DELL Technologies

Impulse la madurez de su ciberseguridad y su confianza cero.

Evite lagunas de recursos y conocimientos para fortalecer sus defensas frente a ciberataques.

DISPOSITIVOS E INFRAESTRUCTURA

DE OPERACIONES

CLOUD

APLICACIONES

DATOS

Las amenazas actuales están en rápida evolución, especialmente con el aumento de la GenAI, y presentan retos nuevos e inesperados, incluso para los especialistas en ciberseguridad con más experiencia. Descubra la forma en la que trabajar con profesionales de seguridad experimentados puede ayudarle a evitar ciberataques y mantener unas prácticas de seguridad sólidas.

Las amenazas cibernéticas son como las hormigas en un pícnic

Nos libramos de una, pero viene otra por detrás.

En un mundo cada vez más interconectado, en el que las organizaciones dependen ciegamente de las infraestructuras digitales y los datos se han convertido en una útil mercancía, lo mejor es asumir que un sofisticado atacante ya ha penetrado en su entorno de TI.

La buena noticia es que hay socios experimentados que se especializan en la intersección entre tecnología y ciberseguridad.

Dell Technologies aporta soluciones innovadoras y una valiosa experiencia, con las que es posible que no cuente de forma interna, para ayudarle a surcar un panorama de amenazas en constante evolución.

- Seguridad de hardware y de software
- Información sobre los riesgos emergentes
- Comprensión de las técnicas de ataque avanzadas
- AIOps para responder ante amenazas en constante cambio
- Nuevos procedimientos recomendados y estrategias de seguridad

Cree capas de defensa que mejoren sin cesar las prácticas de seguridad y adopte un enfoque de confianza cero.

Dell Technologies es un socio de ciberseguridad que ofrece servicios profesionales integrales, soluciones de hardware y software, y un ecosistema de socios sólido que limita las oportunidades de ataque, identifica y minimiza las vulnerabilidades, y le ayuda a restaurar rápidamente las operaciones empresariales.

Reduzca la superficie de ataque →

Detecte ciberamenazas y responda ante ellas →

Recuperación rápida tras un ataque →

Perímetro **Núcleo** **Multicloud**

Servicios profesionales

Ecosistema de socios tecnológicos/empresariales **Cadena de suministro segura**

DELL Technologies

Reduzca la superficie de ataque

Aumente sus defensas y conviértase en un objetivo más pequeño al reducir el número de situaciones que pueden aprovechar los ciberdelincuentes.

Para reforzar su estado de seguridad, necesita identificar y minimizar las vulnerabilidades y los puntos de entrada que pueden comprometer las aplicaciones, los sistemas o las redes en varios dominios, incluido el perímetro, el núcleo y la cloud.

IDENTIFIQUE puntos de vulnerabilidad

- Vulnerabilidades de software
- Configuraciones erróneas
- Mecanismos de autenticación débiles
- Sistemas no actualizados
- Privilegios de usuario excesivos
- Puertos de red abiertos
- Seguridad física deficiente

IMPLEMENTE medidas preventivas

- Trabaje con proveedores seguros
- Aplique una segmentación completa de la red
- Aísle los datos importantes
- Instaure controles de acceso estrictos
- Actualice y aplique parches a los sistemas y las aplicaciones
- Identifique y resuelva las vulnerabilidades mediante IA, evaluaciones periódicas y pruebas

Adopte un enfoque de confianza cero

Una arquitectura de confianza cero conlleva que su organización no confíe automáticamente en nada, ya sea dentro o fuera de sus perímetros. Por tanto, todo lo que se intenta conectar a sus sistemas se verifica antes de concederle acceso.
Es un modelo establecido y recomendado por el Departamento de Defensa de los Estados Unidos e incorpora **7 pilares interrelacionados** que crean madurez de forma sistemática.

1. Confianza en los usuarios
2. Confianza en los dispositivos
3. Confianza en los datos
4. Aplicación y carga de trabajo
5. Red y entorno
6. Visibilidad y análisis
7. Automatización y coordinación

DELL Technologies

Reduzca la superficie de ataque

Identifique los puntos débiles que obstaculizan sus sistemas antes de que lleguen los problemas.

