Descripción general de la solución

WithSecure™ Elements **Endpoint Detección y Respuesta**

WithSecure™ Elements – Reduce el riesgo cibernético, la complejidad y la ineficiencia

Contenido

DESCARGO DE RESPONSABILIDAD: Este documento brinda una descripción general de alto nivel de los componentes clave de seguridad en la solución WithSecure™ Elements Endpoint Detection and Response. Los detalles se omiten para evitar ataques dirigidos contra nuestras soluciones.

WithSecure™ mejora constantemente sus servicios. WithSecure™ se reserva el derecho de modificar las características o la funcionalidad del Software de acuerdo con las prácticas del ciclo de vida del producto.

Última actualización: Mayo de 2021

1. Resumen Ejecutivo

Los ataques de ciberseguridad dirigidos pueden ser difíciles de analizar y responder, y convertirse en un problema extremadamente costoso para las empresas incluso antes de que se conviertan en violaciones de datos reales. La etapa de remediación del ataque por sí sola puede demorar más de dos meses y costar casi dos millones de dólares.[1]

Los ataques sin archivos no suelen ser reconocidos por la protección antivirus tradicional, y los ataques dirigidos suelen pasar desapercibidos durante meses o incluso años.[2] Con la solución WithSecure™ Elements Endpoint Detection and Response, puede obtener visibilidad contextual de su seguridad, automatizar la identificación de amenazas y detener los ataques. antes de que ocurran violaciones de datos que involucren datos sensibles, confidenciales o protegidos expuestos a una parte no autorizada, como un ciberdelincuente

Flexibilidad para crear ciberseguridad resiliente con WithSecure™ Elements

En el entorno empresarial ágil de hoy, la única constante es el cambio. WithSecure™ Elements ofrece a las empresas seguridad todo en uno que se adapta a los cambios tanto en el negocio como en el panorama de amenazas, creciendo junto con la organización. Ofrece flexibilidad en los modelos de licencia y en sus tecnologías de seguridad de elegir y elegir. WithSecure™ Elements integra una gama completa de componentes de ciberseguridad, incluida la gestión de vulnerabilidades, la gestión de parches, la protección de terminales y la detección y respuesta, en un único paquete de software ligero que se gestiona en una consola de gestión unificada basada en la nube. Con la misma consola, las empresas pueden administrar la seguridad de sus servicios de colaboración de Microsoft 365. La solución está disponible como un servicio de suscripción totalmente administrado a través de nuestros socios certificados o como una solución en la nube autogestionada. Los clientes pueden cambiar fácilmente de un servicio autogestionado a un servicio totalmente gestionado, por lo que las empresas que luchan por encontrar empleados con habilidades en seguridad cibernética pueden permanecer protegidas en medio del panorama de ataques en constante desarrollo.

WithSecure™ Elements consta de cuatro soluciones que se administran todas con la misma consola, WithSecure™ Elements Security Center.

WithSecure™ Elements Endpoint Protection:

Con el ganador múltiple de AV-TEST Best Protection de Secure, la protección de endpoints basada en IA y nativa de la nube se puede implementar instantáneamente desde su navegador y administrar la seguridad de todos sus endpoints, manteniendo a su organización protegida de los ataques. WithSecure™ Elements Endpoint Protection cubre dispositivos móviles, equipos de escritorio, portátiles y servidores.

Detección y respuesta de terminales WithSecure™ Elements:

Obtenga una visibilidad completa de las amenazas avanzadas con nuestra detección y respuesta para endpoints. Con nuestra exclusiva Detección de contexto amplio, puede minimizar el ruido de las alertas y centrarse en los incidentes, y con la respuesta automatizada puede detener las infracciones de manera eficaz las 24 horas del día. Con Elementos Secure ™. Endpoint Detection and Response cubre equipos de escritorio, portátiles y servidores.

WithSecure™ Elements Vulnerability Management:

Descubra y administre vulnerabilidades críticas en su red y activos. Al exponer, priorizar y parchear automáticamente las vulnerabilidades, puede reducir su superficie de ataque y minimizar los puntos de entrada para los atacantes.

WithSecure™ Elements Collaboration Protection:

Complemente las capacidades nativas de seguridad de correo electrónico de Microsoft 365 ción fácil de implementar y administrar. proporcionando seguridad avanzada para evitar ataques a través de correo electrónico y URL. La integración de nube a nube hace que la solución sea fácil de implementar y administrar.

WithSecure™ Elements Endpoint Protection, Endpoint Detection and Response y Vulnerability Management se empaquetan en un único paquete de software actualizado automáticamente, lo que le permite ahorrar tiempo y dinero en la implementación y administración del software.

