

Horizon NDR

Despliegue de Horizon NDR on-prem

Edgar Pajuelo R.

Diciembre 2023



Contenido

Horizon NDR	1
Contenido	2
Información Importante	3
Contactos	3
Control de Cambios	3
Contexto	4
Registro en Portal NOW de Check Point	4
Despliegue del sensor NDR	5
Indicadores de Compromiso - IoC	9
Prevención de Amenazas empleando sensor NDR	11
Referencias y Notas:	12



Información Importante

Confidencialidad sobre este documento:

• Este documento no debe ser comentado, divulgado o publicado con terceras partes sin previa autorización explícita de Check Point.

Responsables sobre la utilización del documento:

• Integrantes de la organización "Check Point".

Contactos

	Nombre y Apellido	Correo Electrónico
Check Point	Edgar Pajuelo R.	edgarp@checkpoint.com

Control de Cambios

Fecha	Descripció n	Autor	Versión		
29/12/23	Documento Inicial	Edgar Pajuelo R.	1.0		



Contexto

El objetivo de la presenta guía es poder desplegar un sensor de red con capacidad de detección y respuesta antes amenazas (NDR - Network Detection and Response), empleando Horizon NDR.

Luego de desplegado el sensor NDR, debemos contar con las capacidades de generación de Indicadores de Compromiso (IoC) sobre las amenazas detectadas en la red, y a partir de los cuales se establecen las estrategias de prevención de amenazas.

La facilidad de integracion de los IoC de manera automática con herramientas propias de Check Point o de fabricantes terceros (Firewall, EDR, Proxy, etc.) hace del sensor NDR un complemento importante en la red, para una visibilidad 360° de la seguridad, especialmente en aquellos lugares de la red donde no se cuenta con capacidades de inspeccion avanzada.



Registro en Portal NOW de Check Point

1. Habilitación del Portal NDR de Check Point.

- a. Crear registro en https://portal.now.checkpoint.com/registration/register
- b. El dominio se creará automáticamente y nos llegar un correo de notificación*
- c. Luego podemos realizar el registro de usuarios. La notificación a los usuarios finales llegara a través de la cuenta now@checkpoint.com
- d. Todos los usuarios deben realizar la descarga e instalación del certificado digital, en sus navegadores. Se debe emplear navegador Google Chrome o Firefox, el acceso está basado en autenticación mediante certificado digital.

*En caso el registro sea con una cuenta de dominio externo, distinto a Check Point, deben solicitar autorización a: Arturas Zalenekas <u>azalenek@checkpoint.com</u>



Despliegue del sensor NDR

1. Habilitación del appliance NDR de Check Point

Debemos realizar la instalación GAIA en versión R81.10 JHF 95 o superior (appliance virtual o físico). Debemos instalar el GAIA empleando únicamente el modo "Security Gateway". Si por error seleccionamos la opción de Security Management, debemos empezar nuevamente.

Products		
Products		
Security Gateway		
Clustering	ClusterVI	
Define Security Management as:	Primary	
Automatically download and install f For more information click <u>her</u> 	slade Contracts, new software, and other importar <u>e</u>	nt data (highly recommended)
	< Back	Next > Cancel

Si usamos una máquina virtual (VM) debemos tener las siguientes consideraciones: en VMware, VM con 08 CPU, 16 GB RAM, y 100 GB HHDD. La VM debe contar mínimo con 02 interfaces (eth0 – para Management, eth1 – para Monitor).

NOTA: La interfaz de gestión (Mgmt) del appliance físico no puede ser conectada a la red para la comunicación del sensor NDR hacia la Internet (tenant de Check Point Portal NOW), se deberá emplear una interfaz distinta a la de Mgmt para gestionar el sensor. Debemos colocar dirección IP estática para interfaz de gestión, Gateway y DNS.

Terminada la instalación del GAIA, verificar la conectividad del sensor hacia el tenant de Check Point Portal NOW:

- Conectividad directa vía HTTPS (TCP 443) con dirección destino 35.156.213.136, 18.196.115.85 (portal.now.checkpoint.com) y 35.157.19.226 (feeds.now.checkpoint.com). Debemos realizar pruebas de conectividad hacia estos destinos, ver NOTA 1 al final de la guía.
- Si en caso, el cliente está realizando inspección de tráfico cifrado (HTTPS/TLS) saliente, se debe realizar la excepción de inspección HTTPS para las direcciones IP indicadas, para la dirección IP de gestión del sensor NDR y la dirección de los host destinos.

