

FORTINET®

Fortinet Customer Experience (FCE)

Análisis de ciberseguridad por especialistas

Detalles del beneficio

Año: 2020



Índice

Acerca de Fortinet..... 3

Fortinet Customer Experience (FCE)..... 3

Campo de Acción 4

Detalles del proceso 6

Estructura Básica del reporte entregado..... 7

Confidencialidad.....8

Acerca de Fortinet

Producto de la innovación Fortinet (FTNT) nace en el año 2000 desarrollando equipamiento específico dedicado a mitigar los problemas de seguridad de red y desde entonces se ha posicionado como una de las empresas líderes, siendo hoy reconocida como la marca número 1 en despliegue de soluciones de ciberseguridad.



Recomendada mundialmente por los principales analistas, con más de 455.000 clientes a nivel mundial y 30 líneas de soluciones, Fortinet aprovecha su experiencia y recursos enfocado en entregar mejores soluciones y servicios día a día.

Fortinet Customer Experience (FCE)

Como su nombre lo indica, FCE es una iniciativa de la marca que tiene como objetivo ofrecer una experiencia diferente, otorgando un beneficio único que le permite a sus mayores clientes disponer de un especialista calificado que lo asesore en mejores prácticas de ciberseguridad. Como resultado de dicho análisis se entregarán una serie de recomendaciones que permitirán optimizar el uso de las diferentes soluciones de red y ciberseguridad del cliente, así como también analizar métricas referentes al nivel de exposición a amenazas más comunes.

Alcance

El beneficio cubre dos tipos de necesidades:

- Análisis de red y mejores prácticas
- Exposición a amenazas de ciberseguridad

Análisis de red y mejores prácticas: El especialista se concentrará en las diferentes soluciones desplegadas en la red (foco en los productos Fortinet), atendiendo a los detalles de configuración, versiones, topología, etc. Como resultado se entregará un completo informe con recomendaciones, sugerencias, ajustes, propuestas de mejora y optimización de recursos.

Exposición a amenazas de ciberseguridad: El especialista se concentrará en este punto en las soluciones y arquitecturas requeridas para mitigar el campo de acción de diferentes flagelos informáticos como ser el Malware, DDoS, Phishing, etc.. Como resultado se entregará un completo análisis con ponderación de nivel de exposición, recomendaciones y sugerencias enfocadas a mitigar las diferentes amenazas, basado en un modelo de maduración NIST.

Especialistas Asignados: Para las mencionadas tareas Fortinet pondrá a disposición a sus equipos técnicos de ingeniería y arquitectura de soluciones. En función del cliente y de la especialización requerida, el técnico asignado podrá variar, por lo que se informará en cada caso, el nombre del responsable a asignar, su rol, formación y experiencia en ciberseguridad.

Campo de Acción

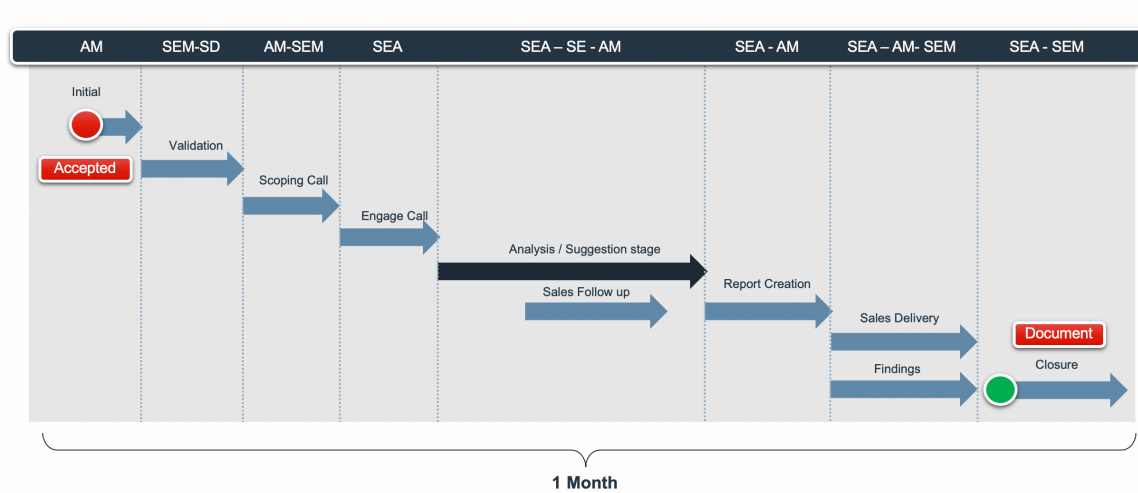
El proceso de relevamiento será del tipo remoto, el equipo de especialistas asignado se contactará con el cliente a fin de relevar las necesidades iniciales y comenzar con el análisis. Para dicho proceso, se intercambiará información en formato cuestionario y se estipularán diferentes reuniones en la cuales los responsables irán despejando dudas y recopilando diferentes datos. Las reuniones serán programadas con antelación y durarán un tiempo variable en función del tamaño del cliente y alcance del servicio a entregar.

