TREND MICRO™

3.0 TREND MICRO™ Deep Discovery Director

Syslog Content Mapping Guide

Breakthrough Protection Against APTs and Targeted Attacks

Endpoint Security

Network Security

Protected Cloud

Document Part No.: APEM38276/180524

Release Date: July 2018

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

Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that Deep Discovery Director collects and provides detailed instructions on how to disable the specific features that feedback the information.

https://success.trendmicro.com/data-collection-disclosure

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Policy:

https://www.trendmicro.com/en_us/about/legal/privacy-policy-product.html

Table of Contents

Preface

Welcome to the Trend Micro Deep Discovery Director (Consolidated Mode) *Syslog Content Mapping Guide*. Learn more about the following topics:

Documentation

The documentation set for Deep Discovery Director (Consolidated Mode) includes the following:

TABLE 1. Product Documentation

DOCUMENT	DESCRIPTION
Administrator's Guide	The Administrator's Guide contains detailed instructions on how to configure and manage Deep Discovery Director (Consolidated Mode), and explanations on Deep Discovery Director (Consolidated Mode) concepts and features.
Syslog Content Mapping Guide	The Syslog Content Mapping Guide provides information about log management standards and syntaxes for implementing syslog events in Deep Discovery Director (Consolidated Mode).
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 Deep Discovery Director (Consolidated Mode) management console. The Online Help contains explanations of Deep Discovery Director (Consolidated Mode) components and features, as well as procedures needed to configure Deep Discovery Director (Consolidated Mode).
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 Deep Discovery Director (Consolidated Mode) 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
Italics	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

Chapter 1

Introduction

The Trend Micro™ Syslog Content Mapping Guide provides information about log management standards and syntaxes for implementing syslog events in Trend Micro Deep Discovery Director (Consolidated Mode).

To enable flexible integration with third-party log management systems, Deep Discovery Director (Consolidated Mode) supports the **Common Event Format (CEF)** syslog format.

CEF is an open log management standard created by HP ArcSight.

Deep Discovery Director (Consolidated Mode) uses a subset of the CEF dictionary.

Chapter 2

Syslog Content Mapping - CEF

The following tables outline syslog content mapping between Deep Discovery Director (Consolidated Mode) log output and CEF syslog types:

- Deep Discovery Inspector logs:
  - *CEF Threat Logs on page 2-2*
  - *CEF Disruptive Application Logs on page 2-7*
  - *CEF Web Reputation Logs on page 2-10*
- Suspicious Objects lists:
  - *CEF Virtual Analyzer Logs: Deny List Transaction Events on page 2-14*

CEF Threat Logs

TABLE 2-1. CEF Threat Logs

CEF KEY	DESCRIPTION	VALUE
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Director (Consolidated Mode)
Header (pver)	Appliance version	Example: 3.0.1200
Header (eventid)	Signature ID	Example: 8
Header (eventName)	Description	Example: Packed executable file copied to a network administrative share
Header (severity)	Severity	• 2: Informational • 4: Low • 6: Medium • 8: High
act	The action in the event	• blocked • not blocked
app	Protocol	Example: HTTP
c6a1	Interested IPv6	Example: 2001:0:0:1::21
c6a1Label	Interested IPv6	Interested IPv6 Address
c6a2	Source IPv6 address	Example: 2001:0:0:1::21
c6a2Label	Source IPv6 address	Source IPv6 Address
c6a3	Destination IPv6 address	Example: 2001:0:0:1::21
c6a3Label	Destination IPv6 address	Destination IPv6 Address

CEF Key	Description	Value
c6a4	Peer IPv6 address	Example: 2001:0:0:1::21
c6a4Label	Peer IPv6 address	Peer IPv6 Address
cat	Event category	Example: File
cnt	Total count	Example: 1
cn1	CCCA detection	0 or 1
cn1Label	CCCA detection	CCCA_Detection
cn3	Threat type	Value between 0 and 4 • 0: Malicious content • 1: Malicious behavior • 2: Suspicious behavior • 3: Exploit • 4: Grayware
cn3Label	Threat type	Threat Type
cs1	Mail subject	Example: hello
cs1Label	Mail subject	MailSubject
cs2	Malware name	Example: HEUR_NAMETRICK.A
cs2Label	Malware name	DetectionName
cs3	Host name	Example: CLIENT1
cs3Label	Host name	HostName_Ext
cs4	Compressed file name	Example: Raider.rar
cs4Label	Compressed file name	FileNameInArchive

