sysmon-config / sysmonconfig-export-block.xml

Neo23x0 Dumpert Imphashes 3ae0fce · 2 years ago History

```
<!--
        sysmon-config | A Sysmon configuration focused on default high-quality event tr
        Source project: https://github.com/SwiftOnSecurity/sysmon-config
        Source license: Creative Commons Attribution 4.0 | You may privatize, fork, edi

        WARNING: THIS CONFIG INCLUDES BLOCKING RULES THAT MAY CAUSE ISSUES ENDSYSTEMS!
                 Test this configuration intensively before using it on productive syst

        LAST CHANGE: 18.08.2022

        REQUIRED: Sysmon version 14 or higher (due to changes in syntax and bug-fixes)
                https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
-->

<Sysmon schemaversion="4.82">
        <!--SYSMON META CONFIG-->
        <HashAlgorithms>md5,sha256,IMPHASH</HashAlgorithms> <!-- Both MD5 and SHA256 ar
        <CheckRevocation/> <!-- Check loaded drivers, log if their code-signing certifi

        <!-- <ImageLoad/> --> <!-- Would manually force-on ImageLoad monitoring, even w
        <!-- <ProcessAccessConfig/> --> <!-- Would manually force-on ProcessAccess moni
        <!-- <PipeMonitoringConfig/> --> <!-- Would manually force-on PipeCreated / Pip
        <!-- <ArchiveDirectory> -->

        <EventFiltering>

        <!--SYSMON EVENT ID 1 : PROCESS CREATION [ProcessCreate]-->
                <!--COMMENT:    All processes launched will be logged, except for what
                        to avoid user-mode executables imitating other process names to
                        Ultimately, you must weigh CPU time checking many detailed rule
                        Beware of Masquerading, where attackers imitate the names and p
                        code signatures to validate, but Sysmon does not support that.

                <!--DATA: UtcTime, ProcessGuid, ProcessID, Image, FileVersion, Descript
        <RuleGroup name="" groupRelation="or">
                <ProcessCreate onmatch="exclude">
                        <CommandLine condition="contains">\Machine\Scripts\Startup\ipam
                        <!--SECTION: Microsoft Windows-->
                        <CommandLine condition="is">"C:\Windows\system32\cscript.exe" /
                        <CommandLine condition="begin with"> "C:\Windows\system32\wermg
                        <CommandLine condition="begin with">C:\Windows\system32\wbem\wm
                        <CommandLine condition="begin with">C:\Windows\system32\wbem\wm
                        <CommandLine condition="is">C:\Windows\system32\wermgr.exe -upl
                        <CommandLine condition="is">C:\Windows\system32\SearchIndexer.e
                        <CommandLine condition="is">C:\windows\system32\wermgr.exe -que
                        <CommandLine condition="is">\??\C:\Windows\system32\autochk.exe
                        <CommandLine condition="is">\SystemRoot\System32\smss.exe</Comm
                        <CommandLine condition="is">C:\Windows\System32\RuntimeBroker.e
                        <Image condition="is">C:\Program Files (x86)\Common Files\micro
                        <Image condition="is">C:\Windows\System32\TokenBrokerCookies.ex
                        <Image condition="is">C:\Windows\System32\plasrv.exe</Image> <!
                        <Image condition="is">C:\Windows\System32\wifitask.exe</Image>
                        <Image condition="is">C:\Windows\system32\CompatTelRunner.exe</
                        <Image condition="is">C:\Windows\system32\PrintIsolationHost.ex
                        <Image condition="is">C:\Windows\system32\SppExtComObj.Exe</Ima
```

```
56                  <Image condition="is">C:\Windows\system32\audiodg.exe</Image> <
57                  <Image condition="is">C:\Windows\system32\conhost.exe</Image> <
58                  <Image condition="is">C:\Windows\system32\mobsync.exe</Image> <
59                  <Image condition="is">C:\Windows\system32\musNotification.exe</
60                  <Image condition="is">C:\Windows\system32\musNotificationUx.exe
61                  <Image condition="is">C:\Windows\system32\powercfg.exe</Image>
62                  <Image condition="is">C:\Windows\system32\sndVol.exe</Image> <!
