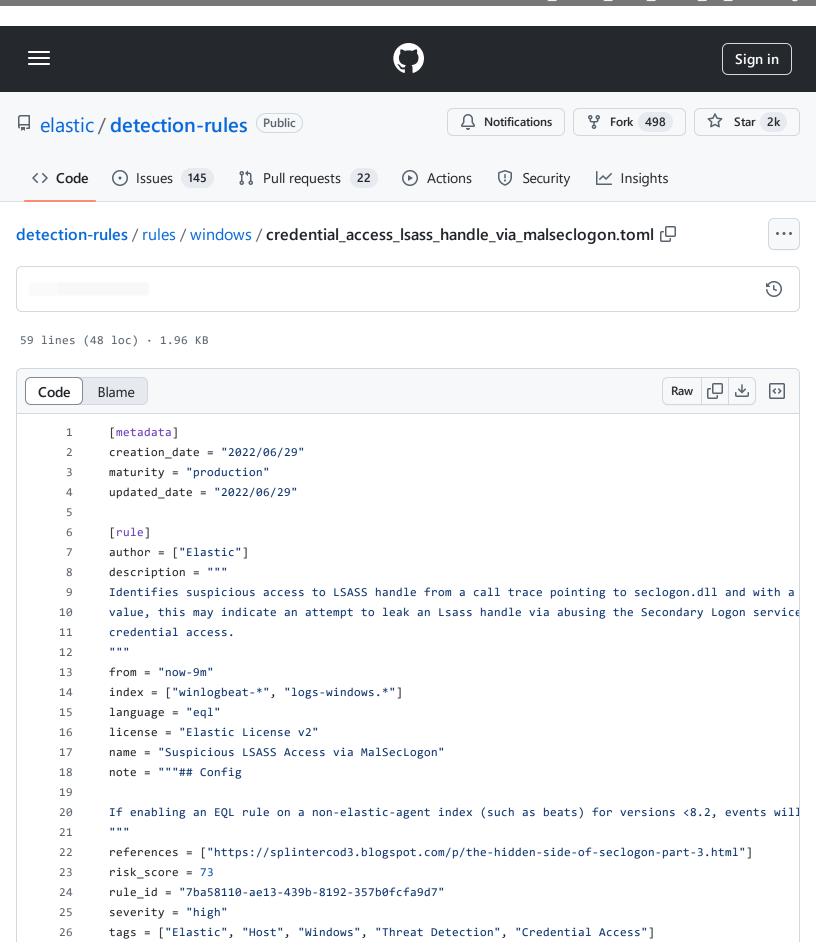
detection-rules/rules/windows/credential_access_lsass_handle_via_malseclogon.toml at 2bc1795f3d7bcc3946452eb4f07ae799a756d94e · elastic/detection-rules · GitHub - 31/10/2024 17:36 https://github.com/elastic/detection-

rules/blob/2bc1795f3d7bcc3946452eb4f07ae799a756d94e/rules/windows/credential access Isass handle via malseclogon



detection-rules/rules/windows/credential_access_lsass_handle_via_malseclogon.toml at 2bc1795f3d7bcc3946452eb4f07ae799a756d94e · elastic/detection-rules · GitHub - 31/10/2024 17:36 https://github.com/elastic/detection-

rules/blob/2bc1795f3d7bcc3946452eb4f07ae799a756d94e/rules/windows/credential access Isass handle via malseclogon

```
27
       timestamp_override = "event.ingested"
28
       type = "eql"
29
       query = '''
30
       process where event.code == "10" and
31
32
         winlog.event_data.TargetImage : "?:\\WINDOWS\\system32\\lsass.exe" and
33
          /* seclogon service accessing lsass */
34
         winlog.event_data.CallTrace: "*seclogon.dll*" and process.name: "svchost.exe" and
35
36
          /* PROCESS_CREATE_PROCESS & PROCESS_DUP_HANDLE & PROCESS_QUERY_INFORMATION */
37
         winlog.event_data.GrantedAccess == "0x14c0"
38
39
       1 \cdot 1 \cdot 1
40
41
       [[rule.threat]]
42
       framework = "MITRE ATT&CK"
43
       [[rule.threat.technique]]
44
       id = "T1003"
45
       name = "OS Credential Dumping"
46
47
       reference = "https://attack.mitre.org/techniques/T1003/"
       [[rule.threat.technique.subtechnique]]
48
       id = "T1003.001"
49
50
       name = "LSASS Memory"
51
       reference = "https://attack.mitre.org/techniques/T1003/001/"
52
53
54
       [rule.threat.tactic]
55
       id = "TA0006"
56
       name = "Credential Access"
57
       reference = "https://attack.mitre.org/tactics/TA0006/"
58
```