Sign in

Neo23x0 / **sysmon-config** Public

Notifications | Fork 61 | Star 452

forked from SwiftOnSecurity/sysmon-config

Code | Issues 2 | Pull requests | Actions | Projects | Security | Insights

sysmon-config / **sysmonconfig-export-block.xml**

```
1480 lines (1397 loc) · 145 KB
```

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

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

        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 are the indust
        <CheckRevocation/> <!-- Check loaded drivers, log if their code-signing certificate has bee

        <!-- <ImageLoad/> --> <!-- Would manually force-on ImageLoad monitoring, even without confi
        <!-- <ProcessAccessConfig/> --> <!-- Would manually force-on ProcessAccess monitoring, ever
        <!-- <PipeMonitoringConfig/> --> <!-- Would manually force-on PipeCreated / PipeConnected e
        <!-- <ArchiveDirectory> -->

        <EventFiltering>

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

                <!--DATA: UtcTime, ProcessGuid, ProcessID, Image, FileVersion, Description, Product
        <RuleGroup name="" groupRelation="or">
                <ProcessCreate onmatch="exclude">
                        <CommandLine condition="contains">\Machine\Scripts\Startup\ipamprovisioning
                        <!--SECTION: Microsoft Windows-->
                        <CommandLine condition="is">"C:\Windows\system32\cscript.exe" /nologo "Moni
                        <CommandLine condition="begin with"> "C:\Windows\system32\wermgr.exe" "-que
                        <CommandLine condition="begin with">C:\Windows\system32\wbem\wmiprvse.exe -
                        <CommandLine condition="begin with">C:\Windows\system32\wbem\wmiprvse.exe -
                        <CommandLine condition="is">C:\Windows\system32\wermgr.exe -upload</Commanc
                        <CommandLine condition="is">C:\Windows\system32\SearchIndexer.exe /Embeddir
                        <CommandLine condition="is">C:\windows\system32\wermgr.exe -queuereporting<
                        <CommandLine condition="is">\??\C:\Windows\system32\autochk.exe *</CommandL
                        <CommandLine condition="is">\SystemRoot\System32\smss.exe</CommandLine> <!-
                        <CommandLine condition="is">C:\Windows\System32\RuntimeBroker.exe -Embeddir
                        <Image condition="is">C:\Program Files (x86)\Common Files\microsoft shared\
                        <Image condition="is">C:\Windows\System32\TokenBrokerCookies.exe</Image> <!
                        <Image condition="is">C:\Windows\System32\plasrv.exe</Image> <!--Windows: F
                        <Image condition="is">C:\Windows\System32\wifitask.exe</Image> <!--Windows:
                        <Image condition="is">C:\Windows\system32\CompatTelRunner.exe</Image> <!--W
                        <Image condition="is">C:\Windows\system32\PrintIsolationHost.exe</Image> <!
                        <Image condition="is">C:\Windows\system32\SppExtComObj.Exe</Image> <!--Winc
                        <Image condition="is">C:\Windows\system32\audiodg.exe</Image> <!--Windows:
                        <Image condition="is">C:\Windows\system32\conhost.exe</Image> <!--Windows:
                        <Image condition="is">C:\Windows\system32\mobsync.exe</Image> <!--Windows:
                        <Image condition="is">C:\Windows\system32\musNotification.exe</Image> <!--W
                        <Image condition="is">C:\Windows\system32\musNotificationUx.exe</Image> <!-
                        <Image condition="is">C:\Windows\system32\powercfg.exe</Image> <!--Microsof
                        <Image condition="is">C:\Windows\system32\sndVol.exe</Image> <!--Windows: V
                        <Image condition="is">C:\Windows\system32\sppsvc.exe</Image> <!--Windows: S
                        <Image condition="is">C:\Windows\system32\wbem\WmiApSrv.exe</Image> <!--Wir
                        <IntegrityLevel condition="is">AppContainer</IntegrityLevel> <!--Windows: D
                        <ParentCommandLine condition="begin with">%%SystemRoot%%\system32\csrss.exe
                        <ParentCommandLine condition="is">C:\windows\system32\wermgr.exe -queuerepc
                        <CommandLine condition="is">C:\WINDOWS\system32\devicecensus.exe UserCxt</C
                        <CommandLine condition="is">C:\Windows\System32\usocoreworker.exe -Embeddir
                        <ParentImage condition="is">C:\Windows\system32\SearchIndexer.exe</ParentIn
                        <!--SECTION: Windows:svchost-->
```