CEF KEY	DESCRIPTION	VALUE
cs5	CCCA log is detected by	Examples: • GLOBAL_INTELLIGENCE • VIRTUAL_ANALYZER • USER_DEFINED
cs5Label	CCCA log is detected by	CCCA_DetectionSource
cs6	Attack Phase	Examples: • Intelligence Gathering • Point of Entry • Command and Control Communication • Lateral Movement • Asset and Data Discovery • Data Exfiltration • Nil (no applicable attack phase)
cs6Label	Attack Phase	pAttackPhase
destinationTranslatedAddress	Peer IP	Example: 10.1.144.199
deviceDirection	Packet direction	0, 1, or 2 • 0: Source is external • 1: Source is internal • 2: Unknown
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536

CEF Key	Description	Value
devicePayloadId	An extendable field. Format: {threat_type}:{log_id}:{with pcap file captured}{:extensions}*	Examples: • With pcap file captured: 2:10245:P • Without pcap file captured: 2:10245:
dhost	Destination host name	Example: dhost1
dmac	Destination MAC	Example: 00:0C:29:6E:CB:F9
dpt	Destination port	Value between 0 and 65535
dst	Destination IP address	Example: 10.1.144.199
duser	Mail recipient	Example: duser1
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: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
filePath	File path	Example: SHARE\\
fileType	Real file type	Example: 1638400
flexNumber1	vLANId	Example: 4095
flexNumber1Label	vLANId	vLANId
fname	File name	Example: excel.rar
fsize	File size	Example: 131372
oldFileHash	Mail attachment SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3

CEF KEY	DESCRIPTION	VALUE
oldFileName	Mail attachment file name	Example: excel.rar
oldFileSize	Mail attachment file size	Example: 150000
oldFileType	Mail attachment file type	Example: 1638400
requestClientApplication	User agent	Example: IE
request	URL	Example: http://1.2.3.4/query?term=value
rt	Log generation time	Example: Mar 09 2015 17:05:21 GMT+08:00
shost	Source host name	Example: shost1
smac	Source MAC	Example: 00:0C:29:6E:CB:F9
sourceTranslatedAddress	Interested IP	Example: 10.1.144.199
src	Source IP address	Example: 10.1.144.199
spt	Source port	Value between 0 and 65535
suid	User name	Example: User1
suser	Mail sender	Example: suser1

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Director|3.0.1200|0|Eicar_t
est_file - HTTP (Response)|8|dvc=172.22.9.32 dvcmac=00:50:56
:AD:03:BD dvchost=localhost deviceExternalId=E9A3FA433916-47
38984C-A4BF-84A0-D603 rt=Jun 22 2017 09:42:47 GMT+08:00 app=
HTTP deviceDirection=1 dhost=172.22.9.5 dst=172.22.9.5 dpt=5
7908 dmac=00:50:56:82:e7:a9 shost=172.22.9.54 src=172.22.9.5
4 spt=80 smac=00:50:56:82:c6:ae cs3Label=HostName_Ext cs3=17
2.22.9.54 cs2Label=DetectionName cs2=Eicar_test_file fname=e
icarcom2.zip fileType=262340608 fsize=308 requestClientAppli
cation=Wget/1.12 (linux-gnu) act=not blocked cn3Label=Threat
 Type cn3=0 destinationTranslatedAddress=172.22.9.5 fileHash
```