NOTA: Es necesario crear un usuario adicional con niveles de administrador, distinto al usuario "admin", esto debido a que el usuario "admin" del appliance cambiará de



contraseña automáticamente en el momento del despliegue del sensor NDR, por lo cual no se podrá usar esta cuenta para acceder al GAIA, ni por consola ni por SSH.

2. Creación del sensor NDR en el tenant de Check Point

Debemos realizar el registro del nuevo sensor en portal Check Point en modo *NDR-Managed*, para ello debemos emplear la dirección MAC del appliance físico (etiqueta del equipo). En caso sea un appliance virtual (VM) el sistema crea una dirección MAC automáticamente.

1 ndrtest								Ĺ	Ĵ	Edgar Pajuelo 😩	~ C	•	CHECK POINT INFINITY PORTAL	
			家 "	_₿ Actions ∨ 🔺 Ne	w 🖍 Edit	🗋 Delete	୯	Refresh	T					1
State	NDR-Managed	Name		MAC Address	Domain			Description	ı				Plan	
 ✓ 		vt4a8cd7e896d5		4a:8c:d7:e8:96:d5	ndrtest					r			Initial-P	2
											NDR-I * Sen: Phy 00:1	Mana sor M sical C:7F	ARC I Virtual :BC:E6:E6	

Nota: Para la MAC debemos usar el formato XX:XX:XX:XX:XX, ya que el sistema no valida el formato, y da error al momento de realizar el registro.

3. Creación del Registration Key y activación del sensor

En el portal, debemos seleccionar el sensor creado previamente e ir a la opción "Actions" y luego "Generate Registration Key". Esta opción nos va a crear un comando que contiene un token único para este sensor, ese comando deberá ser ejecutado en el GAIA en modo experto.





GATEWAY REGISTRATION KEY
Registration Key: RA6Mw4WtX7PvncVI1HahASV1H4URLEcgZVAaxm66gOHN8yUfdp/emQ/Tnqv/svQAWf0euFN dWceIF24fkBHrMCqhfd9QxAR3vrL/0kI/y1uOiYkF Image: COPY KEY Image: COPY KEY
ОК

NOTA: Antes de ejecutar el comando en el GAIA, debemos tener cuidado de las interfaces que habilitaremos como Port-Span (monitor).

Ejemplo. - Si usamos la interface eth1 como interfaz de gestión a través de la cual el sensor se conecta a Internet y se comunica con el tenant de Check Point, no debemos incluir esa interfaz en el comando. Solo debemos considerar la interface que emplearemos en modo "monitor" para el Port-Span, se pueden establecer tantas interfaces como sean necesarias.

El nombre de la interface que colocamos en el comando, debe ser el mismo que figura en el GAIA.



Luego de ejecutar el comando, esas interfaces serán colocadas automáticamente en modo promiscuo (monitor-mode) y el appliance se reiniciará automáticamente.

admin[22215]: [NDR]: setting eth2 in monitor-mode admin[22251]: [NDR]: setting eth3 in monitor-mode admin[22289]: [NDR]: NDR setup finished, gateway will reboot [Expert@3600-fw:0]#

4. Estado del registro del sensor NDR en el Tenant (Portal NOW)

El sensor NDR tiene dos iconos para identificar su estado. El primero de ellos es el "state" (en forma de cruz para el estado inicial) que muestra el estado del registro, y el segundo (forma de foco) nos muestra si se encuentra conectado (verde) o desconectado (gris).



Cuando el icono en forma de foco se encuentra en color "gris" significa que el túnel SNX este caído, y el sensor no reporta información al tenant.

🗎 🗎 nd	rtest 🗸								
					🗞 Actions 🗸	*	New	🖍 Edit 🥤	-
State		NDR-Managed	Name	¢	MAC Address		Domai	n	
+	ê	Ø	gw001c7fbce6e6		00:1C:7F:BC:E6:E6		ndrtest		

Luego del reinicio, el sensor NDR pasara por 02 estados, uno donde se realiza la descarga e instalación de la política inicial en el sensor, y luego al termino pasara a un estado (icono de Check) de finalizado completo. Este proceso toma unos 15 minutos aproximadamente.

