Whitepaper

Guía para Vulnerability Management

Protección inteligente de endpoints y descubrimiento de amenazas de clase mundial

WITH secure

Contenidos

Resumen de gestión 3
Gestión completa de amenazas 3
Industria de tarjetas de pago
Estándar de seguridad de datos (PCI DSS) 5
WithSecure™ Elements Vulnerability
Gestión de un vistazo 6
La historia de Equifax 7
La aplicación de parches no es un hecho 8
Incógnitas conocidas e incógnitas desconocidas 8
No olvides tu Intranet 9
La visibilidad es clave 9
Descripción general de las vulnerabilidades actuales 10
La clave para prevenir ataques cibernéticos 11
Los adversarios no necesitan
Muchas vulnerabilidades Uno es suficiente 12
La línea de tiempo habitual de una intrusión 13
¿Cuáles son las consecuencias
si no cuidas tu superficie? 15
La discusión interna de la empresa sobre el riesgo cibernético .. 17
RGPD: ¿sanciones temibles o una oportunidad para mejorar
su organización? 19
¿Qué ofrece Elements Vulnerability Management? 20
Identificar y exponer las posibles amenazas 21
Descubrimiento de activos de Internet 22
Exploraciones de descubrimiento 23
Escaneos del sistema 24
Escaneos web 25
Aplicaciones web personalizadas 26
Agente de nodo de exploración 26
Agente de Elements Vulnerability Management 27
Administración 28
Informes 28
Propuesta de valor 29
Obtener visibilidad de sus entornos 29
WithSecure™ Elements Vulnerability Management 30

Resumen de gestión

Gestión completa de amenazas

WithSecure™ Elements Vulnerability Management es una plataforma de administración y escaneo de vulnerabilidades integral, fácil de implementar y todo en uno que respalda los programas de seguridad de las organizaciones con una visibilidad clara, procesable y priorizada de los riesgos reales. Elements Vulnerability Management está diseñado principalmente para abordar las necesidades de las pequeñas y medianas empresas (PYME), capacitándolas para proteger la continuidad de su negocio a través de una gestión eficaz de vulnerabilidades. El software sin parches y mal configurado es un vector de ataque clave y un habilitador de infracciones, especialmente cuando se trata de ataques más avanzados. WithSecure™ Elements Vulnerability Management puede reducir significativamente el costo de la seguridad cibernética siendo proactivo e identificando posibles problemas de seguridad antes de que sean explotados. Aprovechar los recursos en la nube de Elements Vulnerability Management permite a las organizaciones reducir sus gastos, lo cual es un factor particularmente importante para las pymes que aún no cuentan con recursos de seguridad dedicados.

Además, WithSecure™ Elements Vulnerability Management es una solución óptima para proveedores de servicios administrados (MSP), que les permite ingresar al negocio de servicios de seguridad cibernética, crecer con WithSecure™ y capturar oportunidades de mercado.

Con Elements Vulnerability Management, el proveedor de servicios gestionados puede ampliar su oferta de servicios a la gestión de vulnerabilidades basada en la nube y ofrecer soluciones y servicios de seguridad cibernética líderes en el mercado de una manera escalable y rentable.

Es probable que los clientes finales que carecen del tiempo o el conocimiento para administrar sus propias evaluaciones de vulnerabilidad ejecuten sus propias evaluaciones de vulnerabilidad y que ejecuten un socio de servicio administrado local. Las leyes de privacidad y datos de la UE (GDPR) incentivan a las empresas clientes a cumplir y buscar ayuda y servicios de un proveedor de servicios gestionados local. Los socios de servicios administrados son los más influyentes entre las implementaciones de clientes finales de menos de 1000 puestos.

Este documento describe los controles de seguridad de alto nivel que emplea WithSecure™ con Elements Vulnerability Management.

Identificar y exponer posibles amenazas.

A diferencia de muchas otras soluciones de administración de vulnerabilidades en el mercado actual, WithSecure™ Elements Vulnerability Management presenta tecnología de rastreo web, llamada Internet Asset Discovery, que también cubre la web profunda. Con esto, puede realizar una amplia variedad de tareas que van desde la evaluación de amenazas hasta la inteligencia empresarial. En esencia, Elements Vulnerability Management le permite navegar fácilmente a través de todos los objetivos para identificar rápidamente los riesgos y las conexiones potencialmente vulnerables, y expandir el análisis de su superficie de ataque más allá de su propia red.

Las marcas y la propiedad intelectual exitosas a menudo convierten a las empresas en el blanco de actividades fraudulentas o maliciosas. Dichas actividades incluyen infracciones de marca, donde terceros se hacen pasar por su empresa, sitios de phishing destinados a estafar o infectar a los visitantes y errores tipográficos, donde alguien registra dominios usando palabras que se parecen a su marca para redirigir el tráfico a través de enlaces que se parecen a los suyos. Muchas empresas tienen poca o ninguna conciencia de este tipo de actividades.

Las muchas formas en que una empresa puede estar expuesta al riesgo cibernético

Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS)

Garantizar el cumplimiento de la normativa actual y futura

Como proveedor de servicios aprobado, WithSecure™ debe realizar las acciones enumeradas aquí para identificar cualquier discrepancia de alcance que exista en la información proporcionada por el cliente de escaneo. La información sobre cualquier discrepancia de alcance debe indicarse en la Declaración de cumplimiento de escaneo en el "Estado de escaneo". Aunque esta información debe informarse como se indica, luego debemos ignorar esta información para determinar el cumplimiento de PCI DSS:

- Incluya cualquier dirección IP o dominio proporcionado previamente a WithSecure™ y que aún sea propiedad o sea utilizado por el cliente de escaneo * que se eliminó a pedido del cliente de escaneo.
- Si el cliente de escaneo ya no posee o tiene la custodia de la dirección IP o el dominio, incluya esa dirección IP o dominio durante al menos un trimestre adicional después de que el cliente de escaneo lo eliminó del alcance o lo liberó.
- Para cada dominio proporcionado, busque la dirección IP del dominio para determinar si ya la proporcionó el cliente de escaneo.
- Para cada dominio proporcionado, realice búsquedas DNS directas e inversas de nombres de host comunes, como "www", "correo", etc., que no proporcionó el cliente de escaneo.
- Identifique cualquier dirección IP encontrada durante la búsqueda de DNS del registro MX.
- Identifique cualquier dirección IP fuera del alcance a la que se accede a través de redireccionamientos web desde servidores web dentro del alcance (cubre todas las formas de redireccionamiento, incluidos: códigos JavaScript, metarredireccionamiento y HTTP 30x).
- Haga coincidir los dominios encontrados durante el rastreo con los dominios proporcionados por el usuario para encontrar dominios no documentados que pertenecen al cliente de escaneo

WithSecure™ Elements Vulnerability Management de un vistazo

Obten el panorama general

Mapee todos los activos del sistema para obtener una descripción general completa de la seguridad. Ningún sistema es demasiado grande: WithSecure™ Elements Vulnerability Management escala a medida que crece.

Gestión de seguridad optimizada

Supervise las vulnerabilidades de manera eficiente con análisis automatizados y programados. Asigne, administre y rastree todos los problemas de seguridad en coordinación con los administradores de sistemas, desarrolladores, auditores y más.

Mejora continua

WithSecure™ Elements Vulnerability Management se actualiza, mejora y prepara automáticamente para una integración perfecta con terceros a través de la API de gestión de vulnerabilidades de WithSecure™ Elements.

Informes personalizados simplificados

Customize and automate standardized reports for all audiences in a variety of formats.

Cumple con las regulaciones de la UE

WithSecure™ Elements Vulnerability Management cumple con las regulaciones de la UE con el cumplimiento de escaneo de vulnerabilidades PCI ASV y ayuda a los clientes a cumplir con GDPR.

WithSecure™ Elements Vulnerability Management a su manera

Ejecute escaneos de vulnerabilidades desde un SaaS seguro basado en la nube o como una solución en el sitio detrás de su firewall corporativo.

