Informe de actividades de entrega de activación, instalación, configuración y puesta en funcionamiento del licenciamiento adquirido.

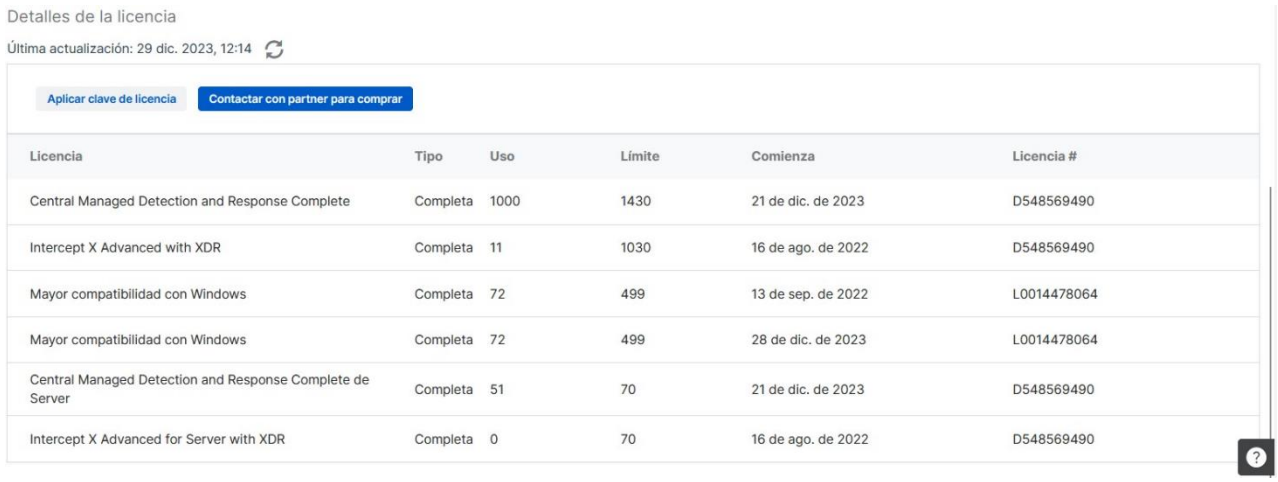
Basados en el contrato ACEPTACIÓN DE OFERTA SASI-UAC-DAAL-073-2023 suscrito entre la ALCALDÍA DE CARTAGENA e ITSEC SAS, en el presente informe se resumen y describen las actividades realizadas en las instalaciones en la Alcaldía de Cartagena por parte de ITSEC SAS el día 28 de diciembre del 2023.

Se conto con el acompañamiento del ing. Carlos Gomez, quien otorgo los permisos correspondientes en las maquinas que se realizó la instalación de Sophos Central Managed Detection and Response Complete.

Contenido

1. Informe de licencias. 2
1.1 Observaciones: 2
2 Informe Malware y PUA bloqueados. 3
2.1 Observaciones: 3
2.2 Recomendaciones: 3
3 Informe estado de los servidores: 4
2.1 Observaciones: 4
2.2 Recomendaciones: 4
3 Informe del estado de dispositivos. 4
3.1 Observaciones: 5
3.2 Recomendaciones: 5
4 Activación de MDR. 5
4.1 Observaciones: 7

1. Informe de licencias.



Detalles de la licencia

Última actualización: 29 dic. 2023, 12:14

Aplicar clave de licencia | Contactar con partner para comprar

Licencia	Tipo	Uso	Límite	Comienza	Licencia #
Central Managed Detection and Response Complete	Completa	1000	1430	21 de dic. de 2023	D548569490
Intercept X Advanced with XDR	Completa	11	1030	16 de ago. de 2022	D548569490
Mayor compatibilidad con Windows	Completa	72	499	13 de sep. de 2022	L0014478064
Mayor compatibilidad con Windows	Completa	72	499	28 de dic. de 2023	L0014478064
Central Managed Detection and Response Complete de Server	Completa	51	70	21 de dic. de 2023	D548569490
Intercept X Advanced for Server with XDR	Completa	0	70	16 de ago. de 2022	D548569490

