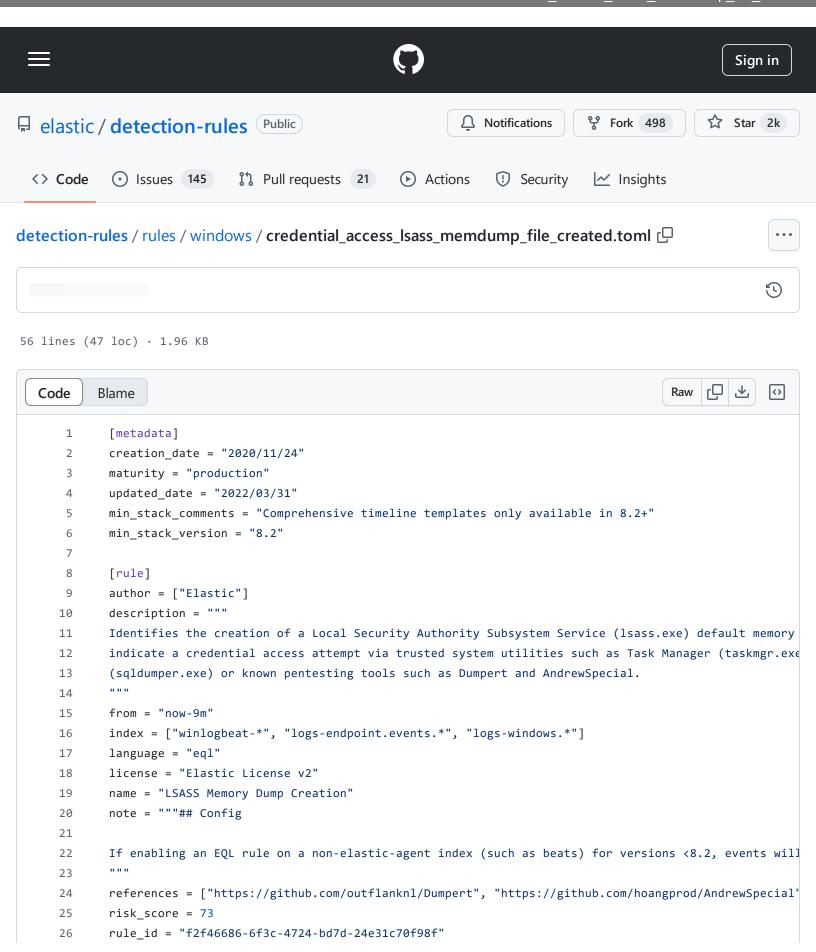
detection-rules/rules/windows/credential\_access\_lsass\_memdump\_file\_created.toml at c76a39796972ecde44cb1da6df47f1b6562c9770 · elastic/detection-rules · GitHub - 31/10/2024 16:18 https://github.com/elastic/detection-

rules/blob/c76a39796972ecde44cb1da6df47f1b6562c9770/rules/windows/credential access Isass memdump file created.



detection-rules/rules/windows/credential\_access\_lsass\_memdump\_file\_created.toml at c76a39796972ecde44cb1da6df47f1b6562c9770 · elastic/detection-rules · GitHub - 31/10/2024 16:18 https://github.com/elastic/detection-

rules/blob/c76a39796972ecde44cb1da6df47f1b6562c9770/rules/windows/credential\_access\_lsass\_memdump\_file\_created.f

```
27
       severity = "high"
28
       tags = ["Elastic", "Host", "Windows", "Threat Detection", "Credential Access"]
       timeline_id = "4d4c0b59-ea83-483f-b8c1-8c360ee53c5c"
29
       timeline_title = "Comprehensive File Timeline"
30
31
       timestamp_override = "event.ingested"
       type = "eql"
32
33
34
       query = '''
       file where file.name : ("lsass*.dmp", "dumpert.dmp", "Andrew.dmp", "SQLDmpr*.mdmp", "Coredump.dmp")
35
36
37
38
39
       [[rule.threat]]
       framework = "MITRE ATT&CK"
40
41
       [[rule.threat.technique]]
       id = "T1003"
42
       name = "OS Credential Dumping"
43
       reference = "https://attack.mitre.org/techniques/T1003/"
44
       [[rule.threat.technique.subtechnique]]
45
46
       id = "T1003.001"
47
       name = "LSASS Memory"
       reference = "https://attack.mitre.org/techniques/T1003/001/"
48
49
50
51
       [rule.threat.tactic]
52
53
       id = "TA0006"
54
       name = "Credential Access"
       reference = "https://attack.mitre.org/tactics/TA0006/"
55
```