Beneficios de las soluciones integradas

La solución modular WithSecure™ Elements se adapta a las necesidades cambiantes de su empresa. La seguridad cibernética unificada significa licencias más sencillas, menos tareas de administración de seguridad y más productividad sin sacrificar la postura de seguridad cibernética de su empresa. La consola basada en la nube, WithSecure™ Elements Security Center, proporciona visibilidad, información y administración centralizadas en todos los puntos finales y servicios en la nube. Es totalmente administrado por uno de nuestros proveedores de servicios administrados certificados, o autoadministrado con soporte a pedido de WithSecure™ para casos difíciles. El Centro de seguridad proporciona una vista única del estado de seguridad que combina Endpoint Protection, Endpoint Protection and Response, Vulnerability Management y Microsoft 365 Protection.

[1] El Informe de costo de una filtración de datos de 2018 de Ponemon Institute indicó que los días para identificar las fugas de datos variaron según el sector de la industria de 150 a 287 días, y las actividades de respuesta posteriores a la filtración de datos solo gastaron $ 1.76 millones durante 69 días como tiempo medio.

[2] El informe Costo de una filtración de datos de 2020 de Ponemon Institute indicó que el tiempo promedio para identificar y contener la filtración de datos es de 280 días.

Todas las soluciones de puntos finales (Elements Endpoint Protection, Endpoint Detection and Response y Vulnerability Management) utilizan un único agente de software que debe implementarse solo una vez. Las soluciones complementarias se pueden activar posteriormente sin tener que implementar soluciones adicionales. WithSecure™ Elements Collaboration Protection es una solución basada en la nube que no requiere instalaciones en los terminales de la empresa.

Además de los beneficios de implementación y administración, las soluciones WithSecure™ Elements están diseñadas para trabajar juntas y maximizar los beneficios de seguridad para la empresa. Al combinar eventos de seguridad y alertas, las capacidades de XDR WithSecure™ Elements pueden proporcionar una seguridad holística que rompe los silos de soluciones desconectadas.

WithSecure™ Elements

	Endpoint Protection Standard	Endpoint Protection Premium	Detección y Respuesta	Gestión de vulnerabilidades	Protección Microsoft 365
Gestión avanzada de parches y antimalware	✓	✓			
Anti-ransomware con protección de datos y control de aplicaciones		✓			
Protección avanzada contra amenazas			✓		
Gestión y priorización de vulnerabilidades				✓	
Seguridad de correo electrónico avanzada para Microsoft 365					✓

Nota: las funciones disponibles pueden variar según la plataforma operativa

Presentamos WithSecure Elements Endpoint Detection and Response

WithSecure™ Elements Endpoint Detection and Response es una solución líder de detección y respuesta de endpoints (EDR) a nivel de contexto para ayudar a las empresas a obtener una visibilidad inmediata de su entorno de TI y estado de seguridad, proteger la empresa y sus datos confidenciales detectando ataques rápidamente y respondiendo rápido con guía experta. Con su profunda inteligencia bidireccional y alto nivel de automatización, la solución de WithSecure protege contra amenazas avanzadas incluso antes de que ocurran las infracciones. Detecta incidentes con clientes ligeros, que están instalados en hosts monitoreados en toda la red de la organización. Los clientes recopilan datos sobre eventos de comportamiento, como el acceso a archivos, los procesos iniciados, la creación de conexiones de red o algo que se escribe en el registro o en los registros del sistema. Estos eventos luego son analizados más a fondo por la solución. Además de las detecciones en tiempo real, la solución también realiza detecciones basadas en datos históricos. Al final del día, utilizar tecnología de punta es solo una parte de la ecuación, ya que la tecnología es tan buena como las personas que la respaldan. Nuestros cazadores e investigadores de amenazas se encuentran entre los principales expertos de la industria y están inmensamente dedicados a brindar lo mejor en el mercado de la ciberseguridad. En WithSecure™, combinamos esa tecnología y esa experiencia humana insuperable para ofrecer una solución de respuesta y detección de punto final de clase mundial.

La solución cuenta con el respaldo exclusivo de WithSecure™, lo que significa que una detección puede elevarse a WithSecure™ para un mayor análisis de amenazas por parte de expertos en ciberseguridad.

La solución también está disponible como un servicio EDR administrado por socios que combina tecnología, inteligencia de amenazas y servicios de socios para proporcionar un servicio de respuesta y detección de infracciones todo en uno. Los servicios EDR administrados liberan los recursos propios de una organización del monitoreo avanzado de amenazas y la administración de incidentes para alertar a la organización solo cuando se detectan amenazas reales.

