BlackBerry
Intelligent Security. Everywhere.

Guía de evaluación

Guía de evaluación de madurez de seguridad cibernética de BlackBerry

Un marco de cuatro niveles para alcanzar la resiliencia cibernética

Introducción

¿Son sus controles de seguridad capaces de prevenir que las amenazas violen sus defensas? ¿Que inversiones debería hacer para cerrar brechas en su arquitectura de seguridad? ¿Debería adquirir recursos y herramientas de seguridad de manera interna o tercerizar a un proveedor de servicios de seguridad gestionada (MSSP)? ¿Cómo se adaptará a medida que los atacantes introduzcan nuevas tácticas, técnicas y procedimientos (TTP) a sus arsenales? Cada organización responderá de manera diferente según sus objetivos, postura de seguridad y tolerancia al riesgo en general

En esta guía, brindamos una metodología y un mapa de ruta que puedan usar organizaciones de todos los tamaños para evaluar y fomentar la madurez de sus programas de gestión de riesgos cibernéticos.

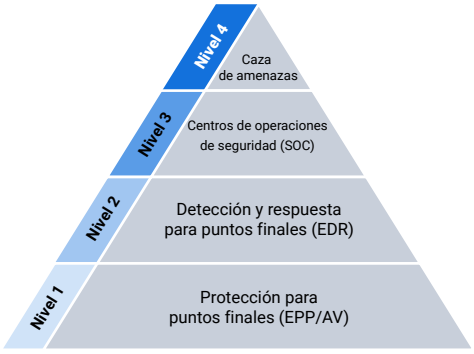
Modelo de madurez de seguridad

Nivel 1: Relevante y aplicable como estrategia para todas las organizaciones, sin importar su tamaño.

Nivel 2: Relevante y aplicable como estrategia para todas las organizaciones, sin importar su tamaño, aunque las organizaciones más pequeñas pueden elegir usar un MSSP para gestionar.

Nivel 3: Más relevante para las organizaciones más grandes y las corporaciones multinacionales debido a los recursos requeridos para dotar de personal y gestionar.

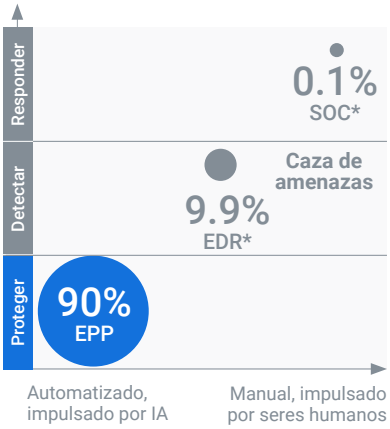
Nivel 4: Solo relevante para las organizaciones más grandes y las corporaciones multinacionales debido a las habilidades requeridas para dotación de personal y



En esta guía, brindamos una metodología y un mapa de ruta que puedan usar organizaciones de todos los tamaños para evaluar y fomentar la madurez de sus programas de gestión de riesgos cibernéticos. Empleamos un marco de cuatro niveles que incluye plataformas de protección para puntos finales (EPP), detección y respuesta para puntos finales (EDR), centros de operaciones de seguridad (SOC) y caza de amenazas. También consideramos los requisitos y criterios de recursos para hacer estas inversiones de seguridad en cada etapa de la madurez en general.

Modelos de aprendizaje automático sofisticados analizan 2,7 millones de características de archivos, desensamblando cada archivo en sus componentes básicos para poder así discernir si es malicioso o benigno.

Una EPP basada en IA debe aportar al menos el 90 % de su estrategia de seguridad de puntos finales



**Porcentaje de las amenazas totales que está mitigando a través de distintos enfoques de seguridad.*

Beneficios de la prevención de amenazas impulsada por IA

Descargue nuestro documento técnico, BlackBerry vs. Enfoques de seguridad tradicionales, para conocer más sobre los beneficios de la prevención de amenazas basada en IA, y si aún no ha reemplazado su AV tradicional, conozca los beneficios de actualizar a un enfoque de IA.

Los sistemas EDR pueden reducir el tiempo de permanencia con una respuesta automatizada que contiene infecciones y recopila datos de telemetría de punto final para el análisis de causa raíz.

