# CyberHound



a Hewlett Packard Enterprise company

## ClearPass

#### **Change Log**

Version	Date	Modified By	Comments
V2019-01	Feb 2019	Jason Atkins	Initial Document Release

#### Copyright

© Copyright 2017 Hewlett Packard Enterprise Development LP.

#### **Open Source Code**

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett- Packard Company. To obtain such source code, send a check or money order in the amount of US \$10.00 to:

Hewlett-Packard Company Attn: General Counsel 3000 Hanover Street Palo Alto, CA 94304 USA

Please specify the product and version for which you are requesting source code. You may also request a copy of this source code free of charge at <u>HPE-Aruba-gplquery@hpe.com</u>.

## ClearPass and CyberHound Integration

#### Contents

Introduction and Overview	5
Software Requirements	5
ClearPass Installation and Deployment Guide	6
CyberHound Prerequisites	7
CyberHound Initial Configuration	7
CyberHound IPS Configuration	8
ClearPass Ingress Event Engine	9
Check Inbound Event Notification is Enabled	9
Check the Ingress Services are running	10
Batch Processing Interval	10
Configure the Ingress Event Dictionary for CyberHound	11
Enable Radius Accounting and Change of Authorization on Network Device	12
Adding a CoA Delay (Optional)	12
Add an Event Source	13
Add Endpoint Dictionary Attributes	13
Building ClearPass Events and Actions	15
Create the Event Service Policy and Profiles	15
Add New Enforcement Profiles	15
Add a New Enforcement Policy	
Create Event Service Policy	19
Create an Authentication Service Policy	20
Creating a Quarantine Captive Portal Page	21
Configuring a ClearPass Captive Portal	21
Removing a Device from Quarantine	22
Access Tracker Results	23
Appendix 1 – IEE_CyberHound.xml file	25

#### **Figures**

Figure 1: CyberHound and ClearPass Integration Overview	5
Figure 2: CyberHound Enable ClearPass IP addressIntegration	7
Figure 3: CyberHound test settings	7
Figure 4: CyberHound IPS Category Configuration	8
Figure 5: ClearPass Enable Ingress Event Engine	9
Figure 6: ClearPass Services Control	10
Figure 7: ClearPass Batch Processing Interval	
Figure 8: ClearPass Ingress Event Dictionaries	
Figure 9: ClearPass Event Dictionary list	
Figure 10: ClearPass CoA Delay	
Figure 11: ClearPass Adding an Event Source	13
Figure 12: ClearPass Adding an Event Source	
Figure 13: ClearPass New Endpoint Attributes	14
Figure 14: Example workflow	
Figure 15: Add Post Authentication Enforcement Profile	
Figure 16: ClearPass Enforcement Profile Examples	17
Figure 17: ClearPass New Event Enforcement Policy	
Figure 18: ClearPass Event Enforcement Policy Rules	
Figure 19: ClearPass Event Service Policy	
Figure 20: ClearPass select the Enforcement Policy	19
Figure 21: ClearPass Authentication Service Policy Enforcement	
Figure 22: ClearPass Find Endpoint	22
Figure 23: ClearPass Endpoint Attributes	22
Figure 24: ClearPass Access Tracker	23



#### www.arubanetworks.com 1344 Crossman Avenue Sunnyvale, CA 94089 Phone: 1-800-WIFI-LAN (+800-943-4526) Fax 408.227.4550

© 2017 Hewlett Packard Enterprise Development LP. All Rights Reserved.

## **Introduction and Overview**

This guide covers the setup required to integrate CyberHound's Advanced Threat Management system with Aruba ClearPass Policy Manager.

The integration provides ClearPass with "real time" event messages for devices identified (by CyberHound) as generating malicious network traffic including Malware, Viruses, Botnets, Vulnerabilities, Worms and more.

Utilizing the Ingress Event Engine [IEE] available in Aruba ClearPass, the "real time" event messages from CyberHound can trigger event workflows in ClearPass to automate a response to Block or Quarantine authenticated devices on the network.

The diagram below describes the end-to-end workflow utilizing CyberHound to discover the malicious traffic and ClearPass to enforce the isolation of the device on the network.



Figure 1: CyberHound and ClearPass Integration Overview

#### **Software Requirements**

The minimum software version required for ClearPass is 6.7.2. At the time of writing, ClearPass 6.7.9 is the latest available and recommended release. Any subsequent ClearPass software release will support this integration. ClearPass runs on either hardware appliances with pre-installed software, or as a Virtual Machine under the following hypervisors. Hypervisors that run on a client computer such as VMware Player are not supported.

- VMware ESXi 5.0, 5.1, 5.5, 6.0, 6.5 or higher
- Microsoft Hyper-V Server 2012 or 2016 R2
- Hyper-V on Microsoft Windows Server 2012 or 2016 R2
- KVM on CentOS 7.5 or later

The minimum software release for CyberHound UTM is V31.7.1.

