Implementación de un sistema de ciberseguridad para minimizar ataques y vulnerabilidades del datacenter de FEMSA - Corporación GPF

Hidalgo Olipa, Danny Alejandro

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Ingeniería en Electrónica y Telecomunicaciones

Trabajo de titulación, previo a la obtención del título de Ingeniero en Electrónica y Telecomunicaciones

Ing. Sáenz Enderica, Fabian Gustavo

31 de junio del 2023

Copyleaks

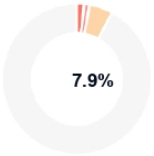
Plagiarism report

TESIS_HIDALGO_V1_ING.pdf

Scan details

Scan time:	Total Pages:	Total Words:
August 2th, 2023 at 15:8 UTC	**61**	**15128**

Plagiarism Detection



Types of plagiarism		Words
Identical	1.6%	248
Minor Changes	1.2%	177
Paraphrased	5%	763
Omitted Words	0%	0

AI Content Detection

Text coverage
- AI text
- Human text

Plagiarism Results: (87)

¿Qué es un sistema de prevención de intrusos (IPS)?... — 1.5%

https://www.checkpoint.com/es/cyber-hub/what-is-ips/

Yael Pan (GEO Cyberhub)

Demostración gratuita Contáctenos Centro de soporte Iniciar sesión Blog ...

¿Qué es la ciberseguridad? | IBM — 0.8%

https://www.ibm.com/es-es/topics/cybersecurity

...

T-ESPEL-MEC-0235.pdf — 0.6%

https://repositorio.espe.edu.ec/bitstream/21000/29351/1/t-e...

Cristina Balseca

1 Carátula Diseño y construcción de un sistema de reacción por pirólisis para la producción de combustible, a partir de polímeros urbano...

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Ingeniería en Electrónica y Telecomunicaciones

Certificación

Certifico que el trabajo de titulación: **Implementación de un sistema de ciberseguridad para minimizar ataques y vulnerabilidades del datacenter de FEMSA - Corporación GPF** fue realizado por el señor **Hidalgo Olipa, Danny Alejandro;** el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizado en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Sangolquí, 02 de agosto del 2023

Firmado electrónicamente por:
FABIAN GUSTAVO
SAENZ ENDERICA

.....

Ing. Sáenz Enderica, Fabian Gustavo

C. C.: 010234398-5

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Ingeniería en Electrónica y Telecomunicaciones

Responsabilidad de Autoría

Yo, **Hidalgo Olipa, Danny Alejandro**, con cédula de ciudadanía 172518725-4, declaro que el contenido, ideas y criterios del trabajo de titulación: **Implementación de un sistema de ciberseguridad para minimizar ataques y vulnerabilidades del datacenter de FEMSA - Corporación GPF** es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 02 de agosto del 2023

.....

Hidalgo Olipa Danny Alejandro

C.C.: 172518725-4

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Ingeniería en Electrónica y Telecomunicaciones

Autorización de Publicación

Yo **Hidalgo Olipa, Danny Alejandro**, con cédula de ciudadanía 172518725-4, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **Implementación de un sistema de ciberseguridad para minimizar ataques y vulnerabilidades del datacenter de FEMSA - Corporación GPF** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 02 de agosto del 2023

.....

Hidalgo Olipa Danny Alejandro

C.C.: 172518725-4

Dedicatoria

En primer lugar, a Dios por permitir que todo esto suceda,

A mi amada mamá, por haberme forjado como la persona que soy en la actualidad todos mis logros son por y para usted, gracias por creer en mí y darme todo el apoyo para que logre culminar mis estudios, es mi mejor ejemplo y mi mayor motivación.

A mis hermanos David y Wendy, por ser enseñarme a ser mejor cada día, brindarme todo su apoyo en todos los momentos y ser mi mayor inspiración, gracias por ser tan unidos y en momentos llegar a convertirnos en una sola persona para alcanzar nuestros objetivos, esto lo hemos hecho juntos.

A mi padre, por enseñarme a ser perseverante en los estudios e impulsarme a convertirme cada día en una mejor persona y profesional, por darme todo su apoyo y motivación para alcanzar grandes metas.

A mi abuelito Humberto por estar siempre presto para cualquier ayuda en todas mis etapas de estudiante y mi vida personal, su apoyo y ejemplo han sido invaluables para lograr culminar este anhelo.

A mis abuelitos y tíos que están en cielo por haberme dejado la enseñanza de siempre estar enfocado en los estudios, no desviarme del buen camino y ser una persona de bien.

A Kathy, por llegar en el momento justo a mi vida, ayudarme a aclarar mis ideas y enfocarme en mis estudios, siempre encontré la solución en ti y contigo, por ser mi mayor apoyo en toda mi etapa estudiantil y en mi vida, gracias por hacerme creer en mí.

Danny Alejandro Hidalgo Olipa

Agradecimiento

Agradezco a Dios, por darme cada día la voluntad, salud y energía para salir adelante y ayudarme a cumplir todas las metas que me he propuesto, por darme a la mejor familia y poner en mi camino a buenas personas.

Agradecer a mi familia quienes han sido el pilar fundamental para cumplir este propósito, este logro es por y para ellos, gracias por estar conmigo en todo momento, bríndame su apoyo incondicional ayudarme a ser cada día mejor persona y ser un ejemplo para mí.

Agradezco a todas las personas que fueron parte de esto y ya no se encuentran aquí, gracias por enseñarme a ser perseverante y dedicado, gracias por darme lo mejor de ustedes y por construir lo que soy ahora.

Mi más sincero agradecimiento a toda área de tecnología de la Corporación GPF por permitirme desarrollar mi trabajo de titulación en sus instalaciones, agradezco todo el apoyo brindado por el equipo de Infraestructura para que el proyecto se pueda consolidar y culminar de la mejor manera.

Agradezco a la universidad por permitirme formarme en tan honorable institución y poner en cada materia a buenos profesores quienes han hecho que todo esto fuese posible.

Finalmente extiendo mi agradecimiento a mis amigos Cristopher y Luis, con quienes logramos muchos objetivos juntos y nos supimos convertir en un gran equipo.

Danny Alejandro Hidalgo Olipa

Índice de Contenidos

Índice de Tablas

Índice de Figuras

Resumen

El presente trabajo de titulación se enfoca en la implementación de un sistema de ciberseguridad destinado a reducir vulnerabilidades y posibles ataques del datacenter de FEMSA - Corporación GPF, que es una empresa consolidada en el Ecuador por más de 90 años enfocada en el retail farmacéutico y productos de conveniencia con más de 700 tiendas a nivel nacional por lo que es esencial salvaguardar la integridad, confidencialidad y disponibilidad de la información para una correcta operación de sus servicios.

El sistema de ciberseguridad está constituido con las consolas SaaS, Cloud One Workload Security y Vision One XDR de Trend Micro porque se someten a auditorías anuales para garantizar el cumplimiento de las mejores prácticas y siguiendo estándares de la industria como certificaciones ISO 27001, ISO 27014, ISO 27017, SOC2 y PCI DSS.

El proceso se divide en dos etapas: la implementación de las consolas y asignación de políticas de seguridad para cada servidor y configuración del sistema en los clientes seleccionados de alrededor de 400 servidores que conforman la infraestructura del data center. Estos clientes serán seleccionados mediante el análisis de su criticidad (alta, media o baja) basada en el sistema operativo, aplicación y ambiente de trabajo en el que se encuentra (Desarrollo, Test o Producción).

La etapa final consiste en la evaluación de la solución implementada que se pudo extraer que el índice de riesgo de los servidores ronda el 65%, que sería un punto de partida para mejorar la seguridad de estos, algunos de los sistemas operativos que están más expuestos son Microsoft Windows Server 2019 y 2016 como la distribución de Linux CentOS 7 los cuales requieren atención por presentar 1148 vulnerabilidades de seguridad conocidas. El retorno de la inversión obtenido en base al último reporte sobre el costo de un informe de violación de datos de IBM es del 3342% .

Palabras clave: Ciberseguridad, Trend Micro, Vulnerabilidades, Parcheo virtual

Abstract

This degree work focuses on the implementation of a cybersecurity system aimed at reducing vulnerabilities and possible attacks of the FEMSA datacenter - Corporation GPF, which is a consolidated company in Ecuador for more than 90 years focused on pharmaceutical retail and convenience products with more than 700 stores nationwide, so it is essential to safeguard integrity, Confidentiality and availability of information for the correct operation of its services.

The cybersecurity system is built on Trend Micro's SaaS, Cloud One Workload Security and Vision One XDR consoles because they undergo annual audits to ensure compliance with best practices and following industry standards such as ISO 27001, ISO 27014, ISO 27017, SOC2 and PCI DSS certifications.

The process is divided into two stages: the implementation of the consoles and assignment of security policies for each server and system configuration in the selected clients of around four hundred servers that make up the data center infrastructure. These clients will be selected by analyzing their criticality (high, medium, or low) based on the operating system, application, and work environment in which it is located (Development, Test or Production).

The final stage consists of the evaluation of the implemented solution that could be extracted that the risk index of the servers is around 65%, which would be a starting point to improve the security of these, some of the operating systems that are most exposed are Microsoft Windows Server 2019 and 2016 as the Linux distribution CentOS 7 which require attention for presenting 1148 known security vulnerabilities. The return on investment obtained based on the latest report on the cost of an IBM data breach report is 3342%.

Keywords: Cybersecurity, Trend Micro, Vulnerabilities, Virtual patching

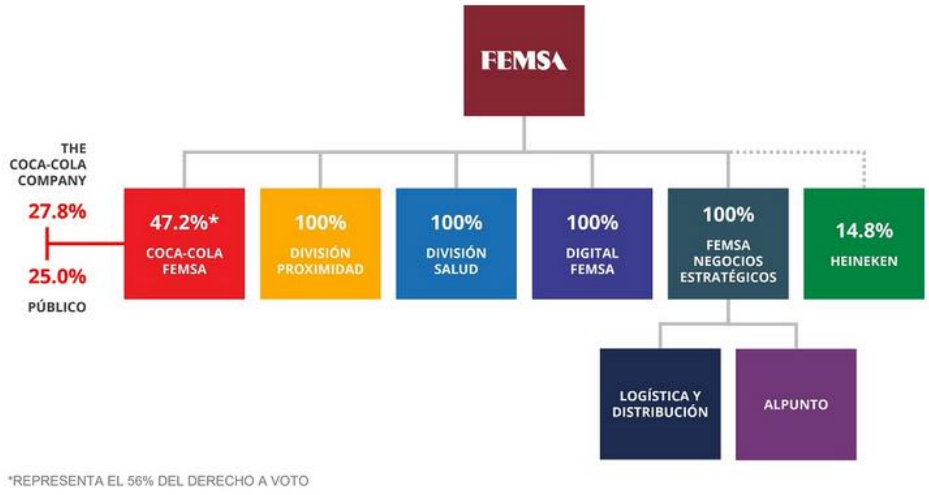
Capítulo I. Introducción

Antecedentes

El Grupo de Fomento Mexicano - FEMSA fue fundado en 1890 y a lo largo de más de 132 años se ha ido diversificando y participando en los mercados mundiales a través de sus diferentes divisiones, tal como la relacionada con tiendas de formato pequeño y servicio, de la que forma parte OXXO, OXXO Gas, y Valora esta última presente en 5 países de Europa. Por otro lado, es el embotellador más grande del mundo de Coca-Cola refiriéndose a volumen de ventas con la participación de Coca-Cola FEMSA, la División Digital maneja temas de servicios financieros; también es el segundo mayor accionista de Heineken, una de las principales empresas cerveceras del mundo. Finalmente se encuentra involucrado en temas de salud que incluyen farmacias y actividades afines con la participación de la División Salud, en la Figura 1 se indica la distribución de los negocios que la conforman y la participación en cada uno de ellos (FEMSA, 2023).

Figura 1

Negocios que conforman al Grupo FEMSA



Nota. Tomado de (CorporacionGPF, 2021)

En 2018 FEMSA con el fin de ampliar su portafolio de negocios ingresa al Ecuador con el área de División Salud adquiriendo el 100% de las acciones del grupo de empresas que conforman a Corporación GPF en Ecuador siendo una de las mayores inversiones en el país de los últimos años.

Corporación GPF es una empresa consolidada en el Ecuador por más de 90 años enfocada en el retail farmacéutico y productos de conveniencia con más de 700 tiendas a nivel nacional con sus marcas de Fybeca, Sana-Sana y Oki Doki, llevando a los hogares ecuatorianos los mejores productos para satisfacer las necesidades de salud, belleza y cuidado personal. (CorporacionGPF, 2021).

Figura 2

Empresas que conforman Corporación GPF

Nota. Tomado de (CorporacionGPF, 2021)

Fybeca.- La principal empresa de farmacias en Ecuador, con una larga historia de 90 años brindando servicios de alta calidad y excelencia, respaldados por nuestra garantía de satisfacción. La propuesta de valor se basa en la proximidad al cliente, adaptándose a las nuevas necesidades mediante servicios de entrega a domicilio y opciones de compra en línea. Cuentan con más de 130 puntos de venta en las principales ciudades del País (CorporacionGPF, 2021).

SanaSana.- Fue fundada en el año 2000 con el objetivo de estar más cerca del cliente mediante sus puntos de venta, cuentan con más de 600 tiendas en las 24 provincias del país con ofertas atractivas para el consumidor y un amplio portafolio de medicinas (CorporacionGPF, 2021).

OkiDoki.- Es la primera franquicia de establecimientos de conveniencia establecida en el año 2010 en el país, que brinda una variedad de servicios como comidas rápidas, bebidas, aperitivos, provisiones para el hogar y productos de cuidado personal, entre otros. (CorporacionGPF, 2021).

Provefarma.- Conformado por el Centro de Abastecimiento de Corporación GPF y el Edificio Corporativo, trabajando con tecnología de punta encargada de distribuir todos los productos que se comercializan en las cadenas Fybeca, SanaSana y OkiDoki en más de 700 puntos de venta a nivel nacional. Es la primera operación logística automatizada en el Ecuador y de las más sofisticadas de la región siendo el 4to de mayor desarrollo tecnológico de Latinoamérica (CorporacionGPF, 2021).

Al pertenecer Corporación GPF al grupo FEMSA, a nivel regional se han venido adoptando diferentes proyectos en las distintas áreas tales como, marketing, finanzas, logística, distribución y tecnología, en esta última se han llevado a cabo distintos cambios tales como la mejora del ERP financiero, actualización de sistemas de almacenamiento (WMS) y el sistema de control de almacenes (WCS) en busca de mejorar la productividad, la experiencia de los empleados y haciendo énfasis a la seguridad de los sistemas (IT ahora - La Revista del Líder de Tecnología , 2022).

El crecimiento continuo del negocio y los cambios suscitados en los últimos años en Corporación GPF ha permitido que el área del sector tecnológico siga creciendo y se ubique a la vanguardia tecnológica, siendo pionero en diferentes hitos a nivel nacional, al momento la infraestructura del datacenter de la Corporación GPF se encuentra en entornos On-Premise y Cloud en donde se tiene más de 400 servidores destinados a ambientes de producción y preproducción, sin contar balanceadores de

carga, switch LAN y SAN, librerías, soluciones de base de datos y respaldos, entre otros. Fuera del datacenter se tiene alrededor de 700 servidores que forman parte de cada punto de venta por lo cual el funcionamiento correcto de área de TI es crítica y vital para la disponibilidad del giro del negocio y a la vez susceptible a diferentes y cada vez más sofisticados ataques cibernéticos.

Justificación e Importancia

El rápido crecimiento de la tecnología y el amplio desarrollo de redes inteligente genera que cada vez el sistema del negocio conlleve más producción para así disfrutar de los beneficios actuales de la tecnología de la información, mientras que cada vez se enfrentan a más diversos riesgos de seguridad. Por lo cual la sociedad ha entrado en la era de la "Gran Seguridad", dicho esto es de suma necesidad complementar el punto ciego de protección y mejorar la capacidad de respuesta frente a vulnerabilidades, amenazas desconocidas, entre otros tipos de malware (Shaji & Subramanian, 2021).

Actualmente el giro del negocio cuenta con los siguientes problemas, el sistema operativo del servidor no se alinea con los requerimientos del sistema empresarial, es decir aplicaciones, base de datos, interacciones entre sistemas de almacenamiento y distribución, entre otros, ya que a menudo hay conflictos o incompatibilidad con la operación de refuerzo de la seguridad del sistema, dando como resultado la falla del aplicativo al instalar y actualizar al último parche de seguridad o si bien la actualización fue exitosa puede conducir a que el sistema no se inicialice, generando grandes pérdidas económicas y mayor esfuerzo humano para generar la reversa de la actualización (Genge et al., 2015).

Por otro lado la implementación del parche de seguridad en el sistema operativo para bloquear vulnerabilidades criticas solicita del reinicio del servidor para que el cambio surja efecto, generando que diferentes áreas a la de tecnología presenten indisponibilidad del sistema para ejecutar sus procesos diarios y por lo general periódicos por lo cual se deben cumplir procesos internos para efectuar la

correcta implementación del parche, causando mayor mano de obra, recursos materiales y costo de tiempo para el reforzamiento de la seguridad. Además, con la finalidad de preservar el funcionamiento actual de los servicios y garantizar el trabajo normal del negocio, se toma como primera premisa de no actualizar al último parche de seguridad temporalmente, dejando en exposición al servidor en cuestión frente a la amenaza de una explotación de vulnerabilidad maliciosa y ataques, generando mayores riesgos de seguridad (Duan et al., 2020).

Con el fin de no afectar al giro del negocio existe una necesidad urgente enfocada en evitar los riesgos de seguridad causadas por vulnerabilidades que podrían generar la indisponibilidad de los servicios, de tal forma que los piratas informáticos no puedan realizar ningún ataque durante la brecha de la instalación del parche de seguridad del servidor y mejorar en gran medida el nivel de seguridad.

El termino de parcheo virtual fue utilizado originalmente por los proveedores de sistemas de prevención de intrusiones (IPS), siendo una tecnología que detecta a nivel de red cualquier tipo de actividad maliciosa que intente aprovechar cualquier vulnerabilidad conocida.

El Web Application Firewall (WAF) es una tecnología que protege a los servidores contra diversos ataques al analizar paquetes de solicitud HTTP/HTTPS y modelos de tráfico. El funcionamiento del WAF se basa en la configuración de una o varias políticas de seguridad en el firewall de aplicaciones web. Esto permite al WAF identificar y bloquear intentos de explotar vulnerabilidades específicas, ya sea a nivel del sistema operativo o de la aplicación. El objetivo es garantizar que el parche virtual funcione adecuadamente. Además, el WAF está alerta ante cualquier actividad maliciosa detectada y puede prevenir, bloquear, redirigir o aislar el tráfico sospechoso, evitando que llegue al servidor (Oracle España, 2020).

En virtud de lo mencionado anteriormente Corporación GPF se ha planteado reforzar su estrategia de múltiples niveles de seguridad incluyendo equipos, protocolos y herramientas que permitan minimizar el impacto de un posible ataque a la organización. En consecuencia, la Corporación GPF ha adquirido 101 licencias para la implementación de un sistema que incluye el servicio de Parcheo Virtual.

El sistema de ciberseguridad permite obtener una seguridad avanzada para servidores físicos, virtuales y en la nube, protegiendo aplicaciones, sistemas operativos y datos de la empresa y de ser necesario ejecuta parches de emergencia contra vulnerabilidades conocidas o desconocidas.

La implementación completa de la solución permitirá a la Corporación GPF minimizar los riesgos frente a vulnerabilidades conocidas y desconocidas, a la vez que permitirá a sistemas operativos descontinuados se encuentren con los últimos parches de seguridad permitiendo que aplicativos que se encuentran en servidores con sistemas operativos legacy, sin soporte de fábrica, continúen en producción.

Esto permitirá el ahorro económico de renovación de equipos como por ejemplo 150 MC utilizados en el centro de distribución para picking, por otro lado, se mejorara la velocidad de detección de amenazas y se acortara el tiempo de respuesta, gracias a los diferentes módulos que posee el sistema de ciberseguridad, que permite la detección y bloqueo de software no autorizado con control de aplicaciones, envía alertas y desencadena prevención proactiva tras detectar actividad sospechosa o malintencionada, rastrea la credibilidad del sitio web y protege a usuarios de sitios no seguros de la web, finalmente el parcheo virtual de servidores permite que el giro de negocio no se detenga y no se generen pérdidas económicas ni indisponibilidad de los sistemas.

