



5.5 TREND MICRO™ TippingPoint™ Advanced Threat Protection Analyzer

Syslog Content Mapping Guide

Breakthrough Protection Against APTs and Targeted Attacks



Endpoint Security



Network Security



Protected Cloud



Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

<http://docs.trendmicro.com>

© 2016 Trend Micro Incorporated. All Rights Reserved. Trend Micro, the Trend Micro t-ball logo, Deep Discovery Advisor, TippingPoint Advanced Threat Protection Analyzer, TippingPoint Advanced Threat Protection for Networks, and Control Manager are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Document Part No.: APEM57302/160118

Release Date: February 2016

Protected by U.S. Patent No.: Patents pending.

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site:

<http://www.trendmicro.com/download/documentation/rating.asp>

Table of Contents

Preface

Preface	iii
Documentation	iv
Audience	v
Document Conventions	vi
About Trend Micro	vii

Chapter 1: Introduction

Terminology	1-3
-------------------	-----

Chapter 2: Syslog Content Mapping - CEF

CEF Virtual Analyzer Analysis Logs: File Analysis Events	2-2
CEF Virtual Analyzer Analysis Logs: URL Analysis Events	2-4
CEF Virtual Analyzer Analysis Logs: Notable Characteristics Events ..	2-6
CEF Virtual Analyzer Analysis Logs: Deny List Transaction Events	2-8

Chapter 3: Syslog Content Mapping - LEEF

LEEF Virtual Analyzer Analysis Logs: File Analysis	3-2
LEEF Virtual Analyzer Analysis Logs: URL Analysis	3-4
LEEF Virtual Analyzer Analysis Logs: Notable Characteristics Events	3-6
LEEF Virtual Analyzer Analysis Logs: Deny List Transaction Events .	3-8

Chapter 4: Syslog Content Mapping - TMEF

TMEF Virtual Analyzer Analysis Logs: File Analysis Events	4-2
TMEF Virtual Analyzer Analysis Logs: URL Analysis Events	4-4
TMEF Virtual Analyzer Analysis Logs: Notable Characteristics Events	4-6

TMEF Virtual Analyzer Analysis Logs: Deny List Transaction Events 4-8

Index

Index IN-1

Preface

Preface

Learn more about the following topics:

- *Documentation on page iv*
- *Audience on page v*
- *Document Conventions on page vi*
- *About Trend Micro on page vii*

Documentation

The documentation set for TippingPoint Advanced Threat Protection Analyzer includes the following:

TABLE 1. Product Documentation

DOCUMENT	DESCRIPTION
Administrator's Guide	PDF documentation provided with the product or downloadable from the Trend Micro website. The Administrator's Guide contains detailed instructions on how to configure and manage Advanced Threat Protection Analyzer, and explanations on Advanced Threat Protection Analyzer concepts and features.
Installation and Deployment Guide	PDF documentation provided with the product or downloadable from the Trend Micro website. The Installation and Deployment Guide contains information about requirements and procedures for planning deployment, installing Advanced Threat Protection Analyzer, and using the Preconfiguration Console to set initial configurations and perform system tasks.
User's Guide	PDF documentation provided with the product or downloadable from the Trend Micro website. The User's Guide contains general information about Advanced Threat Protection Analyzer concepts and features. It introduces selected sections of the management console to users who have been assigned viewer accounts.
Quick Start Card	The Quick Start Card provides user-friendly instructions on connecting Advanced Threat Protection Analyzer to your network and on performing the initial configuration.
Readme	The Readme contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, known issues, and product release history.

DOCUMENT	DESCRIPTION
Online Help	Web-based documentation that is accessible from the Advanced Threat Protection Analyzer management console. The Online Help contains explanations of Advanced Threat Protection Analyzer components and features, as well as procedures needed to configure Advanced Threat Protection Analyzer.
Support Portal	The Support Portal is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Support Portal, go to the following website: http://esupport.trendmicro.com

View and download product documentation from the Trend Micro Online Help Center:

<http://docs.trendmicro.com/en-us/home.aspx>

Audience

The TippingPoint Advanced Threat Protection Analyzer documentation is written for IT administrators and security analysts. The documentation assumes that the reader has an in-depth knowledge of networking and information security, including the following topics:

- Network topologies
- Database management
- Antivirus and content security protection

The documentation does not assume the reader has any knowledge of sandbox environments or threat event correlation.

