Trend Micro Portable Security^{TM} 3

SIEM (Security information and event management) tool for Site Administrator

User Guide

April 14, 2021

Document Version 1.17

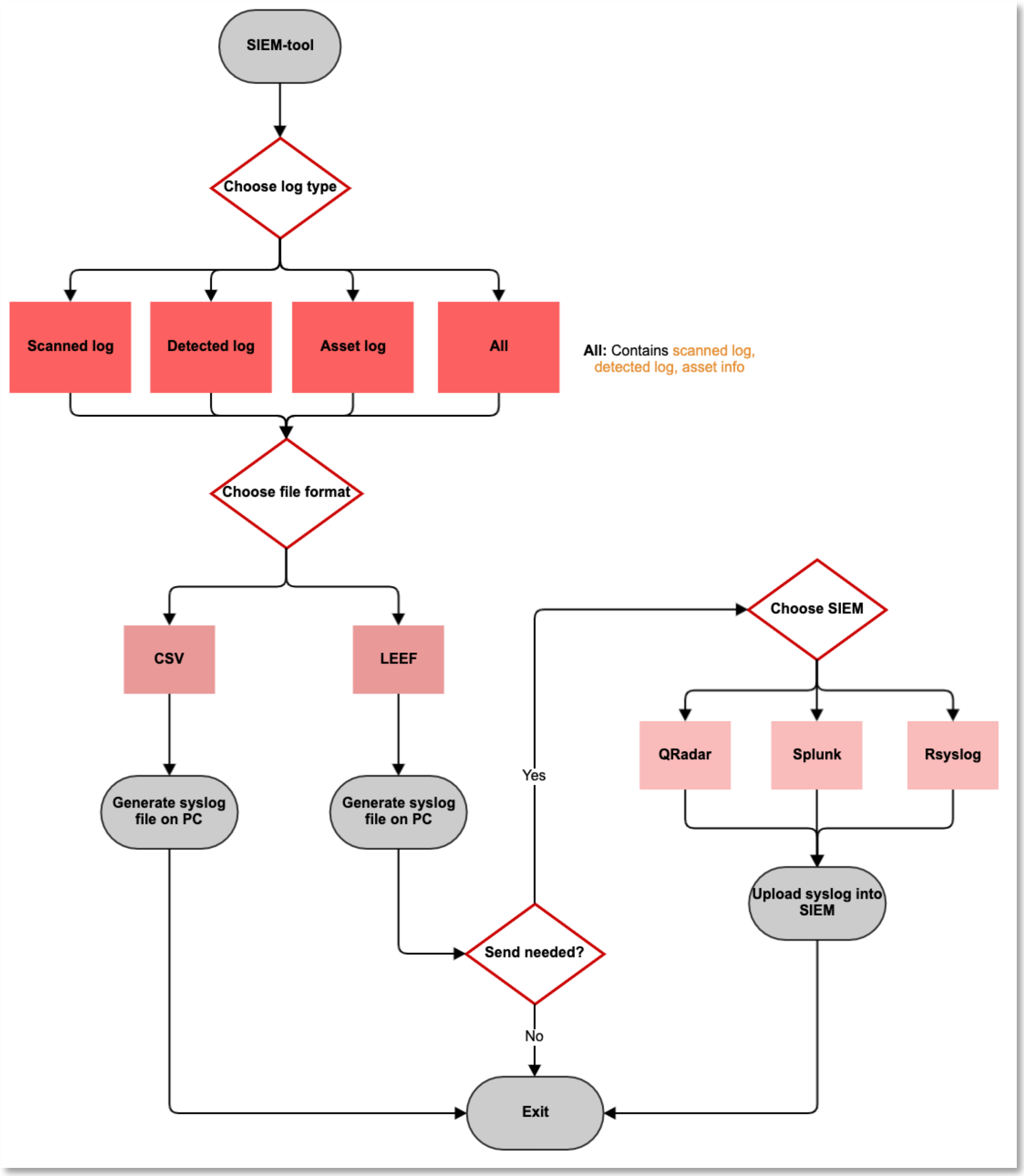
Table of Contents

1. Overview

Deliverable

- SIEM Tool package (SIEM-tool.zip)

Flow chart of SIEM tool



2. About SIEM Tool

1. The SIEM tool is designed as a command line interface and allows the operator to query **logs** to an SIEM server from machines which have Management Program installed.
2. Definition of **logs**: contains "scanned log", "detected log", and "asset info".

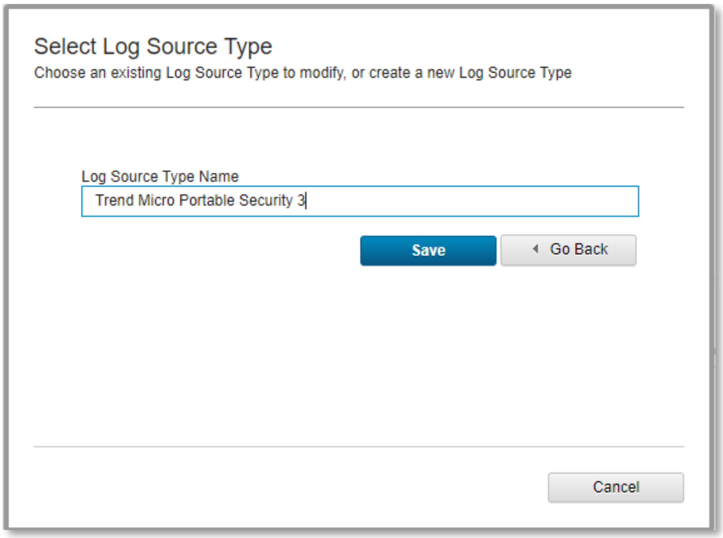
   User can choose one or all of them to export/send.

   - **scanned log**: scanned endpoints list with all scan results including threats detected, no threats found, scan cancelled, and other kinds of results.
   - **detected log**: scanned endpoints list with a result of “threat detected” only. Every detection will be one column the log file. It does not store non-detected results.
   - **asset info**: scanned endpoints list with asset information, including three files:
     - asset info - system and hardware information
     - application info – list of installed applications
     - update info - update information (Microsoft applications only)

3. Prerequisite - Configuration in SIEM Server

Settings in QRadar

1. Create Log Source Type:
    a. Click 'Admin' -> 'DSM Editor' and click 'Create New' in the “Select Log Source Type” window
    b. Provide a name for this **Log Source Type**

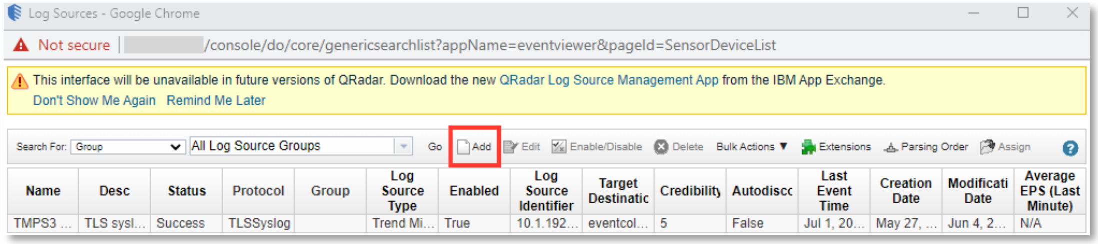


Select Log Source Type

Choose an existing Log Source Type to modify, or create a new Log Source Type

Log Source Type Name: Trend Micro Portable Security 3

2. Create Log Source:
    a. Click ‘Admin’ -> ‘Log Sources’ and click ‘Add’ in Log Sources window



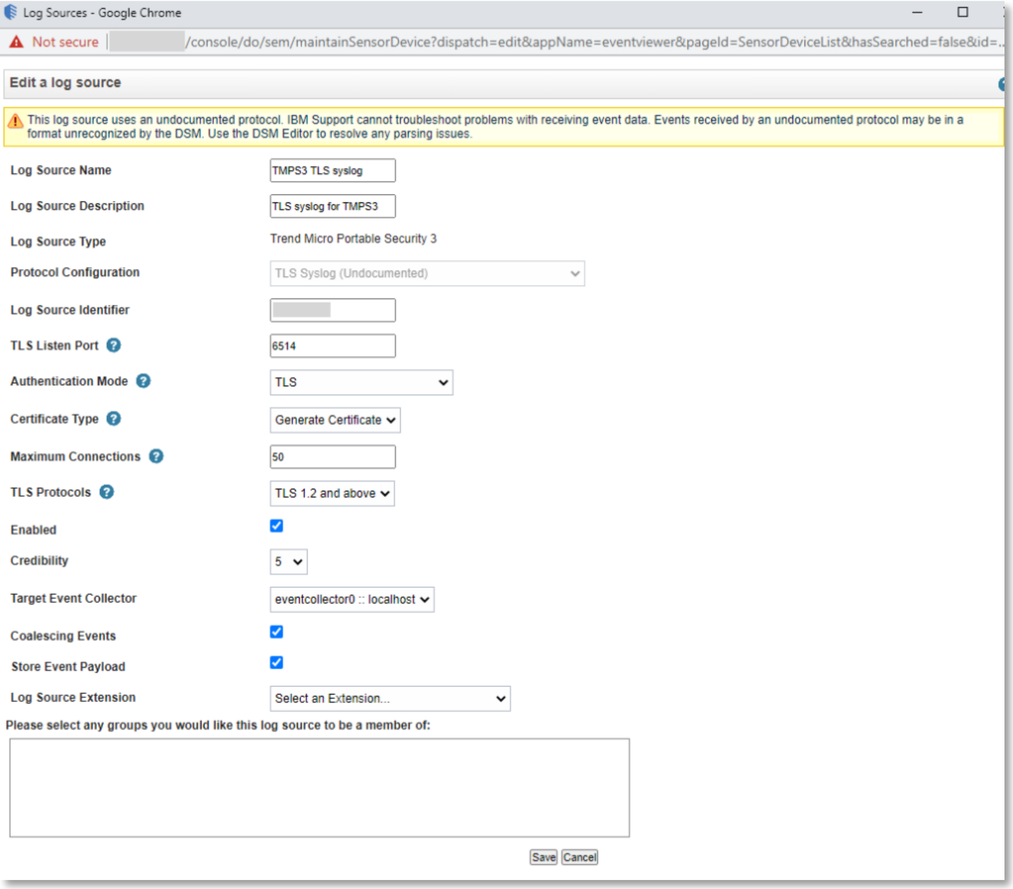
Log Sources - Google Chrome

Not secure | [redacted]/console/do/core/genericsearchlist?appName=eventviewer&pageId=SensorDeviceList

This interface will be unavailable in future versions of QRadar. Download the new QRadar Log Source Management App from the IBM App Exchange.

