Product ▾Solutions ▾Resources ▾Open Source ▾Enterprise ▾Pricing

elastic / detection-rulesPublic

NotificationsFork 498Star 2k

<> CodeIssues 144Pull requests 28ActionsSecurityInsights


[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 12Commits 45Checks 0Files changed 1+47 -0

austinsonger commented on Jun 6, 2021Contributor

Issues

Resolves #1191

Summary

Contributor checklist

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

Reviewers

brokensound77

w0rk3r

Assignees

w0rk3r

Labels

backport: auto

community


















Domain: Cloud

Integration: GCP

Rule: New

Projects

None yet

📁	austinsonger and others added 27 commits 3 years ago		
🔗	 Update impact_iam_deactivate_mfa_device.toml ...	Verified	13b7a2c
🔗	 Update impact_iam_deactivate_mfa_device.toml	Verified	da7d230
🔗	 Update discovery_post_exploitation_external_ip_lookup.toml ...	Verified	b57fd60
🔗	 Merge branch 'main' into main	Verified	b0bddce
🔗	 Merge branch 'main' into main	Verified	178baaf
🔗	 Update rules/aws/impact_iam_deactivate_mfa_device.toml ...	Verified	475a132
🔗	 Revert "Update discovery_post_exploitation_external_ip_lookup.toml" ...		ef40cc2
🔗	 Merge pull request #1 from elastic/main ...	Verified	3c9fed2
🔗	 Merge pull request #2 from elastic/main ...	Verified	76344b7
🔗	 Merge pull request #3 from elastic/main ...	Verified	1f4723e
🔗	 Merge pull request #4 from elastic/main ...	Verified	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

Milestone





No milestone

Development

Successfully merging this pull request may close these issues.

🔗 [New Rule] Kubernetes Creation/Patching of RoleB...

4 participants



Update

Verified

1297aac

privilege_escalation_okta_user_attempted_unauthorized_access.toml

Update

Verified

7d6357a

privilege_escalation_okta_user_attempted_unauthorized_access.toml

Delete

Verified

72ffc88

privilege_escalation_okta_user_attempted_unauthorized_access.toml

Create

Verified

037d240

persistence_new-or-modified-federation-domain.toml

Delete

Verified

5bb487b

persistence_new-or-modified-federation-domain.toml

Merge branch 'elastic:main' into main

0be9c10

Merge branch 'elastic:main' into main

deb69c5

Create

Verified

361766f

credential_access_gcp_kubernetes_rolebindings_creation.toml

Update

Verified

00ff87d

credential_access_gcp_kubernetes_rolebindings_creation.toml

Update

Verified

73452bc

credential_access_gcp_kubernetes_rolebindings_creation.toml

github-actions

bot

added the

backport: auto

label on Jun 6, 2021

austinsonger

added 2 commits

3 years ago

Update

Verified

31b6109

credential_access_gcp_kubernetes_rolebindings_creation.toml

Update

Verified

25a947c

credential_access_gcp_kubernetes_rolebindings_creation.toml

7 hidden items

Load more...

botelastic

bot

added the

stale

label on Sep 21, 2021

Merge branch 'main' into

credential_access_gcp_kubernetes_rolebinding...

...

Verified

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...

...

Verified

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_kubern
etes_rolebindings_creation.toml

Outdated

Show resolved

.gitignore

Outdated

Show resolved

rules/integrations/gcp/credential_access_gcp_kubern
etes_rolebindings_creation.toml Outdated Show resolved

















rules/integrations/gcp/credential_access_gcp_kubern
etes_rolebindings_creation.toml Outdated Show resolved

rules/integrations/gcp/credential_access_gcp_kubern
etes_rolebindings_creation.toml Outdated Show resolved

rules/integrations/gcp/credential_access_gcp_kubern
etes_rolebindings_creation.toml Outdated Show resolved

rules/integrations/gcp/credential_access_gcp_kubern
etes_rolebindings_creation.toml Outdated Show resolved

 austinsonger and others added 8 commits 3 years ago

-   Update .gitignore ... Verified a14dcd9
-   Update rules/integrations/gcp/credential_access_gcp_kubernetes_rolebi... ... Verified 13ef800
-   Update credential_access_gcp_kubernetes_rolebindings_creation.toml Verified 88e9920
-   Update credential_access_gcp_kubernetes_rolebindings_creation.toml Verified 944ac9d
-   Update and rename credential_access_gcp_kubernetes_rolebindings_creat... ... Verified bf530a5
-   Update credential_access_gcp_kubernetes_rolebindings_created_or_patch... ... Verified 35b2ccd
-   Update credential_access_gcp_kubernetes_rolebindings_created_or_patch... ... Verified 3f6c159
-   Merge branch 'main' into credential_access_gcp_kubernetes_rolebinding... ... Verified 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... ... Verified 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_kub
ernetes_rolebindings_created_or_patched.toml Outdated Show resolved


-   remove space from query Verified 65f799a




brokenound77

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.toml` 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](#)