Document Conventions

The documentation uses the following conventions:

TABLE 2. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
<i>Italics</i>	References to other documents
Monospace	Sample command lines, program code, web URLs, file names, and program output
Navigation > Path	The navigation path to reach a particular screen For example, File > Save means, click File and then click Save on the interface
 Note	Configuration notes
 Tip	Recommendations or suggestions
 Important	Information regarding required or default configuration settings and product limitations
 WARNING!	Critical actions and configuration options

About Trend Micro

As a global leader in cloud security, Trend Micro develops Internet content security and threat management solutions that make the world safe for businesses and consumers to exchange digital information. With over 20 years of experience, Trend Micro provides top-ranked client, server, and cloud-based solutions that stop threats faster and protect data in physical, virtual, and cloud environments.

As new threats and vulnerabilities emerge, Trend Micro remains committed to helping customers secure data, ensure compliance, reduce costs, and safeguard business integrity. For more information, visit:

<http://www.trendmicro.com>

Trend Micro and the Trend Micro t-ball logo are trademarks of Trend Micro Incorporated and are registered in some jurisdictions. All other marks are the trademarks or registered trademarks of their respective companies.

Chapter 1

Introduction

The TippingPoint Advanced Threat Protection Analyzer Syslog Content Mapping Guide provides information about log management standards and syntaxes for implementing syslog events in Trend Micro Advanced Threat Protection Analyzer.

To enable flexible integration with third-party log management systems, TippingPoint Advanced Threat Protection Analyzer supports the following syslog formats:

LOG MANAGEMENT SYSTEM	DESCRIPTION
Common Event Format (CEF) For details, see Syslog Content Mapping - CEF on page 2-1	CEF is an open log management standard created by HP ArcSight. TippingPoint Advanced Threat Protection Analyzer uses a subset of the CEF dictionary.
Log Event Extended Format (LEEF) For details, see Syslog Content Mapping - LEEF on page 3-1	LEEF is an event format developed for IBM Security QRadar. TippingPoint Advanced Threat Protection Analyzer uses a subset of the LEEF dictionary.

LOG MANAGEMENT SYSTEM	DESCRIPTION
Trend Micro Event Format (TMEF) For details, see Syslog Content Mapping - TMEF on page 4-1	TMEF is a superset of log fields that allow a third-party syslog collector to better control and mitigate detection events provided by TippingPoint Advanced Threat Protection Analyzer.

Terminology

TERM	DESCRIPTION
CEF	Common Event Format
LEEF	Log Event Extended Format
TMEF	Trend Micro Event Format

Chapter 2

Syslog Content Mapping - CEF

The following tables outline syslog content mapping between TippingPoint Advanced Threat Protection Analyzer log output and CEF syslog types:

- *CEF Virtual Analyzer Analysis Logs: File Analysis Events on page 2-2*
- *CEF Virtual Analyzer Analysis Logs: URL Analysis Events on page 2-4*
- *CEF Virtual Analyzer Analysis Logs: Notable Characteristics Events on page 2-6*
- *CEF Virtual Analyzer Analysis Logs: Deny List Transaction Events on page 2-8*

CEF Virtual Analyzer Analysis Logs: File Analysis Events

TABLE 2-1. CEF Virtual Analyzer Analysis Logs: File Analysis Events

CEF KEY	DESCRIPTION	VALUE
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection Analyzer
Header (pver)	Appliance version	Example: 2.5.0.1161
Header (eventid)	Signature ID	200119
Header (eventName)	Description	Sample file sandbox analysis is finished
Header (severity)	Severity	3
cn1	GRID is known good	• -1: GRID is unknown • 0: GRID is not known good • 1: GRID is known good
cn1Label	GRID is known good	GRIDIsKnownGood

CEF KEY	DESCRIPTION	VALUE
cn2	ROZ rating	-1: Unsupported file type in ROZ 0: No risk found 1: Low risk 2: Medium risk 3: High risk  Note Other negative values refer to errors.
cn2Label	ROZ rating	ROZRating
cn3	PCAP ready	0: PCAP is not ready 1: PCAP is ready
cn3Label	PCAP ready	PcapReady
cs1	Sandbox image type	Example: win7
cs1Label	Sandbox image type	SandboxImageType
cs2	Malware name	Example: HEUR_NAMETRICK.A
cs2Label	Malware name	MalwareName
cs3	Parent SHA1	Example: A29E4ACA70BEF4AF8CE75AF5 1032B6B91572AA0D
cs3Label	Parent SHA1	ParentFileSHA1
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28- A4CE-0462-A536
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost

CEF KEY	DESCRIPTION	VALUE
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5 CAB395E4197C8F3
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar
fsize	File size	Example: 131372
rt	Analysis time	Example: Mar 09 2015 17:05:21 GMT+08:00

Log sample:

```
CEF:0|Trend Micro|TippingPoint Threat Protection Analyzer|5.5.
0.1202|200119|Sample file sandbox analysis is finished|3|rt=Fe
b 27 20 15 09:49:06 GMT+00:00 dvc=10.204.191.249 dvchost=ATPAn
alyzer dvcmac=EC:F4:BB:C6:F1:D0 deviceExternalId=758B04C9-F577
-4B8A-B527-ABCB84FDAC83 fname=Invoice_06202013_QBK.exe fileHas
h=CF1A6CF231BDA185DEBF70B8562301798F286FAD fileType=WIN32 EXE
fsize=117248 cs1Label=SandboxImageType cs1=win8 cs3Label=Paren
tFileSHA1 cs3=FF47AEE003778AA51E0326F53EF235C96D71D7CA cn1Labe
l=GRIDIsKnownGood cn1=-1 cn2Label=ROZRating cn2=3 cs2Label=Mal
wareName cs2=TSPY_FAREIT.WT cn3Label=PcapReady cn3=1
```

CEF Virtual Analyzer Analysis Logs: URL Analysis Events

TABLE 2-2. CEF Virtual Analyzer Analysis Logs: URL Analysis Events

CEF KEY	DESCRIPTION	VALUE
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro

CEF KEY	DESCRIPTION	VALUE
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection Analyzer
Header (pver)	Appliance version	Example: 2.5.0.1161
Header (eventid)	Signature ID	200126
Header (eventName)	Description	URL sandbox analysis is finished
Header (severity)	Severity	3
cn2	ROZ rating	-1: Unsupported file type in ROZ 0: No risk found 1: Low risk 2: Medium risk 3: High risk  Note Other negative values refer to errors.
cn2Label	ROZ rating	ROZRating
cn3	PCAP ready	0: PCAP is not ready 1: PCAP is ready
cn3Label	PCAP ready	PcapReady
cs1	Sandbox image type	Example: win7
cs1Label	Sandbox image type	SandboxImageType
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dvc	Appliance IP address	Example: 10.1.144.199

CEF KEY	DESCRIPTION	VALUE
dvchost	Appliance host name	Example: localhost
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5 CAB395E4197C8F3
request	URL	Example: http:// www.rainking.net/? utm_campaign=4-21-2014 http:// images.rainking.net/eloquaimage
rt	Analysis time	Example: Mar 09 2015 17:05:21 GMT+08:00

Log sample:

```
CEF:0|Trend Micro|TippingPoint Threat Protection Analyzer|5.5.
0.1202|200126|URL sandbox analysis is finished|3|rt=Feb 27 201
5 09:36:26 GMT+00:00 dvc=10.204.191.249 dvchost=ATPAnalyzer dv
cmac=EC:F4:BB:C6:F1:D0 deviceExternalId=758B04C9-F577-4B8A-B52
7-ABCB84FDAC83 request=http://www.baidu.com:80/ fileHash=ACB51
75554463DD2ADBDFF78AD82C7D6BB8C8B6B cs1Label=SandboxImageType
cs1=win8 cn2Label=ROZRating cn2=0 cn3Label=PcapReady cn3=1
```

CEF Virtual Analyzer Analysis Logs: Notable Characteristics Events

TABLE 2-3. CEF Virtual Analyzer Analysis Logs: Notable Characteristics Events

CEF KEY	DESCRIPTION	VALUE
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro

CEF KEY	DESCRIPTION	VALUE
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection Analyzer
Header (pver)	Appliance version	Example: 2.5.0.1161
Header (eventid)	Signature ID	200127
Header (eventName)	Description	Notable Characteristics of the analyzed sample
Header (severity)	Severity	6
cs1	Violated policy name	Example: Internet Explorer Setting Modification
cs1Label	Violated policy name	PolicyCategory
cs2	Violated event analysis	Example: Modified important registry items
cs2Label	Violated event analysis	PolicyName
cs3	Sandbox image type	Example: win7
cs3Label	Sandbox image type	SandboxImageType
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5 CAB395E4197C8F3
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar

