PT005-Microsoft-Windows

Narrative and Use Case Center

Exported on Mar 1, 2017 11:20 AM

Table of Contents

The Microsoft windows operating system is the foundation of information systems in organizations of all sizes. The collection of TAs will allow for modular collection and analysis enabling value for IT workers in all job roles.

1 Key Facts

TA ID	Splunk Base URL	Sec TA URL
Splunk_TA_windows	OS Core https://splunkbase.splunk.com/app/742/	https://bitbucket.org/SPLServices/splunk_ta_windows
Load	Implementation Skill	Onboard Via
LOAD-High	SKILLI-PS-General	DO-Splunk-UF-Local
ES/CIM	Data Sources	Limitations

CIM-Authentication
CIM-Change Analysis
CIM-Inventory
CIM-Network Sessions
CIM-Network Traffic
	• DS003Authentication Authentication occurs for
	  ○ User Authentication
	  ○ Computer Authentication
	• DS006UserActivity
	  ○ DS006UserActivity-ET03Create
	  ○ DS006UserActivity-ET04Update
	  ○ DS006UserActivity-ET05Delete
	• DS007AuditTrail
	  ○ DS007AuditTrail-ET01Clear
	  ○ DS007AuditTrail-ET02Alter
	  ○ DS007AuditTrail-ET03TimeSync
	• DS009EndPointIntel
	  ○ DS009EndPointIntel-ET01ObjectChange
	  ○ DS009EndPointIntel-ET01ProcessLaunch
	• DS010NetworkCommunication
	  ○ DS010NetworkCommunication-ET01Traffic
	  ○ DS010NetworkCommunication-ET02State
	• DS022Performance
	  ○ DS022Performance-ET01General
	• DS023CrashReporting
		The CIM and DS capability of the data source will vary by the events collected and the configuration of the system generating the events.

TA ID	Splunk Base URL	Sec TA URL
	○ DS023CrashReporting-ET01General • DS024ApplicationServer ○ DS024ApplicationServer-ET01General • DS025IPAddressAssignment	

2 Migration Cross Walk

Replacing	Has Support	Change to data provider
ArcSight Connector	Yes	Removal of legacy software
Q1 Connector		

3 Index Guidance

Utilized Indexes

- oswin
- oswinsec
- oswinscripts
- epav (SecKitBase)
- epintel (SecKitBase)
- netipam (SecKitBase)

Input Package	Input	Scope	SourceType	Index	Notes
Splunk_TA_windows_SecKit_0_all_inputs	WinEventLog://Security	All Windows Systems	wineventlog:security	oswinsec	Blacklist for common "noise" events provided
	WinHostMon://Computer WinHostMon://NetworkAdapter WinHostMon://OperatingSystem WinHostMon://Roles		winhostmon:*	oswinscripts	Seldom updated system information used for content clues by security investigators, asset inventory and IT Ops use cases
Splunk_TA_windows_SecKit_1_all_inputs	WinEventLog://Application	Windows Application Servers & endpoints	wineventlog:application	oswin	
	WinEventLog://System		wineventlog:system	oswin	

Input Package	Input	Scope	SourceType	Index	Notes
Splunk_TA_windows_SecKit_1_regmon_inputs	WinRegMon://*		winregmon:*	epintel	
	monitor://$WINDIR\WindowsUpdate.log		WindowsUpdateLog	oswinsec	
	WinHostMon://Process WinHostMon://Processor WinHostMon://Service WinHostMon://Disk WinHostMon://Driver		winhostmon:*		Seldom updated system information used for content clues by security investigators, asset inventory and IT Ops use cases
Splunk_TA_windows_SecKit_1_extendedlogs_inputs	WinEventLog://Microsoft-Windows-AppLocker/			epintel	Used by security and operational teams in endpoint support and ioc detection
	WinEventLog://Microsoft-Windows-WindowsUpdateClient			epintel	
	WinEventLog://Setup			epintel	
	WinEventLog://Microsoft-Windows-Windows Firewall With Advanced Security/Firewall]			epintel	
	WinEventLog://Microsoft-Windows-Application-Experience			epintel	