NIVEL 1

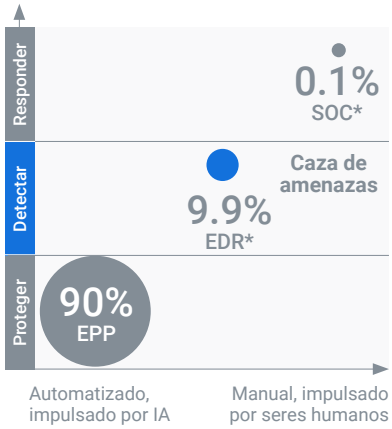
Plataforma de protección para puntos finales (EPP)

Prácticamente cada organización hoy cuenta con algún tipo de protección para puntos finales. Esto es esencial dado que más del 90 % del malware se entrega a los puntos finales mediante ataques de phishing y ataques dirigidos (spear phishing). Sin embargo, cada vez más empresas descubren que los productos antivirus (AV) tradicionales son ineficaces contra las sofisticadas amenazas basadas en archivos y sin archivos de hoy debido a que dependen de tecnologías obsoletas de coincidencia de firmas.

Una firma es una cadena de bits única que funciona como la huella digital de un archivo de malware. Cada vez que un producto antivirus (AV) tradicional se encuentra con un archivo nuevo, compara un byte en el archivo con bytes en su base de datos de firmas. Si hay coincidencia, el producto AV continúa este proceso secuencial de coincidencia byte a byte hasta haber inspeccionado el archivo completo. Para ser marcados como malware, cada byte del archivo examinado debe coincidir exactamente con cada byte de la firma. Sin embargo, las herramientas basadas en firmas pueden evadirse fácilmente si un atacante modifica u ofusca su código, o si el proveedor de AV todavía no ha completado el tedioso proceso manual de crear y distribuir actualizaciones de firmas para una de las 350.000 nuevas variantes de malware lanzadas cada día.

Este proceso de coincidencia byte a byte suele requerir de tantos recursos que los puntos finales pueden volverse inestables o sin respuesta durante los análisis, lo que incomoda a los usuarios finales y reduce su productividad. El AV basado en firmas también es intensivo respecto de la gestión, y requiere que el personal descargue, instale, distribuya y audite un flujo continuo de actualizaciones de archivos de firma.

Una solución EDR debería abordar casi todas las amenazas que evaden su EPP



**Porcentaje de las amenazas totales que está mitigando a través de distintos enfoques de seguridad.*

Beneficios de la solución de EDR de BlackBerry

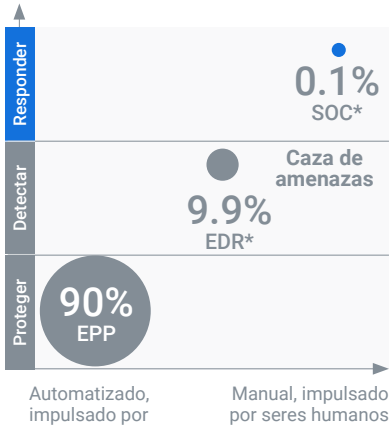
Para conocer más sobre los beneficios de nuestro EDR basado en IA, visite nuestra página dedicada donde encontrará más información o descargue nuestro documento técnico titulado AI-Based Prevention: The Evolution of Endpoint Prevention and Detection.

Establecer y mantener un SOC es una propuesta costosa, de modo que hay muchos factores a tomar en cuenta al momento de evaluar posibles inversiones en SOC.

Afortunadamente, ahora se encuentran disponibles soluciones para puntos finales de última generación más inteligentes que utilizan capacidades más avanzadas para defender contra malware. Por ejemplo, BlackBerry® Protect saca provecho de la ciencia algorítmica para detectar malware y evitar que se ejecute. BlackBerry Protect analiza cada archivo, ya sea que esté adjunto a un documento armado o sea copiado desde el dispositivo USB de un empleado. Modelos de aprendizaje automático sofisticados analizan 2,7 millones de características de archivos, desensamblando cada archivo en sus componentes básicos para poder así discernir si es malicioso o benigno. Este análisis profundo lo realiza en milisegundos un agente ligero y ágil que opera independientemente en cada host, sin basarse en absoluto en una base de datos de firmas, acceso a Internet o conectividad a la nube.

BlackBerry Protect también brinda funciones de control de scripts y aplicaciones, protección de memoria y aplicación de directivas de dispositivos que evitan que los ataques cibernéticos tengan éxito. Este enfoque automatizado basado en IA para la protección de puntos finales puede eliminar el 99,1 % de las amenazas, liberando así los recursos y presupuestos de TI para dedicarlos a otras iniciativas de seguridad más estratégicas.