### **ClearPass Installation and Deployment Guide**

This document assumes your ClearPass environment is already configured and operational. If you require assistance with basic deployment, refer to the following deployment guide: <a href="http://www.arubanetworks.com/techdocs/ClearPass/Aruba\_DeployGd\_HTML/Default.htm">http://www.arubanetworks.com/techdocs/ClearPass/Aruba\_DeployGd\_HTML/Default.htm</a>

## **CyberHound Prerequisites**

You will need the following in order to complete this integration.

- CyberHound version 31.7.1
- A valid CyberHound UTM license
- CyberHound IPS Module installed (please refer to the CyberHound documentation for minimum resource specification)

Please contact CyberHound Support if you require access to the CyberHound IPS module.

## **CyberHound Initial Configuration**

To implement ClearPass integration and apply automated network policy actions, go to **Advanced Firewall > IPS Configuration** and select '**Enabled'** for both **IPS Rules Engine** and **Aruba ClearPass Integration**. Specify the host name or IP address of your ClearPass Policy Manager. Multiple ClearPass Policy Managers are support with comma separated entries.

IPS Rules Engine Settings		4.5	
Enable IPS Rules Engine [Control whether the IPS Rules engine is active. Using the Extended IPS rule set may have performance impacts and can increase the risk of false positives.]	Enabled	~	
Configure Flow Based IPS [ Configure the IPS actions to take, based on threat type and severity ]	Edit	-	
Enable Aruba Clearpass Integration [Control whether the IPS will communicate with Aruba ClearPass ]	Enabled 🗸		
Remote ClearPass servers [Comma separated list of IP addresses or hostnames of remote servers.]	10.33.113.200	<u>ا</u>	
Network Exclusions [ Configure IPS Rules Engine IP-based exclusions ]	Edit		
IPS Rule Overrides [Manage user overridden rules ]	Configure		
Geo IP Management [Configure Geo IP based rules]	Configure		
		Update & Test Settings	Update

Figure 2: CyberHound Enable ClearPass IP addressIntegration

To finalize the configuration, Click Update and test the settings.



Figure 3: CyberHound test settings

## **CyberHound IPS Configuration**

IPS and Network Policy actions may be applied on a 'per category' and 'severity' level basis.

Threat Type	Severity	IPS Action	Clearpass Action
Denial of Service	Severity 0	Drop 🗸	Block 🗸
Denial of Service	Severity 1	Drop 🗸	Quarantine 🗸
Denial of Service	Severity 2	Alert 🗸	Ignore 🗸
Denial of Service	Severity 3	Alert 🗸	Ignore 🗸

Figure 4: CyberHound IPS Category Configuration

*For example:* Denial of Service threats with a severity level 0 (most severe) will be identified and dropped by the CyberHound. To enforce an additional Aruba Clearpass network policy such as quarantining or blocking the offending device from connecting to the network, simply select the desired Clearpass action.

The following matrix outlines the actions that are available to be sent to ClearPass Policy Manager.

Event Action	Description
Block	Instruct ClearPass to dynamically disconnect and block the infected device from rejoining the network.
Quarantine	Instruct ClearPass to dynamically transfer the infected device into a predefined quarantine network
lgnore	Will not send events to ClearPass

By Default, IPS rules are configured to alert only and no threat intelligence feed is transmitted to ClearPass.



ClearPass actions for Block and Quarantine will be sent as syslog events to ClearPass for processing. Please ensure these events do not exceed 100 events per minute.



Note: Optional 3<sup>rd</sup> party IPS event log management may be configured to use additional Remote syslog servers based on log source. This may be used in conjunction with the ClearPass integration. To configure go to *Configuration > Remote Syslog* and specify the 3<sup>rd</sup> party host.

#### **ClearPass Ingress Event Engine**

The integration between ClearPass Policy Manager and CyberHound is driven through a ClearPass capability known as the Ingress Event Engine [IEE]. This feature is part of the ClearPass Exchange Framework and provides ClearPass with the ability to consume inbound syslog messages. Once ingested, ClearPass will parse the message and trigger an event in the form of an Enforcement update for the device.

#### **Check Inbound Event Notification is Enabled**

By default, the IEE feature is disabled. To enable IEE go to **ClearPass Policy Manager > Administration > Server Manager > Server Configuration > [Your CPPM Node] > System**.