```
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k appmodel -s
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k appmodel -p
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k appmodel</Co
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k appmodel -p
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k camera -s Fr
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k dcomlaunch -
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k dcomlaunch -
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k defragsvc</C
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k devicesflow
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k imgsvc</Comm
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k LocalService
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k LocalService
                            <CommandLine condition="is">C:\Windows\System32\svchost.exe -k LocalSystemN
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localSystemN
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localSystemN
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localSystemN
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localSystemN
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localSystemN
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localSystemN
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localSystemN
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localSystemN
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localSystemN
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k netsvcs -p -
                            <CommandLine condition="is">C:\Windows\System32\svchost.exe -k netsvcs -p -
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localSystemN
                            <CommandLine condition="is">C:\Windows\System32\svchost.exe -k localSystemN
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localSystemN
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k netsvcs -p -
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k netsvcs -p -
                            <CommandLine condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s F
```

```
                              <CommandLine condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s B
```

Code Blame

Raw

```
<Hashes condition="contains">IMPHASH=C547F2E66061A8DFFB6F5A3FF63C0A74</Hash
<Hashes condition="contains">IMPHASH=0588081AB0E63BA785938467E1B10CCA</Hash
<Hashes condition="contains">IMPHASH=0D9EC08BAC6C07D9987DFD0F1506587C</Hash
<Hashes condition="contains">IMPHASH=BC129092B71C89B4D4C8CDF8EA590B29</Hash
<Hashes condition="contains">IMPHASH=4DA924CF622D039D58BCE71CDF05D242</Hash
<Hashes condition="contains">IMPHASH=E7A3A5C377E2D29324093377D7DB1C66</Hash
<Hashes condition="contains">IMPHASH=9A9DBEC5C62F0380B4FA5FD31DEFFEDF</Hash
<Hashes condition="contains">IMPHASH=AF8A3976AD71E5D5FDFB67DDB8DADFCE</Hash
<Hashes condition="contains">IMPHASH=0C477898BBF137BBD6F2A54E3B805FF4</Hash
<Hashes condition="contains">IMPHASH=0CA9F02B537BCEA20D4EA5EB1A9FE338</Hash
<Hashes condition="contains">IMPHASH=3AB3655E5A14D4EEFC547F4781BF7F9E</Hash
<Hashes condition="contains">IMPHASH=E6F9D5152DA699934B30DAAB206471F6</Hash
<Hashes condition="contains">IMPHASH=3AD59991CCF1D67339B319B15A41B35D</Hash
<Hashes condition="contains">IMPHASH=FFDD59E0318B85A3E480874D9796D872</Hash
<Hashes condition="contains">IMPHASH=0CF479628D7CC1EA25EC7998A92F5051</Hash
<Hashes condition="contains">IMPHASH=07A2D4DCBD6CB2C6A45E6B101F0B6D51</Hash
<Hashes condition="contains">IMPHASH=D6D0F80386E1380D05CB78E871BC72B1</Hash
<Hashes condition="contains">IMPHASH=38D9E015591BBFD4929E0D0F47FA0055</Hash
<Hashes condition="contains">IMPHASH=0E2216679CA6E1094D63322E3412D650</Hash
<Hashes condition="contains">IMPHASH=ADA161BF41B8E5E9132858CB54CAB5FB</Hash
<Hashes condition="contains">IMPHASH=2A1BC4913CD5ECB0434DF07CB675B798</Hash
<Hashes condition="contains">IMPHASH=11083E75553BAAE21DC89CE8F9A195E4</Hash
<Hashes condition="contains">IMPHASH=A23D29C9E566F2FA8FFBB79267F5DF80</Hash
<Hashes condition="contains">IMPHASH=4A07F944A83E8A7C2525EFA35DD30E2F</Hash
<Hashes condition="contains">IMPHASH=767637C23BB42CD5D7397CF58B0BE688</Hash
<Hashes condition="contains">IMPHASH=14C4E4C72BA075E9069EE67F39188AD8</Hash
<Hashes condition="contains">IMPHASH=3C782813D4AFCE07BBFC5A9772ACDBDC</Hash
<Hashes condition="contains">IMPHASH=7D010C6BB6A3726F327F7E239166D127</Hash
<Hashes condition="contains">IMPHASH=89159BA4DD04E4CE5559F132A9964EB3</Hash
<Hashes condition="contains">IMPHASH=6F33F4A5FC42B8CEC7314947BD13F30F</Hash
<Hashes condition="contains">IMPHASH=5834ED4291BDEB928270428EBBAF7604</Hash
<Hashes condition="contains">IMPHASH=5A8A8A43F25485E7EE1B201EDCBC7A38</Hash
<Hashes condition="contains">IMPHASH=DC7D30B90B2D8ABF664FBED2B1B59894</Hash
<Hashes condition="contains">IMPHASH=41923EA1F824FE63EA5BEB84DB7A3E74</Hash
<Hashes condition="contains">IMPHASH=3DE09703C8E79ED2CA3F01074719906B</Hash
<Hashes condition="contains">IMPHASH=A53A02B997935FD8EEDCB5F7ABAB9B9F</Hash
<Hashes condition="contains">IMPHASH=E96A73C7BF33A464C510EDE582318BF2</Hash
<Hashes condition="contains">IMPHASH=32089B8851BBF8BC2D014E9F37288C83</Hash
<Hashes condition="contains">IMPHASH=09D278F9DE118EF09163C6140255C690</Hash
```

