opentext™

Informe

Respuesta proactiva con OpenText EnCase:

La guía del líder de seguridad para aprovechar al máximo la tecnología EDR – Protección Proactiva

Los equipos de seguridad tienen la tarea de proteger a las empresas de los ciberatacantes, que son cada día más capaces de poner en riesgo las terminales y acceder a los datos confidenciales de una organización. Hoy más que nunca, estos equipos de seguridad necesitan tecnología de seguridad proactiva (EDR) efectiva para combatir con éxito a sus adversarios digitales. Este informe es una guía práctica para abordar los obstáculos en las operaciones de ciberseguridad, como la falta de personas calificadas para responder a incidentes o el exceso de alertas de seguridad, y las soluciones y técnicas que los líderes de seguridad pueden utilizar para responder a una amenaza de cualquier tipo.

opentext™

Contenido

opentext™

El 56,8 % de las personas encuestadas que responden a incidentes informó que el mayor obstáculo para lograr una respuesta a incidentes (IR) efectiva en una organización es la **"falta de personal y competencias"**

Resumen ejecutivo

Los adversarios digitales modernos tienen más acceso que nunca a herramientas, tácticas y procedimientos avanzados. Esto genera un aumento de la efectividad a la hora de poner en riesgo las redes empresariales y robar datos confidenciales. Una nueva investigación del Instituto SANS indica que la limitación de recursos está alcanzando un punto crítico, y menciona que un **77,3 % de los equipos de respuesta a incidentes de seguridad está conformado por cinco miembros o menos.**[1] Dada esta realidad, queda claro que los líderes de seguridad deberían esperar más de su tecnología EDR para poder combatir con éxito a los adversarios digitales, que sacan provecho de una situación que ya es muy beneficiosa para ellos.

Aunque los atacantes son cada vez más capaces de poner en riesgo las terminales e infiltrarse en las máquinas que los grupos de IR deben proteger, **los equipos de seguridad pueden hacerle frente con *confianza* y de forma *exhaustiva*** a cualquier amenaza informática con OpenText™ EnCase™, ya sean ataques generales o dirigidos.

Proteger a las empresas modernas exige hacer más con menos

Escasez de recursos y preocupaciones a largo plazo para los líderes de seguridad

Recientemente un informe del Instituto SANS patrocinado por OpenText demuestra como es casi imposible la tarea de proporcionar seguridad a una organización con recursos limitados. Se encuestaron a conocedores y expertos de la industria acerca de cuestiones específicas de los equipos de IR y el centro de operaciones de seguridad (SOC), así como sobre éxitos notables, debilidades y nuevos patrones para considerar y un inventario general de incidentes y su respuesta a los mismos (IR). El resultado provee un panorama sumamente importante y preciso de la situación de ciberseguridad actual.

El 56,8 % de los encuestados indicó que el mayor obstáculo para lograr una Respuesta a Incidentes efectiva en sus organizaciones es la falta de personal y competencias.[2] Esta es una preocupación conocida y documentada en el sector, pero no obtuvo la atención suficiente y por ende la inversión requerida además del SOC.

Aunque esté relacionada, la preocupación sobre los recursos señalada por el Instituto SANS es un problema que tiene dos causas diferentes:

1. **No hay suficientes personas.** No hay suficiente energía humana en la organización de seguridad empresarial, lo que se puede apreciar en las vacantes laborales y para los roles de seguridad.
2. **No hay suficientes personas capacitadas.** Muchas veces los candidatos considerados no cuentan con todas las competencias ideales para los roles de seguridad vacantes, y los líderes de seguridad están dispuestos a incorporar a candidatos con menor experiencia.

Las empresas de ciberseguridad predicen **que habrá 3,5 millones de ofertas laborales en ciberseguridad en el 2021**[3], lo que confirma aún más la falta de personal humano. En América del Norte, una explicación posible es que las universidades reconocidas comenzaron a incorporar títulos relacionados con los campos de la ciberseguridad hace poco. La mayoría de los programas son nuevos y prometedores, pero actualmente no generan la suficiente cantidad de candidatos para ocupar los puestos de trabajo de ciberseguridad disponibles en todo el mundo. Esto hace que los líderes de seguridad tengan puestos disponibles que quedan vacantes por semanas, meses o incluso años.

