






43 lines (36 loc) · 1.16 KB

CodeBlame

Raw

```
1  [metadata]
2  creation_date = "2020/11/02"
3  maturity = "production"
4  updated_date = "2021/03/03"
5
6  [rule]
7  author = ["Elastic"]
8  description = ""
9  Identifies use of the Windows file system utility (fsutil.exe ) to gather information about attached
10 and components connected to a computer system.
11 ""
12 from = "now-9m"
13 index = ["winlogbeat-*", "logs-endpoint.events.*", "logs-windows.*"]
14 language = " eql "
15 license = "Elastic License v2"
16 name = "Peripheral Device Discovery"
17 risk_score = 21
18 rule_id = "0c7ca5c2-728d-4ad9-b1c5-bbba83ecb1f4"
19 severity = "low"
20 tags = ["Elastic", "Host", "Windows", "Threat Detection", "Discovery"]
21 timestamp_override = "event.ingested"
22 type = " eql "
23
24 query = ''
25 process where event.type in ("start", "process_started") and
26 (process.name : "fsutil.exe" or process.pe.original_file_name == "fsutil.exe") and
```

```
27     process.args : "fsinfo" and process.args : "drives"
28     '''
29
30
31     [[rule.threat]]
32     framework = "MITRE ATT&CK"
33     [[rule.threat.technique]]
34     id = "T1120"
35     name = "Peripheral Device Discovery"
36     reference = "https://attack.mitre.org/techniques/T1120/"
37
38
39     [rule.threat.tactic]
40     id = "TA0007"
41     name = "Discovery"
42     reference = "https://attack.mitre.org/tactics/TA0007/"
```