Input Package	Input	Scope	SourceType	Index	Notes
	WinEventLog://Microsoft-Windows-CodeIntegrity/			epintel	
	WinEventLog://Microsoft-Windows-Defender/Operational			epav	
	WinEventLog://Microsoft-Windows-NetworkProfile/Operational			epintel	
	Microsoft-Windows-Kernel-PnP/Device Configuration			epintel	
	Microsoft-Windows-PrintService/Operational			oswin	
Splunk_TA_windows_SecKit_2_dcadmon_inputs	admon://default		ActiveDirectory	appmsadmon	Deployed on 2 Directory Controllers per domain per data center
Splunk_TA_windows_SecKit_2_dcadmonsync_inputs	admon://default		ActiveDirectory	appmsadmon	Deployed on 1 Directory Controller per domain to load the baseline can be removed when complete
Splunk_TA_windows_SecKit_2_dhcp_inputs	monitor://$WINDIR\System32\DHCP		DhcpSrvLog	netipam	Deployed on any windows server with dhcp role

4 Deployment Guidance

ServerClass	App
seckit_all_2_os_windows_0	Splunk_TA_windows SA-ModularInput-PowerShell Splunk_TA_windows_SecKit_0_all_inputs
seckit_all_2_os_windows_1	Splunk_TA_windows_SecKit_1_all_inputs
seckit_all_2_os_windows_dc	Splunk_TA_windows_SecKit_1_all_inputs
seckit_all_2_os_windows_dns	Splunk_TA_windows_SecKit_1_all_inputs
seckit_all_2_os_windows_dhcp	Splunk_TA_windows_SecKit_2_dhcp_inputs
seckit_all_2_os_windows_dc_admon	Splunk_TA_windows_SecKit_2_dcadmon_inputs
seckit_all_2_os_windows_dc_admon_sync	Splunk_TA_windows_SecKit_2_dcadmonsync_inputs

5 Key Facts

- Impact to index/license
    - Based on log files
        - total size of change in oswin* indexes over 7 days
    - Day 0 Impact, Customers frequently have no or poor retention policy in place on the monitored files and very large windows event logs to support problem resolution when no central solution exists. This can result in a large historical load impacting or exceeding the license utilization for that day. If implementing over multiple days prepare with a license reset key.
- Work Estimates
    - Splunk Core Resource <4 hours
    - Change Control Process 3-4 hours (Possibly require multiple iterations)
    - Meetings 1-2
- Opposition: Low
- Skills: SKILLI-Customer

6 Pre-implementation Requirements

Successful implementation as defined by collection of useful events from the source systems requires preparation work. In many cases the items required may be satisfied by prior security or compliance efforts. These key items should be verified to ensure logs are available for Splunk.

- Ensure the maximum size of all Windows Event Log files is no more than 300 MB. Per Microsoft guidance larger log file can permit conditions to occur where events will not be written to the file and consequently can not be monitored by Splunk. https://technet.microsoft.com/en-us/library/cc778402(v=ws.10).aspx
    - Verify a group policy is in place to enforce the limit absence of policy can permit the incorrect configuration by external means
- Ensure the maximum retain by days for monitored logs is configured to seven (7) for all fixed (desktops/servers) and 21 days for all mobile devices. This configuration will ensure a modest amount of historical data is collected limiting the impact of quarantined event indexing and initial bucket spans
    - Verify a group policy is in place to enforce the limit for the following event logs
        - Application
        - System
        - Security
- Ensure the monitored Windows Event Log retention method is configured to "Overwrite events as needed" this setting prevents a system generating a substantial number of events from encountering a log full condition which could cause the system to halt.
    - Verify a group policy is in place to enforce the limit for the following event logs
        - Application
        - System
        - Security
- Ensure DHCP server logging is enabled
    - Open the DHCP Microsoft Management Console (MMC) snap-in.
    - In the console tree, click the DHCP server you want to configure.
    - On the **Action** menu, click **Properties**.
    - On the **General** tab, select **Enable DHCP audit logging**, and then click **OK**.
- Ensure appropriate logging policy is in place for all windows systems the most common choice is to follow "Stronger" recommendations as prescribed in the following article. In some performance sensitive implementations tuning may be required. https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations
    - Ensure the policy has been in place for at lease 14 days prior to implementation of Splunk. This time window permits a clear delineation between the change of modification of audit policy and its effects prior to the implementation of the universal forwarder.
- Ensure Windows 7 and Windows 2008/R2 have Microsoft Patch KB3004375 applied and a group policy is in place for all Windows systems to ensure the following registry key is set
    - "hklm\software\microsoft\windows\currentversion\policies\system\audit" – Value = ProcessCreationIncludeCmdLine_Enabled - REG_DWORD = 1
- Ensure Powershell logging has been enabled and configured (Requires Powershell 5.0)

