Sign in

Neo23x0 / sysmon-config Public

forked from SwiftOnSecurity/sysmon-config

🔔 Notifications   Fork 61   ☆ Star 452

<> Code   ⊙ Issues 2   ⅄ Pull requests   ▶ Actions   ▦ Projects   ⊘ Security   ⬚ Insights

sysmon-config / sysmonconfig-export-block.xml 🗗   ⋯

1480 lines (1397 loc) · 145 KB

```
1    <!--
2          sysmon-config | A Sysmon configuration focused on default high-quality event tracing and ea
3          Source project: https://github.com/SwiftOnSecurity/sysmon-config
4          Source license: Creative Commons Attribution 4.0 | You may privatize, fork, edit, teach, pu
5
6          WARNING: THIS CONFIG INCLUDES BLOCKING RULES THAT MAY CAUSE ISSUES ENDSYSTEMS!
7                Test this configuration intensively before using it on productive systems
8
9          LAST CHANGE: 18.08.2022
10
11         REQUIRED: Sysmon version 14 or higher (due to changes in syntax and bug-fixes)
12                https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
13   -->
14
15   <Sysmon schemaversion="4.82">
16         <!--SYSMON META CONFIG-->
17         <HashAlgorithms>md5,sha256,IMPHASH</HashAlgorithms> <!-- Both MD5 and SHA256 are the indust
18         <CheckRevocation/> <!-- Check loaded drivers, log if their code-signing certificate has bee
19
20         <!-- <ImageLoad/> --> <!-- Would manually force-on ImageLoad monitoring, even without confi
21         <!-- <ProcessAccessConfig/> --> <!-- Would manually force-on ProcessAccess monitoring, even
22         <!-- <PipeMonitoringConfig/> --> <!-- Would manually force-on PipeCreated / PipeConnected e
23         <!-- <ArchiveDirectory> -->
24
25         <EventFiltering>
```

```xml
26
27              <!--SYSMON EVENT ID 1 : PROCESS CREATION [ProcessCreate]-->
28                  <!--COMMENT:    All processes launched will be logged, except for what matches a ru
29                      to avoid user-mode executables imitating other process names to avoid loggi
30                      Ultimately, you must weigh CPU time checking many detailed rules, against t
31                      Beware of Masquerading, where attackers imitate the names and paths of legi
32                      code signatures to validate, but Sysmon does not support that. Look into Ap
33
34                  <!--DATA: UtcTime, ProcessGuid, ProcessID, Image, FileVersion, Description, Product
35          <RuleGroup name="" groupRelation="or">
36              <ProcessCreate onmatch="exclude">
37                  <CommandLine condition="contains">\Machine\Scripts\Startup\ipamprovisioning
38                  <!--SECTION: Microsoft Windows-->
39                  <CommandLine condition="is">"C:\Windows\system32\cscript.exe" /nologo "Moni
40                  <CommandLine condition="begin with"> "C:\Windows\system32\wermgr.exe" "-que
41                  <CommandLine condition="begin with">C:\Windows\system32\wbem\wmiprvse.exe -
42                  <CommandLine condition="begin with">C:\Windows\system32\wbem\wmiprvse.exe -
43                  <CommandLine condition="is">C:\Windows\system32\wermgr.exe -upload</Command
44                  <CommandLine condition="is">C:\Windows\system32\SearchIndexer.exe /Embeddin
45                  <CommandLine condition="is">C:\windows\system32\wermgr.exe -queuereporting<
46                  <CommandLine condition="is">\??\C:\Windows\system32\autochk.exe *</CommandL
47                  <CommandLine condition="is">\SystemRoot\System32\smss.exe</CommandLine> <!-
48                  <CommandLine condition="is">C:\Windows\System32\RuntimeBroker.exe -Embeddin
49                  <Image condition="is">C:\Program Files (x86)\Common Files\microsoft shared\
50                  <Image condition="is">C:\Windows\System32\TokenBrokerCookies.exe</Image> <!
51                  <Image condition="is">C:\Windows\System32\plasrv.exe</Image> <!--Windows: F
52                  <Image condition="is">C:\Windows\System32\wifitask.exe</Image> <!--Windows:
53                  <Image condition="is">C:\Windows\system32\CompatTelRunner.exe</Image> <!--W
54                  <Image condition="is">C:\Windows\system32\PrintIsolationHost.exe</Image> <!
55                  <Image condition="is">C:\Windows\system32\SppExtComObj.Exe</Image> <!--Wind
56                  <Image condition="is">C:\Windows\system32\audiodg.exe</Image> <!--Windows:
57                  <Image condition="is">C:\Windows\system32\conhost.exe</Image> <!--Windows:
58                  <Image condition="is">C:\Windows\system32\mobsync.exe</Image> <!--Windows:
59                  <Image condition="is">C:\Windows\system32\musNotification.exe</Image> <!--W
60                  <Image condition="is">C:\Windows\system32\musNotificationUx.exe</Image> <!-
61                  <Image condition="is">C:\Windows\system32\powercfg.exe</Image> <!--Microsof