La falta de candidatos completamente calificados generó una falta de competencias, y representa un obstáculo para lograr un Respuesta a Incidentes efectiva. Los líderes de seguridad están ajustando las prácticas de contratación para ser más inclusivas con respecto al personal de seguridad menos calificado o sin experiencia. Esto significa que los equipos tienen una población con menos experiencia y conocimientos técnicos en

relación con años anteriores, lo que genera una falta de contribución de sus miembros, algo a lo que los líderes de seguridad deben adaptarse y sobreponerse. Es interesante remarcar que la falta de personal de IR calificado generó un aumento de asociaciones con servicios confiables de consultoría de seguridad de terceros como una solución a corto plazo para los problemas de falta de personal.

> La detección de terminales y la tecnología de respuesta pueden y deben usarse para disminuir la carga de trabajo de seguridad cuando se tiene en cuenta la falta actual de personal de Respuesta a Incidentes calificado. Los líderes de seguridad pueden volver a inclinar la balanza a su favor en la lucha contra los adversarios digitales modernos si priorizan y seleccionan la información de seguridad más importante y automatizan las tareas manuales y repetitivas.

Además, existe otro indicador de la escasez de recursos en el SOC: el 48,2 % de los encuestados en la misma encuesta de respuesta a incidentes realizada por el Instituto SANS informó que la falta de presupuesto para herramientas y tecnología fue uno de los obstáculos principales para lograr una IR efectiva en su organización.[4] Como el equipo de Seguridad de la Información posee tan solo un 10 % o menos del presupuesto general de TI, que es una fracción del presupuesto general empresarial, los directores de seguridad de la información (CISO) son los últimos en recibir recursos que ayuden a su causa.[5]

Aun así, el grupo de Seguridad de la Información es el responsable de *proteger y defender* la propiedad intelectual de la organización y los datos confidenciales de los clientes y empleados, gestionar el cumplimiento y, cuando corresponda, las demandas de los auditores. El grupo también debe evitar una falla de seguridad importante que dé como resultado la pérdida de confianza del consumidor, multas y daños potencialmente irreparables a la marca. Los presupuestos deben inclinarse a inversiones asociadas a las ganancias de la organización y del líder de seguridad. Debido a que los equipos de seguridad siempre están defendiendo los ingresos y luchan para evitar pérdidas y robos en lugar de generar nuevos ingresos netos para la empresa, la batalla siempre será cuesta arriba.

Cómo mejorar las probabilidades de aumentar los recursos de Seguridad de la Información

- Los líderes de seguridad deben trabajar para mejorar las "habilidades interpersonales" en la empresa que dan lugar a conversaciones que educan a las partes interesadas de las áreas adyacentes de la empresa.
- Realice un seguimiento de las métricas y los KPI que el consejo pueda entender y valorar
- Describa los riesgos de forma precisa y realista a la alta gerencia.
- Tenga un plan para aprovechar de forma eficiente los recursos que llegan al equipo de Seguridad de la Información desde el primer día

opentext™

Detalles de la falla de seguridad de Target

- Los atacantes accedieron a la red de Target a través de un proveedor independiente con un correo electrónico inicial de suplantación de identidad.
- Se utilizó un software malicioso para obtener las credenciales de acceso.
- La tecnología de alerta identificó correctamente la actividad sospechosa de los hackers.
- Debido a la "gran cantidad de eventos técnicos", el equipo de Seguridad de la Información no detectó la alerta.[6]
- El ataque continuó sin ser detectado y creció hasta convertirse en una filtración de datos, que afectó a 70 millones de personas aproximadamente.[7]

Escasez de recursos e impactos en el mundo real

La brecha de seguridad en 2013 de Target nos recuerda que los problemas que los grupos de seguridad tenían que solucionar en ese año aún existen y pueden generar un impacto significativo en la actualidad. Un estudio minucioso de la incidencia de brechas de las organizaciones en el pasado puede ayudar a consolidar las defensas para un futuro más seguro y garantizar que las organizaciones sepan en qué concentrarse y a dónde dirigir su atención.