```
=BEC1B52D350D721C7E22A6D4BB0A92909893A3AE cs4Label=FileName
InArchive cs4=eicar.com sourceTranslatedAddress=172.22.9.54
cnt=1 cat=Malware cs6Label=pAttackPhase cs6=Point of Entry
flexNumber1Label=vLANId flexNumber1=4095 request=http://172
.22.9.54/eicarcom2.zip devicePayloadId=0:143:P
```

CEF Disruptive Application Logs

TABLE 2-2. CEF Disruptive Application Logs

CEF KEY	DESCRIPTION	VALUE
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Director (Consolidated Mode)
Header (pver)	Appliance version	Example: 3.0.1200
Header (eventid)	Signature ID	100120
Header (eventName)	Description	Deep Discovery Inspector detected this protocol in your monitored network.
Header (severity)	Severity	• 2: Informational • 4: Low • 6: Medium • 8: High
app	Protocol	Example: HTTP
c6a1	Interested IPv6	Example: 2001:0:0:1::21
c6a1Label	Interested IPv6	Interested IPv6 Address
c6a2	Source IPv6 address	Example: 2001:0:0:1::21
c6a2Label	Source IPv6 address	Source IPv6 Address

CEF Key	Description	Value
c6a3	Destination IPv6 address	Example: 2001:0:0:1::21
c6a3Label	Destination IPv6 address	Destination IPv6 Address
c6a4	Peer IPv6 address	Example: 2001:0:0:1::21
c6a4Label	Peer IPv6 address	Peer IPv6 Address
cnt	Total count	Peer IPv6 Address
cn3	Threat type	6
cn3Label	Threat type	Threat Type
destinationTranslatedAddress	Peer IP	Example: 10.1.144.199
deviceDirection	Packet direction	0, 1, or 2 • 0: Source is external • 1: Source is internal • 2: Unknown
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
devicePayloadId	An extendable field. Format: {threat_type}:{log_id}:{with pcap file captured}{:extensions}*	Examples: • With pcap file captured: 2:10245:P • Without pcap file captured: 2:10245:
dhost	Destination host name	Example: dhost1
dmac	Destination MAC	Example: 00:0C:29:6E:CB:F9
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

CEF KEY	DESCRIPTION	VALUE
dvchost	Appliance host name	Example: localhost
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
flexNumber1	vLANId	Example: 4095
flexNumber1Label	vLANId	vLANId
rt	Log generation time	Example: Mar 09 2015 17:05:21 GMT+08:00
shost	Source host name	Example: shost1
smac	Source MAC	Example: 00:0C:29:6E:CB:F9
sourceTranslatedAddress	Interested IP	Example: 10.1.144.199
spt	Source port	Value between 0 and 65535
src	Source IP address	Example: 10.1.144.199

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Director|3.0.1200|100120|De
ep Discovery Director detected the protocol in your monitore
d network.|2|dvc=172.22.9.32 dvcmac=00:50:56:AD:03:BD dvchos
t=localhost deviceExternalId=E9A3FA433916-4738984C-A4BF-84A0
-D603 rt=Jun 22 2017 10:06:24 GMT+08:00 app=eDonkey deviceDi
rection=1 dhost=10.1.100.223 dst=10.1.100.223 dpt=4662 dmac=
00:0c:29:a7:72:74 shost=10.1.117.231 src=10.1.117.231 spt=39
933 smac=00:30:da:2d:47:32 cn3Label=Threat Type cn3=6 source
TranslatedAddress=10.1.117.231 destinationTranslatedAddress=
10.1.100.223 cnt=1 flexNumber1Label=vLANId flexNumber1=4095
devicePayloadId=6:11:P
```

CEF Web Reputation Logs

TABLE 2-3. CEF Web Reputation Logs

CEF KEY	DESCRIPTION	VALUE
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Director (Consolidated Mode)
Header (pver)	Appliance version	Example: 3.0.1200
Header (eventid)	Signature ID	100101
Header (eventName)	Description	Example: Dangerous URL in Web Reputation Services database - HTTP (Request)
Header (severity)	Severity	• 2: Informational • 4: Low • 6: Medium • 8: High
app	Protocol	Example: HTTP
c6a1	Interested IPv6	Example: 2001:0:0:1::21
c6a1Label	Interested IPv6	Interested IPv6 Address
c6a2	Source IPv6 address	Example: 2001:0:0:1::21
c6a2Label	Source IPv6 address	Source IPv6 Address
c6a3	Destination IPv6 address	Example: 2001:0:0:1::21
c6a3Label	Destination IPv6 address	Destination IPv6 Address
c6a4	Peer IPv6 address	Example: 2001:0:0:1::21
c6a4Label	Peer IPv6 address	Peer IPv6 Address

CEF KEY	DESCRIPTION	VALUE
cn1	CCCA detection	0 or 1
cn1Label	CCCA detection	CCCA_Detection
cn2	Score	Example: 49
cn2Label	Score	WRSScore
cn3	Threat type	Example: 5
cn3Label	Threat type	Threat Type
cs1	Mail subject	Example: hello
cs1Label	Mail subject	MailSubject
cs2	Category	Example: Gambling
cs2Label	Category	URLCategory
cs3	Host name	Example: CLIENT1
cs3Label	Host name	HostName_Ext
cs4	Attack Phase	• Intelligence Gathering • Point of Entry • Command and Control Communication • Lateral Movement • Asset and Data Discovery • Data Exfiltration • Nil (no applicable attack phase)
cs4Label	Attack Phase	pAttackPhase
destinationTranslatedAddress	Peer IP	Example: 10.1.144.199

