VMware Carbon Black Threat Remediation with Workspace ONE Intelligence

This lab is for the purposes of understanding the integration with Workspace ONE Intelligence and VMware Carbon Black Cloud. You will be required to do a little pre-work to setup the requirements for the integration. Once those are setup you will be able to demo carbon black policy enforce a blacklist policy virtual machine in to Workspace ONE and push out the VMware Carbon Black Sensor installer and connect it to the correct org. We will look at how a threat with it's various severities can be detected by policies we create inside VMware Carbon Black.

Next we will see how Workspace ONE Intelligence is ingesting this information and taking action to re-mediate an issue on that device.

There are four parts to this Lab

- 1. Downloading the VMware Carbon Black Sensor
- 2. Workspace ONE UEM & VMware Carbon Black Sensor Integration
- 3. Workspace ONE IntelligenceAPI integration & Automation
- 4. VMware Carbon Black Incident & Workspace ONE Intelligence Automation

NOTE: Screenshot precedes Instructions in this lab



Part 1: Downloading the VMware Carbon Black Sensor

- 1. On your ControlCenter server
 - Open your Chrome browser
 - Launch a web page to your Carbon Black tenant using the following URL https://defense-prod05.conferdeploy.net
 - On the Sign in page. User your email address and the password VMware1!
 - Select Sign In

• Use the credentials created above to authenticate as administrator.



View company codes
Download sensor kits
Send installation request (Windows and macOS)

ACTIONS

- 2. On your ControlCenter server
 - On the VMware Carbon Black Console
 - On the left navigation pane, expand Inventory
 - Select ENDPOINTS
 - On the top right-hand corner, select the **drop down** next to **Sensor Options**.
 - Select Download sensor kits

NOTE: If you do not see the options on the left pane, reduce the Page Zoom by Navigating to the menu options on top right and click on minus sign.

Download	Sensor	Kits
----------	--------	------

earn more about sensors from: Supported Operating Systems, Sensor Release Notes, and the Sensor Installation Guide				
os	SENSOR VERSION	ACTION		
Windows 64-bit	3.7.0.1503 ~		Download Kit	

- 3. In the VMware Carbon Black Console
 - Select Download Kit next to Windows 64-bit from the Download Sensor Kits page.
 - (Be sure to download the latest)

IF you do not see the Save File as shown above, come back to the VMware Carbon Black Cloud admin console and right-click on Download Kit next to Windows 64-bit and click Save Link As... and then click Save

Close your Carbon Black Cloud Administration Console

This concludes Part 1, please proceed to Part 2

Part 2: Workspace ONE UEM & VMware Carbon Black Sensor Integration

In this lab we will create a software distribution package to install VMware Carbon Black Sensor silently (unattended) using Workspace ONE UEM.

The lab parts are as follows:

- 2.1: Create VMware Carbon Black Sensor installation package through WorkspaceONE UEM
- 2.2: Change Windows 10 Name and IP Address
- 2.3: Observe Device behaviour in VMware Carbon Black console

 \times

2.1: Create VMware Carbon Black Sensor installation package through Workspace ONE UEM

Workspace ONE [™] UEM
Username
Your Email Address
Next
Trouble logging in

1. On the **ControlCenter** server

- Open a **new tab** in Google Chrome
- Navigate to your Workspace ONE UEM admin console with the following URL (https://cn-livefire.awmdm.com)
 - Enter your custom Username, select Next
 - In the **Password** area, enter your **custom password** select **Log in**
 - If prompted close the Workspace ONE UEM Console Highlights window

🖏 Workspace ONE UEM				
GETTING	Groups	~		
STARTED	Organization Groups	>		
₩.	User Groups	\rightarrow		
MONITOR	Assignment Groups			
	App Groups	\rightarrow		
DEVICES	Admin Groups	\rightarrow		
	All Settings	Ø		
嵤	Configurations			
ACCOUNTS				
APPS & BOOKS				
CONTENT				
EMAIL				
C				
GROUPS & SETTINGS				
https://dw-livefire.aw	mdm.com/AirWatch/#/SmartGrou	<		

- 2. In the Workspace ONE UEM Console
 - Navigate to GROUPS & SETTINGS
 - Select Groups
 - Select Assignment Groups

Groups Organization Groups User Groups	× >	Groups & Settings > Groups Assignment Group)S
Assignment Groups	→	Filters » O ADD SM	ART GROUP
Admin Groups All Settings	→ 2	All Corporate Dedicated Devices	Herbertvogal@gmail.com
Configurations		All Corporate Shared Devices	Herbertvogal@gmail.com

- 3. In the Assignment Groups window
 - Select + ADD SMARTGROUP

ame	W10Client01a Managed By Herbertvogal@gmail.com
100se Type	CRITERIA DEVICES OR USERS
Devices	
Devices	
Devices	
Herbertvo	gal@gmail.com VMware Virtual Platform 1 eeATTE
Herbertvoga x86_64_358	gal@gmail.com VMware Virtual Platform 1 eeATTE ADD I@gmail.com Android X1X0Android_Android SDK built for 1240051111110
Herbertvo Herbertvoga x86_64_358	gal@gmail.com VMware Virtual Platform 1 eeATTE ADD I@gmail.com Android X1X0Android_Android SDK built for 240051111110 I@gmail.com VMware Virtual Piatform 1 eeATTENDEE200

- 4. In the Create New Smart Group window
 - Next to Name enter: W10Client01a
 - Next to Choose Type, select DEVICES OR USERS
 - When prompted with a warning message, select **OK**
 - Under **Devices**:
 - Select the Device which you have re-named and enrolled in the introduction section
 - Select ADD



- 5. In the Create New Smart Group window
 - Select **SAVE** in the bottom right corner.



