

# **RSA Security Analytics CEF Implementation Guide**

Last Modified: June 22, 2015

# **Partner Information**

Product Information	
Partner Name	CorreLog, Inc.
Web Site	www.correlog.com
Product Name	CorreLog SIEM Agent for IBM z/OS
Version & Platform	5.5.1 z/OS
Product Description	The CorreLog SIEM Agent for IBM z/OS expands the role of your RSA Security Analytics to include real-time mainframe messages from RACF, ACF2, Top Secret, DB2 accesses, File Integrity and other important user activity data relevant to network security. Complete your SIEM strategy leveraging this powerful and unique real-time mainframe security management component.







# **Solution Summary**

The CorreLog SIEM Agent for IBM z/OS collects and forwards events using a CEF format to RSA Security Analytics.

Enabling this feature allows RSA SA customers to monitor, track and act on any actionable event as needed.







# **Release Notes**

Release Date	What's New In This Release
06/22/2015	Initial support for CorreLog SIEM Agent for IBM z/OS.

■ Important: The RSA SA CEF parser is dependent on the integrating partner adhering to the CEF Rules outlined in the ArcSite guidelines document for CEF Header Information. A copy of the Common Event Format guide can be found on <a href="http://protect724.hp.com/">http://protect724.hp.com/</a>.

Eg. Jan 18 11:07:53 host CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|[Extension]

Important: The time displayed in the CEF log header is parsed into evt.time.str. No other time formats are parsed by default.





# Security Analytics Common Event Format Integration Package

The RSA Security Analytics (SA) Community is an online forum for customers and partners to exchange technical information and best practices with each other. The forum also contains the location to download the SA Integration Package for this guide. All Security Analytics customers and partners are invited to register and participate in the <u>RSA Security Analytics Community</u>.

Once you have downloaded the Live package, the next steps are to deploy this on all log decoders.

Note: For steps to disable or remove the Security Analytics Integration Package, please refer to the Appendix of this Guide.

The RSA Security Analytics Common Event Format Integration package consists of the following files:

Filename	File Function
Common Event Format	SA Live package deployed to parse events from device integrations.





# **Deployment Procedure**

In order to use RSA Partner created content, you must first deploy the *enVision Content File* from the **Security Analytics Live** module. Log into Security Analytics and perform the following actions:

- 1. From the Security Analytics menu, select **Live > Search**.
- 2. In the keywords field, enter: enVision.
- 3. Security Analytics will display the Envision Content File in Matching Resources.
- 4. Select the checkbox next to Envision Content File.

@ Live	earch 🛛 🛠 Conf	igure 🔊 F	eeds				
Search Criteria		Matchin	g Resources				
Keywords		📰 Show Res	ults 💿 📔 🔚 Details 🛛 🗐 De	eploy 🔊 Subscribe   💥 P	ackage 🕑		
envision		Subscribed	Name	Created	Updated	Туре	Description
Resource Types		🗹 yes	Envision Content File	2012-02-09 4:44 PM	2015-05-08 8:39 PM	RSA Log Device	This file is used to update the content file f
	~	🗌 yes	Envision Config File	2014-03-07 4:50 PM	2015-05-08 8:38 PM	RSA Log Device	This file is used to update the Log Device base

#### 5. Click **Deploy** in the menu bar.

🔞 Live 🛛 🔍 Se	arch 🛠 Cont	îgure 🔊 Fe	eeds				
Search Criteria		Matching	g Resources				
Keywords		📰 Show Resi	ults 🕙 📔 Details [🖲 De	ploy 🔊 Subscribe   💥 P	ackage 🕑		
envision		Subscribed	Name	Created	Updated	Туре	Description
Resource Types		🗹 yes	Envision Content File	2012-02-09 4:44 PM	2015-05-08 8:39 PM	RSA Log Device	This file is used to update the content file for
	~	🗌 yes	Envision Config File	2014-03-07 4:50 PM	2015-05-08 8:38 PM	RSA Log Device	This file is used to update the Log Device base

#### 6. Select Next.

Deployment Wizard					
Resources	Services	F	Review	Deploy	
Total resources : 1					
Resource Names	Resource	е Туре	Dependency Of		
Envision Content File	RSA Log	g Device			
				Cancel	Next





7. Select the Log Decoder and Select Next.

Deployment Wizard			
Resources	Services	Review	Deploy
Services Groups			
🗆 💋 Name		Туре ^	6
🗌 🥖 vm3090 - IPDB Extractor		IPDB Extractor	
🗹 🥖 vm3093 - Log Decoder		Log Decoder	
		Cancel	Previous Next

8. Select Deploy.

Deployment Wiz	ard		_	
Resources	;	Services	Review	Deploy
Service	Service Type	Resource Name		Resource Type
Service	bernee type	Resource Hume		Resource type
vm3093 - Log D	Log Decoder	Envision Content File		RSA Log Device
			Cancel	Previous Deploy





9. Select **Close**, to complete the deployment of the Envision Config file.

Deployment Wiza	ard			
Resources		Services	Review	Deploy
Service	Service Type	Resource Name		Resource Type
vm3093 - Log D	Log Decoder	Envision Content File		RSA Log Device
			Cancel F	Previous Deploy





# **Deploy Common Event Format**

▶ Note: In order to use RSA Partner created content, you must first deploy the *enVision Content File* from the Security Analytics Live module.