```
            <Hashes condition="contains">IMPHASH=03866661686829D806989E2FC5A72606</Hash
            <Hashes condition="contains">IMPHASH=E57401FBDADCD4571FF385AB82BD5D6D</Hash

            <!-- Microsoft Office Programs Dropping Executables -->
            <Image condition="image">winword.exe</Image>
            <Image condition="image">excel.exe</Image>
            <Image condition="image">powerpnt.exe</Image>
            <Image condition="image">msaccess.exe</Image>
            <Image condition="image">mspub.exe</Image>
            <Image condition="image">eqnedt32.exe</Image>
            <Image condition="image">visio.exe</Image>
            <Image condition="image">wordpad.exe</Image>
            <Image condition="image">wordview.exe</Image>

            <!-- LOLBINs that can be used to download executables -->
            <Image condition="image">certutil.exe</Image>
            <Image condition="image">certoc.exe</Image>
            <Image condition="image">CertReq.exe</Image>
            <!-- <Image condition="image">bitsadmin.exe</Image> (depends on the environ
            <Image condition="image">Desktopimgdownldr.exe</Image>
            <Image condition="image">esentutl.exe</Image>
            <Image condition="image">expand.exe</Image>
            <Image condition="image">finger.exe</Image>

            <!-- Executables that should never drop an executable to disk (but may afte
            <Image condition="image">notepad.exe</Image>
            <Image condition="image">AcroRd32.exe</Image>
            <Image condition="image">RdrCEF.exe</Image>
            <Image condition="image">mshta.exe</Image>
            <Image condition="image">hh.exe</Image>
        </FileBlockExecutable>
    </RuleGroup>

    </EventFiltering>
</Sysmon>
```