- 6. In the Workspace ONE UEM Console
 - Navigate to Apps & Books > Application > Native
 - Select ADD under the Internal tab

• Select Application File

Add Applicatio	n			
Organization Group	xenlaforman			
Application File*			PLOAD	
Com	wheely a		A fact freed	×
Departure - New Tabler				0 • 11 0
Article annone Constant annone Constant annone Constant annone Constant anno Constant anno	ykny gener (m. 1996) gener (m.	Externational Indication fraction Individual fraction	Spe Fitchler Windons Indeller	Scor 40,000 08
Plename installe	r,vitta,win7,win0-64-3.7.8.1253zmi		 All Files (1/1) Open 	Cancel
Add			×	
Type 🔘 Loca	l File 🔾 Link			
Choo	se File installe97	9.msi		
You have used	0 MB of 20000 MB			
	5/	VE CA	INCEL	
Add		×		
Type 🖲 Local	File OLink			
Choose	File installe_973 msi			
You have used 0	MB of 2000 MB			
	SAVE CA	ICEL		

- 7. In the Add Application window
 - Next to Organization Group ID, leave this default
 - Next to Application File, select UPLOAD
 - 1. Select Choose File and a new window will open,
 - 2. Navigate to the **Download Folder** in the left navigation bar and select the msi you downloaded earlier.
 - 3. Select the **installer....msi** and select **Open**.
 - 4. Select **SAVE** on the final Add page this will upload the application.

Add Application	×
trigenzation finales 10 ⁴	
Apphasion File* Installer_instag	web 46332 11278 w.cea
app ¹ YES	
	CONTRAIT CANCEL
Edit Appli	cation - Carbon Black Cloud Sensor 64-bit
Internal Manage	d By VLS CarbonBlack Application ID: (17431189-140A-4774-8065-CSSE8272F8E1) App Stc.
Details Files Deployer	ent Options Images Terms of Use
Managed By	W.S Carbordlack
Application ID*	(17431189-140A-4774-8065-C55682226861)
Actual File Version *	3 5 8 1627
Build Version	(TOCCE425-8853-4443-8725-422480140186)
Supported Processor	falar v 0
Architecture	2-34 64 32
Chastellor	
Change Log	, e
	SAVE & ASSIGN CANCEL
Edit Ao	alication Carbon Diack Claud Concor 64 bit
EUIL Ap	Menaged Bickeniaforman Application ID: (17431189-1404-4774-8065
	8
Details Files	Deployment Options Images Terms of Use
	manarapi mana-mananini 🖬 🗸
Command "	
Admin Privileg	es yes no ()
Device Restart	Do not restart 👻 🕕
	Do not restart
Retry Count*	User-engaged restart
Retry Interval	5
	SAVE & ASSIGN CANCEL

- 8. In the Add Application window
 - Select **CONTINUE** to verify the application file and that it is not a dependency
 - In the Add Application Carbon Black Cloud Sensor 64-bit window
 - On the **Details** tab
 - Scroll down to Supported Processor Architecture
 - Change it from **32 bit** to **64-bit**
 - Select the Deployment Options tab
 - Scroll down to the Install Command field
 - Paste the *install parameter* from below into the Install Command Field
 - Replace the existing install command in that field already. Ensure the version of Sensor is correct
 - If you typing in the COMPANY_CODE, the number 8 is followed by 'O' and not Zero. (Common Mistake)
 - msiexec /q /i "installer_vista_win7_win8-64-3.7.0.1503.msi" /L*vx Log.txt COMPANY_CODE=S17NA79RWX!K8OJLXA3
 - Scroll further down Deployment options tab
 - Next to Device Restart select "User-engaged restart"
 - Select SAVE & ASSIGN

NOTE: The Company Code determine the VMware Carbon Black Cloud environment and can be retrieve from the VMware Carbon Black admin console. In an environment where you have Super admin rights, you can verify the company code by Navigating to ENDPOINTS > SENSOR OPTIONS > COMPANY CODES in the VMware Carbon Black portal. However, in this lab environment you have only read only access and so this option is not available.

	Carbon Black Sensor for Windows
Description	Assignment Description
Assignment Groups *	To whom do you want to assign this ap;
Assignment Groups * To whom do you	u want to assign this app? retringatignation (X)
Assignment Groups * To whom do you (WhoCherofuche Deployment Begins * 04/04/2021	u word to assign the app? destroyal@pria.com.X
Assignment Groups * To whom do you WOODentoteen Deployment Begins * OK/04/2021 App Delivery Method * O Auto	u want to assign the app? rennogal@penal.com X <u>1200</u> <u>AM ~</u> (GMT-05:00) Eastern Time (US & Canada <u>0</u> On Demand
Assignment Groups * To whom do yo (WOCcentifielde Deployment Begins * 06/04/2021 App Delivery Method * 0 Auto Hide installation Midd installation	u want to assyn the app? Termogational com X
Assignment Groups * To whom do yoo WHOCenetologe Deployment Begins * Oel/04/2021 App Delivery Method * • 04/04/2021 Hide installation Notifications * Notifications *	u want to atsign this app? Intertogat§prais.com X On Demand C C C

- 9. On the Carbon Black Cloud Sensor 64-bit- Assignment page,
 - Under **Distribution** enter next to :
 - Name: Type Carbon Black Sensor for Windows
 - Assignment Groups, select the SMART Group you created earlier, starts with W10Client0a1
 - Deployment Begins, Go back one day (in terms of todays date)
 - App Delivery Method, select Auto radio button
 - Select **CREATE** at the bottom of the page

			Assignment Status All	 Search List
signment Status	Friendly Name	User	Platform	Organization Group
ided	Livefireuser Desktop Windows Desktop 10.0.19041 4 63	Livefireuser	Windows Desktop	xeniaforman
				Page Size _20 V Hems 1 -

10. On the Carbon Black Cloud Sensor 64-bit- Assignment

Select PUBLISH

The CB sensor package will be published to any Windows devices enrolled into this UEM organization group.

