










Sign in


 elastic / **detection-rules** Public


 Notifications


 Fork 498


 Star 2k


 Code


 Issues 145


 Pull requests 20

 Actions

 Security

 Insights

detection-rules / rules / macos / persistence_enable_root_account.toml 




 terrancedejesus and Mikaayenson


[FR] Add Endpoint, APM and Windows Integration Tags t...  4312d8c · 2 years ago 


51 lines (43 loc) · 1.42 KB

CodeBlame

Raw







```
1  [metadata]
2  creation_date = "2020/01/04"
3  integration = ["endpoint"]
4  maturity = "production"
5  min_stack_comments = "New fields added: required_fields, related_integrations, setup"
6  min_stack_version = "8.3.0"
7  updated_date = "2022/12/14"
8
9  [rule]
10 author = ["Elastic"]
11 description = ""
12 Identifies attempts to enable the root account using the dsenableroot command. This command may be
13 for persistence, as the root account is disabled by default.
14 ""
15 from = "now-9m"
16 index = ["auditbeat-*", "logs-endpoint.events.*"]
17 language = "kuery"
18 license = "Elastic License v2"
19 name = "Attempt to Enable the Root Account"
20 references = ["https://ss64.com/osx/dsenableroot.html"]
21 risk_score = 47
22 rule_id = "cc2fd2d0-ba3a-4939-b87f-2901764ed036"
23 severity = "medium"
24 tags = ["Elastic", "Host", "macOS", "Threat Detection", "Persistence"]
25 timestamp_override = "event.ingested"
```

```
26     type = "query"
27
28     query = '''
29     event.category:process and event.type:(start or process_started) and
30     process.name:dsenableroot and not process.args:"-d"
31     '''
32
33
34     [[rule.threat]]
35     framework = "MITRE ATT&CK"
36     [[rule.threat.technique]]
37     id = "T1078"
38     name = "Valid Accounts"
39     reference = "https://attack.mitre.org/techniques/T1078/"
40     [[rule.threat.technique.subtechnique]]
41     id = "T1078.003"
42     name = "Local Accounts"
43     reference = "https://attack.mitre.org/techniques/T1078/003/"
44
45
46
47     [rule.threat.tactic]
48     id = "TA0003"
49     name = "Persistence"
50     reference = "https://attack.mitre.org/tactics/TA0003/"
```