La historia de Equifax

El 7 de septiembre de 2017, Equifax, una agencia de informes crediticios del consumidor, anunció que había sido víctima de un ataque cibernético en el que se accedió a los datos personales de hasta 145,5 millones de personas. En el momento de escribir este artículo, este incidente precipitó la jubilación anticipada del director general de la empresa, dos altos funcionarios de seguridad, el director de información y el director de seguridad.

El análisis forense del incidente indicó que los atacantes aprovecharon una vulnerabilidad sin parche en el software de aplicación web de Equifax, Apache Struts. Esta vulnerabilidad fue descubierta inicialmente por Nike Zheng, un investigador de seguridad chino. Apache lanzó una solución para la vulnerabilidad el 6 de marzo de 2017. Para el 9 de marzo de 2017, los atacantes ya estaban explotando activamente la vulnerabilidad en la naturaleza.

Equifax, como todas las demás empresas que utilizan la plataforma, se enteró del parche el 6 de mayo de 2017. Se envió un memorando sobre la vulnerabilidad al personal de TI el 9 de mayo de 2017, pero debido a una falta de comunicación interna y una serie de investigaciones fallidas, Equifax no parcheó todas sus instalaciones vulnerables de Apache Struts hasta el 29 de julio de 2017, después de que descubrieron evidencia de una violación.

Resulta que los atacantes ingresaron a los sistemas de Equifax el 13 de mayo de 2017, exactamente una semana después de que se lanzó el parche. Una investigación más detallada reveló que Equifax tenía una política de 48 horas para aplicar parches críticos, pero esta política no se cumplió. Si hubieran seguido su política, habrían evitado esta infracción por completo.

Aunque cerca de tres meses parece mucho tiempo para parchear una vulnerabilidad crítica, Equifax ni siquiera está cerca de ser la empresa más lenta para parchear sistemas contra vulnerabilidades críticas. Por ejemplo, todavía hay muchos sistemas en la naturaleza que son susceptibles a las vulnerabilidades de EternalBlue que permitieron a NotPetya y WannaCry durante el verano de 2017. Y aunque la historia de Equifax suena como un caos, la mayoría de las veces es la realidad para los equipos encargados de gestionar infraestructuras informáticas complejas.

La aplicación de parches no es un hecho

La aplicación de parches no es un hecho. La aplicación de actualizaciones de software suele ser el trabajo de varias personas en una organización. Así como los sistemas operativos y el software son muy diversos, también lo son los mecanismos utilizados para aplicar actualizaciones y recibir notificaciones de parches disponibles. Cada proveedor alerta a sus clientes sobre la disponibilidad de actualizaciones a su manera. No existe un único lugar para encontrar toda la información que necesita, y los departamentos de TI aún dependen en gran medida del correo electrónico y de las fuentes RSS para mantenerse en el mapa.

Las actualizaciones y los parches llegan con frecuencia, y con docenas o incluso cientos de aplicaciones separadas para administrar, la mayoría de los departamentos de TI están inundados con diferentes actualizaciones. Para cada uno de estos, alguien debe comprender no solo qué está cambiando en el software en sí, sino también cómo podría afectar a los sistemas circundantes. Por esta razón, las actualizaciones a menudo deben probarse o probarse antes de implementarse en toda la organización. En el caso de las actualizaciones del servidor, las ventanas de mantenimiento deben programarse, especialmente si la aplicación de parches provoca tiempo de inactividad. Esto obliga a los departamentos de TI a priorizar las actividades de aplicación de parches y, en general, solo aplicar parches cuando sea absolutamente necesario. Pero para tomar estas decisiones de priorización, necesitan saber si una vulnerabilidad se está explotando activamente y si esa vulnerabilidad está presente en la superficie de ataque de la organización.

Incógnitas conocidas e incógnitas desconocidas

Para proteger adecuadamente la infraestructura informática, el personal de TI necesita saber qué sistemas requieren parches. Obtener este conocimiento a menudo implica recopilar y mantener un inventario preciso de todos los sistemas y software conocidos en la organización. A medida que las empresas crecen, las funciones comerciales comúnmente implementan sus propios sistemas y aplicaciones sin la participación del departamento de TI. Esos sistemas se convierten en parte de lo que comúnmente se conoce como TI en la sombra y pueden aumentar drásticamente la superficie de ataque de una organización. Los sistemas de TI en la sombra son difíciles de encontrar y su impacto a menudo se subestima en gran medida.

Pero si los sistemas de TI en la sombra representan un conjunto de incógnitas conocidas, los sistemas que pertenecen a la cadena de suministro de una empresa representan un conjunto aún mayor de incógnitas desconocidas. Aún así, los ataques a la cadena de suministro son bastante comunes.

Durante la Navidad de 2013, los delincuentes robaron datos de tarjetas de crédito pertenecientes a más de 60 millones de personas de Target, una gran cadena minorista estadounidense. Los atacantes violaron la red de Target instalando malware (a través de un archivo adjunto de correo electrónico) en un sistema que pertenece a una empresa llamada Fazio Mechanical. En ese momento, Fazio Mechanical suministraba servicios de calefacción y aire acondicionado a Target. Después de que los atacantes violaron Fazio Mechanical, obtuvieron las credenciales de VPN necesarias para conectarse de forma remota a la red corporativa de Target y, una vez dentro, introdujeron software malicioso en las cajas registradoras de unas 1800 tiendas. Las investigaciones sobre el incidente revelaron que no había controles que limitaran el acceso de los atacantes a cualquiera de los sistemas de Target, incluidos los dispositivos dentro de las tiendas, como las cajas registradoras y los servidores del punto de venta (POS). En un caso, los atacantes pudieron comunicarse directamente con las cajas registradoras en los carriles de pago después de comprometer una báscula de carnes frías ubicada en una tienda diferente.

No olvides tu Intranet

Si bien la reparación de vulnerabilidades en los sistemas con acceso a Internet generalmente se toma en serio, la seguridad de los sistemas dentro de una red corporativa a menudo se pasa por alto. Los sistemas detrás del firewall corporativo a menudo se consideran "protegidos" de los ataques y se supone que no hay intrusos en la red. Sin embargo, estas deficiencias de seguridad no siempre están vinculadas a los niveles de parches de software. Las configuraciones incorrectas a menudo brindan a los atacantes acceso a mecanismos de movimiento lateral fáciles.

Identificar configuraciones incorrectas de software es una tarea problemática. Esto se ve agravado por el hecho de que el software no siempre es seguro desde el primer momento y, a menudo, se necesita investigación para descubrir cómo configurar correctamente cada pieza de la infraestructura de TI de una empresa. Tomemos, por ejemplo, un servidor SSH.

Una vez instalado, probablemente desee configurarlo para que no permita inicios de sesión con contraseña, y lo más probable es que desee desactivar la capacidad de iniciar sesión de forma remota en un sistema como root. Un nuevo administrador que configure un sistema necesitaría saber que estos dos cambios de configuración deben realizarse y necesitaría saber cómo hacerlo. Ahora supongamos que tiene un puñado de servidores SSH en su red, todos los cuales fueron instalados en diferentes momentos, por diferentes empleados. Para averiguar si alguno de ellos está mal configurado, debe realizar una auditoría de cada uno. Ahora aplique esa misma lógica a muchas otras piezas de software instaladas en una organización y a la configuración de los propios sistemas operativos. No es una tarea fácil de realizar una vez, y mucho menos de forma frecuente. Entonces, nuevamente, se priorizan tareas como estas.