El proceso de relevamiento puede variar en función del beneficio asignado. Para el caso de exposición al ransomware, los ítems a analizar se concentran en lo siguiente:

Item	Descripción
Acceso Remoto	Evaluaremos potenciales usuarios vulnerables y su proceso de conexión a redes corporativas. Tipo de VPN utilizadas, portales SSL o RDP, tipo y mecanismos de autenticación utilizados, control de postura y remediación de endpoints vulnerados.
Correo electrónico	Mas del 90% de los ataques de ransomware utilizan el correo electrónico como mecanismo de contagio. Evaluaremos detenidamente las soluciones AntiSPAM, tipo y sistemas de correo electrónico, protección activa de phishing y filtrado de contenido embebido.
Flujos de información	La información distribuida puede ser un problema grave a la hora de enfrentar y controlar el malware. Analizaremos detalles de dominio, autenticación, repositorios y sistemas centrales de información, tanto locales como en nube. Para este último caso evaluaremos controles específicos (shadow IT).
Controles Avanzados	El ransomware opera silenciosamente, pero muestra señales que son importantes detectar a tiempo para mitigar la amenaza antes de que sea demasiado tarde. Evaluaremos controles disponibles en la red para detectar anomalías conocidas y ataques de día cero. Analizaremos el alcance de la inspección profunda y cifrada en soluciones tales como NGFW, IPS, Sistemas de inteligencia artificial, NGAV, Sandbox, EDR, DNS filter, endpoint control, etc.
Segmentación	A fin de detener el movimiento lateral por el cual el malware se propaga, buscaremos barreras internas conocidas como firewall de segmentación (ISFW) y analizaremos su rol en la micro-segmentación.
Entrenamiento	El contagio utiliza en un 90% de los casos el engaño a usuarios finales. Los mecanismos de control no siempre son eficaces por lo cual es importante capacitar y formar al personal en materia de ciberseguridad. Evaluaremos el conocimiento general de los usuarios sobre SPAM y phishing. Analizaremos herramientas, frecuencias y mecanismos de capacitación utilizados.
Hardening	En pos del funcionamiento inmediato, los ajustes de configuraciones relativas a ciberseguridad son muchas veces ignorados lo que produce puertas de entrada a numerosos ataques. Consultaremos sobre el nivel de parchado de activos críticos, analizaremos el manejo de usuarios de administración, política de contraseñas, timeout de sesiones, etc.
Contingencia	Ante la imposibilidad de detener un posible ataque, analizaremos los planes de acción y remediación.

Detalles del proceso

La tarea contempla numerosas etapas que comienzan con el comunicado formal del beneficio al cliente final y finalizan con la entrega del informe. A continuación, se detallan cada uno de sus pasos.



Initial: A fin de evaluar el interés, los clientes proclives al beneficio serán contactados e informados de dicho beneficio.

Validation: Si el cliente está de acuerdo en avanzar con el análisis, se designará un equipo de trabajo y se recopilará información sobre las necesidades básicas a cubrir.

Scoping Call: En este punto el equipo asignado (AM/SEM/SD) se comunicará con el cliente a fin de definir los alcances de la tarea y los interlocutores técnicos válidos para realizarla.

Engage Call: El ingeniero a cargo (SE/SEA) se contactará con los técnicos responsables para así comenzar con el trabajo.

Analysis: El ingeniero a cargo comenzará su tarea de relevamiento e investigación, dialogará con el equipo técnico del cliente y con sus contrapartes de ingeniería (SE) con el objetivo de obtener un detalle completo de la red, historia, problemáticas y necesidades del cliente.

Report Creation: El ingeniero a cargo trabajará en la creación del reporte final con sugerencias, recomendaciones de mejora, matrices de ponderación y exposición a diferentes amenazas.

Report Delivery: El equipo de trabajo sostendrá una reunión de presentación del informe con todos los responsables del cliente.

Closure: Se analizarán los resultados finales y se entregarán las últimas recomendaciones y el informe completo.