Log into Security Analytics and perform the following actions:

- 10. From the Security Analytics menu, select Live > Search.
- 11. In the keywords field, enter: CEF

Search C	riter	ia	
Keywords			
cef			
Resource Typ	es		
			~
Tags			
			~
Required Met	a Keys		
Generated M	eta Val	ues	
Resource Cre	ated D	ate:	
Start Date	iii	End Date	
Resource Mo	dified D	Date:	
Start Date	iii	End Date	
Search	Car	ncel	

12. Security Analytics will display the Common Event Format in Matching Resources.

🖗 Live 💿 🔍 Search	🛠 Configure 🔊 Feeds					
Search Criteria	Matching Resources	Matching Resources				
Keywords	📰 Show Results 🙁 📔 Details	📰 Show Results 🛛   🛅 Details 💢 Deploy 🔊 Subscribe   🧩 Package 💿				
cef	Subscribed Name	Created Updated	Туре	Description		
Resource Types	🗌 no Common Event Form	at 2014-09-17 8:49 PM 2015-05-08 7:46 PM	RSA Log Device	10.4 or higher.Log Device content for event s		

#### 13. Select the checkbox next to Common Event Format.

🖗 Live 🛛 💿	Search	🛠 Config	ure 🔊 Fe	eds				
Search Criteria		1	Matching Resources					
Keywords			📓 Show Results 🗵   🔚 Defails 📁 Deploy 🔊 Subscribe   💥 Package 🛇					
cef		Ι	Subscribed	Name	Created	Updated	Туре	Description
Resource Types		1	no no	Common Event Format	2014-09-17 8:49 PM	2015-05-08 7:46 PM	RSA Log Device	10.4 or higher.Log Device content for event s

#### 14. Click **Deploy** in the menu bar.

🖗 Live 🛛 🔍	9 Search	🛠 Configure	Feeds					
Search Criteria		Mat	ching Resources	1.14				
Keywords		E Sh	ow Results 🛞 🕴 🔚 Details 🛛 🔝 De	ploy 🔊 Subscribe 🕴 💥 P	ackage 🛞			
cef		🗆 su	bscribed Name	Created	Updated	Туре	Description	
Resource Types		🗹 ni	Common Event Format	2014-09-17 8:49 PM	2015-05-08 7:46 PM	RSA Log Device	10.4 or higher.Log Device content for event s	



15. Select Next.

Deployment Wizard						
Resources	Services	5	Review	N	Deploy	/
Total resources : 1						
Resource Names		Resource Type	Depe	endency Of		
Common Event Format		RSA Log Device				
					_	
					Cancel	Next

16. Select the Log Decoder and Select Next.

Deployment Wizard		
Resources Services	Review	Deploy
Services Groups		
🗆 💋 Name	Туре ^	
🗌 🕖 vm3090 - IPDB Extractor	IPDB Extractor	
🗹 🥖 vm3093 - Log Decoder	Log Decoder	
	Cancel P	Previous Next





17. Select Deploy.



18. Select Close, to complete the deployment of the Common Event Format.

Deployment Wize	ard					
Resources	;	Services		Review		Deploy
Live deployment t	ask finished succes	sfully				
Service Name	Resource Name		Status		Progress	
vm3093 - Log D	Common Event Fo	ormat	1 of 1			
						Close

Note: In an environment with multiple Log Decoders, deploy the Common Event Format to each Log Decoder in your network.





# **Partner Product Configuration**

## **Before You Begin**

This section provides instructions for configuring the CorreLog SIEM Agent for IBM z/ with RSA Security Analytics. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All CorreLog SIEM Agent for IBM z/OS components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

# **Security Analytics Common Event Format Collection**

## CorreLog SIEM Agent for IBM z/OS Configuration

After completing the previous section, *Deploy Common Event Format Content File*, you can now collect events from most sources supporting the Common Event Format (CEF).

To configure the CorreLog SIEM Agent for IBM z/OS software to support the RSA Security Analytics CEF format event messages, follow the installation steps detailed in the CorreLog SIEM Agent for IBM z/OS Installation and Operation guide, and further configuration options in the Configuration Reference guide.

The following excerpts have been taken from the Installation and Operations guide for reference, but it is recommended that you follow the complete instructions in the actual guide.

#### Tailoring the Installation for a Proprietary Syslog Extension

#### **RSA CEF**

Begin your testing by tailoring the following members of *hlq*.CZAGENT.CNTL (where *hlq* is the z/OS filename "high level qualifier" chosen during installation) as indicated in the table below. (To "comment out" a line, type an asterisk in column 3 so the line begins //\*; to uncomment a line, remove the asterisk in column 3 so the line begins with // and a blank.)