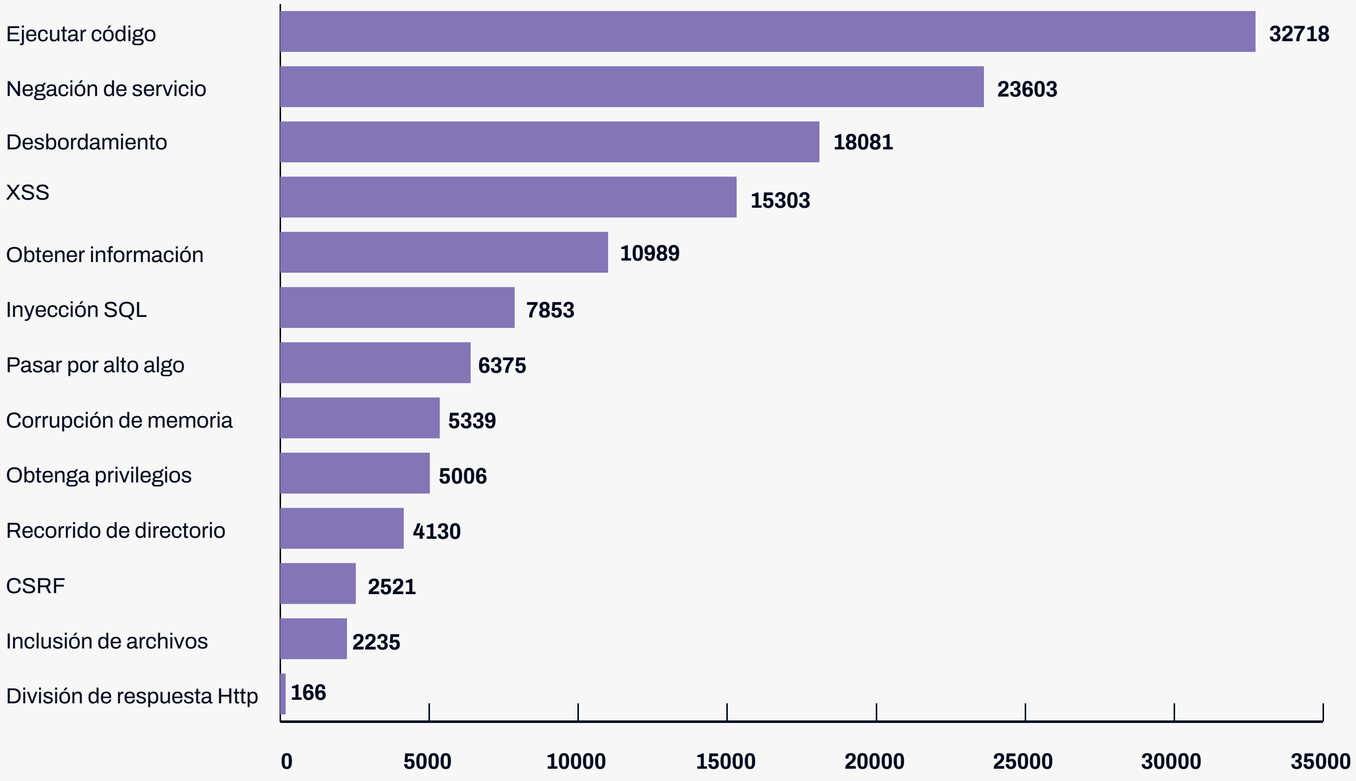
La visibilidad es clave

Mantener los sistemas seguros es abrumadoramente complejo y laborioso. Pero, en última instancia, es importante tener una imagen clara y precisa de su situación actual. Solo entonces puede comenzar a abordar la tarea de proteger adecuadamente su infraestructura. Y para entonces, podrá responder preguntas como:

- ¿Está nuestro nivel de riesgo donde debería estar?
- ¿Cuál es la probabilidad de que se produzca una infracción?
- ¿Cuál sería el impacto probable de una infracción?
- ¿Cuáles de nuestros activos están más expuestos?
- ¿Cuál es nuestro plan para reducir la exposición de los activos en el futuro?
- ¿Cuánto costará llevar nuestro nivel de riesgo a donde debería estar?
- ¿Cómo encaja ese costo en las asignaciones presupuestarias actuales?

Estos son los tipos de preguntas que cualquier equipo de liderazgo le hará a un departamento de TI si están preocupados por la seguridad cibernética (que deberían estarlo). Por lo tanto, al obtener suficiente visibilidad de la infraestructura de su organización (incluidas las incógnitas conocidas y las incógnitas desconocidas), no solo estará en posición de responder esas preguntas de manera proactiva y segura, sino que dormirá mejor por la noche.

Descripción general de las vulnerabilidades actuales



Fuente: http://www.cvedetails.com/vulnerabilities-by-types.php

Prevenir incidentes de forma proactiva

Con las amenazas cibernéticas creciendo más rápido que nunca, el tema de la seguridad se ha puesto en primer plano en la mente de todos los CIO. Hoy en día, el delito cibernético es una empresa de miles de millones de dólares y está en aumento. Según datos de Arbor Networks, la cantidad y el tamaño de los ciberataques aumentaron un 73 % en 2017. Con los incidentes de ciberataques creciendo año tras año, ninguna organización, independientemente de su tamaño o industria, está libre del riesgo de una filtración de datos. . Así que ya no se trata de si su empresa será atacada, sino de cuándo. Por este motivo, ahora más que nunca es importante implementar un enfoque proactivo de la ciberseguridad.

Debido a la idea errónea de que implementar medidas de seguridad costará a las empresas mucho tiempo y dinero, el enfoque predeterminado que las empresas adoptan con la ciberseguridad es "reactivo". Un enfoque reactivo significa que las empresas esperan hasta que se ven afectadas por una amenaza para implementar una solución. Irónicamente, este método probablemente le costará a su negocio mucho más tiempo y dinero que implementar medidas preventivas. Las estadísticas muestran que el ROI de las empresas que implementan medidas de seguridad preventivas se cumple frente a un ataque.

La clave para prevenir ataques cibernéticos

La clave para superar las infracciones causadas por errores humanos es crear un entorno en el que todos los empleados tengan un interés personal en la seguridad. Los empleados deben comprender el valor de proteger la información de clientes y socios, y su función para mantenerla segura. También necesitan conocimientos básicos sobre el panorama de riesgos y una manera de hacer buenos juicios sobre la seguridad en Internet de manera consistente. Para muchas personas, la seguridad parece sentido común, pero es más como “fuera de la vista y fuera de la mente”. La creación de una base segura debe comenzar con la capacitación y educación de los empleados.

Aunque los avances tecnológicos traen nuevas y emocionantes soluciones de seguridad a nuestra industria, los atacantes continúan desarrollando y lanzando nuevas tácticas, técnicas y procedimientos para burlarlos. La seguridad no tiene por qué ser un proceso costoso, pero no hacer nada no debería ser una opción. Ya sea que una empresa pueda permitirse o no una nueva solución de seguridad de alta tecnología, dar un paso atrás y centrarse en la seguridad en un nivel básico debería seguir siendo una prioridad. Ser proactivo con respecto a la seguridad es tarea de todos y requiere una vigilancia constante. Al hacer un esfuerzo consciente para adherirse a los procesos, procedimientos y políticas estándar de seguridad y educar a los empleados, las empresas pueden reducir drásticamente su vulnerabilidad a los ataques.

Los adversarios no necesitan muchas vulnerabilidades
Uno es suficiente

Cada
90
minutos

se identifica una nueva vulnerabilidad de seguridad

Eso es un promedio de
7
vulnerabilidades

por activo en un entorno de TI típico

Eso es un promedio de
8000

vulnerabilidades conocidas y reveladas cada año

50–300
vulnerabilidades críticas

explotable dependiendo de la industria

Se necesita un promedio de
103
días

hasta que se solucionen las vulnerabilidades de seguridad conocidas

Se necesita
15
días

en el promedio que una vulnerabilidad es explotada

La línea de tiempo habitual de una intrusión

En la jerga de la seguridad informática, el “Día Cero” es el día en que la parte interesada (presumiblemente el proveedor del sistema objetivo) se entera de la vulnerabilidad. Hasta ese día, la vulnerabilidad se conoce como vulnerabilidad de día cero. De manera similar, un error explotable que se conoce desde hace treinta días se denominaría vulnerabilidad de 30 días. Una vez que el proveedor se entera de la vulnerabilidad, generalmente creará parches o recomendará soluciones para mitigarla.