Al final del día, utilizar tecnología de punta es solo una parte de la ecuación, ya que la tecnología es tan buena como las personas que la respaldan. Nuestros cazadores e investigadores de amenazas se encuentran entre los principales expertos de la industria y están inmensamente dedicados a brindar lo mejor en el mercado de la ciberseguridad. En WithSecure™, combinamos esa tecnología y esa experiencia humana insuperable para ofrecer una solución de respuesta y detección de punto final de clase mundial.

La prevención dificulta la vida de los atacantes.

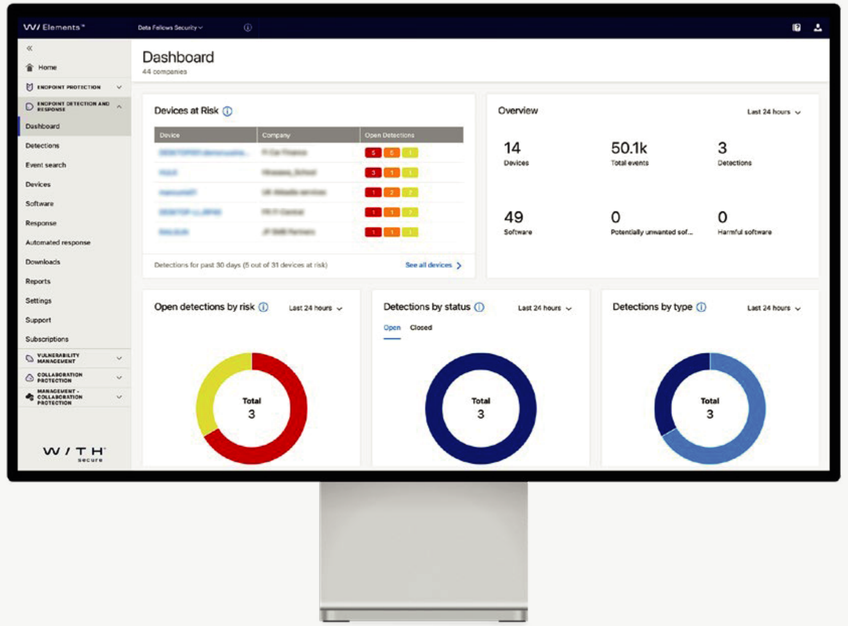
Los atacantes avanzados pueden tener las habilidades para ingresar a su red pase lo que pase, pero no hay necesidad de desplegar la alfombra roja. Al esforzarse en la prevención previa al compromiso, está haciendo que sea un poco más difícil para estos atacantes violar su red. Cuando se ven obligados a esforzarse más, sus estructuras de costos aumentan, lo que ayuda a funcionar como elemento disuasorio.

WithSecure™ Elements Endpoint Detection and Response como solución posterior al compromiso para detectar ataques avanzados aún requiere una solución sólida de protección de endpoints que bloquee las amenazas básicas, como el ransomware.

2. Beneficios clave

Con la solución WithSecure™ Elements Endpoint Detection and Response, puede estar preparado para detectar amenazas avanzadas y ataques dirigidos mediante técnicas sin archivos antes de que ocurran filtraciones de datos, y estar siempre listo para analizarlas y responder rápidamente utilizando la tecnología de vanguardia de WithSecure.

A continuación se enumeran algunos de los beneficios clave que ofrece la solución para la visibilidad, la detección y la respuesta:



Obtenga visibilidad contextual inmediata de su entorno de TI y estado de seguridad

- Mejore la visibilidad del estado y la seguridad del entorno de TI con inventarios de aplicaciones y terminales.
- Detecte fácilmente el mal uso del uso adecuado al recopilar y correlacionar eventos de comportamiento más allá del malware.
- Responda más rápido a los ataques dirigidos identificados gracias a la alerta con contexto amplio y criticidad del host.

Proteja su empresa y sus datos confidenciales detectando infracciones rápidamente

