Beneficios clave

Prevención

- Identificar vulnerabilidades en todo el entorno para priorizar la aplicación de parches
- Detectar controles de seguridad configurados incorrectamente o problemáticos que podrían aprovecharse
- Inspeccionar detenidamente las rutas de alto riesgo que dan acceso a información o recursos valiosos con pruebas de penetración anuales
- Mejorar la vigilancia de los empleados con minicapacitaciones en seguridad impartidas frecuentemente

Respuesta

- Detectar y responder a las amenazas 24x7 en todo el entorno
- Realizar un seguimiento integral de las actividades de los agentes de amenazas
- Utilizar telemetría y correlacionar eventos de diversas herramientas de seguridad populares

Dell Managed Detection and Response Pro Plus

Solución de operaciones de seguridad de 360° completamente administrada en terminales, red y nube

Asumir los desafíos de las operaciones críticas de seguridad

Muchas organizaciones de TI han adoptado el monitoreo y la detección de amenazas para mantenerse a la par del volumen y la variedad de amenazas en constante aumento.

Si bien el monitoreo y la detección de amenazas proporcionan una cobertura vital, es mejor manejar las brechas reparables desde el principio, antes de que los agentes de amenazas tengan la oportunidad de aprovecharlas. Los equipos de TI pueden evitar muchas actividades maliciosas si abordan proactivamente las vulnerabilidades de software, los controles de seguridad configurados incorrectamente y los descuidos de los empleados.

Los profesionales expertos en seguridad saben cómo aplicar parches a las vulnerabilidades, pero para la mayoría de las organizaciones de TI es imposible aplicar parches a todas las vulnerabilidades. En 2021, se informaron más de 1500 vulnerabilidades nuevas cada mes.[1] Para poder manejar esa cantidad de parches, los clientes deben priorizar las vulnerabilidades que presentan el mayor riesgo.

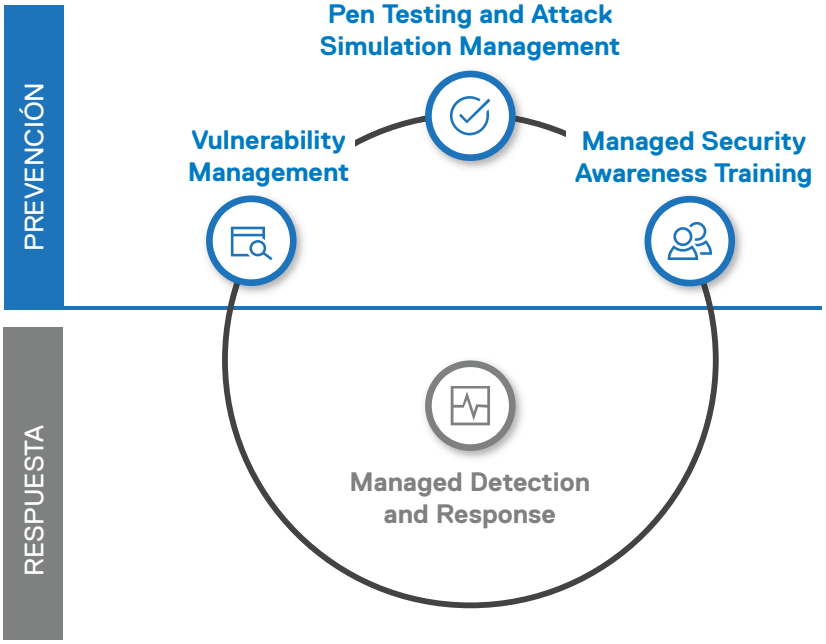
Es igualmente abrumador tratar de validar todos los controles de seguridad, como gateways de correo electrónico o firewalls de aplicaciones web. Debido a los cientos de controles y configuraciones complejas, los equipos de seguridad de TI tienen dificultades para confirmar si los controles de seguridad bloquean las actividades no autorizadas.

Además, las empresas necesitan que los empleados reconozcan cuándo los agentes de amenazas intentan obtener credenciales de inicio de sesión, datos u otra información confidenciales. Un estudio encontró que el 83 % de las empresas que participaron en dicho estudio experimentaron un ataque exitoso de phishing basado en correo electrónico en 2021.[2]

Managed Detection and Response Pro Plus

Los expertos en seguridad de Dell Technologies examinaron detenidamente estas preocupaciones clave relacionadas con las operaciones de seguridad para diseñar un nuevo servicio de operaciones de seguridad de 360°: Managed Detection and Response Pro Plus.