En general, hay demasiada publicidad en torno a las vulnerabilidades de día cero. El sitio web CVE Details muestra una puntuación de vulnerabilidad promedio de 6.8, en todas las vulnerabilidades conocidas en todas las plataformas conocidas. De las más de 80 000 vulnerabilidades conocidas en su base de datos, 12 000 (casi el 15 %) están clasificadas como de gravedad alta. Sin embargo, es bueno recordar que estas vulnerabilidades existen en muchas aplicaciones diferentes del lado del servidor y del cliente (incluyendo, lo adivinó, Adobe Flash).

Desde el punto de vista de una empresa, el manejo de vulnerabilidades de alta gravedad es la prioridad número uno. Y se manejan en organizaciones bien administradas. Las vulnerabilidades de alta gravedad obtienen mucha visibilidad y, debido a esto, se reparan en el acto. Pero las vulnerabilidades por sí solas no constituyen toda la superficie de ataque de su empresa. Su CISO probablemente esté más preocupado por el phishing y los ataques ascendentes que por las configuraciones incorrectas de la red interna y los sistemas internos sin parches.

Como administrador de TI, cuidar la infraestructura es su mayor preocupación.

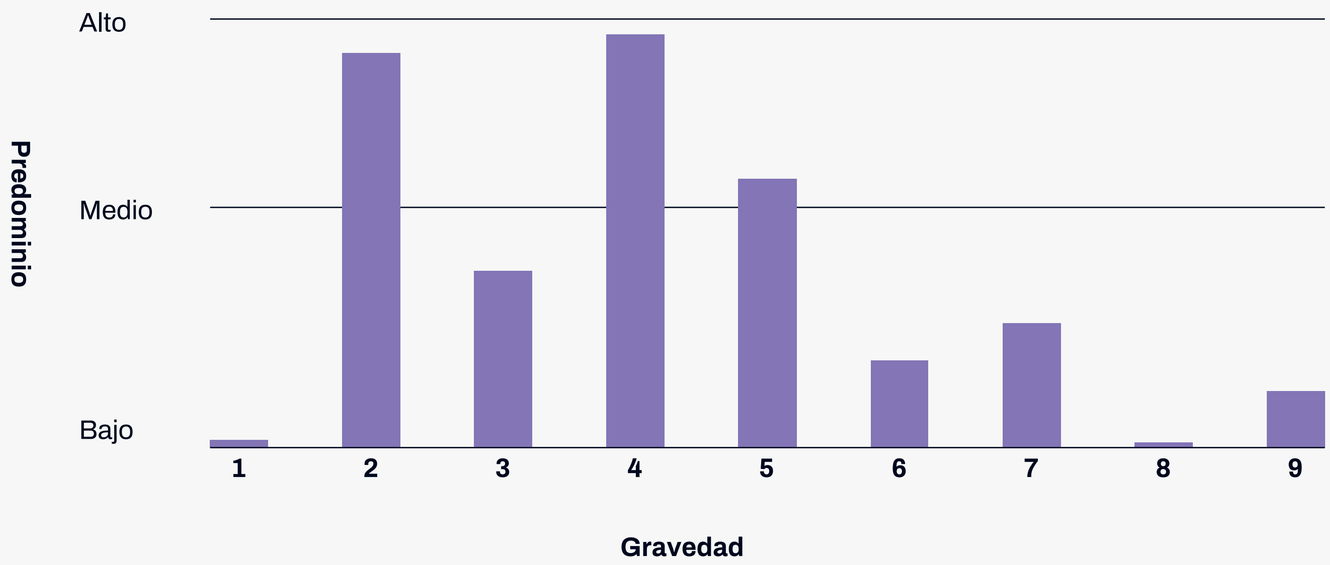
Por supuesto, realizará una clasificación cuando surja una nueva vulnerabilidad de alta gravedad. Pero, ¿y el resto de ellos? Aplicar cada parche a cada pieza de software en cada sistema de su red, a medida que se lanza el parche, simplemente no es factible. Es por eso que los administradores confían en los ciclos de parches periódicos para solucionar las vulnerabilidades de baja gravedad, si es que las solucionan. Tomarse el tiempo de su día para comprender las implicaciones de cada nueva vulnerabilidad es mucho pedir a la mayoría de los administradores de TI.

Y así, en muchos casos, simplemente no se molestan. Cuando buscan aplicar parches, los administradores a menudo hacen preguntas como:

- ¿Qué tan expuesto está el sistema?
- ¿Este parche romperá algo más?
- ¿Sé siquiera lo que significa esta vulnerabilidad?

El uso de nuestro servicio Elements Vulnerability Management para analizar las tendencias de vulnerabilidad dentro de nuestra base de clientes muestra exactamente esto. Las vulnerabilidades de alta gravedad eran raras o inexistentes. La gran mayoría de las vulnerabilidades sin parchear que encontramos eran de gravedad baja a media. De estos, es interesante notar que las configuraciones incorrectas de TLS/SSL y OpenSSH fueron bastante comunes. Recuerde, sin embargo, que aunque están etiquetados como errores de configuración, es posible que estos sistemas se hayan configurado de esa manera para interoperar con el cliente, el socio o los servicios internos propietarios.

Nuestro Gerente de Seguridad de la Información, miembro de nuestra oficina de CISO, miró este gráfico y concluyó que si esto representara la situación en nuestra propia empresa, podría dormir por la noche.



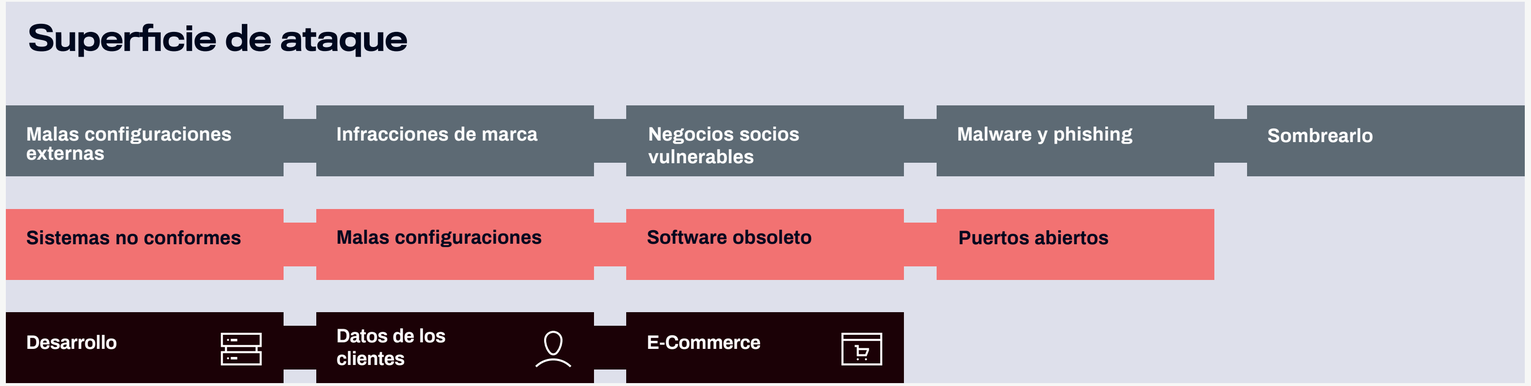
Los datos del gráfico se recopilaron durante los primeros 6 meses de 2018, sobre la base de clientes de WithSecure™, con nuestro producto Elements Vulnerability Management. WithSecure™ Elements Vulnerability Management es una solución de análisis de seguridad y gestión de vulnerabilidades que realiza análisis de vulnerabilidades de plataformas y aplicaciones web.

¿Cuáles son las consecuencias si no cuidas tu superficie?

Los riesgos

Establecer y luego mantener activamente la configuración segura de los sistemas de TIC debe verse como un control de seguridad clave. Los sistemas de TIC que no están bloqueados, fortalecidos o parcheados serán particularmente vulnerables a los ataques que pueden prevenirse fácilmente.

Las organizaciones que no producen ni implementan políticas de seguridad corporativas que gestionen la configuración y parches seguros de sus sistemas de TIC están sujetas a los siguientes riesgos:



Cambios no autorizados en los sistemas

Un atacante podría realizar cambios no autorizados en los sistemas o la información de las TIC, lo que comprometería la confidencialidad, la disponibilidad y la integridad.