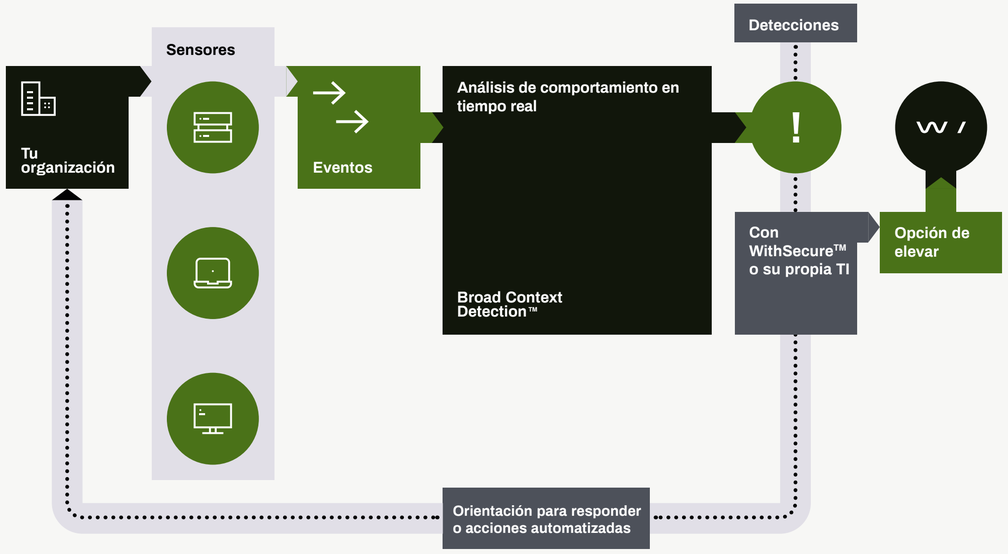
- Detecte y detenga ataques dirigidos rápidamente para evitar interrupciones comerciales y un impacto en la reputación de la empresa,
- Prepárese antes de que se produzcan infracciones configurando funciones avanzadas de detección y respuesta ante amenazas en cuestión de días.
- Identifique amenazas o signos de ataque que se realizaron en el punto final y aún están activos en la memoria cuando se activa la funcionalidad EDR.
- Cumplir con los requisitos reglamentarios de PCI, HIPAA y el RGPD de la Unión Europea, que exigen que se notifiquen las infracciones de datos en un plazo de 72 horas.

Responda rápidamente con automatización y orientación cuando esté bajo ataque, o use datos completos de incidentes para sus propias investigaciones SOC

- Mejore el enfoque de su equipo con automatización e inteligencia integradas que respaldan una respuesta rápida a las amenazas avanzadas reales y los ataques dirigidos.
- Reciba orientación sobre cómo responder cuando reciba alertas, con la opción de automatizar las acciones de respuesta durante todo el día (las funciones de automatización se presentarán como una actualización).
- Supere las brechas de habilidades o recursos en sus equipos subcontratando el monitoreo avanzado de amenazas a un proveedor de servicios administrados certificado por WithSecure™ respaldado por expertos de WithSecure™.
- Alternativamente, para clientes o socios con capacidades de búsqueda de amenazas, WithSecure™ Elements for Endpoint Detection and Response puede proporcionar los datos sin procesar completos sobre los incidentes con el servicio adicional de búsqueda de eventos para la búsqueda de amenazas.

3. Descripción general de la solución

La solución WithSecure Elements Endpoint Detection and Response consiste en una combinación de clientes fácilmente implementables en hosts, un Elements Security Center basado en la nube y servicios opcionales administrados por socios certificados. La solución proporciona funcionalidad para detectar amenazas avanzadas y ataques dirigidos, y detecciones de contexto amplio para aclarar el riesgo y la respuesta generales. La parte in situ de la implementación incluye el monitoreo de puntos finales y el cliente de respuesta que se instala en los puntos finales de una organización.



La figura describe en un alto nivel cómo funciona la solución WithSecure Elements Endpoint Detection and Response:

1. **Los clientes ligeros** monitorean diferentes actividades de punto final que llevan a cabo los atacantes y transmiten eventos de comportamiento a nuestra nube en tiempo real.
2. **El análisis de datos** de comportamiento en tiempo real marca y supervisa tanto los procesos como otros comportamientos que han desencadenado los eventos.
3. **El mecanismo de detección** de contexto amplio reduce aún más los datos, colocando eventos relacionados en contexto entre sí, identificando rápidamente ataques reales y priorizándolos con respecto al nivel de riesgo, la criticidad del host y el panorama de amenazas predominante.
4. Luego de una **detección confirmada**, la solución guía a los equipos de TI y seguridad a través de los pasos necesarios para contener y remediar la amenaza.

3.1 Portal de gestión: Elements Security Center

La solución Elements Endpoint Detection and Response facilita la implementación, la gestión y el control de las amenazas avanzadas en sus puntos finales desde una única consola intuitiva basada en la web. Le brinda visibilidad contextual inmediata del entorno de TI y el estado de seguridad en toda su red, independientemente de si los empleados están en la oficina o en movimiento.

El portal de administración fue diseñado para simplificar y acelerar la administración de la seguridad en entornos exigentes y de múltiples sitios.