Name	Desc	Status	Protocol	Group	Log Source Type	Enabled	Log Source Identifier	Target Destinatic	Credibility	Autodiscc	Last Event Time	Creation Date	Modificati Date	Average EPS (Last Minute)
TMPS3 ...	TLS sysl...	Success	TLSSyslog		Trend Mi...	True	10.1.192...	eventcol...	5	False	Jul 1, 20...	May 27, ...	Jun 4, 2...	N/A

    b. Fill in the IP address of the machine on which Management Program is installed in **Log Source Identifier** as well as other related information.



Log Sources - Google Chrome

Not secure | [redacted]/console/do/sem/maintainSensorDevice?dispatch=edit&appName=eventviewer&pageId=SensorDeviceList&hasSearched=false&id=...

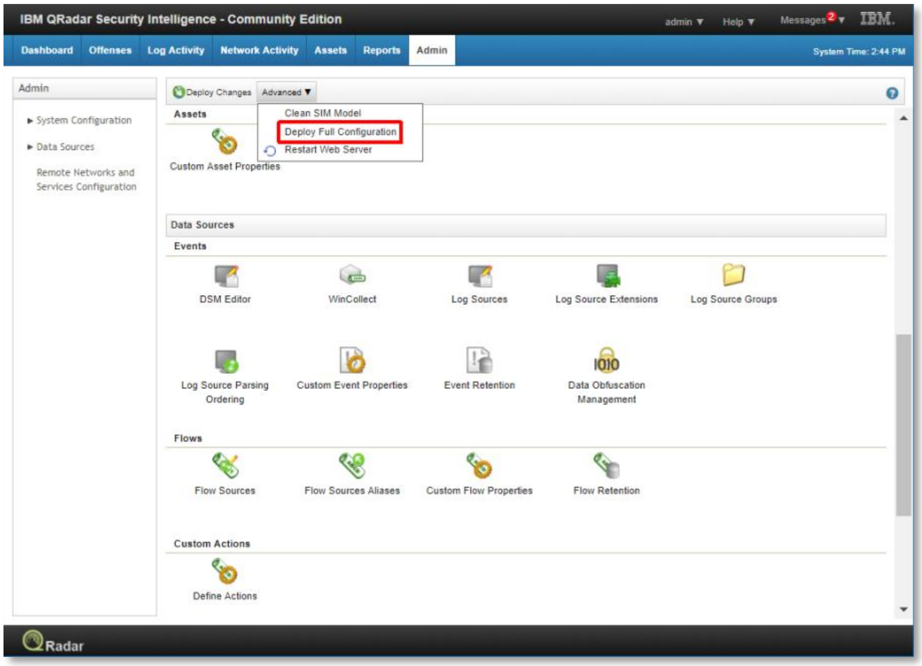
Edit a log source

This log source uses an undocumented protocol. IBM Support cannot troubleshoot problems with receiving event data. Events received by an undocumented protocol may be in a format unrecognized by the DSM. Use the DSM Editor to resolve any parsing issues.

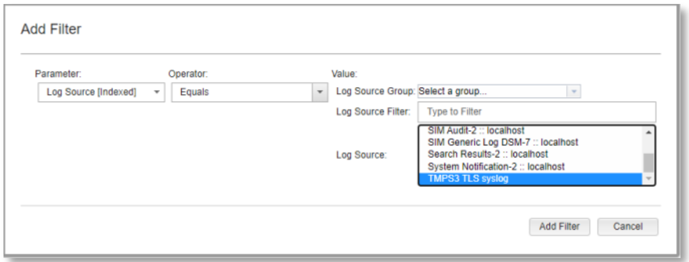
Log Source Name	TMPS3 TLS syslog
Log Source Description	TLS syslog for TMPS3
Log Source Type	Trend Micro Portable Security 3
Protocol Configuration	TLS Syslog (Undocumented)
Log Source Identifier	[redacted]
TLS Listen Port	6514
Authentication Mode	TLS
Certificate Type	Generate Certificate
Maximum Connections	50
TLS Protocols	TLS 1.2 and above
Enabled	☑
Credibility	5
Target Event Collector	eventcollector0 :: localhost
Coalescing Events	☑
Store Event Payload	☑
Log Source Extension	Select an Extension...

Please select any groups you would like this log source to be a member of:

c. After Save, go to the Admin tab and click 'Advanced' -> 'Deploy Full Configuration' to deploy the created log source.



3. Copy QRadar’s Certificate file to the SIEM tool
    a. To send a TLS-encrypted log, the client needs to have certificate file for the SIEM server.
    b. The certificate file for QRadar is located in /opt/qradar/conf/trusted_certificates
    c. Copy /opt/qradar/conf/trusted_certificates/syslog-tls.cert into the SIEM tool folder and make sure the file name is correct in the config.ini for SIEM tool.
4. Refer to the next section, [Preparation Procedure in SIEM tool]() and send logs to QRadar.
5. Back to in QRadar, open a log in DSM editor
    a. Click 'Log Activity'
    b. Click 'Add Filter' and select 'Log Source [Indexed]' as parameter and 'Equals' as operator, then select log source to see logs sent by SIEM tool.



Add Filter

Parameter: Log Source [Indexed]

Operator: Equals

Value:

Log Source Group: Select a group...

Log Source Filter: Type to Filter

Log Source: TMPS3 TLS syslog

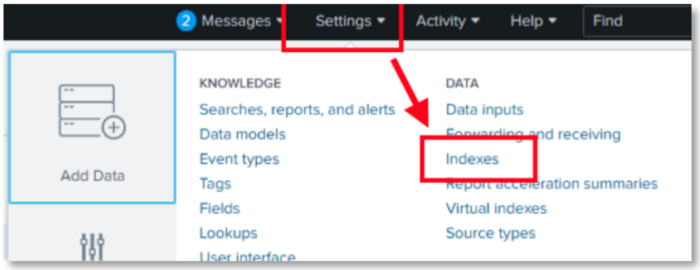
SIM Audit-2 :: localhost
SIM Generic Log DSM-7 :: localhost
Search Results-2 :: localhost
System Notification-2 :: localhost
TMPS3 TLS syslog
Add Filter
Cancel

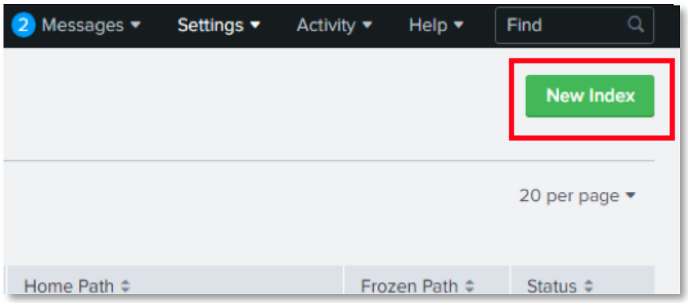
Settings in Splunk

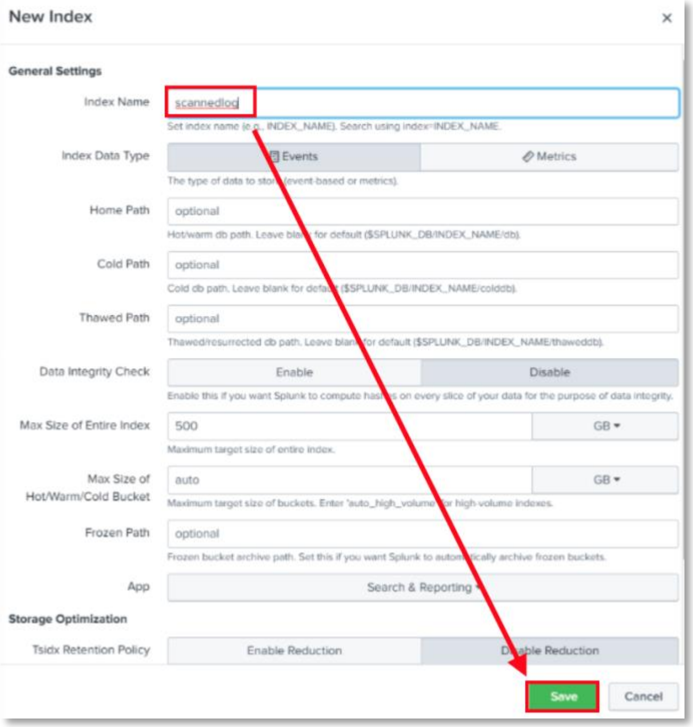
1. Add **New Index** for scanned logs, detected logs, and the three kinds of logs for asset info individually.