Administration » Server Manager » Server Server Configuration - clea	rpass.nb (	10.3.100.1)		
System Services Control Service	Parameters	System Monitoring	Network	FIPS
Hostname:	clearpass.nb			
FQDN:	clearpass.nb			
Policy Manager Zone:	default			
Enable Performance Monitoring Display:	Z Enable this	server for performa	nce monitoring	display
Insight Setting:	Z Enable Ins	ght 🔽 E	nable as Insig	ht Master
Enable Ingress Events Processing:	Enable Ing	ress Events processi	ng on this serv	er
Master Server in Zone:	Primary master	0		

Figure 5: ClearPass Enable Ingress Event Engine

Note when enabling this feature, a warning message is displayed which highlights and warns of the potential consequences. Be aware that IEE processing can generate a significant CPU load on the node. Careful consideration needs to be used and we specifically do not want ClearPass to receive a constant stream of syslog messages that ClearPass will need to process. **ClearPass should only be receiving syslog messages**, **by exception, that it needs to take action on**. If you send a constant stream of syslog then the overhead will likely cause the node to become CPU bound and the potential failure/timeout of the primary function, the Authentication of Users/Computers. **Do not exceed 100 events per minute hitting the IEE**.



Additional guidelines for enabling the IEE feature can be found in the Tech Note titled "ClearPass Ingress Event Engine" which is available for download on the Aruba Support web site (https://support.arubanetworks.com).

### **Check the Ingress Services are running**

Please ensure the Ingress services have been started on the ClearPass node by clicking on the "Services Control" TAB.

Admin	istration » Server Manager » Server Con	figuration - clearpass.nb		
Ser	ver Configuration - clearpas	s.nb (10.3.100.1)		
Syst	em Services Control Service Para	meters System Monitoring Network F	IPS	
-	Service Name		Status	Action
1.	AirGroup notification service	and the second second	Running	Stop
2,	Async DB write service		Running	Stop
3.	Async network services		Running	Stop
4,	ClearPass IPsec service		Running	Stop
5.	DB change notification server		Running	Stop
6.	DB replication service		Running	Stop
7.	Extensions service		Running	Stop
8.	Guest Background Service		Running	Stop
9.	Guest Cache		Running	Stop
10.	Ingress logger service		Running	Stop
11.	Ingress logrepo service		Running	Stop

Figure 6: ClearPass Services Control

#### **Batch Processing Interval**

The batch processing interval determines the frequency for the event engine to check the EventDB for new entries. For testing purposes, you can reduce the batch processing interval to 10 seconds to make the processing of events more "real time". It's recommended to leave this value at 30 seconds for production environments.

Administration * Serv	/er Manager = Server Configurati	ion – ciearpass.nb		
Server Configu	uration - clearpass.nb	(10.3.100.1)		
System Services	Control Service Parameters	System Monitoring Network FIPS		
Select Service:	Async network services	8		
-	Parameter Name	Parameter Value	Default Value	Allowed Values
Ingress Event	Parameter Name	Parameter Value	Default Value	Allowed Values

Figure 7: ClearPass Batch Processing Interval

### **Configure the Ingress Event Dictionary for CyberHound**

As of ClearPass 6.7.9, the CyberHound IEE dictionary is NOT installed by default and will need to be imported before it can be used. As a reference the CyberHound dictionary is provided in the appendix of this document, however our experience has shown that copying and pasting the text and saving it to a local XML file can lead to spurious characters being added depending on the text application being used.



We prefer that you download the file from our support site directly to your local device, you can find it in this folder, Note: support credentials are required to access this location.

https://support.arubanetworks.com/DownloadSoftware/tabid/75/DMXModule/510/EntryId/22752/Default.a <a href="mailto:spx">spx</a>

Once download, the dictionary can be installed *Administration > Dictionaries > Ingress Events > Import* 

Admi	nistrati	ion * Dictionaries * Ingress Events			-
Ing This p	ress	Events Dictionaries			Import Export All
Filter	: Vende	or 🕒 contains 😋 💽 💽 🕢	r s	Show 20	E records
#		Import from file	0		Status
1.					Disabled
2.		Select File: Browse IEE_cyberhound.xml		lg l	Disabled
з.		Enter secret for the file (if any):		1000	Enabled
4.				1000	Disabled
5.				18.07	Disabled
6.					Disabled
7.				ss	Disabled
8.				rs	Disabled
9,				rs	Disabled
10,				rs	Disabled
11		import	Gancel	TS.	Disabled

Figure 8: ClearPass Ingress Event Dictionaries

Once imported, the CyberHound dictionary should be automatically enabled and visible in the list.