A continuación, se muestran algunos ejemplos de cómo se considera la solución. A continuación, se muestran algunos ejemplos de cómo la solución reduce considerablemente la cantidad de tiempo y recursos necesarios para el monitoreo y la gestión avanzados de amenazas:

- La solución está diseñada para funcionar con cualquier solución de protección de puntos finales y funciona con las soluciones de seguridad de puntos finales de WithSecure™ en una infraestructura de administración y de un solo cliente.
- Cuando se combina con WithSecure™ Elements Endpoint Detection and Response, tanto el malware como las amenazas avanzadas se vuelven visibles y manejables.
- Las detecciones se presentan con visualización procesable para proporcionar un contexto más amplio de ataques dirigidos en una línea de tiempo con todos los hosts afectados, eventos relevantes y acciones recomendadas.
- Al consolidar la gestión avanzada de amenazas de puntos finales y herramientas del sistema en un portal de seguridad de endpoints, la gestión general se agiliza considerablemente, ahorrando tiempo.

- Como se trata de un servicio basado en la nube gestionado por WithSecure™, no es necesario instalar ni mantener ningún hardware o software de servidor; todo lo que necesita es un navegador y una conexión a Internet.

El portal de gestión admite las últimas versiones de los siguientes navegadores: Microsoft Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome y Safari.

El portal de gestión está disponible (a partir de mayo de 2021) en inglés, finlandés, francés, alemán, italiano, japonés, polaco, portugués, español (Latinoamérica) y sueco.

La versión administrada por socios del portal de administración incluye funciones diseñadas específicamente para ayudar a los proveedores de servicios, como informes del cliente final, un tablero con una descripción general conveniente de todas las empresas administradas y también acceso al tablero propio de cada empresa administrada.

3.2 Clientes Endpoint

Los clientes de endpoint son herramientas de monitoreo ligeras y discretas diseñadas para la detección de anomalías, incluidos eventos nuevos y previamente no identificados o una secuencia de eventos que muy probablemente resulten de actividades maliciosas, implementables en todas las computadoras Windows y MacOS relevantes dentro de la organización. Los clientes recopilan datos de eventos de comportamiento de los puntos finales, están diseñados para funcionar con cualquier solución de protección de puntos finales y funcionan sin problemas con las soluciones de seguridad de puntos finales de WithSecure en una infraestructura de administración basada en la nube y de un solo cliente.

La tabla describe los sistemas operativos compatibles y las características de cada sistema operativo.

WithSecure™ Elements

	Estación de trabajo de Windows	Servidores Windows	Mac os	Linux
Sistema Operativo	7 / 8 / 10	2019 / 2016 / 2012 /2011 / 2008 R2	10.12 or newer	
Cliente único con WithSecure™	Sí	Sí	Sí	Sí
Eventos de comportamiento	Sí	Sí	Sí	Sí
Visibilidad de las aplicaciones	Sí	Sí	No*	No*
Aislamiento de host remoto	Sí	Sí	Sí	Sí

***Esperado más tarde: la función aún no está disponible. ****Disponible con WithSecure Business Suite a través de acciones manuales.**

Más información sobre los requisitos del sistema y la implementación del cliente en la guía del usuario en https://help.f-secure.-com/product.

html#business/edr/latest/en/deployment-latest-en

3.3 Visibilidad de la aplicación

Obtener una amplia visibilidad de su entorno de TI y servicios en la nube reducirá la exposición a amenazas avanzadas y fugas de datos. La visibilidad de las aplicaciones de nuestra solución le permite enumerar todas las aplicaciones activas que se ejecutan en los puntos finales de la red de su organización para que pueda identificar fácilmente las aplicaciones no deseadas, desconocidas y dañinas.

Con la visibilidad de la aplicación, puede identificar aplicaciones potencialmente no deseadas (PUA) y aplicaciones no deseadas (UA). Las 'aplicaciones potencialmente no deseadas' tienen comportamientos o características que puede considerar indeseables o indeseables. Las 'aplicaciones no deseadas' tienen comportamientos o rasgos con un impacto más severo en su dispositivo o datos.

Las aplicaciones identificadas como "Potencialmente No Deseadas" (PUA) pueden:

- Afectar su privacidad o productividad, por ejemplo, exponer información personal o realizar acciones no autorizadas.
- Ponga una tensión indebida en los recursos de su dispositivo, por ejemplo, use una cantidad excesiva de almacenamiento o memoria
- Comprometer la seguridad de su dispositivo o la información almacenada en él, por ejemplo, exponerlo a contenido o aplicaciones inesperados.

El impacto de estos comportamientos y rasgos en su dispositivo o datos puede variar de leve a grave. Sin embargo, no son lo suficientemente dañinos como para justificar la clasificación de la aplicación como malware.

