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

7d5efd6

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 / impact_elasticache_security_group_modified_or_deleted.toml

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

austinsonger Update 7d5efd6 · 3 years ago History

Code Blame 52 lines (45 loc) · 1.83 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 modified or delet
false_positives = [
    """
    A ElastiCache security group deletion may be done by a system or network administra
    user agent, and/or hostname should be making changes in your environment. Security
    users or hosts should be investigated. If known behavior is causing false positives
    rule.
    """,
]
from = "now-60m"
index = ["filebeat-*", "logs-aws*"]
interval = "10m"
language = "kuery"
license = "Elastic License v2"
name = "AWS ElastiCache Security Group Modified or Deleted"
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 = "1ba5160d-f5a2-4624-b0ff-6a1dc55d2516"
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.act
"Authorize Cache Security Group Ingress" or  "Revoke Cache Security Group Ingress" or "
"RevokeCacheSecurityGroupEgress") and event.outcome:success
'''


[[rule.threat]]
framework = "MITRE ATT&CK"
[[rule.threat.technique]]
id = "T1531"
name = "Account Access Removal"
reference = "https://attack.mitre.org/techniques/T1531/"


[rule.threat.tactic]
id = "TA0040"
name = "Impact"
```

- impact_cloudwatch_log_strea...
- impact_ec2_disable_ebs_encr...
- impact_elasticache_security_g...
- impact_iam_deactivate_mfa_d...
- impact_iam_group_deletion.t...
- impact_rds_cluster_deletion.t...

```
reference = "https://attack.mitre.org/tactics/TA0040/"
```