CEF KEY	DESCRIPTION	VALUE
fsize	File size	Example: 131372
msg	Details	Example: Source: ATSE \nDetection Name: TSPY_FAREIT.WT\nEngine Version: 9.755.1246\nMalware Pattern Version: 11.501.90
rt	Analysis time	Example: Mar 09 2015 17:05:21 GMT+08:00

Log sample:

```
CEF:0|Trend Micro|TippingPoint Threat Protection Analyzer|5.5.
0.1202|200127|Notable Characteristics of the analyzed sample|6
|rt=Feb 27 2015 09:49:06 GMT+00:00 dvc=10.204.191.249 dvchost=
ATPAnalyzer dvcmac=EC:F4:BB:C6:F1:D0 deviceExternalId=758B04C9
-F577-4B8A-B527-ABCB84FDAC83 fname=Invoice_06202013_QBK.exe fi
leHash=CF1A6CF231BDA185DEBF70B8562301798F286FAD fileType=WIN32
EXE fsize=117248 cs1Label=PolicyCategory cs1=Malformed, defec
tive, or with known malware traits msg=Source: ATSE\nDetection
Name: TSPY_FAREIT.WT\nEngine Version: 9.755.1246\nMalware Pat
tern Version: 11.501.90 cs2Label=PolicyName cs2=Detected as kn
own malware
```

CEF Virtual Analyzer Analysis Logs: Deny List Transaction Events

TABLE 2-4. CEF Virtual Analyzer Analysis Logs: Deny List Transaction Events

CEF KEY	DESCRIPTION	VALUE
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection Analyzer

CEF KEY	DESCRIPTION	VALUE
Header (pver)	Appliance version	Example: 2.5.0.1161
Header (eventid)	Signature ID	200120
Header (eventName)	Description	Deny List updated
Header (severity)	Severity	3
act	The action in the event	• Add • Remove
cs1	Deny List type	• Deny List IP/Port • Deny List URL • Deny List File SHA1 • Deny List Domain
cs1Label	Deny List type	type
cs2	Risk level	• Low • Medium • High • Confirmed Malware
cs2Label	Risk level	RiskLevel
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dhost	Destination host name	Example: dhost1
dpt	Destination port	Value between 0 and 65535
dst	Destination IP address	Example: 10.1.144.199
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost

CEF KEY	DESCRIPTION	VALUE
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
end	Deny List expired time	Example: Mar 09 2015 17:05:21 GMT+08:00
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5 CAB395E4197C8F3
request	URL	Example: http:// www.rainking.net/? utm_campaign=4-21-2014 http:// images.rainking.net/eloquaimage
rt	Log generation time	Example: Mar 09 2015 17:05:21 GMT+08:00

Log sample:

```
CEF:0|Trend Micro|TippingPoint Threat Protection Analyzer|5.5.0.1202|200120|Deny List updated|3|rt=Feb 27 2015 09:49:41 GMT+00:00 dvc=10.204.191.249 dvchost=ATPAnalyzer dvcmac=EC:F4:BB:C6:F1:D0 deviceExternalId=758B04C9-F577-4B8A-B527-ABCB84FDAC83 cs1Label=type cs1=Deny List File SHA1 end=Mar 29 2015 09:49:06 GMT+00:00 act=Add fileHash=CF1A6CF231BDA185DEBF70B8562301798F286FAD cs2Label=RiskLevel cs2=High
```

Chapter 3

Syslog Content Mapping - LEEF

The following tables outline syslog content mapping between TippingPoint Advanced Threat Protection Analyzer log output and LEEF syslog types:

- *LEEF Virtual Analyzer Analysis Logs: File Analysis on page 3-2*
- *LEEF Virtual Analyzer Analysis Logs: URL Analysis on page 3-4*
- *LEEF Virtual Analyzer Analysis Logs: Notable Characteristics Events on page 3-6*
- *LEEF Virtual Analyzer Analysis Logs: Deny List Transaction Events on page 3-8*



Note

When using the LEEF log syntax, separate event attributes with <009> as a tab delimiter.