Alcance del Proyecto

El alcance del proyecto de titulación consiste en la implementación de un sistema de ciberseguridad en el datacenter de Corporación GPF como solución frente a vulnerabilidades informáticas, dividiéndose en dos etapas: la implementación de las consolas y asignación de políticas de seguridad para cada servidor (cliente) y configuración del sistema en los clientes seleccionados de alrededor de 400 servidores que conforman la infraestructura del data center. Estos clientes serán seleccionados mediante el análisis de su criticidad (alta, media o baja) basada en el sistema operativo, aplicación y ambiente en el que se encuentre (Desarrollo, Test o Producción).

La etapa final consiste en la evaluación de la solución mediante el análisis cuantitativo de las alertas que se reportan en el sistema de ciberseguridad y de cómo son solventadas mediante la correcta configuración de los módulos del sistema. En consecuencia, se logrará que Corporación GPF no presente indisponibilidad en sus sistemas y aplicativos, logrando que no se generen pérdidas económicas y esfuerzo de personal humano para solventar inconvenientes que la no implementación de la herramienta pueda causar.

Finalmente se obtendrá un manual de usuario para que cualquier personal autorizado pueda hacer uso del sistema de ciberseguridad y administrar las mismas.

Objetivos

Objetivo General

Implementar un sistema de ciberseguridad en los servidores del Data Center de la Corporación GPF definidos en entornos on premise y cloud para la protección frente a amenazas y vulnerabilidades conocidas y desconocidas.

Objetivos Específicos

- Analizar los parámetros de criticidad de los servidores para la efectiva usabilidad de las 101 licencias del agente del sistema de ciberseguridad acorde a la información proporcionada por FEMSA - Corporación GPF.
- Analizar e identificar las funcionalidades de los módulos del sistema de ciberseguridad y realizar los ajustes necesarios para permitir el correcto funcionamiento de detección y respuesta extendidas (XDR).
- Definir y asignar políticas de seguridad especializadas, generando un conjunto de reglas y ajustes de acuerdo con el sistema operativo y la aplicación del servidor.
- Automatizar el sistema de reportes para que envíe la información precisa de los eventos que han ocurrido en cada servidor con frecuencia de 7 días.
- Implementar el Service Gateway mediante un paquete Open Virtualization Format (OVF) sobre VMware e integración con la consola del sistema de ciberseguridad.
- Evaluar la efectividad de la solución frente a vulnerabilidades y el beneficio de la implementación de la herramienta para el negocio.
- Realizar un manual de usuario para el área de infraestructura sobre el correcto uso y configuración del sistema de ciberseguridad

Metodología

La metodología cualitativa permitirá determinar a través de la investigación las buenas prácticas de seguridad informática, estableciendo un proceso bien definido de implementación y configuración de la solución, al establecer un conjunto de directivas o políticas de seguridad adecuadas acorde a los tipos de sistemas operativos de los servidores, su aplicación y/o su criticidad, dependiendo del fin de cada uno de ellos. Por otro, lado la investigación acerca de la solución completa permitirá caracterizar todos

los componentes que dispone la herramienta y como configurarlos en beneficio de la Corporación GPF, permitiendo contrastar la inversión en la solución y permitiendo adquirir los conocimientos necesarios para el levantamiento del manual de usuario.

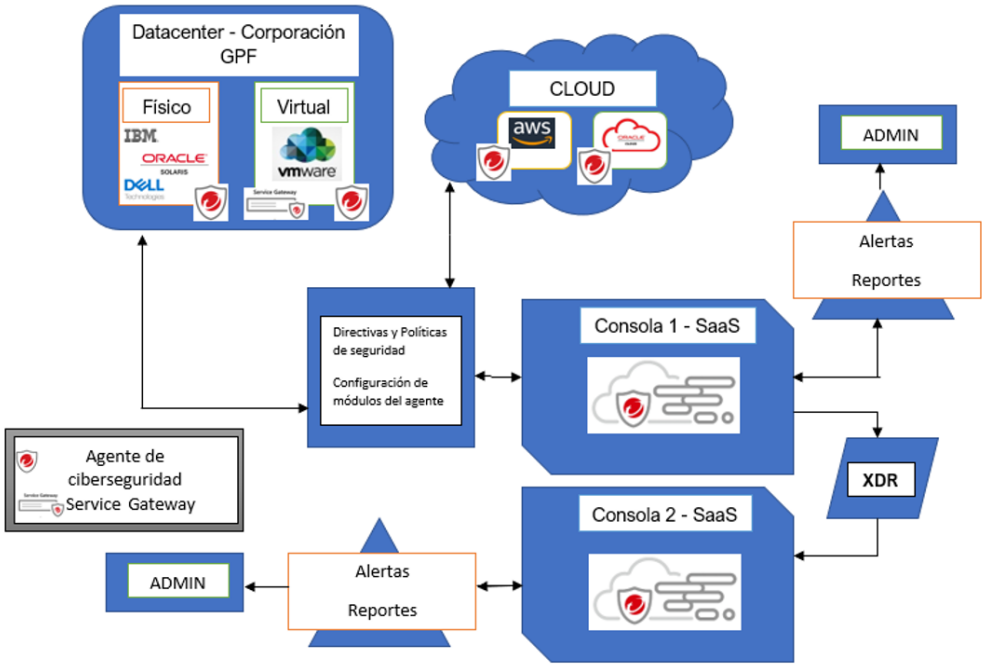
La configuración de los módulos que posee el sistema de ciberseguridad es de suma importancia ya que este permitirá la interrelación con las consolas que este posee, permitiendo que funcione como un sensor recopilando información del equipo y analizado la misma la cual será tratada con XDR, a la vez mediante la integración del Service Gateway se tendrá mejor control sobre el tráfico de la red y las amenazas de seguridad a nivel de servidores virtualizados.

Una vez implementada y configurada la solución y con el fin de determinar el beneficio que esta genera a la empresa, mediante el análisis de riesgos cuantitativo el cual se basa en datos verificados y específicos del número de alertas clasificadas en crítico, advertencia y administrado, los mismos que se muestran en la consola del sistema de ciberseguridad, para posteriormente demostrar la variación de alertas antes y después de implementar la solución.

Finalmente, en la Figura 3 se indica el diagrama de bloques de la implementación de la solución en la infraestructura del datacenter de la Corporación GPF. Donde se utilizarán las consolas Cloud One Workload Security y Vision One XDR de Trend Micro porque se someten a auditorías anuales con personal de confianza para garantizar el cumplimiento de las mejores prácticas y siguiendo estándares de la industria como certificaciones ISO 27001, ISO 27014, ISO 27017, SOC2 y PCI DSS.

Figura 3

Diagrama de bloques a implementar en el datacenter de la Corporación GPF



Capítulo II. Marco conceptual

Infraestructura de TI

La infraestructura de Tecnología de la Información, TI, se refiere a los componentes necesarios para la operación y gestión de los servicios y entornos de tecnología empresariales (IBM, 2023). Estos elementos consisten en hardware, software, componentes de red, un sistema operativo y almacenamiento de datos, que en conjunto se emplean para proporcionar servicios y soluciones de Tecnología de la Información (TI).

La infraestructura de TI puede ser implementada dentro de un sistema de computación en la nube o dentro de las propias instalaciones de la organización. El hardware puede incluir computadoras de escritorio, servidores físicos o virtuales, centros de datos, hubs, routers y switches. El software abarca una variedad de sistemas, como los sistemas de gestión de contenido (CMS), las soluciones de gestión de relaciones con clientes (CRM), los sistemas de planificación de recursos empresariales (ERP), los sistemas operativos y los servidores web (IBM, 2023).

La infraestructura de TI es importante porque la tecnología impulsa casi todos los aspectos del negocio actual, desde el trabajo individual del empleado hasta las operaciones y los bienes y servicios. Cuando está correctamente conectada en red, la tecnología puede optimizarse para mejorar la comunicación, crear eficiencias y aumentar la productividad (IBM, 2023).

Sistemas de computación On-Premise

El concepto on-premise o local hace referencia a la modalidad de instalación de software que se lleva a cabo directamente en los servidores y la infraestructura interna de la empresa. Es el modelo tradicional utilizado en aplicaciones empresariales.

Con el modelo on-premise, la empresa asume la responsabilidad de la seguridad, disponibilidad y gestión del software. Esto implica que la empresa debe contar con un departamento de sistemas dedicado a la administración de la infraestructura en el lugar físico. Sin embargo, el proveedor del software generalmente también ofrece servicios de integración y soporte postventa para asistir a la empresa en estos aspectos (ABRIE, 2020).

Por otro lado, VMware on-premise se refiere a la implementación de soluciones de virtualización de VMware en la infraestructura local de una organización. Esto implica utilizar la tecnología de virtualización de VMware para ejecutar varios sistemas operativos y aplicaciones en un solo servidor, lo que resulta en una mayor eficiencia y una reducción de costos. La virtualización ofrece diversas ventajas, como la capacidad de mover cargas de trabajo fácilmente, mejorar el rendimiento y la disponibilidad de los recursos, y automatizar las operaciones, lo que simplifica la gestión de la infraestructura de TI y disminuye los costos de propiedad y operativos (VMware, 2021).

En base a (Equipo Ekon, 2021) las siguientes son características de sistemas virtualizados:

- Acceso a los recursos por parte de todos los miembros de la organización.
- Altos niveles de seguridad en todos los sistemas informáticos.
- Escalabilidad y flexibilidad de los recursos.
- Implementación e integración rápidas.
- Control total sobre los datos y su acceso.
- Protección de datos, ya que el titular de la licencia mantiene todos sus datos en su propio centro de datos sin acceso de terceros.
- Actualizaciones continuas para ampliar las funciones del programa, mejorar su estabilidad y cerrar posibles brechas de seguridad.

- Confiabilidad, seguridad y control directo sobre los datos.

Sistemas de computación en la nube

La computación en la nube se refiere a la tecnología que permite almacenar y acceder a archivos e información a través de Internet, eliminando la preocupación de contar con suficiente capacidad en el dispositivo propio para alojar dicha información (Atlassian, 2023).

Algunas de las características de la computación en la nube según (NextU , 2022) incluyen:

- Autoservicio bajo demanda: Los usuarios pueden satisfacer sus necesidades de cómputo, como tiempo de servidor y almacenamiento, según sea necesario, sin tener que interactuar directamente con el proveedor de servicios.
- Amplio acceso de red: La información almacenada en la nube puede ser accesible a través de una variedad de dispositivos y ubicaciones a través de Internet.
- Agrupación de recursos: Los recursos de cómputo se comparten y se asignan dinámicamente según la demanda, lo que permite una utilización eficiente de los recursos disponibles.
- Elasticidad rápida: La capacidad de la nube puede expandirse o contraerse de manera ágil y rápida para adaptarse a las necesidades cambiantes de los usuarios.
- Medición de servicios: Los servicios en la nube pueden ser medidos y monitoreados para proporcionar información precisa sobre el uso y los costos asociados.

Servidor

Un servidor, ya sea un dispositivo de hardware o software, es responsable de recibir y responder a solicitudes realizadas a través de una red. El cliente, que es el dispositivo que realiza la solicitud, recibe una respuesta del servidor. En el contexto de Internet, el término servidor se utiliza comúnmente para referirse al sistema informático que recibe solicitudes de archivos web y los envía al cliente (TIC Portal, 2022).

Los servidores desempeñan un papel fundamental en la gestión de operaciones críticas de una organización, como bases de datos, correos electrónicos, aplicaciones y archivos compartidos. Son máquinas de alta potencia que ofrecen un rendimiento superior, redundancia y características de seguridad avanzadas en comparación con una computadora de escritorio estándar. Esto los convierte en elementos clave en el desarrollo de infraestructuras de TI.

Sistema operativo

Un sistema operativo, SO, es un programa informático que administra los recursos de hardware y software de una computadora y brinda servicios comunes a los programas. Funciona como una interfaz entre el usuario y el hardware.

Los sistemas operativos son de gran importancia en las empresas, ya que permiten mejorar la agilidad, flexibilidad y escalabilidad de la infraestructura de TI, al mismo tiempo que generan ahorro de costos significativo. Algunas de las funciones principales de un sistema operativo incluyen

Gestión de recursos: El SO se encarga de asignar y gestionar los recursos del sistema, como la CPU, la memoria y el almacenamiento.

Gestión de archivos: Proporciona un sistema de archivos para organizar, almacenar y recuperar archivos.

Gestión de procesos: Crea, programa y finaliza los procesos que se ejecutan en la computadora.

Interfaz de usuario: Ofrece una interfaz para que el usuario interactúe con la computadora, ya sea mediante una interfaz gráfica o una línea de comandos.

Seguridad: Es responsable de la seguridad del sistema, controlando el acceso a los recursos y protegiendo contra software malicioso.

SaaS

Software as a Service o Software como Servicio, es un modelo de distribución aplicaciones y servicios a través de internet. En lugar de descargar, instalar y mantener el software localmente los usuarios pueden acceder a él a través de un navegador web desde cualquier lugar con conexión a internet. Por lo tanto, SaaS es una solución basada en la nube, donde el proveedor de servicios aloja y mantiene toda la infraestructura necesaria para que el software funcione sin problemas (Amazon Web Services, Inc., 2023).

El funcionamiento de SaaS se basa en un modelo de suscripción, donde los clientes pagan una tarifa periódica (mensual o anual) para acceder al software y utilizar sus funcionalidades. Los proveedores de SaaS se encargan de tareas críticas como el almacenamiento de datos, la seguridad, las actualizaciones y el soporte técnico, liberando a los usuarios de la responsabilidad de mantener y administrar la infraestructura.

Ciberseguridad

La ciberseguridad conocida como seguridad informática, se enfoca en proteger la infraestructura computacional y la información contenida en los sistemas y redes de computadoras. Para reducir al mínimo los riesgos para la infraestructura y la información se emplean protocolos, herramientas, normas, métodos, reglas, y legislaciones creados. (Cisco Systems, 2023).

Según la información de a (IBM, 2020) en 2020 el costo promedio de una violación de datos fue de 3.86 millones de dólares a nivel mundial y de 8.64 millones de dólares en Estados Unidos. Estos costos incluyen los gastos de detección y respuesta a la violación, el tiempo de inactividad y la pérdida de ingresos, así como los daños a largo plazo en la reputación del negocio y la marca. En el 2023 el costo de un informe de violación de datos (IBM, 2023) ha aumentado a 4.43 millones de dólares y el ahorro promedio para organizaciones que utilizan herramientas de seguridad informática de forma exhaustiva es de 1,76 millones de dólares en contraste con otras que no las utilizan.

Las organizaciones que cuentan con una estrategia integral de ciberseguridad pueden enfrentar de manera más efectiva las amenazas cibernéticas para reducir la duración y las consecuencias de las violaciones de seguridad. Una estrategia sólida implica capas de protección para defenderse contra la delincuencia cibernética, las cuales deben abordar aspectos como la seguridad de la infraestructura y de la red.

ROI

Retorno de la inversión traducido es una métrica que permite evaluar la rentabilidad de una inversión. Representa la relación entre los beneficios obtenidos y los costos incurridos,

expresada como un porcentaje. Calcularlo permite determinar si una inversión ha sido exitosa o no, y proporciona información valiosa para la toma de decisiones financieras.

Para calcular el ROI, se deben considerar dos elementos principales: los beneficios obtenidos y los costos asociados a la inversión. Los beneficios pueden incluir ingresos generados, ahorros en costos o cualquier otro valor obtenido como resultado de la inversión. Los costos abarcan todos los gastos directos e indirectos relacionados con ella, como la adquisición de activos, los gastos de mantenimiento y los costos operativos. La fórmula para calcular el ROI:

$$ROI = \frac{Beneficios - Costos}{Costos}$$

El resultado se expresa como un porcentaje. Si el ROI es positivo, indica que la inversión ha generado ganancias, mientras que un ROI negativo significa que se ha producido una pérdida.

Virtual patching

El virtual patching o parcheado virtual, es una técnica empleada en seguridad informática para proteger sistemas y aplicaciones vulnerables sin necesidad de aplicar un parche tradicional refiriéndose a la instalación de parches de seguridad. Consiste en implementar medidas de protección temporales y virtuales con el objetivo de mitigar los riesgos asociados a vulnerabilidades conocidas, sin realizar modificaciones en el código fuente o en el sistema en sí.

Cuando se descubre una vulnerabilidad en un software o sistema operativo, puede llevar tiempo desarrollar y distribuir un parche oficial. Durante ese período, los sistemas pueden quedar expuestos a posibles ataques. El virtual patching proporciona una solución rápida al aplicar reglas o filtros en tiempo real en la capa de red o en el sistema de seguridad, bloqueando de manera proactiva los intentos de explotar la vulnerabilidad conocida (Trend Micro ES, 2021).

Esta técnica utiliza firewalls, sistemas de detección de intrusos (IDS) o sistemas de prevención de intrusiones (IPS) para analizar y filtrar el tráfico en busca de patrones y comportamientos sospechosos que coincidan con ataques conocidos. Cuando se detecta una actividad maliciosa que intenta aprovechar una vulnerabilidad conocida, el virtual patching aplica automáticamente las reglas predefinidas para bloquear o mitigar el ataque.

Sistema de prevención de intrusiones (IPS)

Un sistema de prevención de intrusiones, también conocido como Intrusion Prevention System, es una tecnología que monitorea de manera constante una red con el fin de identificar cualquier actividad dañina que busque aprovechar una vulnerabilidad conocida. Ayuda a las organizaciones a identificar el tráfico malicioso y bloquear de manera proactiva el ingreso de dicho tráfico a su red. Es un software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

La función principal de un sistema de prevención de intrusos consiste en reconocer cualquier actividad que genere sospechas y detectar y, en caso necesario, permitir (IDS) o prevenir (IPS) la amenaza. Los intentos son registrados y se informa a los administradores de red o al personal del Centro de operaciones de seguridad (SOC) (Check Point Software ES, 2021).

Las tecnologías de prevención de intrusiones (IPS) tienen la capacidad de identificar y bloquear ataques de seguridad en redes, como ataques de fuerza bruta, ataques de denegación de servicio (DoS) y explotación de vulnerabilidades. Una vulnerabilidad se refiere a una debilidad presente en un software, y una vulnerabilidad de seguridad es un tipo de ataque que aprovecha esa debilidad con el objetivo de tomar el control de un sistema (Check Point Software ES, 2021).

El método de detección utilizado puede ser basado en firmas o anomalías conocidas. Las firmas predefinidas son patrones específicos de ataques de red que se conocen. El dispositivo IPS compara los flujos de paquetes con estas firmas para determinar si hay una coincidencia de patrones. Algunas compañías que ofrecen servicios de IPS incluyen Fortinet, Trend Micro y Splunk.

XDR

Según la fuente (Trend Micro, 2023) establece que XDR (Extended Detection and Response) es un enfoque de seguridad avanzado que busca mejorar la detección, respuesta y visibilidad de amenazas en los entornos de TI, se basa en la integración y correlación de datos de múltiples fuentes de seguridad, como endpoints, redes, servidores, nubes y registros de actividad.

La idea principal detrás de XDR es proporcionar una visión holística de las amenazas y facilitar la detección temprana de ataques avanzados y persistentes. Al recopilar y analizar datos de múltiples fuentes, XDR permite identificar patrones de comportamiento sospechosos, correlacionar eventos y alertas, y proporcionar una respuesta coordinada a los incidentes de seguridad.

XDR utiliza tecnologías como la analítica de comportamiento, el machine learning y la automatización para mejorar la eficacia y la eficiencia de las operaciones de seguridad. Al agregar contexto y correlación a los datos de seguridad, XDR ayuda a los equipos de respuesta a tomar decisiones informadas y a responder de manera más rápida y efectiva a las amenazas.

Trend Micro

De su página oficial (TrendMicro, 2023) se puede abstraer que Trend Micro es una empresa líder en seguridad cibernética fundada en 1988. Su enfoque principal es proporcionar soluciones de seguridad avanzadas para proteger a los individuos, las empresas y las organizaciones contra las amenazas cibernéticas en constante evolución. Trend Micro ofrece una

amplia gama de productos y servicios diseñados para proteger los sistemas y datos de sus clientes, tanto en entornos físicos como en la nube.

Se dedica a la investigación y desarrollo de tecnologías de seguridad innovadoras para abordar los desafíos actuales y emergentes en el panorama de la seguridad cibernética. Sus soluciones cubren áreas clave como la protección contra malware, la detección y prevención de intrusiones, la gestión de vulnerabilidades, el cifrado de datos, la seguridad en la nube y la protección de aplicaciones y redes.

Entre los productos que ofrece se encuentran soluciones de seguridad basadas en la nube, servicios de detección y respuesta extendida (XDR), así como plataformas de ciberseguridad diseñadas para proteger datos, centros de datos, entornos en la nube, redes y puntos finales.