La ciberseguridad no es una tarea puntual, sino un proceso continuo. Puede identificar y cerrar las brechas para reducir el riesgo realizando auditorías periódicas, pruebas de penetración y evaluaciones de vulnerabilidad con la ayuda de un socio de servicios de seguridad experimentado

Procedimientos seguros de la cadena de suministros	La seguridad empieza antes de lo que cree. Establezca una base de confianza que utilice dispositivos e infraestructuras diseñados, fabricados y entregados mediante una cadena de suministros segura, un ciclo de vida de desarrollo seguro y un modelado riguroso frente a amenazas.
Seguridad integrada	Trabaje con dispositivos e infraestructura que incluyan una seguridad integrada y basada en hardware, diseñada para detectar y rechazar ataques antes de que causen daños.
Actualizaciones periódicas de parches y aplicaciones	Aborde las vulnerabilidades conocidas y minimice el riesgo de explotación manteniendo las aplicaciones, el firmware y los sistemas operativos actualizados con los últimos parches de seguridad.
Menos privilegios	Limite las cuentas de sistemas y usuarios a fin de que cuenten con los derechos de acceso mínimos necesarios para que puedan llevar a cabo sus tareas. Este enfoque limita el impacto potencial que puede tener un atacante sin acceso autorizado.
Segmentación de la red	Aísle los recursos esenciales y limite así el acceso a la red mediante la segmentación moderna de redes para las aplicaciones y grupos empresariales y de datos. Al evitar el movimiento lateral, se limitan los ataques.
Seguridad de las aplicaciones	Implemente prácticas de cifrado seguras, lleve a cabo pruebas de seguridad y revisiones de código con regularidad, y utilice un firewall de aplicaciones web (WAF) para protegerse frente a ataques comunes a nivel de aplicaciones y reduzca la superficie de ataques a aplicaciones web.
Colaboraciones y servicios profesionales	Colabore con proveedores de servicios de ciberseguridad y con socios de tecnología y empresariales para adquirir conocimientos y soluciones con los que es posible que no cuente de forma interna.
Formación y sensibilización de los usuarios	Forme a empleados y usuarios para que reconozcan e informen sobre posibles amenazas de seguridad, intentos de phishing y tácticas de ingeniería social, y así minimizar los riesgos de acciones centradas en aprovecharse de las vulnerabilidades de las personas.

DELL Technologies

Detecte ciberamenazas y responda ante ellas

Las prácticas de seguridad de la vieja escuela son como el internet con marcación telefónica: demasiado lentas e ineficaces en el exigente entorno de hoy en día.

Para enfrentarse a las sofisticadas ciberamenazas, es necesario contar con mejores trucos de seguridad, como la IA y el ML integrados en aplicaciones y metodologías para que identifiquen y respondan frente a lo conocido y lo desconocido.

Implemente sistemas potentes de prevención y detección de intrusiones

Aproveche la IA y el ML para detectar anomalías

Instaure una supervisión en tiempo real del tráfico de red y el comportamiento de los usuarios

Aumente la resiliencia al colaborar con servicios profesionales experimentados para obtener conocimientos especializados.

Como socio tecnológico experimentado, Dell Technologies puede establecer protocolos proactivos de recuperación y respuesta ante incidentes que describan las funciones y responsabilidades, y garanticen una coordinación y comunicación transparentes entre todas las partes.

Mejore su capacidad para detectar ciberamenazas y responder a ellas proactivamente gracias a las siguientes medidas avanzadas:

- Inteligencia contra amenazas
- Respuesta ante incidentes
- Gestión de información y eventos de seguridad
- Protecciones de punto final
- Análisis de comportamiento

Facilite una recuperación rápida y eficiente, y minimice la pérdida de datos mediante:

- Una colaboración y un plan de respuesta ante incidentes bien definidos
- Copias de seguridad periódicas de sistemas y datos esenciales
- Cifrado de datos y soluciones de almacenamiento externo seguras

DELL Technologies

Detecte ciberamenazas y responda ante ellas

Permanezca alerta y tome medidas rápido.

La detección de las ciberamenazas y la respuesta ante ellas conllevar mantenerse alerta y planificar para enfrentarse a la peor situación posible. Establezca un plan de respuesta y recuperación que se actualice continuamente y se practique habitualmente para que toda su organización sepa cómo reducir los efectos de los ataques. Es un proceso continuo e iterativo que requiere una combinación de tecnología, personal cualificado, procesos bien definidos y colaboración en equipo.

Monitorización continua

Puede identificar indicios de acceso sin autorizar, intrusiones, malware y vulneraciones de datos gracias a herramientas de seguridad como sistemas de detección de intrusos (IDS), sistemas de prevención de intrusiones (IPS), análisis de registros e inteligencia contra amenazas.

Detección de amenazas

Aproveche la IA y el ML para analizar los datos con el fin de identificar patrones, anomalías e indicadores de riesgo (IDC) que puedan avisar de una amenaza. Esto incluye poder reconocer las firmas de ataque conocidas e identificar el comportamiento fuera de lo normal.