El SOC debe manejar directamente no más del 0,1 % de las amenazas en forma manual



**Porcentaje de las amenazas totales que está mitigando a través de distintos enfoques de seguridad.*

NIVEL 2

Detección y respuesta para puntos finales (EDR)

Las soluciones de detección y respuesta para puntos finales (EDR) ocupan el siguiente nivel de madurez de nuestro marco de seguridad. Los sistemas de EDR pueden reducir el tiempo de permanencia del ataque con una respuesta automatizada que contiene las infecciones y recopila datos de telemetría de puntos finales para un análisis de causa raíz. Sin embargo, existen algunas consideraciones clave a tener en cuenta al momento de determinar si invertir en EDR es lo ideal para su organización.

- **Relación señal/ruido:** Puede resultar difícil discernir la señal de un ataque desde dentro de la masa ruidosa de datos de EDR. Un solo punto de datos puede ser significativo basado solamente en el contexto en el que aparece y su correlación con otros eventos de seguridad.
- **Aplicación en el punto final:** Muchos productos de EDR tradicionales confían en análisis basado en la nube para descubrir amenazas. Dicho eso, las soluciones de EDR más avanzadas ahora pueden impulsar todas las decisiones de detección y respuesta hacia el punto final, eliminando así la latencia de respuesta que puede marcar la diferencia entre un evento de seguridad menor y un incidente de seguridad mayor no controlado.
- **Romper las reglas:** Los adversarios se encuentran desarrollando constantemente nuevas tácticas, técnicas y procedimientos (TTP) expresamente diseñadas para evadir los sistemas de EDR basados en reglas, dejándolos tan ineficientes y obsoletos como las protecciones para puntos finales (EPP) basadas en firmas. Las soluciones de EDR modernas incorporan múltiples métodos de detección, entre ellos, detección de amenazas impulsada por el contexto e identificación de amenazas mediante aprendizaje automático.
- **Respuestas automatizadas sistemáticas:** Las rutinas de respuesta y reparación deben iniciarse de forma automática y realizarse sistemáticamente en todo el entorno.

NIVEL 3

Centros de operaciones de seguridad (SOC)

El siguiente nivel de madurez de seguridad, el centro de operaciones de seguridad (SOC), está integrado principalmente por empresas que realizan inversiones significativas en infraestructura y personal para reducir los riesgos cibernéticos y preservar la agilidad de sus negocios. Los analistas de los SOC son responsables de seleccionar e implementar controles de seguridad, recopilar y contextualizar datos de eventos, seleccionar alertas, evaluar indicadores de compromiso (IOC) e iniciar los planes de respuesta ante incidentes (IR) que limitan los daños de un ataque exitoso. Establecer y mantener un SOC es una propuesta costosa, de modo que las organizaciones deben tener en cuenta los siguientes factores al momento de evaluar posibles inversiones en SOC.