Explotación de vulnerabilidades no parcheadas

New patches are released almost daily, and the timely application of security patches is critical to preserving the confidentiality, integrity, and availability of ICT systems. Attackers will attempt to exploit unpatched systems to gain unauthorized access to system resources and information. Many successful attacks are enabled by exploiting a vulnerability for which a patch has been issued prior to the attack taking place.

Explotación de configuraciones de sistemas inseguros

Un atacante podría explotar un sistema que no ha sido bloqueado o reforzado por:

- Obtener acceso no autorizado a activos de información o importar malware.
- Explotar funciones innecesarias que no se han eliminado o deshabilitado para realizar ataques y obtener acceso no autorizado a sistemas, servicios, recursos e información.
- Conectar equipos no autorizados para infiltrar información o introducir malware.
- Creando una puerta trasera para futuros esfuerzos maliciosos

Incremento en el número de incidentes de seguridad

Sin un conocimiento sobre las vulnerabilidades y la disponibilidad (o falta de disponibilidad) de parches y correcciones, el negocio se verá cada vez más afectado por incidentes de seguridad.

Las brechas de seguridad dañan más a las pequeñas empresas

Solo el 31 por ciento de las pequeñas empresas toman medidas activas para protegerse contra las infracciones de seguridad.

Además, el 41 por ciento de las pequeñas empresas desconoce los riesgos asociados con el error humano, y solo el 22 por ciento está dispuesto a mejorar sus medidas de seguridad el año pasado.

Puede que no le sorprenda que las brechas de seguridad perjudiquen más a las pequeñas empresas. Más del 70 % de los ataques se dirigen a pequeñas empresas, y se estima que el 60 % de las PYMES pirateadas cierran después de solo seis meses. Esta investigación puede estar un poco sesgada, ya que la cantidad de personas que ignoran la seguridad cibernética es alta. La gente todavía considera suficientes las medidas de seguridad tradicionales, como antivirus y cortafuegos.

El costo de la violación de datos es más alto de lo que piensa

La falta de conciencia, junto con la exposición a las amenazas, ha llevado a un aumento drástico en la cantidad de ataques: la proporción de ataques cibernéticos de violaciones de datos ha aumentado al 31 por ciento desde un mero 18 por ciento en 2014. Si cree que puede obtener lejos fácilmente después de un ataque, piénselo de nuevo. El costo de la recuperación es asombroso y, en la mayoría de los casos, conduce al cierre de negocios. El costo promedio de recuperación de filtraciones de datos de SMB es de $36 000 y puede ocasionar pérdidas de hasta $50 000. Esta cantidad puede incluso ser el valor total de las pequeñas empresas. La recuperación puede ser casi imposible si es víctima de una violación de datos.

Dado que la mayoría de las pequeñas empresas no pueden recuperarse después de las brechas de seguridad, siempre es bueno tener listas las medidas de precaución contra un ataque.

La discusión interna de la empresa sobre el riesgo cibernético

Cuando un CISO se acerca a la gerencia con una solicitud de presupuesto para una nueva tecnología o iniciativa de seguridad, es una reunión entre personas que hablan dos idiomas diferentes. El CFO y el CEO piensan en términos de cantidades monetarias: valor comercial y ROI. Sin esos números a los que referirse, el CISO debe convencer de alguna manera a la alta dirección de que la inversión es necesaria. El CISO recurre al único argumento al que responderán los ejecutivos: el miedo. “Si no hacemos esto, el cielo se nos va a caer encima”.

Después de todo, ninguna empresa quiere ser el próximo titular de noticias por las razones equivocadas.

Pero al final del día, ¿cómo sabe una empresa si sus inversiones en seguridad están reduciendo o eliminando los riesgos de manera efectiva en la medida en que sus ejecutivos esperan o imaginan que lo están? ¿El costoso programa de capacitación de los empleados, el sistema de monitoreo de eventos, el reemplazo del software de seguridad en toda la organización? ¿Cómo sabe una empresa si está invirtiendo en los lugares correctos o si ha adquirido el nivel adecuado de seguro para cubrirse adecuadamente en caso de una violación de datos, un incidente de ransomware o un ataque DDoS?

¿Y cómo muestra el CISO a la alta dirección lo importante que son estas inversiones para la empresa, sin recurrir a FUD (Miedo, Incertidumbre, Duda) para transmitir el mensaje?

La respuesta radica en poder cuantificar el impacto de una brecha cibernética en su empresa, la misma práctica que los CISO suelen evitar. Es cierto que el uso de sistemas de calificación ambiguos o el uso de códigos de color rojo, verde y amarillo para indicar los riesgos no le da mucho para continuar.

“La mayoría de los gerentes confían en la guía cualitativa de los 'mapas de calor' que describen su vulnerabilidad como 'baja' o 'alta' en base a estimaciones vagas que agrupan pérdidas pequeñas frecuentes y pérdidas grandes raras”, escriben Chacko, Sekeris y Herbolzheimer en Harvard Business Artículo de revisión “¿Puede poner una cantidad en dólares en el riesgo cibernético de su empresa?” del 5 de octubre de 2016. “Pero este enfoque no ayuda a los gerentes a comprender si tienen un problema de $10 millones o uno de $100 millones, y mucho menos si deben invertir en defensas de malware o protección de correo electrónico. Como resultado, las empresas continúan juzgando mal qué capacidades de seguridad cibernética deben priorizar y, a menudo, es posible poner números reales en sus evaluaciones de riesgos de seguridad cibernética. Es posible hablar en un idioma que la sala de juntas entienda.

“Implementar esta tecnología costará $100,000, pero reducirá nuestro riesgo en $2 millones”, o “Podemos reducir nuestra cobertura de seguro cibernético en $50 millones, y he aquí por qué”. Estas son afirmaciones que los CISO y los CFOS pueden hacer, y respaldar con confianza, con la ayuda de nuevas formas de medir y cuantificar los riesgos de seguridad cibernética. El método de WithSecure™ se llama Cyber.

Estudio sobre el costo de la filtración de datos de 2019: descripción general mundial

IBM Security and Ponemon Institute, estudio realizado entre julio de 2018 y abril de 2019.

507 compañías
estudiado globalmente

$3.92 millón
es el costo total promedio de la violación de datos

$150
es el costo promedio por registro perdido o robado

25,575
tamaño promedio de una violación de datos

279 días
es el tiempo promedio para identificar y contener una brecha

29,6%
es la probabilidad de sufrir una violación de datos en los próximos dos años

GDPR: ¿sanciones temibles o una oportunidad para elevar su organización?

Como si los costos de recuperación de una violación de datos no fueran suficientes, ahora también se debe considerar el costo de las posibles multas resultantes de la aplicación de GDPR. Según el RGPD, que entró en vigor en mayo de 2018 con el objetivo de proteger la privacidad de los datos de los ciudadanos de la UE, las empresas que sufran una filtración de datos podrían enfrentarse a multas de hasta el 4 % de la facturación anual, o 20 millones de euros (22,5 millones de dólares). cualquiera que sea mayor.

La directiva puede tener como objetivo fortalecer los derechos de privacidad de los ciudadanos de la UE, pero su alcance no se limita a Europa. Según el RGPD, cualquier empresa que procese, almacene o transmita datos personales pertenecientes a residentes de la UE debe cumplir, una delimitación amplia que afecta prácticamente a cualquier empresa con presencia en la Web. Y debido a que es probable que el RGPD establezca un estándar que otros países querrán seguir, tener políticas, procedimientos y tecnologías de la empresa a bordo es una buena idea, ya sea que una empresa se vea afectada técnicamente o no. Es probable que las leyes de privacidad de datos en todo el mundo se fortalezcan, no se debiliten.

Para observar la violación de Equifax a través de la lente del RGPD, se estima que los registros personales de más de 147,9 millones de personas quedaron expuestos. Si la empresa hubiera estado sujeta a GDPR y su plazo de 72 horas para informar una infracción descubierta, habría fallado miserablemente. Equifax descubrió la infracción el 29 de julio de 2017 y la reveló bastante más de un mes después, el 7 de septiembre. Con una facturación anual de más de $3 mil millones, un cálculo aproximado basado en la pena máxima revela que Equifax podría haber enfrentado potencialmente más de cien millones en multas.