63                  <Image condition="is">C:\Windows\system32\sppsvc.exe</Image> <!
64                  <Image condition="is">C:\Windows\system32\wbem\WmiApSrv.exe</Im
65                  <IntegrityLevel condition="is">AppContainer</IntegrityLevel> <!
66                  <ParentCommandLine condition="begin with">%%SystemRoot%%\system
67                  <ParentCommandLine condition="is">C:\windows\system32\wermgr.ex
68                  <CommandLine condition="is">C:\WINDOWS\system32\devicecensus.ex
69                  <CommandLine condition="is">C:\Windows\System32\usocoreworker.e
70                  <ParentImage condition="is">C:\Windows\system32\SearchIndexer.e
71                  <!--SECTION: Windows:svchost-->
72                  <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
73                  <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
74                  <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
75                  <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
```

```
1206                    <QueryName condition="is">mtalk.google.com</QueryName> <!--Goog
1207                    <QueryName condition="is">update.googleapis.com</QueryName> <!-
1208                    <QueryName condition="is">www.googletagservices.com</QueryName>
1209                    <!--SocialNet-->
1210                    <QueryName condition="end with">.pscp.tv</QueryName> <!--Twitte
1211                    <!--OSCP/CRL Common-->
1212                    <QueryName condition="end with">.amazontrust.com</QueryName>
1213                    <QueryName condition="end with">.digicert.com</QueryName>
1214                    <QueryName condition="end with">.globalsign.com</QueryName>
1215                    <QueryName condition="end with">.globalsign.net</QueryName>
1216                    <QueryName condition="end with">.intel.com</QueryName>
1217                    <QueryName condition="end with">.symcb.com</QueryName> <!--Digi
1218                    <QueryName condition="end with">.symcd.com</QueryName> <!--Digi
1219                    <QueryName condition="end with">.thawte.com</QueryName>
1220                    <QueryName condition="end with">.usertrust.com</QueryName>
1221                    <QueryName condition="end with">.verisign.com</QueryName>
1222                    <QueryName condition="end with">ocsp.identrust.com</QueryName>
1223                    <QueryName condition="end with">pki.goog</QueryName>
1224                    <QueryName condition="is">msocsp.com</QueryName> <!--Microsoft:
1225                    <QueryName condition="is">ocsp.comodoca.com</QueryName>
1226                    <QueryName condition="is">ocsp.entrust.net</QueryName>
1227                    <QueryName condition="is">ocsp.godaddy.com</QueryName>
1228                    <QueryName condition="is">ocsp.int-x3.letsencrypt.org</QueryNam
1229                    <QueryName condition="is">ocsp.msocsp.com</QueryName> <!--Micro
1230                    <QueryName condition="is">pki.goog</QueryName>
1231                    <QueryName condition="end with">.pki.goog</QueryName>
1232                    <QueryName condition="is">ocsp.godaddy.com</QueryName>
1233                    <QueryName condition="is">amazontrust.com</QueryName>
1234                    <QueryName condition="end with">.amazontrust.com</QueryName>
1235                    <QueryName condition="is">ocsp.sectigo.com</QueryName>
1236                    <QueryName condition="is">pki-goog.l.google.com</QueryName>
1237                    <QueryName condition="end with">.usertrust.com</QueryName>
1238                    <QueryName condition="is">ocsp.comodoca.com</QueryName>
1239                    <QueryName condition="is">ocsp.verisign.com</QueryName>
1240                    <QueryName condition="is">ocsp.entrust.net</QueryName>
1241                    <QueryName condition="is">ocsp.identrust.com</QueryName>
1242                    <QueryName condition="end with">.ocsp.identrust.com</QueryName>
1243                    <QueryName condition="is">status.rapidssl.com</QueryName>
1244                    <QueryName condition="is">status.thawte.com</QueryName>
1245                    <QueryName condition="is">ocsp.int-x3.letsencrypt.org</QueryNam
1246                    <!-- SECTION: PRTG -->
1247                    <Image condition="is">C:\Program Files (x86)\PRTG Network Monit
1248                </DnsQuery>
1249            </RuleGroup>
```

```
1250
1251            <!--SYSMON EVENT ID 23 : FILE DELETE [FileDelete]-->
1252                    <!--EVENT 23: "File Delete"-->
1253                    <!--COMMENT:    Sandbox usage. When a program signals to Windows a file
1254                            Tries to save a copy of the deleted file in the archivedirector
1255                            operating system files (Recommended)" from Folder Options). Can
