Implementación

Documento Técnico Final Cortex XDR

Versión 1.0

Alcaldía de Medellín
Distrito de
Ciencia, Tecnología e Innovación

CUIDAD:	Medellin
FECHA:	15 Abril 2024
EMPRESA:	Secretaría de Seguridad y Convivencia de Medellín
DIRECCION:	Calle 45 N° 55 65, Edificio Business Plaza
TELEFONO:	315 8153441
PERSONA DE CONTACTO:	Cristian Morales
CARGO:	Profesional Seguridad Informática
RESPONSABLE BOYRA:	Proyectos y servicios

LISTA DE CONTACTOS

SECRETARIA DE MEDELLIN

Nombre	Cargo	Teléfono	Email
Cristian Morales Garcés	Profesional Seguridad Informática	315 8153441	cristian.morales@medellin.gov.co

BOYRA S.A.

Nombre	Cargo	Teléfono	Email
Andres Alvarez	Gerente Proyectos y servicios	+601 9156130	helpdesk@boyra.com andres.alvarez@boyra.com

TABLA DE CONTENIDO

1. OBJETIVO 5
2. RESUMEN EJECUTIVO 5
3. DETALLE DEL LICENCIAMIENTO 6
4. ARQUITECTURA DE LA SOLUCIÓN 7
5. CONFIGURACIÓN CORTEX XDR 9
5.1. SETTINGS 9
5.1.1. ACCESS MANAGEMENT 9
5.1.2. GENERAL 11
5.1.3. INTEGRATIONS - CLOUD IDENTITY ENGINE 15
5.1.4. CORTEX XDR – ANALYTICS 16
5.1.5. BROKER VMS 17
5.1.6. EXCEPTIONS CONFIGURATION 18
5.2. ENDPOINTS & ENDPOINTS GROUPS 19
5.3. PREVENTION POLICIES 20
5.3.1. PROFILES 20
5.3.2. GLOBAL EXCEPTIONS 26
5.3.3. PREVENTION POLICY RULES 26
5.4. EXTENSION POLICIES 30
5.4.1. PROFILES 30
5.4.2. EXTENSION POLICY RULES 31
5.5. DETECTION RULES 33
5.5.1. IOC RULES 33
5.5.2. BIOC RULES 34
5.6. INCIDENT RESPONSE 35
5.6.1. BLOCK LIST 35
5.6.2. ALLOW LIST 35
5.6.3. SCORING RULES 36
6. PENDIENTES 37
7. RECOMENDACIONES 37

NOTA DE PROPIEDAD

La información y datos contenidos en todas las páginas de este documento de naturaleza comercial, técnica o financiera elaborado por *BOYRA* es información confidencial y privilegiada de *BOYRA*, y Sistema Integrado de Emergencia y Seguridad Metropolitana (SIES-M). La citada información se facilita a Sistema Integrado de Emergencia y Seguridad Metropolitana (SIES-M) bajo las más estrictas obligaciones de confidencialidad, en el bien entendido que éste no la usará sin permiso de BOYRA, para propósitos distintos al uso interno del presente proyecto.

1. OBJETIVO

Este documento detalla la infraestructura del Tenant de Cortex XDR Pro ***sies-m.xdr.us.paloaltonetworks.com*** de Palo Alto Networks, incluyendo su plataforma, componentes y configuración implementada en para **SIES-M**.

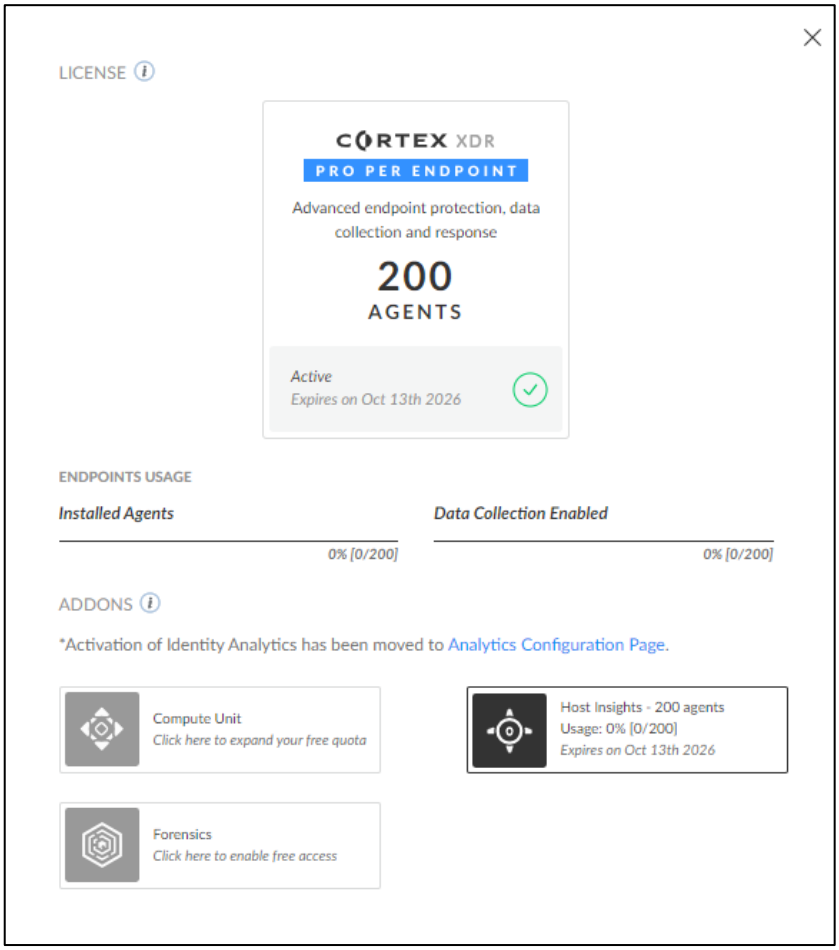
2. RESUMEN EJECUTIVO

SIES-M ha adquirido 200 licencias de agentes para la solución de Cortex XDR Pro de Palo Alto Networks en conjunto con el add-on de Host Insights, permitiendo tener una visibilidad completa del comportamiento del usuario y la actividad de endpoints, y simplifica la investigación de amenazas al correlacionar los logs de los sensores para revelar las causas y líneas de tiempo alrededor de las amenazas o actividades sospechosas. La aplicación también permite realizar acciones de respuesta inmediata y finalmente, para detener futuros ataques, se definen reglas para detectar y responder a actividades maliciosas.

3. DETALLE DEL LICENCIAMIENTO

La siguiente tabla detalla el número de licencias adquiridas para el uso de la solución de Protección Avanzada – Cortex Pro y sus respectivos addons adquiridos.

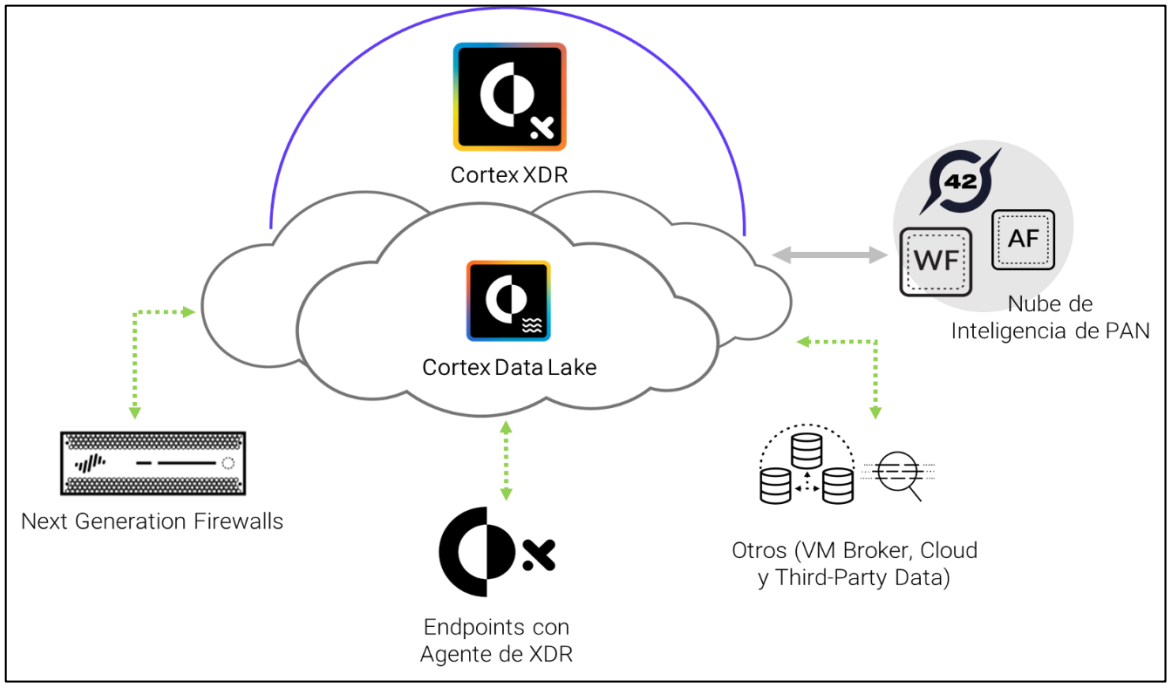
Tenant ID	SIES-M
URL	*https://sies-m.xdr.us.paloaltonetworks.com/*
Region	United States - Americas
Serial Number	0220980000024432
Licenciamiento	Pro per endpoint 200 Add-ons: Host Insights



Licenciamiento

4. ARQUITECTURA DE LA SOLUCIÓN

La arquitectura de Cortex XDR es ilustrada en la siguiente imagen.



Topología de la red

El despliegue incluye los siguientes componentes:

- Integración con WildFire, nube de inteligencia de PAN.
- Endpoints con agente de Cortex XDR.

La siguiente tabla detalla las versiones actuales de la solución Cortex XDR:

CORTEX XDR VERSION	UI VERSION	SERVER VERSION	WILDFIRE SERVER
Cortex XDR V3.8	v3.8.0-3896-gc022a50fa	master-v3.8.0-5168-g941e6	wildfire.paloaltonetworks.com



Detalle del versionamiento de Cortex XDR

5. CONFIGURACIÓN CORTEX XDR

La configuración actual de los componentes de Cortex XDR será detallada en esta sección.

5.1. SETTINGS

5.1.1. ACCESS MANAGEMENT

Se muestra a continuación los **roles** configurados para la gestión de Cortex XDR.

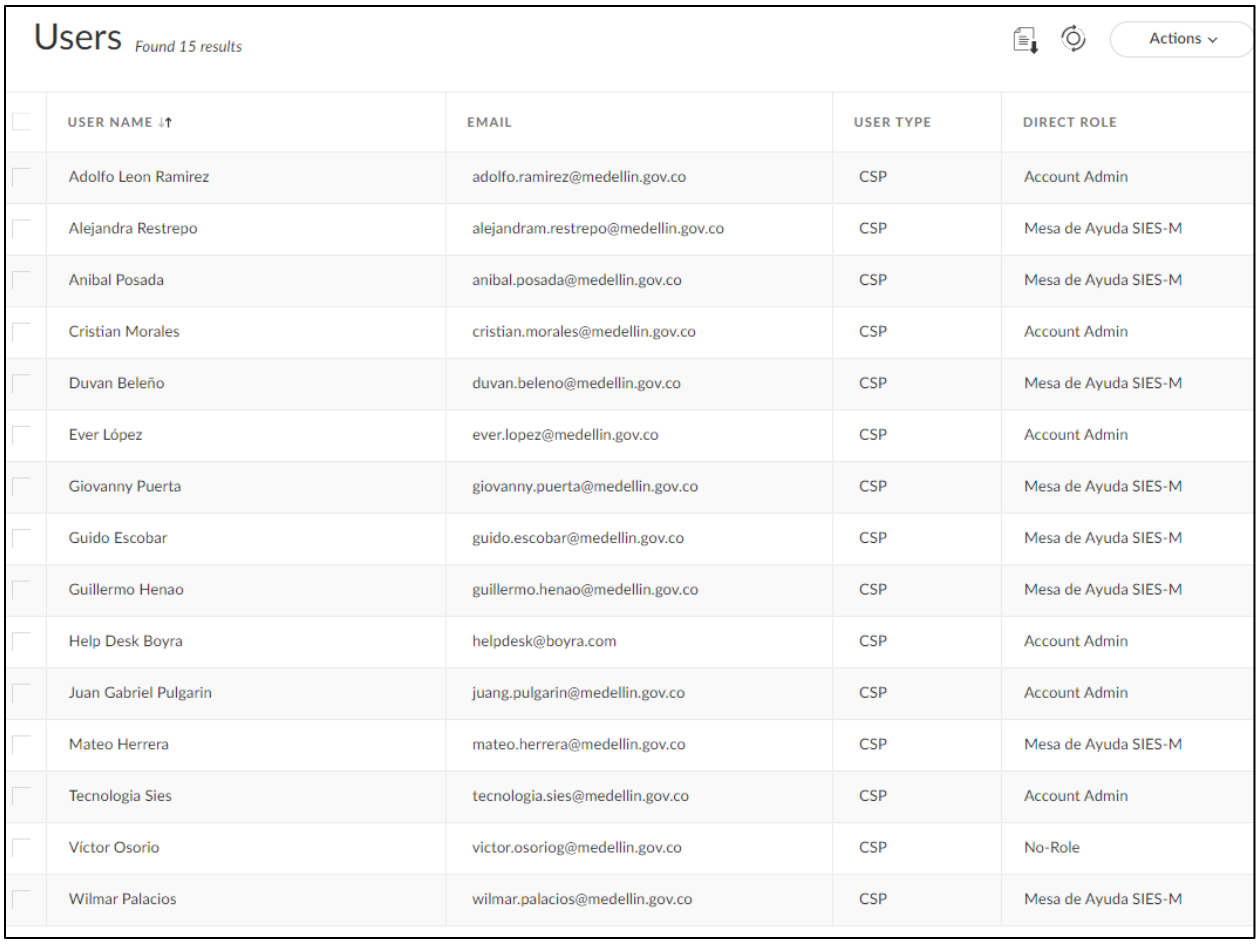
Roles Found 16 results

+ New Role | Type your search here

ROLE NAME	CREATED BY	DESCRIPTION
Mesa de Ayuda SIES-M	helpdesk@boyra.com	Perfil para los analistas de Mesa de Ayuda
Super user	tecnologia.sies@medellin.gov.co	Rol creado para el deploy de XDR
Scoped Endpoint Admin	Palo Alto Networks	Access only to product areas that support endpoint scoped based access control (SBAC) - Endpoint Administration, Action C...
Privileged Investigator	Palo Alto Networks	Can view and triage alerts, incidents and rules, and the view profiles and policies and Analytics management screens.
IT Admin	Palo Alto Networks	Can manage and control endpoints and installations, configure brokers, view profiles and policies, and view alerts.
Account Admin	Palo Alto Networks	The user(s) have full access to the given app(s), including all instances added of the app(s) in the future. App Administrator ca...
Viewer	Palo Alto Networks	Can view the majority of the features of the XDR app for this instance.
Deployment Admin	Palo Alto Networks	Can manage and control endpoints and installations, and configure brokers.
Instance Administrator	Palo Alto Networks	The user(s) have full access to the app instance for which this role is assigned. The Instance Administrator can also make othe...
Investigator	Palo Alto Networks	Can view and triage alerts and incidents
Privileged IT Admin	Palo Alto Networks	Can manage and control endpoints and installations, configure brokers, create profiles and policies, view alerts, and initiate Li...
Security Admin	Palo Alto Networks	Can triage and investigate alerts and incidents, respond (excluding Live Terminal), and edit profiles and policies.
Privileged Responder	Palo Alto Networks	Can view and triage alerts and incidents, access all response capabilities, and configure rules, policies, and profiles.
Responder	Palo Alto Networks	Can view and triage alerts, and access all response capabilities excluding Live Terminal.
Privileged Security Admin	Palo Alto Networks	Can triage and investigate alerts and incident, respond, and edit profiles and policies.
Investigation Admin	Palo Alto Networks	Can view and triage alerts and incidents, configure rules, and view the profiles and policies and Analytics management screen...