Si un riesgo no se soluciona, este seguirá creciendo y dañando las redes de TI hasta que eventualmente se transforme en una filtración de datos. Si alguien roba información confidencial, se pone en riesgo la confianza en la marca, y las organizaciones deberán enfrentar sanciones por incumplimiento de las normas y comenzar un largo y arduo proceso de recuperación.

Todas las situaciones de riesgo deben tratarse, y todos los esfuerzos destinados a anticipar los problemas de recursos o de personal traerán beneficios inmediatos y a largo plazo para los líderes de seguridad. La triste realidad es que las situaciones de riesgo son un hecho cotidiano que el SOC trata de resolver. Las situaciones de riesgo no necesariamente equivalen a una filtración de datos instantánea o grave, pero si no se descubren, es posible que termine sucediendo.

La buena noticia es que existe tecnología para abordar esos problemas y ayudar a aliviar la inminente sensación de preocupación y ansiedad relacionada con la visibilidad y validación de los eventos de seguridad.

El papel de la tecnología EDR en el abordaje de la eficacia en las competencias del equipo

Si bien son efectivas contra las vulnerabilidades tradicionales, las tecnologías de seguridad de protección del perímetro no garantizan la prevención total de amenazas. Las tecnologías de prevención dependen de la historia y el contexto para tener éxito. Las vulnerabilidades tradicionales del pasado aún existen, y las tecnologías de prevención que supervisan las amenazas tradicionales y conocidas son una capa importante en una estrategia de seguridad exitosa.

Cuando hablamos del delito informático actual, los ataques avanzados y dirigidos son el principal medio para causar un daño. Los ataques avanzados y dirigidos suelen aprovechar las tácticas de ingeniería social, con un reconocimiento extenso, múltiples

opentext™

No hay suficiente tiempo en un día o suficiente energía humana disponible para que los equipos de seguridad gestionen las cargas de trabajo cómodamente ***sin*** **la ayuda de la tecnología EDR.**

tácticas de infiltración, comando y control con credenciales comprometidas, escalación de privilegios y, por último, filtración de datos. En otras palabras, las tecnologías de prevención existen para abordar las vulnerabilidades tradicionales y son menos efectivas contra los nuevos ataques avanzados o dirigidos de día cero.

Los líderes de seguridad inteligentes abordan las amenazas de día cero, los ataques avanzados persistentes infiltrados con malware (APT), el robo de infiltrados con privilegios y los ataques avalados por el estado con tecnología de detección y respuesta de terminales (EDR). EDR es la última línea de defensa de una organización contra el robo digital y se centra en descubrir y solucionar una situación de riesgo inofensiva antes de que se transforme en una filtración de datos intrusiva.

Detección de amenazas y la necesidad de visualizar las terminales de forma continua

Si bien este informe se centra en la respuesta proactiva, la cuestión es simple: las organizaciones no pueden responder a una amenaza que no pueden detectar. Los equipos de seguridad deben verlo todo, aunque esto signifique encargarse del resultado de gestionar demasiadas alertas de seguridad. Los líderes de seguridad no pueden arriesgarse a no detectar una amenaza, aunque sea "una aguja en un pajar", ya que puede convertirse en un problema de seguridad grave.

La investigación industrial adicional que realizó el equipo Verizon Risk Team en su informe anual Data Breach Investigations Report indicó que el 56 % de las brechas de seguridad eventuales tardan semanas o incluso meses en desarrollarse y no son detectadas por los equipos de Seguridad de la Información.[8] Todos los esfuerzos destinados a reducir el tiempo promedio de detección (tomar conciencia de una vulnerabilidad de seguridad) y el tiempo promedio de respuesta (habilitación segura de un servidor previamente comprometido) traerá beneficios para los líderes de seguridad en su búsqueda del éxito.

Detección de amenazas con OpenText EnCase

- Reglas en función de políticas para la detección de ataques avanzados y dirigidos
- "Disparadores" conductuales que indican una situación de riesgo para las terminales
- Personalización en la detección de anomalías
- Unificar detecciones y eventos de otras fuentes y EnCase como un solo panel con el SIEM, IPS, IDS y tecnologías de alerta para responder a incidentes

Los líderes de seguridad deben pecar de cautelosos y tratar de que la visibilidad y detección de amenazas sean totales. Si bien esto puede no ser completamente posible en el presente como metodología y principio rector, sí permitirá encontrar más eventos y detecciones que requieran respuestas que podrían convertirse en un desastre si no se solucionan. Una vez que un equipo de seguridad alcanza la visibilidad máxima y detecta casi la totalidad de las amenazas posibles, ***tendrá demasiadas alertas.*** Esta es una consecuencia inevitable de la visibilidad y constituye un problema que se debe abordar, ya que genera una cantidad exorbitante de eventos de seguridad.