   NOTE: The naming of the index must be the same as the log name.

   Ex. scannedlog, detectedlog, assetinfo, applicationinfo and updateinfo







New Index ×

General Settings

Index Name: scannedlog
Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type: [✓ Events] Metrics
The type of data to store (event-based or metrics).

Home Path: optional
Hot/warm db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/db).

Cold Path: optional
Cold db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path: optional
Thawed/resurrected db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/thaweddb).

Data Integrity Check: Enable [✓ Disable]
Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Max Size of Entire Index: 500 GB
Maximum target size of entire index.

Max Size of Hot/Warm/Cold Bucket: auto GB
Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.

Frozen Path: optional
Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.

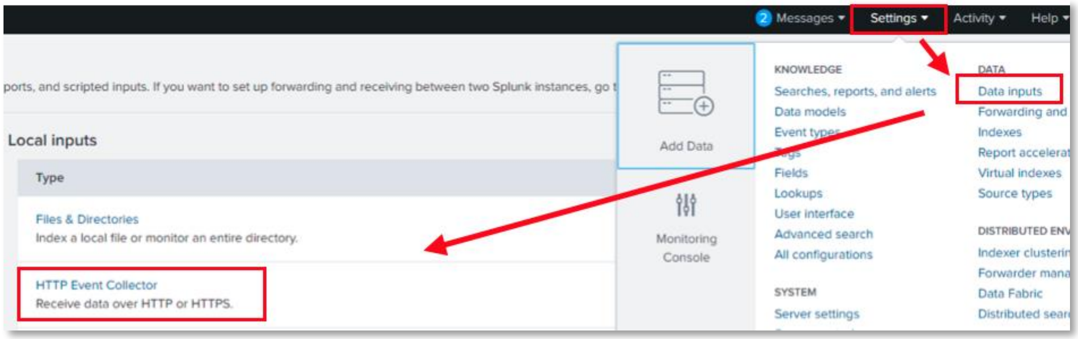
App: Search & Reporting

Storage Optimization

Tsidx Retention Policy: Enable Reduction [✓ Disable Reduction]

Save Cancel

2. Set up HTTP Event Collector following the step-by-step process shown below.



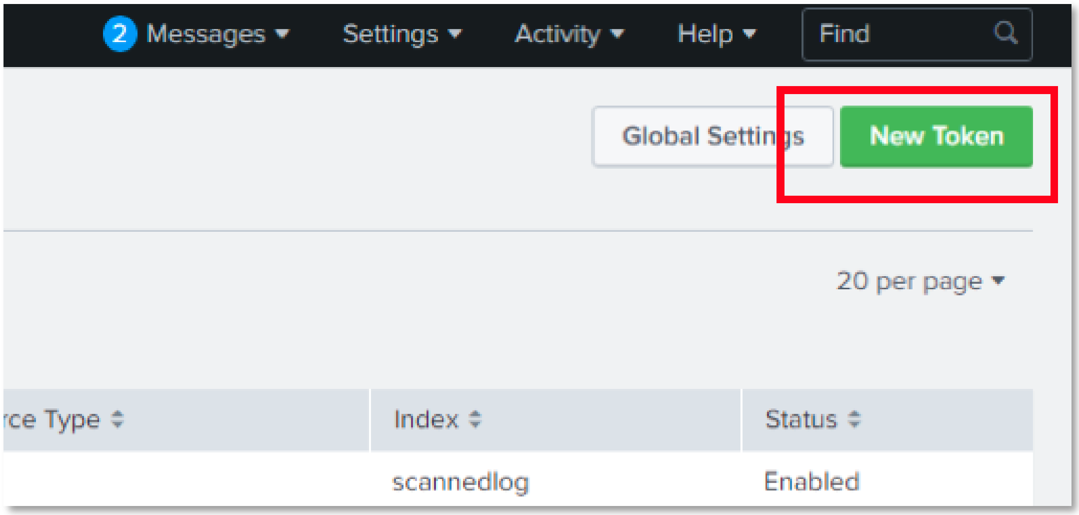
ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go t

Local inputs

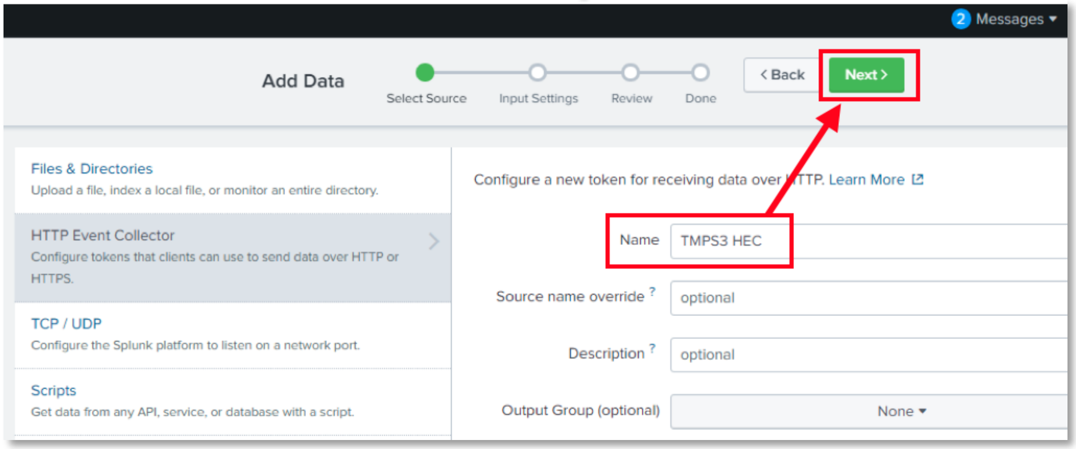
Type

Files & Directories
Index a local file or monitor an entire directory.

HTTP Event Collector
Receive data over HTTP or HTTPS.



ce Type ⇕	Index ⇕	Status ⇕
	scannedlog	Enabled



Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Scripts
Get data from any API, service, or database with a script.

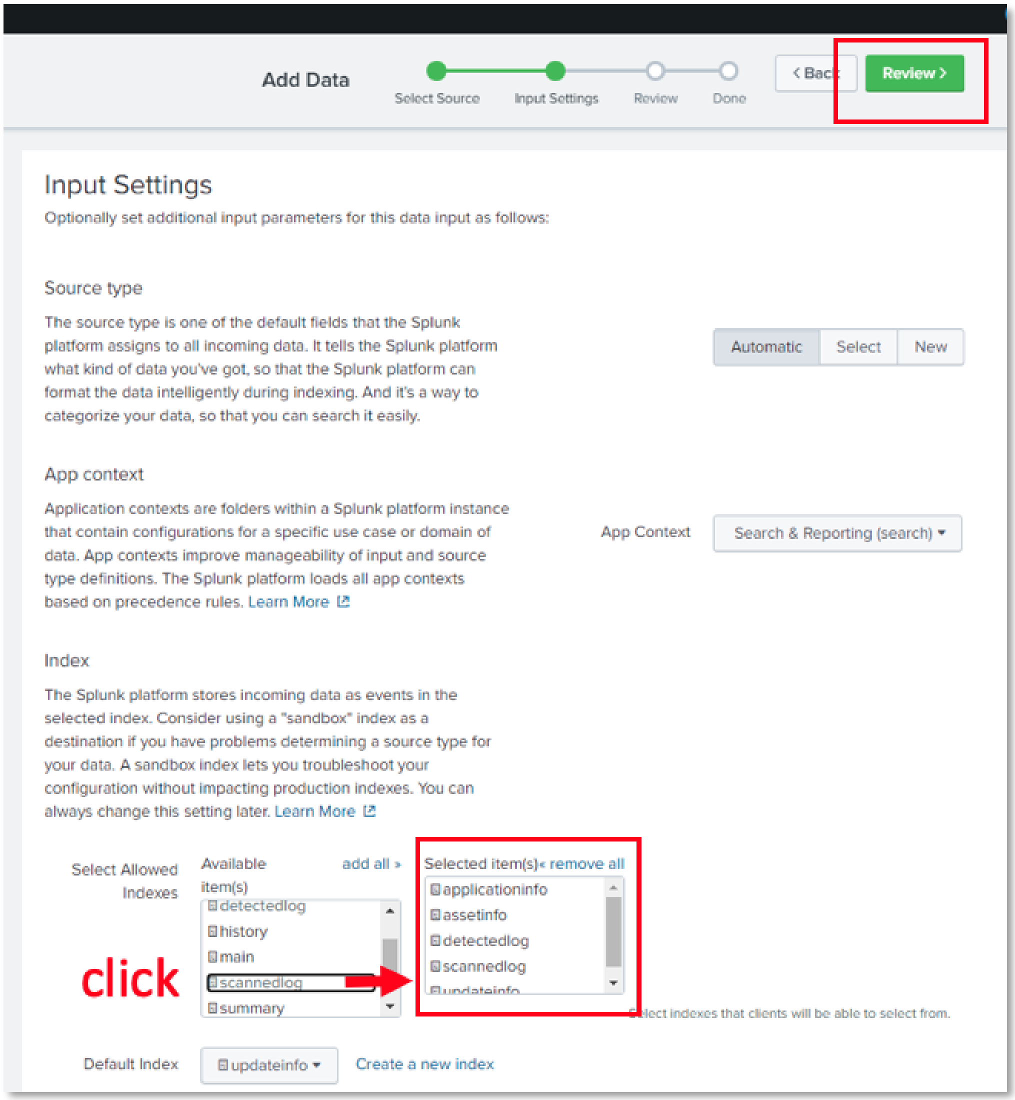
Configure a new token for receiving data over HTTP. Learn More