2.2: Observe device behaviour in VMware Carbon Black

Workspace ONE UEM will push the VMware Carbon Black MSI package and install the Sensor with the correct company Code.

Note: This may take up to 5 minutes. Take a break!

🖏 Works	pace ONE UEM		xeniaforman	Add 🗸	Q \$ \$ 6	xeniaforman_ ~
E GETTING STARTED	Dashboard List View Configure	ß	Devices > List View Livefireuser Desktop Windows Deskt VMvare Virtual Platform 10.0.19041 Ownership: Corporate - Dedi Summary Compliance Profiles Baselines Apps Updates	Content More 🗸	QUERY SEND	< 1/1 > Reset Lia LOCK MORE ACTIONS ¥
BENGES 85 ACCOUNTS		_	Installation Status Last Scan: Tuesday, January 12, 2021 11:15 AM		Last Scan: Tuesda	y, January 12, 2021 11:15 AM
			Name	App Status	Installation Status	Assignment Status 💌
APPS & BOOKS			Carbon Black Cloud Sensor 64-bit	⊘ Installed (3.6.0.1979)	Managed	Assigned (3.6.0.1979) 03
				-		
		Carbon installe Workspace	Black Cloud Sensor 64-bit is d te ONE Notifier 1 new notification 222 PM			
			^ 도 4. 3/11/2021			

- 1. On the ControlCenter server,
 - If you aren't already signed into your Workspace ONE UEM console
 - Login to the **cn-livefire.awmdm.com** tenant
 - Navigate to **Devices** > List View
 - Select your **device**
 - Select the Apps Tab
 - Make sure the **VMware Carbon Black Cloud Sensor 64-bit** has a green Check box next to it.

If you see the status as failed or Not Installed, re-trace your steps and double check the MSI install command in the previous chapter.

Carbon Black.	•	frank (cb-internal-ws1-livefine.vmwa) >
CB-INTERNAL-WS1-LI	View data 2 weeks V All policies V V	e Dashboard
dashboard	Attacks Stopped	<u>با</u>
 ▲ ALERTS ♦ INVESTIGATE ♥ LIVE QUERY ♦ ENFORCE 	Non-Malware 16 Potential malware 2 Malware 1 19 PUPs	
© SETTINGS →	Potentially Suspicious Activity Non-Malware 1 Potential malware 0 Malware 1 2 PUPs	<u>ل</u>

- 2. On the **ControlCenter** desktop
 - Open a browser and navigate to https://defense-prod05.conferdeploy.net/
 - Sign in with your **e-mail address** and **password** assigned to you.

S my-ip.livefire.lab/ip V	Mware Horizo
vm Carbon B	lack Cl
C cb-internal-ws1-live	3h 1d
Dashboard	Get
\land Alerts	
🖨 Investigate	A8
Live Query >	ৎ
⊘ Enforce >	۲
ြ Inventory 🗸	
Endpoints	
Sensor Groups	
Image: Settings →	Alex

- 3. In the VMware Carbon Black Cloud console
 - In the left hand navigation, expand **Inventory**
 - Select Endpoints
 - Identify your Device with the computer name that you set. (i.e. AttendeeXXX)

• Click on the **Check Box** next to your device



- 4. In the Endpoints window
 - Select Take Action drop down and click Change policy

Change policy	×
Zero Trust LiveFire Start typing a policy Monitored Standard Advanced Demo	
VMware TS Zero Trust LiveFire	
Change policy	×
Zero Trust LiveFire Update the 1 selected devices Update all 29 devices matching the search	
Change Cancel	

- 5. In the Change Policy window
 - In the dropdown, select Zero Trust LiveFire

Select Change. (NOTE: Ensure you have the selection set to 'Update the 1 selected devices'.

This will change the Endpoint policy to **Zero Trust Livefire** Policy. Lets look at what exactly this policy is enforcing on our endpoints.



- 6. In **Carbon Black Admin** console, in the left navigation panel,
 - Navigate to Enforce > Policies

NAME	DEVICES	General Prevention Local Scan Sensor
Monitored	0	— General
Standard	4	
Advanced	0	* Policy name
Demo	0	Monitored
VMware TS	0	Policy description
		No prevention. Use to detect activity before moving endpoints into a prevention policy, or for mission critical endpoints. Target value Multiplier when calculating the threat level for detected issues and resulting alerts. Medium is the baseline/default. Medium Sensor UI: Detail message

- 7. Under NAME for the list of available policies,
 - Select the Zero Trust Livefire Policy.

Ger	neral Prevention Lo	cal Scan Sensor
Use +	these rules to configure how sensor Permissions	s control process behavior Allow specific operations or bypass application activity entirely. Takes precedence over blocking and isolation settings below.
+	Blocking and Isolation	Deny or terminate processes and applications.
+	Uploads	Deny or allow upload paths.

8. Click on the **Prevention** tab.

0

You will see Permission, blocking & isolation and uploads rules to configure how sensors controls our endpoints.

Gen	eral Preve	ntion	Local Scan Sensor
Use	these rules to conf	igure how sen	isors control process behavior
_	Permissions		Allow specific operations or bypass application activity entirely. Takes precedence over blocking and isolation setti
	Application(s) at path:	
_	C:\Program	Files\dfndr.e	2xe
+	Blocking and	Isolation	Deny or terminate processes and applications.
+	Uploads		Deny or allow upload paths.
			ACTION
			Bypass

9. Under the **Prevention** tab

0

- Expand Permissions,
- Notice, the Application(s) at path: C:\Program Files\dfndr.exe is set to Bypass for any operation.

This can be an example of an internal application which needs to be excluded from any sensor actions.