1.1 Observaciones:

Se evidencia el estado actual de licenciamiento para:

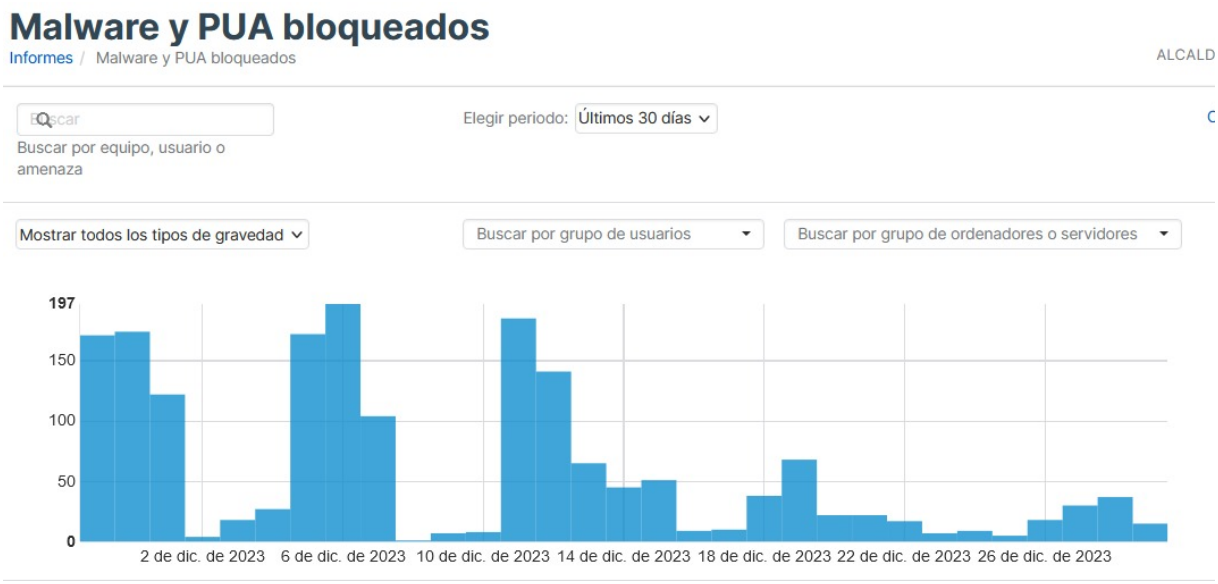
Central Managed Detection and Response Complete Estaciones de trabajo y Servers, adicionalmente con Extenden Support for Windows.

- Se tiene un total de 1430 licencias donde se tienen en uso 1000, las cuales tienen una vigencia hasta el 20/12/2024 correspondiente a EndPoint.

- Se tiene un total de 70 licencias donde se tiene en uso 51 el cual tiene una vigencia hasta el 20/12/2024 correspondiente a Server.

- Se tiene un total de 499 licencias el cual se tiene en unos 72 y tiene una vigencia hasta el 20/12/2024 correspondientes a Extenden Support for Windows.

2 Informe Malware y PUA bloqueados.



2.1 Observaciones:

- Los picos máximos se registraron aproximadamente entre los días 2, 6 y 11 de diciembre, con un total aproximado entre 150 y 197 bloqueos.

- Se identifican que, en el transcurso del mes más o menos hay entre 10 a 20 ataques por día, donde la protección realiza los bloqueos satisfactoriamente y no permite vulnerar los sistemas de información.

2.2 Recomendaciones:

- Instalar los parches de seguridad lanzados por Microsoft -Windows.

- Hacer la instalación de Sophos EndPoint Agent en la totalidad de los equipos de la empresa.