Name: TMPS3 HEC

Source name override ?: optional

Description ?: optional

Output Group (optional): None ▾



Input Settings

Optionally set additional input parameters for this data input as follows:

Source type

The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Automatic | Select | New

App context

Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. Learn More

App Context: Search & Reporting (search) ▾

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More

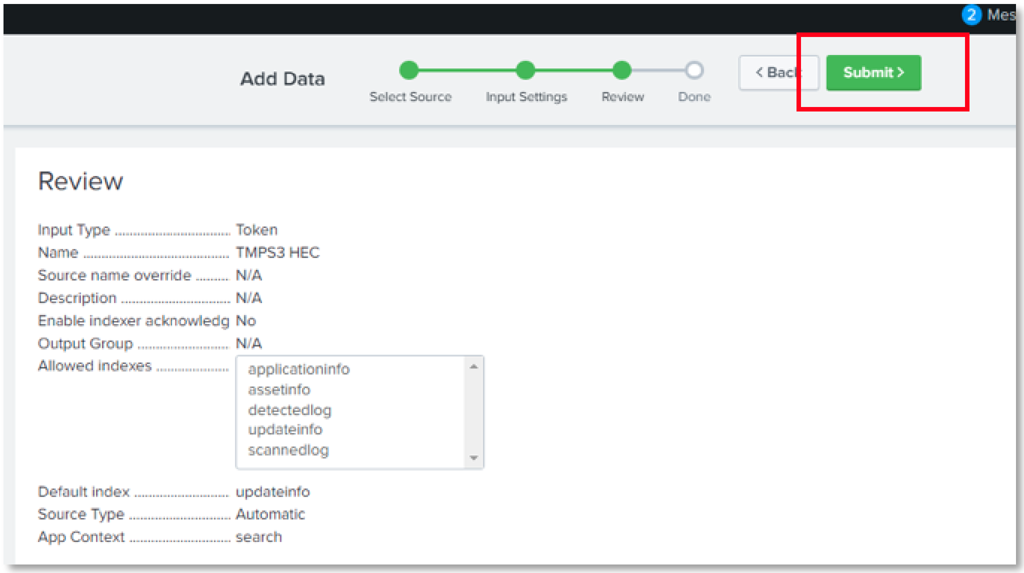
Select Allowed Indexes

Available item(s) — add all »
- detectedlog
- history
- main
- scannedlog
- summary

Selected item(s) « remove all
- applicationinfo
- assetinfo
- detectedlog
- scannedlog
- updateinfo

Select indexes that clients will be able to select from.

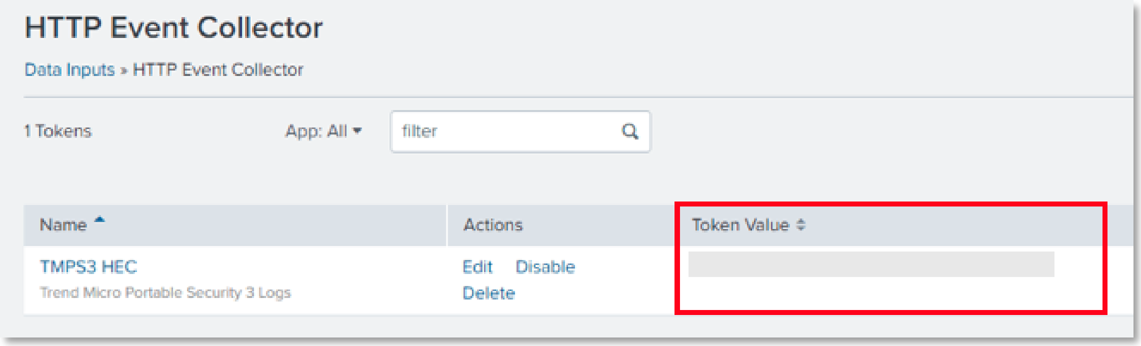
Default Index: updateinfo ▾ — Create a new index



Review

Input Type .... Token
Name .... TMPS3 HEC
Source name override .... N/A
Description .... N/A
Enable indexer acknowledg No
Output Group .... N/A
Allowed indexes .... applicationinfo
assetinfo
detectedlog
updateinfo
scannedlog
Default index .... updateinfo
Source Type .... Automatic
App Context .... search

3. Copy Token Value to config.ini file under the parameter ‘[Splunk] Token’.



HTTP Event Collector

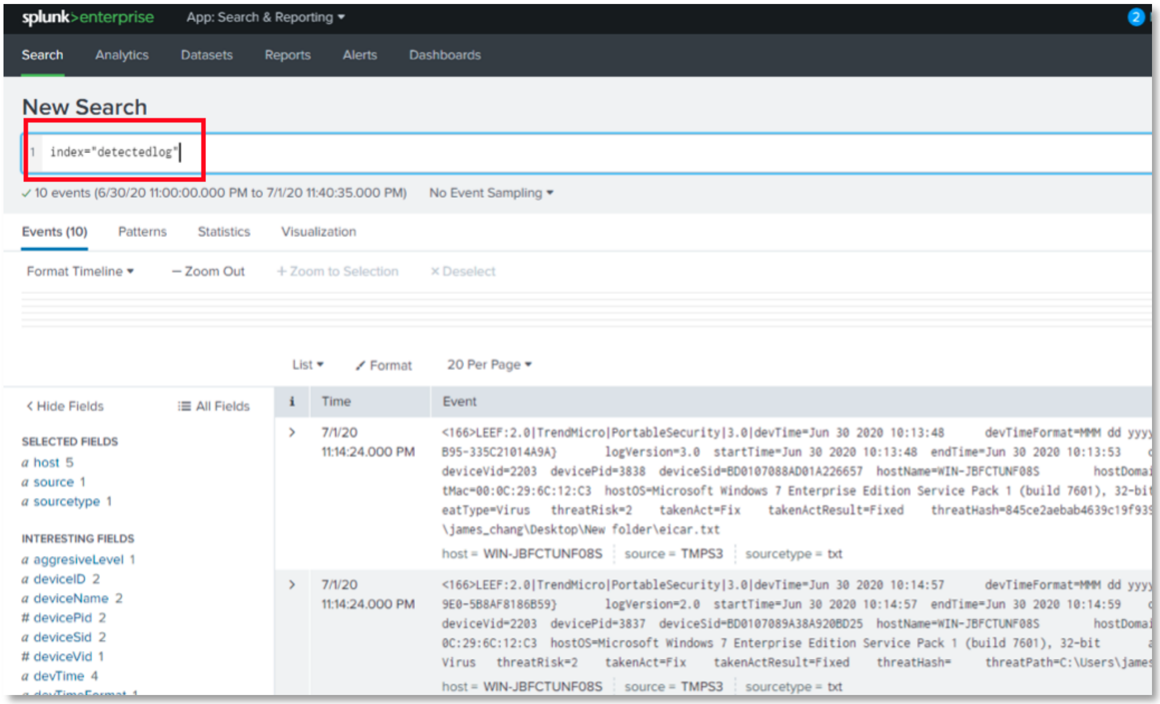
Data Inputs » HTTP Event Collector

1 Tokens   App: All ▾   filter

Name ▴	Actions	Token Value ⇕
TMPS3 HEC Trend Micro Portable Security 3 Logs	Edit Disable Delete	[redacted]

4. Refer to the next section, [Preparation Procedure in SIEM Tool]() and send logs to Splunk.

Back to Splunk, search indexes which have been created to see logs sent from SIEM Tool.



New Search

```
index="detectedlog"
```

✓ 10 events (6/30/20 11:00:00.000 PM to 7/1/20 11:40:35.000 PM)   No Event Sampling ▾

Events (10)

SELECTED FIELDS
a host 5
a source 1
a sourcetype 1

INTERESTING FIELDS
a aggresiveLevel 1
a deviceID 2
a deviceName 2
# devicePid 2
a deviceSid 2
# deviceVid 1
a devTime 4

i	Time	Event

>	7/1/20
	11:14:24.000 PM
		<166>LEEF:2.0|TrendMicro|PortableSecurity|3.0|devTime=Jun 30 2020 10:13:48 devTimeFormat=MMM dd yyyy
		B95-335C21014A9A} logVersion=3.0 startTime=Jun 30 2020 10:13:48 endTime=Jun 30 2020 10:13:53
		deviceVid=2203 devicePid=3838 deviceSid=BD0107088AD01A226657 hostName=WIN-JBFCTUNF08S hostDomai
		tMac=00:0C:29:6C:12:C3 hostOS=Microsoft Windows 7 Enterprise Edition Service Pack 1 (build 7601), 32-bit
		eatType=Virus threatRisk=2 takenAct=Fix takenActResult=Fixed threatHash=845ce2aebab4639c19f939
		\james_chang\Desktop\New folder\eicar.txt
		host = WIN-JBFCTUNF08S source = TMPS3 sourcetype = txt

>	7/1/20 11:14:24.000 PM	<166>LEEF:2.0|TrendMicro|PortableSecurity|3.0|devTime=Jun 30 2020 10:14:57 devTimeFormat=MMM dd yyyy 9E0-5B8AF8186B59} logVersion=2.0 startTime=Jun 30 2020 10:14:57 endTime=Jun 30 2020 10:14:59 deviceVid=2203 devicePid=3837 deviceSid=BD0107089A38A920BD25 hostName=WIN-JBFCTUNF08S hostDomai 0C:29:6C:12:C3 hostOS=Microsoft Windows 7 Enterprise Edition Service Pack 1 (build 7601), 32-bit Virus threatRisk=2 takenAct=Fix takenActResult=Fixed threatHash= threatPath=C:\Users\james host = WIN-JBFCTUNF08S source = TMPS3 sourcetype = txt

Settings in RSyslog

Related modifications can be listed in the RSyslog configuration to prevent some issues.