Recopilación de datos de eventos para detectar y contener amenazas

WithSecure™ Elements Endpoint Detection and Response recopila datos de una variedad de puntos finales para ayudar a detectar y contener amenazas en su entorno. Estos datos se proporcionan de tres maneras diferentes:

1. **Detección de contexto amplio:** este método automatizado de identificación de amenazas está diseñado para detectar amenazas reales a partir de una gran cantidad de datos de eventos de comportamiento recopilados de los puntos finales de la empresa. Además, con la función integrada WithSecure™ Elevate, puede solicitar orientación profesional de nuestros expertos especializados en seguridad cibernética para resolver casos difíciles.
2. **Búsqueda de eventos:** con esta función integrada, puede ver, buscar y explorar los datos de eventos recopilados de los puntos finales de su empresa que están relacionados con cualquier detección de contexto amplio.
3. **Búsqueda de eventos para la caza de amenazas:** esta función avanzada se utiliza para explorar e interactuar con todos los datos de eventos sin procesar recopilados desde los puntos finales. Sus sofisticadas capacidades de filtrado permiten a los expertos en seguridad cibernética de SOC ejecutar una búsqueda proactiva de amenazas para detectar y detener las amenazas ocultas más sofisticadas. Event Search for Threat Hunting es un componente opcional de WithSecure ™ Elements Endpoint Detection and Response.

3.4 Análisis de comportamiento

Como una funcionalidad central para identificar amenazas avanzadas entre cantidades masivas de eventos de datos de comportamiento para detectar eventos sospechosos o una secuencia de eventos que no se han visto antes y que probablemente sean maliciosos.

WithSecure™ utiliza análisis de comportamiento, reputación y big data en tiempo real con aprendizaje automático para recopilar múltiples eventos sospechosos que se pueden vincular, por ejemplo, en función de las actividades. El análisis de comportamiento aprovecha la inteligencia artificial para detectar actividad maliciosa y oculta basada en pequeños eventos individuales que se ejecutan como parte de las tácticas, técnicas y procedimientos del atacante. El análisis de comportamiento se utiliza en la identificación automática del perfil del host que afecta la puntuación de riesgo, las detecciones en relación con la empresa y el host monitoreados, y el entorno de TI en general.

La inteligencia artificial incluye capacidades de aprendizaje automático que se aplicarán para mejorar continuamente las detecciones y reducir los falsos positivos. La capacidad de análisis de comportamiento es un excelente ejemplo en el que WithSecure™ combina la ciencia de datos y la experiencia en ciberseguridad, un enfoque al que WithSecure ™ se refiere como "hombre y máquina".

3.5 Broad Context Detection™

Las metodologías patentadas de detección de contexto amplio de WithSecure están diseñadas para reducir la cantidad de detecciones a una pequeña cantidad de incidentes significativos que pueden indicar que los sistemas o los datos se han visto comprometidos.

Broad Context Detection™ señala indicaciones de posibles infracciones al alertar a los administradores sobre tácticas, técnicas y procedimientos (TTP) utilizados en ataques dirigidos. Esto puede incluir, por ejemplo, las siguientes acciones posiblemente sospechosas:

- Actividad anormal de los programas estándar
- Llamadas a procesos en ejecución desde ejecutables no estándar
- Ejecución de scripts inesperados
- Ejecución inesperada de herramientas del sistema desde procesos estándar

Broad Context Detection™ muestra solo las detecciones relevantes y les asigna una criticidad basada en el nivel de riesgo, información sobre las criticidades del host afectado y el panorama de amenazas predominante. Un solo evento puede no ser una indicación de un ataque, sin embargo, si ocurren varias detecciones en un corto período de tiempo, puede generar una alerta de mayor gravedad y activar una detección de contexto amplio ™ como advertencia de un posible incidente.

Como resultado de este enfoque, los equipos de TI cuentan con una lista relativamente corta de detecciones confirmadas, cada una marcada con distintos niveles de prioridad y acciones de respuesta recomendadas.

Entonces, los equipos no solo saben en qué concentrarse primero, sino que también saben cómo responder y pueden hacerlo de manera rápida y decisiva.

Para obtener más información sobre Broad Context Detection ™, consulte nuestro documento técnico Detecting Advanced Attacks.

3.4 Análisis de comportamiento

La solución tiene una función de gestión de incidentes integrada para ver y gestionar las detecciones de contexto amplio. Las nuevas detecciones activarán una alerta por correo electrónico que contiene acceso directo al portal de administración para ver detalles y tomar medidas.

Las detecciones de contexto amplio se enumeran en el panel fácil de usar que ayuda a priorizar los incidentes en función de su puntuación de riesgo, que se calcula automáticamente en función de los niveles de criticidad y confianza. También se enumeran las detecciones de contexto amplio no críticas con puntuaciones de riesgo bajas, ya que los ataques que evolucionan lentamente pueden convertirse en incidentes más graves con puntuaciones de riesgo altas.