En cuanto a la seguridad, el RGPD no detalla requisitos específicos para mantener los datos seguros. Pero debido a que la implementación de prácticas de seguridad sólidas es fundamental para proteger los datos y cumplir con las normas, debe implementarse un programa de seguridad integral que abarque la predicción de amenazas, la prevención y la detección y respuesta de infracciones. La gestión eficaz de vulnerabilidades, como ilustra el caso de Equifax, es una parte fundamental de ese programa y del cumplimiento del RGPD.

Otro aspecto importante del RGPD es el inventario de datos: saber qué está almacenando, dónde lo está almacenando y dónde se encuentran varias copias de datos en la infraestructura de su empresa. Descubrir y documentar la máquina donde pueden residir los datos es el primer paso en este proceso. Las capacidades de escaneo de descubrimiento de WithSecure™ Element Vulnerability Management pueden ayudarlo a encontrar y mapear sus activos de red y la sombra de TI. Un conjunto de servidores por el departamento de marketing para la campaña del año pasado, por ejemplo, puede contener información del cliente que no forma parte de los procesos de GDPR de la empresa.

En definitiva, el RGPD es una realidad que debe abordarse de dos maneras: como una sanción temible que debe evitarse cumpliendo los requisitos mínimos de cumplimiento; o como una oportunidad para apreciar sus objetivos y elevar de manera proactiva su organización a donde debería estar en nuestro mundo cada vez más impulsado por los datos.

¿Qué ofrece Elements Vulnerability Management?

La mejor respuesta ante amenazas es predecir y mapear sus amenazas de ciberseguridad. Ninguna otra tecnología lo hace mejor que la gestión de vulnerabilidades.

La superficie de ataque de una organización atraviesa todas las infraestructuras de red, software, IOT y aplicaciones web internamente y en Internet global. Incluye una comprensión de todos los puntos de interacción. Los administradores de seguridad de la información deben poder abordar la evaluación de vulnerabilidades desde varias perspectivas para obtener una evaluación precisa de los riesgos, minimizar las amenazas a la seguridad y mantener el cumplimiento.

A diferencia de cualquier otra solución de vulnerabilidad en el mercado, WithSecure™ Elements Vulnerability Management cuenta con tecnología de rastreo web, llamada Internet Asset Discovery, que también cubre la web profunda. Elements Vulnerability Management le permite navegar fácilmente a través de todos los objetivos para identificar rápidamente los riesgos y las conexiones potencialmente vulnerables, y expandir el análisis de la posible superficie de ataque más allá de su propia red.

Identificar y exponer las posibles amenazas.

Las marcas y la propiedad intelectual exitosas a menudo convierten a las empresas en el blanco de actividades fraudulentas o maliciosas. Con un poco de experiencia con Elements Vulnerability Management, cualquier administrador de seguridad de TI puede generar un informe de evaluación de amenazas relacionado con actividades como la violación de la marca o los sitios de phishing destinados a estafar o infectar a los visitantes.

WithSecure Elements Vulnerability Management identifica los activos de su organización y señala exactamente dónde son vulnerables, lo que le permite minimizar su superficie de ataque y reducir el riesgo. Con Elements Vulnerability Management, su equipo de seguridad de TI mapea la superficie de ataque de su organización en el agregado de:

- todas las vulnerabilidades conocidas, desconocidas y potenciales críticas para el negocio
- control en todo el software, hardware, firmware y red
- Shadow IT, sistemas externos mal configurados, sitios web de malware, hosts vinculados a sitios web
- entropía de seguridad de socios y contratistas
- infracciones de marca y phishing

Tablero de gestión de vulnerabilidades

Manténgase al tanto del estado actual de vulnerabilidades e incidentes, prepare informes estándar y personalizados sobre riesgos y cumplimiento, y más

Descubrimiento de activos de Internet

Enumere los posibles vectores de ataque con una evaluación de amenazas web y de Internet

Exploraciones de descubrimiento

Mapee su superficie de ataque con escaneo de redes y puertos.

Exploraciones de vulnerabilidad

Escanear sistemas y aplicaciones web en busca de vulnerabilidades conocidas públicamente

Agente de punto final de gestión de vulnerabilidades

Recopile automáticamente datos de todos sus puntos finales

Gestión de vulnerabilidades

Recopile automáticamente datos de todos sus puntos finales de forma centralizada con alertas de seguridad y análisis forense

Cumplimiento Pci dss

Garantice el cumplimiento de las normativas actuales y futuras para reducir el riesgo de pérdida de datos

Descubrimiento de activos de Internet

Puede encontrar los sistemas orientados a Internet de su organización en Elements Vulnerability Management con detección de Internet. La detección de Internet utiliza el rastreo y la asignación de puertos para permitirle recopilar datos en sistemas públicos. Puede buscar datos según la ubicación, el dominio de nivel superior, el dominio de nivel de pago, las palabras clave, el nombre de host y la dirección IP.

Puede agregar los hosts descubiertos a un grupo de escaneo para el escaneo de vulnerabilidades mediante el escaneo pasivo o activo. Los escaneos pasivos buscan vulnerabilidades sin conectarse al host de destino. El escaneo activo ejecuta un escaneo regular del sistema en el host. El descubrimiento de activos de Internet incluye todo esto:

- Enumeración de superficie de ataque
- BGP (IP to AS)
- Fuentes públicas (RIPE, BGP público, CERNET)
- IP e información de servicio
- Escaneo de puertos y pancartas
- Nombres de dominio
- DNS inverso, transferencia de zona, fuerza bruta
- Información de quién es
- Uniendo todo lo anterior
- Geolocalización
- Bases de datos públicas/privadas

Exploraciones de descubrimiento

Elements Vulnerability Management Discovery es responsable del primer paso en el proceso de flujo de trabajo de gestión de vulnerabilidades y auditoría de seguridad. Le permite descubrir hosts y dispositivos de red en su infraestructura (dentro de rangos de red definidos).

El análisis de descubrimiento utiliza técnicas de análisis ICMP PING/TCP SYN/UDP/análisis de fragmentos para enumerar todos los hosts disponibles en una red. Además, enumera los servicios que cada host está exponiendo y qué sistemas operativos están ejecutando.

El rango de IP es la única información de entrada necesaria para realizar un análisis de descubrimiento de red. Las otras opciones de configuración son las siguientes:

- Escaneo de puertos TCP y definición del rango de puertos
- Escaneo de puertos UDP y definición del rango de puertos
- Limitar el rango de puertos a los 100 o 1000 puertos abiertos más comunes
- Habilitación de la detección de los servicios en los hosts descubiertos
- Detección del sistema operativo en cada host en vivo
- Escaneo de hosts que no responden a la solicitud PING
- Controle el rendimiento del escaneo agregando un tiempo de retraso adicional entre los paquetes subsiguientes enviados
- Controle la cantidad de subprocesos simultáneos utilizados durante el escaneo

El resultado de un escaneo de descubrimiento de red es un informe con la lista de todos los objetivos escaneados con todos los servicios detectados, acompañado de información adicional según las opciones que se utilicen.

En el caso de que el único propósito del análisis sea determinar si el host está vivo, no los servicios que está ejecutando, se puede habilitar el "modo de descubrimiento". El procedimiento de escaneo en modo de descubrimiento, para cada host en el alcance, incluye resolución ARP (en segmentos locales), ICMP PING y un escaneo de puerto limitado de los puertos predeterminados para SSH, HTTP, HTTPS y servicios de escritorio remoto. Si alguno de ellos indica que el host está activo, el escaneo marca el host como activo y continúa con el siguiente objetivo.

Escaneos del sistema

El escaneo del sistema es un escáner de vulnerabilidades basado en la red que puede escanear cualquier sistema con una IP El escaneo del sistema es un escáner de vulnerabilidades basado en la red que puede escanear cualquier sistema con una IP

Nota: El análisis del sistema no es disruptivo y está diseñado para no causar condiciones de denegación de servicio en sus sistemas.