Roles

Se muestra a continuación los **usuarios** configurados para la gestión y el acceso al tenant de Cortex XDR.



Users *Found 15 results*

Actions

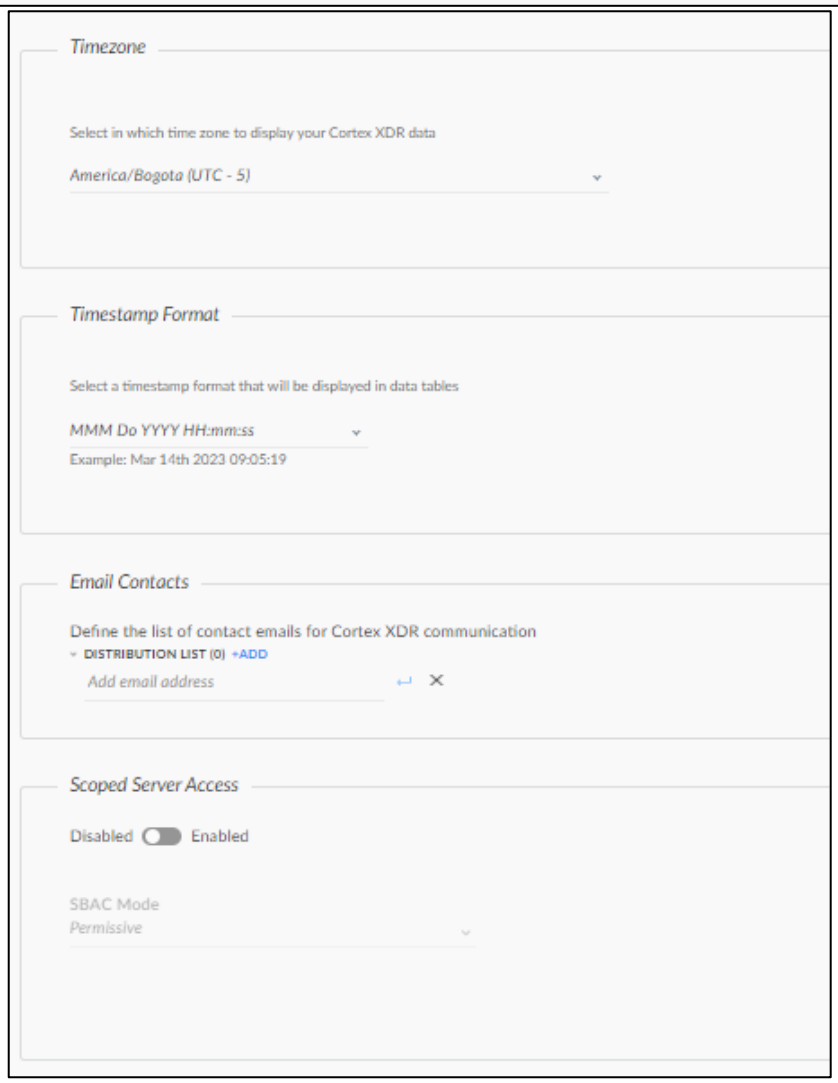
USER NAME	EMAIL	USER TYPE	DIRECT ROLE
Adolfo Leon Ramirez	adolfo.ramirez@medellin.gov.co	CSP	Account Admin
Alejandra Restrepo	alejandram.restrepo@medellin.gov.co	CSP	Mesa de Ayuda SIES-M
Anibal Posada	anibal.posada@medellin.gov.co	CSP	Mesa de Ayuda SIES-M
Cristian Morales	cristian.morales@medellin.gov.co	CSP	Account Admin
Duvan Beleño	duvan.beleno@medellin.gov.co	CSP	Mesa de Ayuda SIES-M
Ever López	ever.lopez@medellin.gov.co	CSP	Account Admin
Giovanny Puerta	giovanny.puerta@medellin.gov.co	CSP	Mesa de Ayuda SIES-M
Guido Escobar	guido.escobar@medellin.gov.co	CSP	Mesa de Ayuda SIES-M
Guillermo Henao	guillermo.henao@medellin.gov.co	CSP	Mesa de Ayuda SIES-M
Help Desk Boyra	helpdesk@boyra.com	CSP	Account Admin
Juan Gabriel Pulgarin	juang.pulgarin@medellin.gov.co	CSP	Account Admin
Mateo Herrera	mateo.herrera@medellin.gov.co	CSP	Mesa de Ayuda SIES-M
Tecnologia Sies	tecnologia.sies@medellin.gov.co	CSP	Account Admin
Víctor Osorio	victor.osoriog@medellin.gov.co	CSP	No-Role
Wilmar Palacios	wilmar.palacios@medellin.gov.co	CSP	Mesa de Ayuda SIES-M

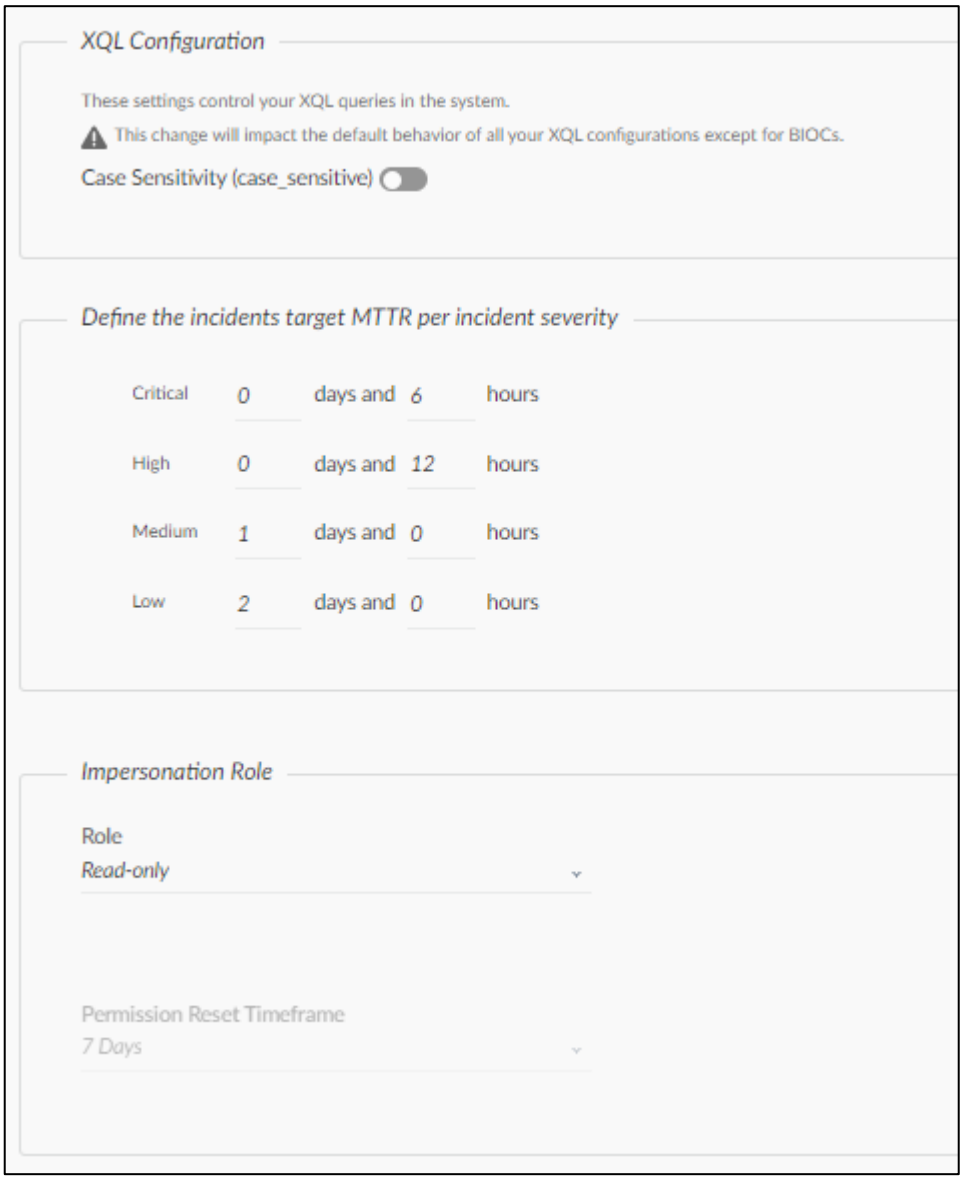
Usuarios

5.1.2. GENERAL

Se muestra a continuación la configuración realizada para **Server Settings** de Cortex XDR.

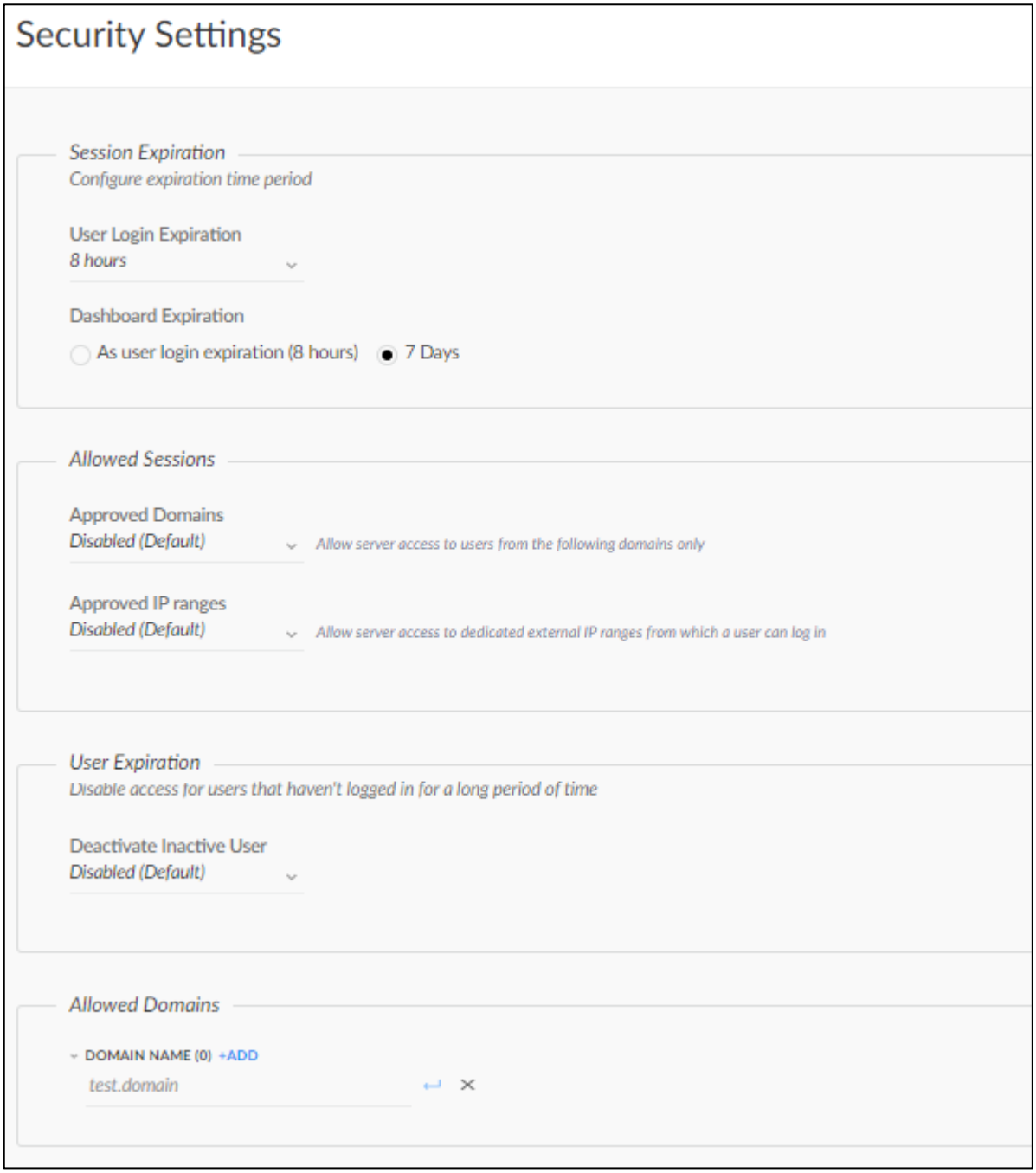






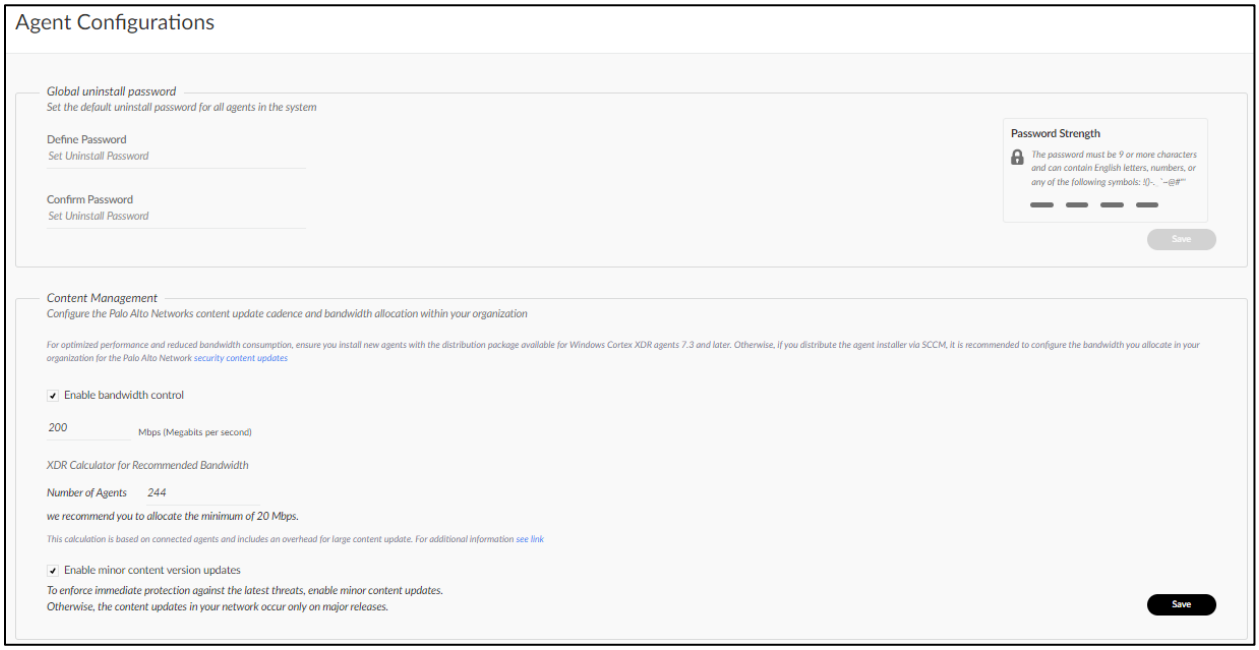
Server Settings.