		Notifications ¹⁵ Help >	Rohit Masa	and (cb-internal-ws1-live	efire.vmwa
Blocking and Isolation Deny or terminate processes and app PROCESS	ications.	OPERATION ATTEMPT	OS .	ACTION	
Known malware		Runs or is running Test rule 🖉	\$ ∆ #	Terminate process	0
Application on the company blacklist		Runs or is running Test rule 🖉	\$ ∆ #	Terminate process	0
Unknown application or process		Scrapes memory of another process Test rule @ Executes code from memory Test rule @ Invokes an untrusted process Test rule @ Invokes a command interpreter Test rule @ Performs ransomware-like behavior Test rule @ Execute a difess soript Test rule @ Injects code or modifies memory of another process Test rule @	6 11	Terminate process Terminate process Terminate process Terminate process Terminate process Terminate process	0
Adware or PUP 🔟		Communicates over the network Test rule 🖉 Performs ransomware-like behavior Test rule 🖉	6 11	Terminate process Terminate process	0
Suspected malware		Runs or is running Test rule 🖉	6 15	Terminate process	0
Not listed application		Scrapes memory of another process Test rule @ Executes code from memory Test rule @ Invokes an untrusted process Test rule @ Invokes a command interpreter Test rule @ Performs ransomware-like behavior Test rule @ Executes a fileless script Test rule @	6 1	Terminate process Terminate process Terminate process Terminate process Terminate process Terminate process Terminate process	0

Application(s) at path:	Runs or is running Test rule 🖉	6.12	Terminate process	80
**\notepad.exe **\powershell.exe **\powershell*exe **\notepad++.exe		-		
Each path must start on a new line. Do not separate with commas.				
С				

- 10. Next, observe the Blocking and Isolation Rules,
 - Notice it lists all the processes, their operation attempt and the actions this policy will take to prevent an attack.
 - In our policy example, we have added NOTEPAD.exe & Powershell.exe as blacklisted applications,
 - Any executed processes will **TERMINATE** and any existing attempt to run will be **BLOCKED**

In our LAB environment, you only have read only access and hence cannot make any changes to the policy. In real world, you can choose to perform a deny operation or terminate operation depending upon the use case.

You have successfully completed this section. Please proceed to the next section.

Part 3. Workspace ONE Intelligence API integration & Automation

In this lab you will create the integration between VMware Carbon Black Cloud and Workspace ONE Intelligence.

- 3.1: Create API & SIEM Notifications
- 3.2: Create VMware Carbon Black & Workspace ONE UEM Connectors
- 3.3: Create Dashboard and Widget
- 3.4: Create Automation

3.1: Create API Keys

С	arbon Black.	
СВ-	C INTERNAL-WS1-LI	API ACCESS Establish and manage integration with other sec API Keys Access Levels
alti	DASHBOARD	
	ALERTS	ORG KEY: 7W2F4KVN ORG ID: 9456
	INVESTIGATE	NAME
۵	LIVE QUERY	SIEM key
	ENFORCE 🕨	Roar SIEM
₽	ENDPOINTS	empower104
¢	SETTINGS -	
	General	Attendee101
	Users	
	Roles	rohit test
	Notifications	
	API Access	Zero Trust test_rohit
	Inbox	
	Audit Log	Rohit SIEM key
ratio	n Documentation	+ Add API Key
U	AST REPORTED TIM	E ACTIONS
	2:19:08 am Jun 4, 2020	Edit

- 1. Adding an API Key.
 - On the left hand navigation pane. Expand Settings and select API Access
 - In the top right corner of the Admin Console, select + Add API Key

Add API Key		
lame		
Attendee222		
Description		
/	3	
ccess Level type	* Custom Access Level	
Custom	* Custom Access Level	
Access Level type	Custom Access Level Zero Trust	\ \
Custom	Custom Access Level Zero Trust	which com for all
Custom This permission set r currently supported.	Custom Access Level Zero Trust may contain unversioned APIs. Visit developer, carbo /versioned APIs.	mbiack.com for all
Custom Custom This permission set a currently supported.	may contain unversioned APIs. Visit developer carbo	mblack.com for all
Custom This permission set of currently supported.	may contain unversioned APIs. Visit developencarios	oriblack com for all
Access Level type Custom This permission set of currently supported. Authorized IP addresses pecify a comma separated list of single IP	A Custom Access Level Zero Trust may contain unversioned APIs. Visit developer carbin /versioned APIs. address, or an IP address range in CIDR notation (for example, 203.0.11)	mblack.com for all
Access Level type Custom This permission set of currently supported. Authorized IP addresses ipecify a comma separated list of single IP	A Custom Access Level Zero Trust may contain unversioned APIs. Visit developer, carbo /versioned APIs. address, or an IP address range in CIDR notation (for example, 203.0.11)	nitilaisk som for all 13.5/22).
Access Level type Custom This permission set of currently supported. Authorized IP addresses ipecify a comma separated list of single IP	address, or an IP address range in CIDR notation (for example, 203.0.11	onblack com for all
Access Level type Custom This permission set of currently supported. Authorized IP addresses specify a comma separated list of single IP	address, or an IP address range in CIDR notation (for example, 203.0.11	niblack.com for all
Access Level type Custom This permission set t Currently supported Authorized IP addresses Specify a comma separated list of single IP	Access Level Zero Trust may contain unversioned APIs. Visit developer, carbo Aversioned APIs. address, or an IP address range in CIDR notation (for example, 203.0.11)	nitietk com for all
Access Level type Custom This permission set t Currently supported Authorized IP addresses pecify a comma separated list of single IP	Access Level Zero Trust may contain unversioned APIs. Visit developer, carbo Aversioned APIs. address, or an IP address range in CIDR notation (for example, 203.0.11)	Initiate com for all
Access Level type Custom This permission set of Currently supported. Authorized IP addresses Specify a comma separated list of single IP	w Custom Access Level custom	niblack.com for all

- 2. Enter the below information,
 - 1. Name the API key your unique attendee Identifier. EXAMPLE: Attendee101
 - 2. Select **Custom** in the Access Level type
 - 3. Select Zero Trust for Custom Access Level
 - 4. Select **Save** at the bottom of the window.