CEF Key	Description	Value
deviceDirection	Packet direction	0, 1, or 2 • 0: Source is external • 1: Source is internal • 2: Unknown
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
devicePayloadId	An extendable field.	Examples: • With pcap file captured: 2:10245:P • Without pcap file captured: 2:10245:
dhost	Destination host name	Example: dhost1
dmac	Destination MAC	Example: 00:0C:29:6E:CB:F9
dpt	Destination port	Value between 0 and 65535
dst	Destination IP address	Example: 10.1.144.199
duser	Mail recipient	Example: duser1
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
flexNumber1	vLANId	Example: 4095
flexNumber1Label	vLANId	vLANId
request	URL	Example: http://1.2.3.4/query?term=value
requestClientApplication	User agent	Example: IE

CEF KEY	DESCRIPTION	VALUE
rt	Log generation time	Example: Mar 09 2015 17:05:21 GMT+08:00
shost	Source host name	Example: shost1
smac	Source MAC	Example: 00:0C:29:6E:CB:F9
sourceTranslatedAddress	Interested IP	Example: 10.1.144.199
spt	Source port	Value between 0 and 65535
src	Source IP address	Example: 10.1.144.199
suser	Mail sender	Example: suser1

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Director|3.0.1200|100101|Ra
nsomware URL in Web Reputation Services database - HTTP (Req
uest)|8|dvc=172.22.9.32 dvcmac=00:50:56:AD:03:BD dvchost=loc
alhost deviceExternalId=E9A3FA433916-4738984C-A4BF-84A0-D603
 rt=Jun 22 2017 10:00:17 GMT+08:00 cs3Label=HostName_Ext cs3
 =ca95-1.winshipway.com cn2Label=WRSScore cn2=49 cn3Label=Th
 reat Type cn3=5 dmac=00:16:c8:65:98:d5 shost=172.22.9.5 src
 =172.22.9.5 spt=41757 smac=00:50:56:82:e7:a9 sourceTranslat
 edAddress=172.22.9.5 cn1Label=CCCA_Detection cn1=1 request=
 http://ca95-1.winshipway.com/ requestClientApplication=Wget
 /1.12 (linux-gnu) app=HTTP deviceDirection=1 dhost=150.70.1
 62.115 dst=150.70.162.115 dpt=80 cs2Label=URLCategory cs2=R
 ansomware destinationTranslatedAddress=150.70.162.115 cs4La
 bel=pAttackPhase cs4=Command and Control Communication flex
 Number1Label=vLANId flexNumber1=4095 request=http://ca95-1.
 winshipway.com/ devicePayloadId=5:17:
```

CEF Virtual Analyzer Logs: Deny List Transaction Events

TABLE 2-4. CEF 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	Deep Discovery Director (Consolidated Mode)
Header (pver)	Appliance version	Example: 3.0.1200
Header (eventid)	Signature ID	200120
Header (eventName)	Description	Deny List updated
Header (severity)	Severity	3 (fixed value)
act	The action in the event	• Add • Remove
cs1	Type	• Deny List IP/Port • Deny List URL • Deny List File SHA1 • Deny List Domain
cs1Label	Type	type
cs2	Risk level	• Low • Medium • High
cs2Label	Risk level	RiskLevel

CEF Key	Description	Value
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
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
end	Report end time	Example: Mar 09 2015 17:05:21 GMT+08:00
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
request	URL	Example: http://1.2.3.4/query?term=value
rt	Analysis time	Example: Mar 09 2015 17:05:21 GMT+08:00

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Director|3.0.0.1200|200120|
Deny List updated|3|rt=Jun 28 2018 13:29:55 GMT+08:00 dvc=19
2.168.156.239 dvchost=ddd3-239 dvcmac=00:0c:30:05:a0:8b devi
ceExternalId=FA68DBC5-D354-444C-A834-60352F1A4027 cs1Label=t
ype cs1=Deny List Domain end=Jul 28 2018 13:25:40 GMT+08:00
act=Add dhost=mt6x.ejvu50k.6x.org cs2Label=RiskLevel cs2=Med
ium
```

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: APEM38276/180524