Deep security

Deep Security es una solución de seguridad de Trend Micro que proporciona una plataforma integral para proteger los entornos de infraestructura y aplicaciones en la nube, virtualizados y físicos. Está diseñada para proteger contra amenazas de seguridad, como malware, intrusiones, vulnerabilidades y ataques cibernéticos.

Deep Security ofrece una amplia gama de funciones de seguridad, que incluyen detección y prevención de intrusiones (IPS), protección contra malware y ransomware, control de aplicaciones, protección de vulnerabilidades, firewall de host, seguridad de contenedores y protección de servidores virtuales. La solución se basa en un agente ligero que se instala en los sistemas a proteger y se administra de forma centralizada a través de una consola de administración.

Utiliza técnicas como el machine learning y el análisis de comportamiento para detectar y prevenir amenazas de forma proactiva. Además, proporciona informes detallados y registros de auditoría para facilitar la supervisión y el cumplimiento normativo.

Cloud One Workload Security

Trend Micro Cloud One Workload Security es una solución de seguridad diseñada específicamente para proteger las cargas de trabajo en entornos de nube pública, privada e híbrida. Esta solución aborda los desafíos de seguridad únicos que surgen al migrar aplicaciones y datos a entornos de nube.

Cloud One Workload Security ofrece una amplia gama de funciones de seguridad, como detección y prevención de intrusiones, protección contra malware, firewall de host, control de aplicaciones y seguridad de contenedores. Estas características ayudan a garantizar que las cargas de trabajo en la nube estén protegidas contra amenazas y ataques cibernéticos. Esta solución protege endpoints, servidores y workloads en la nube a través de una visibilidad unificada, gestión y control de acceso basado en roles.

Además, Cloud One Workload Security proporciona una administración centralizada y un monitoreo continuo de las cargas de trabajo en la nube, lo que permite una visibilidad completa y un control de seguridad efectivo. Esto incluye la capacidad de aplicar políticas de seguridad, detectar comportamientos sospechosos y responder a incidentes de seguridad de manera rápida y eficiente.

Trend Vision One

Es una plataforma de ciberseguridad unificada y completa de Trend Micro que ofrece capacidades de prevención, detección y respuesta impulsadas por inteligencia artificial, investigación e inteligencia de amenazas líderes en el mercado. Esta plataforma permite a las

empresas gestionar su seguridad de manera holística y controlar sus riesgos cibernéticos a través de una única plataforma.

La solución XDR líder en la industria se integra con la protección, detección y respuesta de endpoints para ofrecer una cobertura nativa del sensor para endpoints, identidad, correo electrónico, red y carga de trabajo en la nube con un amplio soporte para integraciones de terceros.

Capitulo III. Implementación del sistema de ciberseguridad

La implementación del sistema de ciberseguridad se lo realiza con los servicios Cloud One Workload Security y Vision One XDR de Trend Micro con la adquisición de 101 licencias para instalar en diferentes servidores del data center de la Corporación GPF que serán elegidos posterior al análisis de criticidad y el ambiente de trabajo de estos.

En la Figura 3 se muestra un diagrama de bloques sobre la incorporación del sistema de ciberseguridad en el datacenter de la corporación GPF donde se incorporan dos consolas SaaS con los servicios de Cloud One Workload Security en la primera para la utilización del sistema de prevención de intrusiones (IPS) y Deep Security y Trend Vision One en la segunda que permite la detección y respuesta ampliadas (XDR) y la visualización de la información obtenida con el módulo de Activity Monitoring que resume los riegos presentes en los agentes configurados.

Los agentes que serán utilizados son servidores físicos, virtualizados o en la nube administrados en el data center de la Corporación GPF.

Criticidad de los servidores

El data center de la Corporación GPF administra alrededor de 400 servidores que permite el correcto funcionamiento de sus operaciones, los varían entre físicos, virtualizados y en la nube con diferentes sistemas operativos que van de Linux a Windows Server en sus diferentes versiones.

El personal ha definido una criticidad de los servidores que varían entre alta, media y baja los cuales se establecieron con un análisis basado en el sistema operativo que trabaja y su versión, el ambiente en el que se encuentra, desarrollo, test o producción y finalmente la aplicación final dentro de las operaciones.

Los servidores con sistemas operativos legacy que ya no tienen soporte son una prioridad por la falta de actualizaciones de seguridad por lo que serán seleccionados sin importar su criticidad y ambiente de trabajo.

En la Tabla 1 se muestra los servidores elegidos para la instalación de los agentes de deep security, que se encuentran ordenados por su sistema operativo.

Tabla 1

Servidores para la instalación de agentes de deep security

Hostname	Sistema Operativo	Ambiente de trabajo	Criticidad
UIOWS***	Microsoft Windows Server 2003 (32 bit)	Producción	Media
UIOVI***	Microsoft Windows Server 2003 (32 bit)	Test	Baja
UIOVI***	Microsoft Windows Server 2003 (32 bit)	Test	Baja
UIOVI***	Microsoft Windows Server 2003 (32 bit)	Producción	Baja
UIOVT***	Microsoft Windows Server 2008 R2 (64 bit)	Producción	Alta
UIOER***	Microsoft Windows Server 2008 R2 (64 bit)	Producción	Baja
UIOVI***	Microsoft Windows Server 2008 R2 (64 bit)	Producción	Media
UIOVI***	Microsoft Windows Server 2012 R2 (64 bit)	Producción	Alta
UIOVI***	Microsoft Windows Server 2012 R2 (64 bit)	Producción	Alta
UIOAD***	Microsoft Windows Server 2012 R2 (64 bit)	Producción	Alta
UIOVI***	Microsoft Windows Server 2012 R2 (64 bit)	Test	Baja
UIOVI***	Microsoft Windows Server 2012 R2 (64 bit)	Producción	Baja
UIOVI***	Microsoft Windows Server 2012 R2 (64 bit)	Test	Baja
UIOVI***	Microsoft Windows Server 2012 R2 (64 bit)	Producción	Media
UIOVI***	Microsoft Windows Server 2012 R2 (64 bit)	Producción	Media

Hostname	Sistema Operativo	Ambiente de trabajo	Criticidad
UIOVI***	Microsoft Windows Server 2012 R2 (64 bit)	Producción	Media
UIOVA***	Microsoft Windows Server 2012 R2 (64 bit)	Test	Media
UIOAD***	Microsoft Windows Server 2012 R2 (64 bit)	Producción	Media
CUEAD***	Microsoft Windows Server 2012 R2 (64 bit)	Producción	Media
UIOVI***	Microsoft Windows Server 2012 R2 (64 bit)	Producción	Media
UIOVI***	Microsoft Windows Server 2016 (64 bit)	Producción	Alta
UIOVI***	Microsoft Windows Server 2016 (64 bit)	Producción	Alta
UIOVI***	Microsoft Windows Server 2016 (64 bit)	Producción	Alta
UIONA***	Microsoft Windows Server 2016 (64 bit)	Producción	Alta
UIOAD***	Microsoft Windows Server 2016 (64 bit)	Producción	Alta
UIOVP***	Microsoft Windows Server 2016 (64 bit)	Producción	Baja
UIOTA***	Microsoft Windows Server 2016 (64 bit)	Producción	Baja
UIOOC***	Microsoft Windows Server 2016 (64 bit)	Test	Baja
UIOVI***	Microsoft Windows Server 2016 (64 bit)	Producción	Media
UIOVI***	Microsoft Windows Server 2016 (64 bit)	Producción	Media
UIOVI***	Microsoft Windows Server 2016 (64 bit)	Producción	Media
UIOVI***	Microsoft Windows Server 2016 (64 bit)	Producción	Media
UIOVI***	Microsoft Windows Server 2016 (64 bit)	Producción	Media
UIOVI***	Microsoft Windows Server 2016 (64 bit)	Producción	Media
UIOVI***	Microsoft Windows Server 2016 (64 bit)	Producción	Media
UIOVI***	Microsoft Windows Server 2016 (64 bit)	Producción	Media
UIOVI***	Microsoft Windows Server 2016 (64 bit)	Test	Media
UIOVD***	Microsoft Windows Server 2016 (64 bit)	Test	Media

Hostname	Sistema Operativo	Ambiente de trabajo	Criticidad
UIODF***	Microsoft Windows Server 2016 (64 bit)	Producción	Media
AWSEX***	Microsoft Windows Server 2016 (64 bit)	Producción	Media
UIOAD***	Microsoft Windows Server 2016 (64 bit)	Producción	Media
UIOVT***	Microsoft Windows Server 2019 (64 bit)	Producción	Alta
UIOVT***	Microsoft Windows Server 2019 (64 bit)	Producción	Alta
UIOVL***	Microsoft Windows Server 2019 (64 bit)	Producción	Alta
UIOVJ***	Microsoft Windows Server 2019 (64 bit)	Producción	Alta
UIOVD***	Microsoft Windows Server 2019 (64 bit)	Producción	Alta
UIOVA***	Microsoft Windows Server 2019 (64 bit)	Producción	Alta
UIOVA***	Microsoft Windows Server 2019 (64 bit)	Producción	Alta
UIOVA***	Microsoft Windows Server 2019 (64 bit)	Producción	Alta
UIOVA***	Microsoft Windows Server 2019 (64 bit)	Producción	Alta
UIOVW***	Microsoft Windows Server 2019 (64 bit)	Producción	Baja
UIOVP***	Microsoft Windows Server 2019 (64 bit)	Producción	Baja
UIOVI***	Microsoft Windows Server 2019 (64 bit)	Producción	Baja
UIOVI***	Microsoft Windows Server 2019 (64 bit)	Producción	Baja
UIOVI***	Microsoft Windows Server 2019 (64 bit)	Producción	Baja
UIOVI***	Microsoft Windows Server 2019 (64 bit)	Test	Baja
UIOOC***	Microsoft Windows Server 2019 (64 bit)	Test	Baja
UIVNE***	Microsoft Windows Server 2019 (64 bit)	Producción	Media
UIOVS***	Microsoft Windows Server 2019 (64 bit)	Producción	Media
UIOVL***	Microsoft Windows Server 2019 (64 bit)	Producción	Media
UIOVI***	Microsoft Windows Server 2019 (64 bit)	Producción	Media

Hostname	Sistema Operativo	Ambiente de trabajo	Criticidad
UIOVI***	Microsoft Windows Server 2019 (64 bit)	Producción	Media
UIOVI***	Microsoft Windows Server 2019 (64 bit)	Producción	Media
UIOVB***	Microsoft Windows Server 2019 (64 bit)	Producción	Media
UIOVB***	Oracle Linux Release 6 (64 bit)	Producción	Media
UIOVW***	Oracle Linux Release 7 (64 bit)	Producción	Alta
UIOVT***	Oracle Linux Release 7 (64 bit)	Producción	Alta
UIOVI***	Oracle Linux Release 7 (64 bit)	Producción	Alta
UIOWS***	Red Hat Enterprise 5 (32 bit)	Producción	Alta
UIOVI***	Red Hat Enterprise 5 (32 bit)	Producción	Alta
UIOVI***	Red Hat Enterprise 5 (32 bit)	Producción	Media
UIOVI***	Ubuntu Linux 20 (64 bit)	Producción	Baja
UIOVI***	Ubuntu Linux 20 (64 bit)	Producción	Media
UIOVI***	Ubuntu Linux 20 (64 bit)	Producción	Media
UIOVI***	Ubuntu Linux 20 (64 bit)	Producción	Media
UIOVI***	CentOS 6 (64 bit)	Producción	Alta
UIOVI***	CentOS 6 (64 bit)	Producción	Alta
UIOVI***	CentOS 6 (64 bit)	Producción	Alta
UIOVI***	CentOS 6 (64 bit)	Producción	Alta
UIOVI***	CentOS 6 (64 bit)	Producción	Alta
UIOVI***	CentOS 6 (64 bit)	Producción	Alta
UIOVI***	CentOS 6 (64 bit)	Producción	Alta
UIOFA***	CentOS 6 (64 bit)	Producción	Alta
UIOAP***	CentOS 6 (64 bit)	Producción	Alta

Hostname	Sistema Operativo	Ambiente de trabajo	Criticidad
UIOAP***	CentOS 6 (64 bit)	Producción	Alta
UIOVI***	CentOS 6 (64 bit)	Producción	Media
UIOVI***	CentOS 6 (64 bit)	Producción	Media
UIOVI***	CentOS 7 (64 bit)	Producción	Alta
UIOVI***	CentOS 7 (64 bit)	Producción	Alta
UIOVI***	CentOS 7 (64 bit)	Producción	Alta
UIOVI***	CentOS 7 (64 bit)	Producción	Alta
UIOVI***	CentOS 7 (64 bit)	Producción	Alta
UIOVI***	CentOS 7 (64 bit)	Producción	Alta
UIOFA***	CentOS 7 (64 bit)	Producción	Alta
UIOVI***	CentOS 7 (64 bit)	Producción	Baja
UIOSI***	CentOS 7 (64 bit)	Producción	Baja
UIOVP***	CentOS 7 (64 bit)	Producción	Media
UIOVI***	CentOS 7 (64 bit)	Producción	Media
UIOVI***	CentOS 7 (64 bit)	Producción	Media
UIOVI***	CentOS 7 (64 bit)	Producción	Media

En la Tabla 2 se muestra un resumen con el conteo de los diferentes servidores por su criticidad, con un total de cien lo que deja abierta una licencia para un nuevo servidor de importancia que se encuentra en desarrollo.

Tabla 2

Resumen de servidores por sistemas operativos y criticidad

Sistemas Operativos	Criticidad			Total
	Alta	Baja	Media	
CentOS 6 (64 bit)	10		2	12
CentOS 7 (64 bit)	7	2	4	13
Microsoft Windows Server 2003 (32 bit)		3	1	4
Microsoft Windows Server 2008 R2 (64 bit)	1	1	1	3
Microsoft Windows Server 2012 R2 (64 bit)	3	3	7	13
Microsoft Windows Server 2016 (64 bit)	5	3	13	21
Microsoft Windows Server 2019 (64 bit)	9	7	7	23
Oracle Linux Release 6 (64 bit)			1	1
Oracle Linux Release 7 (64 bit)	3			3
Red Hat Enterprise 5 (32 bit)	2		1	3
Ubuntu Linux 20 (64 bit)		1	3	4
Total	**40**	**20**	**40**	**100**

Se tiene que el 64% de los servidores seleccionados funcionan bajo Microsoft Windows Server en diferentes versiones mientras que el 36% restante trabajan con Linux en diferentes distribuciones.

También se observa que los servidores con criticidad alta y media corresponden al 40% respectivamente y el 20% restante tienen una criticidad baja.

Módulos de los agentes

El agente Deep Security tiene módulos integrados que mejoran y amplían las capacidades de seguridad. La activación de cada uno tendrá una repercusión en la funcionalidad del sistema de ciberseguridad, donde el más importante es referente al IPS para la implementación del virtual patching en los diferentes servidores.

El detalle de la funcionalidad de cada uno de ellos se presenta a continuación en base a la información de (Trend Micro, 2023).

Anti-Malware

El módulo Anti-Malware proporciona protección a sus sistemas operativos Windows y distribuciones de Linux frente a software malicioso, incluyendo malware, spyware y troyanos.

Firewall

El módulo Firewall se encarga de gestionar el flujo de datos que entran y salen de la red, registrando eventos para facilitar auditorías.

Web Reputation

El módulo de reputación web ofrece filtrado de contenido al bloquear el acceso a dominios maliciosos y a servidores reconocidos de comunicación y control que son utilizados por ciberdelincuentes.

Activity Monitoring

El módulo de supervisión de actividades es una medida de seguridad que ofrece una visión completa de las acciones en los sistemas operativos. Cuando se activa este módulo, se envía a la información siguiente a la consola Trend Vision One (XDR) para su análisis y presentación:

- Actividad de procesos
- Actividad de archivos
- Actividad de la red
- Actividad de conexiones
- Actividad de consultas de dominio
- Actividad del Registro de Windows
- Actividad de cuentas de usuarios

Device Control

El módulo de control de dispositivos administra el acceso a unidades de almacenamiento externos conectados a computadoras. Esta función ayuda a prevenir la pérdida y filtración de datos.

Application Control

El módulo control de aplicaciones registra todos los cambios en el software en contraste con el original y genera eventos cuando detecta programas nuevos o modificados en el sistema de archivos. Cuando se detecte algún cambio, existe la posibilidad de permitir o bloquear el software, en casos extremos hasta bloquear el equipo de manera opcional.

Intrusion Prevention

El módulo Prevención de intrusiones inspecciona el tráfico entrante y saliente para detectar y bloquear actividades sospechosas. Esto evita la explotación de vulnerabilidades conocidas y de día cero. Workload Security admite la "aplicación de parches virtuales": puede utilizar las reglas de prevención de intrusiones para protegerse de vulnerabilidades conocidas hasta que se puedan parchear, lo que exigen muchas normativas de cumplimiento.

El módulo de prevención de intrusiones examina el tráfico de datos que entra y sale para detectar y bloquear actividades sospechosas, evitando así el exploit de vulnerabilidades conocidas. Este sistema utiliza parches virtuales basado en reglas de prevención de intrusiones para protegerse de vulnerabilidades conocidas hasta que se pueda aplicar un parche oficial.

Integrity Monitoring

El módulo de monitoreo de integridad ofrece la funcionalidad de rastrear y registrar cambios permitidos como los no permitidos realizados en un sistema, y además permite recibir alertas sobre modificaciones no planificadas o potencialmente maliciosas.

Log Inspection

El módulo de inspección de registros captura y examina los registros del sistema con el fin de ofrecer pruebas para auditorías o cumplir con requisitos internos la organización. Es posible enviar eventos sospechosos a un Sistema de Gestión de Información y Eventos de Seguridad (SIEM) o a un servidor de registro centralizado, lo que facilita la correlación, generación de informes y almacenamiento de la información.

Figura 4

Configuración de módulos

En la Figura 4 se muestra la configuración de los módulos con los que contaran los servidores para su seguridad. Donde los módulos desactivados se deben a que la funcionalidad de estos se encuentra administrada por otro servicio o dispositivo o no son necesarios para el objetivo planteado.

El papel del módulo Anti-Malware lo cumple el software Symantec Endpoint Protection utilizado con antelación en el data center. El Firewall es administrado por otros dispositivos con el personal de redes de la corporación. El control de dispositivos y aplicación no se implementa ya que se tiene un control exhaustivo de los usuarios que acceden a los servidores y los únicos con permisos para hacer cambios son los administradores. Al no contar con un Sistema de Gestión de Información y Eventos de Seguridad (SIEM) no es necesaria la incorporación de del módulo de inspección de registros.

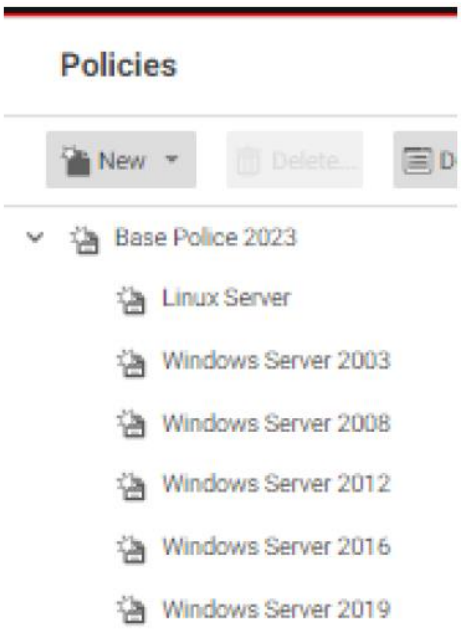
Directivas o Políticas de seguridad

Las directivas se utilizan para almacenar reglas y opciones de configuración que pueden ser aplicadas fácilmente a múltiples equipos. Estas directivas se crean con el propósito de configurar el comportamiento de los módulos de seguridad que están en uso. Su objetivo es simplificar la asignación de configuraciones y garantizar una consistencia en la protección de los sistemas (Trend Micro Incorporated, 2023).

Se crearon políticas con la nomenclatura para cada versión de sistema operativo que corresponde a los servidores seleccionados anteriormente, aunque las distribuciones de Linux se agrupo en una sola, esto se evidencia en la Figura 5.