LEEF Virtual Analyzer Analysis Logs: File Analysis

TABLE 3-1. LEEF Virtual Analyzer Analysis Logs: File Analysis

LEEF KEY	DESCRIPTION	VALUE
Header (logVer)	LEEF format version	LEEF: 1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection Analyzer
Header (pver)	Appliance version	Example: 2.5.0.1161
Header (eventName)	Event Name	FILE_ANALYZED
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:56:B3:57
deviceProcessHash	Parent SHA1	Example: A29E4ACA70BEF4AF8CE75AF5 1032B6B91572AA0D
devTime	Log generation time	Example: Jan 28 2015 02:00:36 GMT+08:00
devTimeFormat	Time format	MMM dd yyyy HH:mm:ss z
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5 CAB395E4197C8F3
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar

LEEF KEY	DESCRIPTION	VALUE
fsize	File size	Example: 131372
gridIsKnownGood	GRID is known good	-1: GRID is unknown 0: GRID is not known good 1: GRID is known good
malName	Malware name	Example: HEUR_NAMETRICK.A
pcapReady	PCAP ready	0: PCAP is not ready 1: PCAP is ready
pComp	Detection engine / component	Sandbox
rozRating	ROZ rating	-1: Unsupported file type in ROZ 0: No risk found 1: Low risk 2: Medium risk 3: High risk  Note Other negative values refer to errors.
sev	Severity	Value between 0 and 10

**Note**

When using the LEEF log syntax, separate event attributes with <009> as a tab delimiter.

Log sample:

```
LEEF:1.0|Trend Micro|TippingPoint Threat Protection Analyzer|5.
5.0.1202|FILE_ANALYZED|devTime=Feb 28 2015 02:45:48 GMT+00:00<0
09>devTimeFormat=MMM dd yyyy HH:mm:ss z<009>sev=3<009>pComp=San
```

```

dbox<009>dvc=10.204.191.249<009>dvchost=ATPAnalyzer<009>deviceMacAddress=EC:F4:BB:C6:F1:D0<009>deviceGUID=758B04C9-F577-4B8A-B527-ABC84FDAC83<009>fname=Invoice_06202013_QBK.exe<009>fileHash=CF1A6CF231BDA185DEBF70B8562301798F286FAD<009>deviceProcessHash=FF47AEE003778AA51E0326F53EF235C96D71D7CA<009>malName=TSPY_FARBIT.WT<009>fileType=WIN32_EXE<009>fsize=117248<009>deviceOSName=win8<009>gridIsKnownGood=-1<009>rozRating=3<009>pcapReady=1

```

LEEF Virtual Analyzer Analysis Logs: URL Analysis

TABLE 3-2. LEEF Virtual Analyzer Analysis Logs: URL Analysis

LEEF KEY	DESCRIPTION	VALUE
Header (logVer)	LEEF format version	LEEF: 1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection Analyzer
Header (pver)	Appliance version	Example: 2.5.0.1161
Header (eventName)	Event Name	URL_ANALYZED
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:56:B3:57
deviceOSName	Sandbox image type	Example: win7
devTime	Log generation time	Example: Jan 28 2015 02:00:36 GMT+08:00
devTimeFormat	Time format	MMM dd yyyy HH:mm:ss z
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost

LEEF KEY	DESCRIPTION	VALUE
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5 CAB395E4197C8F3
pcapReady	PCAP ready	0: PCAP is not ready 1: PCAP is ready
pComp	Detection engine / component	Sandbox
rozRating	ROZ rating	-1: Unsupported file type in ROZ 0: No risk found 1: Low risk 2: Medium risk 3: High risk  Note Other negative values refer to errors.
sev	Severity	Value between 0 and 10
url	URL	Example: http://1.2.3.4/query?term=value

**Note**

When using the LEEF log syntax, separate event attributes with <009> as a tab delimiter.

Log sample:

```
LEEF:1.0|Trend Micro|TippingPoint Threat Protection Analyzer|5.5.0.1202|URL_ANALYZED|devTime=Feb 27 2015 09:36:26 GMT+00:00<009>devTimeFormat=MMM dd yyyy HH:mm:ss z<009>sev=3<009>pComp=Sandbox<009>dvc=10.204.191.249<009>dvchost=ATPAnalyzer<009>deviceMacAddress=EC:F4:BB:C6:F1:D0<009>deviceGUID=758B04C9-F577-4B8A-B5
```

```
27-ABC84FDAC83<009>fileHash=ACB5175554463DD2ADBDF78AD82C7D6BB
8C8B6B<009>deviceOSName=win8<009>url=http://www.baidu.com:80/<0
09>rozRating=0<009>pcapReady=1
```