Las acciones en la gestión de incidentes son reconocer las detecciones de contexto amplio o marcarlas para que estén en curso, controlando, cerradas como confirmadas, cerradas como falso positivo o cerradas como no confirmadas. Marcar Broad Context Detection™ como falso positivo cerrará automáticamente las futuras detecciones que coincidan con el mismo tipo de detección, procesará los parámetros como "Auto falso positivo".

3.7 Orientación para responder

Después de una detección confirmada, la guía integrada de la solución ayuda a tomar las medidas necesarias para contener y remediar la amenaza. Los pasos de contención y remediación incluyen acciones de respuesta recomendadas, como informar a los usuarios y aislar hosts.

Los expertos en seguridad cibernética de WithSecure™ han utilizado su propia experiencia para analizar una gama de amenazas comunes para entrenar la solución. Como resultado, la solución puede proporcionar una guía fácil de entender para responder a una amplia gama de amenazas avanzadas y una guía relacionada sobre cómo responder. La guía para responder hace que sea más fácil, incluso para los miembros del equipo de seguridad y TI menos capacitados, tomar las medidas correctas para contener y remediar la amenaza.

La siguiente lista contiene algunos ejemplos de actividades que provocan una detección.

La lista no solo se limita a los ataques conocidos, ya que los datos de detección se analizan continuamente y las metodologías de detección de contexto amplio y los cazadores de amenazas de WithSecucure identifican continuamente más tipos de ataques.

- **Ataque dirigido** a un host.
- **Movimiento lateral** que implica movimiento entre huéspedes.
- **Suplantación de información** involucrada como parte de un ataque.
- **Persistencia,** por ejemplo, mediante el uso de un proceso en el mismo host
- **Escalada de privilegios,** por ejemplo, mediante privilegios de administrador de fuerza bruta.
- **Acceso de credenciales** que da como resultado acceso y control sobre una máquina/red de destino.
- **Exfiltración** para ayudar al adversario a extraer información de la máquina/red de destino.
- **Ejecución anormal de procesos,** por ejemplo, con parámetros sospechosos.
- **Acceso anormal a archivos,** por ejemplo, múltiples tipos de documentos, archivos del sistema de acceso no root.
- **La manipulación del cliente intenta,** por ejemplo, cambiar la configuración del cliente para deshabilitar el cliente.
- **Intentos de inyección a otro proceso,** por ejemplo, modo kernel u otra aplicación.
- **Conexión de red** de comando y control abierta a un host remoto.
- **Secuencia de comandos de Powershell** de la ubicación del atacante marcada como una ubicación habitual para cargar una secuencia de comandos.
- **PowerShell** modificó un script de PowerShell que generalmente forma parte del logro de la persistencia.
- **Uso anormal de DLL** con PowerShell utilizado desde un proceso que cargó el módulo.
- **Conexión remota** y ejecución potencialmente utilizada para el movimiento lateral.

3.8 Elevar a WithSecure™

WithSecure™ proporciona un servicio de análisis de amenazas opcional en caso de que una detección requiera más análisis de amenazas y orientación de los expertos en seguridad cibernética de WithSecure. Elevate to WithSecure™ es un servicio premium que debe solicitarse con anticipación para analizar un conjunto de casos.

Las solicitudes de Elevate to WithSecure™ a través de la solución otorgarán permiso a los analistas de amenazas de WithSecure para acceder a la totalidad de los metadatos recopilados de los clientes instalados en torno a una detección específica.

Los analistas de amenazas en turno de WithSecure elegirán la solicitud dentro de un SLA objetivo de 2 horas y comenzarán a identificar el tipo de incidente potencial mediante la recopilación de evidencia adicional y brindando más orientación experta a través de la solución a la amenaza y, opcionalmente, brindando una investigación de amenazas.

- Threat Validation proporciona información adicional sobre un Broad Context Detection™ descubierto durante los últimos 7 días. Esto incluye un resumen escrito por expertos y una descripción de la detección, junto con cualquier otro dato relevante para ayudarlo a determinar si requiere acciones de respuesta.

- Threat Investigation proporciona una investigación muy detallada sobre una detección de contexto amplio específica, aprovechando todos los datos recientes e históricos. Esta opción también incluye una guía práctica de respuesta a incidentes de nuestros expertos en seguridad cibernética, junto con un informe completo del tipo de ataque detectado.

El servicio Elevate to WithSecure™ se enfoca en analizar la evidencia técnica relacionada con los posibles incidentes en cuestión, como métodos y tecnologías, rutas de red, orígenes de tráfico y plazos. Sin embargo, el equipo de WithSecure™ solo brinda orientación a través de la solución, y los servicios profesionales adicionales para respaldar la respuesta a incidentes deben acordarse por separado. Si el cliente sospecha de un delito, recomendamos ponerse en contacto con las autoridades pertinentes y proporcionar el informe de Investigación de amenazas.

