






[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

A screenshot of a file explorer interface. At the top, there's a header bar with a folder icon and the text "Files". Below this is a search bar containing the text "c76a397" and a magnifying glass icon. Under the search bar is a text input field with the placeholder "Go to file". The main area displays a directory tree. The root is "Files". It contains several folders: ".github", "detection_rules", "docs", "kibana", "kql", "rta", "rules", and "integrations". The "rules" folder is expanded, showing subfolders: "_deprecated", "apm", "cross-platform", and "aws". The "aws" folder is further expanded, listing a long list of files, each with a document icon: "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_guarddduty_...", "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...", and "exfiltration_rds_snapshot_rest...".

detection-rules / rules / integrations / aws

/ persistence_route_53_domain_transfer_lock_disabled.toml

rw-access [Fleet] Track integrations in folder and metadata (#1372)

1882f44 · 3 years ago

History

CodeBlame64 lines (55 loc) · 2.06 KBRawCopyDownloadCompare

```
1      [metadata]
2      creation_date = "2021/05/10"
3      maturity = "production"
4      updated_date = "2021/07/20"
5      integration = "aws"
6
7      [rule]
8      author = ["Elastic", "Austin Songer"]
9      description = ""
10     Identifies when a transfer lock was removed from a Route 53 domain. It is recommended t
11     action unless intending to transfer the domain to a different registrar.
12     ""
13     false_positives = [
14         ""
15         A domain transfer lock may be disabled by a system or network administrator. Verify
16         agent, and/or hostname should be making changes in your environment. Activity from
17         be investigated. If known behavior is causing false positives, it can be exempted f
18         "",
19     ]
20     from = "now-60m"
21     index = ["filebeat-*", "logs-aws*"]
22     interval = "10m"
23     language = "kuery"
24     license = "Elastic License v2"
25     name = "AWS Route 53 Domain Transfer Lock Disabled"
26     note = ""## Config
27
28     The AWS Fleet integration, Filebeat module, or similarly structured data is required to
29     references = [
30         "https://docs.aws.amazon.com/Route53/latest/APIReference/API_Operations_Amazon_Rout
31         "https://docs.aws.amazon.com/Route53/latest/APIReference/API_domains_DisableDomainT
32     ]
33     risk_score = 21
34     rule_id = "12051077-0124-4394-9522-8f4f4db1d674"
35     severity = "low"
36     tags = ["Elastic", "Cloud", "AWS", "Continuous Monitoring", "SecOps", "Asset Visibility
37     timestamp_override = "event.ingested"
38     type = "query"
39
40     query = ''
41     event.dataset:aws.cloudtrail and event.provider:route53.amazonaws.com and event.action:
42     ''
43
44
45     [[rule.threat]]
46     framework = "MITRE ATT&CK"
47     [[rule.threat.technique]]
48     id = "T1098"
49     name = "Account Manipulation"
50     reference = "https://attack.mitre.org/techniques/T1098/"
51
52
53     [rule.threat.tactic]
54     id = "TA0003"
55     name = "Persistence"
56     reference = "https://attack.mitre.org/tactics/TA0003/"
```

- 📄 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...

```
56     reference = "https://attack.mitre.org/tactics/TA0005/"
57     [[rule.threat]]
58     framework = "MITRE ATT&CK"
59
60     [rule.threat.tactic]
61     id = "TA0006"
62     name = "Credential Access"
63     reference = "https://attack.mitre.org/tactics/TA0006/"
```