Alertas y notificación

Cuente con advertencias tempranas para lograr investigaciones y respuestas rápidas. Alertas de burbuja y notificaciones a la vista para actuar rápido con seguridad integrada. Alimente la telemetría a nivel de dispositivo por encima del SO para acelerar la detección de amenazas y que el personal de seguridad o un centro de operaciones de seguridad (SOC) actúen cuando se detectan posibles amenazas o incidentes.

Respuesta ante incidentes

Ponga en marcha un plan de respuesta para investigar y mitigar los incidentes de seguridad confirmados. Esto implica contener el impacto, identificar la causa raíz e implementar las acciones necesarias para restaurar los sistemas y evitar mayores daños.

Análisis forense

Lleve a cabo un análisis detallado de los incidentes para comprender la metodología de los ataques, determinar el alcance de la vulneración, identificar los sistemas o datos afectados y recopilar evidencias para encontrar y abordar las vulnerabilidades de seguridad.

Corrección y recuperación

Tome medidas para corregir las vulnerabilidades y los sistemas de parches, eliminar el malware e implementar medidas de seguridad mejoradas para prevenir incidentes similares. Restaure los sistemas y datos afectados a su estado normal para completar el proceso de recuperación.

DELL Technologies

Recuperación tras ciberataques

Pise el acelerador a fondo y vuelva a situar a su empresa en el carril izquierdo.

La ciberresiliencia es necesaria en el mundo basado en datos en el que vivimos hoy en día y tanto los clientes como los socios esperan que esté presente. Para tener éxito, necesita varias capas de protección para garantizar que los datos esenciales estén protegidos y aislados, de modo que se puedan recuperar rápidamente con confianza tras un ataque. Evalúe su ciberresiliencia ›

- Actúe para mitigar los daños causados por un ataque cibernético
- Reconstruya servicios y dispositivos comprometidos o interrumpidos
- Analice el incidente para evitar futuros ataques
- Cumpla con los SLA empresariales y devuelva la normalidad a las operaciones

Cree una estrategia de ciberseguridad integral para que su organización pueda recuperarse de manera eficaz y eficiente.

Para recuperarse de un ataque cibernético, es necesario un esfuerzo coordinado en el que participen equipos de TI, profesionales de ciberseguridad y gestión, y en ocasiones, expertos externos. La clave para la recuperación es volver a tener el control de los sistemas y las operaciones con rapidez mientras se aprende del incidente para reducir las interrupciones y el tiempo de inactividad, restaurar los servicios e integridad de los datos, minimizar los impactos en las finanzas y la reputación, y fortalecer la ciberseguridad para evitar ataques similares en el futuro.

- Evalúe el impacto de un ataque sobre las operaciones empresariales
- Priorice los servicios esenciales
- Implemente sistemas de protección de datos
- Informe sobre cualquier incidente y progreso en la recuperación
- Desarrolle un plan y practíquelo constantemente para garantizar la continuidad

DELL Technologies

Recuperación tras ciberataques

Vuelva a la pista de baile gracias a la recuperación de sistemas, redes y datos tras un incidente.

Al conseguir una estrategia de ciberresiliencia, se incorpora a las personas, los procesos y la tecnología a un marco integral que protege toda la organización.

Contención de incidentes

El primer paso es aislar y contener el impacto del ataque cibernético. Para ello, es necesario desconectar los sistemas afectados de la red, deshabilitar las cuentas comprometidas e implementar medidas para evitar propagaciones o daños adicionales.

Restauración de sistemas o dispositivos

Una vez que se haya contenido el incidente, los sistemas y redes afectados se restauran a un estado limpio y seguro. Esto puede implicar la reconstrucción de sistemas comprometidos, la reinstalación del software y la aplicación de parches de seguridad y actualizaciones. La automatización y la autorreparación pueden tener un papel importante para volver a tener un funcionamiento normal.

Recuperación de datos

Es necesario recuperar los datos que puedan haberse comprometido, cifrado o eliminado durante el ataque. Esto puede suponer la restauración de los datos a partir de copias de seguridad o el empleo de técnicas especializadas de recuperación de datos para archivos perdidos o cifrados.

Análisis forense

Tras un ataque, es crucial comprender cómo se produjo la vulneración, qué vulnerabilidades se aprovecharon y cómo evitar ataques similares. Existen sistemas como la gestión de información y eventos de seguridad (SIEM), y capacidades como las comparaciones de BIOS fuera del host, las cuales proporcionan información útil.

Evaluación de la respuesta ante incidencias

Tras la recuperación, es esencial evaluar el proceso de respuesta ante incidentes e identificar las áreas susceptibles de mejora. Las lecciones aprendidas con el ataque se pueden usar para mejorar las prácticas de seguridad, actualizar los planes de respuesta ante incidentes y ofrecer una mejor protección frente a futuros incidentes.

