# RSA<sup>®</sup> NETWITNESS<sup>®</sup> Security Operations Implementation Guide

Secdo Platform

Jeffrey Carlson, RSA Partner Engineering Last Modified: November 27<sup>th</sup>, 2017





### **Solution Summary**

Secdo integrates with RSA NetWitness to automatically correlate alerts with historical and real-time endpoint data to reveal the full context of each alert – including root cause, attack chain, damage assessment, and more. Secdo offers a wide array of surgical response and remediation tools, enabling rapid, remote, and precise containment and cleanup of all threats from any one or several endpoints or servers at once. Secdo provides unmatched endpoint visibility at the thread-level – the single-most granular view possible into endpoints – along with insights and unlimited querying capabilities, to enable threat hunting of advanced and new attacks missed by other detection systems. Secdo makes it easy for security teams to create their own traditional or behavioral indicators of compromise (IOCs or BIOCs) to proactively identify and clock activity that matches or resembles the criteria provided.

Per	sernalina tyaWrap.exe			·····					4 1440
2	NEER PRESENCE (175				10.1.07				-
	ALERTS -		0	0	0 0	8			
* ¥	EXAMPLE :	•	•		• •	•			
0. 	ADDELTS DARELTION +	1			14 1414			•	
t	1410A0 10111	-	4		-	h			
10	THESTAND			1994	***	**			
0	29-8-2013 160 023	Petyderap.see	Dana Osbarne	tangung	142	943	write to 198 yusuddriwyd		
	28-8-2017/08:10.54	#F0.01#	Daniel Babarre	Persidency	402	7540	Greated schwitzeled lank		
.0	28-8-207108-1054	parent and	Daniel Oxforme	Lateral Movement	\$206	944	PE file dropped on ADMINK shares		
	284.207.0815-0	Petpathtap.ore	Devisitiobarrie	PotScaring	542	540	Surved entire subrat for SVB share		
	28-0-2017/08/50118	Perjultrupane	Darkel Optione	Asteral Mountered	942	9429	Surprises connection attempt on service SMB purit		





### **RSA NetWitness Configuration**

RSA NetWitness sends alerts and events to Secdo Platform via CEF-formatted syslog messages. For more information on the out of the box CEF Meta Keys in RSA NetWitness visit: <u>https://community.rsa.com/docs/DOC-74333</u>

1. Login to the RSA NetWitness System:



2. Navigate to Administration > Services > Reporting Engine > Actions > View > Config:

Administration 🔍 🖛 Hosts 🛛 Services	Cvent Source	s 🔍 Health & Wellness	🗮 System	Security							0
Groups	Services										7
+ - 🛛 C	+ 0 - 2	📔 🚟 Licenses 🛞							🕈 🛞 Filter		×
Name	Name	5e ~			Licensed	Host	Туре	Version		Actions	
⊖ All	🗊 🗹 😐 ՠ	vybrid - Reporting Engine			0	nwhybrid	Reporting Engine	10.6.2.0		۰ 🗘	
	• • • • • • • • • • • • • • • • • • •	ybrid - Packet Decoder			۲	nwhybrid	Decoder	10.6.2.0	System View	v >	
	• • • • • • • • • • • • • • • • • • •	ybrid - Malware Analysis			۲	nwhybrid	Malware Analysis	10.6.2.0	Explore Edit	ete	
	🗆 🔶 nwt	ybrid - Incident Management				nwhybrid	Incident Management	10.6.2.0	Logs Sta	τ	
	🗆 😐 met	ybrid - Concentrator			0	nwhybrid	Concentrator	10.6.2.0	Res	tart	
	O me	salog - Log Decoder			0	nwesalog	Log Decoder			0	
	0 o me	salog - Log Collector			0	nwesalog	Log Collector			•	
	0 mm	salog - Event Stream Analysis			0	nwesalog	Event Stream Analysis			•	
	0 mm	salog - Context Hub			0	nwesalog	Context Hub			•	
	0 o me	salog - archiver			0	nwesalog	Archiver			•	