Fatiga por alertas

50

Soluciones de

×

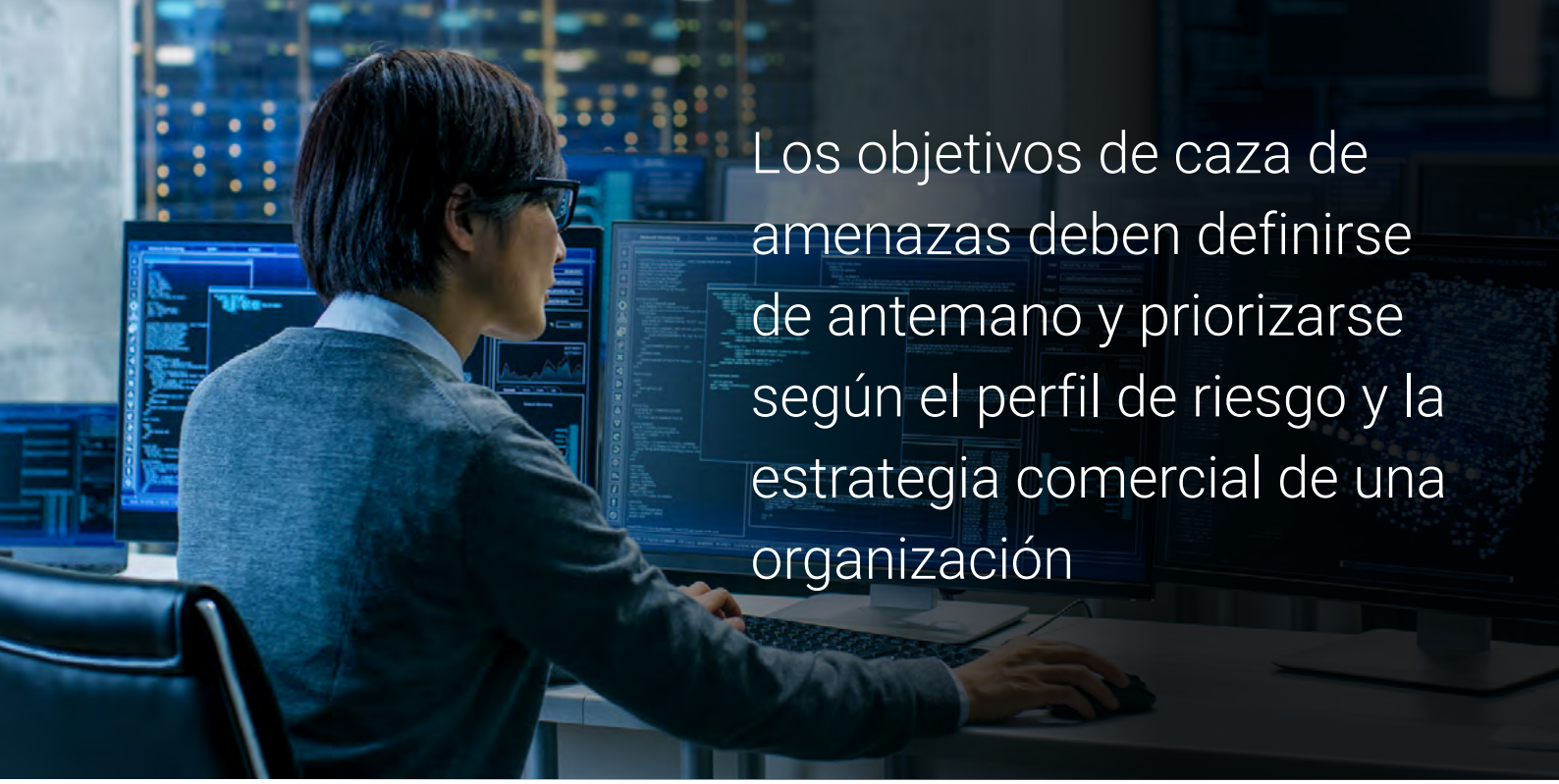
Miles de alertas

425

Horas perdidas

44 %

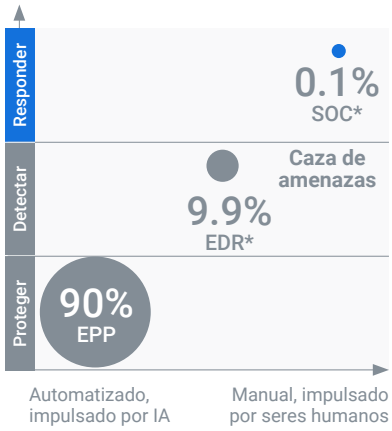
de alertas no investigadas debido a la fatiga por alertas



Los objetivos de caza de amenazas deben definirse de antemano y priorizarse según el perfil de riesgo y la estrategia comercial de una organización