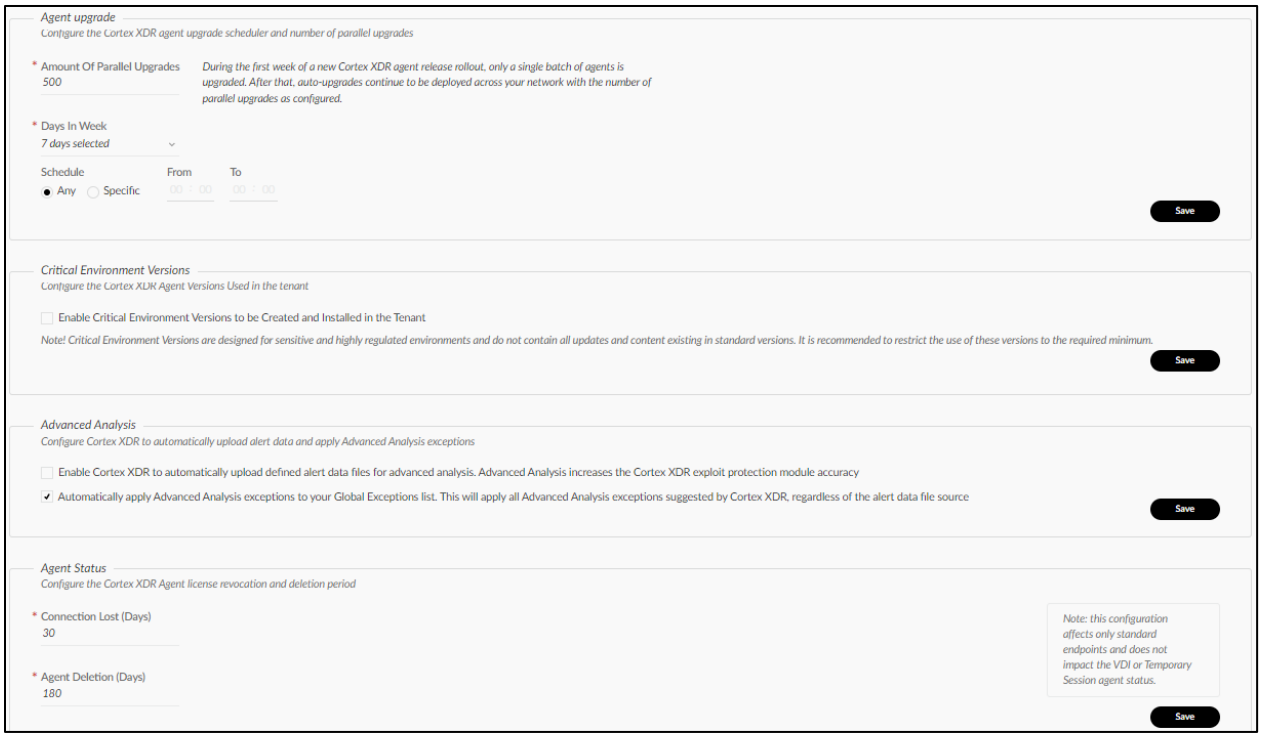
Se muestra a continuación la configuración realizada para **Security Settings** de Cortex XDR.

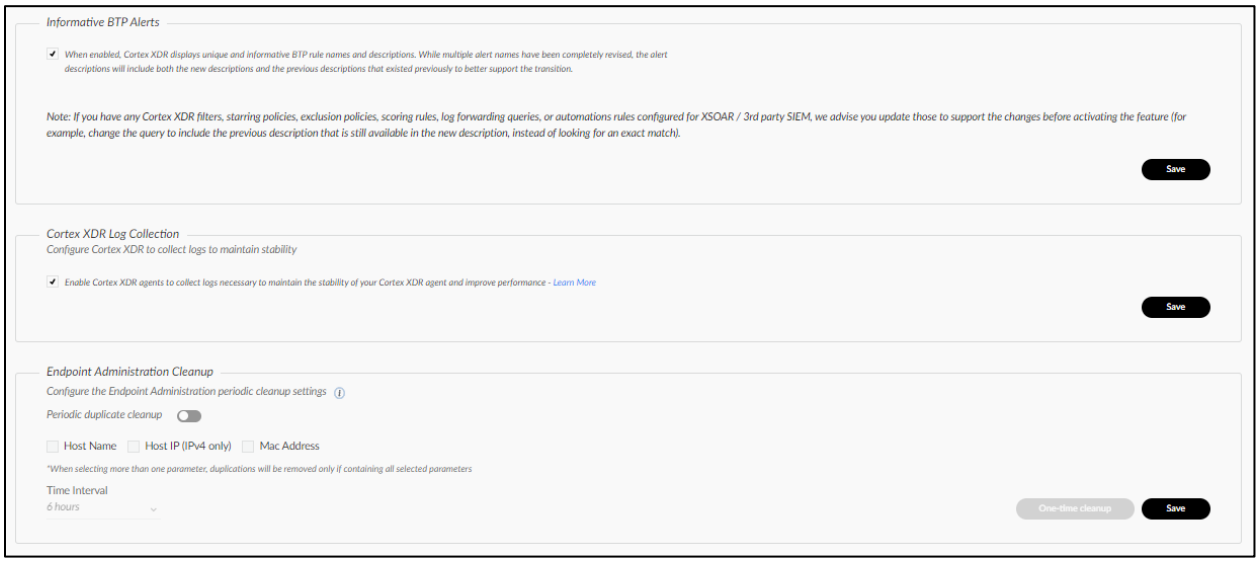


Security Settings.

Se muestra a continuación la configuración realizada para **Agent Configuration** de Cortex XDR.



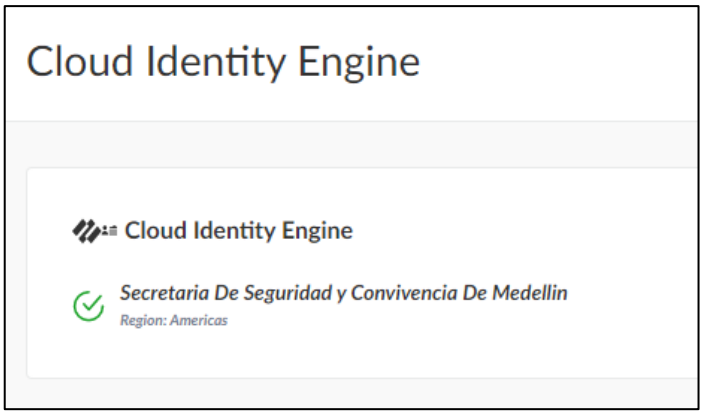




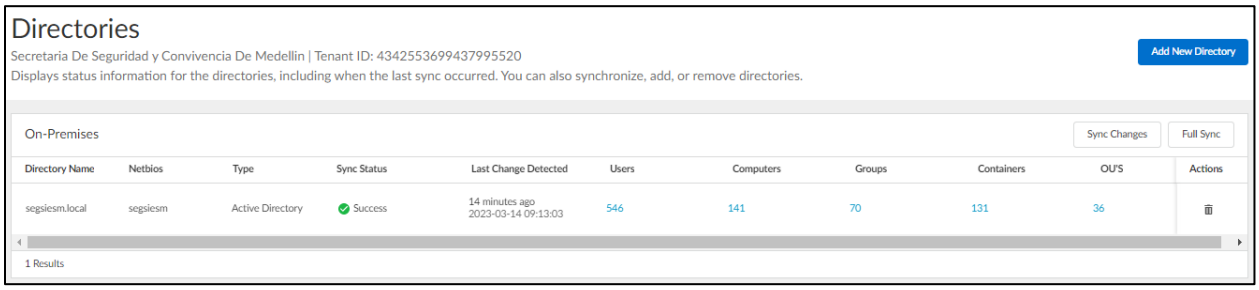
Agent Configuration.

5.1.3. INTEGRATIONS - CLOUD IDENTITY ENGINE

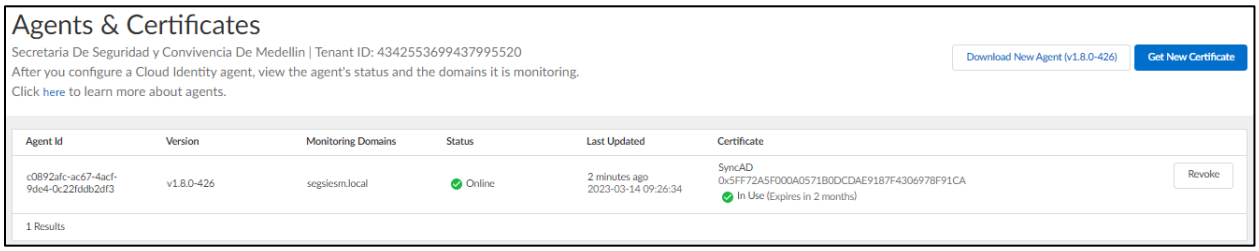
Se muestra a continuación la configuración realizada para la integración con el **Cloud Identity Engine** y Cortex XDR.



Cloud Identity Engine - Cortex XDR.



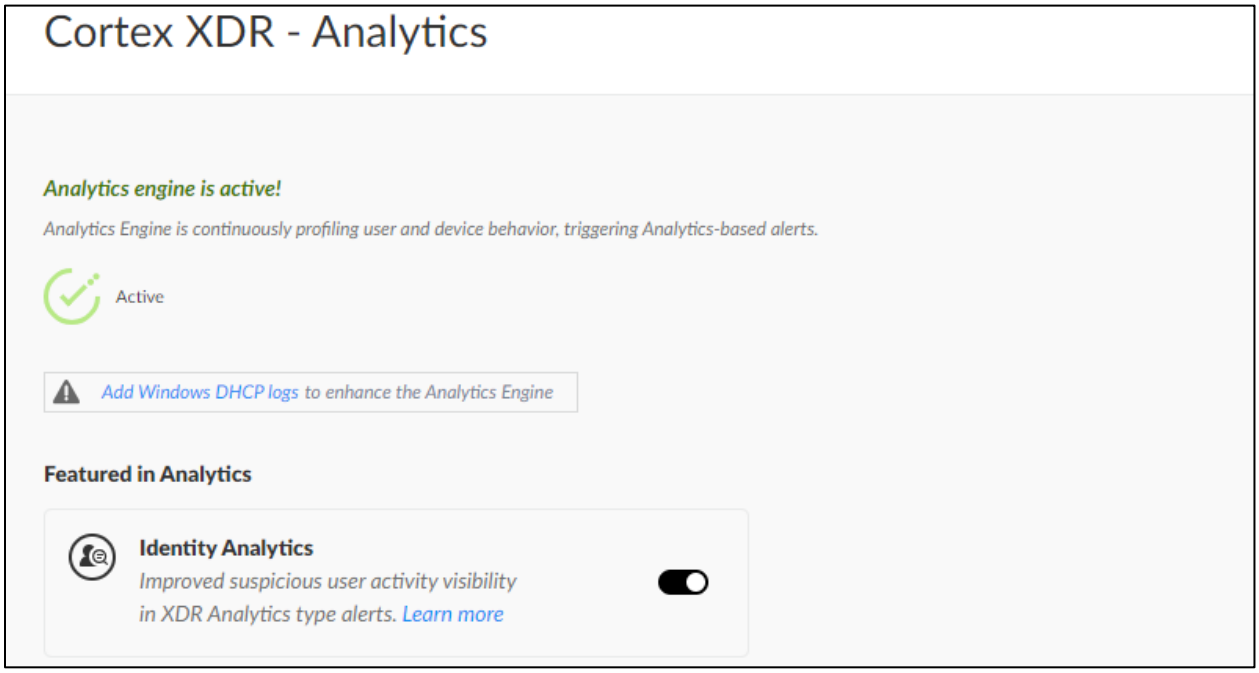
Cloud Identity Engine – Directory Sync.



Cloud Identity Engine – Agents & Certificates.