Admin	istrati	ion » Dictionaries » Ingres	ss Events			
Ingr	ess	Events Dictionari	es			Import Export Al
			Add	ded 1 Events Dictionary		- cohoire th
This p	age al	llows you to enable or exp	ort Ingress Events Dictionarie	25.		
Filter:	Venda	or	contains	Go Clear Filter	Sho	ow 20 🖸 récord
-	_					
		Vendor .	Format Name		Prefix	Status
1.	0	Vendor  Aruba IntroSpect	Format Name IntroSpect-Action-Syst	log	Prefix IntroSpect-SS	Status Disabled
1. 2.	0.0	Vendor  Aruba IntroSpect Check Point	Format Name IntroSpect-Action-Syst CheckPoint-Log	log	Prefix IntroSpect-SS CheckPoint-Log	Status Disabled Disabled
1. 2. 3.	0.0.0	Vendor  Aruba IntroSpect Check Point CyberHound	Format Name IntroSpect-Action-Sysl CheckPoint-Log CyberHound-SIEM-Stri	log uctured-Syslog	Prefix IntroSpect-SS CheckPoint-Log CyberHound	Status Disabled Disabled Enabled

Figure 9: ClearPass Event Dictionary list

## Enable Radius Accounting and Change of Authorization on Network Device

ClearPass will receive the IP address of the malicious device via the Event message from CyberHound. ClearPass will use Radius Accounting to identify the current session for that IP address which, in turn, will provide the Policy Engine with the MAC Address of the malicious device. Once the MAC Address is known, ClearPass will be able to write details to the Endpoint Repository and also issue Radius Terminate message to disconnect the intended device.

Please ensure;

- 1. Network Access Device is configured to send Radius Accounting to ClearPass
- 2. Both the Network Access Device and ClearPass are configured for Radius CoA

#### Adding a CoA Delay (Optional)

If you would like to disconnect devices after an event is received then you may need to add a delay to the triggering of the CoA message. This will allow ClearPass to write the Endpoint Attributes to the database before the device automatically reconnects. This value may need to be tweaked depending on your cluster design. For this example the delay will be set to 10 seconds. Go to *Administration > Server Manager > Server Configuration > [select your node]* and open the **Service Parameters** TAB.

Administration * Server Manager * Server Configuration - dearpass.nb Server Configuration - clearpass.nb (10.3.100.1)									
System Services Select Service:	Control Service Parameters	System Monitoring Ne	twork FIPS						
	Parameter Name	Paramet	er Value	Default Value	Allowed Values				
Ingress Event									
Batch Processing Inte	rval	10	seconds	30	10-300				
Command Control									
CoA Delay		10	seconds	2	0-15				

Figure 10: ClearPass CoA Delay

### Add an Event Source

The IP address of the CyberHound appliance must be added before ClearPass before incoming events will be processed. The new event source can be configured under *Configuration* > *Network* > *Event Sources* > *ADD*.

Config	uratio	n * Network	» Event Sources				_		-	
Ever	nt So	ources							4	Add Import Export All
The ev ignore	vent si d.	ource is the d	levice that sends	s Syslog events to ClearPass, ,	Any events sent l	hat are not f	rom configure	ed event sources a	ire	
			Edit Event Sou	Irce	•	and Ciller			Chow an	E recorde
Filter:	Name		Name:	Swanlake		lear rinter	-		SHOW 20	records
#		Name .	Description:	Swanlake Netbox			Туре	Vendor		Status
1.		oldrel		The second s			Syslog	CyberHound		Enabled
2.		Suphound			11.	1000	Syslog	CyberHound		Enabled
3.		Swanlake	IPAddress:	10.107.11.108		1000	Syslog	CyberHound		Enabled
4.		Test	Type:	Syslog	0		Syslog	CyberHound		Enabled
Showi	00 1-4	lof 4	Vendor:	CyberHound	0				Export	Delete
SHOWI	ing 1-4	014	Enable:						- schon	Detore
				Sav	Cancel					
						1000				

Figure 11: ClearPass Adding an Event Source

#### **Add Endpoint Dictionary Attributes**

To ensure that the CyberHound events do not affect other endpoint attributes it is recommended that you create three (3) new attributes specifically for the CyberHound integration.

Go to Administration > Dictionaries > Dictionary Attributes and click ADD.

Admi	inistra	tion » Dictionaries » Diction	nary Attributes			
Dic	tion	ary Attributes				Add Add Export Export All
The / endp	Attribu oints,	utes dictionary page allows and devices,	you to specify unique sets	s of criteria for local users	, guest users,	
Filter	: Nar	ne 😒	contains 📀	<u>⊕</u> Go 0	lear Filter Show	20 🖸 records
#		Name 🔺	Entity	Data Type	Is Mandatory	Allow Multiple
1.	D	[airgroup_enable]	GuestUser	String	No	No
2.	10	[airgroup shared]	GuestUser	String	No	No

Figure 12: ClearPass Adding an Event Source

Next, create three (3) new Endpoint attributes (screen shots on next page)

- 1. CyberHound\_Event\_Action (as string)
- 2. CyberHound\_Event\_DateTime (as date-time)
- 3. CyberHound\_Event\_ThreatName (as string)