LEEF Virtual Analyzer Analysis Logs: Notable Characteristics Events

TABLE 3-3. LEEF Virtual Analyzer Analysis Logs: Notable Characteristics Events

LEEF KEY	DESCRIPTION	VALUE
Header (logVer)	LEEF format version	LEEF: 1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection Analyzer
Header (pver)	Appliance version	Example: 2.5.0.1161
Header (eventName)	Event Name	NOTABLE_CHARACTERISITICS
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:56:B3:57
deviceOSName	Sandbox image type	Example: win7
devTime	Log generation time	Example: Jan 28 2015 02:00:36 GMT+08:00
devTimeFormat	Time format	MMM dd yyyy HH:mm:ss z
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5 CAB395E4197C8F3

LEEF KEY	DESCRIPTION	VALUE
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar
fsize	File size	Example: 131372
msg	Details	Example: Process ID: 884 \nFile: %TEMP% \~DF7A0C28F4D7D9E792.TMP \nType: VSDT_ERROR
pComp	Detection engine / component	Sandbox
ruleCategory	Violated policy name	Example: Internet Explorer Setting Modification
ruleName	Violated event analysis	Example: Modified important registry items
sev	Severity	Value between 0 and 10

**Note**

When using the LEEF log syntax, separate event attributes with <009> as a tab delimiter.

Log sample:

```
LEEF:1.0|Trend Micro|TippingPoint Threat Protection Analyzer|5.5.0.1202|NOTABLE_CHARACTERISTICS|devTime=Feb 28 2015 02:46:33 GMT+00:00<009>devTimeFormat=MMM dd yyyy HH:mm:ss z<009>sev=6<009>pComp=Sandbox<009>dvc=10.204.191.249<009>dvchost=ATPAnalyzer<009>deviceMacAddress=EC:F4:BB:C6:F1:D0<009>deviceGUID=758B04C9-F577-4B8A-B527-ABCB84FDAC83<009>fname=a254i.doc<009>fileHash=7A75D6934C5CDAAF6CA13F8FA4CA03E46DAA7623<009>fileType=Microsoft RTF<009>fsize=86016<009>ruleCategory=File drop, download, sharing, or replication<009>ruleName=Deletes file to compromise the system or to remove traces of the infection<009>msg=Process ID: 884\nFile: %TEMP%\~DF7A0C28F4D7D9E792.TMP\nType: VSDT_ERROR
```

LEEF Virtual Analyzer Analysis Logs: Deny List Transaction Events

TABLE 3-4. LEEF Virtual Analyzer Analysis Logs: Deny List Transaction Events

LEEF KEY	DESCRIPTION	VALUE
Header (logVer)	LEEF format version	LEEF: 1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection Analyzer
Header (pver)	Appliance version	Example: 2.5.0.1161
Header (eventName)	Event Name	DENYLIST_CHANGE
act	The action in the event	• Add • Remove
deviceExternalRiskType	Risk level	• Low • Medium • High • Confirmed Malware
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:56:B3:57
devTime	Log generation time	Example: Jan 28 2015 02:00:36 GMT+08:00
devTimeFormat	Time format	MMM dd yyyy HH:mm:ss z
dhost	Destination host name	Example: dhost1
dpt	Destination port	Value between 0 and 65535
dst	Destination IP address	Example: 10.1.144.199

LEEF KEY	DESCRIPTION	VALUE
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
end	Report end time	Example: Mar 09 2015 17:05:21 GMT+08:00
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5 CAB395E4197C8F3
pComp	Detection engine / component	Sandbox
sev	Severity	Value between 1 and 10
type	Deny List type	- Deny List IP/Port - Deny List URL - Deny List File SHA1 - Deny List Domain
url	URL	Example: http://1.2.3.4/query?term=value

**Note**

When using the LEEF log syntax, separate event attributes with <009> as a tab delimiter.

Log sample:

```
LEEF:1.0|Trend Micro|TippingPoint Threat Protection Analyzer|5.
5.0.1202|DENYLIST_CHANGE|devTime=Feb 28 2015 02:50:03 GMT+00:00
<009>devTimeFormat=MMM dd yyyy HH:mm:ss z<009>sev=3<009>pComp=S
andbox<009>dvc=10.204.191.249<009>dvchost=ATPAnalyzer<009>devic
eMacAddress=EC:F4:BB:C6:F1:D0<009> deviceGUID=758B04C9-F577-4B8
A-B527-ABCB84FDAC83<009>end=Mar 30 2015 02:45:48 GMT+00:00<009>
act=Add<009>fileHash=CF1A6CF231BDA185DEBF70B8562301798F286FAD<0
09>deviceExternalRiskType=High<009>type=Deny List File SHA1
```