5.1.4. CORTEX XDR – ANALYTICS

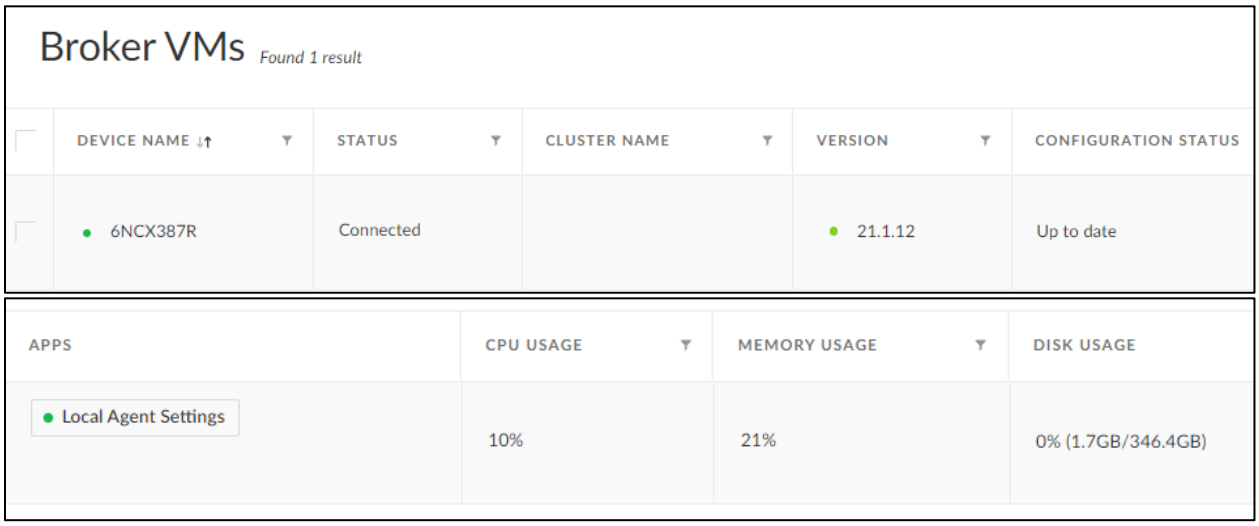
Se muestra a continuación la configuración realizada para la activación del **Analytics Engine** y el **Identity Analytics.**



Cortex XDR – Analytics.

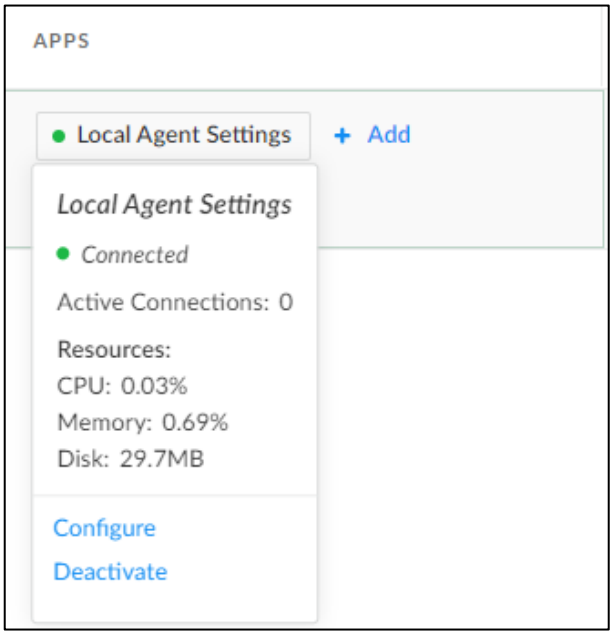
5.1.5. BROKER VMS

Se muestra a continuación la correcta sincronización y el detalle de la configuración del servidor asignado como Broker VM y sus respectivos porcentajes de uso en los recursos de este.



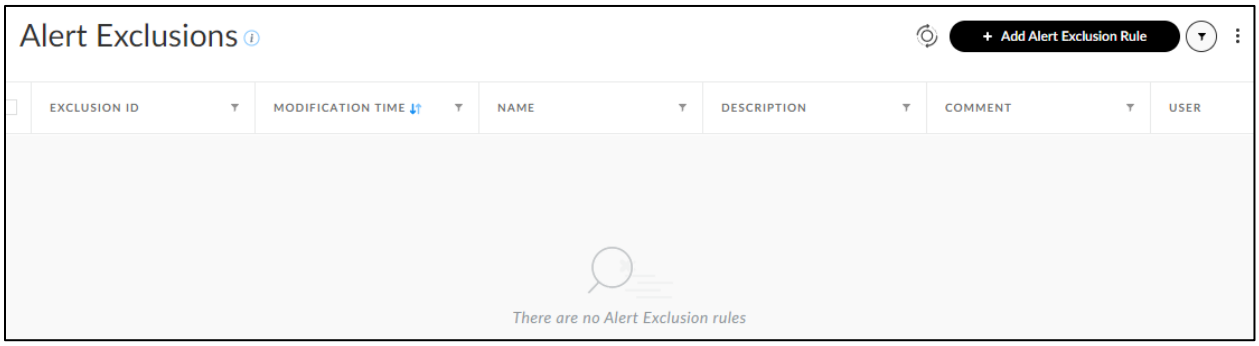
Broker VMs – Servidor Z34QJMQM.

Adicionalmente, se muestra las aplicaciones activas



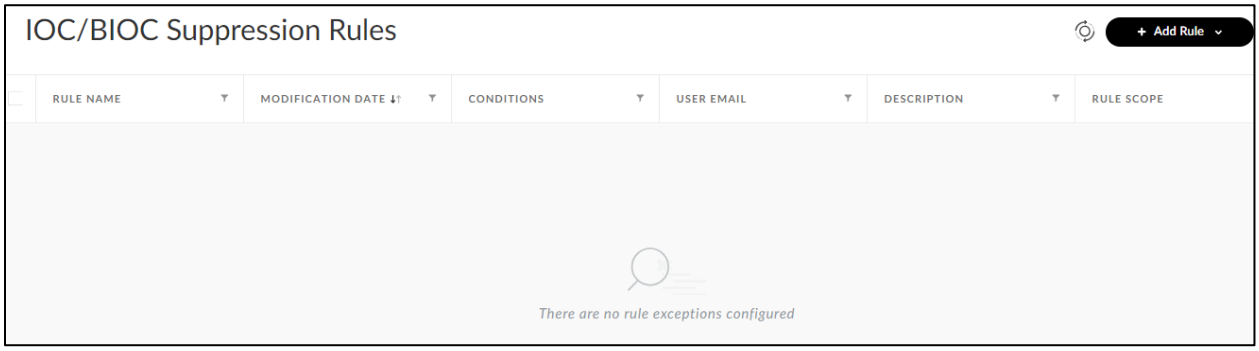
5.1.6. EXCEPTIONS CONFIGURATION

Se muestra a continuación las excepciones configuradas en base al análisis de los incidentes que se presentaron en el momento de realizar a la implementación de Cortex XDR.



Alert Exclusions.

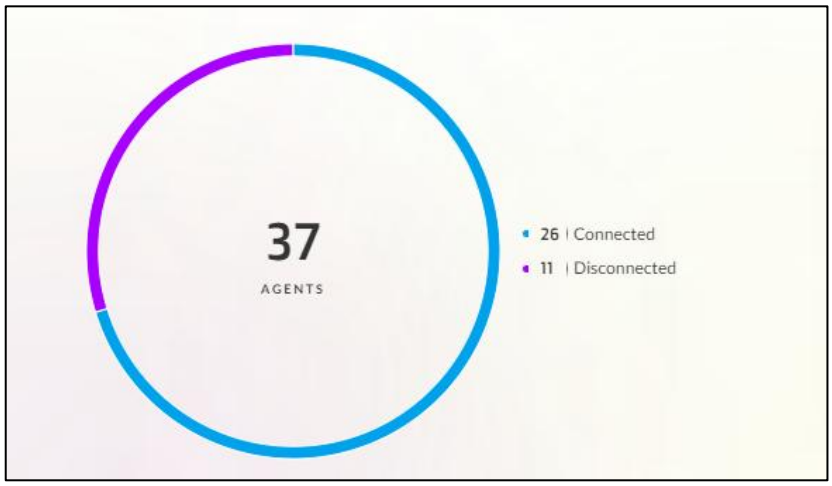
No se realizó ninguna exclusión a raíz de alguna alerta o incidente detectado por Cortex XDR.



IOC/BIOC Suppresion Rules.

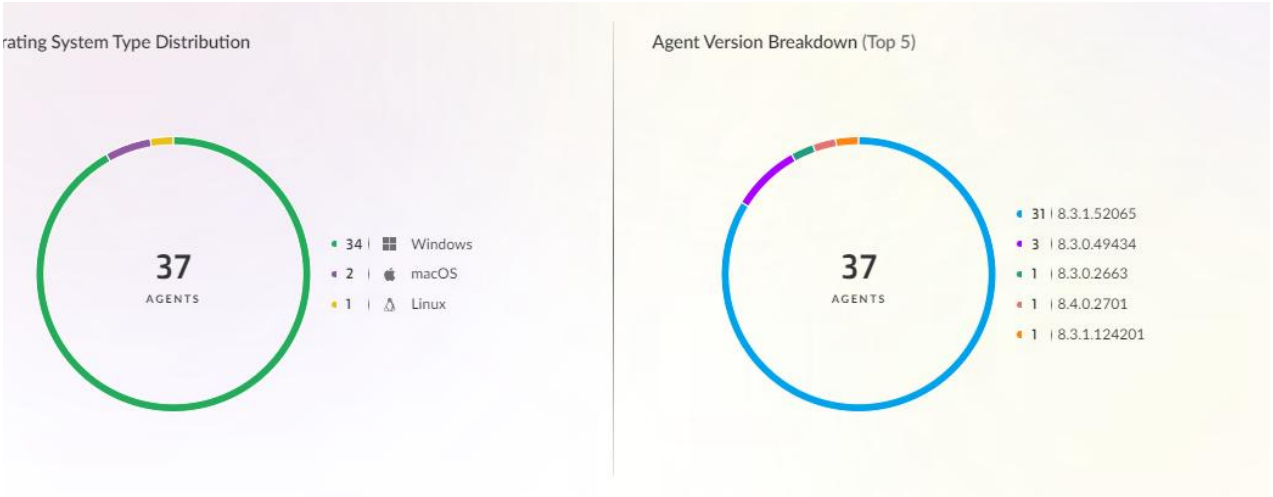
5.2. ENDPOINTS & ENDPOINTS GROUPS

Al momento se tiene un total de **37 endpoints** con el agente de Cortex XDR instalado.



Endpoints.

Se muestra a continuación que tipo de sistemas operativos se tiene en la consola y la versión de la agente instalada en estos endpoints.



Operation System & Agent Version Enpoitns

Se muestra a continuación los **1 Endpoints Groups** configurados en la plataforma.



Endpoint Groups Found 1 result

LAST UPDATED	GROUP NAME	GROUP TYPE	DESCRIPTION	FILTER	MEMBERS COUNT
Mar 8th 2023 16:14:40	VPN Users SIES-M	Static	Protección para usuarios VPN GP SIES-M	*endpoint* in VOSORIOG, JORGEGARCIA, CMORALEG **AND** *status* != *Uninstalled*	3

Endpoints Groups.

5.3. PREVENTION POLICIES

5.3.1. PROFILES

Se muestra a continuación los **Prevention Profiles** tipo **Exploit** para Windows configurados en la plataforma, incluyendo el perfil Default.

PLATFORM	TYPE	NAME	ASSOCIATED TARGETS	SUMMARY	USAGE COUNT
Windows (3)					
	Exploit	Visibility	*operating system contains Windows*	Browser Exploits Protection - Report Logical Exploits Protection - Report Known Vulnerable Processes Protection - Report Operating System Exploit Protection - Report Exploit Protection for Additional Processes - Report Unpatched Vulnerabilities Protection - Do not modify system settings	1
	Exploit	Enforcement	*operating system contains Windows*	Browser Exploits Protection - Block Logical Exploits Protection - Block Known Vulnerable Processes Protection - Block Operating System Exploit Protection - Block Exploit Protection for Additional Processes - Block Unpatched Vulnerabilities Protection - Do not modify system settings	1
	Exploit	Default	*Any*	Browser Exploits Protection - Block Logical Exploits Protection - Block Known Vulnerable Processes Protection - Block Operating System Exploit Protection - Block Exploit Protection for Additional Processes - Disabled Unpatched Vulnerabilities Protection - Do not modify system settings	1

Prevention Profiles Exploit Windows.

Se muestra a continuación los **Prevention Profiles** tipo **Exploit** para macOS configurados en la plataforma, incluyendo el perfil Default.

PLATFORM	TYPE	NAME	ASSOCIATED TARGETS	SUMMARY
macOS (1)				
	Exploit	Default	*Any*	Browser Exploits Protection - Block Logical Exploits Protection - Block Known Vulnerable Processes Protection - Block Operating System Exploit Protection - Block Exploit Protection for Additional Processes - Disabled

Prevention Profiles Exploit macOS.

Se muestra a continuación los **Prevention Profiles** tipo **Exploit** para Linux configurados en la plataforma, incluyendo el perfil Default.

PLATFORM	TYPE	NAME	ASSOCIATED TARGETS	SUMMARY
Linux (1)				
	Exploit	Default	*Any*	Known Vulnerable Processes Protection - Block Operating System Exploit Protection - Block Exploit Protection for Additional Processes - Disabled

Prevention Profiles Exploit Linux.

Se muestra a continuación los **Prevention Profiles** tipo **Malware** para Windows configurados en la plataforma, incluyendo el perfil Default.

PLATFORM	TYPE	NAME	ASSOCIATED TARGETS	SUMMARY
Windows (3)				
	Malware	Visibility	***operating system*** *contains Windows*	Portable Executable and DLL Examination - Report Office Files with Macros Examination - Report Global Behavioral Threat Protection Rules - Report Respond to Malicious Causality Chains - Enabled Ransomware Protection - Report Malicious Child Process Protection - Report Endpoint Scanning - Enabled + 8 more
	Malware	Enforcement	***operating system*** *contains Windows*	Portable Executable and DLL Examination - Block Office Files with Macros Examination - Block Global Behavioral Threat Protection Rules - Block Respond to Malicious Causality Chains - Enabled Ransomware Protection - Block Malicious Child Process Protection - Block Endpoint Scanning - Enabled + 8 more
	Malware	Default	*Any*	Portable Executable and DLL Examination - Block Office Files with Macros Examination - Block Global Behavioral Threat Protection Rules - Block Respond to Malicious Causality Chains - Enabled Ransomware Protection - Block Malicious Child Process Protection - Block Endpoint Scanning - Disabled + 8 more

Prevention Profiles Malware Windows.

Se muestra a continuación los **Prevention Profiles** tipo **Malware** para macOS configurados en la plataforma, incluyendo el perfil Default.



PLATFORM	TYPE	NAME	ASSOCIATED TARGETS	SUMMARY
macOS (1)				
	Malware	Default	*Any*	Global Behavioral Threat Protection Rules - Block Endpoint Scanning - Disabled Mach-O Files Examination - Block Credential Gathering Protection - Block Anti Webshell Protection - Block Financial Malware Threat Protection - Block Cryptominers Protection - Block + 1 more

Prevention Profiles Malware macOS.