NOTE: For the integration with Intelligence the API Access Level must include the "Data Forwarder" settings

API Credentials	×
API ID UMDJM7VAFV	
API Secret Key WDE19ZMUUJD5EBHVC6UCVSK4	
In Untitled - Notepad	
Pile soft Format View Help	
API Secret key: WDE19ZMUUJD5EBHVC6UCVSK4	

- 3. You will now be shown the **API Credentials**.
 - 1. Copy both the API ID and the API Secret Key to Notepad.
 - 2. Close out of the API Credentials windows by clicking X

3.2: Configuring VMware Carbon Black & Workspace ONE UEM Connectors

In order to send Alerts received in VMware Carbon Black portal to Workspace ONE Intelligence, we will be configuring a VMware Carbon Black Connector in Workspace ONE Intelligence. This requires us to use both VMware Carbon Black console API Key & SIEM API Key. Security Information and Event Management (SIEM) API allows you to capture security events generated on the VMware Carbon Black platform in your Workspace ONE Intelligence console.

k@v Υ	Add 🗸	ୟୁଠୁ ☆ୁ ⊘ sfrankøvm… > 🗰
> Groups > Organiza		MY SERVICES
		Workspace ONE Hub Services
		Workspace ONE Identity Manager
com		Workspace ONE Intelligence
		Workspace ONE UEM

- 1. On the ControlCenter
 - Switch to your Workspace ONE UEM console,
 - If necessary navigate to https://cn-livefire.awmdm.com.
 - Sign in using your admin credentials (E-mail used to attend the course)
 - In the top right corner, select the MY SERVICES icon (9 squares)
 - Select Workspace ONE Intelligence



- 2. In the Workspace ONE Intelligence Admin console
 - Select the Integrations tab

Workspace



- 3. Under Integrations section
 - Scroll down to find the Carbon Black tile,
 - Select SET UP

Intelligence would like	to get access to Carbon Black for the following:	
> Connector Perr	missions	515
✓ Authorization D	Details	
Click have for	more information on how to set up this connector More information	
(i) Click here for	more information on how to set up this connector. <u>More information</u>	
(j) Click here for Payload Body	more information on how to set up this connector. <u>More information</u>	
Click here for t Payload Body Base URL	more information on how to set up this connector. <u>More information</u> https://defense-prod05.conferdeploy.net	
Click here for t Payload Body Base URL API ID	More information on how to set up this connector. More information https://defense-prod05.conferdeploy.net M49BYIQFQZ	
 Click here for I Payload Body Base URL API ID API Secret Key 	more information on how to set up this connector. More information https://defense-prod05.conferdeploy.net	0

- 4. In the Authorize Connector: Carbon Black console
 - Expand the Authorization Details dropdown. Enter the following information, next to: Base URL: https://defense-prod05.conferdeploy.net

- API ID: {Paste the API ID from your notepad above}
- API Secret Key: {Paste the API secret Key from the notepad above}
- Org Key: 7W2F4KVN
- Select AUTHORIZE

NOTE: The Org Key identifies the Carbon Black Tenant and is unique to each Carbon Black Cloud instance.

3.3: Create Dashboard & Widget



- 1. In the Workspace ONE Intelligence Console
 - In menu bar, select the **Dashboards** tab
 - In the **Dashboards** area
 - Select Get Started
 - In the My Dashboards section
 - Select +ADD

Add Dashboard	
Carbon Black Add description (optional)	
CANCEL	

- 2. In the Add Dashboard window
 - Name the dashboard Carbon Black
 - In the bottom right of the page, select **SAVE**

 We collect data to learn more or disat 	deliver, an ble certain	alyze and impi cookies, see o	rove the service, ur Cookie Usage	to customize your e page.	xperience, ar	nd for other purpo	oses set out
🔘 Workspa	ice ON	E Intellige	ence Q	DASHBOARDS ~	Search Da		
Home Getting S	Started	Solutions	Dashboards	Automations	Reports	Integrations	Settings
		~					
			INTELLIG	ENCE DASHBOARD	S		
Intelligence Das	shboards	~	My D	ashboard	ls > Ca	rbon Bla	ck
My Dashboards			Crosted		nto@amail.c	om a Last Mos	lified: Auc
Security Risk			ADD WI		MIZE		ineu. Aug
OS Updates							
User Risk			Y Add F	ilter			
Apps							
Devices							

- 3. In my **My Dashboards** > **Carbon Black** area
 - Select ADD WIDGET

	INTELLIGENCE DASHBOARDS
1	My Dashboards > Carbon Black
	Created By: majonne.duponte@gmail.com • Last Modified: ,
	ADD WIDGET ~ CUSTOMIZE
-	From Template
	Custom Widget

- 4. In the MY Dashboards > Carbon Black
 - From the dropdown, select **Custom Widget**

🖏 Works	pace ONE Intelligen	ice Q
Add Wid	dget	
Select a tem	plate category to get :	started.
CATEGORY ~	Workspace ONE UEM	>
	Intelligence SDK	>
	BETTER Mobile	>
	Carbon Black	>
	Check Point	>
	Employee Experience	>
	Workspace ONE Access	>
	Intelligence	
BETTER MO	obile >	
Carbon Bla	ck >	oon Black Threats
Check Poin	t >	Ser Elder Hiredes
Employee I	Experience >	

- 5. In the Add Widget window
 - Select the **dropdown** next to **CATEGORY**
 - Select Carbon Black > Carbon Black Threats



- 6. In the Add Widget screen,
 - Replacing the "Name your widget" with Medium & High Severity

Data Visualization ①



Chart Type								
In VERTICAL	🛛 AREA 🛛 LINE	12 METRIC	₩ TABLE	Ш НЕАТ МАР]			
Measure	Count		of Carbon	Black Device II				
Group by (Optional)	Carbon Black Dev	vice E × Carbo	n Black Extern	al × Carbon Bl	ack Incident	\times Carbon Black Severity	V × Platform	×
Results per group	10							
Date Range (Optional)	Last 28 days	~						