El SOC promedio recibe 10.000 alertas de seguridad por día, 80% de las cuales son falsos positivos.[9] Muchas empresas y organizaciones de gran tamaño informan cifras mucho mayores y el 27 % de los equipos de TI enfrentan más de un millón de amenazas por día.[10] En promedio, los equipos de Respuesta a incidentes están integrados por 2 a 5 miembros, y con esa información en mente, los cálculos no cuadran.[11] Simplemente no hay suficiente tiempo en un día o suficiente energía humana disponible para que los equipos de seguridad gestionen las cargas de trabajo cómodamente ***sin*** **la ayuda de la tecnología EDR.**

opentext™

Respuesta proactiva con OpenText EnCase Endpoint Security

Con OpenText™ EnCase™ Endpoint Security, los equipos de Respuesta a incidentes con o sin experiencia pueden hacerle frente con confianza y de forma exhaustiva a cualquier amenaza, así como a las vulnerabilidades tradicionales, los ataques externos dirigidos y las amenazas de entes infiltrados.

Evite el borrado manual y la restauración con reparación precisa en línea

El éxito de los equipos de Respuesta a incidentes contra los ataques cibernéticos es real y tangible, e increíblemente lo logran con una gran dependencia en los procesos manuales para la mitigación. El 53 % de las organizaciones siguen usando la "restauración o restablecimiento de máquinas comprometidas desde una imagen segura como su método de reparación preferido.[12]

Una dependencia excesiva en los procesos manuales deriva en tiempos de respuesta prolongados y grandes cantidades de alertas de seguridad que requieren atención y conocimiento de Respuesta a incidentes, y que, en última instancia, provocan alteraciones en la actividad comercial y los procesos. Por ejemplo, la reparación manual que consiste en el borrado y la restauración casi siempre requiere tener posesión física del dispositivo, formatear el disco duro y volver a instalar un perfil con acceso a los archivos y sistemas. Utilizar este proceso o un flujo de trabajo de reparación similar no es algo escalable ni recomendable para las necesidades de seguridad de una empresa.

Ventajas de las capacidades de respuesta remota a través de la red con OpenText EnCase

- Acceso global a cualquier terminal conectada a la red
- Reparación precisa: solo se interactúa con la información y los sistemas afectados
- Evita el tiempo de inactividad de las terminales o alteraciones prolongadas de la actividad comercial debido a sistemas comprometidos
- Supervisión asíncrona de empleados no tradicionales con conectividad intermitente a la red corporativa
- Coloca las terminales comprometidas en cuarentena para reducir la propagación lateral
- Determina el alcance del incidente e identifica las terminales que están comprometidas de forma similar
- Mitiga los procesos maliciosos y elimina los archivos corruptos que los generaron
- Restablece las claves de registro afectadas que permiten que las amenazas avanzadas sobrevivan a un reinicio en memoria

Hacemos más sencilla para que los analistas de seguridad de primer nivel

Los líderes de seguridad pueden brindar a su personal de respuesta a incidentes menos experto acceso a EnCase con la visibilidad y profundidad requerida. EnCase permite que los analistas de seguridad sin experiencia tengan un impacto inmediato y visible en las operaciones de seguridad, sobre todo en relación con la clasificación de eventos y las respuestas de primer nivel.