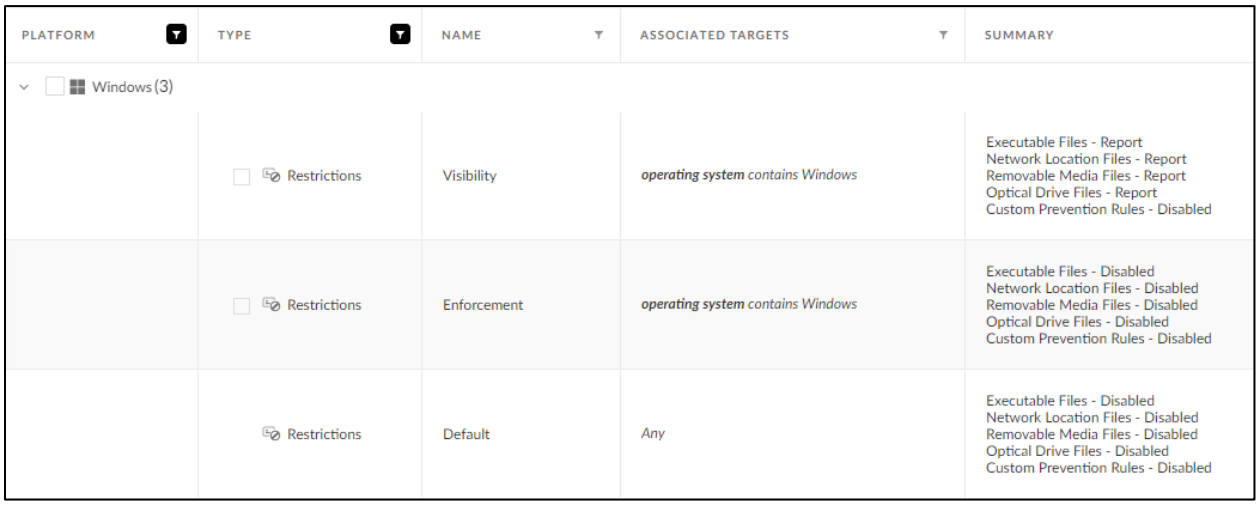
Se muestra a continuación los **Prevention Profiles** tipo **Malware** para Linux configurados en la plataforma, incluyendo el perfil Default.



PLATFORM	TYPE	NAME	ASSOCIATED TARGETS	SUMMARY
Linux (1)				
	Malware	Default	*Any*	Global Behavioral Threat Protection Rules - Block Endpoint Scanning - Disabled ELF Files Examination - Block Reverse Shell Protection - Block Local File Threat Examination - Enabled Credential Gathering Protection - Block Anti Webshell Protection - Block + 2 more

Prevention Profiles Malware Linux.

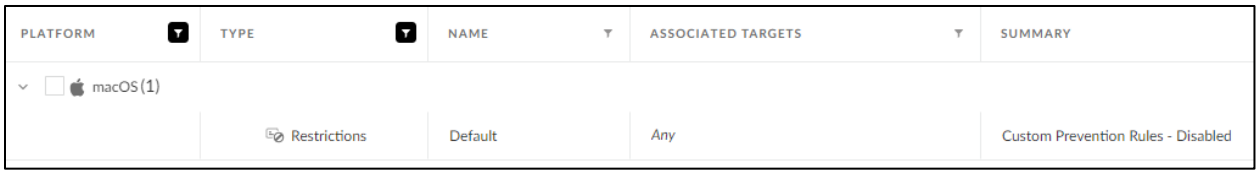
Se muestra a continuación los **Prevention Profiles** tipo **Restrictions** para Windows configurados en la plataforma, incluyendo el perfil Default.



PLATFORM	TYPE	NAME	ASSOCIATED TARGETS	SUMMARY
Windows (3)				
	Restrictions	Visibility	***operating system*** *contains Windows*	Executable Files - Report Network Location Files - Report Removable Media Files - Report Optical Drive Files - Report Custom Prevention Rules - Disabled
	Restrictions	Enforcement	***operating system*** *contains Windows*	Executable Files - Disabled Network Location Files - Disabled Removable Media Files - Disabled Optical Drive Files - Disabled Custom Prevention Rules - Disabled
	Restrictions	Default	*Any*	Executable Files - Disabled Network Location Files - Disabled Removable Media Files - Disabled Optical Drive Files - Disabled Custom Prevention Rules - Disabled

Prevention Profiles Restrictions Windows.

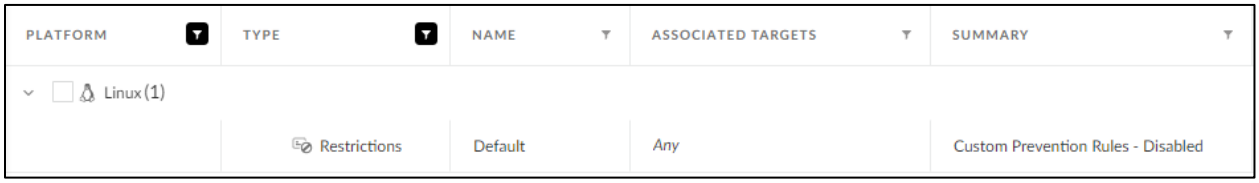
Se muestra a continuación los **Prevention Profiles** tipo **Restrictions** para macOS configurados en la plataforma, incluyendo el perfil Default.



PLATFORM	TYPE	NAME	ASSOCIATED TARGETS	SUMMARY
macOS (1)				
	Restrictions	Default	Any	Custom Prevention Rules - Disabled

Prevention Profiles Restrictions macOS.

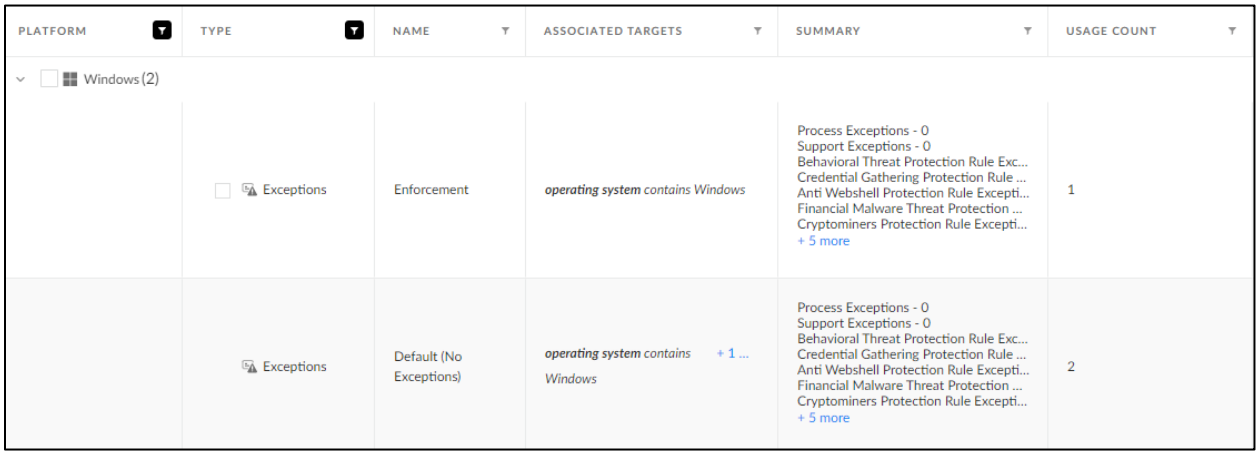
Se muestra a continuación los **Prevention Profiles** tipo **Restrictions** para Linux configurados en la plataforma, incluyendo el perfil Default.



PLATFORM	TYPE	NAME	ASSOCIATED TARGETS	SUMMARY
Linux (1)				
	Restrictions	Default	Any	Custom Prevention Rules - Disabled

Prevention Profiles Restrictions Linux.

Se muestra a continuación los **Prevention Profiles** tipo **Exceptions** para Windows configurados en la plataforma, incluyendo el perfil Default.



PLATFORM	TYPE	NAME	ASSOCIATED TARGETS	SUMMARY	USAGE COUNT
Windows (2)					
	Exceptions	Enforcement	*operating system contains Windows*	Process Exceptions - 0 Support Exceptions - 0 Behavioral Threat Protection Rule Exc... Credential Gathering Protection Rule ... Anti Webshell Protection Rule Excepti... Financial Malware Threat Protection ... Cryptominers Protection Rule Excepti... + 5 more	1
	Exceptions	Default (No Exceptions)	*operating system contains* + 1 ... *Windows*	Process Exceptions - 0 Support Exceptions - 0 Behavioral Threat Protection Rule Exc... Credential Gathering Protection Rule ... Anti Webshell Protection Rule Excepti... Financial Malware Threat Protection ... Cryptominers Protection Rule Excepti... + 5 more	2

Prevention Profiles Exceptions Windows.

Se muestra a continuación los **Prevention Profiles** tipo **Exceptions** para macOS configurados en la plataforma, incluyendo el perfil Default.



PLATFORM	TYPE	NAME	ASSOCIATED TARGETS	SUMMARY	USAGE COUNT
macOS (1)					
	Exceptions	Default (No Exceptions)	Any	Process Exceptions - 0 Support Exceptions - 0 Behavioral Threat Protection Rule Exc... Credential Gathering Protection Rule ... Anti Webshell Protection Rule Excepti... Financial Malware Threat Protection ... Cryptominers Protection Rule Excepti... + 2 more	1

Prevention Profiles Exceptions macOS.

Se muestra a continuación los **Prevention Profiles** tipo **Exceptions** para Linux configurados en la plataforma, incluyendo el perfil Default.



PLATFORM	TYPE	NAME	ASSOCIATED TARGETS	SUMMARY	USAGE
Linux (1)					
	Exceptions	Default (No Exceptions)	Any	Process Exceptions - 0 Support Exceptions - 0 Behavioral Threat Protection Rule Exception - 0 Credential Gathering Protection Rule Exception - 0 Anti Webshell Protection Rule Exception - 0 Financial Malware Threat Protection Rule Exception - 0 Cryptominers Protection Rule Exception - 0 + 3 more	1

Prevention Profiles Exceptions Linux.

Se muestra a continuación los **Prevention Profiles** tipo **Agent Settings** para Windows configurados en la plataforma, incluyendo el perfil Default.

PLATFORM	TYPE	NAME	ASSOCIATED TARGETS	SUMMARY	USAGE COUNT
Windows (3)					
	Agent Settings	Agent Pro	*operating system contains* Windows + 1 ...	Disk Space - 5000MB User Interface - Some Enabled Agent Security - Enabled Windows Security Center Integration ... Alert data dump file size - Full Automatically upload alert data dump... XDR Cloud License - Auto-Detect + 7 more	2
	Agent Settings	Agent Pro Broker VM		Disk Space - 5000MB User Interface - Some Enabled Agent Security - Enabled Windows Security Center Integration ... Alert data dump file size - Full Automatically upload alert data dump... XDR Cloud License - Auto-Detect + 7 more	0
	Agent Settings	Default	*Any*	Disk Space - 5000MB User Interface - Some Enabled Agent Security - Enabled Windows Security Center Integration ... Alert data dump file size - Full Automatically upload alert data dump... XDR Cloud License - Auto-Detect + 7 more	1

Prevention Profiles Agent Settings Windows.

Se muestra a continuación los **Prevention Profiles** tipo **Agent Settings** para macOS configurados en la plataforma, incluyendo el perfil Default.

PLATFORM	TYPE	NAME	ASSOCIATED TARGETS	SUMMARY	USAGE COUNT
macOS (1)					
	Agent Settings	Default	*Any*	Disk Space - 5000MB User Interface - Some Enabled Agent Security - Enabled Automatically upload alert data dump file - Disabled Collect prevention data - Enabled XDR Cloud License - Auto-Detect XDR Pro Endpoints - Disabled + 6 more	1

Prevention Profiles Agent Settings macOS.

Se muestra a continuación los **Prevention Profiles** tipo **Agent Settings** para macOS configurados en la plataforma, incluyendo el perfil Default.

PLATFORM	TYPE	NAME	ASSOCIATED TARGETS	SUMMARY	USAGE COUNT
Linux (1)					
	Agent Settings	Default	*Any*	Disk Space - 5000MB Automatically upload alert data dump file - Disabled Collect prevention data - Enabled XDR Cloud License - Auto-Detect Compliance collection - Disabled XDR Pro Endpoints - Disabled Content auto update - Enabled + 5 more	1

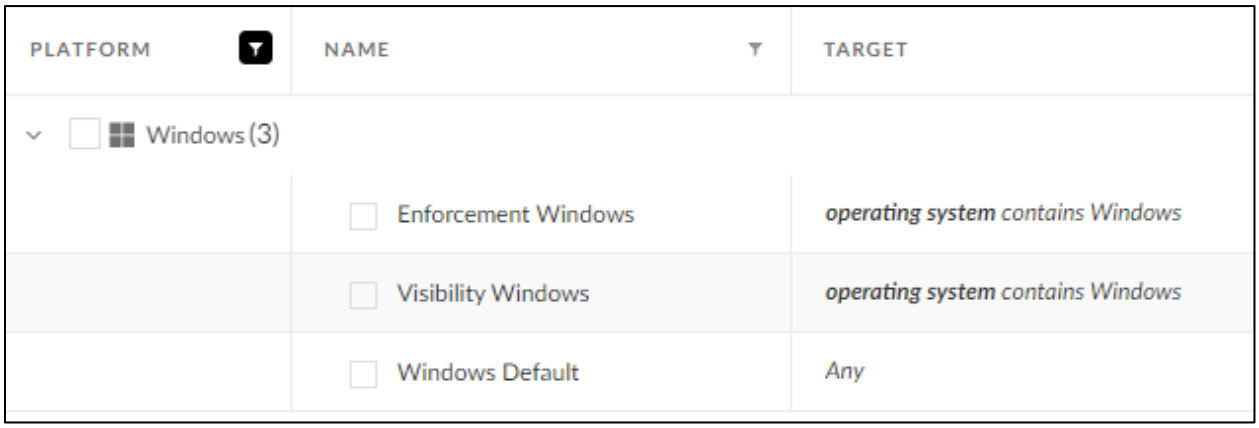
Prevention Profiles Agent Settings Linux.

5.3.2. GLOBAL EXCEPTIONS

No se creó ninguna **Global Exceptions** en el transcurso de la implementación.