Cuando inicia una exploración del sistema, primero realiza una exploración del puerto del objetivo y, una vez que se han identificado todos los puertos abiertos (servicios), se evalúan en busca de vulnerabilidades. Estos son solo algunos de los sistemas que se pueden examinar con análisis de sistemas:

- Servidores web
- Firewalls
-
- Enrutadores y conmutadores
- Controladores de dominio
- Servidores DNS
- Puertas de enlace antivirus
- Estaciones de trabajo

Las comprobaciones que ejecuta el escáner incluyen las siguientes:

- Detección de servicios y descubrimiento del sistema operativo (UDP/TCP/ICMP)
- Pruebas de vulnerabilidades y configuraciones incorrectas en los servicios
- Pruebas de vulnerabilidades y configuraciones incorrectas en los sistemas operativos
- Pruebas de vulnerabilidades y configuraciones incorrectas en dispositivos de red
- Pruebas de configuración segura (SSL/SSH)
- Detección de contraseñas predeterminadas (sistemas operativos/servicios/red/dispositivos)

Todas las vulnerabilidades se informan con una puntuación CVSSv2, CVE, BID, BugTraq y otras referencias cuando están disponible.

Escaneos web

Los escaneos web le permiten examinar y probar aplicaciones web. Puede utilizar exploraciones web durante el desarrollo de nuevas aplicaciones como parte del ciclo de vida del desarrollo. Dado que las vulnerabilidades se descubren en las primeras etapas del proceso de desarrollo, el costo y la cantidad de recursos necesarios para mitigar las vulnerabilidades en una etapa posterior se reducen significativamente.

El escaneo web se considera un escaneo complementario, que se puede aplicar sobre un escaneo del sistema existente. En otras palabras, se recomienda que cada vez que escanee un objetivo con un Escaneo del sistema, los sistemas con aplicaciones web también se escaneen con un Escaneo web.

Definición de objetivos para escaneos web

Cuando defina la URL de destino para un escaneo web, tenga en cuenta que el descubrimiento automatizado de sitios (rastreo y lo que realmente se está escaneando) se limita a las ubicaciones que tienen:

- el mismo número de puerto que el objetivo de escaneo definido (es decir, puerto 80 - predeterminado para http:// .. , puerto 443 - predeterminado para https:/ , puerto 8080 - si se especifica explícitamente así: https://www.algún-sitio.com:8080/)
- el mismo protocolo que el objetivo de exploración definido (en otras palabras, si especifica la URL http://www-company.com, a exploración no explora automáticamente https://www.company.com además)
- el mismo FQDN definido en el destino del análisis (en otras palabras, si especifica la URL https://service.com, el análisis no cubre automáticamente el contenido disponible en https://www.service.com)

Esto es para proteger contra el escaneo de algo que el cliente no tiene la intención de escanear. Por ejemplo, http://www.bank.com puede consistir en un sitio web oficial de un banco con información genérica. Mientras que https://www.bank.com puede albergar un servicio completamente diferente, por ejemplo, la banca en línea, el mismo escaneo web no tiene necesariamente la intención de escanear ambos.

Aplicaciones web personalizadas

Antes de crear un escaneo web nuevo, primero debe comprender las situaciones en las que será efectivo. Como regla general, solo debe escanear aplicaciones web personalizadas. Si tiene un sistema que ejecuta una implementación estándar de WordPress (sin ningún módulo personalizado instalado), por ejemplo, no tiene sentido escanearlo con un escaneo web, porque los escaneos del sistema pueden detectar la versión de WordPress y cualquier vulnerabilidad conocida. Sin embargo, si sabe que su WordPress contiene módulos desarrollados a medida, tiene sentido escanearlo con escaneos web y del sistema. Tenga en cuenta que solo necesita escanear el código o módulo personalizado, y no todo el sitio web.

Estamos usando ambas categorías: las 10 principales y las 55 estáticas

Los escaneos web detectan vulnerabilidades de seguridad dentro de aplicaciones web comerciales y personalizadas, probando numerosas vulnerabilidades, incluido OWASP Top 10.

- Un escáner de aplicaciones web: capaz de identificar vulnerabilidades en aplicaciones personalizadas
- Admite autenticación simple basada en formularios
- Soporta rastreo asistido (grabaciones)
- Escalable para cubrir necesidades en expansión
- Herramienta de escaneo PCI ASV certificado

Además de los 10 primeros, WithSecure™ Elements Vulnerability Management también hace referencia a las 55 categorías estáticas de clasificación de amenazas definidas por el Consorcio de seguridad de aplicaciones web (WASC).

La clasificación de amenazas WASC es un esfuerzo cooperativo para aclarar y organizar diferentes amenazas a la seguridad de sitios web. Los miembros del Consorcio de seguridad de aplicaciones web crearon el proyecto para desarrollar y promover la terminología estándar de la industria, de modo que los desarrolladores de aplicaciones, los profesionales de seguridad, los proveedores de software y los auditores de cumplimiento tengan acceso a un lenguaje y definiciones coherentes para los problemas relacionados con la seguridad web.

Agente de nodo de exploración

Scan Node Agent es un componente de gestión de vulnerabilidades de WithSecure™ Elements que administra todos los procesos de escaneo que se ejecutan en el nodo de escaneo.

Protege todos los trabajos de análisis (la lista de análisis del sistema, web y de detección) y se pone en contacto con el Panel de administración de vulnerabilidades, comprobando si hay nuevos trabajos de análisis esperando en la cola.

El Scan Node también tiene su propia capacidad y sabe cuántos escaneos simultáneos puede ejecutar en un momento dado según las configuraciones. Una vez que finaliza un análisis, el agente del nodo de análisis envía el informe de vuelta al panel de administración de vulnerabilidades y elimina todos los datos de análisis temporales del nodo, incluidos el informe y el registro del análisis. Es muy importante tener en cuenta que el nodo de exploración no almacena ningún dato de vulnerabilidad una vez que se ha completado la exploración.

Es un componente de gestión de vulnerabilidades de elementos que se puede intercambiar, mediante la reinstalación, en cualquier momento cuando no haya análisis en curso.

El Scan Node Agent se ejecuta como un servicio en elsistema operativo, y se implementa y envía junto con una aplicación adicional para los administradores del sistema que les permite obtener una vista previa del nodo de escaneo, es decir, los detalles de los escaneos que se ejecutan actualmente en el nodo.

Agente de gestión de vulnerabilidades de elementos

Cuando se trata de identificar y corregir vulnerabilidades en su red interna, existen dos enfoques que compiten (pero no se excluyen mutuamente). Existe el enfoque más tradicional, ejecutar escaneos de red internos en una caja conocida como "dispositivo" de escaneo (un nodo de escaneo) que se implementa en su infraestructura. Luego está el enfoque aún más moderno, que ejecuta "agentes" en sus dispositivos que informan a un servidor central.

Las herramientas de exploración de vulnerabilidades, como Elements Vulnerability Management, generalmente usaban un enfoque de exploración basado en la red. El nodo de exploración estaba evaluando la postura de seguridad de los dispositivos restantes mediante la ejecución de una exploración de vulnerabilidades a través de la red, con o sin autenticación. Esta forma tradicional de escaneo tiene sus propias limitaciones que el escaneo basado en agentes puede superar.

Elements Vulnerability Management admite ambas formas de realizar escaneos de vulnerabilidades y brinda la capacidad al usuario del portal para administrar vulnerabilidades utilizando una vista de activos común, independientemente del método utilizado para recopilar los hallazgos de vulnerabilidad.

Los beneficios del escaneo basado en agentes son numerosos:

- Brinda capacidades extendidas de análisis de vulnerabilidades basadas en endpoints.
- Simplifica las configuraciones de redes, ya que se necesitan menos reglas de red para permitir el análisis de Elements Vulnerability Management. No es necesario abrir las puertas a su propiedad más valiosa: los dispositivos.
- Dispositivos volátiles. Facilita el escaneo de puntos finales que residen fuera de la red de la empresa, por ejemplo, trabajo remoto.
- Inventario detallado, incluso con direcciones IP que cambian dinámicamente.
- Implementación sencilla sobre el producto WithSecure™ Elements existente, ya que el agente forma parte del agente unificado para puntos finales de Elements.
- Las capacidades integradas de administración de parches están disponibles con el cliente, cuando el cliente compra/posee suscripciones de Elements Endpoint Protection.