62                  <Image condition="is">C:\Windows\system32\sndVol.exe</Image> <!--Windows: V
63                  <Image condition="is">C:\Windows\system32\sppsvc.exe</Image> <!--Windows: S
64                  <Image condition="is">C:\Windows\system32\wbem\WmiApSrv.exe</Image> <!--Win
65                  <IntegrityLevel condition="is">AppContainer</IntegrityLevel> <!--Windows: D
66                  <ParentCommandLine condition="begin with">%%SystemRoot%%\system32\csrss.exe
67                  <ParentCommandLine condition="is">C:\windows\system32\wermgr.exe -queuerepo
68                  <CommandLine condition="is">C:\WINDOWS\system32\devicecensus.exe UserCxt</C
69                  <CommandLine condition="is">C:\Windows\System32\usocoreworker.exe -Embeddin
70                  <ParentImage condition="is">C:\Windows\system32\SearchIndexer.exe</ParentIm
71                  <!--SECTION: Windows:svchost-->
```

```
 72                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k appmodel -s
 73                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k appmodel -p
 74                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k appmodel</Co
 75                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k appmodel -p
 76                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k camera -s Fr
 77                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k dcomlaunch -
 78                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k dcomlaunch -
 79                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k defragsvc</C
 80                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k devicesflow
 81                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k imgsvc</Comm
 82                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
 83                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
 84                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k LocalService
 85                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
 86                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
 87                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
 88                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
 89                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
 90                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
 91                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
 92                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
 93                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k LocalService
 94                          <CommandLine condition="is">C:\Windows\System32\svchost.exe -k LocalSystemN
 95                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
 96                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
 97                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
 98                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
 99                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localSystemN
100                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localSystemN
101                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localSystemN
102                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localSystemN
103                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localSystemN
104                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localSystemN
105                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localSystemN
106                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localSystemN
107                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localSystemN
108                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
109                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
110                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k netsvcs -p -
111                          <CommandLine condition="is">C:\Windows\System32\svchost.exe -k netsvcs -p -
112                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localSystemN
113                          <CommandLine condition="is">C:\Windows\System32\svchost.exe -k localSystemN
114                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localSystemN
115                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k netsvcs -p -
116                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k netsvcs -p -
117                          <CommandLine condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s F
```