- Enable Module Logging
  - In the “Windows PowerShell” GPO settings, set “Turn on Module Logging” to enabled.
  - In the “Options” pane, click the button to show Module Name.
  - In the Module Names window, enter ***** to record all modules.
    - Optional: To log only specific modules, specify them here. (Note: this is not recommended.)
  - Click “OK” in the “Module Names” Window.
  - Click “OK” in the “Module Logging” Window.
- Enable Script Block Logging
  - In the “Windows PowerShell” GPO settings, set “Turn on PowerShell Script Block Logging” to enabled.

7 Data Acquisition Procedure Microsoft Windows XP/2008R2+

Data collection for security use case today requires collection via universal forwarder using windows event log classic format. Other options such as WMI, Snare and Windows Event Log XML are known to produce search results that are able to provide with expected values.

- Deployment Server Role "SRV"
    - Stage the following apps to deployment-apps
        - Splunk_TA_windows
        - Index app SecKit_splunk_index_2_win_*
        - Splunk_TA_windows_SecKit_0_all_inputs
        - Splunk_TA_windows_SecKit_1_all_inputs
        - Splunk_TA_windows_SecKit_2_dcadmon_inputs
        - Splunk_TA_windows_SecKit_2_dcadmonsync_inputs
        - Splunk_TA_windows_SecKit_2_dhcp_inputs
        - Splunk_TA_windows_SecKit_1_regmon_inputs
        - Splunk_TA_windows_SecKit_1_extendedlogs_inputs
    - Update SecKit_all_deploymentserver_2_oswin/local/serverclass.conf define the whitelist.0 to capture all hosts where more complete logging should be applied. In most cases this should apply to all servers.

```
[serverClass:seckit_all_2_os_windows_1]
whitelist.0 = ^-
```

    - Update SecKit_all_deploymentserver_2_oswin/local/serverclass.conf define the whitelist.0 to capture host naming standards for Active Directory servers

```
[serverClass:seckit_all_2_os_windows_dc]
whitelist.0 = ^-
```

-
    - Update SecKit_all_deploymentserver_2_oswin/local/serverclass.conf define whitelist.0 to include exactly one Active Directory server per domain

```
[serverClass:seckit_all_2_os_windows_dc_admon_sync]
whitelist.0 = ^-
```

    - Wait until "sync" events are no longer streaming into index=appmsad expect on 30-90 min
    - Replace SecKit_all_deploymentserver_2_oswin/local/serverclass.conf entry above as follows including 2-6 Active Directory servers per domain

```
[serverClass:seckit_all_2_os_windows_dc_admon]
machineTypesFilter = windows-*
whitelist.0 = ^-
```