1. While configuring Syslog messages, if you want <Priority> information to be in every sent message:

   Instead of **$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat**,

   please use **$ActionFileDefaultTemplate RSYSLOG_SyslogProtocol23Format**

2. To prevent garbled data:

   Please set **$EscapeControlCharactersOnReceive off**

After modifying the above settings in **/etc/rsyslog.conf**, please restart **rsyslogd**.

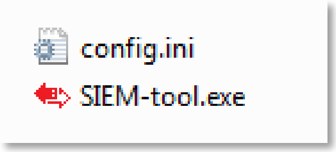
4. Preparation Procedure in SIEM Tool

Target Environment

The machine where Management Program has been installed.

Configure SIEM Tool

1. Store SIEM-Tool folder, including sub folders and files, in an appropriate location (e.g. C:\work\SIEM-tool\)



config.ini
SIEM-tool.exe

2. Please check and modify config.ini file under the SIEM-Tool folder if necessary

a. Open config.ini file under SIEM-Tool folder using a text editor.

b. Modify config.ini to align the configured SIEM Server settings.

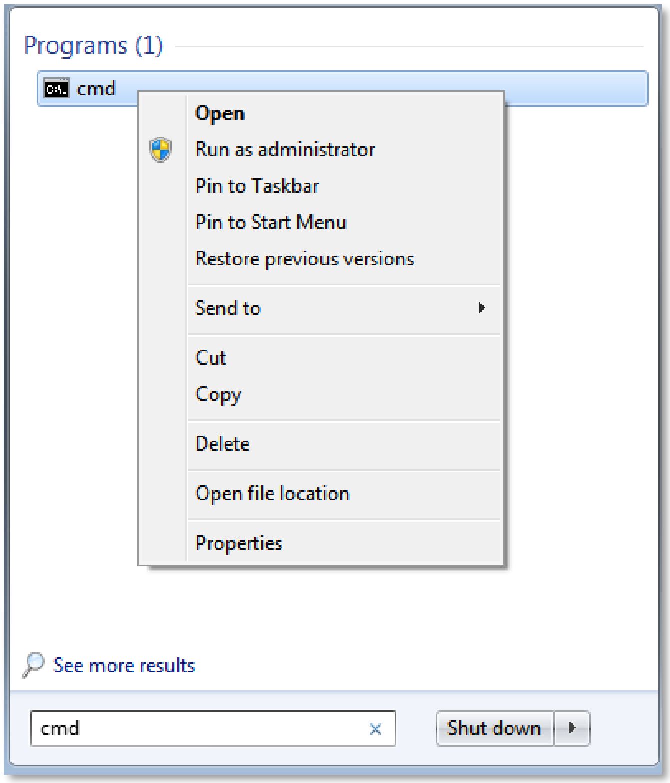
Configuration in config.ini

[Section] Parameter	Description
[General Setting]	This .ini file provides some default settings. These settings will be overwritten if the tool execute with the same option from Command Line Interface.
Startdate	Specify the starting date to query from "Startdate" to now. **Note**. 1. The value is left empty value, the tool will query the oldest record in Management Program. 2. This value will update automatically when the SIEM Tool completes log forwarding to SIEM successfully. 3. The time of each log depends on the local time of each machine. To not miss log forwarding based on time stamp, please make sure each machine has been synced to a standard time zone.
Facility	Facility code integer value for SIEM server to identify the log category. The default is LOG_LOCAL4 (20)
InstalledFolder	Please remove the symbol (;) if the Management Program is not in the default installed path and update with the custom installed path.
Event=1xxx	Default severity level for events in the ‘scanned’ log. This default value for each event is used in the logfile under the status and result to identify the severity of incoming events.
Event=2xxx	Default severity level for events of the ‘detected’ log. This default value for each event is used in the logfile under the status and result to identify the severity of incoming events.
Event=3xxx	Default severity level for events of the ‘asset info’ log.
[Splunk]	This section has the settings for Splunk
ServerAddress	IP or hostname for Splunk
ServerPort	Listening port for Splunk
Token	Token for communication with Splunk
[QRadar]	This section has the settings for QRadar
ServerAddress	IP or hostname for QRadar

ServerPort	Listening port for QRadar
CertFile	File path of certificate file for communication with QRadar
[RSyslog]	
ServerAddress	IP or hostname for RSyslog
ServerPort	Listening port for RSyslog
Protocol	Network protocol for RSyslog – currently, only UDP is supported

5. How to Use SIEM Tool

1. Launch command prompt
   a. **Windows 7**
      i. Press the Windows key on your keyboard
      ii. Type in “cmd”
      iii. Right-click “cmd” and “Run as administrator” to launch the command prompt