NOTAS:

- Dependiendo del tipo de beneficio, las tareas pueden demorar entre 7 y 30 días.
- La duración de las tareas está sujeta; entre otras cosas, a la disponibilidad del cliente.
- Nomenclatura, Fortinet: AM (ejecutivo de cuentas), SEM (Manager de ingeniería), SD (Director de ventas), SE (Ingeniero especialista), SEA (Ingeniero Arquitecto)

Estructura Básica del reporte entregado

La iniciativa FCE ofrece un completo reporte final que contiene en líneas generales la siguiente información:

- Detalles de FCE y del especialista SEA asignado
- Plan de trabajo
- Minutas y resúmenes de las reuniones sostenidas
- Análisis de red (tecnologías actuales y sugeridas)
- Puntos de mejora (reconfiguración y ajustes)
- Análisis gráfico de riesgo basado en NIST
- Propuesta de solución integral
- Planes de acción
- Próximos pasos
- Anexos e información adicional

A continuación, se muestran algunas imágenes del mencionado reporte y presentaciones al cliente:

FORTINET Análisis de Solución y Mejores Prácticas

Análisis Inicial

Para definir una estrategia de seguridad, con recomendaciones de cliente, se identificaron 3 puntos a analizar:

- Tecnologías Actuales:** Son las soluciones que posee actual implementadas y operando en su red. Si bien sobre muchas de alcance claro de funciones implementadas y licenciamiento así interpretar el valor intrínseco que debería proveer las mismas y pueden asumir ciertas funciones. Sobre dichas soluciones, se plantearán posibles escenarios de mayor valor posible.
- Tecnologías Necesarias:** Son diferentes soluciones que, si permiten completar una arquitectura de seguridad que abarque riesgos que una organización como "Transener" puede afrontar.
- Objetivo Deseado:** Es el objetivo que el cliente expuso explícito con la adición de algunos valores adicionales que creemos que fundamentales en la construcción de una arquitectura de seguridad.

Tecnologías Actuales	<ul style="list-style-type: none"> NAC WAF SIEM AAA (RADIUS) VPN Control de Acceso Routing Firewalling
Tecnologías Necesarias	<ul style="list-style-type: none"> SIEM Seguridad externa OT EDR/DR Control de Navegación CASB Seguridad de Correo SOA
Objetivo deseado	<ul style="list-style-type: none"> Integración sencilla Reducción de consolas Respuesta ante incidentes

www.fortinet.com

FORTINET Análisis de Solución y Mejores Prácticas

Plan de acción a corto plazo

Dentro del escenario de solución a corto plazo, se recomiendan 4 medidas concretas que fueron desarrolladas teniendo en cuenta: el riesgo, la facilidad de implementación, la eficiencia y la reducción del costo operativo.

Configuración de SSL Deep Inspection

Como primera medida, se analizó la forma en que FortiGate que están desplegados.

A simple vista se observan mejoras de configuraciones aplicables según prácticas, pero en particular hay un punto que es crítico y conlleva un riesgo muy grande: la inspección de tráfico cifrado.

Dado que contamos con las herramientas, se solicitó a Druclis que realice el "CyberTreat Analysis" con el FortiManager, que ampe los siguientes:

www.fortinet.com

FORTINET Análisis de Solución y Mejores Prácticas

Se asume que hay un control sobre la navegación de los usuarios mediante la tecnología de Cisco Umbrella (análisis de DNS requests), que permite hacer un control granular sobre la navegación a internet. Sin embargo, este escenario, no es completo, ya que una vez analizado el request (al momento de una sesión), resto queda totalmente invisible a los motores de AntiMalware, DLP e IPS, los cuales solo trabajarán en el porcentaje indicado como HTTP (menos del 5% del tráfico HTTP).

Beneficios:

La inspección de tráfico cifrado es algo para lo que los FortiGate están diseñados y tienen procesadores específicos que permiten realizar dicha tarea sin afectar el rendimiento de la solución. Dentro de los beneficios de inspeccionar el tráfico podemos mencionar:

- Detección y bloqueo de Malware antes de que acceda al perímetro de la red
- Detección y bloqueo de Malware de Día 0 mediante Sandboxing en la nube
- Remoción de contenido explotable en documentos (Content Disarm and Reconstruction)
- Identificación de acciones dentro de las aplicaciones, no solo acceso. Ejemplo: No solo ver que se accede a aShare, sino también ver que acciones ocurren dentro del sitio.

www.fortinet.com

Análisis de soluciones del cliente

Beneficios de implementar la recomendación

FORTINET Análisis de Solución y Mejores Prácticas

Incluso en etapas posteriores de la arquitectura de seguridad, se podría automatizar el flujo de reporting de correo malicioso o sospechoso, junto con herramientas de Threat Hunting logrando eliminar procesos manuales recurrentes para seguridad con proceso automatizado.