117   <CommandLine Condition="is">C:\Windows\System32\svchost.exe -k netsvcs -s L

Code   Blame

Raw

```
1407                <Hashes condition="contains">IMPHASH=C547F2E66061A8DFFB6F5A3FF63C0A74</Hash
1408                <Hashes condition="contains">IMPHASH=0588081AB0E63BA785938467E1B10CCA</Hash
1409                <Hashes condition="contains">IMPHASH=0D9EC08BAC6C07D9987DFD0F1506587C</Hash
1410                <Hashes condition="contains">IMPHASH=BC129092B71C89B4D4C8CDF8EA590B29</Hash
1411                <Hashes condition="contains">IMPHASH=4DA924CF622D039D58BCE71CDF05D242</Hash
1412                <Hashes condition="contains">IMPHASH=E7A3A5C377E2D29324093377D7DB1C66</Hash
1413                <Hashes condition="contains">IMPHASH=9A9DBEC5C62F0380B4FA5FD31DEFFEDF</Hash
1414                <Hashes condition="contains">IMPHASH=AF8A3976AD71E5D5FDFB67DDB8DADFCE</Hash
1415                <Hashes condition="contains">IMPHASH=0C477898BBF137BBD6F2A54E3B805FF4</Hash
1416                <Hashes condition="contains">IMPHASH=0CA9F02B537BCEA20D4EA5EB1A9FE338</Hash
1417                <Hashes condition="contains">IMPHASH=3AB3655E5A14D4EEFC547F4781BF7F9E</Hash
1418                <Hashes condition="contains">IMPHASH=E6F9D5152DA699934B30DAAB206471F6</Hash
1419                <Hashes condition="contains">IMPHASH=3AD59991CCF1D67339B319B15A41B35D</Hash
1420                <Hashes condition="contains">IMPHASH=FFDD59E0318B85A3E480874D9796D872</Hash
1421                <Hashes condition="contains">IMPHASH=0CF479628D7CC1EA25EC7998A92F5051</Hash
1422                <Hashes condition="contains">IMPHASH=07A2D4DCBD6CB2C6A45E6B101F0B6D51</Hash
1423                <Hashes condition="contains">IMPHASH=D6D0F80386E1380D05CB78E871BC72B1</Hash
1424                <Hashes condition="contains">IMPHASH=38D9E015591BBFD4929E0D0F47FA0055</Hash
1425                <Hashes condition="contains">IMPHASH=0E2216679CA6E1094D63322E3412D650</Hash
1426                <Hashes condition="contains">IMPHASH=ADA161BF41B8E5E9132858CB54CAB5FB</Hash
1427                <Hashes condition="contains">IMPHASH=2A1BC4913CD5ECB0434DF07CB675B798</Hash
1428                <Hashes condition="contains">IMPHASH=11083E75553BAAE21DC89CE8F9A195E4</Hash
1429                <Hashes condition="contains">IMPHASH=A23D29C9E566F2FA8FFBB79267F5DF80</Hash
1430                <Hashes condition="contains">IMPHASH=4A07F944A83E8A7C2525EFA35DD30E2F</Hash
1431                <Hashes condition="contains">IMPHASH=767637C23BB42CD5D7397CF58B0BE688</Hash
1432                <Hashes condition="contains">IMPHASH=14C4E4C72BA075E9069EE67F39188AD8</Hash
1433                <Hashes condition="contains">IMPHASH=3C782813D4AFCE07BBFC5A9772ACDBDC</Hash
1434                <Hashes condition="contains">IMPHASH=7D010C6BB6A3726F327F7E239166D127</Hash
1435                <Hashes condition="contains">IMPHASH=89159BA4DD04E4CE5559F132A9964EB3</Hash
1436                <Hashes condition="contains">IMPHASH=6F33F4A5FC42B8CEC7314947BD13F30F</Hash
1437                <Hashes condition="contains">IMPHASH=5834ED4291BDEB928270428EBBAF7604</Hash
1438                <Hashes condition="contains">IMPHASH=5A8A8A43F25485E7EE1B201EDCBC7A38</Hash
1439                <Hashes condition="contains">IMPHASH=DC7D30B90B2D8ABF664FBED2B1B59894</Hash
1440                <Hashes condition="contains">IMPHASH=41923EA1F824FE63EA5BEB84DB7A3E74</Hash
1441                <Hashes condition="contains">IMPHASH=3DE09703C8E79ED2CA3F01074719906B</Hash
1442                <Hashes condition="contains">IMPHASH=A53A02B997935FD8EEDCB5F7ABAB9B9F</Hash
1443                <Hashes condition="contains">IMPHASH=E96A73C7BF33A464C510EDE582318BF2</Hash
1444                <Hashes condition="contains">IMPHASH=32089B8851BBF8BC2D014E9F37288C83</Hash
1445                <Hashes condition="contains">IMPHASH=09D278F9DE118EF09163C6140255C690</Hash
```

```
1446                            <Hashes condition="contains">IMPHASH=03866661686829D806989E2FC5A72606</Hash
1447                            <Hashes condition="contains">IMPHASH=E57401FBDADCD4571FF385AB82BD5D6D</Hash
1448
1449                            <!-- Microsoft Office Programs Dropping Executables -->
1450                            <Image condition="image">winword.exe</Image>
1451                            <Image condition="image">excel.exe</Image>
1452                            <Image condition="image">powerpnt.exe</Image>
1453                            <Image condition="image">msaccess.exe</Image>
1454                            <Image condition="image">mspub.exe</Image>
1455                            <Image condition="image">eqnedt32.exe</Image>
1456                            <Image condition="image">visio.exe</Image>
1457                            <Image condition="image">wordpad.exe</Image>
1458                            <Image condition="image">wordview.exe</Image>
1459
1460                            <!-- LOLBINs that can be used to download executables -->
1461                            <Image condition="image">certutil.exe</Image>
1462                            <Image condition="image">certoc.exe</Image>
1463                            <Image condition="image">CertReq.exe</Image>
1464                            <!-- <Image condition="image">bitsadmin.exe</Image> (depends on the environ
1465                            <Image condition="image">Desktopimgdownldr.exe</Image>
1466                            <Image condition="image">esentutl.exe</Image>
1467                            <Image condition="image">expand.exe</Image>
1468                            <Image condition="image">finger.exe</Image>
1469
1470                            <!-- Executables that should never drop an executable to disk (but may afte
1471                            <Image condition="image">notepad.exe</Image>
1472                            <Image condition="image">AcroRd32.exe</Image>
1473                            <Image condition="image">RdrCEF.exe</Image>
1474                            <Image condition="image">mshta.exe</Image>
1475                            <Image condition="image">hh.exe</Image>
1476                    </FileBlockExecutable>
1477            </RuleGroup>
1478
1479        </EventFiltering>
1480    </Sysmon>
```