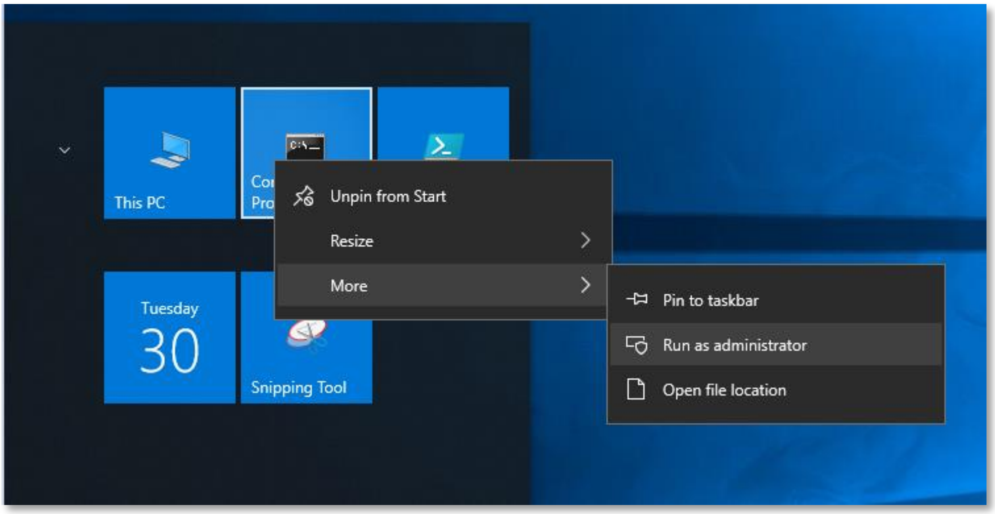


b. **Windows 10**

   i. Right-click the Windows Logo in bottom menu

   ii. Right-click “Command Prompt” in the menu item that appears

   iii. Choose “More” and “Run as administrator” to launch the command prompt



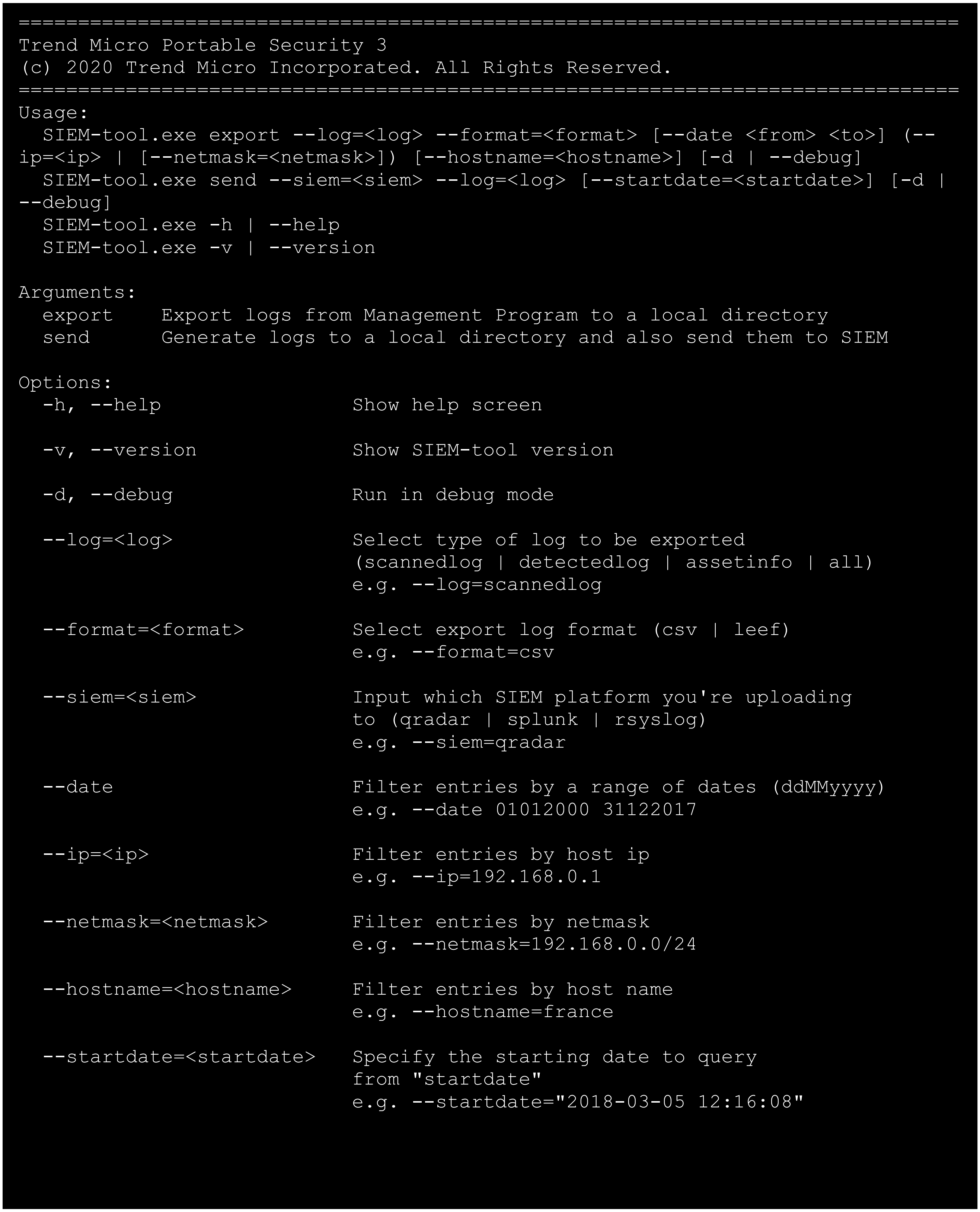
2. Change the current folder to the folder containing SIEM-Tool.exe. You can do this by typing in the following and then pressing ‘enter’.

```
C:\> cd C:\work\SIEM-Tool
```

3. Your command prompt should change its cursor to the location of your “SIEM tool” And then you can type in the following executable name with option -h and press **Enter** to execute:

```
C:\work\SIEM-Tool> SIEM-Tool.exe -h
```

4. ‘Help’ information will show



```
================================================================================
Trend Micro Portable Security 3
(c) 2020 Trend Micro Incorporated. All Rights Reserved.
================================================================================
Usage:
  SIEM-tool.exe export --log=<log> --format=<format> [--date <from> <to>] (--
ip=<ip> | [--netmask=<netmask>]) [--hostname=<hostname>] [-d | --debug]
  SIEM-tool.exe send --siem=<siem> --log=<log> [--startdate=<startdate>] [-d |
--debug]
  SIEM-tool.exe -h | --help
  SIEM-tool.exe -v | --version

Arguments:
  export    Export logs from Management Program to a local directory
  send      Generate logs to a local directory and also send them to SIEM

Options:
  -h, --help                   Show help screen

  -v, --version                Show SIEM-tool version

  -d, --debug                  Run in debug mode

  --log=<log>                  Select type of log to be exported
                               (scannedlog | detectedlog | assetinfo | all)
                               e.g. --log=scannedlog

  --format=<format>            Select export log format (csv | leef)
                               e.g. --format=csv

  --siem=<siem>                Input which SIEM platform you're uploading
                               to (qradar | splunk | rsyslog)
                               e.g. --siem=qradar

  --date                       Filter entries by a range of dates (ddMMyyyy)
                               e.g. --date 01012000 31122017

  --ip=<ip>                    Filter entries by host ip
                               e.g. --ip=192.168.0.1

  --netmask=<netmask>          Filter entries by netmask
                               e.g. --netmask=192.168.0.0/24

  --hostname=<hostname>        Filter entries by host name
                               e.g. --hostname=france

  --startdate=<startdate>      Specify the starting date to query
                               from "startdate"
                               e.g. --startdate="2018-03-05 12:16:08"
```

5. Common use cases:

    a. Export and send all logs to the QRadar server with the default LEEF format:

```
C:\work\SIEM-Tool> SIEM-Tool.exe send --log=all --siem=qradar
```

NOTE:

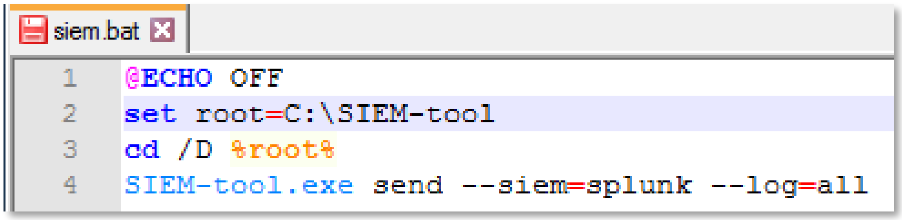
1. Please make sure all settings in the QRadar section have been setup correctly.

2. We only support sending logs to the SIEM server (QRadar/Splunk) with the LEEF format.

    b. Automatically export and send all logs to Splunk with the default LEEF format using **Task Scheduler**.

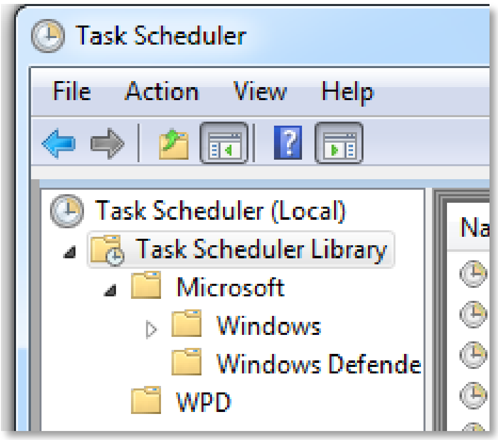
        i. Prepare a batch script for automation jobs.

        Here is an example for reference:

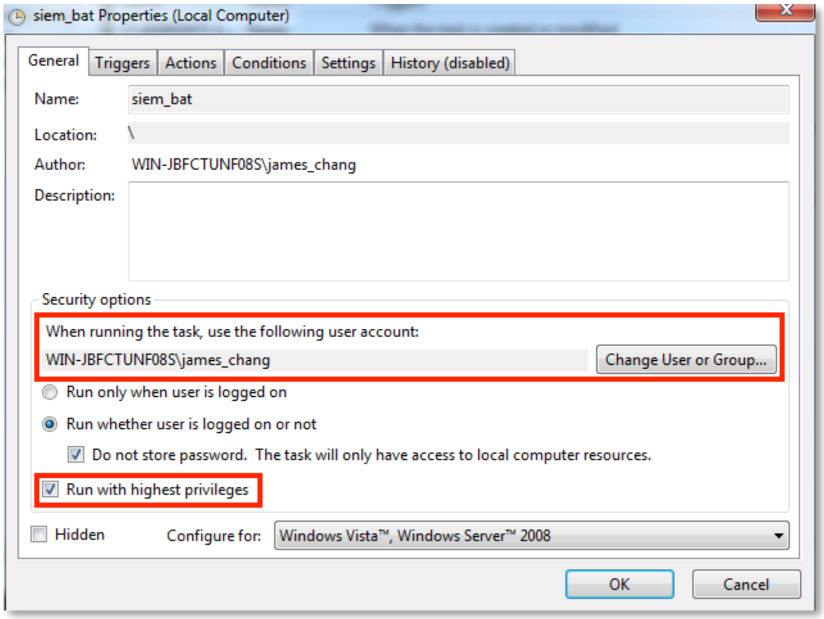


```
@ECHO OFF
set root=C:\SIEM-tool
cd /D %root%
SIEM-tool.exe send --siem=splunk --log=all
```

        ii. Find and launch the **Task Scheduler** in the Windows menu.



iii. Setup user privileges in the **General** tab of Task Scheduler.



siem_bat Properties (Local Computer)

General | Triggers | Actions | Conditions | Settings | History (disabled)

Name: siem_bat

Location: \

Author: WIN-JBFCTUNF08S\james_chang

Description:

Security options

When running the task, use the following user account:

WIN-JBFCTUNF08S\james_chang — Change User or Group...

○ Run only when user is logged on

● Run whether user is logged on or not

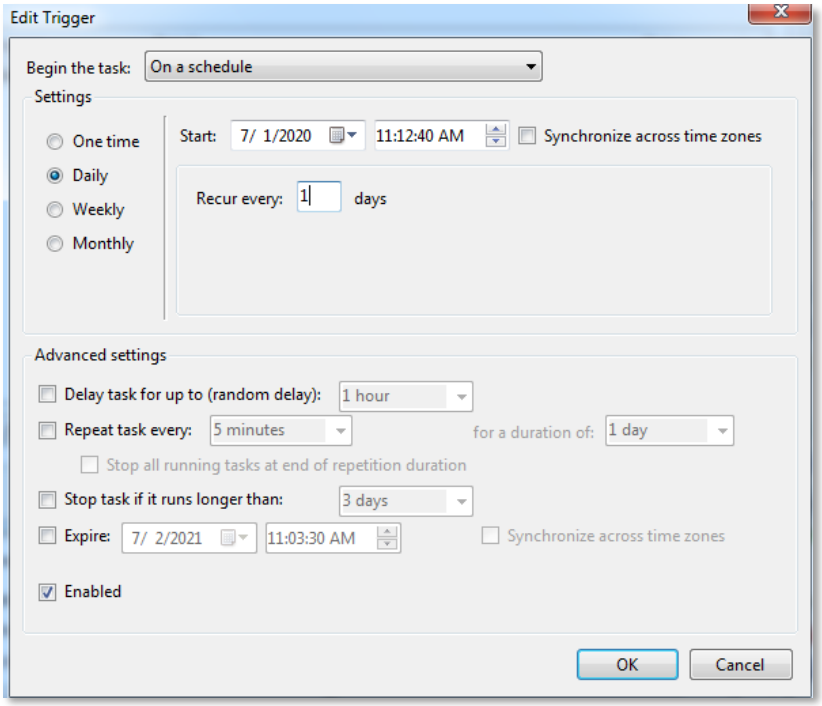
☑ Do not store password. The task will only have access to local computer resources.

