```
[metadata]
creation_date = "2022/06/29"
maturity = "production"
updated_date = "2022/06/29"

[rule]
author = ["Elastic"]
description = """
Identifies suspicious access to LSASS handle from a call trace pointing to seclogon.dll and with a
value, this may indicate an attempt to leak an Lsass handle via abusing the Secondary Logon service
credential access.
"""
from = "now-9m"
index = ["winlogbeat-*", "logs-windows.*"]
language = "eql"
license = "Elastic License v2"
name = "Suspicious LSASS Access via MalSecLogon"
note = """## Config

If enabling an EQL rule on a non-elastic-agent index (such as beats) for versions <8.2, events will
"""
references = ["https://splintercod3.blogspot.com/p/the-hidden-side-of-seclogon-part-3.html"]
risk_score = 73
rule_id = "7ba58110-ae13-439b-8192-357b0fcfa9d7"
severity = "high"
tags = ["Elastic", "Host", "Windows", "Threat Detection", "Credential Access"]
```

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