En resumen

Beneficios

- **Más seguridad** gracias a un enfoque integral que aborda la preparación y la respuesta
- **Más confianza en las protecciones activas** a través de una metodología comprobada, una inteligencia única y un equipo con experiencia
- **Mayor visibilidad** y comprensión más profunda de las operaciones y la infraestructura gracias al uso de tecnología innovadora y al constante análisis extensivo a cargo de expertos

Servicio de respuesta ante incidentes de seguridad de Cisco (Cisco Security Incident Response Service)

Actual panorama dinámico de amenazas

Las organizaciones sufren ataques por todos los frentes. En 2014, las violaciones a la seguridad costaron casi USD 500 mil millones, según IDC. Mientras tanto, en el mundo hay pocos profesionales de la seguridad y se estima que hay un millón de brechas sin resolver, según el informe anual de seguridad de Cisco de 2015. Esta escasez de talentos, combinada con un aumento en los incidentes, ha generado un estado de seguridad que suele ser débil en la mayoría de las organizaciones. Los ataques se traducen en enormes pérdidas monetarias, en detrimento de la propiedad intelectual, en riesgos para la información del cliente y la confianza, y en valoraciones corporativas menos ventajosas.

El servicio Cisco® Security Incident Response refuerza considerablemente las defensas de la red y la seguridad de la información. Con las mejores prácticas y la inteligencia más actualizadas, este servicio presenta un proceso en el que participan todas las capas de defensa y proporciona una amplia variedad de funcionalidades destinadas a ayudar a las organizaciones en la preparación y la administración de incidentes, así como también en la respuesta y la recuperación posteriores, con rapidez y eficacia.

Un estado de seguridad más sólido con la preparación y la respuesta

El servicio de respuesta ante incidentes de seguridad de Cisco es una solución dentro de Cisco Advisory Security Services que brinda los conocimientos necesarios para evaluar y diseñar un enfoque de seguridad que fomente el crecimiento de la empresa, reduzca los costos y mitigue los riesgos. Mediante la combinación de las mejores prácticas y el uso de marcos de seguridad eficaces del sector, el equipo de respuesta ante incidentes de Cisco (Cisco's Incident Response Team) proporciona una amplia variedad de funcionalidades para ayudar a las organizaciones. Nuestro equipo de respuesta ante incidentes está formado por expertos en seguridad de la información que se ajustan a una fórmula única basada en el cumplimiento de la leyes, la seguridad empresarial y la experiencia en seguridad de la tecnología. Nuestro equipo trabaja directamente en conjunto con el grupo de Cisco Collective Security Intelligence (CSI) para identificar amenazas conocidas y desconocidas, para cuantificar el riesgo y establecer un orden de prioridad, así como también para reducir el riesgo en el futuro.

Permita que nuestros expertos colaboren con usted para desarrollar un nuevo plan, reevaluar los planes existentes o proporcionar asistencia rápida en el transcurso de un ataque.

Solo el 50% de los directores de seguridad de la información (CISO) está plenamente de acuerdo con la idea de que “es fácil determinar el alcance de un riesgo, contenerlo y remediar las vulnerabilidades” (Informe anual de seguridad de Cisco de 2015).

Pasos siguientes

Visite www.cisco.com/go/securityservices para obtener más información sobre las soluciones de seguridad de Cisco.

Tabla 1. Componentes del servicio de respuesta ante incidentes de seguridad de Cisco

Preparación	Respuesta
Evaluación del estado de preparación ante una violación de la infraestructura · Mediante la evaluación del diseño de la red, los controles de seguridad, los sistemas operativos, la configuración de seguridad del personal, los sistemas de revisión automatizada, los firewalls, el registro y otros sistemas relacionados, Cisco obtiene un profundo conocimiento del entorno del cliente y puede predecir los posibles vectores de ataque, además de recomendar los controles de seguridad necesarios. **Evaluación de la preparación de las operaciones de seguridad** · Gracias a una evaluación de la preparación de su equipo de seguridad, basada en los incidentes anteriores y en las funciones y responsabilidades actuales, Cisco ofrece recomendaciones para saber si su organización cuenta con los recursos, el conocimiento y las herramientas necesarias para diversos tipos de investigación. **Evaluación de la preparación de las operaciones** · Mediante una evaluación de sus actividades y modelo de operaciones, le proporcionamos recomendaciones destinadas a ayudarlo en futuros eventos. **Evaluación de las comunicaciones en caso de violación** · Cisco proporciona asistencia en la creación de un marco de comunicaciones con una estructura de cumplimiento adecuada para lograr la coordinación en la identificación y la respuesta en el nivel ejecutivo, en toda la cadena de suministro de la organización y en el ámbito externo con los clientes. **Capacitación sobre la respuesta ante incidentes y las operaciones de seguridad (Security Operations and Incident Response Training)** · Se brinda capacitación sobre las habilidades que se necesitan actualmente para dirigir, coordinar y ofrecer soporte ante un incidente. Además, se brinda capacitación técnica a los empleados de operaciones de seguridad sobre el análisis de software malicioso y las diversas herramientas de seguridad.	**Evaluación e investigación** · Determina el método de ataque y presenta un desglose del código malicioso, incluida su trayectoria, su destino y su objetivo final, a través de una revisión técnica de los sistemas infectados. **Desarrollo de contrataque** · Desarrolla contrataques para asistir en la detección, la cuarentena, el seguimiento y la interrupción de otras acciones por parte del atacante. De este modo, pueden obtenerse indicadores de riesgo, de filtración de información y de explotación de vulnerabilidades. **Implementación del contrataque** · Implementa todos los contrataques que se hayan desarrollado para asistir en la detección y la interrupción del incidente, siguiendo las mejores prácticas de seguridad de la información y del proveedor. **Validación del contrataque** · Valida la eficacia de los contrataques recientemente implementados y compila una revisión del rendimiento de cualquier mejora que deba aplicarse al diseño. El resultado incluye la documentación para presentar ante el consejo directivo, los organismos regulatorios y las autoridades encargadas del cumplimiento de las leyes, y contiene el resumen de los eventos, la mitigación y la pérdida, si corresponde. La respuesta ante incidentes de Cisco puede incluir uno de los siguientes puntos (o todos ellos) a fin de aislar y remediar un ataque: · Evaluación del origen del registro · Análisis y extracción de datos · Análisis de imagen forense · Instrumentación dinámica del sistema infectado · Ingeniería inversa del malware · Análisis de vulnerabilidades y segunda implementación

C45-734212-00 04/15