1256                            Use EVENT ID 26 if a copy is not needed.
1257                            [ https://isc.sans.edu/forums/diary/Sysmon+and+File+Deletion/26
1258                    -->
1259
1260                    <!--DATA: RuleName, UtcTime, ProcessGuid, ProcessId, User, Image, Targe
1261
1262            <!--
1263            <RuleGroup name="" groupRelation="or">
1264                    <FileDelete onmatch="include">
1265                    </FileDelete>
1266            </RuleGroup>
1267            -->
1268
1269            <!--SYSMON EVENT ID 24 : CLIPBOARD EVENT MONITORING [ClipboardChange]-->
1270                    <!--EVENT 24: "Clipboard changed"-->
1271                    <!--COMMENT:    Sandbox usage. Sysmon can capture the contents of clipb
1272                            An example of what could be a production usage on restricted de
1273
1274                    <!--DATA: EventType, UtcTime, ProcessGuid, ProcessId, Image, Session, C
1275
1276            <!--
1277            <RuleGroup name="" groupRelation="or">
1278                    <ClipboardChange onmatch="include">
1279                            <Image condition="end with">wscript.exe</Image>
1280                            <Image condition="end with">cscript.exe</Image>
1281                            <Image condition="end with">powershell.exe</Image>
1282                            <Image condition="end with">rdpclip.exe</Image>
1283                    </ClipboardChange>
1284            </RuleGroup>
1285            -->
1286
1287            <!--SYSMON EVENT ID 25 : PROCESS TAMPERING [ProcessTampering]-->
1288                    <!--EVENT 25: "Process Tampering"-->
1289                    <!--COMMENT:    This event is generated when a process image is changed
1290                            This may or may not provide value in your environment as it req
1291                            [ https://medium.com/falconforce/sysmon-13-process-tampering-de
1292
1293                    <!--DATA: EventType, RuleName, UtcTime, ProcessGuid, ProcessId, Image,
1294
1295            <!--
1296            <RuleGroup name="" groupRelation="or">
1297                    <ProcessTampering onmatch="exclude">
1298                            <Image condition="begin with">C:\Program Files (x86)\Microsoft\
1299                    </ProcessTampering>
1300            </RuleGroup>
1301            -->
1302
1303            <!--SYSMON EVENT ID 26 : FILE DELETE LOGGED [FileDeleteDetected]-->
1304                    <!--EVENT 26: "File Delete logged"-->
1305                    <!--COMMENT:    This event is generated when a program signals to Windo
1306                            Unlike event ID 23 it does not archive a copy of the file delet
```

Files

3f808d9

Go to file

- .github
- .gitignore
- README.md
- sysmonconfig-export-block.xml
- sysmonconfig-export.xml
- sysmonconfig-trace.xml

sysmon-config / sysmonconfig-export-block.xml ↑ Top

Code | Blame 1480 lines (1397 loc) · 145 KB Raw

```
1311                    <!--DATA: RuleName, UtcTime, ProcessGuid, ProcessId, User, Image, Targe
1312
1313            <!--SYSMON EVENT ID 255 : ERROR-->
1314                    <!--"This event is generated when an error occurred within Sysmon. They
1315                            and certain tasked could not be performed or a bug exists in th
1316                            Sysinternals forum or over Twitter (@markrussinovich)."-->
1317                    <!--Cannot be filtered.-->
1318
1319
1320            <!--SYSMON EVENT ID 27 : FILE BLOCK [FileBlockExecutable]-->
1321                    <!--EVENT 27: "File Block Executable"-->
1322                    <!--COMMENT:    This event is generated when an executable gets blocked