Figura 5

Directivas implementadas

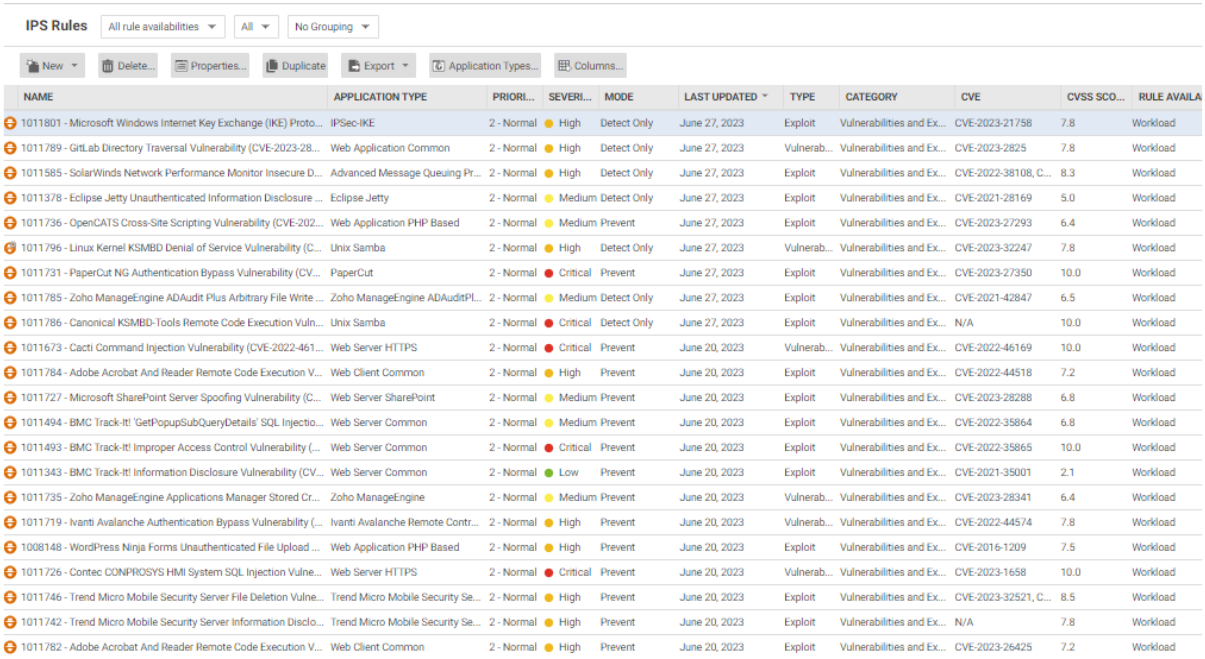


Se creo una directiva principal denominada Base Police 2023 la cual tiene la configuración general de los módulos y las reglas que utilizaran y de esta se hereda al resto que agruparan a cada sistema operativo para tener una mejor organización y gestión.

Para el sistema de Prevención de Intrusos la empresa Trend Micro dispone de una base de datos de 8.480 firmas o IPS rules como lo muestra la Figura 6 que se refieren a posibles vulnerabilidades para los diferentes sistemas operativos y con ello prevenir cualquier ataque con el parcheo virtual.

Figura 6

Base de datos del IPS

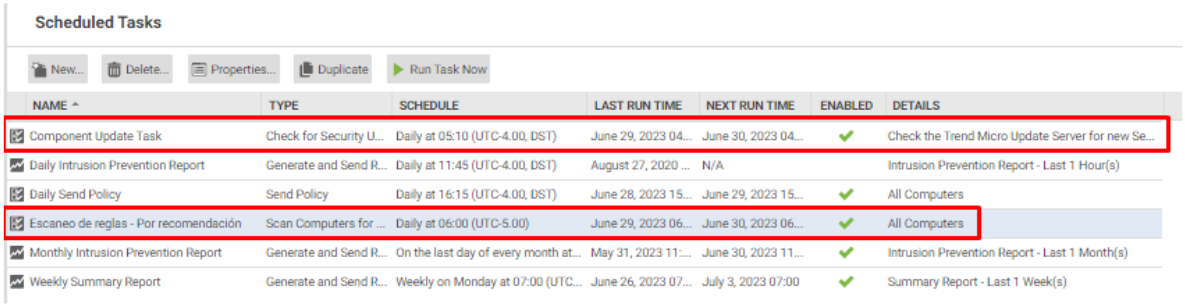


NAME	APPLICATION TYPE	PRIORI...	SEVERI...	MODE	LAST UPDATED	TYPE	CATEGORY	CVE	CVSS SCO...	RULE AVAILA
1011801 - Microsoft Windows Internet Key Exchange (IKE) Proto...	IPSec-IKE	2 - Normal	High	Detect Only	June 27, 2023	Exploit	Vulnerabilities and Ex...	CVE-2023-21758	7.8	Workload
1011789 - GitLab Directory Traversal Vulnerability (CVE-2023-28...	Web Application Common	2 - Normal	High	Detect Only	June 27, 2023	Vulnerab...	Vulnerabilities and Ex...	CVE-2023-2825	7.8	Workload
1011585 - SolarWinds Network Performance Monitor Insecure D...	Advanced Message Queuing Pr...	2 - Normal	High	Detect Only	June 27, 2023	Exploit	Vulnerabilities and Ex...	CVE-2022-38108, C...	8.3	Workload
1011378 - Eclipse Jetty Unauthenticated Information Disclosure ...	Eclipse Jetty	2 - Normal	Medium	Detect Only	June 27, 2023	Exploit	Vulnerabilities and Ex...	CVE-2021-28169	5.0	Workload
1011736 - OpenCATS Cross-Site Scripting Vulnerability (CVE-202...	Web Application PHP Based	2 - Normal	Medium	Prevent	June 27, 2023	Exploit	Vulnerabilities and Ex...	CVE-2023-27293	6.4	Workload
1011796 - Linux Kernel KSMBD Denial of Service Vulnerability (C...	Unix Samba	2 - Normal	High	Detect Only	June 27, 2023	Vulnerab...	Vulnerabilities and Ex...	CVE-2023-32247	7.8	Workload
1011731 - PaperCut NG Authentication Bypass Vulnerability (CV...	PaperCut	2 - Normal	Critical	Prevent	June 27, 2023	Exploit	Vulnerabilities and Ex...	CVE-2023-27350	10.0	Workload
1011785 - Zoho ManageEngine ADAudit Plus Arbitrary File Write ...	Zoho ManageEngine ADAuditPl...	2 - Normal	Medium	Detect Only	June 27, 2023	Exploit	Vulnerabilities and Ex...	CVE-2021-42847	6.5	Workload
1011786 - Canonical KSMBD-Tools Remote Code Execution Vuln...	Unix Samba	2 - Normal	Critical	Detect Only	June 27, 2023	Exploit	Vulnerabilities and Ex...	N/A	10.0	Workload
1011673 - Cacti Command Injection Vulnerability (CVE-2022-461...	Web Server HTTPS	2 - Normal	Critical	Prevent	June 20, 2023	Vulnerab...	Vulnerabilities and Ex...	CVE-2022-46169	10.0	Workload
1011784 - Adobe Acrobat And Reader Remote Code Execution V...	Web Client Common	2 - Normal	High	Prevent	June 20, 2023	Exploit	Vulnerabilities and Ex...	CVE-2022-44518	7.2	Workload
1011727 - Microsoft SharePoint Server Spoofing Vulnerability (C...	Web Server SharePoint	2 - Normal	Medium	Prevent	June 20, 2023	Exploit	Vulnerabilities and Ex...	CVE-2023-28288	6.8	Workload
1011494 - BMC Track-It! 'GetPopupSubQueryDetails' SQL Injectio...	Web Server Common	2 - Normal	Medium	Prevent	June 20, 2023	Exploit	Vulnerabilities and Ex...	CVE-2022-35864	6.8	Workload
1011493 - BMC Track-It! Improper Access Control Vulnerability (...	Web Server Common	2 - Normal	Critical	Prevent	June 20, 2023	Exploit	Vulnerabilities and Ex...	CVE-2022-35865	10.0	Workload
1011343 - BMC Track-It! Information Disclosure Vulnerability (CV...	Web Server Common	2 - Normal	Low	Prevent	June 20, 2023	Exploit	Vulnerabilities and Ex...	CVE-2021-35001	2.1	Workload
1011735 - Zoho ManageEngine Applications Manager Stored Cr...	Zoho ManageEngine	2 - Normal	Medium	Prevent	June 20, 2023	Vulnerab...	Vulnerabilities and Ex...	CVE-2023-28341	6.4	Workload
1011719 - Ivanti Avalanche Authentication Bypass Vulnerability (...	Ivanti Avalanche Remote Contr...	2 - Normal	High	Prevent	June 20, 2023	Vulnerab...	Vulnerabilities and Ex...	CVE-2022-44574	7.8	Workload
1008148 - WordPress Ninja Forms Unauthenticated File Upload ...	Web Application PHP Based	2 - Normal	High	Prevent	June 20, 2023	Exploit	Vulnerabilities and Ex...	CVE-2016-1209	7.5	Workload
1011726 - Contec CONPROSYS HMI System SQL Injection Vulne...	Web Server HTTPS	2 - Normal	Critical	Prevent	June 20, 2023	Vulnerab...	Vulnerabilities and Ex...	CVE-2023-1658	10.0	Workload
1011746 - Trend Micro Mobile Security Server File Deletion Vulne...	Trend Micro Mobile Security Se...	2 - Normal	High	Prevent	June 20, 2023	Exploit	Vulnerabilities and Ex...	CVE-2023-32521, C...	8.5	Workload
1011742 - Trend Micro Mobile Security Server Information Disclo...	Trend Micro Mobile Security Se...	2 - Normal	High	Prevent	June 20, 2023	Exploit	Vulnerabilities and Ex...	N/A	7.8	Workload
1011782 - Adobe Acrobat And Reader Remote Code Execution V...	Web Client Common	2 - Normal	High	Prevent	June 20, 2023	Exploit	Vulnerabilities and Ex...	CVE-2023-26425	7.2	Workload

Por el volumen de información y la complejidad para la asignación de estas firmas se cuenta con un escaneo de recomendaciones inteligente programado para las 6:00 am que las asignara automáticamente adaptándose al sistema operativo, su versión y aplicación. Como se observa en la Figura 7 se tiene configurada las tareas de escaneo de reglas a una hora establecida y también la búsqueda de actualizaciones de esta base de datos.

Figura 7

Tareas programadas



NAME	TYPE	SCHEDULE	LAST RUN TIME	NEXT RUN TIME	ENABLED	DETAILS
Component Update Task	Check for Security U...	Daily at 05:10 (UTC-4.00, DST)	June 29, 2023 04...	June 30, 2023 04...	✔	Check the Trend Micro Update Server for new Se...
Daily Intrusion Prevention Report	Generate and Send R...	Daily at 11:45 (UTC-4.00, DST)	August 27, 2020 ...	N/A		Intrusion Prevention Report - Last 1 Hour(s)
Daily Send Policy	Send Policy	Daily at 16:15 (UTC-4.00, DST)	June 28, 2023 15...	June 29, 2023 15...	✔	All Computers
Escaneo de reglas - Por recomendación	Scan Computers for ...	Daily at 06:00 (UTC-5.00)	June 29, 2023 06...	June 30, 2023 06...	✔	All Computers
Monthly Intrusion Prevention Report	Generate and Send R...	On the last day of every month at...	May 31, 2023 11:...	June 30, 2023 11...	✔	Intrusion Prevention Report - Last 1 Month(s)
Weekly Summary Report	Generate and Send R...	Weekly on Monday at 07:00 (UTC...	June 26, 2023 07...	July 3, 2023 07:00	✔	Summary Report - Last 1 Week(s)

Para evidencia el funcionamiento de la asignación automática de las reglas IPS se muestra en la Figura 8 a un servidor con SO legacy con Windows Server 2003 el cual se ha asignado 693 reglas mientras que en la Figura 9 se muestra un servidor con Windows Server 2016 con únicamente 59 reglas.

Figura 8

IPS en servidor con Microsoft Windows Server 2003 (32 bit)

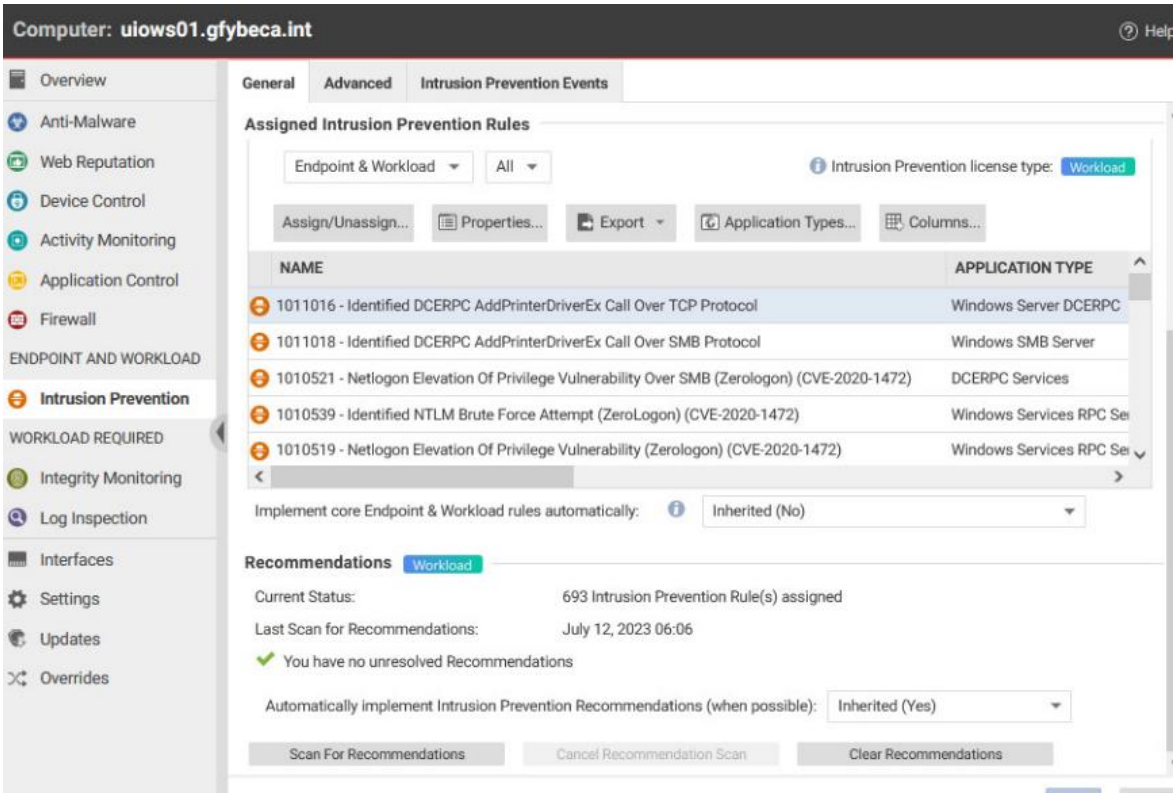
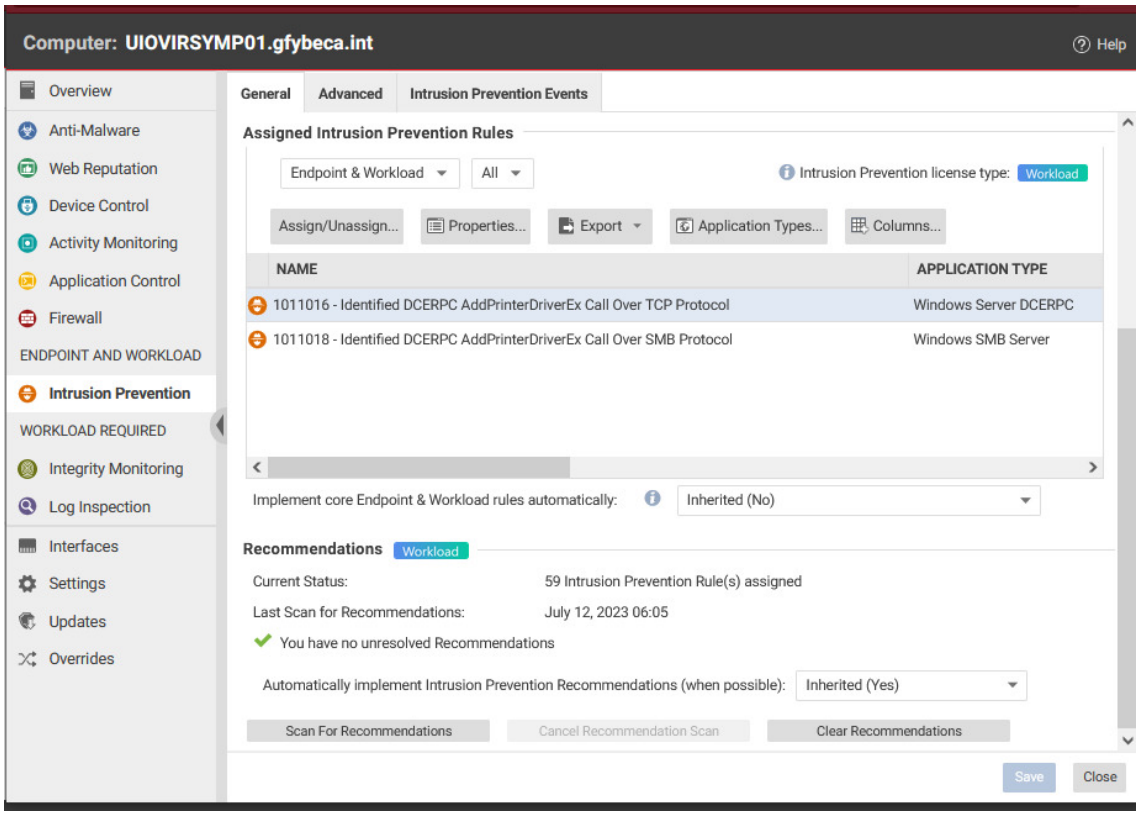


Figura 9

IPS en servidor con Microsoft Windows Server 2016 (64 bit)



Implementación de agentes

El agente de seguridad es implementado manualmente en los servidores descritos en la Tabla 1, los cuales proporcionaran la información de los diferentes módulos que fueron configurados en las directivas.

Requisitos del sistema

Los requisitos del sistema para la instalación de los agentes de Deep security se describen en la Tabla 3 que son muy similares para las distribuciones de Linux y Windows en general, únicamente variando la memoria RAM.

Tabla 3

Requisitos para instalación de agentes

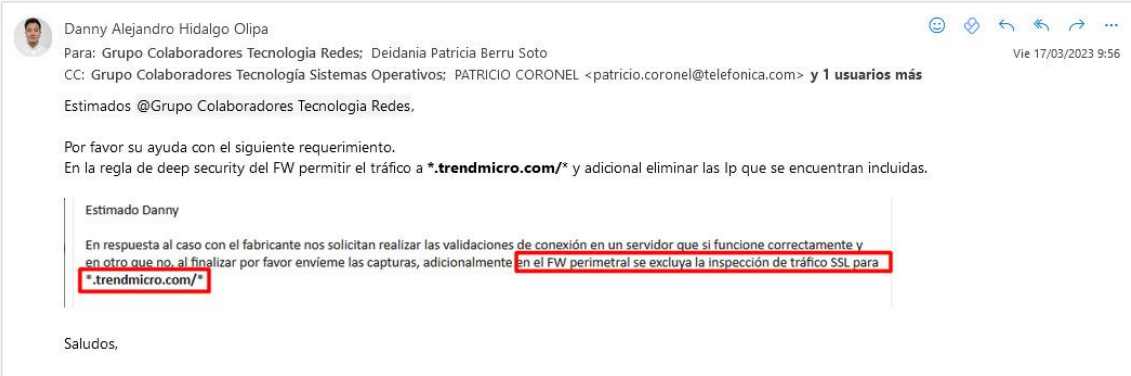
Componente del sistema	Requisitos
Procesador	• Servidor físico: Intel Pentium Dual-Core o equivalente mínimo, 4 núcleos o superior recomendado • Máquina virtual: se recomiendan 4 vCPU o más
Memoria RAM	2 GB como mínimo, se recomiendan 4 GB para Windows y 5GB para Linux
Almacenamiento	1 GB

Nota. Tomado de (Trend Micro Incorporated, 2023)

En cuanto a la comunicación entre la consola SaaS Cloud One Workload Security y los servidores es necesario permitir el tráfico de datos hacia los recursos del Trend Micro. Por lo tanto, es necesario solicitar al equipo de redes de la corporación establecer una regla en el FW para permitir el tráfico de datos hacia el dominio *.trendmicro.com/* como se muestra en la Figura 10 que se realiza el respectivo perdido a través de correo electrónico.