- 7. In the Add Widget screen,
 - 1. Under Data Visualization > Chart Type, Select TABLE.
 - 2. Fill in the following fields: Next TO
 - Measure: Count of Carbon Black Device ID. (Choose from drop down)
 - Group by (Optional): select from the dropdown Carbon Black Device Email,
 - Next to Carbon Black Device Email, select ADD SUBGROUP
 - Select from the dropdown Carbon Black Device External IP Address
 - Next to Carbon Black Device External IP Address, select ADD SUBGROUP
 - Select from the dropdown Carbon Black Incident ID, select ADD SUBGROUP
 - Select from the dropdown add Carbon Black Severity Score, select ADD SUBGROUP
 - Select from the dropdown select **Platform**.
 - Next to Date Range, ensure that the Last 28 days is configured

Note: These are mere suggestions, any given attribute coming from VMware Carbon Black could be selected to be displayed

r <u>Em</u>	<u>pty Rule</u>			
r Se	arch		Search for value	×
				\oplus
T T	Empty Rule Search		Sea	arch for value
	Normalized Threat	>	Threat Severity	(vormalized)

Filte	r ©			CLOSE
Ψ	Threat Severity includes (Medium, High)			© ≫
	Threat Severity 💿 Includes 🗸	Medium X High X)	+ 🗇
			No Values Found	
		SELECT ALL	CLEAR ALI	

- 8. In your Custom Widget
 - Under Filter,
 - In the Search area, under Empty Rule, select Threat > Threat Severity
 - In the second drop down select INCLUDES
 - In the third drop down type Medium and hit ENTER on your Keyboard
 - In the same field, type **High** and hit **Enter** on your Keyboard.
 - Select **SAVE** at the top of the page.

INTELLIGENCE DASHBOARDS

My Dashboards > Carbon Black

Created By: rmasand@vmware.com • Last Modified: Sep 5, 2021 • Last Modified By: rmasand@vmware.com • Last Modified Widget: Medium & High Severity

	Date Range v	
T 2	Device Organization Group Name includes All AND Organization Group Hierarchy includes All	
ADI	D WIDGET V CUSTOMIZE	
7	\dd Filter	
М	edium & High Severity	
æ	Platform v 🖆 Date Range v 🎹 Table v	

9. In INTELLIGENCE DASHBOARDS

• Select **SAVE**

NOTE: If you are not seeing Medium in the dropdown, it means Workspace ONE Intelligencehas not yet received any Medium Alerts from VMware Carbon Black Portal. You can simply type in **medium** and hit **enter**.

Part 4: Create Automation

We now will create an automation from the widget we have just created.

My Dashboards > Carbon Black created By: masand@vmvare.com + Last Modified: Sep 5,2021 + Last Modified By: masand@vmvare.com + Last Modified Widget: Modum & High Severity Date Range Cost Organization Group Name includes All 2 AND Organization Group Name includes All 2 AND Organization Group Name includes All 2 AND Organization Group Hierarchy includes All Cost Owner Add Filter Medium & High Severity Date Range If Table Date Range If Table No Data Available VIEW	INTELLIGENCE DASHBOARDS		
Created By: masand@vmware.com + Last Modified: Sep 5, 2021 + Last Modified By: masand@vmware.com + Last Modified Widget: Medium & High Severity	My Dashboards > Carbon Black		
Device Organization Group Name Includes All ADD Organization Group Hierarchy Includes All ACD WIGGET CUSTOMIZE V Add Filter Medium & High Severity Image: Customize and Custo	Created By: rmasand@vmware.com • Last Modified: Sep 5, 2021 • Last Modified By: rmasand@vmware	.com • Last Modified Widget: Medium & High	h Severity
Device Organization Group Name Includes All AND Organization Group Hierarchy includes All ADD WIDGET CUSTOMIZE V Add Filter Medium & High Severity Info Date Range Info I	Date Range v		
Add Filter Medium & High Severity	Device Organization Group Name includes All AND Organization Group Hierarchy includes All		
✓ Add Filter Medium & High Severity □	ADD WIDGET ~ CUSTOMIZE		
Medium & High Severity	Add Filter		
	Medium & High Severity	Π	
Info Edit Automate Refresh Export as .CSV Copy to Add to Bookmarks Duplicate Rename Set as thumbnail Delete	& Platform · Date Range · H Table ·		
VIEW			
VIEW		Info	
No Data Available Refresh Export as .CSV Copy to Add to Bookmarks Duplicate Rename Set as thumbnail Delete VIEW		Edit Automate	
No Data Available Export as .CSV Copy to Add to Bookmarks Duplicate Rename Set as thumbnall Delete VIEW		Refresh	
VIEW Copy to Add to Bookmarks Duplicate Rename Set as thumbnall Delete		Export as .CSV	
VIEW	No Data Available	Copy to	
VIEW Duplicate Rename Set as thumbnail Delete		Add to Bookmarks	
VIEW Carry Control of C		Duplicate	
VIEW Carry Control of C		Rename	
VIEW Carry ····		Set as thumbnail	
VIEW 212 ····		Delete	
	VIEW	212	

1. In the **Carbon Black** Dashboard,

- In the Medium & High Severity widget
 - At the bottom , right corner of the widget, select the **more options** icon (**three horizontal dots**).
 - Select Automate

NOTE: if you don't see the three dots, you may not have saved the dashboard at the top of the page

Workspace ONE Intelligence Q AUTOMATIONS - Search Automation Name
Add Workflow
Category: Carbon Black: Carbon Black Threats
Name your workflow 0
Generated from widget: Low&Medium Severity (Carbon Black)
Trigger (When) ③
Carbon Black: Carbon Black Threats Data
Automatic 🗸 🛈
Threat Severity equals (medium)