- Capacitar al personal en buenas prácticas del uso de los sistemas de información para que la prevención de vulnerabilidades sea más alta, ya que la mayoría de los ataques exitosos son por ingeniería social.

3 Informe estado de los servidores:



2.1 Observaciones:

- 49 servidores se encuentran activos.
- 2 servidores se encuentran inactivo en más de 2 semanas.
- 21 servidores se encuentran inactivos hace más de 2 meses.
- 40 servidores sin protección.

2.2 Recomendaciones:

- Validar el inventario de los servidores con el fin de asegurar que todos cuenten con la protección instalada.
- Validar que los servidores que no cuentan con la protección se implemente la protección.

3 Informe del estado de dispositivos.



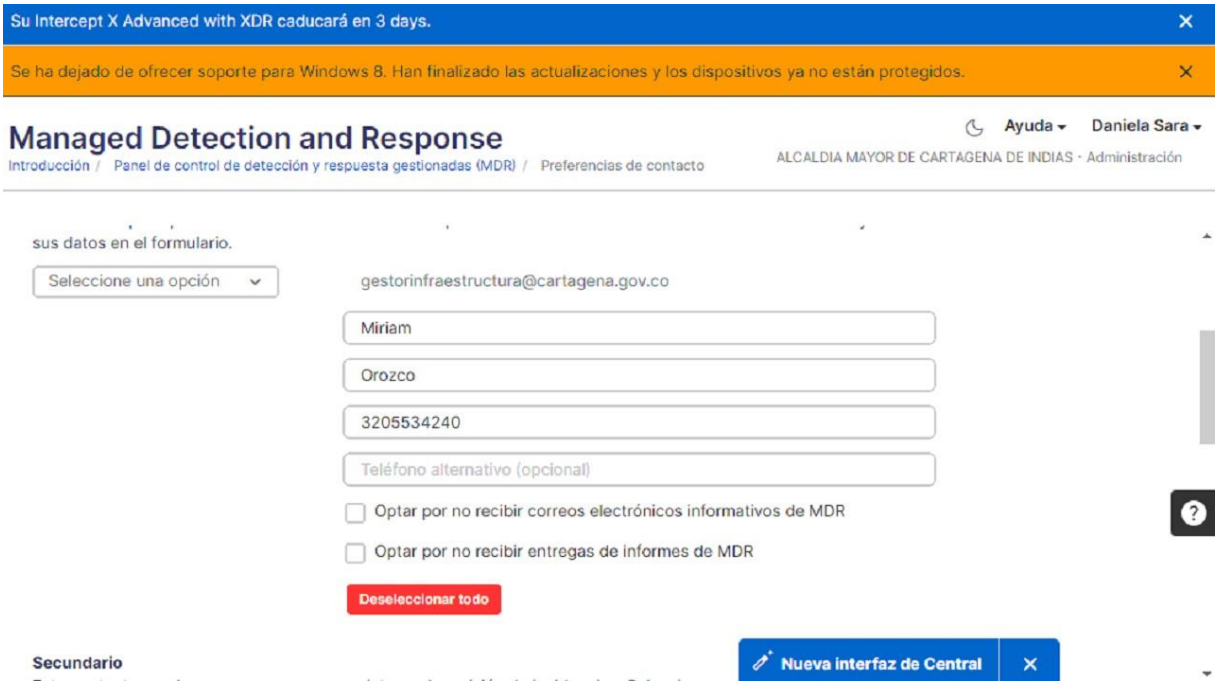
3.1 Observaciones:

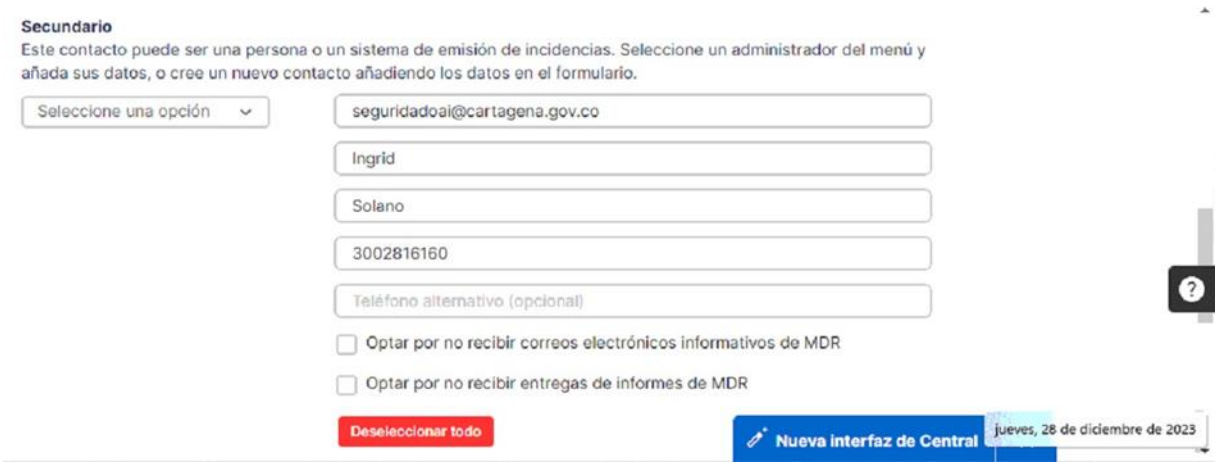
- 1067 dispositivos se encuentran activos.
- 106 dispositivos se encuentran inactivos en más de 2 semanas.
- 539 dispositivos se encuentran inactivos hace más de 2 meses.
- 910 no se encuentran protegidos.

3.2 Recomendaciones:

- Validar el inventario de los dispositivos con el fin de asegurar que todos cuenten con la protección instalada.
- Validar que los dispositivos que no cuentan con la protección en donde se debe implementar la protección.

4 Activación de MDR.




Secundario
Este contacto puede ser una persona o un sistema de emisión de incidencias. Seleccione un administrador del menú y añada sus datos, o cree un nuevo contacto añadiendo los datos en el formulario.
Seleccione una opción
seguridadoai@cartagena.gov.co
Ingrid
Solano
3002816160
Teléfono alternativo (opcional)
Optar por no recibir correos electrónicos informativos de MDR
Optar por no recibir entregas de informes de MDR
Deseleccionar todo
Nueva interfaz de Central
jueves, 28 de diciembre de 2023


Terciario
Este contacto puede ser una persona o un sistema de emisión de incidencias. Seleccione un administrador del menú y añada sus datos, o cree un nuevo contacto añadiendo los datos en el formulario.
Seleccione una opción
soportesigob@cartagena.gov.co
Daniela
Sara
3217821328
Teléfono alternativo (opcional)
Optar por no recibir correos electrónicos informativos de MDR
Optar por no recibir entregas de informes de MDR
Deseleccionar todo
Nueva interfaz de Central

4.1 Observaciones:

Se realiza la respectiva configuración y activación del Central Managed Detection and Response (MDR), a los corres indicados por el área de tecnología

- gestorinfrastructura@cartagena.gov.co. Perteneciente a Miriam Orozco
- seguridadoai@cartagena.gov.co. Perteneciente a Ingrid Solano
- mailto:soportesigob@cartagena.gov.co. Perteneciente a Daniela Sara

En dado caso, si se presentara alguna incidencia o evento que sea critico en base a la seguridad, a estos correos van a llegar mensajes del grupo de Sophos Central Managed Detection and Response (MDR), el cual se debe tener en cuenta que esta información es suministrada y junto con el soporte será en inglés.

Cordialmente,

Juan Carlos Barreto Garcia.
Ingeniero de soporte.
ITSEC SAS.