### Secdo Secdo Platform

3. Next, click on the **Output Actions** tab and scroll down to the **Syslog Configurations** section.

Administration =	- Isosis	Services	A livert Source	s Thea	th & Wellness	a tystem	Security
Change Service	🛙 nwhybrid - R	sporting Engine	Confg ⊕				
General Sources	Output Ac	tions Manage	loge				
Concession in the local division in the loca	1.4400						
ADDAY							
Syslog Configu	rations						
+ - 2							
2 Syring Name - 1	Investing	(mar)	Part	Max larger	Intensity Dring	Dataset Pres	
D OEMAA, SYS. 1	/10	locefront :	.514	2048		000	
CETO CARBAILE	and a second						
SETP Configure	ations						
*	100	11222	1.0		0102101		
LI - WIT Name -	- mest	Pyrt	- United and	. 0	anow Auder	Evalue Compression	
		SETP Config	puration in Repo	stillig Engin	e.		

- 4. Create a new syslog output using the + button and add the data shown in the image below.
- 5. Set the Server Name to the IP or FQDN of the SECDO server you will be forwarding Syslog events too.

New Syslog Cor	nfiguration	۱		
Syslog Name *	SECDO			
Encoding *	UTF8			
Server Name *	10.10.10.1	0		
Server Port *	514	٥		
Max Length *	2048	0		
Identity String				
Include the loc	al hostname	in syslo	g messages.	
Truncate overl	y large syslog	g messaj	ges.	
Optionally use	IDENT proto	col.		
Include the loc	al timestamp	in syste	g messages.	
Transport Protocol *	UDP		~	
			Cancel	Save

6. Click Save.



### Secdo Secdo Platform

7. Navigate to the **Reports** section.

Dashboard		
Dashboard	ard < 👳 🕂 🗕 🗹 🛛   🐌 Å 🖄   < Share 🛛	
Investigation	>	2014
A⊬ Incidents	·	E.GX
Alerts	> (	() ±
🕍 Reports 💦 🔥		
🔊 Administration	>	_
n Live	<b>&gt;</b>	
1 Profile		_
🖒 Sign Out		
0	EMPTY ALERT	_

8. Next, click on the **Alerts** button under the **Manage** tab, then the **Template** button.

anage	View			
Rules	Reports	Charts Alerts Lists W	arehouse Analytics	
lert			_	
+ - 2	l 😐 Enab	le 🔿 Disable   😋 🏟 🛛 🔳 🎞 Temp	late 🛄 View Schedule 🖓 View Alerts	
	Durhad 2	Mama	Description	
Enabled	Pusrieu r	Harric	Description	
Enabled	Yes	Suspected Gh0st RAT	Description	
Enabled	Yes Yes	Suspected Gh0st RAT File Upload from Critical Systems to Dynamic	DNS	
Enabled	Yes Yes Yes	Suspected Gh0st RAT File Upload from Critical Systems to Dynamic Phishing_Attempt	DNS	
Enabled     Enabled     enabled     enabled	Yes Yes Yes Yes	Suspected Gh0ss RAT File Upload from Critical Systems to Dynamic Phishing_Attempt Phishing - Obfuscated Zip Attachment	DNS	

9. Now create a new **Template** as show below.

CEF:0|RSA|NetWitness|10.6.2|\${statement}|\$severity}| src={sourceAddress} dst=\${destinationAddress} spt=\${sourcePort} dpt=\${destinationPort} rt=\${timestamp}

### Secdo Secdo Platform

cate mov	any remplote
Name	SECDO
Message	<u>CEP.018SA1NetWitness110.6.2</u> [\$istatement]]\$(severity)] <u>src=\$(sourceAddress)</u> <u>dst=\$(destinationAddress) spt=\$(sourcePort</u> ) dpt=\$( <u>destinationPort</u> ) rt=\$( <u>timestamp</u> )
	Correl Control