- Deployment Server Role "WRK"
  - Stage the following apps to deployment-apps
    - Splunk_TA_windows
    - Index app SecKit_splunk_index_2_win_*
    - Splunk_TA_windows_SecKit_0_all_inputs
    - Splunk_TA_windows_SecKit_1_all_inputs
    - Splunk_TA_windows_SecKit_1_regmon_inputs
    - Splunk_TA_windows_SecKit_1_extendedlogs_inputs
  - Update SecKit_all_deploymentserver_2_oswin/local/serverclass.conf define the whitelist.0 so that all machines connected to this DS will utilize enhanced logging

```
[serverClass:seckit_all_2_os_windows_1]
whitelist.0 = *
```

8 PT005-Microsoft-Windows-ActiveDirectory

The Microsoft windows operating system is the foundation of information systems in organizations of all sizes. The collection of TAs will allow for modular collection and analysis enabling value for IT workers in all job roles.

8.1 Key Facts

TA ID	Splunk Base URL	Sec TA URL
Splunk_TA_microsoft_activedirectory	Windows Active Directory https://splunkbase.splunk.com/app/3207/	https://bitbucket.org/SPLServices/splunk_ta_microsoft_ad
Load	Implementation Skill	Onboard Via
LOAD-High	SKILLI-PS-General	DO-Splunk-UF-Local
ES/CIM	Data Sources	
None	• DS022Performance ○ DS022Performance-ET01General	

8.2 Migration Cross Walk

Replacing	Has Support	Change to data provider
ArcSight Connector	Yes	Removal of legacy software
Q1 Connector		

8.3 Index Guidance

Utilized Indexes

- appmsad
- appmsadmon (Windows Base Config)
- oswinperf (Windows Base Config)

Input Package	Input	Scope	Source Type	Index	Notes
Splunk_TA_microsoft_ad_SecKit_0_all_inputs	WinEventLog://DFS Replication	All Windows DCs		appmsad	Blacklist for common "noise"

Input Package	Input	Scope	Source Type	Index	Notes
					events provided
	WinEventLog://Directory Service			appmsad	
	WinEventLog://File Replication Service			appmsad	
	WinEventLog://Key Management Service			appmsad	
	script://.\bin\runpowershell.cmd nt6-repl-stat.ps1			appmsad	
	powershell://Replication-Stats] script = & "$SplunkHome\etc\apps\Splunk_TA_microsoft_ad\bin\Invoke-MonitoredScript.ps1" -Command ".\powershell\2012r2-repl-stats.ps1			appmsad	
	script://.\bin\runpowershell.cmd nt6-health.ps1			appmsad	
	powershell://AD-Health] script = & "$SplunkHome\etc\apps\Splunk_TA_microsoft_ad\bin\Invoke-MonitoredScript.ps1" -Command ".\powershell\2012r2-health.ps1			appmsad	
	script://.\bin\runpowershell.cmd nt6-siteinfo.ps1			appmsad	
	powershell://Siteinfo			appmsad	
	perfmon			oswinperf	
	monitor://C:\Windows\debug\netlogon.log			appmsad	

8.4 Key Facts

- Impact to index/license
  - variable
- Work Estimates
  - Splunk Core Resource <4 hours
  - Change Control Process 3-4 hours (Possibly require multiple iterations)
  - Meetings 1-2

- Opposition: Low
- Skills: SKILLI-Customer

8.5 Pre-implementation

- Deploy Supporting Addon for PowerShell https://splunkbase.splunk.com/app/1477/ by staging the app in deployment-apps
- Complete deployment for Windows Base PT005-Microsoft-Windows

8.6 Data Acquisition Procedure Microsoft 2008R2+

Data collection for operational use cases including Windows Infra Structure App and general active directory functional monitoring

- Deployment Servers
    - Stage the following apps to deployment-apps
        - Splunk_TA_microsoft_ad
        - Splunk_TA_microsoft_ad_SecKit_0_all_inputs
    - Reload Deployment Server

8.7 Post Implementation

Post Implementation continue to the following

- PT002-Splunk-Stream-DHCP
- PT002-Splunk-Stream-DNS

9 PT005-Microsoft-Windows-DNS

The Microsoft windows operating system is the foundation of information systems in organizations of all sizes. The collection of TAs will allow for modular collection and analysis enabling value for IT workers in all job roles.