					🗞 Actions 🗸 🔺	+ Nev	V 🗡 E	idit 👕 👕
State		NDR-Managed	Name	>	MAC Address	D	omain	
C		•	gw001c7fbce6e6	(00:1C:7F:BC:E6:E6	nc	lrtest	
					🎭 Actions 🗸	*	New	🖍 Edit
State		NDR-Managed	Name	0	MAC Address		Domai	n
\checkmark	ê	Ø	gw001c7fbce6e6		00:1C:7F:BC:E6:E6	5	ndrtest	

Luego de ello, debemos conectar los equipos de red del cliente a las interfaces de monitor y configurar los switches para poder capturar la información:

- Appliance Físico: Se requiere configurar port-span o vlan-span en los equipos de red, para reenviar todo el tráfico necesario que se requiere inspeccionar hacia el(los) puerto(s) en modo *monitor-mode* del sensor NDR.
- Appliance virtual VMware: Esta configuración requiere la creación de una VM Network específica para estos fines, y a través de la cual se va a reenviar el tráfico de las maquinas virtuales al sensor NDR virtual. Si se va a desplegar en un clúster de contiene varios host y VM Networks, se debe tener consideraciones adicionales (Ver Nota 2 al final de la guía).



Indicadores de Compromiso - IoC

Luego de algunos días de captura de información, debemos ver en la consola si el sensor está creando registros de amenazas basados en sus motores de IPS, Antivirus, Anti-bot y Threat Emulation, ya que luego de ello creara de manera automática Indicadores de Compromiso (IoC) que nos permitirán prevenir las amenazas identificadas en la propia red del cliente.

Los loC aparecen en la sección Intel > *Indicators*, por defecto todos los loC se crean inicialmente en modo *detect*, los administradores deben seleccionar aquellos loC que deseen bloquear en la red y pasarlos a modo *prevent*.

						v	_
indicators						+ Add from File PREVEN	Т
🛼 Data Sets	Enabled 🗘	Action 🗘	Blade 🗘	Name 🇘	Туре 🗘	Value 🇘	[
G Feeds	Ø	PREVENT	Anti-Virus	Behavioral.Geo.Belgium.Out	IP	89.249.73.202	0
	Ø	PREVENT	Anti-Virus	Behavioral.Geo.Brazil.C2.Out	DOMAIN	testupdate.info	C
	•	DETECT	Anti-Virus	Behavioral.Geo.Kazakhstan.C2.Ou	URL	http://www.testupdate.info/upd	С

Si tenemos loC que no deseamos que formen parte de la política de prevención, podemos deshabilitarlos (disable) o eliminarlos (delete). En caso queramos realizar acciones sobre varios loC de manera simultánea, podemos seleccionar varios loC y luego la opción "Bulk Edit".

						+ Add from File	PREVENT 📦 Bulk Edit	🌯 Actions ∽ 🛛 米 New
	Enabled 🗘	Action 🗘	Blade 🗘	Name 🗘	Туре 🗘	Value 🗘	Description	Selected 1 indicator(s)
~	×	DETECT	Anti-Virus	Behavioral.Geo.Kazakhsta	e URL	http://www.testupdate.info/upd	Class: Infecting URL,Risk:	ENABLE
	\bigcirc	PREVENT	Anti-Virus	Behavioral.Geo.Belgium.	: IP	89.249.73.202	Owner: M247 Ltd, Class: II	-
		PREVENT	Anti-Virus	Behavioral.Geo.Brazil.C2.	DOMAIN	testupdate.info	Class: Infecting URL,Risk:	X DISABLE
		DETECT	Anti-Virus	Behavioral.Geo.Kazakhsta	URL	http://www.testupdate.info/clrls	Class: Infecting URL,Risk:	DETECT
	\bigcirc	DETECT	Anti-Virus	Behavioral.Geo.Nigeria.O	IP	83.229.3.151	Owner: SkyVision Global N	
		DETECT	Anti-Virus	Behavioral Geo Iceland O	IP	82 221 103 244	Owner: Thor Data Center	



Los IoC se publican a través de URL Feeds (direcciones URL propias de la plataforma de Portal NOW de Check Point). El URL Feed que usaremos principalmente será el basado en comportamiento (Behavioral) que se crea automáticamente, debemos hacer que este URL Feed sea accesible a través de Internet, habilitando el modo *Public.*

HORIZON NDR	าdrtest v	Д.	dgar Pajuelo	S × ∞ <
🎯 Indicators		🔉 Regenerate URLs 🛛 👁 Show Data Set URLs 🛛 \star New 🍞 Edit 📄 Delete 🛛 😋 Refr	sh T	
🛼 Data Sets	Name	Description	🗘 🛛 Public 🗘	Last Pull 🗘
📢 Feeds	Behavioral	Threat indicators generated by AI/ML engines	×	2022-11-27 21:19

* Name		* Name	
Behavioral		Behavioral	
Description		Description	
Threat indicators g	enerated by AI/ML engines	Threat indicators g	enerated by AI/ML engines
Public	Apply on NDR Sensors ¹	Public	Apply on NDR Sensors ¹
	¹ of the current domain		¹ of the current domain

Luego, el URL Feeds ya serán accesibles y se podrá utilizar para incorporarlos en herramientas de seguridad de Check Point o fabricantes terceros. La opción "Show Data Ser URLs" nos mostrara las direcciones URL, debemos utilizar la URL Feed de *Prevent URL*, que es la que contiene los loC habilitados (enabled) para prevención de amenazas en formato csv.