Figura 10

Requerimiento de FW

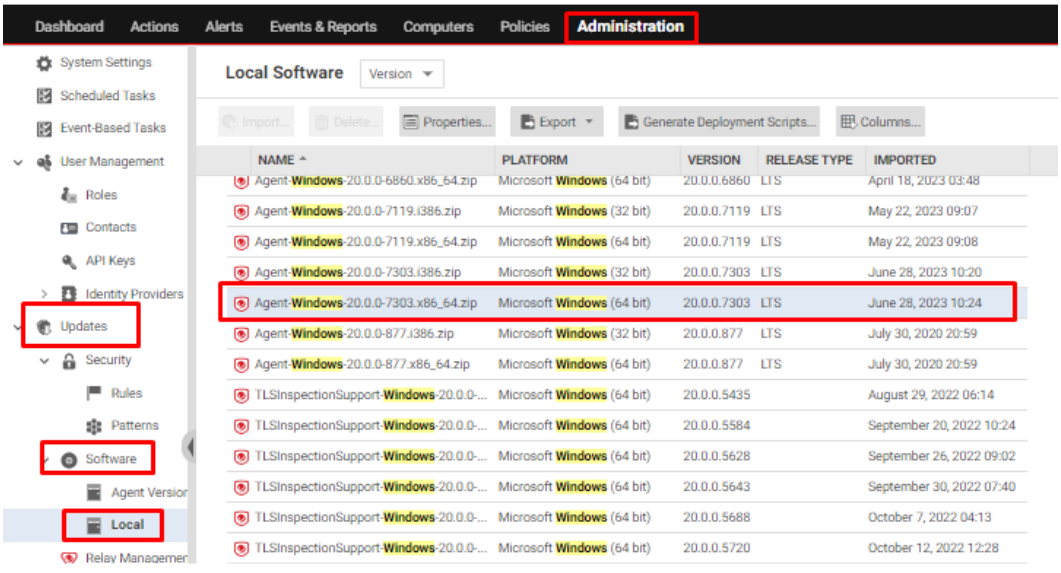


Instalación y configuración

Para la instalación de los agentes en los diferentes servidores es necesario descargar el instalador de la lista disponible seleccionando el sistema operativo y versión de kernel en caso de distribuciones Linux procurando utilizar la versión más actual, un ejemplo se visualiza en la Figura 11 para el instalador de un paquete para Windows.

Figura 11

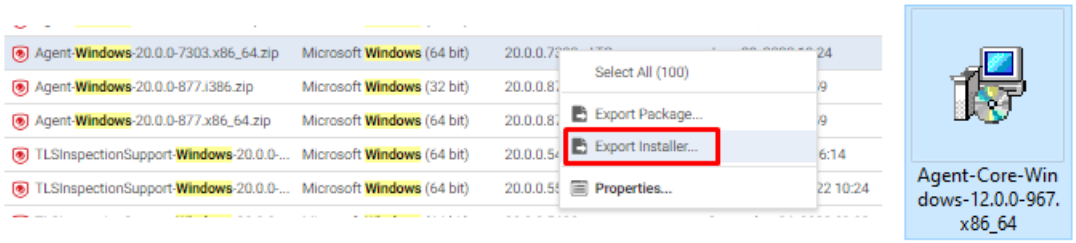
Descarga de instalador de agente Windows



Es necesario exportar el instalador como se muestra en la Figura 12 para luego copiarlo al servidor o al sistema que será gestionado.

Figura 12

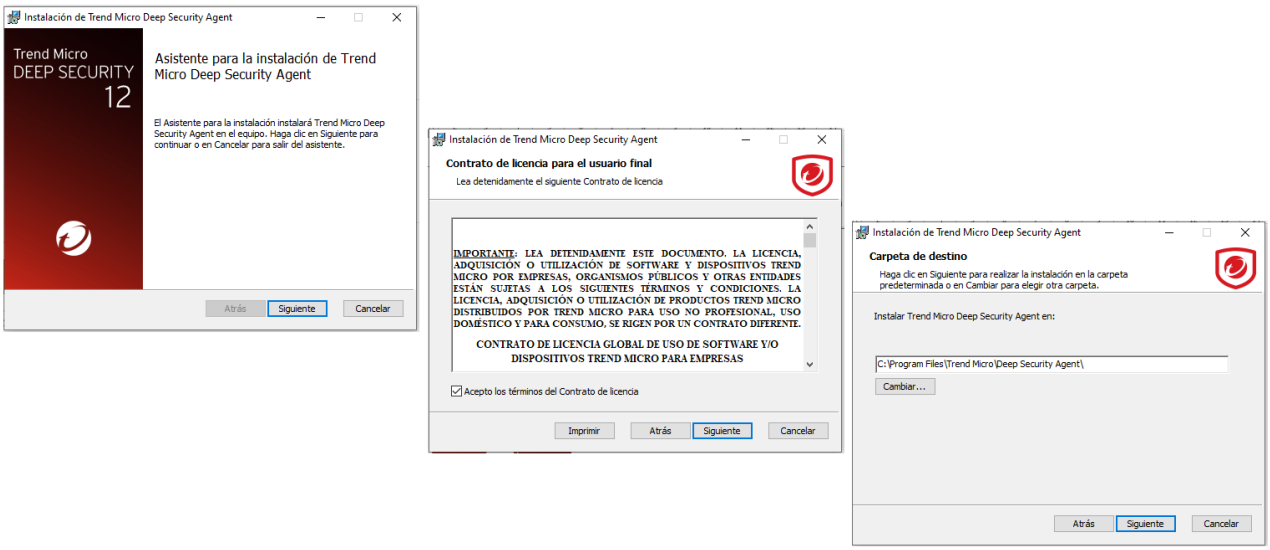
Exportar instalador de agente Windows



Al encontrarse en el dispositivo se debe iniciar el ejecutable con normalidad brindando los permisos con el usuario administrador para la instalación, siguiendo la ejecución normal, aceptando los términos del contrato de licencia y dejando por defecto la ubicación de almacenamiento de los archivos como se muestra en la Figura 13.

Figura 13

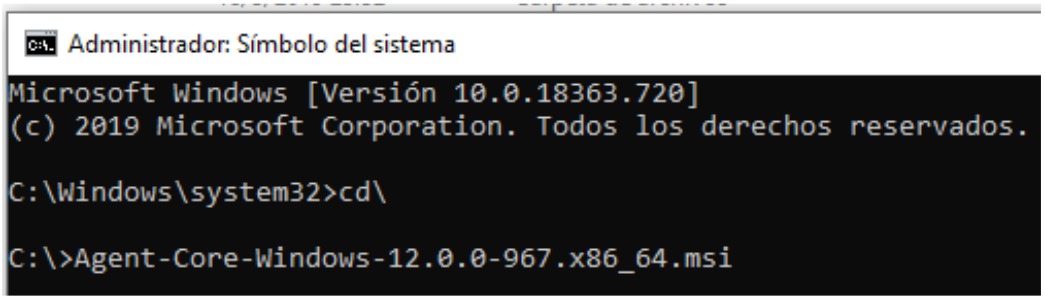
Instalación de agente Deep Security en Windows



Para los sistemas que se encuentren blindados y no sea posible lanzar el instalador será necesario ejecutar el .MSI desde la consola de comandos o CMD como administrador del sistema como se muestra en la Figura 14

Figura 14

Instalación desde el CMD

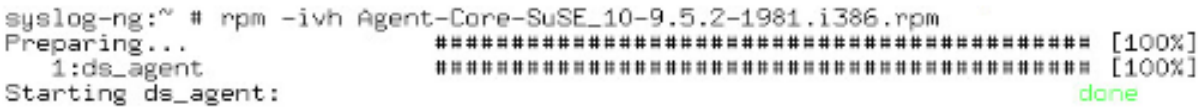


Para los equipos Linux desde Terminal y con usuario root, se debe ejecutar el siguiente comando brindando los permisos de ejecución anteriormente como se muestra en la Figura 15.

rpm -i <path_to_package_name>

Figura 15

Instalación en equipos Linux



Una vez concluida la instalación independiente del equipo, se tendrá en la barra de notificaciones el Icono de Workload Security y se demora alrededor de 5 minutos en sincronizar con la consola.

Activación

Antes de que el agente instalado pueda proteger al servidor debe activarse el agente con Workload Security. La activación registra al agente con el administrador durante una comunicación inicial, para lo cual se deben seguir los siguientes pasos:

1. En el equipo que ya se instaló el agente, abrir un CMD con permisos de administrador e ir a la ubicación: C:\Program Files\Trend Micro\Deep Security Agent\
2. Ejecute el siguiente comando extraído de Script de despliegue de la consola de Workload.

Comando para Windows:

dsa_control -a dsm://agents.deepsecurity.trendmicro.com:443/ "tenantID:191DE082-51DB-3D30-B942-DD5B59F1702F" "token:816AD695-*****-9D53-C18B-352E08*******" "policyid:206"

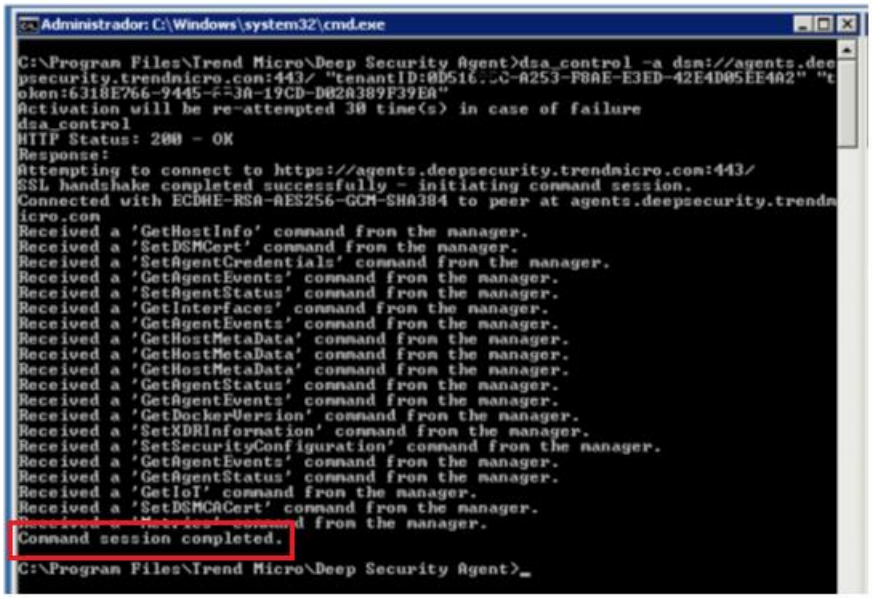
Comando para Linux:

/opt/ds_agent/dsa_control -a dsm://agents.deepsecurity.trendmicro.com:443/ "tenantID:191DE082-51DB-3D30-B942-DD5B59F1702F" " token:816AD695-*****-9D53-C18B-352E08*******" "policyid:202"

En la Figura 16 se muestra la ejecución de los pasos en un servidor Windows Server 2003, el proceso es el mismo sin importar la versión del sistema operativo.

Figura 16

Activación de agente en Windows



Este proceso de activación dura aproximadamente 5 minutos y muestra un mensaje informando que la ejecución del comando fue completada. En el dashboard de la consola cambia el estado el estado del equipo de Unmanaged en color gris a Managed en color verde y Online, en el caso de que esté Offline significa que no hay comunicación o le equipo se encuentra apagado o requiere un reinicio.

El proceso de activación de los módulos de protección es automático, en la consola ya fueron creadas las directiva o políticas con la respectiva configuración para que se activen los módulos licenciados, pero es necesario establecer a bajo cual directiva opera el equipo.

El proceso de asignación del grupo al que pertenece el nuevo equipo y la política a la cual se regirá se debe escoger de manera manual como se muestra en la Figura 17 que se asigna a un SO Windows Server 2003 escogiendo del grupo creado anteriormente de la Figura 5; con ello el equipo ya se encuentra protegido.

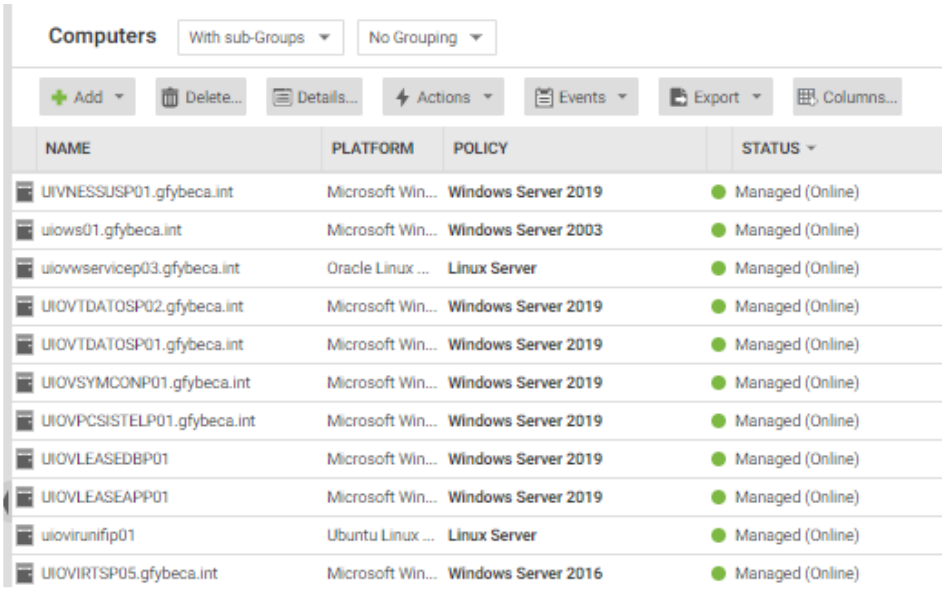
Figura 17

Asignación de directivas o políticas

La instalación de los agentes en los servidores fue manualmente en ventanas de mantenimiento programadas, como se muestra en la Figura 18 se instaló en sistemas operativos Windows y Linux en sus diferentes versiones, aunque la lista no está completa, pero se puede visualizar el estado Managed que indica la correcta comunicación y trabajo del agente.

Figura 18

Lista de Servidores con agentes activos



Versión de agentes actuales

En la Figura 19 y Figura 20 se muestra las versiones actuales con las que se instalan los agentes en Windows la versión actual es 20.0.0.7303 y en Linux es la versión 20.0.0.7303.

Figura 19

Versiones de Agentes Windows

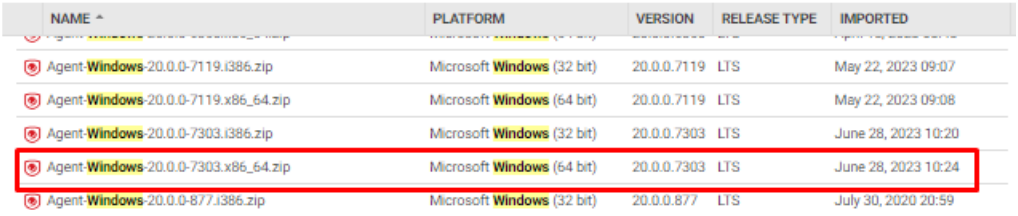


Figura 20

Versiones de Agentes Linux

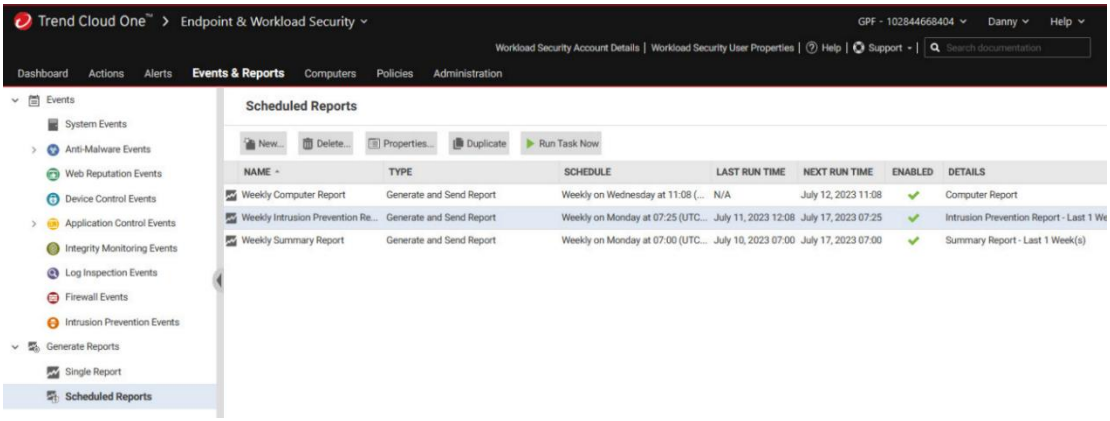
Sistema de reportes

Para tener un control periódico del estado de los agentes de los equipos se generan reportes programados semanalmente que envía al correo electrónico del grupo de administradores encargados de la gestión del sistema de ciberseguridad los mostrados en la Figura 21, que serán tres:

- Reporte de los equipos o computadoras
- Reporte de IPS
- Reporte de resumen de incidencias

Figura 21

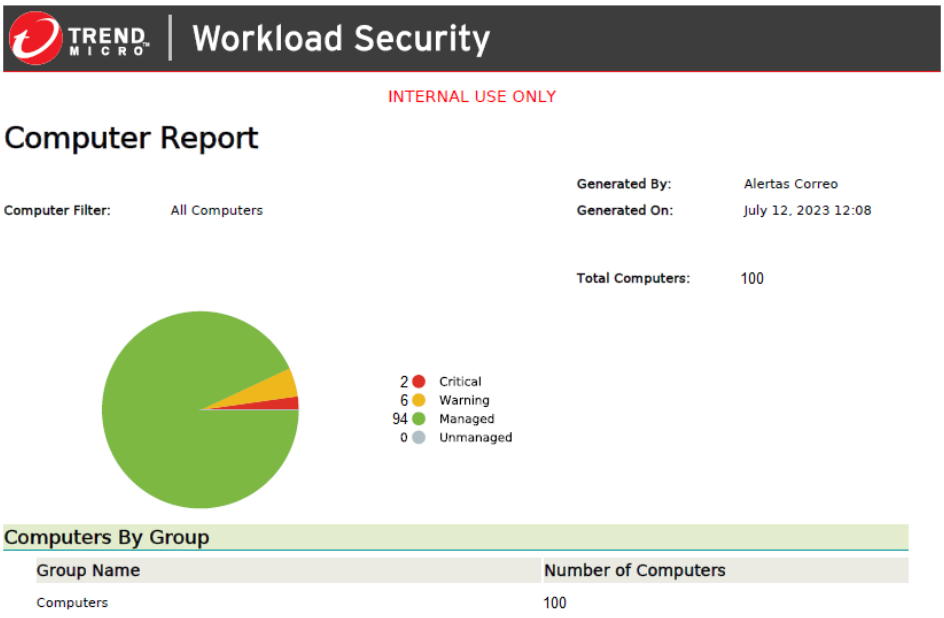
Programación de reportes



Por cuestiones de confidencialidad se mostrará únicamente el reporte de los equipos donde se tendrá un resumen del estado del agente en los servidores como se muestra en la Figura 22 viendo un global de los 100 equipos con los que se trabaja y cambia el estado a critico en caso de que el servidor este offline y advertencia por problemas de comunicación.

Figura 22

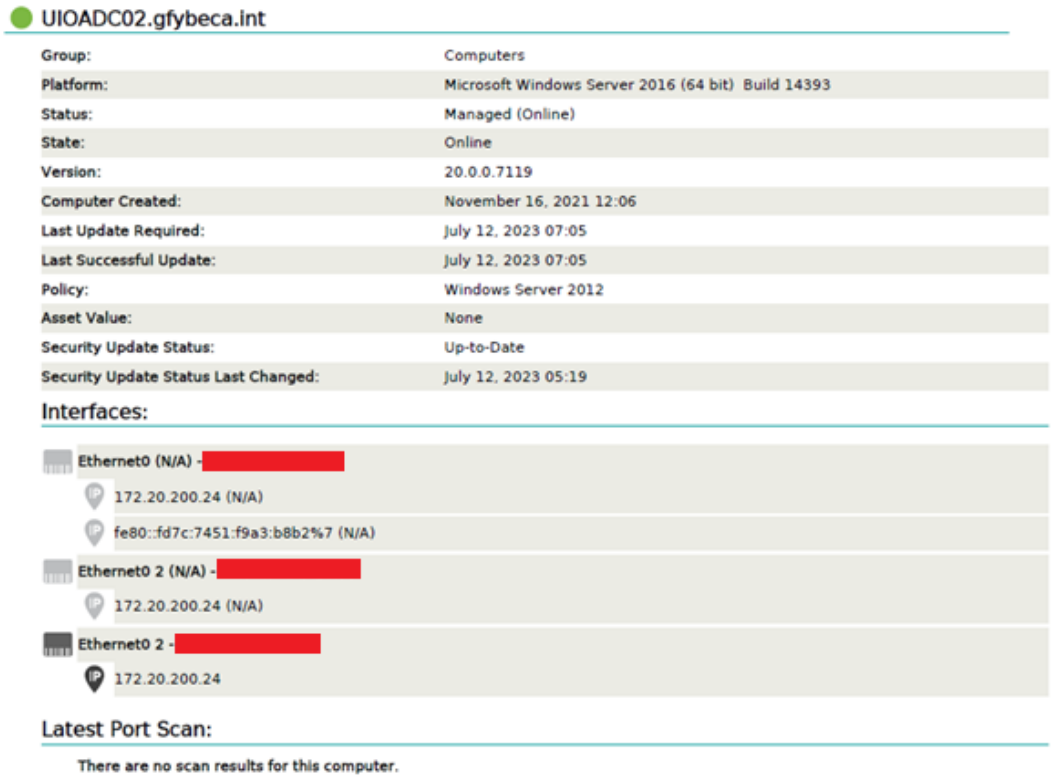
Reporte de los equipos



A parte de la visión general se detalla uno a uno los servidores como se muestra en la Figura 23 donde se tienen datos del sistema operativo, la versión del agente, el estado, las interfaces de red con las que cuenta y constantemente se monitorea y por cuestiones de confidencialidad se cubrió la dirección MAC de cada una de estas.