9.1 Key Facts

TA ID	Splunk Base URL	Sec TA URL
Splunk_TA_microsoft_dns	Windows Active Directory https://splunkbase.splunk.com/app/3208/	https://bitbucket.org/SPLServices/splunk_ta_microsoft_dns
Load	Implementation Skill	Onboard Via
LOAD-Low	SKILLI-PS-General	DO-Splunk-UF-Local
ES/CIM	Data Sources	
None	• DS022Performance ○ DS022Performance-ET01General	

9.2 Migration Cross Walk

Replacing	Has Support	Change to data provider
ArcSight Connector	Yes	Removal of legacy software
Q1 Connector		

9.3 Index Guidance

Utilized Indexes

- appmsadmon (Windows Base Config)
- oswinperf (Windows Base Config)
- appmsad

Input Package	Input	Scope	Source Type	Index	Notes
Splunk_TA_microsoft_dns_SecKit_0_all_inputs	perfmon	All DNS Server	perfmon	oswinperf	
	WinEventLog://DNS Server			appmsad	

Input Package	Input	Scope	Source Type	Index	Notes
	MonitorNoHandle://C:\Windows\System32\Dns\dns.log				
	script://.\bin\runpowershell.cmd dns-zoneinfo.ps1				
	script://.\bin\runpowershell.cmd dns-health.ps1				

9.4 Key Facts

- Impact to index/license
  - variable
- Work Estimates
  - Splunk Core Resource <4 hours
  - Change Control Process 3-4 hours (Possibly require multiple iterations)
  - Meetings 1-2
- Opposition: Low
- Skills: SKILLI-Customer

9.5 Pre-implementation

- Complete deployment for Windows Base PT005-Microsoft-Windows

9.6 Data Acquisition Procedure Microsoft 2008R2+

Data collection for operational use cases including Windows Infra Structure App and general active directory functional monitoring

- Deployment Servers
  - Stage the following apps to deployment-apps
    - Splunk_TA_microsoft_dns
    - Splunk_TA_microsoft_dns_SecKit_0_all_inputs
  - Reload Deployment Server

10 PT005-Microsoft-Windows-IIS

The Microsoft windows operating system is the foundation of information systems in organizations of all sizes. This collection extension expands the base log collection for IIS hosted applications.

10.1 Key Facts

TA ID	Splunk Base URL	Sec TA URL
Splunk_TA_microsoft_iis	https://splunkbase.splunk.com/app/3185/	https://bitbucket.org/SPLServices/splunk_ta_microsoft-iis
Load	Implementation Skill	Onboard Via
LOAD-Low	SKILLI-PS-General	DO-Splunk-UF-Local
ES/CIM	Data Sources	

CIM-Authentication
CIM-Network Traffic
CIM-Web
	• DS003Authentication Authentication occurs for
	  ○ User Authentication
	  ○ Computer Authentication
	• DS006UserActivity
	  ○ DS006UserActivity-ET03Create
	  ○ DS006UserActivity-ET04Update
	  ○ DS006UserActivity-ET05Delete
	• DS014WebServer
	  ○ DS014WebServer-ET01Access
	• DS022Performance
	  ○ DS022Performance-ET01General	

10.2 Migration Cross Walk

Replacing	Has Support	Change to data provider
ArcSight Connector	Yes	Removal of legacy software
Q1 Connector		

10.3 Key Facts

- Impact to index/license
  - Based on log files
    - total size of change in oswin* indexes over 7 days
  - Day 0 Impact, Customers frequently have no or poor retention policy in place on the monitored files and very large windows event logs to support problem resolution when no central solution exists. This can result in a large historical load impacting or exceeding the license utilization for that day. If implementing over multiple days prepare with a license reset key.
- Work Estimates
  - Splunk Core Resource <4 hours
  - Change Control Process 3-4 hours (Possibly require multiple iterations)
  - Meetings 1-2
- Opposition: Low
- Skills: SKILLI-Customer