10. Edit the alert that you would like to syslog to SECDO on the **Alerts** page under the **Manage** tab.

Manaş	ge View		
Rule	Reports	Charts Alerts Lists Ware	house Analytics
Aler	t		
-			
+ -	- 🗹 🔍 Ena	ble 🔿 Disable 🕴 🖸 🍄 🐵 🕴 🧱 Templat	te 🇰 View Schedule 😪 View Alerts
+ -	wbled	ble O Disable   O 🕹 🗉   🏛 Templat	e 🇰 View Schedule 🚭 View Alerts Description
+ -	whied total d 7	ble O Disable   O I Templat Name Suspected Gh0st RAT	e III View Schedule & View Alerts Description
+ - - m - m	wbled rate d 7 Yes	ble O Disable   O 😫 😑   🚟 Templat Name Suspected GN0st RAT File Upload from Critical Systems to Dynamic Di	e III View Schedule & View Alerts Description
	wbied Con d 7 Yes Yes	ble O Disable   O & I Templat Name Suspected GN0st RAT File Upload from Critical Systems to Dynamic DI Philshing_Attempt	e III View Schedule & View Alerts Description
	Ves     Yes	ble O Disable   O Bable   E Templat Name Suspected GN0st RAT File Upload from Critical Systems to Dynamic DI Philshing_Attempt Philshing - Obfuscated Zip Attachment	te III View Schedule & View Alerts Description





#### Secdo Secdo Platform

11. Make sure to check the Syslog checkbox as shown below, then add a new Syslog config as shown below.



- 12. Now click on the + to add the Syslog Server
- 13. The following window will popup. Fill it out as shown below. Note that selecting the Body Template **SECDO** will populate the **Body** field:

Syslog Configs	SECDO	~		
Execute	Each event	~		
Facility	Local7 (23)	~		
Severity	Warning	~		
Body	CEF:0 RSA Net severity}  src={ dst=\${destination dpt=\$destination	Witness 10.6.2 sourceAddress onAddress} spt onPort} rt=\${tin	: \${statement} \$ } =\$sourcePort} nestamp}	
Body Template	SECDO	~		

14. Click Save.





15. Now you should see the following:

M Reports	0			0 🕫
Manage	View [ALRT] Suspected Gh0st RAT O			
Create/Mo	odify Alert			
Enable	8			
Rule Basis:	Suspected Ghöst RAT Browse			
Data Sources:	nwhybrid - Concentrator 🛛 👻 Push to decoders			
Description				
Severity:	High v			
Notification	Record SMTP SNMP System			
	Record SMTP SNMP Syslog			
	+ - 🗵			
	🗹 Sysleg Name ^	Execute	Severity	Facility
	⊠ secoo	FOR_EACH	WARNING	LOCAL7

16. Now click **save** and you're finished.

### **Partner Product Configuration**

#### **Before You Begin**

This section provides instructions for configuring Secdo with RSA NetWitness. 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 Secdo components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

**!** Important: The configuration shown in this Implementation Guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure Secdo is properly configured and secured before deploying to a production environment. For more information, please refer to the Secdo documentation or website.

### Secdo Configuration

Create an overview of the steps that will be taken to provide interoperability. Use the overview steps as headings for each section as you document the integration.

1. Login to Secdo, and switch to the relevant company.

#### Secdo Secdo Platform

2. Navigate to <a href="https://secDOIP>/#/siemConfigurations">https://secDOIP>/#/siemConfigurations</a>.

•	SIEM CONFIGURATIONS secto -		3	ini 10 1M 20-04-2017 18:20:49 - 21-05-:
SECO	SUMMARY Currently Showing 570735 Alerts in Total		inore ID secdo_id_570906	
V		1.00 million 100		
18128		[ UNWAPPED ]	connets pource:udp:514[host:100.64.3.249]cef	(INDEXTIME 1494485689
*Q			3183AL 570912	.si scdianspi001,main
6	SIGALIT SIGAL(\$75699)	sourcetype	71M8 1494485689	ACTION close
ę	+ FORTINET FORTINET(18)	Alert Category   Please Select	*	
鼎	+ FORTINET FORTIGATE(18)	Secdo Field	Alert Field Value	Formatted Value
11				

- 3. On the left side of the screen, the vendor/product pair should be seen once an alert in RSA NetWitness has been triggered.
- 4. Click on the new vendor/product pair



- 5. Click Unmapped.
- 6. Choose the relevant **Alert Category**, for example, **Outgoing connection event**.

