Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

elastic / detection-rules Public

Notifications Fork 498 Star 2k

Code Issues 144 Pull requests 28 Actions Security Insights

Files

598f3d7

Go to file

.github
detection_rules
docs
etc
kibana
kql
rta
rules
_deprecated
apm
cross-platform
integrations
aws
NOTICE.txt
collection_cloudtrail_logging_...
credential_access_aws_iam_as...
credential_access_iam_user_a...
credential_access_root_consol...
credential_access_secretsman...
defense_evasion_cloudtrail_lo...
defense_evasion_cloudtrail_lo...
defense_evasion_cloudwatch_...
defense_evasion_config_servi...
defense_evasion_configuratio...
defense_evasion_ec2_flow_lo...
defense_evasion_ec2_networ...
defense_evasion_guardduty_...
defense_evasion_s3_bucket_c...
defense_evasion_waf_acl_dele...
defense_evasion_waf_rule_or_...
exfiltration_ec2_full_network_...
exfiltration_ec2_snapshot_cha...
exfiltration_ec2_vm_export_fai...
exfiltration_rds_snapshot_exp...
impact_cloudtrail_logging_up...
impact_cloudwatch_log_grou...

detection-rules / rules / integrations / aws / persistence_elasticache_security_group_creation.toml

⚠ This commit does not belong to any branch on this repository, and may belong to a fork outside of the repository.

austinsonger Update 598f3d7 · 3 years ago History

Code Blame 54 lines (47 loc) · 1.77 KB Raw

```
[metadata]
creation_date = "2021/07/19"
maturity = "production"
updated_date = "2021/07/19"

[rule]
author = ["Austin Songer"]
description = "Identifies when an ElastiCache security group has been created."
false_positives = [
    """
    A ElastiCache security group may be created by a system or network administrator. V
    agent, and/or hostname should be making changes in your environment. Security group
    or hosts should be investigated. If known behavior is causing false positives, it c
    """,
]
from = "now-60m"
index = ["filebeat-*", "logs-aws*"]
interval = "10m"
language = "kuery"
license = "Elastic License v2"
name = "AWS ElastiCache Security Group Created"
note = """## Config

The AWS Fleet integration, Filebeat module, or similarly structured data is required to
references = ["https://docs.aws.amazon.com/AmazonElastiCache/latest/APIReference/Welcom
risk_score = 21
rule_id = "7b3da11a-60a2-412e-8aa7-011e1eb9ed47"
severity = "low"
tags = ["Elastic", "Cloud", "AWS", "Continuous Monitoring", "SecOps", "Monitoring"]
timestamp_override = "event.ingested"
type = "query"

query = '''
event.dataset:aws.cloudtrail and  event.provider:elasticache.amazonaws.com and event.ac
event.outcome:success
'''


[[rule.threat]]
framework = "MITRE ATT&CK"
[[rule.threat.technique]]
id = "T1136"
name = "Create Account"
reference = "https://attack.mitre.org/techniques/T1136/"
[[rule.threat.technique.subtechnique]]
id = "T1136.003"
name = "Cloud Account"
reference = "https://attack.mitre.org/techniques/T1136/003/"


[rule.threat.tactic]
```

impact_cloudwatch_log_strea...
impact_ec2_disable_ebs_encr...
impact_iam_deactivate_mfa_d...
impact_iam_group_deletion.t...
impact_rds_cluster_deletion.t...
impact_rds_group_deletion.to...

```
52     id = "TA0003"
53     name = "Persistence"
54     reference = "https://attack.mitre.org/tactics/TA0003/"
```