Sobre este punto podemos mencionar un reporte de SE Labs reciente que indica nivel de seguridad ofrecido por las diferentes soluciones.

[SE Labs - Email Security Services Protection](#)

Tenemos una herramienta de análisis llamada CTAP, que puede ayudarnos a medir en qué situación están con respecto a la seguridad de correo y que es la aplicación sobre la plataforma productiva.

[Reporte CTAP Ejemplo](#)

Seguridad en el Endpoint

Según la información provista por el cliente durante la llamada de relevamiento en proceso de análisis sobre la solución de Endpoint.

Por un lado, tienen implementado Trend Micro y siguiendo la estrategia de un proveedor de seguridad, lo lógico sería apuntar a soluciones de Cisco y que son los que más presencia tienen en la red.

Dicho esto, y habiendo analizado el ambiente de Transener, la solución más adecuada para la protección del Endpoint de Fortinet es FortiEDR.

PRE-INFECTION	POST-INFECTION
<ul style="list-style-type: none"> Detectar & Predecir Prevent 	<ul style="list-style-type: none"> Detect Defuse Respond & Investigate Remediate

¿Por qué no ofrecer FortiClient?

- FortiClient cumple un rol fundamental en la aplicación de políticas de seguridad base al estado de cumplimiento. Sin embargo, este rol puede ser tomado por la integración de ISE con FortiManager, por lo que sería un control redundante.
- La propia solución de FortiEDR, ofrece todo un set de herramientas de protección como AntiMalware basado en ML, protección anti Ransomware, protección contra ataques fileless, que pueden solaparse eventualmente con funciones de AntiMalware del propio FortiClient.
- No cuenta con herramientas integradas de Analisis Forense y respuesta.

www.fortinet.com

FORTINET Análisis de Solución y Mejores Prácticas

- Detección y bloqueo de amenazas a las aplicaciones de tipo cliente con el IPS (~3500 protecciones)
- Detección y bloqueo de botnets por medio de patrones de tráfico (No exclusivamente por motores DNS)

Complejidad: Media - Este tipo de inspección puede afectar al tráfico regular, por lo que la inspección profunda debe ser aplicada gradualmente y con excepciones en las categorías críticas, para reducir la posibilidad de impacto en el cliente final. En términos de licenciamiento, los FortiGate poseen el licenciamiento necesario para aplicar los controles mencionados.

Tareas:

- Configuración de FortiGate para poder inspeccionar el tráfico cifrado.
 - Esta configuración debe aplicarse de forma controlada y en etapas, pudiendo afinar la configuración de forma ordenada y evitar de este modo el impacto en los usuarios finales.
 - Se recomienda aplicación por reglas específicas, que trabajen sobre grupos de usuarios reducidos.
 - Se recomienda utilizar el AD como CA ya que evita que tengamos que desplegar certificados en cada cliente.

Documentación relacionada:

- [Paso 1 - Configurar al FortiGate como CA subordinada al dominio](#)
- [Paso 2 - Repetir el proceso con cada FortiGate donde se requiera análisis de tráfico cifrado](#)
- [Paso 3 - Bloqueo de protocolo QUIC](#)
- [Paso 4 - Configuración de excepciones sobre SSL inspection](#)
- [Video Explicativo](#)

Implementación de una solución de CASB

Indicó durante la reunión de relevamiento que han reducido el uso de las aplicaciones de ofimática locales, pasando a hacer un uso extensivo de las soluciones de ofimática en nube de Google, que además les provee la infraestructura de colaboración. Este tipo de implementaciones requiere en paralelo una solución de seguridad que permita identificar:

- Exfiltración de información confidencial, accidental o consciente
- Propagación de malware
- Cumplimiento de compliance
- Análisis de información en reposo

www.fortinet.com

Sugerencias de automatización y mejora de procesos de detección. Nivel de complejidad de la implementación

Documentación relacionada e información adicional

NOTAS: La estructura del reporte puede variar en función del beneficio asignado.

Confidencialidad:

Las tareas a realizarse se acuerdan exclusivamente entre el cliente, el integrador y Fortinet. En caso de ser requerido se podrá evaluar la firma de un acuerdo de confidencialidad que garantice la no divulgación de la información recopilada. En todos los casos los pormenores de este punto podrán ser evaluados en la reunión inicial de alcance (Scoping call).