- **Disponibilidad de personal de seguridad cibernética calificado:** Incluso las organizaciones grandes con mucho dinero tienen dificultades para reclutar y retener equipos de SOC con la experiencia y las calificaciones requeridas en seguridad de puntos finales, seguridad del perímetro, redes, programación y análisis forense. Según un estudio de investigación reciente de Frost and Sullivan, dos tercios de las organizaciones encuestadas informaron tener muy pocos trabajadores de seguridad cibernética como para satisfacer las necesidades actuales, una escasez global de talento de seguridad que no muestra señales de disminuir. Como resultado, muchos analistas de SOC son graduados universitarios recientes o trabajadores con poca experiencia práctica que deben lidiar con desafíos de seguridad complejos. Los problemas de dotación de personal se ven exacerbados por la necesidad de SOC en empresas globales que operan las 24 horas del día, los 365 días del año, ya que los adversarios no siguen el horario de oficina y suelen lanzar ataques desde ubicaciones en el extranjero. Si se tienen en cuenta las vacaciones y los días de licencia médica, un SOC con una dotación de personal completa necesitaría un mínimo de 12 a 15 analistas de tiempo completo para lograr la cobertura deseada.
- **Agotamiento de los analistas debido a la fatiga por alertas:** Los analistas de SOC están sujetos a fatiga por alertas y agotamiento por el inmenso volumen de alertas de seguridad que la mayoría de ellos deben clasificar cada día. Una empresa grande puede contar con hasta 50 soluciones de seguridad diferentes que colectivamente generan decenas de miles de alertas diarias. Más de la mitad de las alertas de seguridad son falsos positivos, según investigaciones del Ponemon Institute, lo que hace que los analistas pierdan 425 horas de tiempo cada semana en investigaciones inútiles. Como resultado, el 44 % de las alertas nunca se investiga debido a la fatiga por alertas, y solo la mitad de las alertas legítimas restantes se solucionan, según investigaciones de Cisco. Los controles de seguridad modernos pueden reducir notablemente los volúmenes de alertas y mejorar la fidelidad respecto de las alertas al utilizar técnicas de automatización e IA de avanzada, y al incorporar reglas de detección mapeadas al Marco de MITRE ATT&CK®. Sin embargo, a las organizaciones más pequeñas y con

La caza de amenazas es un proceso de alto valor pero principalmente manual para abordar el pequeño porcentaje de actividad maliciosa que evade los EDR y EPP



**Porcentaje de las amenazas totales que está mitigando a través de distintos enfoques de seguridad.*

menor cantidad de recursos puede resultarles más rentable aprovechar las soluciones de detección y respuesta gestionadas (MDR) basadas en una suscripción, como BlackBerry® Guard, que no requieren de una inversión anticipada en software de seguridad y servicios de implementación.

- **Inversiones en plataformas de Big Data:** Los analistas de los SOC necesitan contar con acceso fluido a datos de alertas y eventos de seguridad para poder rastrear actividades sospechosas e identificar a los atacantes. Esto requiere de inversiones en plataformas de Big Data que extraigan, analicen, normalicen y almacenen datos de registros en bruto de puntos finales, servidores, defensas del perímetro y productos de gestión de redes. Los costos de almacenamiento pueden aumentar rápidamente, ya sea que una organización opte por alojar los datos localmente o utilizar un servicio en la nube como Amazon Web Services. Luego, se pueden extraer los datos más significativos del almacén de registros a una plataforma de información de seguridad y administración de eventos (SIEM), donde pueden filtrarse, contextualizarse, enriquecerse con datos analíticos y correlacionarse con datos de fuentes de distribución de inteligencia de amenazas externas como VirusTotal. Los costos de SIEM también pueden aumentar rápidamente, ya que muchos proveedores determinan el precio de sus soluciones sobre la base de cuántos eventos capturaron por segundo. El personal de los SOC debe controlar y gestionar estas plataformas para garantizar que los datos estén continuamente actualizados y validados.
- **La importancia crítica de los procesos y planes de respuesta ante incidentes:** Con demasiada frecuencia, las organizaciones invierten en personal e infraestructura de SOC pero no satisfacen las expectativas en lo que respecta al desarrollo de procesos y planes de respuesta ante incidentes (IR), algo que equivale a enviar fuerzas armadas a la batalla sin un plan de ataque. De hecho, según un estudio de Telstra de 2018[10], un cuarto de los encuestados no tenían o no sabían si tenían un plan de IR establecido. Un plan de IR debe especificar cada medida a tomar cuando ocurre un incidente, comenzando por la asignación de miembros al equipo de IR. Esto típicamente incluirá no solo a los analistas del SOC más experimentados, sino también a personal de seguridad sénior con experiencia en recopilación de pruebas, análisis forense de redes y puntos finales, y análisis de malware, así como un gerente de incidentes que lidere al equipo y proporcione actualizaciones de estado a las partes interesadas clave de tecnología y negocios. Los procesos de IR deben ser lo suficientemente granulares para definir cosas tales como los procesos para acceder a datos de memoria, discos rígidos y redes, y las decisiones a tomar cuando se identifican sistemas comprometidos. Por ejemplo, el proceso puede especificar si se debe dejar sin conexión a Internet al sistema o si se lo debe dejar conectado para preservar el acceso a los datos de la pila de su red. Todos los procesos y criterios de decisión deben especificarse de antemano mediante una colaboración cercana con los ejecutivos de nivel C (incluso el CISO), los especialistas de seguridad con experiencia relevante y los propietarios de negocios de los datos o las aplicaciones pertinentes. Los profesionales de seguridad deben ofrecer opiniones técnicas. Sin embargo, los planes de IR deben definirse basados en los objetivos estratégicos de la organización y su tolerancia al riesgo, y no en las mejores prácticas de seguridad teóricas. En última instancia, es esencial que todos los involucrados, desde el conjunto C a la gerencia de línea de negocios, acepten los riesgos y lo resultados de las decisiones de IR.