Chapter 4

Syslog Content Mapping - TMEF

The following tables outline syslog content mapping between TippingPoint Advanced Threat Protection Analyzer log output and TMEF syslog types:

- *TMEF Virtual Analyzer Analysis Logs: File Analysis Events on page 4-2*
- *TMEF Virtual Analyzer Analysis Logs: URL Analysis Events on page 4-4*
- *TMEF Virtual Analyzer Analysis Logs: Notable Characteristics Events on page 4-6*
- *TMEF Virtual Analyzer Analysis Logs: Deny List Transaction Events on page 4-8*

TMEF Virtual Analyzer Analysis Logs: File Analysis Events

TABLE 4-1. TMEF Virtual Analyzer Analysis Logs: File Analysis Events

TMEF KEY	DESCRIPTION	VALUE
Header (logVer)	TMEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection Analyzer
Header (pver)	Appliance version	Example: 2.5.0.1161
Header (eventid)	Signature ID	200119
Header (eventName)	Description	FILE_ANALYZED
Header (severity)	Severity	3
cn1	GRID is known good	-1: GRID is unknown 0: GRID is not known good 1: GRID is known good
cn1Label	GRID is known good	GRIDIsKnownGood
cn2	ROZ rating	-1: Unsupported file type in ROZ 0: No risk found 1: Low risk 2: Medium risk 3: High risk  Note Other negative values refer to errors.

TMEF KEY	DESCRIPTION	VALUE
cn2Label	ROZ rating	ROZRating
cn3	PCAP ready	0: PCAP is not ready 1: PCAP is ready
cn3Label	PCAP ready	PcapReady
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
deviceOSName	Sandbox image type	Example: win7
deviceProcessHash	Parent SHA1	Example: A29E4ACA70BEF4AF8CE75AF5 1032B6B91572AA0D
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5 CAB395E4197C8F3
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar
fsize	File size	Example: 131372
malName	Malware name	Example: HEUR_NAMETRICK.A
pComp	Detection engine / component	Sandbox
rt	Analysis time	Example: Mar 09 2015 17:05:21 GMT+08:00

Log sample:

```
CEF:0|Trend Micro|TippingPoint Threat Protection Analyzer|5.5.0.1221|200119|FILE_ANALYZED|3|rt=Jun 26 2015 05:29:57 GMT+00:00 pComp=Sandbox dvc=10.204.70.173 dvchost=ATPAnalyzer deviceMacAddress=00:0C:29:69:19:03 deviceGUID=6EDFB737-5EBA-42B7-8D2E-D0789F19FEF4 fname=Establishes_uncommon_connection fileHash=0C450F48E48CEF0B161C254C9E57816CD20FA918 deviceProcessHash=A754E779292F392AE7692D0D2A55D2ECB71B5332 malName=BKDR_NORAWEC.SMG fileType=UPX EXE fsize=149504 deviceOSName=fsdf cn1Label=GRIDIsKnownGood cn1=-1 cn2Label=ROZRating cn2=3 cn3Label=PcapReady cn3=1
```

TMEF Virtual Analyzer Analysis Logs: URL Analysis Events

TABLE 4-2. TMEF Virtual Analyzer Analysis Logs: URL Analysis Events

TMEF KEY	DESCRIPTION	VALUE
Header (logVer)	TMEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection Analyzer
Header (pver)	Appliance version	Example: 2.5.0.1161
Header (eventid)	Signature ID	200126
Header (eventName)	Description	URL_ANALYZED
Header (severity)	Severity	3

TMEF KEY	DESCRIPTION	VALUE
cn2	ROZ rating	-1: Unsupported file type in ROZ 0: No risk found 1: Low risk 2: Medium risk 3: High risk  Note Other negative values refer to errors.
cn2Label	ROZ rating	ROZRating
cn3	PCAP ready	0: PCAP is not ready 1: PCAP is ready
cn3Label	PCAP ready	PcapReady
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
deviceOSName	Sandbox image type	Example: win7
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5 CAB395E4197C8F3
pComp	Detection engine / component	Sandbox

TMEF KEY	DESCRIPTION	VALUE
request	URL	Example: http://www.rainking.net/?utm_campaign=4-21-2014 http://images.rainking.net/eloquaimage
rt	Analysis time	Example: Mar 09 2015 17:05:21 GMT+08:00