1323                            [ https://medium.com/@olafhartong/sysmon-14-0-fileblockexecutab
1324                    -->
```

```
1325
1326        <RuleGroup name="ImageBlock" groupRelation="or">
1327                <FileBlockExecutable onmatch="include">
1328                        <!-- Executables dropped to suspicious folders -->
1329                        <TargetFilename condition="begin with">C:\Users\Public\</Target
1330                        <TargetFilename condition="begin with">C:\Perflogs\</TargetFile
1331                        <TargetFilename condition="begin with">C:\Windows\Fonts\</Targe
1332                        <TargetFilename condition="begin with">C:\Windows\debug\</Targe
1333                        <TargetFilename condition="begin with">C:\Windows\Tasks\</Targe
1334                        <TargetFilename condition="begin with">C:\Windows\tracing\</Tar
1335                        <TargetFilename condition="begin with">C:\Windows\Help\</Target
1336                        <TargetFilename condition="begin with">C:\Windows\Logs\</Target
1337                        <TargetFilename condition="begin with">C:\Windows\System32\spoo
1338                        <TargetFilename condition="begin with">C:\Windows\System32\spoo
1339                        <TargetFilename condition="begin with">C:\Windows\Help\</Target
1340                        <TargetFilename condition="contains all">C:\Users\;\Music\</Tar
1341                        <TargetFilename condition="contains all">C:\Users\;\Pictures\</
1342                        <TargetFilename condition="contains all">C:\Users\;\Videos\</Ta
1343                        <TargetFilename condition="contains all">C:\Users\;\Contacts\</
1344
1345                        <!-- Executables double extensions -->
1346                        <TargetFilename condition="end with">.pdf.exe</TargetFilename>
1347                        <TargetFilename condition="end with">.doc.exe</TargetFilename>
1348                        <TargetFilename condition="end with">.docx.exe</TargetFilename>
1349                        <TargetFilename condition="end with">.xls.exe</TargetFilename>
1350                        <TargetFilename condition="end with">.xlsx.exe</TargetFilename>
1351                        <TargetFilename condition="end with">.xlsm.exe</TargetFilename>
1352                        <TargetFilename condition="end with">.docm.exe</TargetFilename>
1353                        <TargetFilename condition="end with">.ppt.exe</TargetFilename>
1354                        <TargetFilename condition="end with">.pptx.exe</TargetFilename>
1355                        <TargetFilename condition="end with">.txt.exe</TargetFilename>
1356                        <TargetFilename condition="end with">.rtf.exe</TargetFilename>
1357                        <TargetFilename condition="end with">.htm.exe</TargetFilename>
1358                        <TargetFilename condition="end with">.html.exe</TargetFilename>
1359                        <TargetFilename condition="end with">.iso.exe</TargetFilename>
1360                        <TargetFilename condition="end with">.zip.exe</TargetFilename>
1361                        <TargetFilename condition="end with">.rar.exe</TargetFilename>
1362                        <TargetFilename condition="end with">.7z.exe</TargetFilename>
1363
1364                        <!-- Hacktool Blocks based on Imphashes -->
1365                        <Hashes condition="contains">IMPHASH=BCCA3C247B619DCD13C8CDFF5F
1366                        <Hashes condition="contains">IMPHASH=3A19059BD7688CB88E70005F18
1367                        <Hashes condition="contains">IMPHASH=bf6223a49e45d99094406777eb