Colaboraciones y servicios profesionales

Los proveedores de servicios de ciberseguridad y los socios de tecnología aportan recursos y conocimientos valiosos para la recuperación de su organización. Pueden ayudarle con tareas como el análisis forense, la identificación del caso de vulneración y la recomendación de medidas para prevenir futuros incidentes.

DELL Technologies

Extienda la ciberseguridad al perímetro y entornos de cloud

A medida que las redes se extienden del núcleo al perímetro y a la cloud, los entornos se han convertido en un punto crucial de vulnerabilidad.

A medida que desarrolle su estrategia de ciberseguridad, su organización debería extender los principios de confianza cero al perímetro y a la cloud para garantizar rigurosos controles de acceso, autenticación continua y visibilidad y control integrales del tráfico de red. A medida que los entornos de amenazas evolucionan, es aconsejable implementar funcionalidades de IA como primera línea de defensa. Además, una estrategia solo estará completa si sus entornos principales de red y cloud cuentan con medidas de seguridad, como la segmentación de la red, el cifrado y la monitorización continua.

Los servicios profesionales de ciberseguridad le puede ayudar a adoptar un enfoque integral.

La conexión entre varias soluciones de seguridad puede ser un reto. Al colaborar con servicios profesionales que se especializan en la seguridad del perímetro, el núcleo y la cloud le aporta la experiencia necesaria para implementar medidas eficaces que protejan su organización desde todos los ángulos.

Perímetro

Establezca varias capas de seguridad en el perímetro, en la red y dentro del hardware y el software.

Núcleo

Alinee su infraestructura con un enfoque de confianza cero mediante la IA, el ML y la automatización.

Multicloud

Proteja cualquier carga de trabajo en cualquier entorno, incluidas las cargas de trabajo nativas de la cloud, contenedores y la cloud pública.

DELL Technologies

GenAI: Una espada de doble filo para la ciberseguridad

La última generación de IA nos acerca a nuevos riesgos, pero también mejora la seguridad.

La GenAI, la siguiente fase de la IA, abarca sistemas que pueden comprender, aprender, adaptar e implementar conocimientos en una serie de tareas.

Por un lado, promete mejorar la detección de amenazas y la respuesta ante ellas, las capacidades predictivas y la eficiencia operacional. Por otro lado, presenta nuevos retos que requieren estrategias de ciberseguridad en constante evolución que aborden riesgos mediante medidas de seguridad sólidas, supervisión continua, actualizaciones regulares y parches, y un enfoque en constante evolución sobre la ética y la privacidad de datos.

Asegurar organizaciones con GenAI

La GenAI se ha convertido en una aliada crucial respecto a la ciberseguridad y abre nuevas posibilidades para proteger las organizaciones.

- Mejore la eficacia de la detección de amenazas y la respuesta ante ellas.
- Prediga las amenazas futuras o identifique posibles vulnerabilidades.
- Automatice la detección de amenazas y proporcione eficiencia.
- Análisis forense para identificar rápidamente patrones, anomalías e indicadores de riesgo.
- Formación personalizada relacionada con la concienciación sobre la seguridad
- Escale las operaciones de seguridad con un acceso más rápido a información más detallada.

Asegurar los sistemas de GenAI

Aunque la GenAI ofrece importantes beneficios de seguridad, su funcionalidad puede usarse de forma malintencionada si no está adecuadamente protegida.

- Garantice la integridad y la privacidad de los datos.
- Mitigue los ataques de adversarios diseñados para provocar que los sistemas de IA fallen.
- Detecte el uso indebido del sistema de la IA malintencionada y responda ante el mismo.
- Audite y mitigue los problemas éticos y las preferencias.
- Implemente controles de acceso sólidos para los sistemas de IA.
- Proteja y recupere modelos de lenguaje colosales (LLM) de forma segura.

La ciberseguridad moderna debe ser inteligente, ampliable y automatizada

Dell Technologies puede ayudarle a establecer una seguridad integral que le proteja frente a las amenazas cibernéticas en evolución. A medida que la tecnología avanza, nuestro enfoque hacia la ciberseguridad sigue un paso por delante y aprovecha la potencia de la IA y el ML para proteger sus infraestructuras digitales y mantener la confianza en el mundo digital. Independientemente de dónde se encuentre en su viaje hacia la ciberseguridad, trabajaremos con usted para avanzar solo mediante la protección de su organización con pasos que le mantengan ágil y resiliente.

DELL Technologies

Dell.com/SecuritySolutions
Solicite una llamada
Chatear con un asesor de seguridad
Llame al 1-800-433-2393