10.4 Pre-Implementation

- Clean old log information from all servers and ensure retention on server of know more than 7 days. The method of cleanup is at the customer discretion common choices are
  - Customer developed script/service
  - PowerShell Script - https://gallery.technet.microsoft.com/scriptcenter/Delete-andor-Archive-IIS-e9ccd0cb
  - VBScript "Housekeeping script, automatic log locations, logs are just deleted:" - http://www.808.dk/?code-iis-log-housekeeping

```
Option Explicit
WScript.Timeout = 82800

' This Script deletes IIS log files older than a
specified number
' of days.
'
' Run it as a daily scheduled task on high traffic web
servers to
' avoid running out of disc space.
'
' Edit the value for intDelAge to set retention times
needed on
' the server.
'
' The locations of the IIS log files are found
automatically (for this
' to also work on IIS 7.x on Windows Vista, Windows
Server 2008 or
' Windows 7, please enable "IIS 6 Metabase
Compatibility" aka
' "IIS Metabase and IIS 6 configuration
compatibility").

Dim intDelAge
intDelAge = 30
```

```
Dim objIIS
Dim objWeb
Dim objIISOuter
Dim objWebOuter
Set objIISOuter = GetObject("IIS://LOCALHOST")
For Each objWebOuter in objIISOuter
  If LCase(objWebOuter.Class) = "iiswebservice" Then
    Set objIIS = GetObject("IIS://LOCALHOST/W3SVC")
    For Each objWeb in objIIS
      If LCase(objWeb.Class) = "iiswebserver" Then
        Call DeleteLogFiles( _
          objWeb.LogFileDirectory & "\W3SVC" &
objWeb.Name, _
          intDelAge)
      End If
    Next
  ElseIf LCase(objWebOuter.Class) = "iissmtpservice"
Then
    Set objIIS = GetObject("IIS://LOCALHOST/SMTPSVC")
    For Each objWeb in objIIS
      If LCase(objWeb.Class) = "iissmtpserver" Then
        Call DeleteLogFiles( _
          objWeb.LogFileDirectory & "\SMTPSVC" &
objWeb.Name, _
          intDelAge)
      End If
    Next
  ElseIf LCase(objWebOuter.Class) = "iisftpservice"
Then
    Set objIIS = GetObject("IIS://LOCALHOST/MSFTPSVC")
    For Each objWeb in objIIS
      If LCase(objWeb.Class) = "iisftpserver" Then
        Call DeleteLogFiles( _
          objWeb.LogFileDirectory & "\MSFTPSVC" &
objWeb.Name, _
          intDelAge)
      End If
    Next
  End If
Next

Set objIIS = nothing
Set objIISOuter = nothing

Function DeleteLogFiles(strLogPath, intDelAge)
  Dim objFs
  Dim objFolder
  Dim objSubFolder
  Dim objFile
  Dim objWShell
  Set objWShell = CreateObject("WScript.Shell")
  Set objFs =
CreateObject("Scripting.FileSystemObject")
  If Right(strLogPath, 1) <> "\" Then
    strLogPath = strLogPath & "\"
  End If
  If objFs.FolderExists(strLogPath) Then
    Set objFolder = objFs.GetFolder(strLogPath)
      For Each objSubFolder in objFolder.subFolders
        DeleteLogFiles strLogPath & objSubFolder.Name,
intDelAge
      Next
      For Each objFile in objFolder.Files
        If (InStr(objFile.Name, "ex") > 0) _
          And (Right(objFile.Name, 4) = ".log") Then
          If
```

```
            DateDiff("d",objFile.DateLastModified,Date) >
            intDelAge Then
                        objFs.DeleteFile(strLogPath &
            objFile.Name)
                      End If
                    End If
                  Next
                Set objFs = Nothing
                Set objFolder = Nothing
                Set objWShell = nothing
              End If
            End Function
```