3.9 Automatización de acciones

Las acciones de respuesta automática están disponibles para reducir el impacto de los ataques cibernéticos dirigidos al contenerlos automáticamente fuera del horario comercial siempre que los niveles de riesgo sean lo suficientemente altos. La automatización se ha diseñado específicamente para equipos que supervisan detecciones y están disponibles para responder a incidentes solo durante el horario comercial para realizar una acción de respuesta inicial durante la noche o el fin de semana.

4. Seguridad de los datos

4.1 Protección de datos y confidencialidad

Los datos de eventos de comportamiento recopilados de los puntos finales se almacenan dentro de la Unión Europea (Irlanda) durante un año de forma continua durante el compromiso del cliente y se eliminan dentro de los dos meses posteriores a la terminación del compromiso.

La solución no está diseñada para monitorear actividades no relacionadas con la seguridad, como la creación de perfiles de las actividades, los intereses o las interacciones de los empleados. El enfoque de la recopilación de datos no está en empleados individuales, documentos comerciales o contenido de correo electrónico. Consulte la política de privacidad específica de la solución para obtener más detalles.

Como WithSecure™ tiene su sede en Finlandia, cumplimos con las estrictas leyes de seguridad y privacidad de Finlandia y la Unión Europea. Somos compatibles con el marco de privacidad de la Unión Europea y comprendemos las necesidades de privacidad de nuestros clientes. WithSecure™ opera bajo la implementación finlandesa de la directiva de protección de datos de la UE y la solución WithSecure™ Elements Endpoint Detection and Response se ha diseñado de acuerdo con el Reglamento general de protección de datos (GDPR) de la Unión Europea. Para obtener más información sobre el cumplimiento de WithSecure con el RGPD, consulte https://www.WithSecure.com/GDPR.

4.2 Medidas de seguridad de datos

Como empresa de seguridad, nos tomamos muy en serio la seguridad de nuestros centros de datos y utilizamos docenas de medidas de seguridad para garantizarla, como:

- Seguridad por diseño: Nuestros sistemas están diseñados desde cero para ser seguros. Integramos la privacidad y la seguridad en el desarrollo de nuestras tecnologías y sistemas desde las primeras etapas de conceptualización y diseño hasta la implementación y operación.
- Controles de acceso rigurosos: solo un pequeño grupo examinado de empleados de WithSecure™ tiene acceso a los datos del cliente. Los derechos y niveles de acceso se basan en la función y el rol de su trabajo, utilizando el concepto de privilegio mínimo y ajustándolo a las responsabilidades definidas.
- Sólida seguridad operativa: la seguridad operativa es una parte cotidiana de nuestro trabajo, incluida la gestión de vulnerabilidades, la prevención de malware y procesos sólidos de gestión de incidentes para eventos de seguridad que pueden afectar la confidencialidad, integridad o disponibilidad de sistemas o datos.

4.3 Centros de datos

Nuestra solución de detección y respuesta de puntos finales utiliza centros de datos de Amazon Web Services (AWS) para garantizar la mayor disponibilidad y tolerancia a fallas posibles, además de mejores tiempos de respuesta y la capacidad de escalar según sea necesario. AWS afirma que cada uno de sus centros de datos está alineado con las pautas de Nivel 3+. Para obtener más información sobre los centros de datos de AWS, consulte https://aws.amazon.com/compliance/

Los datos de eventos de comportamiento recopilados de los puntos finales se almacenan en AWS en Europa (Irlanda). La retención de datos durante un año está incluida en la suscripción de Elements Endpoint Detection and Response y no hay cargos adicionales por almacenamiento de datos en función de la cantidad de datos recopilados.

Quiénes somos

WithSecure™ es el socio confiable de la seguridad cibernética. Los proveedores de servicios de TI, los MSSP y las empresas junto con las instituciones financieras más grandes, los fabricantes y miles de los proveedores de tecnología y comunicaciones más avanzados del mundo confían en nosotros para la seguridad cibernética basada en resultados que protege y habilita sus operaciones. Nuestra protección impulsada por IA protege los puntos finales y la colaboración en la nube, y nuestra detección y respuesta inteligente está impulsada por expertos que identifican los riesgos comerciales al buscar amenazas de manera proactiva y confrontarlas en vivo para desarrollar resiliencia a través de consejos de seguridad basados en evidencia. Con más de 30 años de experiencia en la creación de tecnología que cumple con los objetivos comerciales, hemos construido nuestra cartera para crecer con nuestros socios a través de modelos comerciales flexibles.

WithSecure™ es parte de F-Secure Corporation, fundada en 1988 y cotiza en NASDAQ OMX Helsinki Ltd.

WITH secure™