Figura 23

Detalle de un equipo



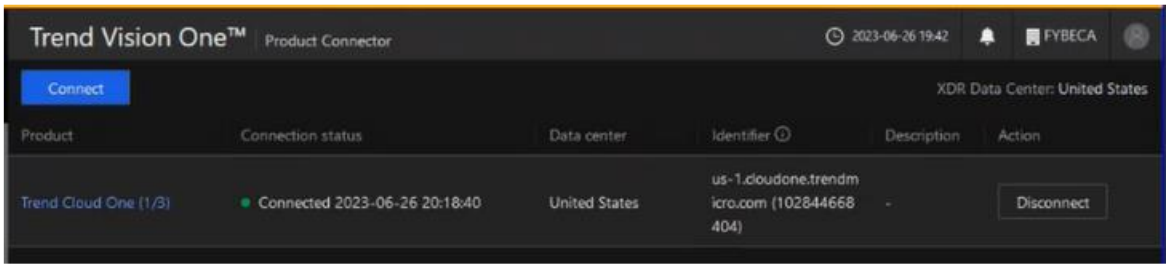
Configuración de XDR

La consola de administración de la herramienta se la realiza desde el portal de XDR con las credenciales entregadas al administrador, la plataforma de detección y respuesta extendida XDR, está conectada a las plataformas de Workload Security y los agentes instalados en cada uno de los servidores por medio del módulo de Activity Monitoring que enviará la información sobre actividades de procesos, archivos, tráfico de red, conexión, registros de Windows y cuentas de usuarios.

En la Figura 24 se muestra la conexión activa con la consola de Cloud One Workload Security.

Figura 24

Conexión Trend Vision One y Cloud One Workload Security



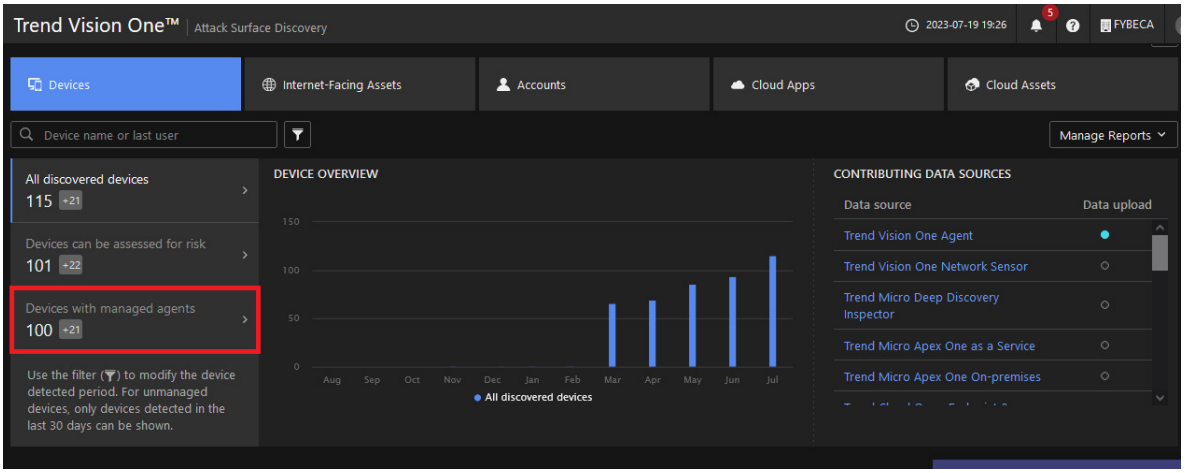
Durante el despliegue del sensor se habilitaron cien equipos enviando la telemetría hacia Vision One. Cada una de las plataformas y sensores son vitales para determinar el nivel de riesgo.

En la Figura 25 se muestra los 100 dispositivos que tienen los agentes instalados y actualmente están enviando información a la plataforma para su análisis y cálculo de riesgo. Se puede observar en el gráfico de barras sobre la descripción general del dispositivo que mide los dispositivos administrados y que desde el mes de marzo han ido aumentando.

Se supera los 100 dispositivos ya que al utilizar Service Gateway para integrar los servicios de actualizaciones y objetos sospechosos también revisa la actividad del resto de los servidores virtualizados en VMware a los que no se han instalado los agentes de deep security.

Figura 25

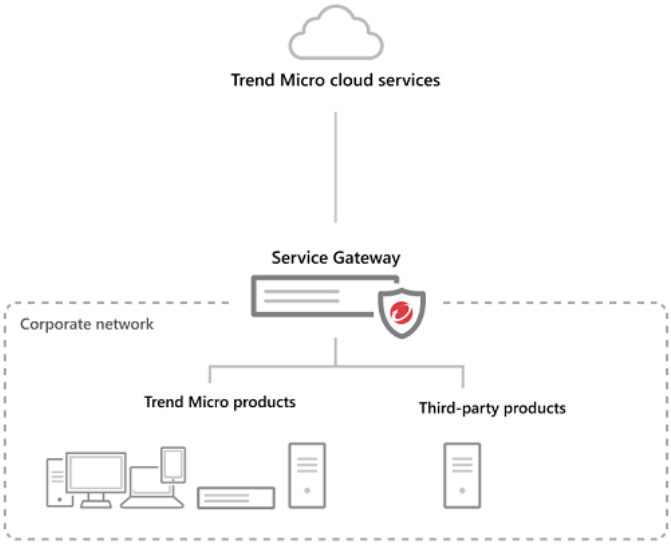
Equipos conectados



Implementación de Service Gateway sobre VMware

Figura 26

Service Gateway en una red híbrida



Nota. Tomado de (Trend Micro Incorporated, 2023)

Service Gateway, una parte esencial de Trend Micro Vision One, se implementa en la red local y cumple como intermediario entre Trend Micro Vision One y otros productos, incluidos

aquellos de terceros, instalados en la misma infraestructura como se muestra en la Figura 26. Esta configuración permite aprovechar los servicios en la nube de Trend Micro de manera eficiente al reducir el tráfico de Internet y compartir información relevante sobre posibles amenazas. Al estar enlazado con la red local, el dispositivo virtual del Service Gateway facilita servicios vitales como ActiveUpdate, Smart Protection Services y la sincronización de listas de objetos sospechosos para los productos locales de Trend Micro.

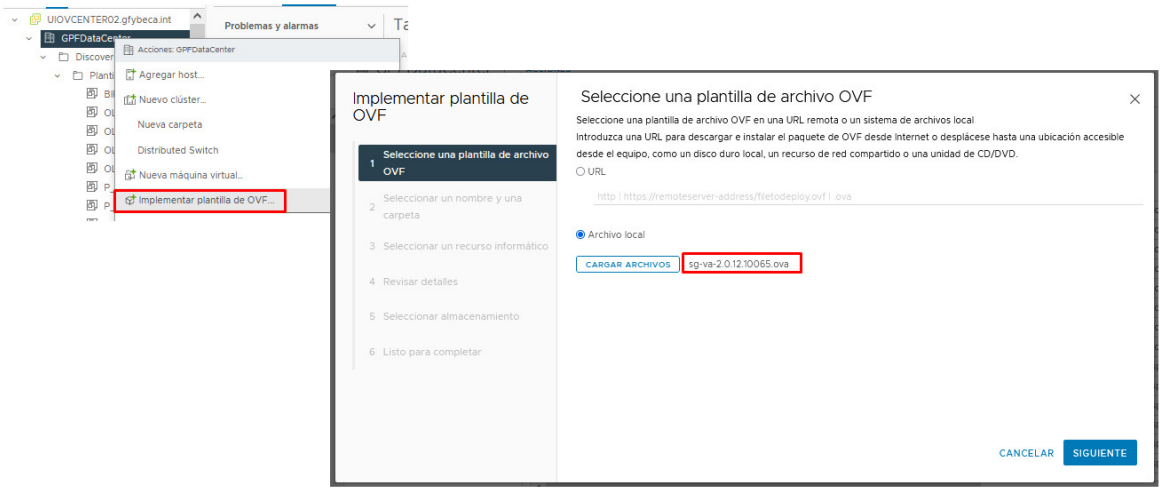
A continuación, se muestra como implementar Trend Micro Vision One Service Gateway en entornos locales, es decir, en un servidor virtualizado VMware.

Para descargar el dispositivo virtual se debe ingresar a la consola de Trend Micro Vision One y dirigirse a gestión de puerta de enlace de servicios. Para luego aceptar la licencia de usuario final y obtener la imagen iso.

Para iniciar el proceso es necesario acceder al hipervisor Vmware Sphere con los permisos de usuarios adecuados para la implementación de un plantilla OVF y para seleccionar de un archivo local la imagen iso descargada anteriormente.

Figura 27

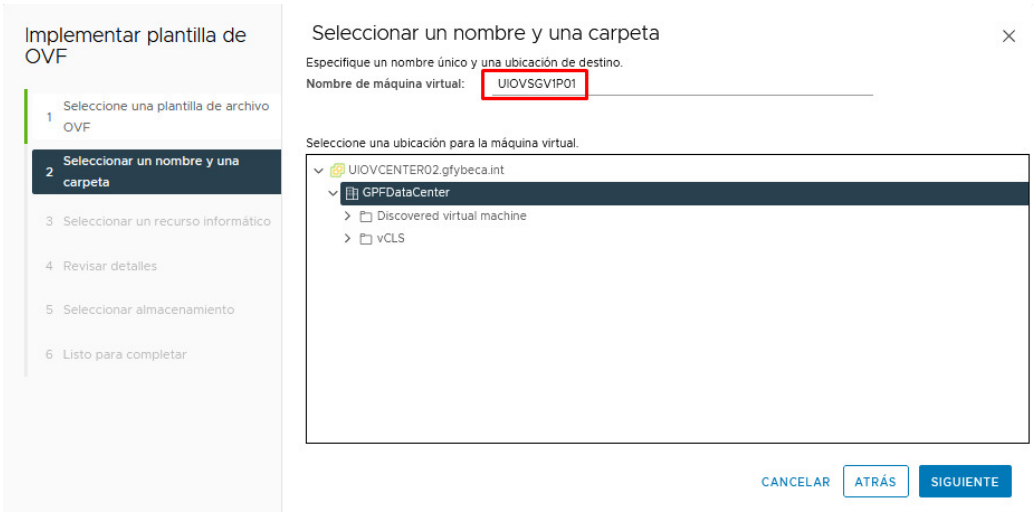
Implementación de plantilla OVF



Se continua con el asistente de instalación para lo cual el siguiente paso es colocar el nombre de la máquina virtual o del servidor virtualizado de Service Gateway y seleccionar su directorio, por políticas de la organización el nombre tiene una codificación que informa de la ubicación del servidor, el servicio que ofrece, el ambiente en el que trabajara y el puesto que ocupa.

Figura 28

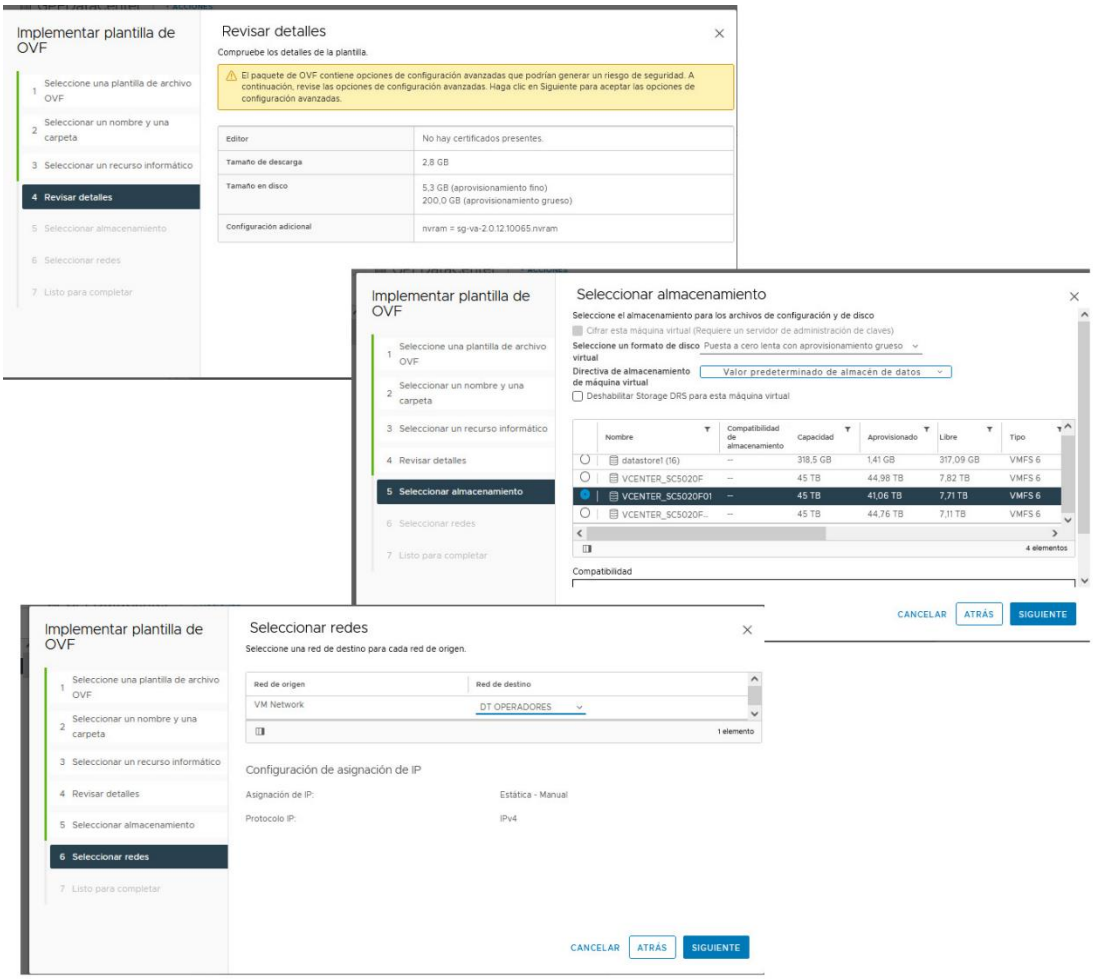
Nombre del servidor virtualizado



Es necesario seleccionar los recursos informáticos como se muestra en la Figura 29, eligiendo el almacenamiento, la capacidad de procesamiento, memoria RAM y la red que ocupará.

Figura 29

Configuración de recursos del servidor



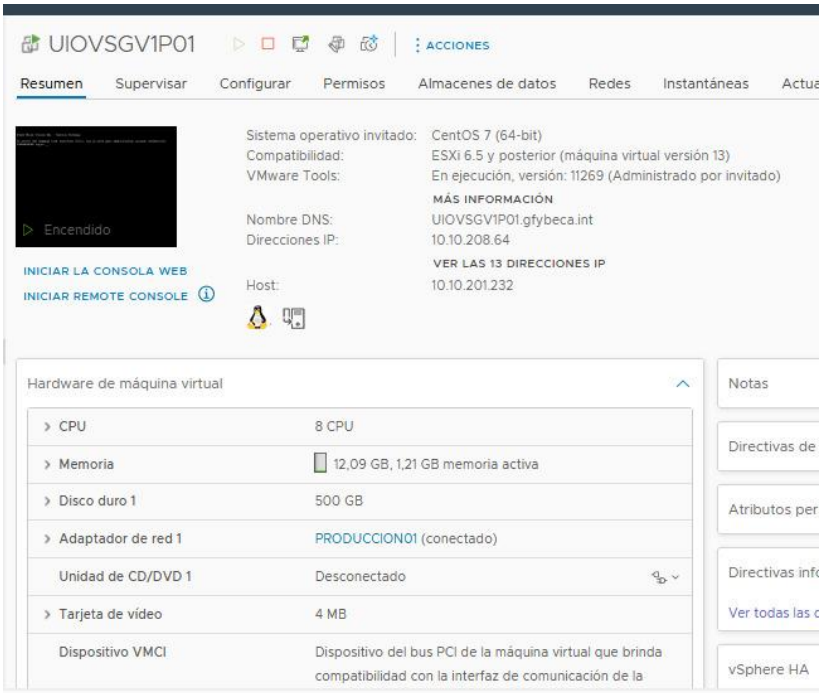
En la Figura 30 se muestra un resumen de los componentes y la plantilla que utilizara el servidor de Service Gateway previo a la finalización del proceso de implementación.

Figura 30

Resumen del servidor

Figura 31

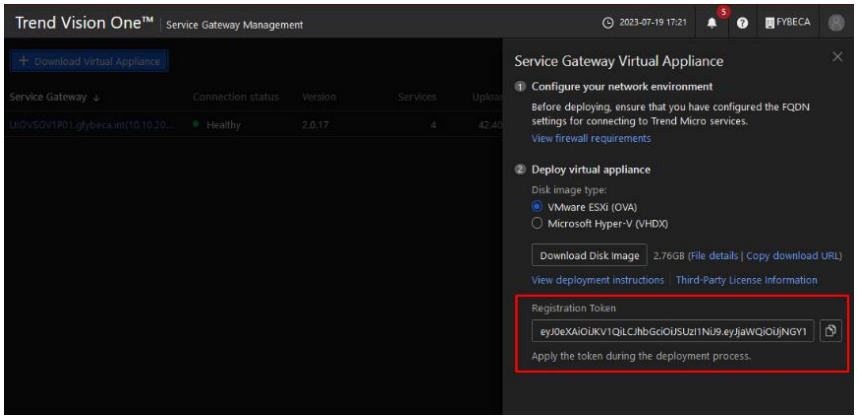
Servidor implementado



En la Figura 31 se muestra al servidor implementado ya implementado con un resumen de los recursos que utiliza y se puede evidencia que el sistema operativo en el que trabajo es una distribución de Linux, con esto ya se puede acceder a la consola CLI para su respectiva configuración de red y verificar la comunicación con los servidores de Trend Micro Vision One Cloud, para poder mantener la comunicación este servidor se implementó en la red de producción con permisos especiales para comunicarse con el resto de servidores.

Figura 32

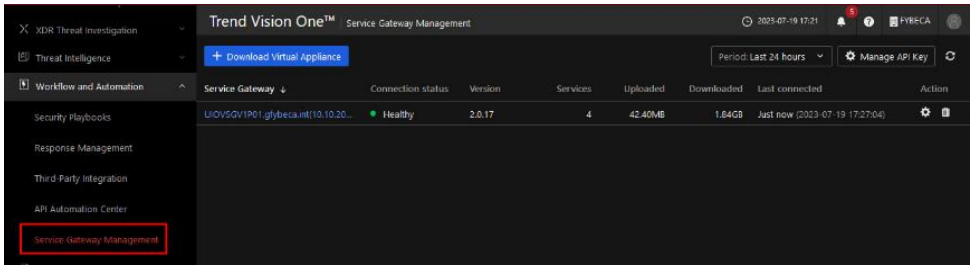
Registro de token



Para la activación del servidor y autorizar la comunicación entre los diferentes servicios de Trend Micro es necesario utilizar un token como se muestra en la Figura 32 que licencia la aplicación.