Add Attribute		2
Entity	Endpoint	0
Name	CyberHound_Event_Action	
Data Type	String	0
Is Mandatory	🗇 Yes 💿 No	
Allow Multiple	Yes 💿 No	
Default Value (optional)		(Enter String without special characters e.g., firstfloor)
		Add Cancel

Add Attribute				0
Entity	Endpoint			
Name	CyberHound_Event_DateTime			
Data Type	Date-Time	0		
Is Mandatory	🔿 Yes 🧿 No			
Default Value (optional)				
			Add	Cancel

Add Attribute		
Entity	Endpoint	
Name	CyberHound_Event_ThreatName	
Data Type	String	3
Is Mandatory	🗇 Yes 🧿 No	
Allow Multiple	🗇 Yes 💿 No	
Default Value (optional)		(Enter String without special characters e.g., firstfloor)
		Add

Figure 13: ClearPass New Endpoint Attributes

The initial setup of ClearPass is now completed.

## **Building ClearPass Events and Actions**

The next phase of the configuration is to write a service policy to process the incoming Events and trigger the appropriate actions. This will involve the creation of Enforcement Profiles, Enforcement Policies and Event Services.

The following workflow will be used to demonstrate the integration between CyberHound and ClearPass. Your environment may require a modified workflow so please feel free to modify as required.



Figure 14: Example workflow

#### **Create the Event Service Policy and Profiles**

When creating the Event Service Policy it is best to work from right to left by creating the Enforcement Profiles, Enforcement Policies before finally creating the Event Service Policy.

#### **Add New Enforcement Profiles**

Go to **Configuration > Enforcement > Profiles** and click the ADD option. Use the "ClearPass Entity Update Enforcement" template to create a Post\_Authentication enforcement profile.

Configuration » Enforcer Enforcement Pro	nent » Profiles » Add Enforcement Profile ofiles
Profile Attributes	Summary
Template:	ClearPass Entity Update Enforcement 🛛 🟮
Name:	CyberHound Quarantine
Description:	Quarantine Event
Type:	Post_Authentication

Figure 15: Add Post Authentication Enforcement Profile

Create three (3) enforcement profiles, one for each action sent by CyberHound (Quarantine, Block and Ignore). The Enforcement Profile will write attributes to the Endpoint repository which will be used to take action on the device.

Attribute	Value
Endpoint.CyberHound_Event_ThreatName	%{Event:CyberHound:threat}
Endpoint. CyberHound_Event_Action	Choose between Quarantine or Block
Endpoint. CyberHound_Event_DateTime	%{Event:CyberHound:eventdatetime}

En	forcement	rofiles - CyberHound QUARANTINE				
S	ummary Pro	Attributes				
Pro	file:	and the second se				
Nar	ne:	CyberHound QUARANTINE				
Des	scription:	Quarantine event				
Тур	e:	Post_Authentication				
Act	ion:					
Dev	vice Group List:					
Att	ributes:					
Туре		Name Value				
1.	Endpoint	CyberHound_Event_ThreatName = %{Event:CyberHound:threat}				
2.	Endpoint	CyberHound_Event_Action = Quarantine				
3.	Endpoint	CyberHound_Event_DateTime = %{Event:CyberHound:eventdatetime}				

Er	forcem	ent Pro	ofiles - Cy	berHound BLOCK				
s	Summary Profile Attributes							
Pro	file:		1.0	- A				
Na	me:		CyberHou	Ind BLOCK				
De	scription:		Block eve	nt				
Тур	be:		Post_Aut	nentication				
Act	ion:							
De	vice Group	List:	2497					
Att	ributes:							
	Туре			Name		Value		
1.	Endpoint			CyberHound_Event_ThreatName	=	%{Event:CyberHound:threat}		
2.	Endpoint			CyberHound_Event_Action	=	Block		
3.	Endpoint			CyberHound_Event_DateTime	=	%{Event:CyberHound:eventdatetime}		

Enforcem	Inforcement Profiles - CyberHound IGNORE					
Summary	Profile	Attributes				
Profile:		and the second se				
Name:		CyberHound IGNORE				
Description:		Ignore event				
Type:		Post_Authentication				
Action:						
Device Group	List:					
Attributes:						
Туре		Name		Value		
1. Endpoir	it	Threat Category	-	Ignore		

Figure 16: ClearPass Enforcement Profile Examples

#### Add a New Enforcement Policy

Create a new enforcement policy that will react to the "action" received from CyberHound. If the event action is Quarantine or Block then database update will occur and then a terminate message will also be sent to force the device to disconnect from the network.

When creating the Enforcement Policy, make sure you select the Enforcement Type of EVENT. See image below for clarification.