- 2. In the **Add Workflow** window
 - In the Name your workflow area, give the Workflow a title: Tag Malware Device & Notify Admin

Threat Severity includes	Medium, High)		D 98
Threat Severity	includes	v (2 selected X)	+1

- 3. Under the Filter (if) area
 - In Threat Severity row, at the end select the + icon

2	AND Carbon	n Black Device Name equals ((EUC-L	JVEFIRE\GrantFLZT	(29)				0
		Threat Squarity		Fouals		High medium			
ſ	AND -	- meat sevening					T		
(AND -	Carbon Black Device Name		Equals	~	EUC-LIVEFIRE\GrantFLZT29	+	1	= U ± 1

- 4. Under the Filter (if) area
 - Under Threat Severity in the Search area, select Carbon Black Device Name
 - Next to Carbon Black Device Name, from the dropdown change includes to equals
 - In the third n choose your **device** (eg **Attendee22**)

Action (Then) ①	
	\oplus

- 3. In the Add Workflow window
 - Scroll down to Action (Then) and select the \oplus



- 4. In the Add Workflow window
 - Under Available Connectors, select Workspace ONE UEM
 - Scroll down to the right and select Add Tag to Device

Action	(Then) 🗊		
G	Workspace ONE UEM	→ Add Tag to Device ①	Û
	Body		
	Device ID	\${airwatch.device_id}	
	Path Variables		
		 Search for existing values Enter custom value 	
(Tag ID	<u> </u>	
	TEST		

5. In the Tag ID field, Type **10000.** This sets the Tag "**Quarantine**" on the device. At the bottom of the **Action (Then)** area select

Note the Tag Name Quarantine is a custom TAG created in Workspace ONE UEM

To view the location,

- Go to Groups & Settings > Groups > All Settings > Device & Users > Advanced > Tags
- Note the Quarantine Tag has already been defined

Tag ID	10003	n for existing values 🛛 💽 Er	ter c
TEST TE	st successful ①	Ð	
		Ð	
Available (Connectors (3)		
	nova		
Workspace ONE UEM	ServiceNow	Slack	
0			
Send Emai	I		
Send Email to a	user through the SMT	P	
CONJOR CONTINUES	d with workspace ON	IE	
UEM			

- 6. In the Action (Then) area
 - At the bottom select the + sign
 - Under Available Connectors,
 - Select the Workspace ONE UEM connector,
 - Select the Send Email Connector

Workspace ONE UEM	Workspace ONE UEM → Send Email ①						
Body							
To Address	rmasand@vrr	asand@vmware.com					
Subject	Malware de	Malware detected					
Message	The followi	(⁺⊒) ◀					
		Normalized >	Alert Category Normalized				
Path Variables			Carbon Black CB Defense Event ID				
Device ID	\${airwatch.de		Carbon Black Device Email				
TEST			Carbon Black Device ID				
			Carbon Black Device Name				
			Carbon Black Device OS Version				
			Carbon Black Device Priority Code				
			Carbon Black Device Priority Type				
			Carbon Black Event Description				
			Carbon Black Event Occurred Time				
			Carbon Black External IP Address				
			Carbon Black Group Name				
			Carbon Black Incident ID				
			Carbon Black Internal IP Address				
		1	Carbon Black Main Process Hash (

- 7. In the Workspace ONE UEM > Send Email
 - In the Send Email, add the following next to
 - Address: your e-mail address
 - Subject: Malware detected
 - Message :
 - USE THE LOOKUP OPTION TO POPULATE THE BELOW INFORMATION OR MANUALLY TYPE IT IN, DONT COPY AND PASTE

The following threat is detected on your device :

Device ID - \${carbonblack.threat.threatinfo_threatcause_causeeventid}

Device name - \${carbonblack.threat.deviceinfo_devicename}

Threat - \${carbonblack.threat.threatinfo_threatcause_actorname}

Threat Severity - \${carbonblack.threat_threat_severity}

Threat time -\${carbonblack.threat.first_event_time}

Platform - \${carbonblack.threat._device_platform}



- 8. In the Workflow interface
 - Look in the bottom right-corner and you will notice a toggle with **Enable workflow** next to it
 - Move the **Toggle** to the right

0	grantflenderman@gmail.com grantZTRNEL	/ ==
	CANCEL	SAVE
	Summary	
1		

- 9. In the Workflow interface
 - In the top right corner, select **SAVE**



- 10. In the **Save Workflow** window
 - Next to One-time Manual Run, move the toggle from an OFF position to the right to turn on
 - Select SAVE & RUN

Your automation should now be live. Let's trigger an event on your device to see this take effect.

Part 5. VMware Carbon Black Incident & Workspace ONE Intelligence Automation

You are now ready to demo threat remediation using Workspace ONE intelligence and VMware Carbon Black. This section had two parts:

- 5.1: Incident
- 5.2: Notification

5.1: Incident

We will now create an incident. As we don't have the means to infect this vm with malware we will use Notepad++ as an example of a malicious application.





1. On the **ControlCenter**

- Open the **Remote Desktop** folder
- Connect to your **W10client01 RDP** virtual machine with your new hostname.