HORIZON NDR	า Indrtest v		
🞯 Indicators		Ð	Regenerate URLs 🛛 Show Data Set URLs 👫 New
🛱 Data Sets	Name	2	Description
🔇 Feeds	Behavioral		Threat indicators generated by AI/ML engines

DATASET URLS					
Prevent URL: https://feeds.now.checkpoint.com/public_feeds/5w2XTBo6ALu_0jWdKOQARrbH.csv COPY URL COPY FULL COMMAND COPY FULL COMMAND					



Prevención de Amenazas empleando sensor NDR

Quantum Gateways. - La URL Feed de *Prevent URL*, la podemos incorporar como un *IoC Indicator* en los firewalls de Check Point, de manera que todo tráfico que coincida con ese IoC (hash, IP, dominio, URL, etc.) será bloqueado de manera automática por el firewall, tanto para tráfico entrante como saliente (requiere R81 o superior.).

Dentro del Smart Console, en la política de Prevención de Amenazas (Threat Prevention), debemos ir a **Indicators** y luego *New*, llenamos la información y colocamos la *URL Feed Prevent* del Portal NDR, al finalizar debemos verificar la descarga con "Test Conectivity"

	Indicator Q 😯 🗙
	NDR Enter Object Comment
Custom Policy Tools ······	To use Thread Indicators the Autonomous Thread Dravention
Profiles	• To use milear indicators, the Autonomous milear prevention
IPS Protections	✓ Active
Protections	Feed URL: https://feeds.now.checkpoint.com/public_feeds/zzSV 🧶
Nhitelist Files	✓ Use gateway proxy for connection
Indicators	Authentication 🗸
🗘 Updates	Custom feed settings
🛇 UserCheck	Test Connectivity
惧 Threat Wiki 🖗	
Installation History	Add Tag
	OK Cancel

Adicionalmente, podemos también verificar la descarga de los IoC, colocando la URL Feed en un navegador, descargara un archivo en formato CSV, con los IoC habilitados y en modo *prevent* que se han creado en el Portal NOW del NDR.

	А		С	D			G
	# UNIQ-NAME	VALUE	ТҮРЕ	CONFIDENCE	SEVERITY	PRODUCT	COMMENT
2	Behavioral.Geo.Brazil.C2.Out	testupdate.info	Domain	HIGH	HIGH	AV	Class: Infecting URL,Risk: 100
3	Behavioral.Geo.Belgium.Out.	89.249.73.202	IP	LOW	HIGH	AV	Owner: M247 Ltd, Class: Infection Source,Risk: 64
4							



Referencias y Notas:

Horizon NDR Deployment Guide

https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Horizon-NDR-DeploymentGuide/Content/Topics-NDR-DG/Introduction.htm

NOTA 1: Para verificar conectividad hacia el portal NOW de Check Point desde el GAIA, debemos ejecutar en modo experto:

curl_cli portal.now.checkpoint.com >> Resolucion DNS nslookup https://portal.now.checkpoint.com >> Conectividad con Portal NDR cpopenssl s_client -showcerts -connect 35.156.213.136:443 cpopenssl s_client -showcerts -connect 18.196.115.85:443 cpopenssl s_client -showcerts -connect 35.157.19.226:443

NOTA 2: En caso de implementar NDR para análisis de trafico de servidores virtuales en infraestructura VMware, debemos verificar que modo de VM Network emplean los hosts que conforman el clúster de VMware:

- Distributed Switch:
 - Debemos desplegar una VM de NDR por cada host (ESXi Server) del cluster.
 - Debemos usar Distributed Port (DP) Mirror, para tener un "mirror"
 - La security policy en el DP debe tener "promiscuous accept", "forged Accept" y la 3era opción también en accept
- Standard Switch:
 - Debemos desplegar una VM de NDR por cada VM Network (VLAN) que deseamos monitorizar.
 - Cada VM de NDR debe tener una vNic en "promiscuous mode"