Configuration » Enfo	ient » Policies » Add	
Enforcement	cies	
Enforcement R	Summary	
Name:	CyberHound Enforcement Policy	
Description:		
Enforcement Type:	🔿 RADIUS 🔿 TACACS+ 🔿 WEBAUTH (SNMP/Agent/CLI/CoA) 🔿 Application 💿 Ev	ent
Default Profile:	[Post Authentication] CyberHour	

Figure 17: ClearPass New Event Enforcement Policy

Set the Default Profile to the "CyberHound IGNORE" Profile

Go to the Rules TAB and configure the policy rules to match the CyberHound Actions.

Enforcement Policies - CyberHound Enforcen Summary Enforcement Rules	ment Policy
Rules Evaluation Algorithm: <b>•</b> Select first match <b>•</b> Select all r	matches
Conditions	Actions
1. (Event:CyberHound:action EQUALS Quarantine)	CyberHound QUARANTINE, [ArubaOS Wireless - Terminate Session]
2. (Event:CyberHound:action EQUALS Block)	CyberHound BLOCK, [ArubaOS Wireless - Terminate Session]
	Add Rule Move Up↑ Move Down↓ Edit Rule Remove Rule

Figure 18: ClearPass Event Enforcement Policy Rules

### **Create Event Service Policy**

Go to **Configuration > Services > Add**. Select the type of "Event-based Enforcement"

Configuration * Services *	Add		
Services	City and the second second		
Service Enforcement	Summary		
Туре:	Event-based Enforcement		
Name:	CyberHound_Ingress_Event		
Description:	Service for ingress events based enforcement		
Monitor Mode: More Options:	Enable to monitor network access without enforcement	nt	
		Service Rule	
Matches ANY or O AL	L of the following conditions:		
Туре	Name	Operator	Value
1. Click to add			

Figure 19: ClearPass Event Service Policy

Go to the Enforcement TAB and select the Enforcement policy you created earlier.

Services - CyberHo	ound_Ingress_Event			
Summary Service	inforcement			
Use Cached Results:	Use cached Roles and Posture attributes	from previous sessions		
Enforcement Policy:	CyberHound Enforcement Policy	Modify Add New Enforcement Policy		
	Enforcer	nent Policy Details		
Description:				
Default Profile:	CyberHound IGNORE			
Rules Evaluation Algorithm:	first-applicable			
Conditions	the second s	Enforcement Profiles		
1. (Event:CyberHound:	action EQUALS Quarantine)	CyberHound QUARANTINE, [ArubaOS Wireless - Terminate Session]		
2. (Event:CyberHound:	(Event: CyberHound:action EQUALS Block) CyberHound BLOCK, [ArubaOS Wireless - Terminate Session			

Figure 20: ClearPass select the Enforcement Policy



When using the EQUALS operator in the condition statement, the text entered is the value is case sensitive.

#### **Create an Authentication Service Policy**

Use the ClearPass Service Template & Wizard to create a working authentication service policy that matches your requirements. Configuring the service policy from scratch is not detailed in this document.

For this example I have created a simple 802.1X Service Policy that authenticates users that are in the "staff" AD group.

Next, I will modify the Enforcement Policy to check the "*Endpoint.CyberHound\_Event\_Action*" field in the Endpoint Repository.



Make sure you add the Endpoint Repository as an Authorization Source to your Service Policy.

Services	- Mercury	y SSID				
			Note: This	Service is	s created by Se	ervice Template
Summary	Service	Authentication	Authorization	Roles	Enforcement	
Use Cached I	Results:	Use cached I	Roles and Posture	attributes	from previous	sessions
Enforcement	Policy:	Mercury DOT1X			0	Modify
				Enforce	ment Policy Det	ails
Description:						
Default Profi	le:	Mercury Limite	ed Access			
Rules Evalua	tion Algorithm	: first-applicable	e			
Conditi	ions					<b>Enforcement Profiles</b>
1. (Endp	oint:CyberHou	ind_Event_Action	EQUALS Block)	(		[Deny Access Profile]
2. (Endp	oint:CyberHou	ind_Event_Action	EQUALS Quara	ntine)		Quarantined
3. (Autho	(Authorization:HOME-AD:groupName EQUALS staff) Mercury Full Access					

Figure 21: ClearPass Authentication Service Policy Enforcement

### **Creating a Quarantine Captive Portal Page**

The result of quarantining clients on the network will vary depending on your specific requirements. In any case, the Enforcement Profile will return a radius attribute to the network access device which will place the device in a quarantined user role or maybe a quarantine VLAN.

The quarantine user role on an Aruba Mobility Controller or Aruba Instant AP may be configured to forward the user to a Captive Portal.

When redirecting users to a Captive Portal it is a good idea to display a message that identifies the issue so they can easily convey this information to the help desk.

#### **Configuring a ClearPass Captive Portal**

Our preference is to re-use one of the default pages to create the quarantine page.