Figura 33

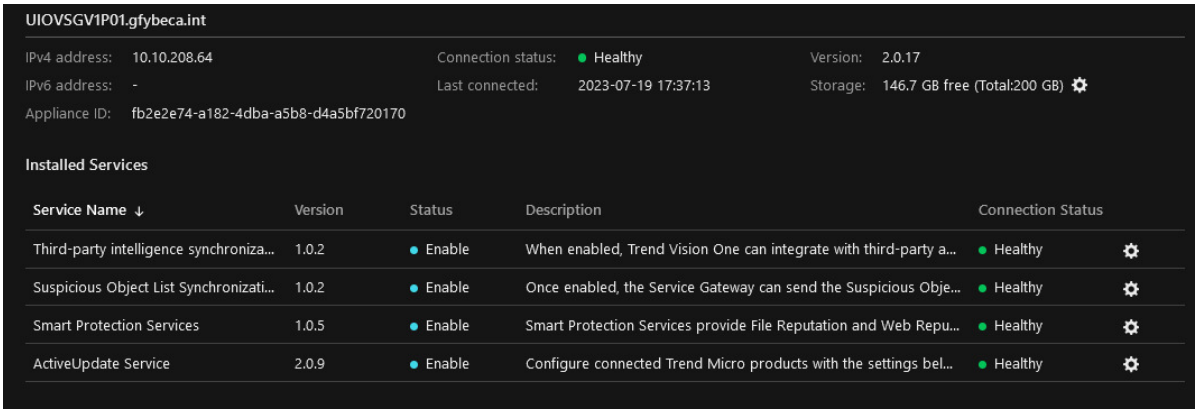
Estatus del Service Gateway



En la Figura 33 se observa como el servidor UIOVSGV1P01 que incorpora el Service Gateway se encuentra con un estado de comunicación saludable y en la Figura 34 se muestra los servicios instalados que constan de la sincronización de Trend Vision One con productos de tercero, la sincronización de la Lista de objetos sospechosos que puede enviar el Service Gateway, el servicio de protección inteligente que revisa la reputación de archivos y sitios web y finalmente la actualización de los servicios de Trend Micro.

Figura 34

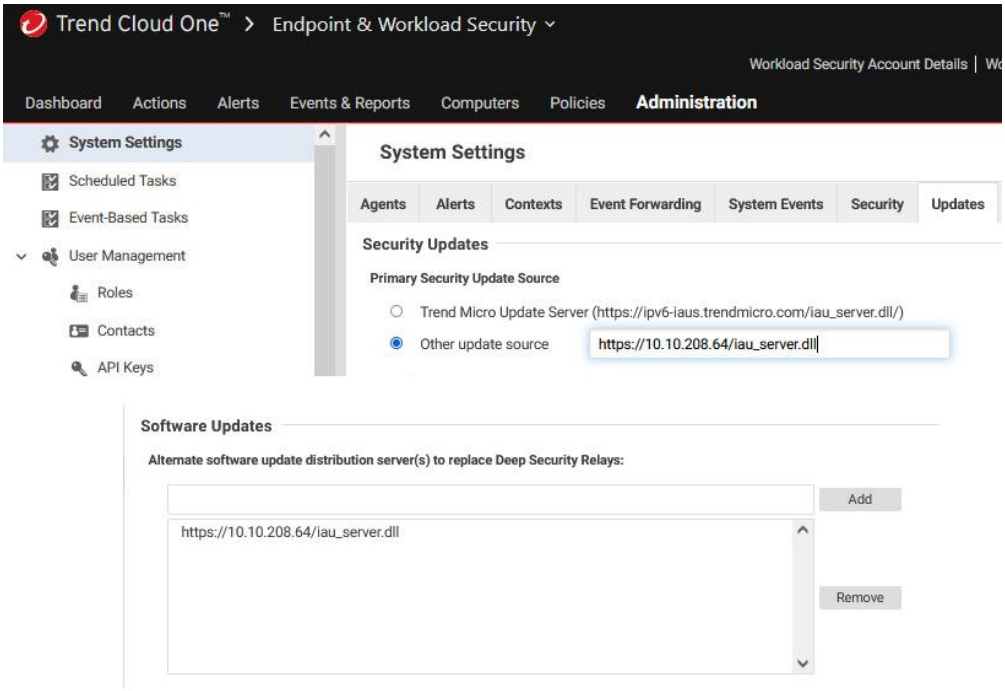
Servicios instalados del Service Gateway



Actualmente el tráfico de información desde los agentes de Deep Security hacia los servicios de Trend Micro lo realizan a través del Service Gateway como lo indica la Figura 26 por lo que para utilizar el servicio de actualización instalado es necesario configurar en la consola del Cloud One Workload Security que la fuente primaria de actualizaciones es el servidor virtualizado en VMware UIOVSGV1P01 como se muestra en la Figura 35.

Figura 35

Configuración de actualizaciones Cloud One Workload Security



Capítulo IV. Análisis de efectividad

Una vez implementada y configurada la solución y con el fin de determinar el beneficio que esta genera a la empresa, se realiza un análisis de efectividad del sistema para obtener el riego al cual se encuentran sujetos los servidores, el cual se basa en datos verificados y específicos del número de alertas clasificadas en crítico, advertencia y administrado, los mismos que se muestran en la consola del sistema de ciberseguridad.

Dashboard consola Cloud One Workload Security

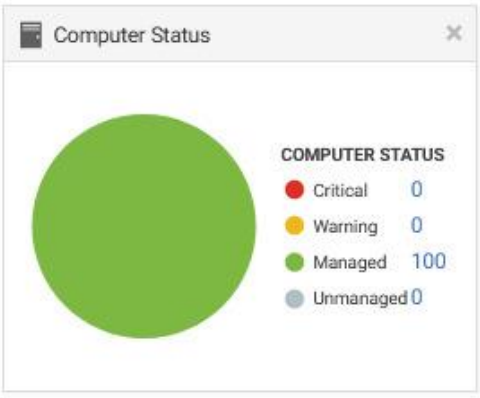
En este dashboard de la consola uno se observa la información recopilada a través de los módulos instalados en los agentes, la cual se actualiza en tiempo real, y lo que se muestra se puede configurar periodos de tiempo de los datos y filtros para modificar la información y adaptarlo a las necesidades del usuario.

Informe informático

Con ese informe se analizará el estado de los agentes instalados en los cien servidores de la Corporación GPF, donde se evalúa la conexión hacia el servicio de Trend Micro y la información que envían los módulos.

Figura 36

Estado de servidores



Según la Figura 36 el 100% de los servidores están siendo manejados correctamente, lo que implica que la comunicación es la adecuada. Estos valores pueden variar en ocasiones ya que los servidores pueden estar en mantenimiento y perder la comunicación o también presenta alguna alarma de advertencia.

Eventos de IPS

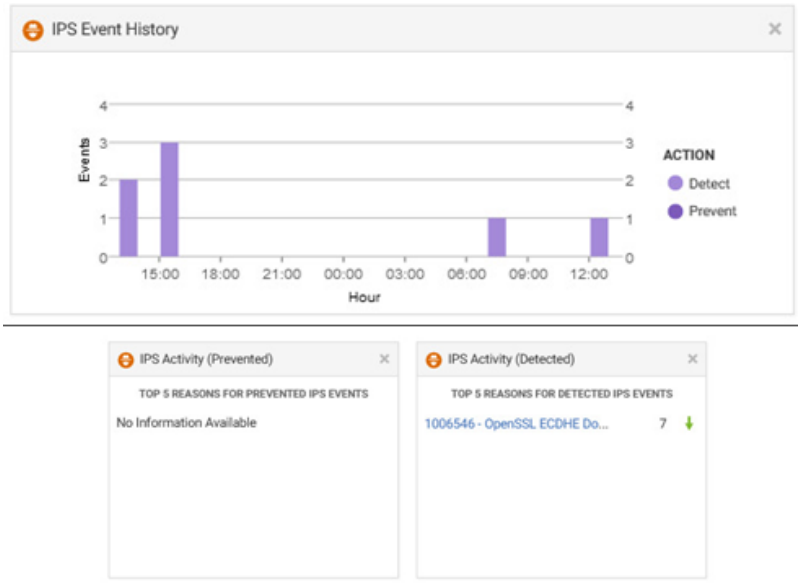
El informe presenta una variedad de datos relacionados con la actividad de prevención de intrusiones y tipos de aplicaciones detectadas y prevenidas. En primer lugar, muestra los cinco tipos de aplicaciones detectados y prevenidos más frecuentes, junto con la cantidad de veces que se activaron. También incluye mapas de árbol que ilustran la gravedad de los eventos y su frecuencia para cada tipo de aplicación. Además, se destacan los cinco principales motivos de detección y prevención de intrusiones, así como los cinco equipos y direcciones IP de origen más involucrados en dichos eventos.

Por último, se ofrece un historial de eventos recientes y las razones detrás de los eventos detectados y prevenidos desde la última actualización. Toda esta información proporciona una visión general completa del panorama de seguridad y actividades relacionadas con la prevención de intrusiones.

Como se muestra en la Figura 37 se observa eventos que se han ejecutado en diferentes horarios y actividades detectadas. Aunque la información es poca esta se actualiza en tiempo real y dejando que el sistema trabaje por más tiempo este obtendrá más datos.

Figura 37

Eventos de prevención de intrusiones



Eventos de Monitoreo de integridad

El informe detalla la actividad de monitoreo de integridad, destacando las cinco principales razones detrás de los eventos, identificando las reglas que se activaron junto con su frecuencia. Además, se muestran los cinco equipos principales en los que se produjeron estos eventos, proporcionando una visión clara de su distribución. El historial de eventos de supervisión de integridad muestra eventos recientes junto con la gravedad de cada uno.

Por otro lado, el informe también resalta las cinco claves principales relacionadas con los eventos de supervisión de integridad, donde la fuente de la clave puede variar según el conjunto de entidades. Para archivos y directorios, se utiliza su ruta como clave, mientras que, para los puertos, se emplea su protocolo único, dirección IP, número de puerto como identificador. Esta información es esencial para comprender la naturaleza y el origen de los eventos de supervisión de integridad, permitiendo una mejor gestión y toma de decisiones en términos de seguridad y monitoreo de la integridad del sistema.

Figura 38

Eventos de integridad de monitoreo

En la Figura 38 nos muestra la información recopilada por el módulo de monitoreo de integridad de los 100 servidores, donde se han generado alrededor de 200 eventos de nivel medio.

Índice de riesgo

El índice de riesgo es calculado considerando múltiples elementos, tales como indicadores y la cantidad de usuarios, dispositivos y aplicaciones riesgosas a lo largo del tiempo. A través del panel de control, se muestra el índice de riesgo organizacional, clasificando los factores de riesgo y evaluando cómo afectan específicamente a la red. Para obtener una evaluación de riesgos más completa, es importante configurar más fuentes de datos.

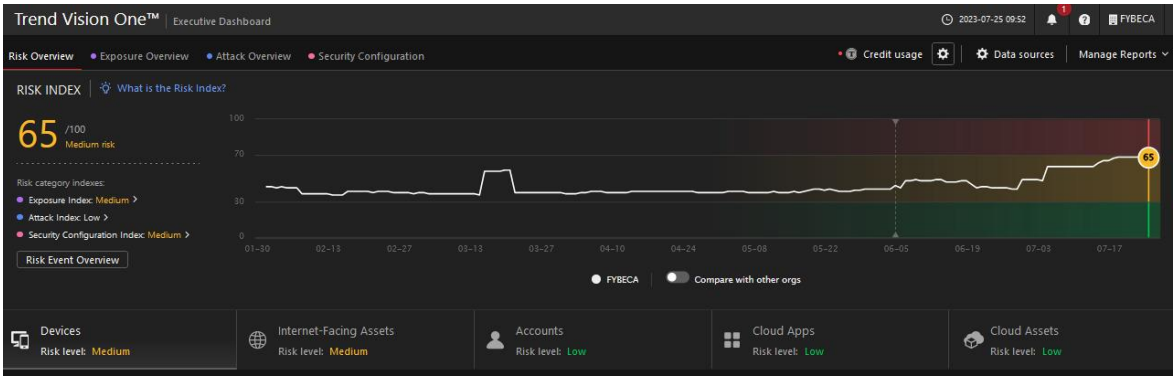
Trend Vision One permite reducir los riesgos presentes en el entorno proporcionando pasos para solucionar los problemas y medidas preventivas. Mediante esta herramienta, se facilita la mitigación de riesgos y la implementación de acciones correctivas para mantener un ambiente seguro y protegido.

La Figura 38 se muestra en índice de riesgo actual de los cien servidores que incorporan los agentes de Deep Security que alcanza el 65% correspondiente a un nivel medio. Del cual se puede desglosar el índice de riego de los dispositivos conectados que también se encuentra en medio, activos orientados a internet con un nivel medio, cuentas de usuarios con un nivel bajo,

aplicaciones y activos en la nube con un nivel bajo. Lo que nos indica que el mayor riesgo presente se encuentra en los cien servidores que fueron instalados los agentes de Deep Security.

Figura 39

Índice de riesgo actual

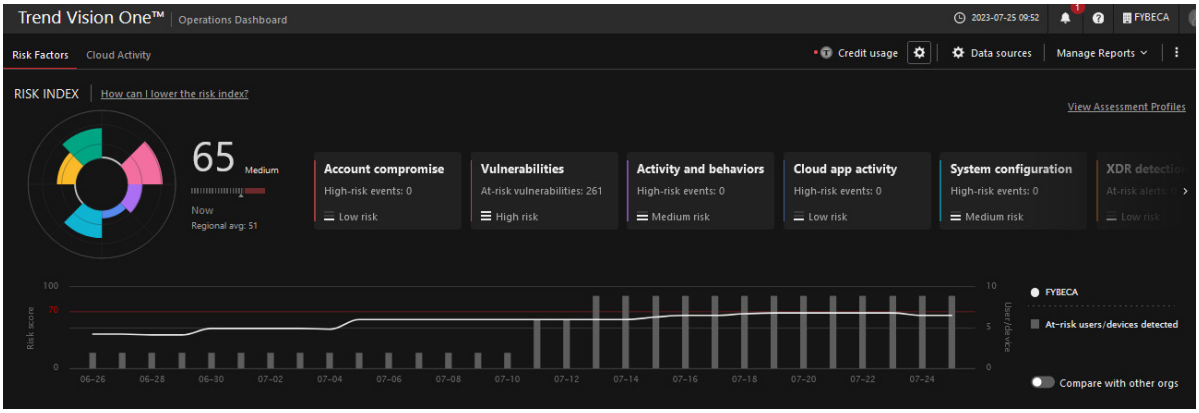


Para una visión más detallada se tienen herramientas que desglosa los datos obtenidos bien sea por cada uno de los servidores o englobando a factores como se muestra en la Figura 40 donde se evalúa lo siguiente:

- Cuentas comprometidas que actualmente tiene un riesgo bajo y ningún evento riesgoso.
- Vulnerabilidades de los servidores con un alto riesgo y alrededor de 261 eventos presentes.
- Actividades y comportamientos de los usuarios que ingresan a los equipos con una nivel de riego medio, pero sin ningún evento importante.
- Actividades que realizan los usuarios en la nube con un riesgo bajo y sin eventos presentes.
- Las configuraciones de los sistemas con un riesgo bajo.

Figura 40

Factores de riesgo detallados



A continuación, se detalla las cosas que toma en cuenta cada uno de los factores de riesgo.

El factor account compromise o compromiso de cuenta se identifica diversos aspectos clave relacionados con la seguridad y el riesgo en línea. Entre ellos se encuentra la detección de cuentas filtradas, que indica la presencia de usuarios cuyas cuentas han sido comprometidas y aparecen en la dark web. También se presta atención a la actividad sospechosa del usuario, la cual puede revelar intenciones maliciosas cuando se observa una actividad anómala creada intencionalmente. Asimismo, se considera las cuentas de usuario objetivo, aquellas que presentaron actividades anómalas de alto riesgo o que fueron específicamente objetivo de campañas de correo electrónico maliciosas.

El factor vulnerabilities o vulnerabilidades realizar detecciones exhaustivas de vulnerabilidades para sistemas operativos como a aplicaciones instaladas. Se identifican vulnerabilidades explotables en el sistema operativo, lo que indica posibles debilidades y puntos de acceso susceptibles a ataques. Además, también se encuentran vulnerabilidades en las aplicaciones instaladas, las cuales podrían ser aprovechadas por atacantes para comprometer el punto final. Estos hallazgos resaltan la importancia de implementar medidas de parcheo y

actualización periódicas para mantener un nivel óptimo de seguridad y protección en el entorno informático.

El factor Activity and Behaviors o actividad y comportamientos examinan la actividad de la red en busca de comportamientos anómalos o maliciosos que podrían indicar posibles amenazas. También se presta atención a la actividad de almacenamiento en la nube, como OneDrive, SharePoint, Outlook entre otros; para descubrir cuentas cuyo uso difiere significativamente del patrón normal de otras cuentas en la empresa. Además, se analiza detalladamente las preferencias y patrones de comportamiento de los usuarios y los dispositivos para detectar actividades inusuales, lo que resulta crucial para detectar posibles brechas de seguridad o actividades sospechosas.

El factor Cloud App Activity o actividad de la aplicación en la nube es un indicador crítico que evalúa se basa en datos históricos de la aplicación, así como en el análisis de sus funciones de seguridad conocidas y el conocimiento compartido por la comunidad. Mediante este proceso de evaluación integral, se determina la confiabilidad y la potencial presencia de riesgos asociados a las aplicaciones, permitiendo tomar decisiones informadas para garantizar la seguridad y protección en el entorno en la nube.

Resultados del índice de riesgo

La consola Trend Vision One que utiliza el XDR permite obtener información más detallada sobre el índice de riesgo en cada uno de los dispositivos, los factores que afectan la seguridad de este y también algunas medidas para reducir este índice.

De la información obtenida de la consola se clasifico el índice de riesgo de los diferentes sistemas operativos de Windows Server y distribuciones de Linux en la Tabla 4 donde todos los equipos están en un nivel medio cercano al 65% del índice de todo el sistema de ciberseguridad.

Tabla 4

Promedio de índice de riesgo por sistemas operativos

Sistema Operativo	Promedio de índice de riesgo
CentOS 6 (64 bit)	**62**
CentOS 7 (64 bit)	**69**
Microsoft Windows Server 2003 (32 bit)	**63**
Microsoft Windows Server 2008 R2 (64 bit)	**64**
Microsoft Windows Server 2012 R2 (64 bit)	**64**
Microsoft Windows Server 2016 (64 bit)	**65**
Microsoft Windows Server 2019 (64 bit)	**65**
Oracle Linux Release 6 (64 bit)	**62**
Oracle Linux Release 7 (64 bit)	**61**
Red Hat Enterprise 5 (32 bit)	**60**
Ubuntu Linux 20 (64 bit)	**51**

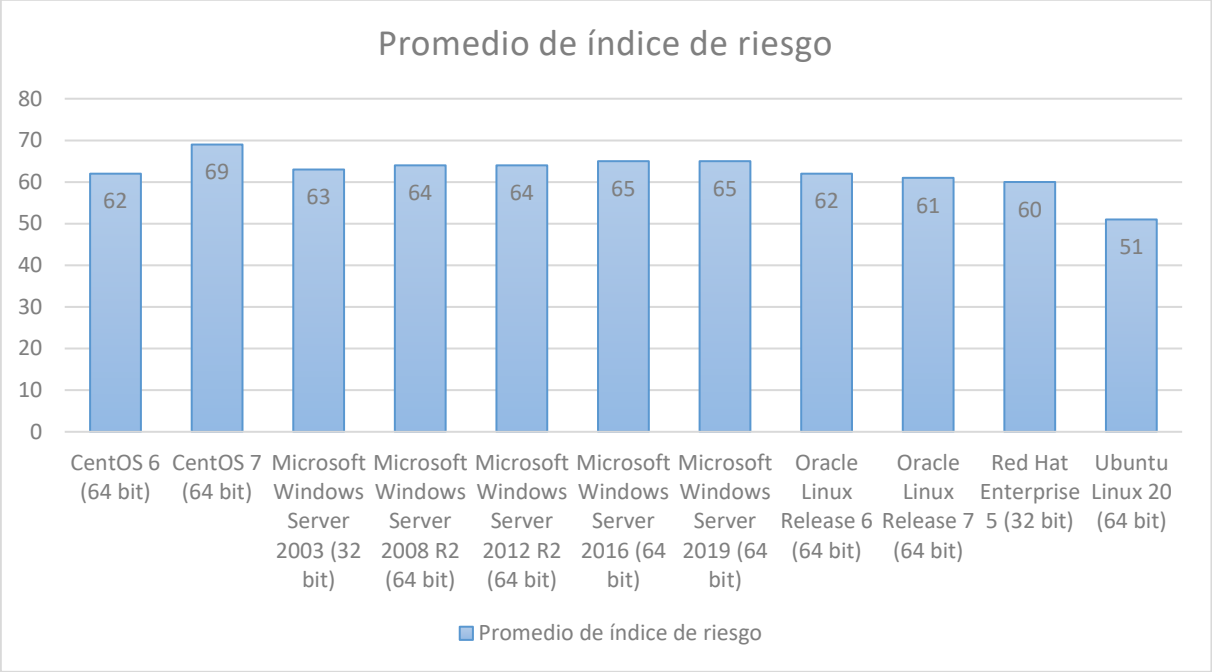
En la Figura 41 se muestra un gráfico de barras sobre el promedio de los índices de riesgo donde se observa que el sistema operativo con menor índice son los cuatro equipos que funcionan bajo el sistema operativo Ubuntu Linux 20 (64 bit).