Conozca más

Para conocer más sobre la solución de detección de amenazas y MDR de BlackBerry Guard visite *nuestra página dedicada donde encontrará más información* o *descargue nuestra hoja de datos*.

NIVEL 4

Caza de amenazas

La caza de amenazas ocupa el cuarto y último nivel de nuestro marco de seguridad. En esta etapa de desarrollo, las organizaciones más exitosas y maduras han logrado una postura de seguridad que prioriza la prevención, lo que significa que más del 90 % de las amenazas se desvían o neutralizan automáticamente. Las políticas de seguridad se aplican con controles de seguridad eficaces y las plataformas de grandes volúmenes de datos recopilan y contextualizan datos para la gestión de alertas y el análisis posterior al incidente. Los procesos y planes de respuesta ante incidentes están bien definidos y garantizan que las incursiones serias se solucionen de manera rápida y eficiente.

Al contar con estos recursos, se puede asignar a los analistas sénior con habilidades especializadas y experiencia a detectar proactivamente pruebas de actividad maliciosa anteriormente no detectada. Los cazadores de amenazas utilizan tanto procesos basados en metodología como inteligencia para identificar patrones de comportamiento y eventos de seguridad anómalos que se combinan para indicar que un adversario puede estar involucrado activamente en una o más etapas de la cadena de ataque. Si bien la caza de amenazas puede beneficiar a una organización, es conveniente tener en cuenta los siguientes requisitos antes de realizar una inversión.

- **Objetivos priorizados según el riesgo:** La caza de amenazas emplea los mismos métodos de prueba de hipótesis iterativos utilizados en la investigación científica. Por ejemplo, para probar la hipótesis de que puede estar ocurriendo un ataque de exfiltración, un cazador de amenazas podría buscar los indicadores de compromiso (IOC) asociados con flujos de red anómalos o los comportamientos de despliegue y acceso a datos sospechosos de parte de usuarios finales. Los objetivos de la caza de amenazas deben estar definidos de antemano y priorizados sobre la base de la estrategia comercial y el perfil de riesgo de la organización.
- **Desafíos del reclutamiento y la retención de personal:** La escasez global de profesionales de seguridad calificados es aun más marcada en lo que respecta a los analistas con habilidades especializadas y amplia experiencia que se requieren para la caza de amenazas. A las organizaciones puede resultarles casi imposible reclutar y retener a expertos en caza de amenazas que se ven atraídos por los salarios más altos y las condiciones laborales más favorables que ofrecen los proveedores de servicios de seguridad gestionada (MSSP) y las firmas de consultoría de seguridad.
- **Capacitación continua y perfeccionamiento de habilidades:** De la misma manera en que las empresas desarrollan continuamente sus procesos fundamentales para optimizar las ganancias, los atacantes lo hacen con sus vectores de ataque y TTP. Para mantener la paridad, las organizaciones deben invertir en capacitación continua para garantizar que los cazadores de amenazas sean técnicamente competentes, conozcan de negocios y estén altamente en sintonía con los riesgos presentados por los objetivos en desarrollo, las superficies de ataque y los procesos comerciales de la organización.

Conozca más

Para conocer más sobre la solución de detección de amenazas y MDR de BlackBerry Guard visite *nuestra página dedicada donde encontrará más información* o *descargue nuestra hoja de datos*.

- **Temor de exponer datos internos:** Las organizaciones que carezcan de recursos de caza de amenazas internos pueden mostrarse reacias a tercerizar las operaciones de detección de amenazas por temor a revelar datos internos pueda presentar riesgos de exposición desconocidos e inaceptables.