- 1. Go to *ClearPass Guest* then select *Configuration* > *Pages* > *Web Pages*.
- 2. Duplicate the "WebCC Blocked" page and call it **cyberhound\_quarantined**.
- 3. Edit your new page and set the Title field to "Quarantined!".
- 4. Copy the following HTML code into the HTML field.

```
<link href="external/font-awesome/css/font-awesome.min.css" rel="stylesheet"</pre>
type="text/css">
<div style="width: 300px; margin: 0 auto; text-align: center;">
<!--
   refer to http://fortawesome.github.io/Font-Awesome/examples/ for icon docs
   -->
 <span class="fa-stack fa-lg" style="font-size: 100px; color: #FFF;">
  <i class="fa fa-ban fa-stack-1x"></i>
 </span>
<h1 style="margin: 20px 5px;">Device Quarantine</h1>
You have been Quarantined due to the network traffic generated by your
device.Please contact a network administrator to resolve this issue.
<b>Device IP Address:<fre>{$smarty.server.REMOTE ADDR|escape}<br />
 <b>Device MAC Address:</b> {$_endpoint.mac address|escape}<br />
 <b>Threat Name:</b> {$ endpoint.CyberHound Event ThreatName|escape}<br />
</div>
```



#### **Removing a Device from Quarantine**

The example workflow created in this document relies on the **manual clearing** of the device before connectivity can be restored for the device in question. To do this, the ClearPass Administrator will be required to find the device in the EndPoint Repository using it's MAC address and then clear the "Threat" attributes.

Firstly, go to **Configuration > Identity > Endpoints** and search for the MAC Address.

Configu	uration	» Identity » Endpo	ints			
Endp	oint	s				
This pa laptops Filter:	ge aut s, smar MAC Ad	omatically lists all a t phones, tablets, e Idress	uthenticated endpoints. An end tc.),	point device is an Internet-capable	e hardware device on a T(	CP/IP network (e.g.
#		MAC Address	Hostname	Device Category	Device OS Family	Status
1.	П	b853ac9a4671	jason.iphone7	SmartDevice	Apple	Known
Showin	g 1-1	of 1	Authentication Records	Bulk Update Bulk Delete	Trigger Server Action	Update Fingerprint

Alternatively, you can list all endpoints with the **CyberHound\_Event\_Action** flag set by searching for an attribute.

Filter:	Attribute	•	equals 🗘	cybe 🔹 co	ontains 📀 Quarantine	*	+ Go	Clear Filter
#		MAC Address	Host	CyberHound_Event_Action	Device Category	D	evice OS I	Family
1.	0	b853ac9a4671	jason	CyberHound_Event_ThreatN	lame SmartDevice	A	pple	

Figure 22: ClearPass Find Endpoint

Click the Endpoint and select the Attributes TAB. You will need to DELETE the Threat Attributes and bounce the device off/on the network.

Edit	Endpoint						
E	ndpoint	Attributes	Device Fingerprints	Poli	cy Cache		
	Attribut	e			Value		
1.	CyberHo	und_Event_Ac	tion	=	Quarantine		T
2.	CyberHo	und_Event_Da	ateTime	=	2018-02-20 09:11:00	6	Ŧ
з.	CyberHo	und_Event_Th	nreatName	=	ET TROJAN Overtoolbar.net Backdoor ICMP Checkin Response	<b>B</b>	Ť
4.	Last Kno	wn Location		=	192.168.0.232:Office-205		T
5.	Last_SSI	ID		=	Mercury		T

Figure 23: ClearPass Endpoint Attributes

## **Access Tracker Results**

Access Tracker will display incoming Radius authentications and Events from CyberHound.

Monito	oring » Live Monitori 255 Tracker Fet ccess Tracker page p	ng » Access Tracker o 20, 2019 13:48:37 AEDT provides a real-time display	of per-session acc	ess activity on the selected	server or domain.	🕑 Auto Refresh
	[All Requests]	mercury.clearpas	ss.info (192.168.0.)	250)	ng Last 1 da	iy before Today
Filter:	Host MAC Address	contains 😒 467	1	Go Clear Filter		Show 20 C records
- 20	Source	Host MAC Address	Username	Service	Login Status	Request Timestamp Enforcement Profile
1.	RADIUS	b853ac9a4671	jason	Mercury SSID	ACCEPT	2019/02/20 13:48:12 Quarantined
2.	Event	b853ac9a4671	Jason	CyberHound_Ingress_	ACCEPT	CyberHound 2019/02/20 13:48:01 QUARANTINE, [ArubaOS Wireless - Terminate Session]
3.	RADIUS	b853ac9a4671	jason	Mercury SSID	ACCEPT	2019/02/20 13:47:11 Update Endpoint, Mercury Full Access

#### Figure 24: ClearPass Access Tracker

Let me explain the workflow depicted in the Access Tracker images above. The **#number** below indicates the line number for the messages seen above.