El índice de riesgo es similar para todas las versiones de Windows Server, pero las medidas que se deben tomar para la reducción de este son diferentes ya que algunos de ellos ya no tienen soporte de fábrica.

Estos datos pueden irse modificando, esperando una tendencia a la reducción del índice con el paso del tiempo y la continuidad del funcionamiento de ciberseguridad.

Figura 41

Promedio de índice de riesgo



Otra información relevante es la exposición de los sistemas operativos a vulnerabilidades y exposiciones comunes (CVEs) altamente explotables, lo que sería un peligro constante que podría poner en riesgo el funcionamiento de este, en la Tabla 5 se detalla los SO con más CVEs explotables siendo el Microsoft Windows Server 2019 y 2016 los más expuestos que requieren una actualización de sus parches de seguridad. El CentOS 7 tiene un año más de soporte por lo que también es posible su actualización con mayor facilidad.

Los datos de la Tabla 5 pueden ir variando ya que con la continuidad del funcionamiento del sistema de ciberseguridad y el funcionamiento de sistema IPS reducirá e informará sobre las vulnerabilidades de los agentes de Deep Security.

Tabla 5

SO con vulnerabilidades y exposiciones comunes altamente explotables

Sistemas operativos	CVEs altamente explotables
CentOS 7	358
Microsoft Windows Server 2016	344
Microsoft Windows Server 2019	446
Total	1148

Medidas de prevención

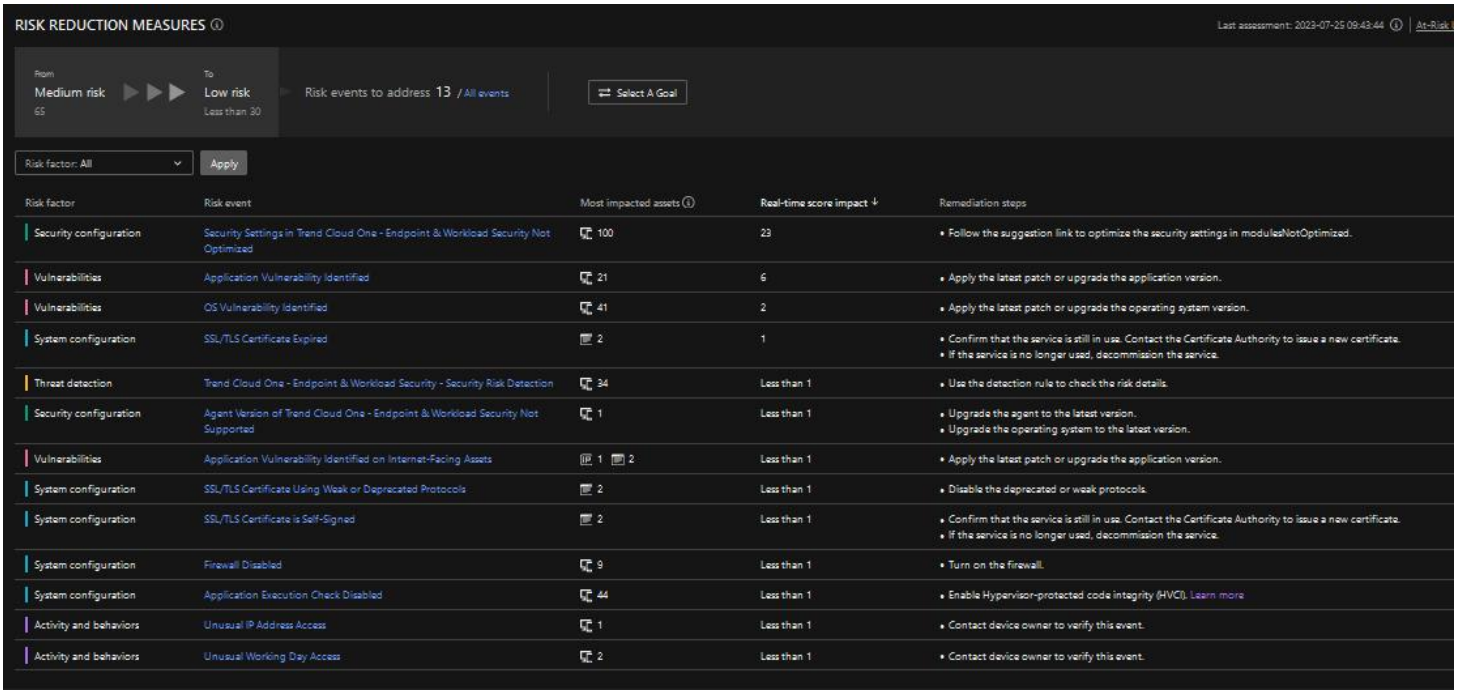
El sistema brinda recomendaciones para la remediación de vulnerabilidades y problemas detectados en los equipos lo que posibilita el ajuste automáticamente del índice de riesgo en función de los eventos registrados.

Por ejemplo, se sugiere aplicar los parches más recientes o actualizar el sistema operativo cuando se detecten eventos de riesgo relacionados con vulnerabilidades. Dado que las evaluaciones de vulnerabilidades se llevan a cabo diariamente, las acciones de reparación tomadas hoy no afectarán el cálculo del índice de riesgo para el día siguiente. De esta manera, se logra mantener un nivel óptimo de seguridad y mitigar potenciales riesgos, garantizando un ambiente más seguro y protegido en todo momento.

En la Figura 43 se muestran trece medidas que permitían pasar de un índice de riesgo medio del 65% a un índice bajo inferior al 30% y se puede observar los equipos que serán afectado. Con esto se tomarían acciones respecto a la configuración de seguridad de los equipos, combatir vulnerabilidades con actualizaciones de sistema operativo, detección de amenazas y la revisión de actividades y comportamientos de los usuarios que se conectan.

Figura 42

Medidas para reducción de riesgo



Las medidas para reducir el riesgo que tendrán mayor impacto consiste principalmente en actualización del sistema operativo de los servidores y también actualizar las aplicaciones que se utilizan, aunque esto requiere una planificación con las diferentes áreas.

Para reducir cerca de un 23% el índice de riesgo es necesario tomar medidas en los cien servidores siguiendo las recomendaciones que se detallan en cada uno, que principalmente mostrarán vulnerabilidades a las que está expuesto y como solucionarlas.

ROI

De último reporte sobre el costo de un informe de violación de datos de (IBM, 2023) se abstrae que las empresas que incorporan herramientas de ciberseguridad ahorran en promedio 1.76 millones de dólares, partiendo de este valor se calcula el retorno de la inversión con el costo de las licencias compradas a Trend Micro por las dos consolas que conforman el sistema de ciberseguridad implementado.

Para lo cual se adaptará la siguiente fórmula para el cálculo.

$$ROI = \frac{Beneficios - Costos}{Costos} \times 100\%$$

$$ROI = \frac{1\,760\,000 - 51\,134}{51\,134} \times 100\%$$

$$ROI = 33.42 \times 100\%$$

$$\boldsymbol{ROI = 3342\%}$$

El ROI obtenido del 3342% implica que la inversión de los servicios Cloud One Workload Security y Vision One XDR de Trend Micro como medida de seguridad informática han generado un retorno significativo en términos de reducción de pérdidas financieras relacionadas a un posible ahorro en caso de una violación de datos según el reporte de IBM.

Una alta tasa de retorno en ciberseguridad podría deberse a factores como prevención de ataques, reducción de costos de recuperación, protección de la reputación y cumplimiento normativo:

Capítulo V. Conclusiones y recomendaciones

Conclusiones

La implementación del sistema de ciberseguridad en los servidores del Data Center de la Corporación GPF, abarcando tanto los entornos on premise locales como cloud, se realizó con éxito y representa una medida esencial para salvaguardar la infraestructura informática contra amenazas y vulnerabilidades conocidas y desconocidas. Al utilizar las soluciones Cloud One Workload Security y Vision One XDR de Trend Micro, la organización se dota de herramientas que permiten una protección integral contra las crecientes y sofisticadas ciberamenazas del entorno digital actual y actualmente el 100 % de los agentes de Deep Security instalados se comunican correctamente y reportan la información adecuada para el funcionamiento del sistema.

El análisis de los parámetros de criticidad de los servidores se vuelve fundamental para garantizar una efectiva utilización de las 101 licencias del agente del sistema de ciberseguridad. De acuerdo con los datos obtenidos, se ha determinado que el 64% de los servidores seleccionados funcionan bajo Microsoft Windows Server en diversas versiones, mientras que el 36% restante opera con Linux en distintas distribuciones. Este enfoque de análisis permite una optimización en el despliegue de recursos de seguridad, asegurando una protección adecuada de los servidores más críticos y maximizando la seguridad de la infraestructura informática de la organización. Es importante destacar que el 40% de los servidores posee una criticidad alta o media, mientras que el 20% restante tiene una criticidad baja, lo que sugiere posibles modificaciones en las licencias de agentes para aquellos servidores con criticidad baja.

Los módulos del sistema de ciberseguridad que se implementan en los agentes Deep Security resultan fundamentales para garantizar un correcto funcionamiento del sistema y constituyen los recursos necesarios para habilitar la detección y respuesta extendidas (XDR). El

más importante es referente al sistema de prevención de intrusiones, IPS, para la implementación del virtual patching en los diferentes servidores y el monitoreo de actividades permite la implementación adecuada de la tecnología XDR para tener una visión integral y unificada de los eventos de seguridad en toda la infraestructura, facilitando la identificación de patrones y amenazas emergentes para una protección más proactiva y eficiente.

La definición y asignación de políticas de seguridad, así como la creación de directivas que se adaptan automáticamente a cada sistema operativo del servidor y juegan un papel fundamental en el fortalecimiento de la seguridad de la organización. Esta estrategia proactiva garantiza una respuesta más rápida y efectiva ante incidentes de seguridad, asegurando la integridad y confidencialidad de los datos.

Para mantener un control periódico sobre el estado de los agentes de los equipos, se generan reportes programados de manera semanal. Estos informes permiten revisar tanto el estado general como en detalle de los servidores, además de proporcionar una visión de los eventos relacionados con el sistema de prevención contra intrusos y un resumen de todas las incidencias detectadas en los distintos módulos. Esta práctica de generación de informes brinda una panorámica completa y actualizada del entorno de seguridad, facilitando la toma de decisiones informadas y la adopción de medidas preventivas y correctivas oportunas.

La implementación exitosa del Service Gateway en un servidor virtualizado sobre VMware y su integración con la consola del sistema de ciberseguridad garantiza una protección efectiva de la red local al ser un intermediario con los productos de Trend Micro Vision One; mediante esta se dispone de servicios vitales como la sincronización de listas de objetos sospechosos para los productos locales de Trend Micro, el servicio de protección inteligente que revisa la reputación de archivos y sitios web y finalmente la actualización de los servicios.

La evaluación de la efectividad de la solución de ciberseguridad y el notable ROI del 3342% en caso de sufrir una vulneración a su información evidencian una decisión acertada por parte de la Corporación al invertir en medidas de protección digital con los servicios de Cloud One Workload Security y Vision One XDR de Trend Micro. La implementación de la herramienta ha demostrado ser efectiva en la mitigación de vulnerabilidades y la prevención de posibles amenazas cibernéticas.

La herramienta brinda información acerca del riesgo presente en los servidores con los agentes de Deep Security que ronda el 65%, que sería un punto de partida para mejorar la seguridad de estos, algunos de los sistemas operativos que están más expuestos son Microsoft Windows Server 2019 y 2016 como la distribución de Linux CentOS 7 los cuales requieren atención por presentar 1148 CVEs.

El manual de usuario dirigido al área de infraestructura está enfocado en el correcto uso y configuración del sistema de ciberseguridad, será una herramienta invaluable para fortalecer la seguridad de la organización al asegurar que los usuarios tengan el conocimiento y las pautas necesarias para utilizar eficientemente el sistema; este se encuentra adjunto en la sección de apéndice.

Recomendaciones

Para garantizar la seguridad y eficiencia de las operaciones, es fundamental llevar a cabo dos acciones clave. En primer lugar, depurar de manera periódica la lista de usuarios que tienen acceso a la consola, así como revisar y mantener actualizado el directorio de contactos para alertas y reportes. Esto asegurará que solo el personal autorizado tenga acceso a información confidencial y mantener un flujo de comunicación efectivo ante posibles incidentes.

En segundo lugar, realizar una validación exhaustiva de los accesos a la plataforma de Vision One, que se utiliza para administrar el XDR. Al verificar y controlar quiénes acceden a esta herramienta, se fortalece la defensa contra amenazas cibernéticas para garantizar que solo aquellos con los permisos adecuados puedan gestionar la solución de detección y respuesta ante incidentes.

Es altamente recomendable que se lleve a cabo una investigación extendida sobre el resto de las funcionalidades disponibles en la herramienta. A menudo, las soluciones tecnológicas ofrecen una amplia gama de características y capacidades que pueden no ser evidentes a primera vista. Al profundizar en la exploración de todas las funcionalidades, es posible descubrir recursos adicionales que podrían potenciar significativamente la eficiencia y productividad. Esta investigación permitirá aprovechar al máximo la herramienta, optimizando su uso y obteniendo el máximo valor de la inversión realizada.

Referencias

ABRIE, A. (8 de Abril de 2020). *Software on-premise y software en la nube*. ICM: https://www.icm.es/2020/04/08/software-on-premise-y-software-en-la-nube/#:~:text=%C2%BFQu%C3%A9%20es%20el%20software%20on-premise%3F%20A%20diferencia%20del,la%20configuraci%C3%B3n%2C%20manejo%20y%20seguridad%20de%20los%20datos.

Amazon Web Services, Inc. (2023). *¿Qué es el SaaS? - Explicación del software como servicio*. Amazon Web Services: https://aws.amazon.com/es/what-is/saas/#:~:text=para%20crear%20SaaS%3F-,%C2%BFQu%C3%A9%20es%20SaaS%3F,acceder%20a%20ellos%20bajo%20demanda.

Atlassian. (2023). *¿Qué es la computación en la nube? Visión general de la nube*. Atlassian: https://www.atlassian.com/es/microservices/cloud-computing

Check Point Software ES. (26 de Julio de 2021). *¿Qué es un sistema de prevención de intrusos (IPS)?* Check Point Software ES: https://www.checkpoint.com/es/cyber-hub/what-is-ips/

Cisco Systems. (Enero de 2023). *Cisco Threat Response Overview*. Cisco: https://www.cisco.com/c/es_mx/products/security/what-is-it-security.html#:~:text=La%20seguridad%20de%20TI%20es%20un%20conjunto%20de,confidencial%2C%20y%20bloquea%20el%20acceso%20a%20hackers%20sofisticados.

CorporacionGPF. (22 de Noviembre de 2021). *La Corporación - CorporacionGPF*. CorporacionGPF: https://www.corporaciongpf.com/la-corporacion/#Organigrama

Duan, X., Liu, S., y Gu, L. (2020). Research and application of server security protection based on virtual patch. *International Conference on Information Science, Parallel and Distributed Systems (ISPDS)*, 52-55. https://doi.org/10.1109/ispds51347.2020.00018

Equipo Ekon. (13 de Septiembre de 2021). *On Premise vs. Cloud*. Ekon: https://www.ekon.es/blog/on-premise-vs-cloud-que-es-mejor/

FEMSA. (10 de Julio de 2023). *Quiénes Somos - FEMSA*. FEMSA: https://www.femsa.com/es/acerca-de-femsa/quienes-somos/

Genge, B., Graur, F., y Enăchescu, C. (2015). Non-intrusive techniques for vulnerability assessment of services in distributed systems. *Procedia Technology, 19*, 12-19. https://doi.org/10.1016/j.protcy.2015.02.003

IBM. (2020). *¿Qué es la ciberseguridad?* . ibm.com: https://www.ibm.com/es-es/topics/cybersecurity

IBM. (2023). *Cost of a data breach 2023*. Ibm.com: https://www.ibm.com/reports/data-breach

IBM. (2023). *What is IT Infrastructure?* Ibm.com: https://www.ibm.com/topics/infrastructure

IT ahora - La Revista del Líder de Tecnología . (1 de Julio de 2022). *Corporación GPF trabaja estratégicamente en la eficiencia de la cadena de valor*. IT ahora - La Revista del Líder de Tecnología : https://itahora.com/2020/07/01/corporacion-gpf-trabaja-estrategicamente-en-la-eficiencia-de-la-cadena-de-valor/

Manufacturing Enterprise Solutions Association | MESA International. (15 de Julio de 2022). History of the MESA Models: https://mesa.org/topics-resources/mesa-model/history-of-the-mesa-models/

NextU . (9 de Septiembre de 2022). *Computación en la nube*. Blog | NextU LATAM: https://www.nextu.com/blog/computacion-en-la-nube-rc22/#:~:text=Las%20caracter%C3%ADsticas%20de%20la%20computaci%C3%B3n%20en%20la%20nube,elasticidad%20...%205%205.%20Medici%C3%B3n%20de%20servicios%20

Oracle España. (2020). *¿Qué es un WAF? Definición de un Web Application Firewall*. Oracle.com: https://www.oracle.com/es/database/security/que-es-un-waf.html

RedHat. (2019). *What is IT infrastructure?* Redhat.com: https://www.redhat.com/en/topics/cloud-computing/what-is-it-infrastructure

Shaji, E., y Subramanian, N. (2021). Assessing Non-Intrusive Vulnerability Scanning methodologies for detecting web application vulnerabilities on large scale. *2021 International Conference on System, Computation, Automation and Networking (ICSCAN)*. https://doi.org/10.1109/icscan53069.2021.9526423

TIC Portal. (5 de Diciembre de 2022). *¿Qué es un servidor, cómo funciona y qué tipos hay?* TIC Portal: https://www.ticportal.es/glosario-tic/servidores

Trend Micro. (2023). *About the Workload Security protection modules - Workload Security*. Trend Micro Cloud One™ Documentation: https://cloudone.trendmicro.com/docs/workload-security/protection-modules/#Device

Trend Micro. (2023). *Trend Micro Vision One - Service Gateway Overview*. Online Help Center Trend Micro: https://docs.trendmicro.com/en-us/enterprise/trend-micro-xdr-help/ServiceGatewayOverview

Trend Micro. (2023). *What Is XDR?* Trend Micro: https://www.trendmicro.com/en_us/what-is/xdr.html

Trend Micro Cloud One™ Documentation. (2023). *About the Workload Security components - Workload Security*. Trendmicro.com: https://cloudone.trendmicro.com/docs/workload-security/components/

Trend Micro ES. (2021). *Security 101: Virtual Patching*. Trendmicro.com: https://www.trendmicro.com/vinfo/es/security/news/security-technology/security-101-virtual-patching#:~:text=Virtual%20patching%20%E2%80%94%20or%20vulnerability%20shielding%20%E2%80%94%20acts,taking%20network%20paths%20to%20and%20from%20a%20vulnerability.

Trend Micro Incorporated. (2023). *Create policies - Workload Security*. Trend Micro Cloud One™ Documentation: https://cloudone.trendmicro.com/docs/workload-security/policy-create/

Trend Micro Incorporated. (2023). *Service Gateway Overview*. Online Help Center: https://docs.trendmicro.com/en-us/enterprise/trend-micro-xdr-help/ServiceGatewayOverview

Trend Micro Incorporated. (2023). *System requirements - Workload Security*. Trend Micro Cloud One™ Documentation: https://cloudone.trendmicro.com/docs/workload-security/system-requirements/#trend-micro-cloud-one-console-requirements

TrendMicro. (2023). *TrendMicro*. trendmicro.com: https://www.trendmicro.com/en_us/forHome.html

VMware. (15 de Junio de 2021). *Virtualization Technology & Virtual Machine Software: What is Virtualization?* VMware: https://www.vmware.com/es/solutions/virtualization.html

Apéndice