EnCase ofrece flujos de trabajo que priorizan la seguridad y una IU intuitiva pensada para que los analistas de seguridad sin experiencia puedan responder de forma inmediata. Los analistas de primer nivel pueden realizar acciones guiadas y temporales a fin de detener los efectos y la propagación lateral del software malicioso hasta que los recursos de segundo y tercer nivel estén disponibles para una investigación y respuesta más avanzadas.

opentext™

EnCase se integra fácilmente con tecnologías de seguridad adyacentes para una máxima eficiencia operativa, que incluyen:

- SIEM
- IPS
- IDS
- Fuentes de inteligencia de amenazas
- Entorno de prueba/ análisis dinámico
- Organización de seguridad
- OST comúnmente usados
- + API de RESTful o abierta con SDK documentado para integraciones a pedido

Por ejemplo, pensemos en una APT detectada en la red corporativa. Esa detección se presenta como un evento de seguridad y se indica que se necesitan más analistas. Un analista de primer nivel puede verificar la alerta rápidamente, entender por qué esa alerta es maliciosa o sospechosa, actuar rápido para aislar la terminal y enviar la detección por la cadena interna para que otro analista de segundo o tercer nivel la revise.

Amplíe las habilidades de los usuarios avanzados con flujos de trabajo sugeridos y creadores para el personal con menos experiencia

Ya hablamos sobre la falta de expertos disponibles para ayudar a los CISO en la lucha contra los atacantes informáticos de hoy en día, y sobre el hecho de que **los líderes de seguridad están cambiando su enfoque a fin de maximizar las contribuciones de sus expertos más valiosos.**

Los usuarios avanzados de Respuesta a incidentes pueden adicionar a las reglas de detección de amenazas con reglas de anomalías personalizadas adicionales para una máxima ya incluidas en EnCase. Las necesidades de detección de los equipos de seguridad varían en gran medida según la industria, el tipo de organización, los vectores de ataque comunes y otras incontables variables. La capacidad de implementar reglas de detección personalizadas permite lanzar una red más amplia y precisa para obtener una mejor visibilidad de las vulnerabilidades potenciales. La panacea de que todos los ataques son iguales para todos los clientes y pueden todos ser resueltos igual no son tan eficaces como se anuncian, y la capacidad de personalizar la detección después de una implementación es un componente clave del éxito.

Estas reglas de anomalías dirigidas y adicionales crean nuevos eventos y detecciones que se envían a los analistas de primer nivel para una clasificación general y una respuesta simple.

Integración fácil con tecnologías de seguridad adyacentes para una máxima eficiencia operativa

La defensa en profundidad (DiD) es una práctica estándar y una metodología generalizada para proteger una empresa. A menudo, se requieren muchas personas y diferentes tecnologías de seguridad para lograr la protección de una empresa y la seguridad digital. Los líderes de seguridad suelen usar una variedad de soluciones de seguridad para satisfacer sus necesidades. Existen muchas capas de soluciones de terminales, red, análisis de datos, inteligencia y respuesta, que se superponen para obtener la cobertura total deseada.

Esta preferencia de los líderes de seguridad implica que los proveedores de tecnología de seguridad deben trabajar bien con las tecnologías de seguridad adyacentes, compartir información fácilmente de una herramienta a otra y proporcionar un acceso fácil entre las diferentes IU con la mínima cantidad de operaciones engorrosas.

EnCase se integra fácilmente con una gran variedad de tecnologías de seguridad adyacentes. La API de RESTful y el kit de desarrollo de software de EnCase se pueden utilizar para integraciones a pedido y poco tradicionales donde no exista una integración preconfigurada lista para usar.

De esta forma, se puede realizar la mayor cantidad posible de automatizaciones en el SOC. Las tareas críticas aún requieren que una persona que responda a incidentes haga una revisión y análisis manuales, ya que demasiada automatización puede ser perjudicial para las tareas y causar daños.

La automatización mediante integraciones hace que el total valga más que la suma de sus partes, dado que la tecnología funciona conjuntamente con eficacia y simplifica las operaciones de seguridad.

opentext™

Priorice la respuesta a alertas con inteligencia de amenazas y contexto incorporados

Los volúmenes de eventos de seguridad son preocupantemente altos, y cada una de ellos requiere clasificación y revisión a fin de mitigar con éxito cualquier brecha de seguridad. Si bien alrededor del 80 % de los eventos son falsos positivos, los líderes de seguridad deben pecar de cautelosos.[13] Esta necesidad de cautela da como resultado una gran cantidad de eventos de seguridad que los equipos de respuesta a incidentes deben analizar y abordar: una situación indeseada pero inevitable.