MDR Pro Plus es una solución de operaciones de seguridad completamente administrada en la que los mejores expertos en seguridad utilizan herramientas de vanguardia para prevenir amenazas, detectar y contener los intentos de ataque rápidamente e iniciar la recuperación en caso de una vulneración. MDR Pro Plus lo ayuda a fortalecer de forma continua la postura de seguridad de su empresa.



Sellar las aberturas en el software y controles de seguridad

Vulnerability Management analiza su entorno mensualmente en busca de vulnerabilidades y emplea el aprendizaje automático para priorizar aquellas que tienen más probabilidades de ser aprovechadas y tener un gran impacto. La lista de prioridades ayuda al equipo de TI a enfocarse en las vulnerabilidades de mayor valor.

Tal como los agentes de amenazas saben buscar vulnerabilidades sin parches, también buscan controles de seguridad configurados incorrectamente o desactualizados, por lo que las organizaciones de TI deben buscarlos y encontrarlos primero. **Pen Testing and Attack Simulation Management** cuenta con simulaciones de ataques y vulneraciones automatizadas mensuales (BAS) y pruebas de penetración anuales.

BAS detecta controles de seguridad defectuosos en dispositivos y software en el entorno de TI. Las pruebas de penetración complementan las BAS, ya que intentan alcanzar un objetivo específico, como un sistema de alto valor. Los evaluadores de penetración calificados emulan las técnicas de los agentes de amenazas, incluidas las técnicas de pivote y adaptación para llegar al objetivo.

Dell ejecuta análisis de vulnerabilidades y simulaciones BAS en bases de datos actualizadas continuamente para ayudarlo a asegurarse de que los parches y los controles de seguridad permanezcan actualizados.

Ayudar a los empleados a mantenerse alerta

Un modelo común para la capacitación en concientización sobre seguridad es una sesión de capacitación anual de varias horas. A menudo, los empleados no retienen esta información, ya que puede convertirse en una "tarea meramente informativa". En caso de que sean objeto de una táctica de ingeniería social o de un correo electrónico con un enlace malicioso, es posible que no reaccionen con suficiente precaución.

Managed Security Awareness Training ofrece minimódulos de capacitación en seguridad durante todo el año, lo que mantiene a los empleados comprometidos activamente con rutas de aprendizaje personalizadas y pone la seguridad en primer lugar. Las rutas de aprendizaje se crean con base en la función del empleado, el nivel de exposición a amenazas y el progreso.

Detectar y contener intentos de ataque rápidamente

Dell MDR Pro Plus cuenta con **Managed Detection and Response** 24x7. Los analistas calificados monitorean su entorno e investigan las amenazas mediante una plataforma de análisis de seguridad avanzada XDR. Los análisis impulsados por el aprendizaje automático y profundo de la telemetría y los eventos proporcionan a los analistas información valiosa para rastrear la ruta y las actividades del atacante. A continuación, el equipo de Dell le brinda instrucciones para contener y resolver la amenaza. En caso de que se produzca un incidente de seguridad, Dell Technologies lo ayuda a iniciar el proceso para volver a poner en marcha su empresa.

Mejorar las operaciones de seguridad con Dell

MDR Pro Plus ayuda a prevenir actividades maliciosas mediante informes periódicos de las brechas de vulnerabilidad, los controles de seguridad configurados incorrectamente y las rutas de alto riesgo que dan acceso a recursos valiosos. Además, proporcionamos capacitaciones en seguridad concisas y fáciles de recordar para los empleados durante todo el año. La detección y respuesta ante amenazas proporciona monitoreo y seguimiento constantes de las actividades sospechosas.

MDR Pro Plus le ofrece una solución inteligente de operaciones de seguridad de TI de 360°, con servicios basados en tecnología avanzada y proporcionados por expertos. Todo administrado por Dell Technologies: una empresa en la que las organizaciones de todos los tamaños en todo el mundo ponen su confianza cuando se trata de dispositivos, infraestructura y servicios de TI innovadores.

Obtenga más información sobre Dell Managed Detection and Response Pro Plus

Contactar a un experto de Dell Technologies

[1] Fuente: With 18,378 vulnerabilities reported in 2021, NIST records fifth straight year of record numbers, ZDNet, 8 de diciembre de 2021. https://www.zdnet.com/article/with-18376-vulnerabilities-found-in-2021-nist-reports-fifth-straight-year-of-record-numbers/

[2] Fuente: 2020 Phishing Attack Landscape Report [Greathorn]. Cybersecurity Insiders. (2020). Información obtenida el 15 de noviembre de 2022 de https://www.cybersecurity-insiders.com/portfolio/2020-phishing-attack-landscape-report-greathorn/