¿Qué analiza el agente de gestión de vulnerabilidades de Elements?

El contenido del análisis del Agente de gestión de vulnerabilidades de Elements es similar al SystemScan autenticado con la exclusión de los hallazgos de vulnerabilidades que solo se pueden probar mirando el cuadro desde el punto de vista de la red. Un ejemplo de dicho hallazgo es la configuración incorrecta de SSL/TLS clpher sultes en su servidor web. Los hallazgos típicos incluyen:

- lista de puertos abiertos
- lista de hardware
- lista de programas
- vulnerabilidades relacionadas con el software instalado
- vulnerabilidades relacionadas con el sistema operativo

Administración

La página de administración de cuentas le permite controlar el acceso de los usuarios a la administración de vulnerabilidades de elementos utilizando los principios de control de acceso basado en roles (RBAC). La gestión de usuarios en Elements Vulnerability Management implica tres conceptos: Usuarios, Grupos de usuarios y Roles.

Usuarios

La página de administración de cuentas le muestra una lista de todos los usuarios con acceso a su cuenta de Elements Vulnerability Management. En esta página puede revisar los usuarios y a qué tienen acceso y, por supuesto, agregar o eliminar usuarios

Grupos de usuarios

Los grupos de usuarios actúan como un contenedor para uno o más usuarios. Con los grupos, puede tener acceso y con qué permisos (roles). La columna de problemas del usuario le muestra a qué grupo pertenece cada usuario de la lista.

Roles

Los roles se usan para definir el contenido al que puede acceder un usuario. Por ejemplo, puede crear funciones como “Solo lectura”, “Propietario del sistema” y “Administrador”. Para ver y editar los roles de su cuenta de Elements Vulnerability Management, haga click en el botón del menú de administración de cuentas y seleccione administrar roles.

Reportando

La generación de informes es otra parte extremedamente vital del panel de Vulnerability Management. Con Elements Vulnerability Management puede generer informes personalizados que se adapten a las necesidades de su gerente, administrador del sistema o su proveedor de servicios externo.

Puede crear su propio informe en la página Informes. Una vez que se crea el informe, se agrega a la lista en la página Informes resumidos. Puede ver cada informe en varios formatos:

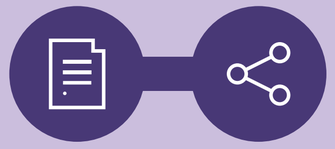
- **XML:** descargue los datos del informe sin procesar en formato XML.
- **Informe de Word agrupado por hosts:** Contiene todos los detalles técnicos de los hosts en el alcance, organizados por el host. Esto es útil cuando su alcance no cubre una gran cantidad de hosts.
- **Word reportado agrupado por vulnerabilidades:** Contiene todos los detalles técnicos de los hosts en alcance, organizados por tipo de vulnerabilidad. Esto le da un informe más pequeño si el alcance es muy grande.
- **Informe de Excel agrupado por vulnerabilidades:** contiene todos los detalles técnicos del host en el alcance y le brinda la libertad de usar las funciones disponibles en Excel.
- **Informe de Word, resumen ejecutivo:** diseñado para ser un informe liviano con unas pocas páginas, incluso si el alcance del informe de resumen cubre miles de hosts.

Nota: Después de generar un informe, crea una instantánea del estado actual de sus vulnerabilidades. Para actualizar el informe, haga clic en el icono de menú en la columna de acciones y seleccione Actualizar datos del informe. Seleccione Crear un nuevo informe basado en esto si no desea sobrescribir el informe existente.

Propuesta de valor

Estratégico
Proteger la marca evitando incidentes
Cumple con las normas
La seguridad es igual a la calidad y se aplica a cualquier oferta

Tácticas
Gestion de seguridad



Ejecución
Capacidades de detección de vulnerabilidades para protege los sistemas
Desarrollar aplicaciones seguras

Obtener visibilidad de sus entornos

Los mayores temores de cualquier empresa incluyen el daño a la reputación, la publicidad negativa y la pérdida de confianza debido a la incompetencia o la negligencia. Además de lo anterior, otras consecuencias negativas incluyen la pérdida de productividad, la desintegración de la ventaja competitiva de una empresa debido al robo de propiedad intelectual clave y posibles violaciones regulatorias asociadas con el RGPD.

Lo que necesita es visibilidad de la superposición entre las vulnerabilidades de sus entornos y los agujeros de seguridad que se explotan en la naturaleza. Además, debe centrarse en las vulnerabilidades con mayor impacto en su negocio y priorizar primero los problemas en estos entornos.

Complete threat management, done by WithSecure™ Elements Vulnerability Management

WithSecure™ Elements Vulnerability Management es un servicio de análisis y gestión de vulnerabilidades operado por WithSecure™ Corporation. WithSecure™ Elements Vulnerability Management está disponible como una solución de servicio basada en la nube (SaaS) o como una solución in situ. Elements Vulnerability Management consta de los siguientes componentes:

- Agente de gestión de vulnerabilidades
- Nodos de exploración de Elements Vulnerability Management
- Panel de administración de vulnerabilidades

Los nodos de escaneo realizan el escaneo real. El panel de administración de vulnerabilidades administra y coordina los nodos de escaneo, recopila los resultados y proporciona informes de los hallazgos.

WithSecure™ Elements Vulnerability Management detecta debilidades y amenazas de inmediato, lo que aumenta la seguridad de la red y las aplicaciones y garantiza el cumplimiento normativo. Los informes centralizados sin precedentes y el análisis en profundidad mejoran de forma eficaz la gestión de la seguridad

WithSecure™ Elements Vulnerability Management

Visibilidad integral

Mapeo de seguridad efectivo a través del descubrimiento y mapeo preciso de todos los activos, sistemas y aplicaciones en la red y más allá.

Gestión optimizada de la productividad y la seguridad

Resuelva rápidamente los problemas en múltiples dominios con un flujo de trabajo de servicio eficiente, que incluye monitoreo de vulnerabilidades, escaneos programados automatizados y emisión de tickets para corrección y verificación prioritarias.

Gestión de seguridad optimizada

Integración simplificada con un flujo de trabajo de servicio eficiente y un sistema de emisión de tickets que monitorea las vulnerabilidades con análisis programados automatizados y las asigna para la aplicación de parches prioritaria y la coordinación con los administradores del sistema (por ejemplo, Service Now)

Informes sobre el riesgo

Produzca informes con información creíble sobre la postura de seguridad de su organización a lo largo del tiempo. Muestre y justifique cómo la seguridad de TI permite la continuidad del negocio.

Costos reducidos

La gestión de vulnerabilidades puede reducir significativamente el costo de la seguridad. Es menos costoso lidiar con la seguridad antes de problemas serios que durante una crisis o recuperación de incidentes. Además, los recursos en la nube de Elements Vulnerability Management permiten a las organizaciones reducir sus gastos.

Garantizar el cumplimiento de la normativa actual y futura

WithSecure™ Elements Vulnerability Management cumple con los requisitos de análisis de vulnerabilidades PCI ASV. Somos su socio con sede en la UE que cumple con las regulaciones de la UE. Cuando usa WithSecure™ Elements Vulnerability Management, logra el cumplimiento con una solución de escaneo PCI ASV aprobada y cumple con PCI con un socio de Qualified Security Assessor (QSA). Realice pruebas periódicas e identifique nuevas vulnerabilidades. Genere informes fáciles de usar para todos los usuarios.

Quienes 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 enfrentar ataques en vivo. Nuestros consultores se asocian con empresas y desafíos tecnológicos 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™ forma parte de F-Secure Corporation, fundada en 1988 y cotiza en NASDAQ OMX Helsinki Ltd.

WITH secure