1368                        <Hashes condition="contains">IMPHASH=0C106686A31BFE2BA931AE1CF6
1369                        <Hashes condition="contains">IMPHASH=0D1447D4B3259B3C2A1D4CFB7E
1370                        <Hashes condition="contains">IMPHASH=1B0369A1E06271833F78FFA70F
1371                        <Hashes condition="contains">IMPHASH=4C1B52A19748428E51B14C278D
1372                        <Hashes condition="contains">IMPHASH=4D927A711F77D62CEBD4F322CB
1373                        <Hashes condition="contains">IMPHASH=66EE036DF5FC1004D9ED5E9A94
1374                        <Hashes condition="contains">IMPHASH=672B13F4A0B6F27D29065123FE
1375                        <Hashes condition="contains">IMPHASH=6BBD59CEA665C4AFCC2814C132
1376                        <Hashes condition="contains">IMPHASH=725BB81DC24214F6ECACC0CFB3
1377                        <Hashes condition="contains">IMPHASH=9528A0E91E28FBB88AD433FEAB
1378                        <Hashes condition="contains">IMPHASH=9DA6D5D77BE11712527DCAB86D
1379                        <Hashes condition="contains">IMPHASH=A6E01BC1AB89F8D91D9EAB7203
1380                        <Hashes condition="contains">IMPHASH=B24C5EDDAEA4FE50C6A96A2A13
1381                        <Hashes condition="contains">IMPHASH=D21BBC50DCC169D7B4D0F01962
1382                        <Hashes condition="contains">IMPHASH=FCC251CCEAE90D22C392215CC9
1383                        <Hashes condition="contains">IMPHASH=23867A89C2B8FC733BE6CF5EF9
1384                        <Hashes condition="contains">IMPHASH=A37FF327F8D48E8A4D2F757E1B
1385                        <Hashes condition="contains">IMPHASH=6118619783FC175BC7EBECFF07
1386                        <Hashes condition="contains">IMPHASH=959A83047E80AB68B368FDB3F4
1387                        <Hashes condition="contains">IMPHASH=563233BFA169ACC7892451F71A
1388                        <Hashes condition="contains">IMPHASH=87575CB7A0E0700EB37F2E3668
1389                        <Hashes condition="contains">IMPHASH=13F08707F759AF6003837A150A
1390                        <Hashes condition="contains">IMPHASH=1781F06048A7E58B323F0B9259
1391                        <Hashes condition="contains">IMPHASH=233F85F2D4BC9D6521A6CAAE11
1392                        <Hashes condition="contains">IMPHASH=24AF2584CBF4D60BBE5C6D1B31
1393                        <Hashes condition="contains">IMPHASH=632969DDF6DBF4E0F53424B75E
1394                        <Hashes condition="contains">IMPHASH=713C29B396B907ED71A7248275
1395                        <Hashes condition="contains">IMPHASH=749A7BB1F0B4C4455949C0B2BF
1396                        <Hashes condition="contains">IMPHASH=8628B2608957A6B0C6330AC3DE
1397                        <Hashes condition="contains">IMPHASH=8B114550386E31895DFAB371E7
1398                        <Hashes condition="contains">IMPHASH=94CB940A1A6B65BED4D5A8F849
```

```
1399                     <Hashes condition="contains">IMPHASH=9D68781980370E00E0BD939EE5
1400                     <Hashes condition="contains">IMPHASH=B18A1401FF8F444056D29450FB
1401                     <Hashes condition="contains">IMPHASH=CB567F9498452721D77A451374
1402                     <Hashes condition="contains">IMPHASH=730073214094CD328547BF1F72
1403                     <Hashes condition="contains">IMPHASH=17B461A082950FC63322285721
1404                     <Hashes condition="contains">IMPHASH=DC25EE78E2EF4D36FAA0BADF1E
1405                     <Hashes condition="contains">IMPHASH=819B19D53CA6736448F9325A85
1406                     <Hashes condition="contains">IMPHASH=829DA329CE140D873B4A8BDE2C
1407                     <Hashes condition="contains">IMPHASH=C547F2E66061A8DFFB6F5A3FF6