☑ Run with highest privileges

□ Hidden — Configure for: Windows Vista™, Windows Server™ 2008

OK | Cancel

iv. Set up a trigger on a schedule under the **Triggers** tab.



Edit Trigger

Begin the task: On a schedule

Settings

○ One time
● Daily
○ Weekly
○ Monthly

Start: 7/ 1/2020 11:12:40 AM □ Synchronize across time zones

Recur every: 1 days

Advanced settings

□ Delay task for up to (random delay): 1 hour

□ Repeat task every: 5 minutes for a duration of: 1 day

□ Stop all running tasks at end of repetition duration

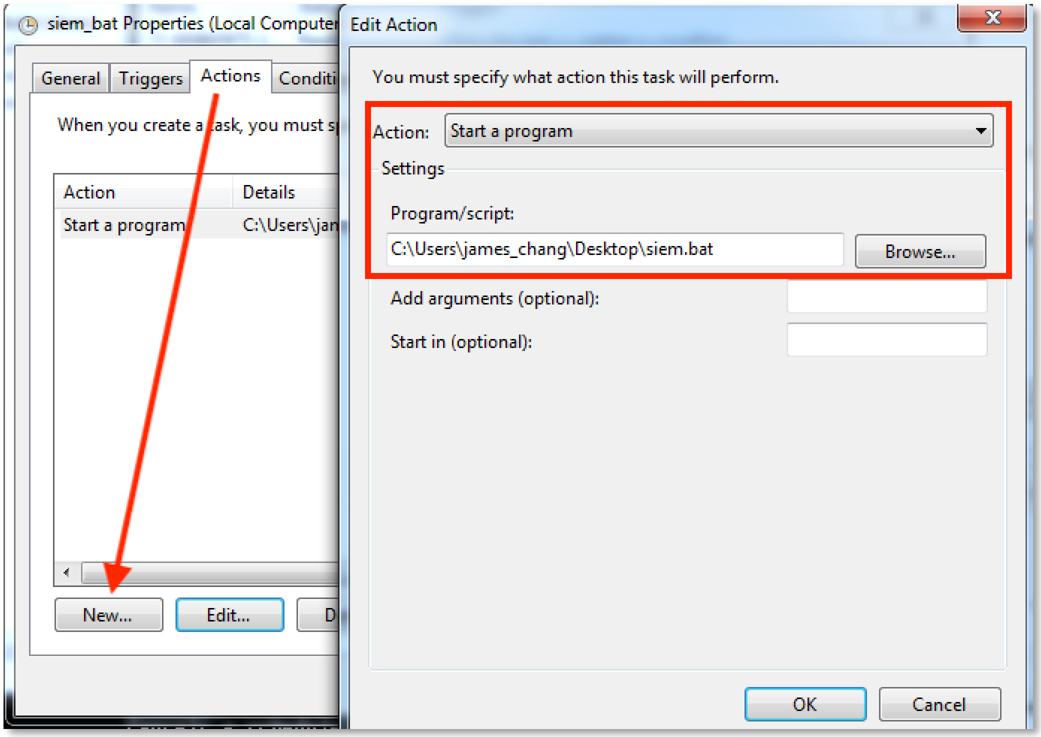
□ Stop task if it runs longer than: 3 days

□ Expire: 7/ 2/2021 11:03:30 AM □ Synchronize across time zones

☑ Enabled

OK | Cancel

v. Set up **Actions** with the batch script that includes the tasks for SIEM-tool.exe, then click OK. Once the top is triggered, the Splunk server will receive logs at the interval you’ve set (example: every 5 minutes).



When you create a task, you must s

Action	Details
Start a program	C:\Users\jan

You must specify what action this task will perform.

Action: Start a program

Settings

Program/script: C:\Users\james_chang\Desktop\siem.bat

Add arguments (optional):

Start in (optional):

c. Export scannedlog to a in local directory with CSV format from 2000/01/01 to 2017/12/31:

```
C:\work\SIEM-Tool> SIEM-Tool.exe export --log=scannedlog --format=csv
--date 01012000 31122017
```

6. How to Collect the Debug Log

1. Enable debug mode by typing -d followed by the existing command which caused an error.
2. Debug messages will be collected into **debug_log_SIEM-tool.txt**

7. TMPS3 Log LEEF Format Definition

Base LEEF 2.0 format

LEEF:2.0|Vendor|Product|Version|EventID|Custom Event Keys Block

Custom Event Keys Block

- scannedlog

Column	Description	Example
devTime	Date & Time	devTime=Jul 10 2020 17:01:08
devTimeFormat	Date & Time format	devTimeFormat=MMM dd yyyy HH:mm:ss
sev	Severity	sev=2
eventId	Event ID	eventId=1000
logID	Log ID (Unique Key)	logID={A125CB7E-6A6B-4E8C-8D73-17CD67773CBE}
logVersion	Log Version (3.0)	logVersion=3.0
startTime	Event Start Time (ddMMyyyy HH:mm:ss)	startTime=Jul 10 2020 17:03:42
endTime	Event End Time (ddMMyyyy HH:mm:ss)	endTime=Jul 10 2020 17:03:42
deviceID	Device ID	deviceID={868057F8-ADDC-49AB-934C-B5B88E704521}
deviceName	Device Name	deviceName=TMPS3
deviceVid	Device USB Vendor ID	deviceVid=2203
devicePid	Device USB Product ID	devicePid=3838
deviceSid	Device USB Serial ID	deviceSid=BD0107089A38A920BD25
scannerVersion	Scanner Version	scannerVersion=1.61.1162

scanEngineVersion	Virus Scan Engine Version	scanEngineVersion=12.0.1008
patternVersion	Virus Pattern Version	patternVersion=14.557.0
hostName	Host Name	hostName=DESKTOP-2EOANGR
hostDomain	Host Domain	hostDomain=NT AUTHORITY
userName	Host Login User Name	userName=admin
hostIP	Host IPV4 Address	hostIP=192.168.137.129
hostMac	Host Mac Address	hostMac=00:0C:29:7A:88:6C
hostOS	Host OS	hostOS=Microsoft Windows 10 Enterprise Edition (build 16299), 64-bit
scannedStatus	Result Status (Scan completed, Scan canceled, Scan suspended)	scannedStatus=Scan completed
scannedFiles	Result Scanned Files	scannedFiles=23
infectedFiles	# Of Infected Files	infectedFiles=0
fixedFiles	# Of Fixed Files	fixedFiles=0
scanTarget	Option Scan Target (All, Quick, Specified, SafeLockApplicationLockdown)	scanTarget=Specified
exclusionPath	Excluded Path	exclusionPath=Specified
exclusionFile	Excluded Files	exclusionFile=c:\users\admin\downloads\test.txt
exclusionExtension	Excluded Extensions	exclusionExtension=txt
comment	Result Comments	comment=No threats found

Example for scannedlog:

LEEF:2.0|TrendMicro|PortableSecurity|3.0|**devTime**=Jul 10 2020 17:01:08 **devTimeFormat**=MMM dd yyyy HH:mm:ss **sev**=2 **eventId**=1000 **logID**={06BFDC81-8E9F-4A07-AE95-C079B452C19B} **logVersion**=3.0 **startTime**=Jul 10 2020 17:01:08 **endTime**=Jul 10 2020 17:01:09 **deviceID**={868057F8-ADDC-49AB-934C-B5B88E704521} **deviceName**=TMPS3 **deviceVid**=2203 **devicePid**=3838 **deviceSid**=BD0107089A38A920BD25 **scannerVersion**=1.61.1162 **scanEngineVersion**= **patternVersion**=14.557.0 **hostName**=DESKTOP-2EOANGR **hostDomain**=NT AUTHORITY **userName**=admin **hostIP**=192.168.137.129 **hostMac**=00:0C:29:7A:88:6C

hostOS=Microsoft Windows 10 Enterprise Edition (build 16299), 64-bit **scannedStatus**=Scan completed **scannedFiles**=23 **infectedFiles**=0 **fixedFiles**=0 **scanTarget**=Specified **exclusionPath**=Specified **exclusionFile**= **exclusionExtension**= **comment**=No threats found