La madurez de seguridad es un proceso continuo

Esperamos que encuentre útil este modelo de madurez de cuatro niveles al evaluar sus necesidades de seguridad actuales y futuras. Cada nivel presenta capacidades nuevas e importantes para fortalecer la postura de seguridad de una organización. Sin embargo, no es necesario que cada organización busque soluciones en los cuatro niveles o intente desarrollar capacidades para cada nivel internamente.

Si su empresa es de pequeña a mediana, no sería práctico invertir en un SOC para clasificar alertas o implementar una plataforma de grandes volúmenes de datos para facilitar la detección de amenazas. En cambio, le resultaría más rentable sacar provecho del personal y la experiencia de los servicios detección de amenazas y MDR, como BlackBerry Guard, o contratar a consultores para realizar evaluaciones de respuesta ante incidentes y pruebas de penetración periódicas. Otros pueden beneficiarse de tercerizar funciones de SOC de rutina a un MSSP, de modo que el personal interno se pueda enfocar en proyectos de seguridad que apoyen y fomenten los objetivos de la empresa. Como siempre, lo que importa es la calidad de la ejecución, y no de dónde proviene la experiencia. Ante todo, la madurez significa comprometerse con un programa continuo de automejora de seguridad cibernética y gestión del riesgo responsable.

Aprender más

BlackBerry está listo para ser su socio, con una cartera completa de Soluciones y servicios adecuados para organizaciones en todas las etapas de la ciberseguridad madurez.

BlackBerry Protect: ofrece prevención de malware impulsada por inteligencia artificial, combinada con control de aplicaciones y secuencias de comandos, protección de memoria y aplicación de políticas de dispositivos para identificar y prevenir amenazas antes de que puedan ejecutarse

BlackBerry® Optics: es una solución EDR que extiende la prevención de amenazas entregado por BlackBerry Protect al proporcionar una verdadera prevención de incidentes de IA, análisis de causa raíz, búsqueda inteligente de amenazas y capacidades automatizadas de detección y respuesta. es una solución MDR basada en suscripción que aprovecha nuestro nativo

BlackBerry Guard: La plataforma de IA y el soporte 24x7 de un equipo de respondedores de incidentes de BlackBerry y expertos en prevención.

Incident Readiness Assessments: Nuestro equipo lo ayudará a elaborar un plan de IR y establecer de procesos que se alinean con sus objetivos de gestión de riesgos y ayudan a demostrar el cumplimiento normativo.

Incident Containment and Forensics: Si ocurre un incidente, lo ayudaremos a rastrearlo, contenerlo y remediarlo rápidamente, antes de que se convierta en un evento importante.

Red Team Services: Investigaremos las lagunas y vulnerabilidades en su seguridad. tejido que puede ser explotado por actores de amenazas internas y externas.

1 To learn more, download our eBook entitled, *Artificial Intelligence: The Smarter Approach To Information Security*.

2 *5 Cybersecurity Statistics Every Small Business Should Know in 2018*. Alert Logic.

3 Signatures Can't Keep Up

4 *The Numbers and Results Don't Lie*

5 *NSS Labs Advanced Endpoint Protection: Cylance Security Value Map,* April 2018. The BlackBerry Protect solution was formerly known as CylancePROTECT®.

6 *2017 Global Information Security Workforce Study (GISWS)*

7 *Dark Reading. Fighting Alert Fatigue with Actionable Intelligence*. Article cites Ponemon Study entitled, The Cost of Insecure Endpoints

8 *Dark Reading. Fighting Alert Fatigue with Actionable Intelligence*. Article cites Ponemon Study entitled, The Cost of Insecure Endpoints

9 *Cisco 2018 Annual Cybersecurity Report* | The defender landscape.

Acerca de BlackBerry

BlackBerry (NYSE: BB; TSX: BB) brinda servicios y software de seguridad inteligente a empresas y gobiernos alrededor del mundo. La compañía protege a más de 500 millones de puntos finales, lo que incluye a 150 millones de automóviles que están en las calles hoy en día. Con sede en Waterloo, Ontario, la compañía emplea IA y aprendizaje automático para brindar soluciones innovadoras en las áreas de la seguridad cibernética, soluciones de seguridad y privacidad de datos, y es líder en los campos de gestión de seguridad de puntos finales, cifrado y sistemas incorporados. La visión de BlackBerry es clara: garantizar un futuro conectado en el que pueda confiar.

BlackBerry
Intelligent Security. Everywhere.

MK20-0266 | 200629