Member	Comment out	Uncomment
CZAGENT	// PARMS=CZAPARMS	//* PARMS=CZAPCEF
CZAGNJOB	// SET PRMS=CZAPARMS	//* SET PRMS=CZAPCEF
CZASEND	// SET PRMS=CZAPARMS	//* SET PRMS=CZAPCEF

#### **Parameter File**

The parameter file is normally the CZAPARMS member of the *hlq*.CZAGENT.CNTL dataset (where *hlq* is the "high level qualifier" you specified during installation). For RSA CEF compatibility, use the member CZAPCEF.





## Configuring the SIEM type

Ensure that the CZAPCEF parameter member contains the statement

OPTIONS SIEM(CEF)

to format the SYSLOG output messages to the Common Event Format as required by your RSA Security Analytics system.

#### **Configuring the License statement**

You must obtain a LICENSE statement from CorreLog support. Carefully paste it *without any changes* into the parameter file member between the two lines that read

; Insert the LICENSE statement between these two lines ; Insert the LICENSE statement between these two lines

Do not make any changes to the operands of the LICENSE statement. (Blanks between parameters are not significant.) For example, if your organization name is spelled incorrectly, do not change the LICENSE statement; instead contact CorreLog for a new LICENSE statement.

#### **Configuring the Syslog Server Address**

You must, at a minimum, edit the parameter file and specify the IP address of the RSA Security Analytics console. You must also specify the IP port number if it is not the standard Syslog default, port 514. The IP address and optional port are specified on the SERVER statement in the parameter file as a hostname or in standard IPv4 "dotted" format, for example

SERVER ip. addr. example TRANS(TCP) MAXMSG(3000)

or

SERVER serverx.ourshop.com: 10514

(Parameter file statements are free format. You may use any reasonable number of spaces between the word SERVER and the IP address. The IP address and optional port must be punctuated as shown with no embedded blanks.)

Example CZAPCEF Parameter file in an ISPF Edit Session on z/OS

```
Scroll =
                                                                          CSR
000001 ; CZAPCEF: Parameter file for CZAGENT and CZASEND with CEF compliance
000002
000003 ; Major differences:
000004 ; SIEM(CEF)
000005 ;
          Elimination of SMF30STPD
000006 ;
          TRANS (TCP) MAXMSGLEN (2000)
000007 ;
          HOST HOSTNAME and SMFxxxCAT added to every record type
000008
000009 OPTIONS SIEM(CEF)
000010
000011 ; Insert the LICENSE statement between these two lines
000012 ; Insert the LICENSE statement between these two lines
000013
000014 ; You *MUST* edit the SERVER statement per the install documentation
000015 SERVER ip.addr.example TRANS(TCP) MAXMSG(3000) ; You MUST edit per doc
000016
000017 ; Uncomment and edit the following TIME statement if desired
000018 ; TIME UTC DUR(ISO8601 T) TIMEOFDAY(ISO8601 T) ZONE(TZ)
000019
```





## **Certification Checklist for RSA Security Analytics**

Certification Environment						
Product Name	Version Information	Operating System				
RSA Security Analytics	10.4	Virtual Appliance				
CorreLog SIEM Agent for IBM z/OS	5.5.1	z/OS				

Security Analytics Test Case	Result
Device Administration	
Partners device name appears in Device Parsers Configuration	$\checkmark$
Device can be enabled from Device Parsers Configuration	$\checkmark$
Device can be disabled from Device Parsers Configuration	$\checkmark$
Device can be removed from Device Parsers Configuration	$\checkmark$
Investigation	
Device name displays properly from Device Type	$\checkmark$
Displays Meta Data properly within Investigator	$\checkmark$
DRP / PAR	✓ = Pass × = Fail N/A = Non-Available Function

Date Tested: June 22, 2015





## **Known Issues**

RSA Partner Engineering identified an issue with the RSA SA CEF parser when collecting and parsing cn1, cs3 and cs5 elements. The cn1, cs3 and cs5 elements cannot be viewed or parsed as a result. The issue is being investigated by RSA engineering at the time this guide was published.





# Appendix

## Security Analytics Disable the Common Event Format Parser

To disable the Security Analytics Common Event Format Parser and not delete it perform the following:

1. Select the Security Analytics **Administration > Services menu**.



2. Select the Log Decoder, then select View > Config.

	vm3093 - Log Decoder	0	vm3093	Log Decoder	10.4.0.1.3351	0
•	vm3095 - Concentrator	0	vm3095	Concentrator	System	View >
					Stats	Delete
					Config	Edit
					Explore	Start
					Logs	Stop
					Security	Restart
					1	

3. From the **Service Parses Configuration** window, scroll down to the CEF parser and uncheck the Config Value checkbox.

Service Parsers Configuration		Enable All	Disable All
Name	Config Value		
caitm			<b>^</b>
casiteminder			=
cef	$\checkmark$		

4. Click Apply to save settings.





#### **Security Analytics Remove Device Parser**

To remove the Security Analytics Integration Package files from the environment, perform the following:

1. Connect to the Security Analytics Log Decoder/Collector Server using SSH and open the /etc/netwitness/ng/envision/etc/devices folder.



2. Search for and delete the CEF folder and its contents.