Log sample:

```
CEF:0|Trend Micro|TippingPoint Threat Protection Analyzer|5.5.0.1221|200126|URL_ANALYZED|3|rt=Jun 26 2015 05:24:26 GMT+00:00
pComp=Sandbox dvc=10.104.70.173 dvchost=ATPAnalyzer deviceMacAddress=00:0C:29:69:19:03 deviceGUID=6EDFB737-5EBA-42B7-8D2E-D0789F19FEF4 request=https://wx.qq.com:443/ fileHash=BA4AA53108D98F5195D1F490D05716F0B6D7B7EA deviceOSName=fsdf cn2Label=ROZR
ating cn2=-14 cn3Label=PcapReady cn3=0
```

TMEF Virtual Analyzer Analysis Logs: Notable Characteristics Events

TABLE 4-3. TMEF Virtual Analyzer Analysis Logs: Notable Characteristics Events

TMEF KEY	DESCRIPTION	VALUE
Header (logVer)	TMEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection Analyzer
Header (pver)	Appliance version	Example: 2.5.0.1161
Header (eventid)	Signature ID	200127
Header (eventName)	Description	NOTABLE_CHARACTERISITICS

TMEF KEY	DESCRIPTION	VALUE
Header (severity)	Severity	6
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FB8B28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
deviceOSName	Sandbox image type	Example: win7
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5 CAB395E4197C8F3
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar
fsize	File size	Example: 131372
msg	Details	Example: ATSE\nDetection Name: TROJ_FAM_00004f2.TOMA \nEngine Version: 9.826.1078\nMalware Pattern Version: 11.749.92
pComp	Detection engine / component	Sandbox
rt	Analysis time	Example: Mar 09 2015 17:05:21 GMT+08:00
ruleCategory	Violated policy name	Example: Internet Explorer Setting Modification
ruleName	Violated event analysis	Example: Modified important registry items

Log sample:

```
CEF:0|Trend Micro|TippingPoint Threat Protection Analyzer|5.5.0.1221|200127|NOTABLE_CHARACTERISTICS|6|rt=Jun 26 2015 05:24:01 GMT+00:00 pComp=Sandbox dvc=10.204.70.173 dvchost=ATPAnalyzer deviceMacAddress=00:0C:29:69:19:13 deviceGUID=6EDFB737-5EBA-42B7-8D2E-D0789F19FEF4 fname=Sends_email fileHash=1A37D76D3669FC0BF0CBAABB3C149BAC43491663 fileType=WIN32 EXE fsize=92160 ruleCategory=Malformed, defective, or with known malware traits ruleName=Detected as probable malware msg=Source: ATSE\nDetection Name: TROJ_FAM_00004f2.TOMA\nEngine Version: 9.826.1078\nMalware Pattern Version: 11.749.92 deviceOSName=fsdf
```

TMEF Virtual Analyzer Analysis Logs: Deny List Transaction Events

TABLE 4-4. TMEF Virtual Analyzer Analysis Logs: Deny List Transaction Events

TMEF KEY	DESCRIPTION	VALUE
Header (logVer)	TMEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection Analyzer
Header (pver)	Appliance version	Example: 2.5.0.1161
Header (eventid)	Signature ID	200120
Header (eventName)	Description	DENYLIST_CHANGE
Header (severity)	Severity	3
act	The action in the event	- Add - Remove

TMEF KEY	DESCRIPTION	VALUE
cs1	Deny List type	- Deny List IP/Port - Deny List URL - Deny List File SHA1 - Deny List Domain
cs1Label	Deny List type	type
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
deviceExternalRiskType	Risk level	- Low - Medium - High - Confirmed Malware
dhost	Destination host name	Example: dhost1
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
end	Report end time	Example: Mar 09 2015 17:05:21 GMT+08:00
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5 CAB395E4197C8F3
pComp	Detection engine / component	Sandbox
rt	Log generation time	Example: Mar 09 2015 17:05:21 GMT+08:00

Log sample:

```
CEF:0|Trend Micro|TippingPoint Threat Protection Analyzer|5.5.0.1221|200120|DENYLIST_CHANGE|3|rt=Jun 26 2015 05:55:02 GMT+00:00 pComp=Sandbox dvc=10.204.70.17 dvchost=ATPAnalyzer deviceMacAddress=01:0C:29:69:19:03 deviceGUID=6EDFB737-5EBA-42B7-8D2E-D0789F19FEF4 cs1Label=type cs1=Deny List Domain end=Jul 26 2015 05:47:16 GMT+00:00 act=Add dhost=ns1.player1352.com deviceExternalRiskType=High
```

Index



TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: APEM57302/160118