- Ensure the IIS log configuration has been updated to include at least the following information

```
Date, Time, ClientIP, UserName, SiteName, Host, ComputerName,
ServerIP, Method, UriStem, UriQuery, HttpStatus, TimeTaken,
Win32Status, ServerPort, UserAgent, HttpSubStatus, BytesSent,
BytesRecv, TimeTaken, Referer
```

- If an external load balancer is providing x-forward* information review the following article and ensure X-FORWARDED-FOR is assigned to ClientIP
    - http://www.loadbalancer.org/blog/iis-and-x-forwarded-for-header

10.5 Data Acquisition Procedure Microsoft 2008R2+

The following deployment methodology will collect all data into indexes for internal and external IIS instances, best practice is to define the index based on the application or related group of applications allowing for application of appropriate access controls. Starting with this configuration is often appropriate while being aware there will be a need to refine the configuration at some appropriate time in the future.

- Deployment Servers
    - Stage the following apps to deployment-apps
        - Splunk_TA_microsoft-iis
        - Splunk_TA_microsoft-iis_seckit_0_auto_inputs
        - Splunk_TA_microsoft-iis_seckit_0_default_inputs
        - Splunk_TA_microsoft-iis_seckit_1_autoext_inputs
        - Splunk_TA_microsoft-iis_seckit_1_defaultext_inputs

- Update SecKit_all_deploymentserver_3_iis/local/serverclass.conf define the whitelist.0 to capture hosts with the IIS role servicing internal clients

```
[serverClass:seckit_all_3_os_windows_0_iisauto]
whitelist.0 = ^-
```

- Update SecKit_all_deploymentserver_3_iis/local/serverclass.conf define the whitelist.0 to capture hosts with the IIS role servicing external clients

```
[serverClass:seckit_all_3_os_windows_1_iisauto_ext]
whitelist.0 = ^-
```

11 PT005-Microsoft-Windows-Sysmon

The microsoft additional tool sysmon generates additional detailed information for process execution and communication often utilized for discovery of endpoint malware

11.1 Key Facts

TA ID	Splunk Base URL	Sec TA URL
TA-microsoft-sysmon	https://splunkbase.splunk.com/app/1914/	https://bitbucket.org/SPLServices/ta-microsoft-sysmon
Load	Implementation Skill	Onboard Via
LOAD-Moderate	SKILLI-PS-General	DO-Splunk-UF-Local
ES/CIM	Data Sources	

None	• DS009EndPointIntel
	  ○ DS009EndPointIntel-ET01ProcessLaunch
	• DS010NetworkCommunication
	  ○ DS010NetworkCommunication-ET01Traffic	

11.2 Migration Cross Walk

Replacing	Has Support	Change to data provider
ArcSight Connector	Yes	Removal of legacy software
Q1 Connector		

11.3 Index Guidance

Utilized Indexes

- epintel

Input Package	Input	Scope	SourceType	Index	Notes
TA-microsoft-sysmon_seckit_0_all_inputs	WinEventLog://Microsoft-Windows-Sysmon/Operational	All endpoints and session hosts		epintel	

11.4 Key Facts

- Impact to index/license
  - variable
- Work Estimates
  - Splunk Core Resource <4 hours
  - Change Control Process 3-4 hours (Possibly require multiple iterations)
  - Meetings 1-2
- Opposition: Low
- Skills: SKILLI-Customer