1408                     <Hashes condition="contains">IMPHASH=0588081AB0E63BA785938467E1
1409                     <Hashes condition="contains">IMPHASH=0D9EC08BAC6C07D9987DFD0F15
1410                     <Hashes condition="contains">IMPHASH=BC129092B71C89B4D4C8CDF8EA
1411                     <Hashes condition="contains">IMPHASH=4DA924CF622D039D58BCE71CDF
1412                     <Hashes condition="contains">IMPHASH=E7A3A5C377E2D29324093377D7
1413                     <Hashes condition="contains">IMPHASH=9A9DBEC5C62F0380B4FA5FD31D
1414                     <Hashes condition="contains">IMPHASH=AF8A3976AD71E5D5FDFB67DDB8
1415                     <Hashes condition="contains">IMPHASH=0C477898BBF137BBD6F2A54E3B
1416                     <Hashes condition="contains">IMPHASH=0CA9F02B537BCEA20D4EA5EB1A
1417                     <Hashes condition="contains">IMPHASH=3AB3655E5A14D4EEFC547F4781
1418                     <Hashes condition="contains">IMPHASH=E6F9D5152DA699934B30DAAB20
1419                     <Hashes condition="contains">IMPHASH=3AD59991CCF1D67339B319B15A
1420                     <Hashes condition="contains">IMPHASH=FFDD59E0318B85A3E480874D97
1421                     <Hashes condition="contains">IMPHASH=0CF479628D7CC1EA25EC7998A9
1422                     <Hashes condition="contains">IMPHASH=07A2D4DCBD6CB2C6A45E6B101F
1423                     <Hashes condition="contains">IMPHASH=D6D0F80386E1380D05CB78E871
1424                     <Hashes condition="contains">IMPHASH=38D9E015591BBFD4929E0D0F47
1425                     <Hashes condition="contains">IMPHASH=0E2216679CA6E1094D63322E34
1426                     <Hashes condition="contains">IMPHASH=ADA161BF41B8E5E9132858CB54
1427                     <Hashes condition="contains">IMPHASH=2A1BC4913CD5ECB0434DF07CB6
1428                     <Hashes condition="contains">IMPHASH=11083E75553BAAE21DC89CE8F9
1429                     <Hashes condition="contains">IMPHASH=A23D29C9E566F2FA8FFBB79267
1430                     <Hashes condition="contains">IMPHASH=4A07F944A83E8A7C2525EFA35D
1431                     <Hashes condition="contains">IMPHASH=767637C23BB42CD5D7397CF58B
1432                     <Hashes condition="contains">IMPHASH=14C4E4C72BA075E9069EE67F39
1433                     <Hashes condition="contains">IMPHASH=3C782813D4AFCE07BBFC5A9772
1434                     <Hashes condition="contains">IMPHASH=7D010C6BB6A3726F327F7E2391
1435                     <Hashes condition="contains">IMPHASH=89159BA4DD04E4CE5559F132A9
1436                     <Hashes condition="contains">IMPHASH=6F33F4A5FC42B8CEC7314947BD
1437                     <Hashes condition="contains">IMPHASH=5834ED4291BDEB928270428EBB
1438                     <Hashes condition="contains">IMPHASH=5A8A8A43F25485E7EE1B201EDC
1439                     <Hashes condition="contains">IMPHASH=DC7D30B90B2D8ABF664FBED2B1
1440                     <Hashes condition="contains">IMPHASH=41923EA1F824FE63EA5BEB84DB
1441                     <Hashes condition="contains">IMPHASH=3DE09703C8E79ED2CA3F010747
1442                     <Hashes condition="contains">IMPHASH=A53A02B997935FD8EEDCB5F7AB
1443                     <Hashes condition="contains">IMPHASH=E96A73C7BF33A464C510EDE582
1444                     <Hashes condition="contains">IMPHASH=32089B8851BBF8BC2D014E9F37
1445                     <Hashes condition="contains">IMPHASH=09D278F9DE118EF09163C61402
1446                     <Hashes condition="contains">IMPHASH=03866661686829D806989E2FC5
1447                     <Hashes condition="contains">IMPHASH=E57401FBDADCD4571FF385AB82
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
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 (
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>
```