5.3.3. PREVENTION POLICY RULES

Se muestra las **Prevention Policy Rules** configuradas para **Windows**, incluyendo la política Windows Default.



Prevention Policy Rules - Windows.

A continuación, se muestra el detalle de la política **Enforcement Windows**.



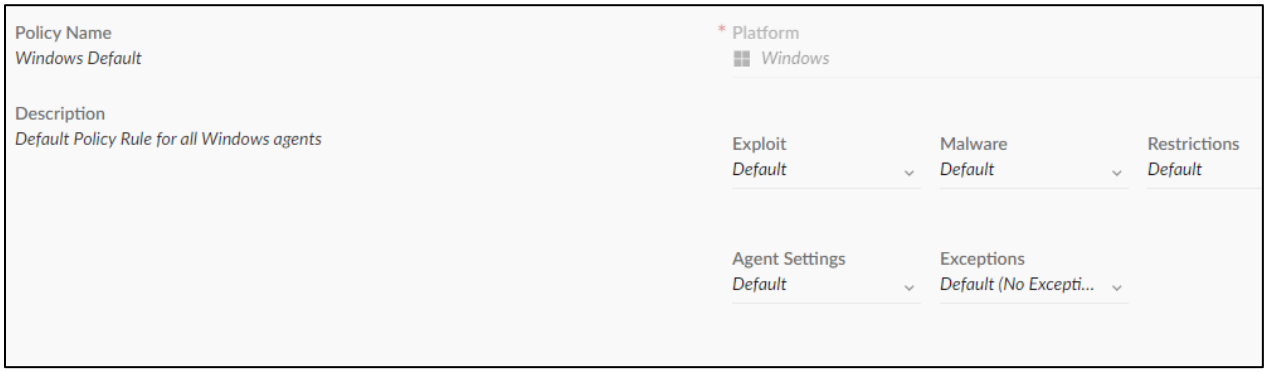
Prevention Policy Rules Enforcement Windows

A continuación, se muestra el detalle de la política **Visibility Windows.**



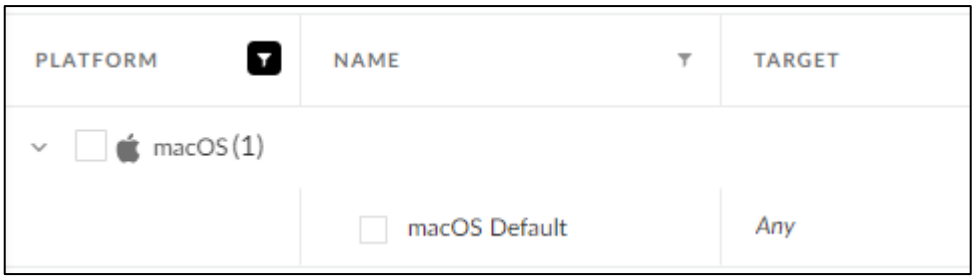
Prevention Policy Rules Visibility Windows.

A continuación, se muestra el detalle de la política **Windows Default.**



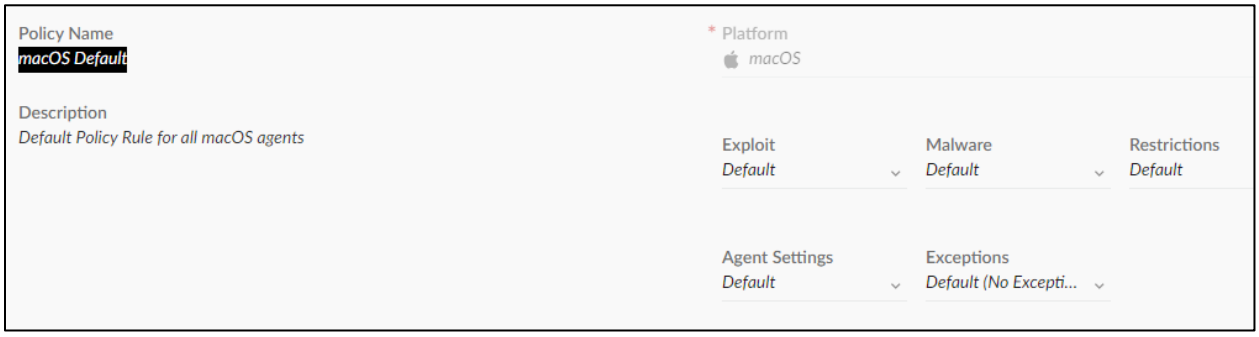
Prevention Policy Rules Windows Default.

Se muestra las **Prevention Policy Rules** configuradas para **macOS**, incluyendo la política macOS Default**.**



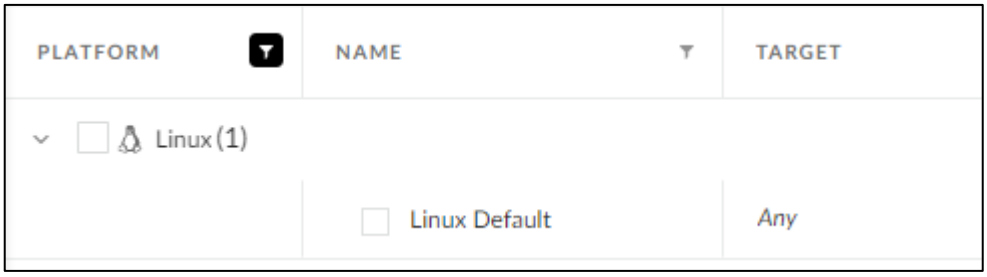
Prevention Policy Rules - macOS.

A continuación, se muestra el detalle de la política **macOS Default.**



Prevention Policy Rules macOS Default.

Se muestra las **Prevention Policy Rules** configuradas para **Linux**, incluyendo la política Linux Default**.**



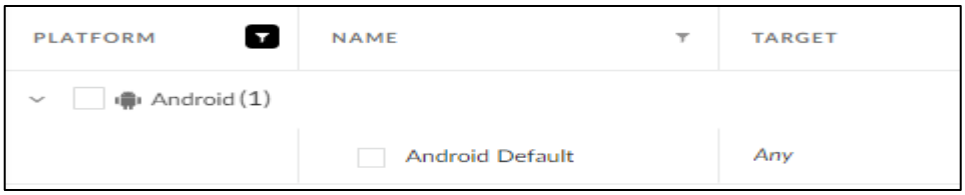
Prevention Policy Rules - Linux.

A continuación, se muestra el detalle de la política **Linux Default.**



Prevention Policy Rules Linux Default.

Se muestra las **Prevention Policy Rules** configuradas para **Android**, incluyendo la política Android Default



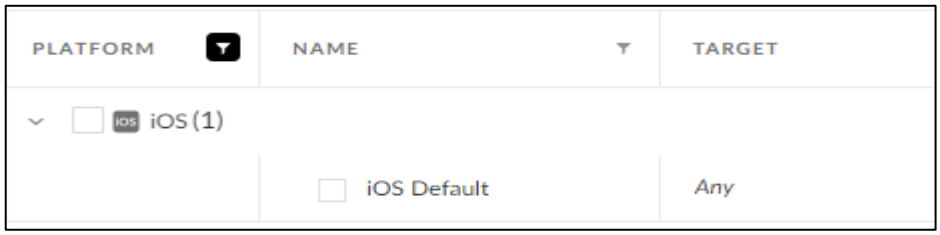
Prevention Policy Rules - Android.

A continuación, se muestra el detalle de la política **Android Default.**



Prevention Policy Rules - Android Default.

Se muestra las **Prevention Policy Rules** configuradas para **iOS**, incluyendo la política iOS Default.



Prevention Policy Rules – iOS.

A continuación, se muestra el detalle de la política **iOS Default.**

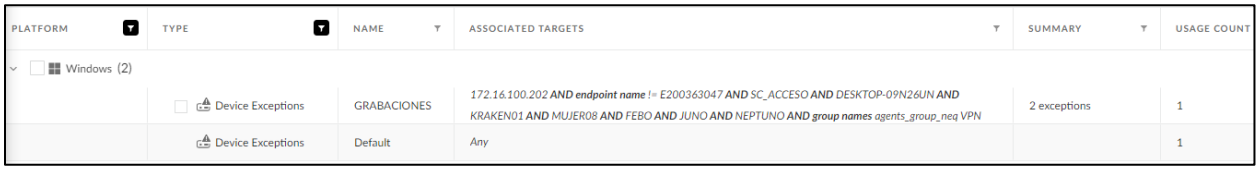


Prevention Policy Rules iOS Default.

5.4. EXTENSION POLICIES

5.4.1. PROFILES

Se muestra a continuación los **Extension Profiles** tipo **Device Exceptions** para Windows configurados en la plataforma, incluyendo el perfil Default.



PLATFORM	TYPE	NAME	ASSOCIATED TARGETS	SUMMARY	USAGE COUNT
Windows (2)					
	Device Exceptions	GRABACIONES	172.16.100.202 **AND endpoint name** != E200363047 **AND** SC_ACCESO **AND** DESKTOP-09N26UN **AND** KRAKEN01 **AND** MUJER08 **AND** FEBO **AND** JUNO **AND** NEPTUNO **AND group names** agents_group_neq VPN	2 exceptions	1
	Device Exceptions	Default	Any		1

Extension Profiles Device Exceptions Windows.

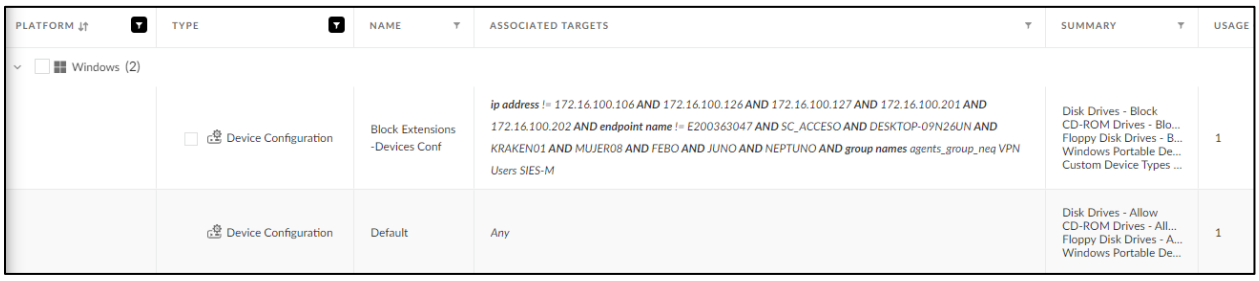
Se muestra a continuación los **Extension Profiles** tipo **Device Exceptions** para MacOS configurados en la plataforma, incluyendo el perfil Default.



PLATFORM	TYPE	NAME	ASSOCIATED TARGETS	SUMMARY	USAGE COUNT
macOS (1)					
	Device Exceptions	Default	Any		1

Extension Profiles Device Exceptions macOS.

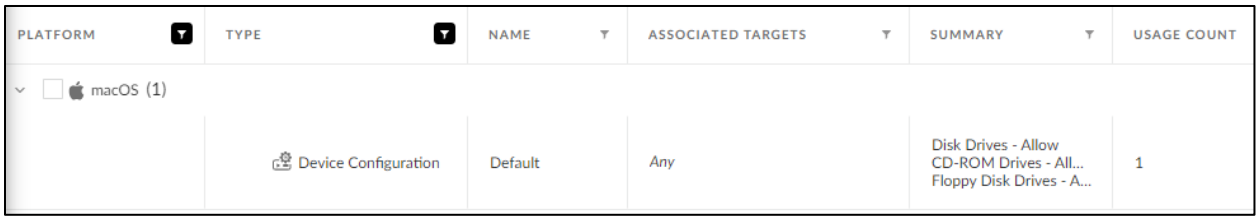
Se muestra a continuación los **Extension Profiles** tipo **Device Configuration** para Windows configurados en la plataforma, incluyendo el perfil Default.



PLATFORM	TYPE	NAME	ASSOCIATED TARGETS	SUMMARY	USAGE
Windows (2)					
	Device Configuration	Block Extensions -Devices Conf	**ip address** != 172.16.100.106 **AND** 172.16.100.126 **AND** 172.16.100.127 **AND** 172.16.100.201 **AND** 172.16.100.202 **AND endpoint name** != E200363047 **AND** SC_ACCESO **AND** DESKTOP-09N26UN **AND** KRAKEN01 **AND** MUJER08 **AND** FEBO **AND** JUNO **AND** NEPTUNO **AND group names** agents_group_neq VPN Users SIES-M	Disk Drives - Block CD-ROM Drives - Blo... Floppy Disk Drives - B... Windows Portable De... Custom Device Types ...	1
	Device Configuration	Default	Any	Disk Drives - Allow CD-ROM Drives - All... Floppy Disk Drives - A... Windows Portable De...	1

Extension Profiles Device Configuration Windows.

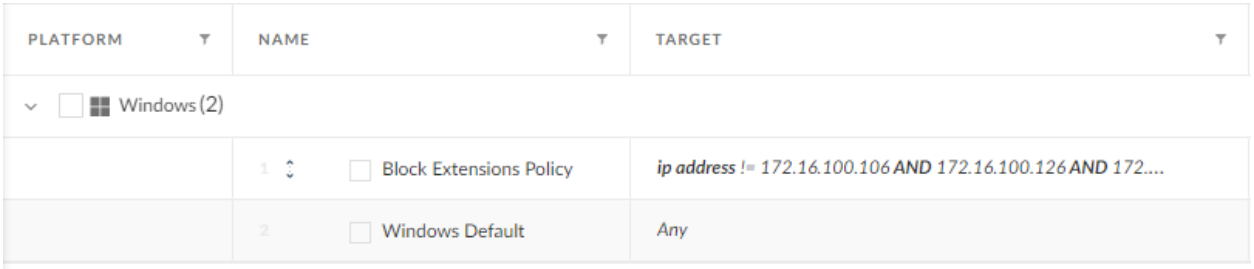
Se muestra a continuación los **Extension Profiles** tipo **Device Configuration** para macOS configurados en la plataforma, incluyendo el perfil Default.



Extension Profiles Device Configuration macOS.