11.5 Pre-implementation

- Complete deployment for Windows Base PT005-Microsoft-Windows
- Deploy Microsoft sysmon 5.x (refrain from latest) to all endpoints and servers using the customers internally approved tools and methods. If established patterns do not exist review the following article for guidance
  - https://p0w3rsh3ll.wordpress.com/2015/04/21/deploy-sysmon-with-powershell-desired-state-configuration/
- Use the following XML as the baseline configuration for sysmon customize as required to excluded high volume sources

```
<Sysmon schemaversion="3.1">
  <HashAlgorithms>SHA1</HashAlgorithms>
  <EventFiltering>
    <!-- Log all drivers except if the signature -->
    <!-- contains Microsoft or Windows -->
 <DriverLoad onmatch="exclude">
    <Signature condition="contains">microsoft</Signature>
    <Signature condition="contains">windows</Signature>
 </DriverLoad>
      <!-- Exclude certain processes that cause high event volumes -->
    <ProcessCreate onmatch="exclude">
    <Image condition="contains">splunk</Image>
        <Image condition="contains">streamfwd</Image>
        <Image condition="contains">splunkd</Image>
    <Image condition="contains">splunkD</Image>
    <Image condition="contains">splunk</Image>
    <Image condition="contains">splunk-optimize</Image>
    <Image condition="contains">splunk-MonitorNoHandle</Image>
    <Image condition="contains">splunk-admon</Image>
    <Image condition="contains">splunk-netmon</Image>
    <Image condition="contains">splunk-regmon</Image>
    <Image condition="contains">splunk-winprintmon</Image>
    <Image condition="contains">btool</Image>
    <Image condition="contains">PYTHON</Image>
 </ProcessCreate>
 <ProcessTerminate onmatch="exclude">
    <Image condition="contains">splunk</Image>
    <Image condition="contains">streamfwd</Image>
    <Image condition="contains">splunkd</Image>
    <Image condition="contains">splunkD</Image>
    <Image condition="contains">splunk</Image>
    <Image condition="contains">splunk-optimize</Image>
    <Image condition="contains">splunk-MonitorNoHandle</Image>
```

```
    <Image condition="contains">splunk-admon</Image>
    <Image condition="contains">splunk-netmon</Image>
    <Image condition="contains">splunk-regmon</Image>
    <Image condition="contains">splunk-winprintmon</Image>
    <Image condition="contains">btool</Image>
    <Image condition="contains">PYTHON</Image>
  </ProcessTerminate>
  <FileCreateTime onmatch="exclude">
    <Image condition="contains">splunk</Image>
    <Image condition="contains">streamfwd</Image>
    <Image condition="contains">splunkd</Image>
    <Image condition="contains">splunkD</Image>
    <Image condition="contains">splunk</Image>
    <Image condition="contains">splunk-optimize</Image>
    <Image condition="contains">splunk-MonitorNoHandle</Image>
    <Image condition="contains">splunk-admon</Image>
    <Image condition="contains">splunk-netmon</Image>
    <Image condition="contains">splunk-regmon</Image>
    <Image condition="contains">splunk-winprintmon</Image>
    <Image condition="contains">btool</Image>
    <Image condition="contains">PYTHON</Image>
    <Image condition="contains">sysmon</Image>
      </FileCreateTime>
  <ImageLoad onmatch="exclude">
    <Image condition="contains">splunk</Image>
    <Image condition="contains">streamfwd</Image>
    <Image condition="contains">splunkd</Image>
    <Image condition="contains">splunkD</Image>
    <Image condition="contains">splunk</Image>
    <Image condition="contains">splunk-optimize</Image>
    <Image condition="contains">splunk-MonitorNoHandle</Image>
    <Image condition="contains">splunk-admon</Image>
    <Image condition="contains">splunk-netmon</Image>
    <Image condition="contains">splunk-regmon</Image>
    <Image condition="contains">splunk-winprintmon</Image>
    <Image condition="contains">btool</Image>
    <Image condition="contains">PYTHON</Image>
    <Image condition="contains">sysmon</Image>
  </ImageLoad>
    </EventFiltering>
</Sysmon>
```

11.6 Data Acquisition Procedure Microsoft Windows 7/2008R2 +

Data collection for operational use cases including Windows Infra Structure App and general active directory functional monitoring

- Deployment Servers
    - Deploy to apps SecKit_all_deploymentserver_3_ms_sysmon
    - Stage the following apps to deployment-apps
        - TA-microsoft-sysmon
        - TA-microsoft-sysmon_seckit_0_all_inputs
    - Reload Deployment Server