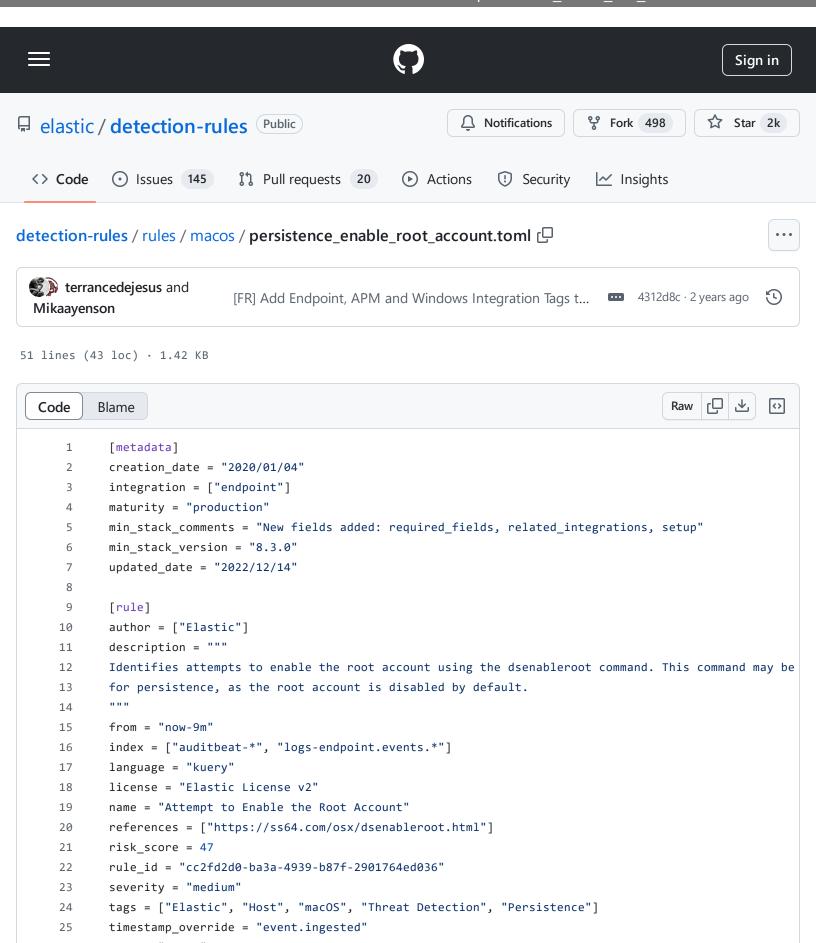
detection-rules/rules/macos/persistence_enable_root_account.toml at 4312d8c9583be524578a14fe6295c3370b9a9307 · elastic/detection-rules · GitHub - 31/10/2024 15:10 https://github.com/elastic/detection-

rules/blob/4312d8c9583be524578a14fe6295c3370b9a9307/rules/macos/persistence enable root account.toml



detection-rules/rules/macos/persistence_enable_root_account.toml at 4312d8c9583be524578a14fe6295c3370b9a9307 · elastic/detection-rules · GitHub - 31/10/2024 15:10 https://github.com/elastic/detection-

rules/blob/4312d8c9583be524578a14fe6295c3370b9a9307/rules/macos/persistence enable root account.toml

```
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]]
       id = "T1078"
37
       name = "Valid Accounts"
38
39
       reference = "https://attack.mitre.org/techniques/T1078/"
40
       [[rule.threat.technique.subtechnique]]
       id = "T1078.003"
41
42
       name = "Local Accounts"
43
       reference = "https://attack.mitre.org/techniques/T1078/003/"
44
45
46
47
       [rule.threat.tactic]
       id = "TA0003"
48
       name = "Persistence"
49
       reference = "https://attack.mitre.org/tactics/TA0003/"
```