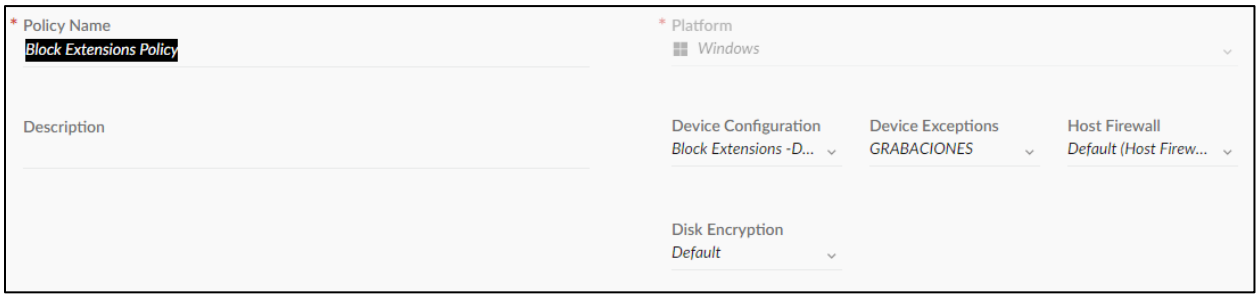
5.4.2. EXTENSION POLICY RULES

Se muestra las **Extension Policy Rules** configuradas para **Windows**, incluyendo la política Windows Default.



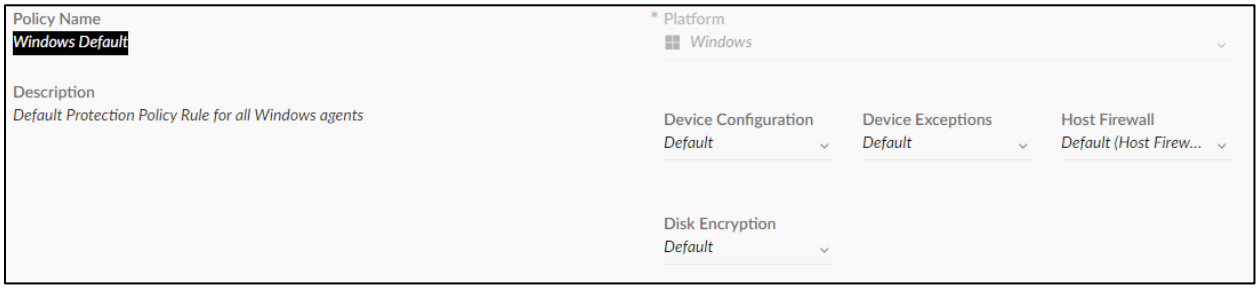
Extension Policy Rules - Windows.

A continuación, se muestra el detalle de la política **Block Extensions Policy.**



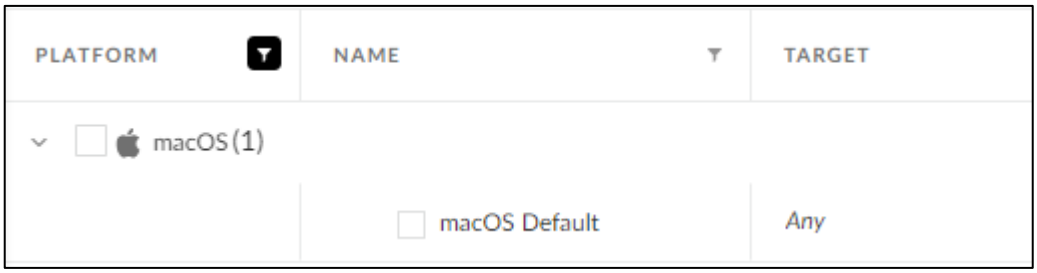
Extension Policy Rules Block Extensions Policy.

A continuación, se muestra el detalle de la política **Windows Default.**



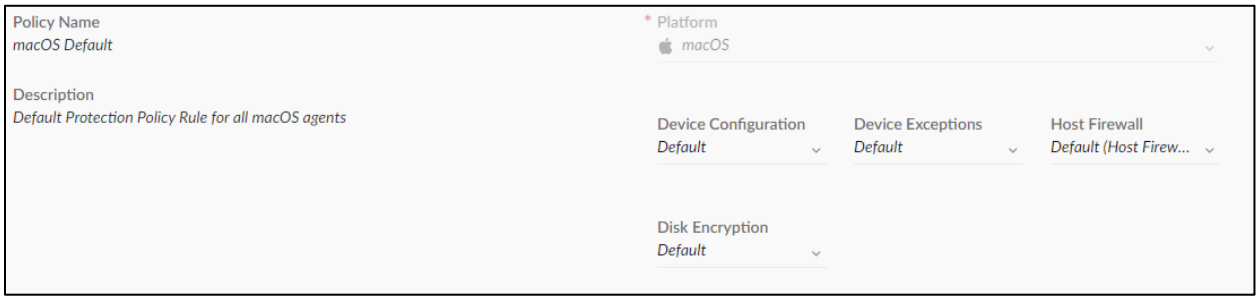
Extension Policy Rules Windows Default.

Se muestra las **Extension Policy Rules** configuradas para **macOS**, incluyendo la política macOS Default.



Extension Policy Rules - macOS.

A continuación, se muestra el detalle de la política **macOS Default.**

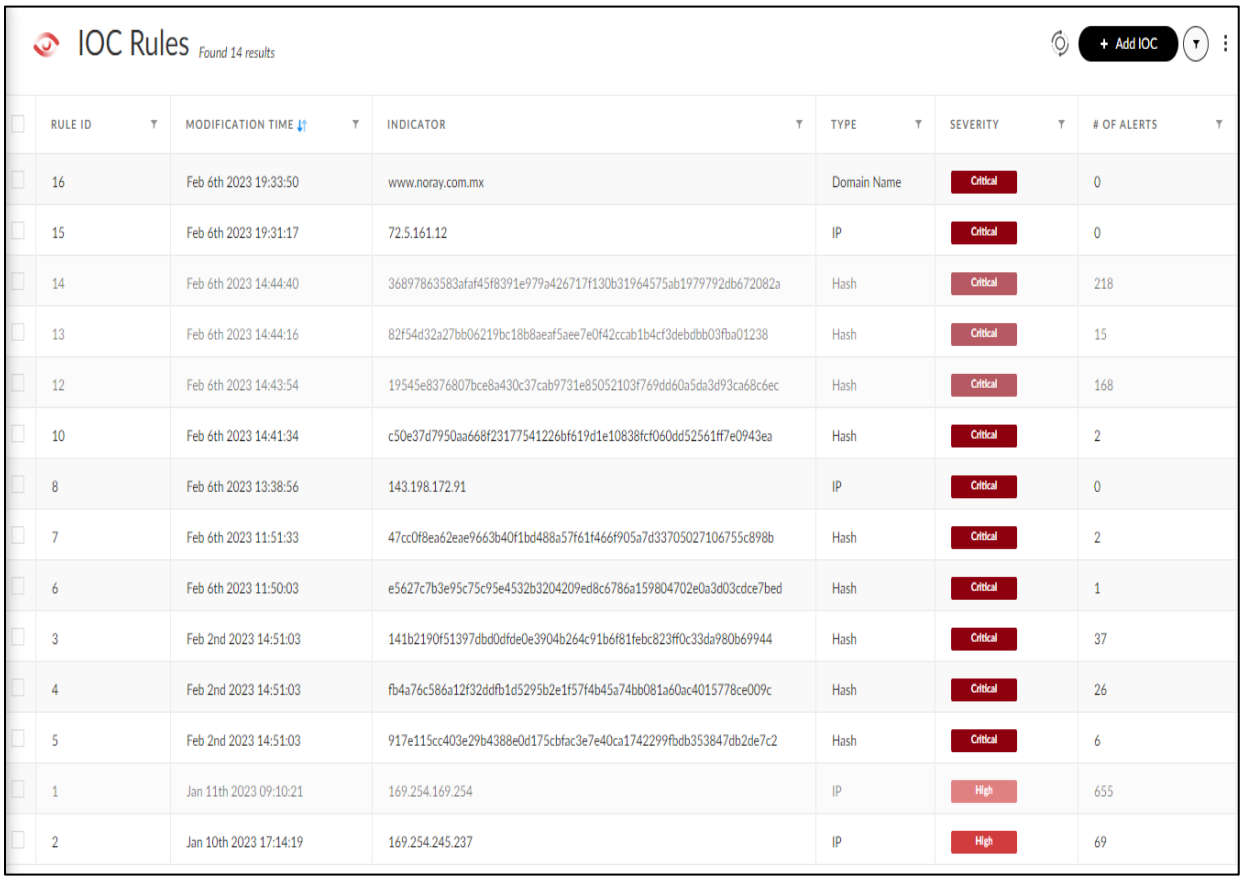


Extension Policy Rules macOS Default.

5.5. DETECTION RULES

5.5.1. IOC Rules

Se muestra a continuación los **14 IOC Rules** configurados en la plataforma.



IOC Rules Found 14 results

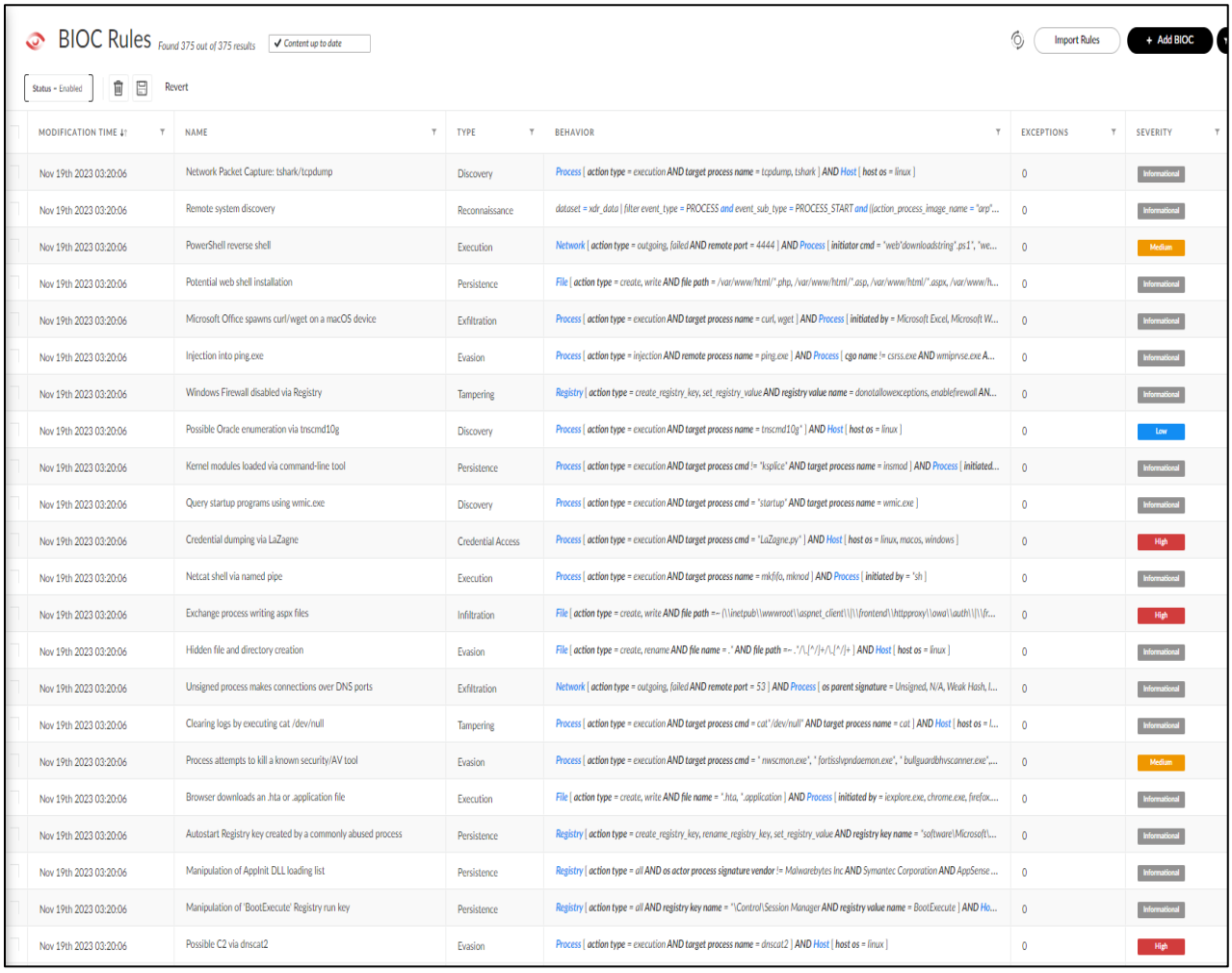
+ Add IOC

RULE ID	MODIFICATION TIME	INDICATOR	TYPE	SEVERITY	# OF ALERTS
16	Feb 6th 2023 19:33:50	www.noray.com.mx	Domain Name	Critical	0
15	Feb 6th 2023 19:31:17	72.5.161.12	IP	Critical	0
14	Feb 6th 2023 14:44:40	36897863583afaf45f8391e979a426717f130b31964575ab1979792db672082a	Hash	Critical	218
13	Feb 6th 2023 14:44:16	82f54d32a27bb06219bc18b8aeaf5aee7e0f42ccab1b4cf3debdbb03fba01238	Hash	Critical	15
12	Feb 6th 2023 14:43:54	19545e8376807bce8a430c37cab9731e85052103f769dd60a5da3d93ca68c6ec	Hash	Critical	168
10	Feb 6th 2023 14:41:34	c50e37d7950aa668f23177541226bf619d1e10838fcf060dd52561ff7e0943ea	Hash	Critical	2
8	Feb 6th 2023 13:38:56	143.198.172.91	IP	Critical	0
7	Feb 6th 2023 11:51:33	47cc0f8ea62eae9663b40f1bd488a57f61f466f905a7d337050271067 55c898b	Hash	Critical	2
6	Feb 6th 2023 11:50:03	e5627c7b3e95c75c95e4532b3204209ed8c6786a159804702e0a3d03cdce7bed	Hash	Critical	1
3	Feb 2nd 2023 14:51:03	141b2190f51397dbd0dfde0e3904b264c91b6f81febc823ff0c33da980b69944	Hash	Critical	37
4	Feb 2nd 2023 14:51:03	fb4a76c586a12f32ddfb1d5295b2e1f57f4b45a74bb081a60ac4015778ce009c	Hash	Critical	26
5	Feb 2nd 2023 14:51:03	917e115cc403e29b4388e0d175cbfac3e7e40ca1742299fbdb353847db2de7c2	Hash	Critical	6
1	Jan 11th 2023 09:10:21	169.254.169.254	IP	High	655
2	Jan 10th 2023 17:14:19	169.254.245.237	IP	High	69

IOC Rules.

5.5.2. BIOC Rules

Se muestra a continuación los **375 BIOC Rules** suministradas directamente por el fabricante.