Mere	red						
e	Apps and Features						
	Power Options						
2	Event Viewer	_				_	
	System	C:\Users\A	\dministrator\AppData\R	carning\Microsoft\Win	dows\Start Menu\Progr	ams\Window X	
	Device Manager	8	is file does not have an a to or, if one is already ins	pp associated with it fo talled, create an associa	r performing this action tion in the Default Apos	Please install an Settings page.	
NC	Network Connections		,,				
ø	Disk Management					OK	
	Computer Management						
	Windows PowerShell						
	vinuuvo ruveianei (Aumin)						
	Teck Manager						
	Settinos						
	File Explorer						
	Search						
	Run						
	Shut down or sign out >						
	Desktop	() 희 💽	📮 🔒 💼		-	
	19 ¹ Prop.						
Ci	arbon Black Cloud						
Tł	nreats Blocked						
	An application was blocked C:\windows\system32\windowspowe powershelLexe	ershell\v1.0\	1/13/2021 150 AM				
	An application was blocked C\windows\system32\windowspowe powershell_ise.exe	ershell\v1.0\	1/13/2021 139 AM				
	An application was blocked C\windows\syswow64\windowspow powershell_ise_exe	ershell\v1.0\	1/13/2021 139 AM				
			ок Ок 2 Ф. 1:54 АМ 1/13/2021	R			

- 2. On the W10Client02 virtual machine
 - Right-click the **Start** button,
 - Select Windows PowerShell.
 - Notice the PowerShell message
 - Select the **Carbon Black** Sensor in the right-hand corner
 - Notice the configured Threats that have been blocked.
 - Select **OK** to close



- 3. On your Windows Desktop
 - Select Start > Run
 - Enter the following UNC Path \\horizon.euc-livefire.com\software\Applications\ Lab3.2_Only(App Volumes)\notepad
 - Copy the Notepad++ msi to your Desktop
 - Attempt to **execute** this MSI.
 - Notice the installation of Notepad++ is blocked
 - Note that this is not a standard Notepad++ msi package but a ThinApp package that offers application isolation and even with this, the sensor is able to block the installation and execution on the device.
 - Attempt to **rename** the MSI and re-execute see what happens

5.2: Alert & Automation

vm Carbon Black Cloud									
c cb-internal-ws1-liv	ALERTS								
 Dashboard 	FILTERS Clear : «	4 results							
▲ Alerts	Type (3) CB Analytics 4	STATUS I							
🖨 Investigate	Watchlists 0 USB Device Control 0	Policy Applied S Policy Applied S Ran J							
Live Query >	— Priority (1)	© Policy Applied							
⊘ Enforce >	Target value Alert severity	⊛ Ran J							
🗗 Endpoints	- + - 3 +	Policy Applied							
	Threat 4	⊛ Kan '							
	Device (2) Search EUC-LIVEFIRE\ReinhartZT99 3 Attendee222 1	© Policy Applied f ⊗ Ran I							

- 1. Log into the Carbon Black **Cloud Admin console**.
 - 1. Navigate to **Alerts** from the left menu bar.
 - 2. Under FILTERS menu, expand DEVICE and select your endpoint i.e. AttendeeXXX.
 - In the right-hand pane, observe **STATUS** of Alert as a Deny Policy Action and the Alert Severity.

	Search Guide
veeks	~ Q
	Group alerts On
	ACTIONS
r Atte	
nia Forr	nan (cb-internal-ws1-livefire.vmwa) >
	Search Guide
~ ~	2 weeks \lor Q
	Group alerts 🔵 💓
/ICE	ACTIONS
ninistra	tor Atte

NOTE: Ensure GROUP ALERTS is set to OFF. If not, ensure to set it to OFF to view your specific endpoint alert.

• Move the **Toggle** in the right-hand corner from **On** to **Off**



- 2. Switch to the Workspace ONE Intelligence console.
 - Login to **cn-livefire.awmdm.com** with your admin credentials.
 - Navigate to Monitoring > Intelligence.
 - Select LAUNCH



3. In the Workspace ONE Workspace ONE IntelligenceConsole,

- 1. Select Automations
- 2. Select **VIEW** on your Carbon Black automation
- 3. Next to Overview, select the Activity tab
 - You should see the events, the tag being assigned and the e-mail being sent to the admin.

0	xeniaforman@	a gmail.c xeniafori	com v 🔛					
MY SER	RVICES							
Øv	Vorkspace ONE Ir	ntellige	nce					
Øv	Vorkspace ONE U	JEM						
GETTING	Dashboard		Devices	•				
STARIED	List View		List View					* *
	Details View							
MONITOR	Device Updates		Filters 30	ADD DEVICE	(LAYOUT Y 6 E	XPORT 🛩 Sea	rch List
0	Lifecycle	>	Last Seen	General Info	Platform	User	Tags	Enrollment (
ORVERS	Profiles & Resources	>		Fisher Desktop Windows Desktop 10.0.18362.6 a1	Windows Desktop	fsmin@no-reply.com		1.
答	Compliance Policies	>	- 4fm	VLS CarbonBlack MDM Corporate - Dedicated	VMware Virtual Platform 10.0.18362	Fisher Fisher Mint	Canada	Enrolled
ACCOUNTS:	Certificates	>						
***	Percipicality							

- 4. Switch to the Workspace ONE UEM console,
 - 1. Navigate to **Devices > List View**
 - 2. You will notice the enrolled device has the **QUARANTINE** tag assigned to it

= M Gmail	Q Search mail	•	? :::
- Compose	□ - C :	1-50 of 476 <	> ¢
Inbox 390	Primary	Social Promotions 25 new Shopify, The Okta Team, The P	
★ Starred	🔲 🚖 🗁 AirWatch	Walware detected - DEVICE ID - BA52D8888BBFC3499833C40381134DEF DEVICE NAME - empower102 Thr	8:45 PM
Snoozed	🔲 ☆ ➤ noreply	Please confirm your registration with Carbon Black Cloud - CONFIRM ACCOUNT Click to confirm your admi	1:19 PM

r.	Walware detected \sum Inbox ×			•	Ø
	AirWatch <noreply@awmdm.com> to me ▼</noreply@awmdm.com>	8:45 PM (12 minutes ago)	☆	*	:
	DEVICE ID - BA52D8888BBFC3499833C40381134DEF DEVICE NAME - empower102 Threat - [t_pol_term_child : (notepad++.exe)] Threat Severity - medium Threat Time - 1589132596623 Platform - windows				

5. Now navigate to your e-mail and notice you have an e-mail from **AirWatch** that has the information for the device that has been compromised.

This ends the lab for VMware Carbon Black Integration with Workspace ONE Intelligence.