ðŸ"Œ USB/Removable activity detected

1 message

<rangammabokka46@gmail.com> Fri, May 23, 2025 at 6:32 PM
Reply-to: rangammabokka46@gmail.com
To: rangammabokka46@gmail.com

USB or Removable Drive File Creation

@timestamp: 2025-05-23T13:00:13.910Z
_id: 9Yo6_ZYBjh1G8l0z5gzA
_index: .ds-winlogbeat-8.10.2-2025.05.14-000001
agent: {
"ephemeral_id": "4afc8c03-fd46-4b66-bcf8-8e0b467551fc",
"id": "e5e3a761-acc3-41a2-88c5-ee2b2b236970",
"name": "Viticm-SOC",
"type": "winlogbeat",
"version": "8.10.2"
}
ecs: {
"version": "1.12.0"
}
event: {
"action": "Process Create (rule: ProcessCreate)",
"category": [
"process"
],
"code": "1",
"created": "2025-05-23T13:00:18.083Z",
"ingested": "2025-05-23T13:00:17.962754Z",
"kind": "event",
"module": "sysmon",
"provider": "Microsoft-Windows-Sysmon",
"type": [
"start"
]
}
host: {
"architecture": "x86_64",
"hostname": "viticm-soc",
"id": "7e25c1a1-4745-47c6-abe9-ec7f50bf1d98",
"ip": [
"fe80::2674:6aaf:881:b09b",
"192.168.52.131"
],
"mac": [
"00-0C-29-C5-7F-10"
],
"name": "viticm-soc",
"os": {
"build": "19045.5854",
"family": "windows",
"kernel": "10.0.19041.5848 (WinBuild.160101.0800)",
"name": "Windows 10 Home",
"platform": "windows",
"type": "windows",
"version": "10.0"
}
}
log: {
"level": "information"
}
message: Process Create:
RuleName: -
UtcTime: 2025-05-23 13:00:13.910
ProcessGuid: {7e25c1a1-715d-6830-4601-000000002300}
ProcessId: 6956
Image: C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.25040.2-0\NisSrv.exe

```
    "computer_name": "Viticm-SOC",
    "event_data": {
        "Company": "Microsoft Corporation",
        "Description": "Microsoft Network Realtime Inspection Service",
        "FileVersion": "4.18.25040.2 (82640e7cfde5ee75f6010c8d2c06272146d2bb6b)",
        "IntegrityLevel": "System",
        "LogonGuid": "{7e25c1a1-6b85-6830-e503-000000000000}",
        "LogonId": "0x3e5",
        "ParentUser": "NT AUTHORITY\\SYSTEM",
        "Product": "Microsoft® Windows® Operating System",
        "TerminalSessionId": "0"
    },
    "event_id": "1",
    "opcode": "Info",
    "process": {
        "pid": 2468,
        "thread": {
            "id": 3116
        }
    },
    "provider_guid": "{5770385f-c22a-43e0-bf4c-06f5698ffbd9}",
    "provider_name": "Microsoft-Windows-Sysmon",
    "record_id": "24616",
    "task": "Process Create (rule: ProcessCreate)",
    "user": {
        "domain": "NT AUTHORITY",
        "identifier": "S-1-5-18",
        "name": "SYSTEM",
        "type": "User"
    },
    "version": 5
}
```