Files

c76a397

Go to file

- .github
- detection_rules
- docs
- 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_elasticache_...
      - defense_evasion_elasticache_...
      - 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...
      - exfiltration_rds_snapshot_rest...

detection-rules / rules / integrations / aws / persistence_route_53_domain_transferred_to_another_account.toml

rw-access [Fleet] Track integrations in folder and metadata (#1372) 1882f44 · 3 years ago History

Code Blame 59 lines (50 loc) · 1.89 KB Raw

```
[metadata]
creation_date = "2021/05/10"
maturity = "production"
updated_date = "2021/07/20"
integration = "aws"

[rule]
author = ["Elastic", "Austin Songer"]
description = "Identifies when a request has been made to transfer a Route 53 domain to
false_positives = [
    """
    A domain may be transferred to another AWS account by a system or network administr
    identity, user agent, and/or hostname should be making changes in your environment.
    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 Route 53 Domain Transferred to Another Account"
note = """## Config

The AWS Fleet integration, Filebeat module, or similarly structured data is required to
references = ["https://docs.aws.amazon.com/Route53/latest/APIReference/API_Operations_A
risk_score = 21
rule_id = "2045567e-b0af-444a-8c0b-0b6e2dae9e13"
severity = "low"
tags = ["Elastic", "Cloud", "AWS", "Continuous Monitoring", "SecOps", "Asset Visibility
timestamp_override = "event.ingested"
type = "query"

query = '''
event.dataset:aws.cloudtrail and event.provider:route53.amazonaws.com and event.action:
'''


[[rule.threat]]
framework = "MITRE ATT&CK"
[[rule.threat.technique]]
id = "T1098"
reference = "https://attack.mitre.org/techniques/T1098/"
name = "Account Manipulation"


[rule.threat.tactic]
id = "TA0003"
reference = "https://attack.mitre.org/tactics/TA0003/"
name = "Persistence"
[[rule.threat]]
framework = "MITRE ATT&CK"

[rule.threat.tactic]
id = "TA0006"
```

impact_aws_eventbridge_rule...

impact_cloudtrail_logging_up...

impact_cloudwatch_log_grou...

impact_cloudwatch_log_strea...

impact_ec2_disable_ebs_encr...

impact_efs_filesystem_or_mo...

```
id = "TA0006"
reference = "https://attack.mitre.org/tactics/TA0006/"
name = "Credential Access"
```