BIOC Rules Found 375 out of 375 results | Content up to date | Import Rules | + Add BIOC

Status = Enabled | Revert

MODIFICATION TIME	NAME	TYPE	BEHAVIOR	EXCEPTIONS	SEVERITY
Nov 19th 2023 03:20:06	Network Packet Capture: tshark/tcpdump	Discovery	Process [action type = execution AND target process name = tcpdump, tshark] AND Host [host os = linux]	0	Informational
Nov 19th 2023 03:20:06	Remote system discovery	Reconnaissance	dataset = xdr_data | filter event_type = PROCESS and event_sub_type = PROCESS_START and ((action_process_image_name = "arp"...	0	Informational
Nov 19th 2023 03:20:06	PowerShell reverse shell	Execution	Network [action type = outgoing, failed AND remote port = 4444] AND Process [initiator cmd = "web'downloadstring".ps1", "we...	0	Medium
Nov 19th 2023 03:20:06	Potential web shell installation	Persistence	File [action type = create, write AND file path = /var/www/html/".php, /var/www/html/".asp, /var/www/html/".aspx, /var/www/h...	0	Informational
Nov 19th 2023 03:20:06	Microsoft Office spawns curl/wget on a macOS device	Exfiltration	Process [action type = execution AND target process name = curl, wget] AND Process [initiated by = Microsoft Excel, Microsoft W...	0	Informational
Nov 19th 2023 03:20:06	Injection into ping.exe	Evasion	Process [action type = injection AND remote process name = ping.exe] AND Process [cgo name != csrss.exe AND wmiprvse.exe A...	0	Informational
Nov 19th 2023 03:20:06	Windows Firewall disabled via Registry	Tampering	Registry [action type = create_registry_key, set_registry_value AND registry value name = donotallowexceptions, enablefirewall AN...	0	Informational
Nov 19th 2023 03:20:06	Possible Oracle enumeration via tnscmd10g	Discovery	Process [action type = execution AND target process name = tnscmd10g*] AND Host [host os = linux]	0	Low
Nov 19th 2023 03:20:06	Kernel modules loaded via command-line tool	Persistence	Process [action type = execution AND target process cmd != "ksplice" AND target process name = insmod] AND Process [initiated...	0	Informational
Nov 19th 2023 03:20:06	Query startup programs using wmic.exe	Discovery	Process [action type = execution AND target process cmd = "startup" AND target process name = wmic.exe]	0	Informational
Nov 19th 2023 03:20:06	Credential dumping via LaZagne	Credential Access	Process [action type = execution AND target process cmd = "LaZagne.py"] AND Host [host os = linux, macos, windows]	0	High
Nov 19th 2023 03:20:06	Netcat shell via named pipe	Execution	Process [action type = execution AND target process name = mkfifo, mknod] AND Process [initiated by = "sh]	0	Informational
Nov 19th 2023 03:20:06	Exchange process writing aspx files	Infiltration	File [action type = create, write AND file path =~ (\\inetpub\\wwwroot\\aspnet_client\\\|\\frontend\\httpproxy\\owa\\auth\\\|\\fr...	0	High
Nov 19th 2023 03:20:06	Hidden file and directory creation	Evasion	File [action type = create, rename AND file name = "." AND file path =~ "/\.[^/]+\.[^/]+] AND Host [host os = linux]	0	Informational
Nov 19th 2023 03:20:06	Unsigned process makes connections over DNS ports	Exfiltration	Network [action type = outgoing, failed AND remote port = 53] AND Process [os parent signature = Unsigned, N/A, Weak Hash, I...	0	Informational
Nov 19th 2023 03:20:06	Clearing logs by executing cat /dev/null	Tampering	Process [action type = execution AND target process cmd = cat" /dev/null" AND target process name = cat] AND Host [host os = l...	0	Informational
Nov 19th 2023 03:20:06	Process attempts to kill a known security/AV tool	Evasion	Process [action type = execution AND target process cmd = " nwscmon.exe", " fortisslvpndaemon.exe", " bullguardbhvscanner.exe",...	0	Medium
Nov 19th 2023 03:20:06	Browser downloads an .hta or .application file	Execution	File [action type = create, write AND file name = ".hta, ".application] AND Process [initiated by = iexplore.exe, chrome.exe, firefox....	0	Informational
Nov 19th 2023 03:20:06	Autostart Registry key created by a commonly abused process	Persistence	Registry [action type = create_registry_key, rename_registry_key, set_registry_value AND registry key name = "software\Microsoft\...	0	Informational
Nov 19th 2023 03:20:06	Manipulation of AppInit DLL loading list	Persistence	Registry [action type = all AND os actor process signature vendor != Malwarebytes Inc AND Symantec Corporation AND AppSense ...	0	Informational
Nov 19th 2023 03:20:06	Manipulation of 'BootExecute' Registry run key	Persistence	Registry [action type = all AND registry key name = "\Control\Session Manager AND registry value name = BootExecute] AND Ho...	0	Informational
Nov 19th 2023 03:20:06	Possible C2 via dnscat2	Evasion	Process [action type = execution AND target process name = dnscat2] AND Host [host os = linux]	0	High

BIOC Rules.

5.6. INCIDENT RESPONSE

5.6.1. BLOCK LIST

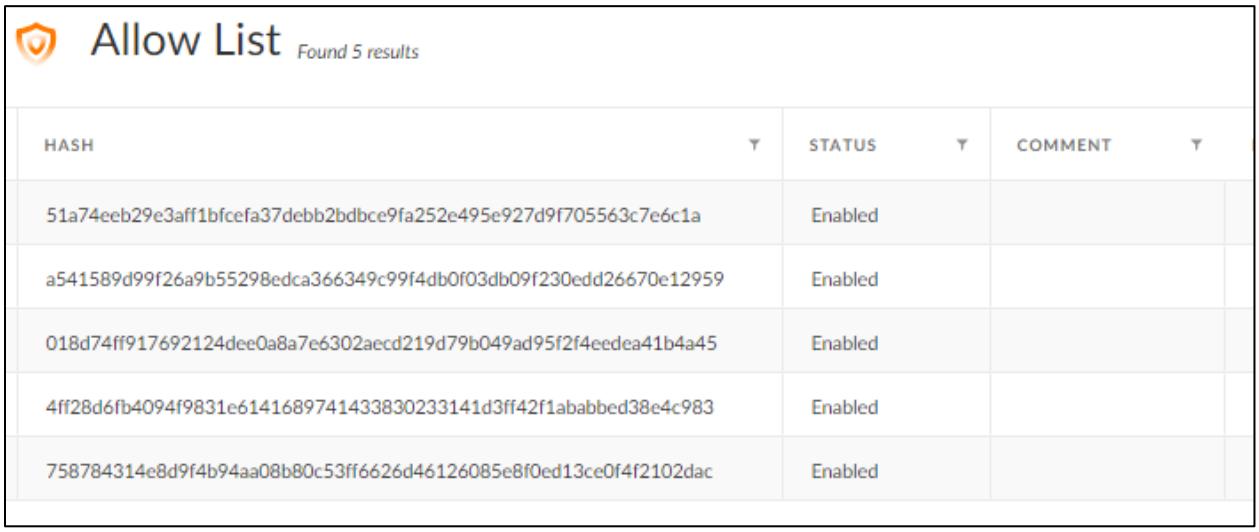
Se muestra a continuación el listado de **6 Hash** pertenecientes al **Block List** configurado en la plataforma.



Block List – Action Center.

5.6.2. ALLOW LIST

Se muestra a continuación el listado de **5 Hash** pertenecientes al **Allow List** configurado en la plataforma.



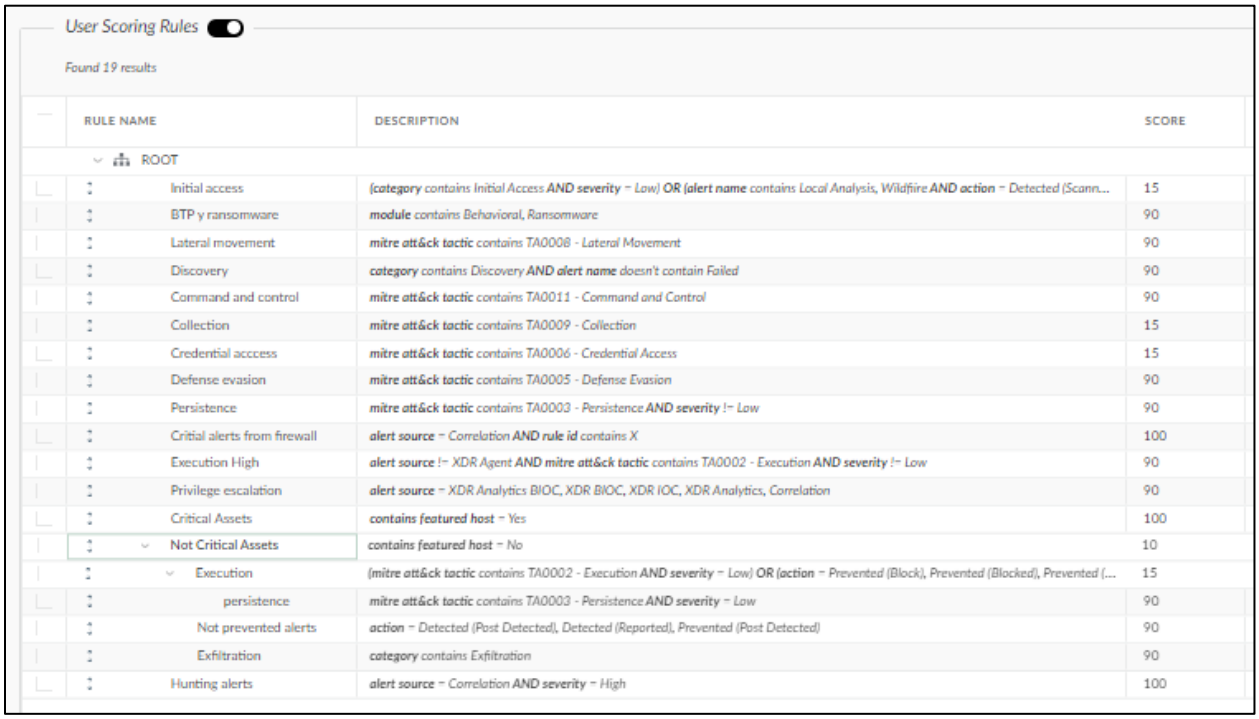
Allow List – Action Center.

5.6.3. SCORING RULES

Cortex XDR utiliza "stitching logic" para recopilar y asignar alertas a incidentes en función de un conjunto de reglas que tienen en cuenta diferentes atributos de alerta, como SHA256 de archivos involucrados y direcciones IP. Los incidentes que se muestran en la Tabla de incidentes se pueden priorizar de acuerdo con estos atributos de alerta.

Cuando se activa una alerta, Cortex XDR hace coincidir la alerta con cada una de las reglas de incidentes personalizadas que creó. Si la alerta coincide con una o más de las reglas, la alerta recibe la puntuación definida por cada regla. Una regla de incidente también puede contener una subregla que le permite crear una jerarquía de reglas. Cuando existe una subregla, si la misma alerta coincide con una o más de las subreglas, la alerta también recibe la puntuación definida por cada subregla. De forma predeterminada, se aplica una puntuación solo a la primera alerta que coincide con la regla y la subregla definidas. Dentro de cada incidente, Cortex XDR agrega los puntajes de alerta y asigna al incidente un puntaje total.

Se realiza una configuración de reglas de scoring, que permite priorizar los incidentes reportados por la consola, de acuerdo con la descripción descrita en la siguiente tabla.



User Scoring Rules

Found 19 results

RULE NAME	DESCRIPTION	SCORE
ROOT		
Initial access	**(category** contains Initial Access **AND severity** = Low) **OR (alert name** contains Local Analysis, Wildfire **AND action** = Detected (Scann...	15
BTP y ransomware	**module** contains Behavioral, Ransomware	90
Lateral movement	**mitre att&ck tactic** contains TA0008 - Lateral Movement	90
Discovery	**category** contains Discovery **AND alert name** doesn't contain Failed	90
Command and control	**mitre att&ck tactic** contains TA0011 - Command and Control	90
Collection	**mitre att&ck tactic** contains TA0009 - Collection	15
Credential acccess	**mitre att&ck tactic** contains TA0006 - Credential Access	15
Defense evasion	**mitre att&ck tactic** contains TA0005 - Defense Evasion	90
Persistence	**mitre att&ck tactic** contains TA0003 - Persistence **AND severity** != Low	90
Critial alerts from firewall	**alert source** = Correlation **AND rule id** contains X	100
Execution High	**alert source** != XDR Agent **AND mitre att&ck tactic** contains TA0002 - Execution **AND severity** != Low	90
Privilege escalation	**alert source** = XDR Analytics BIOC, XDR BIOC, XDR IOC, XDR Analytics, Correlation	90
Critical Assets	**contains featured host** = Yes	100
Not Critical Assets	**contains featured host** = No	10
Execution	**(mitre att&ck tactic** contains TA0002 - Execution **AND severity** = Low) **OR (action** = Prevented (Block), Prevented (Blocked), Prevented (...	15
persistence	**mitre att&ck tactic** contains TA0003 - Persistence **AND severity** = Low	90
Not prevented alerts	**action** = Detected (Post Detected), Detected (Reported), Prevented (Post Detected)	90
Exfiltration	**category** contains Exfiltration	90
Hunting alerts	**alert source** = Correlation **AND severity** = High	100

Reglas de scoring configuradas.

6. PENDIENTES

El cliente completara al 100% el despliegue de los agentes de Cortex XDR en los diferentes endpoints de la compañía. Una vez se confirma el cierre de las actividades, se notifica que los agentes faltantes quedan a cargo del área de TI de la Secretaría. Es importante tener presente que esta implementación es complementaria a la ya ejecutada en el año 2022, por lo tanto, tienen claro el proceso de despliegue. De igual manera Boyra estará atento a cualquier eventualidad.

7. RECOMENDACIONES

- Realizar monitoreo constante de las nuevas versiones de las Broker VM y realizar su respectiva actualización en base al Release Note entregado por el fabricate. https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Release-Notes/Broker-VM

- Continuar con el despliegue de agentes de Cortex XDR en los endpoints de la compañía y de esta manera brindar más información para la **Analytics Engine** y el **Identity Analytics.**

- Activar Sinlge Sign-On para la autenticación.

- Tener presente que Cortex XDR cuenta con control de ancho de banda que por defecto esta configurado en 200 Mbps, este valor se puede ajustar a los recursos que maneja actualmente la red y de este modo evitar saturación y lentitud en las operaciones diarias por causa del agente de Cortex.