**#3** – User 'jason' connects to the Mercury SSID using EAP-TLS and is granted "Mercury Full Access".

In the background a Radius Accounting Start message hits ClearPass to map the MAC Address 'b853ac9a4671' to IP Address '192.168.0.37'.

User 'jason' is going about his work until CyberHound notices some malicious traffic coming from his IP Address. CyberHound fires a syslog event at ClearPass

**#2** – ClearPass receives an Event message via the IEE. The message has an action of 'Quarantine' and provides the IP Address of the device causing the issue.

ClearPass performs a lookup of the active sessions and returns the MAC Address (which can be seen in #2 above).

ClearPass writes the attribute 'Threat Category' = 'Quarantine' to the Endpoint DB.

ClearPass issues a Radius CoA to the Access Point to terminate the session for the MAC Address in question.

**#1** – The device automatically reconnects to the Mercury SSID. The Endpoint Repository is used as an Authorization Source and the 'Threat Category' attribute will contain 'Quarantine'. The Enforcement Profile results in an Aruba-User-Role = 'Quarantine' being returned to the Access Point.

The Access Point has a User Role called 'Quarantine' which places the device in a Captive Portal role which points to the 'cyberhound\_quarantined' web page.

## Appendix 1 – IEE\_CyberHound.xml file

The following text can be copied and saved as an XML file for upload to ClearPass as an Event Dictionary.

<pre></pre> <pre>&lt;</pre>
<pre><pre></pre><pre></pre><pre></pre></pre>
<ingressevents></ingressevents>
<ingressevent></ingressevent>
<formatname>CyberHound-SIEM-Structured-Syslog</formatname>
<pre><pormat>syslag_priority,version,syslag_datetime,host1,host2,host3,var1,eventdatetime,action,infectedhost1P,threat</pormat> <pre></pre></pre>
<enabled>true</enabled>
<pre><sample.slt;1346gt;1 "dave"="" (ips-clearpass)="" 10="" 10.3.103.100="" 11:40:03="" 12="" 15:50:37="" 2018-10-10="" block="" et="" ips-clearpass[18760]:="" oct="" overtoolbar.net<="" pre="" swanlake="" trojan="" xi=""></sample.slt;1346gt;1></pre>
<pre>stackgoor LCMP Checkin Kequest <filter>filter&gt;filter</filter></pre>
grok (
match = sqt; { 'message' = sqt;
<pre>alts(revsin(systad) = (rsitsystad) = (rsitsyst</pre>
) if ("CyberHound" in [fags]) {
mutate {
<pre>add field =&gt; [ 'Event:priority', '% [syslog priority}' ] add_field ==ft, [ 'Event:priority' = 15(priority)' ]</pre>
add_iteld =sqt; [ 'Event:Username', '{username'}]
add_field => [ 'Event:Source-IP-Address', '%{infectedhostIP}' ]
add_field =sgt; [ 'Event:Event-Name', '%[threat]'] add_field =srt; [ 'Event:Event-Name', '%[threat]']
add_leid = sgr. [ 'Event:Timestamp', '% (syslg datetime)' ]
add_field => [ 'Event:device-vendor', 'CyberHound' ]
add_field =&gf [ 'Event:action', '%{action}' ]
ruby (
code =sgt; "
data = event.close.clo
<pre>if (!k.start_with?('Event:') and !k.start_with?('@'))</pre>
newFieldName = 'Event:CyberHound:'+ k event[newFieldName] = v
event.remove(k)
end
ena tstamp = Time.now.to i
<pre>tstamp_str = Time.at(tstamp).strftime('%Y-%m-%d %H:%M:%S')</pre>
event['Event:Timestamp'] = tstamp_str
<pre>//filer/ <pre></pre></pre>
<field allowedvalues="" datatype="Integer" name="syslog_priority"></field>
<field allowedvalues="" datatype="Integer" name="version"></field>
<pre><field allowedvalues="" datatype="String Name=" host1"=""></field></pre>
<field allowedvalues="" datatype="String" name="host2"></field>
<field allowedvalues="" datatype="String" name="nost3"></field> <field allowedvalues="" datatype="String" name="usi1"></field>
<pre><field allowedvalues="" datatype="String" name="eventdatetime"></field></pre>
<field allowedvalues="" datatype="String" name="action"></field>
<pre><rractu "batatupe="String" aitowedvalues="bataTupe=" name="threat" string"=""></rractu></pre>
<pre><genericfieldmapping> </genericfieldmapping></pre>
<pre></pre>
<field genericname="Source-IP-Address" name="infectedhostIP"></field>
/cinetichieldMapping /cinetichieldMapping