¢	ID se	cdo_id_570939		>
				Q
	_CONFSTR source::udp:514 ho	it::100.64.3.249 forti	INDEXTIME 1495383549	
NV 1	SERIAL		, <b>Si</b> sedianspi001,main	
,SOURCETYPE forti	,TIME 1495383549		ACTION	
Alert Category   Please Sele	vet v			
Secdo Field	Alert Field	Value	Formatted Value	

### Secdo Secdo Platform



7. Map the marked fields that are mandatory to map the alert with the data from the alert field by field

	ID see	do_id_570939			
					(Q)
[	converts more selection/more selection	100.04.3.249(4)/6	Name of Street o		
and a second sec	hand handstelete		achias (itee		
Aver Calogory ( Dagong Calo	ector faces -				
heads field	Aburt Panta	Table		Remained Value	
• BIDD, Sheeramp		- hereaster		sessates	-
<ul> <li>НОЩовани, ф</li> </ul>	Sou	- NE21E734.101		14,252,04.940	-
+ BIDIO pasaros Australian	Sec. 1	. tetre		2miles	-
···· B000 destination (b	2 mile	- 192, 194, 200 14		112 148,250 18	
· BIOD, destruction, features	1000	- Defer		24794	
- 90000, dominantes, per	Deport -	. 40		-	

- 8. Hit Save and Apply.
- 9. Navigate to <u>https://<SECDOIP>/#/siemapp</u>
- 10. See the new alerts in the **Alerts** screen:

SIEM CONFIGURATIONS	secdo -				24H   7D   1M	20-04-2017 19:25:0
Case Analysis	Alerts					
ALL 20 CASI	ES O SYSTEM ERRO	DRS 18				
TIMESTAMP	VENDOR T	PRODUCT T	HOST NAME	туре	CCO NAME T	PROCESS NAME
21-05-2017 19/19/09	Check point	firewall-1	Cr-Laptop	Network	chrome.exe	chrome.exe
21-05-2017 19:19:09	Check point	firewall-1	T Or-Laptop	Network	chrome.exe	chrome.exe
21-05-2017 18:18:09	fortinet	fortigate	Pr-Laptop	Network	svchost.exe	svchost.exe
21-05-2017 18:18:09	fortinet	fortigate	Tor-Laptop	Network	svchost.exe	svchost.exe

### Secdo Secdo Platform

- Or-Laptop | chrome.exe | 1632 FILTER -OR-LAPTOPher 4 OBLAPTOPH ORLAPIOP Q 0 0 + T CAUSE SIGNATURE SUSPICIOUS USER NAME PATH ene:
- 11. Right-click the relevant line and click on **Open Card** to see the event details:



### **Certification Checklist for RSA NetWitness**

Date Tested: October 20<sup>th</sup>, 2017

Certification Environment					
Product Name	Version Information	Operating System			
RSA NetWitness	10.6.4	Virtual Appliance			
Secdo Platform	5.0				

RSA NetWitness Test Case	Result
Inline Query/Enrichment	
Query NetWitness for IP Info (source/destination IP)	N/A
Query NetWitness for User Info (usernames, user behavior)	N/A
Query NetWitness for Specific Meta (Other)	N/A
Retrieve NetWitness Log/Packet Data	N/A
Retrieve NetWitness PCAP files	N/A
Alerting / Incident Creation	
NetWitness alert via syslog	✓
NetWitness alert via email	N/A
NetWitness alert via ESA/scripting	N/A
Send alert to NetWitness (Syslog, CEF, or custom parser)	N/A
RSA NetWitness Intel Feeds	
Update NetWitness Intel Feed (CSV, STIX)	N/A

 $\checkmark$  = Pass  $\times$  = Fail N/A = Non-Available Function