Con EnCase, los equipos de seguridad pueden priorizar respuestas con rapidez según la importancia de las amenazas. Dado que todas las alertas de seguridad poseen un análisis de reputación de archivos y análisis dinámico con puntuaciones de amenaza, las personas que responden a incidentes tienen el contexto necesario para evaluar y priorizar con éxito las amenazas válidas, y reducir en gran medida la cantidad de falsos positivos que requieren una investigación individual. Los equipos de seguridad pueden abordar primero las alertas graves y de prioridad elevada que tengan las puntuaciones de amenaza más altas, lo que indica que existen pruebas sólidas y verificadas de actividad maliciosa o sospechosa. A partir de allí, los analistas de primer nivel pueden trabajar desde abajo y abordar las alertas menos críticas hasta que, por último, las únicas alertas restantes sean falsos positivos.

Evalúe completamente los ataques avanzados y dirigidos con un conjunto integral de características DFIR/de tercer nivel

Para conseguir resultados realmente buenos como grupo, los equipos de Seguridad de la Información deben priorizar la capacidad de descubrir y remediar ataques avanzados y dirigidos. Los ataques informáticos avanzados patrocinados por una nación suelen parecerse mucho a las tácticas usadas por los infiltrados con privilegios que escapan con los datos confidenciales que se les confiaron, lo que significa que un enfoque en investigaciones con Digital Forensic Incident Response (DFIR) es uno de los únicos métodos probados para la detección y la respuesta. Los agentes maliciosos pondrán en riesgo a los usuarios y usarán credenciales y privilegios de forma fraudulenta para obtener, con el tiempo, acceso a los datos confidenciales.

Además de identificar y acceder a los protocolos de gestión, las soluciones de investigación de tercer nivel son uno de los únicos métodos comprobados para descubrir, evaluar y remediar por completo los ataques avanzados y dirigidos.

opentext™

Responda sin miedo y logre una recuperación completa con OpenText™ | EnCase™ Endpoint Security

¿Tiene preguntas?

opentext.com/security encase@opentext.com

OpenText ofrece el estándar de oro en investigaciones digitales y fue el ganador del premio "Best Computer Forensic Solution" de la revista SC Magazine del 2019 por décimo año consecutivo. Los examinadores pueden investigar en cualquier parte gracias a una compatibilidad incomparable con dispositivos, sistemas operativos, Nubes y tecnologías de cifrado, lo que garantiza que la evidencia nunca estará fuera de su alcance durante una investigación crítica. OpenText proporciona las soluciones de detección de amenazas y respuesta a incidentes líderes del mercado que permiten una rápida detección y reparación de las terminales comprometidas mediante la restitución eficiente y total de las terminales a un estado confiable, gracias a una reparación precisa e integral.

Los equipos pueden confiar en OpenText, la solución forense disponible con mayor compatibilidad para abordar las necesidades de investigación modernas más demandantes.

Sobre OpenText

OpenText, The Information Company, permite a las organizaciones adquirir conocimientos a través de soluciones de gestión de información de primer nivel, en las instalaciones o en la nube. Para obtener más información sobre OpenText (NASDAQ: OTEX, TSX: OTEX), visite: opentext.com.

Contáctenos:

- Blog de Mark Barrenechea, CEO de OpenText
- Twitter | LinkedIn

Sources

[1] SANS, *SANS 2019 Incident Response (IR) Survey: It's Time for a Change*, 31 de julio de 2019.

[2] Ibid.

[3] Cybercrime Magazine, *Cybersecurity Jobs Report 2018-2021*, 31 de mayo de 2017.

[4] SANS, *SANS 2019 Incident Response (IR) Survey: It's Time for a Change*, 31 de julio de 2019

[5] Ibid.

[6] New York Times, *Target Missed Signs of a Data Breach*, 13 de marzo de 2014

[7] Ibid.

[8] Verizon, *2019 Data Breach Investigations Report.*

[9] DarkReading, *Security Analysts Are Only Human*, 21 de febrero de 2019.

[10] Imperva, Survey: 27 Percent of IT professionals receive more than 1 million security alerts daily, 28 de mayo de 2018.

[11] SANS, *SANS 2019 Incident Response (IR) Survey: It's Time for a Change*, 31 de julio de 2019.

[12] Ibid.

[13] DarkReading, *Security Analysts Are Only Human*, 21 de febrero de 2019..

opentext.com/contact