- detectedlog

Column	**Description**	**Example**
devTime	Date & Time	devTime=Jul 10 2020 17:01:08
devTimeFormat	Date & Time format	devTimeFormat=MMM dd yyyy HH:mm:ss
sev	Severity	sev=2
eventId	Event ID	eventId=1000
logID	Log ID (Not Unique Key)	logID={29FD789F-CA78-48FD-92B9-E598F1187C2E}
logVerison	Log Version (3.0)	logVersion=3.0
startTime	Event Start Time (ddMMyyyy HH:mm:ss)	startTime=Jul 10 2020 17:09:04
endTime	Event End Time (ddMMyyyy HH:mm:ss)	endTime=Jul 10 2020 17:09:05
deviceID	Device ID	deviceID={868057F8-ADDC-49AB-934C-B5B88E704521}
deviceName	Device Name	deviceName=TMPS3
deviceVid	Device USB Vendor ID	deviceVid=2203
devicePid	Device USB Product ID	devicePid=3838
deviceSid	Device USB Serial ID	deviceSid=BD0107089A38A920BD25
hostName	Host Name	hostName=WIN-JBFCTUNF08S
hostDomain	Host Domain	hostDomain=NT AUTHORITY
userName	Host Login User Name	userName=james_chang
hostIP	Host IPV4 Address	hostIP=192.168.137.251

hostMac	Host Mac Address	hostMac=00:0C:29:6C:12:C3
hostOS	Host OS	hostOS=Microsoft Windows 7 Enterprise Edition Service Pack 1 (build 7601), 32-bit
aggressiveLevel	Aggressive Level	aggressiveLevel=0
threatName	Threat Name	threatName=FILE_ADS
threatType	Threat Type:	threatType=Other
threatRisk	Threat Risk Level (0: Low, 1: Medium, 2: High)	threatRisk=2
takenAct	Action Type (fix, ignore)	takenAct=Fix
takenActResult	Action Result (Fixed, Unable to fix, Fixed at restart, Ignored)	takenActResult=Fixed
threatHash	Threat Hash	threatHash=c0839455963609be3363f52397d3353743697d504518dca639c77062b42a3a8c
threatPath	Threat Path	threatPath=C:\Users\james_chang\Desktop\test.zip

Example for detectedlog:

LEEF:2.0|TrendMicro|PortableSecurity|3.0|**devTime**=Jul 10 2020 17:09:04 **devTimeFormat**=MMM dd yyyy HH:mm:ss **sev**=2 **eventId**=2008 **logID**={29FD789F-CA78-48FD-92B9-E598F1187C2E} **logVersion**=3.0 **startTime**=Jul 10 2020 17:09:04 **endTime**=Jul 10 2020 17:09:05 **deviceID**={868057F8-ADDC-49AB-934C-B5B88E704521} **deviceName**=TMPS3 **deviceVid**=2203 **devicePid**=3838 **deviceSid**=BD0107089A38A920BD25 **hostName**=WIN-JBFCTUNF08S **hostDomain**=NT AUTHORITY **userName**=james_chang **hostIP**=192.168.137.251 **hostMac**=00:0C:29:6C:12:C3 **hostOS**=Microsoft Windows 7 Enterprise Edition Service Pack 1 (build 7601), 32-bit **aggressiveLevel**=0 **threatName**=Eicar_test_file **threatType**=Other **threatRisk**=2 **takenAct**=Fix **takenActResult**=Fixed **threatHash**=542f0327d3c2d3d2d6095321e80ca8850ac83816436df87fa9a87957cf774e7e **threatPath**=C:\

- assetinfo

Column	Description	Example
sev	Severity	sev=2
eventId	Event ID	eventId=3000
hostID	Host ID (defined by TMPS)	hostID=554328661
hostName	Host Name	hostName=DESKTOP-DQVS8QS
domain	Domain	domain=DESKTOP-DQVS8QS
Mac	Mac Address	Mac=00:0C:29:DC:07:3A
IP	IPV4 Address	IP=192.168.137.235
OS	OS	OS=Microsoft Windows 10 Enterprise Edition (build 19041), 32-bit
OSType	Window or Linux	OSType=WINDOWS
vendorName	Vendor Name	vendorName=VMware, Inc.
hwModel	HW Model	hwModel=VMware Virtual Platform
hwSerialNum	HW Serial Number	hwSerialNum=VMware-56 4d 7e 74 92 98 22 24-39 26 f9 86 65 dc 07 3a
biosVersionAndDate	BIOS Version and Date	biosVersionAndDate={INTEL - 6040000, PhoenixBIOS 4.0 Release 6.0 }(Release Date: 2017-05-19 00:00:00.000)
biosType	BIOS Type	biosType=UEFI
secureBoot	Secure Boot	secureBoot=False
CPU	CPU	CPU=Intel(R) Core(TM) i7-9700 CPU @ 3.00GHz
CPUArchitecture	CPU Architecture	CPUArchitecture=X64
processorsAndCores	Processors and Cores	processorsAndCores=NumberOfCores: 1 ,NumberOfLogicalProcessors: 1
physicalMemory	Physical Memory	physicalMemory=2096628KB
availableMemory	Available Memory	availableMemory=929560KB

OSVersionAndBuild	OS Version and Build	OSVersionAndBuild=Microsoft Windows 10 Enterprise 10.0.19041
OSServicePack	OS Service Pack	OSServicePack=1.0
OSProductID	OS Product ID	OSProductID=00328-90000-00000-AAOEM
OSLanguage	OS Language	OSLanguage=en-US
OSInstalledDateAndTime	OS Installed Date and Time	OSInstalledDateAndTime=05032020 11:18:20
IEVersionAndBuild	IE Version and Build	IEVersionAndBuild=11.329.19041.0
IEServicePack	IE Service Pack	IEServicePack=KB4561603
IEUpdateVersion	IE Update Version	IEUpdateVersion=11.0.195
windowsDirectory	Windows directory	windowsDirectory=C:\Windows
systemDirectory	System Directory	systemDirectory=C:\Windows\system32
systemDriveSize	System Drive Size	systemDriveSize=39GB
systemDriveAvailableSize	System Drive Available Space	systemDriveAvailableSize=24GB
bootDrive	Boot Drive	bootDrive=\Device\HarddiskVolume1
timezone	Time Zone	timezone=UTC +08:00
systemDateAndTime	System Date and Time	systemDateAndTime=10072020 11:41:21
loggedinAccount	Logged in Account	loggedinAccount=abc
loggedinDomain	Logged in Domain	loggedinDomain=DESKTOP-DQVS8QS

Example for assetinfo:

LEEF:2.0|TrendMicro|PortableSecurity|3.0|**sev**=2 **eventId**=3000 **hostID**=554328661 **hostName**=DESKTOP-DQVS8QS **domain**=DESKTOP-DQVS8QS **Mac**=00:0C:29:DC:07:3A IP=192.168.137.235 **OS**=Microsoft Windows 10 Enterprise Edition (build 19041), 32-bit **OSType**=WINDOWS **vendorName**=VMware, Inc. **hwModel**=VMware Virtual Platform **hwSerialNum**=VMware-56 4d 7e 74 92 98 22 24-39 26 f9 86 65 dc 07 3a **biosVersionAndDate**={INTEL - 6040000, PhoenixBIOS 4.0 Release 6.0   }(Release Date: 2017-05-19 00:00:00.000) **biosType**=UEFI **secureBoot**=False **CPU**=Intel(R) Core(TM) i7-9700 CPU @ 3.00GHz **CPUArchitecture**=X64 **processorsAndCores**=NumberOfCores: 1 ,NumberOfLogicalProcessors: 1

physicalMemory=2096628KB **availableMemory**=929560KB **OSVersionAndBuild**=Microsoft Windows 10 Enterprise 10.0.19041 **OSServicePack**= **OSProductID**=00328-90000-00000-AAOEM **OSLanguage**=en-US **OSInstalledDateAndTime**=05032020 11:18:20 **IEVersionAndBuild**=11.329.19041.0 **IEServicePack**=KB4561603 **IEUpdateVersion**=11.0.195 **windowsDirectory**=C:\Windows **systemDirectory**=C:\Windows\system32 systemDriveSize=39GB **systemDriveAvailableSize**=24GB **bootDrive**=\Device\HarddiskVolume1 **timezone**=UTC +08:00 **systemDateAndTime**=10072020 11:41:21 **loggedinAccount**=abc **loggedinDomain**=DESKTOP-DQVS8QS

- applicationinfo

Column	Description	Example
sev	Severity	sev=2
eventId	Event ID	eventId=3000
hostID	Host ID (defined by TMPS)	hostID=554328661
name	Application Name	name=7-Zip 19.00
publisher	Publisher	publisher=Igor Pavlov
installedDate	Date of Installation	installedDate=22062020
size	File Size	size=3772KB
version	Application Version	version=19.00
installPath	Application Install Path	installPath=C:\Program Files\7-Zip\

Example for applicationinfo:

LEEF:2.0|TrendMicro|PortableSecurity|3.0|**sev**=2 **eventId**=3000 **hostID**=554328661 **name**=7-Zip 19.00 **publisher**=Igor Pavlov **installedDate**= **size**=3772KB **version**=19.00 **installPath**=C:\Program Files\7-Zip\

- updateinfo

Column	Description	Example
sev	Severity	sev=2
eventId	Event ID	eventId=3000
hostID	Host ID (defined by TMPS)	hostID=554328661

name	Update Program Name	name=Update for Microsoft Windows (KB4557957)
program	Program Name	program=Microsoft Windows
version	Program Version	version=
publisher	Publisher of the Program	publisher=Microsoft Corporation
installedDate	Date of Installation	installedDate=16062020

Example for updateinfo:

LEEF:2.0|TrendMicro|PortableSecurity|3.0|**sev**=2 **eventId**=3000 **hostID**=554328661 **name**=Update for Microsoft Windows (KB4552925) **program**=Microsoft Windows **version**= **publisher**=Microsoft Corporation installedDate=16062020