 63a9473

w0rk3r mentioned this pull request on Oct 18, 2021

[New Rule] Azure Kubernetes Rolebindings Created #1576 Merged

austinsonger deleted the `credential_access_gcp_kubernetes_rolebindings_creation…` branch 3 years ago

CyberTaoFlow commented on Jan 23, 2022 ···

@austinsonger Can we have the system:addon-manager user provided as an exception by default for this otherwise its quite noisy.

Sign up for free **to join this conversation on GitHub**. Already have an account? Sign in to comment

Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information

© 2024 GitHub, Inc.