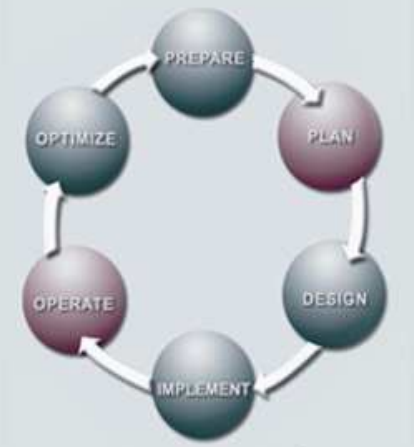
Security IntelliShield Alert Manager Service de Cisco

METODOLOGIA DEL CICLO DE VIDA DE LOS SERVICIOS



La metodología exclusiva del Ciclo de Vida de los Servicios de Cisco define las actividades necesarias en cada fase del ciclo de vida de la red para ayudar a asegurar la excelencia de los servicios. A través de esta metodología, que une las fuerzas de Cisco, nuestros partners especializados en redes y nuestros clientes, es posible obtener mejores resultados.

Fases del Ciclo de la Red

- **Preparación -** Desarrollo de plan de negocios para justificar la inversión tecnológica
- **Planeación -** Evaluación del estado actual de la red para soportar la solución propuesta
- **Diseño -** Creación de un diseño detallado para manejar requerimientos técnicos y de negocios
- **Implementación -** Despliegue de la nueva tecnología
- **Operación -** Mantenimiento de la salud de la red en el día a día de las operaciones
- **Optimización -** Alcance de la excelencia operacional a través de mejoras permanentes

EL Security IntelliShield Alert Manager Service de Cisco proporciona una solución amplia y costo-efectiva para brindar la inteligencia de seguridad que las organizaciones requieren para ayudar a prevenir, mitigar y remediar rápidamente potenciales ataques tecnológicos.

VISIÓN GENERAL DEL SERVICIO

En ambientes de misión crítica, el personal de seguridad de tecnología debe tomar pasos proactivos para mitigar las amenazas antes de que éstas puedan impactar el negocio. Sin embargo, para tomar dichos pasos, las organizaciones requieren de inteligencia de seguridad oportuna, veraz y fidedigna. Con miles de amenazas y vulnerabilidades reportadas cada año y docenas de servicios independientes reportando nuevos problemas, el personal de seguridad enfrenta el constante reto de encontrar la inteligencia apropiada y confiable que requiere para tomar decisiones rápidas.

El Security IntelliShield Alert Manager Service de Cisco® filtra las innumerables alertas de las organizaciones que reportan para proporcionar inteligencia de seguridad estratégica y específica que los clientes pueden utilizar para responder proactivamente a potenciales amenazas tecnológicas, mitigar riesgos e incrementar la continuidad del negocio. Al contar con este servicio, el personal de seguridad de tecnología puede ocupar menos tiempo revisando listas de correos y sitios Web de proveedores para buscar nuevas alertas y enfocarse en soluciones y protección proactiva dentro de sus propias redes de misión crítica.

DESAFÍO

Proteger la infraestructura de tecnológica de virus, gusanos (worms) y otras amenazas se ha vuelto cada vez más difícil. El primer paso para asegurar la red de negocios es comprender dónde existen vulnerabilidades. Esto surge porque el personal de seguridad de tecnología que busca inteligencia de seguridad veraz se enfrenta a:

- **Demasiada información**—Nuevas amenazas pueden ser reportadas por numerosos servicios públicos y organizaciones privadas, cientos de veces cada año.
- **Demasiados formatos**—Nuevas alertas de amenazas pueden ser publicadas por docenas de diferentes fuentes, cada una en diferente formato y cada una utilizando un diferente proceso para identificar, caracterizar, confirmar y reportar el problema.
- **Dificultad para determinar la importancia de una nueva amenaza**—Con tantas entidades independientes publicando alertas, al personal de seguridad puede dificultársele encontrar información objetiva acerca de la credibilidad, urgencia y severidad de un nuevo reporte de amenaza.
- **Dificultad para rastrear el estatus y progreso de la labor de solución**—Aun cuando el equipo de seguridad cuente con información confiable y oportuna acerca de una nueva

amenaza y la acción que debe tomarse para resolverlo, pocas organizaciones poseen los sistemas necesarios para rastrear efectivamente el estatus de los esfuerzos para solucionar la amenaza.

El proceso de obtener información de seguridad relevante y confiable se convierte en labor intensa y costosa para el personal de seguridad tecnológico de una organización.

SOLUCIÓN

El Security IntelliShield Alert Manager Service de Cisco es un servicio de alerta de amenaza y vulnerabilidad que permite a las organizaciones obtener fácil acceso a información oportuna y veraz acerca de potenciales vulnerabilidades en su ambiente, sin tener que invertir mucho tiempo en investigación. El servicio proporciona una solución exhaustiva y costo-efectiva para brindar la inteligencia de seguridad que las organizaciones requieren para ayudar a prevenir, mitigar y solucionar rápidamente potenciales ataques tecnológicos. Las organizaciones que utilizan el Security IntelliShield Alert Manager Service de Cisco personalizan tanto su portal al definir las redes, sistemas y aplicaciones únicas que conforman su infraestructura, como el criterio al utilizar un sistema estandarizado de calificación de riesgos para determinar las amenazas y vulnerabilidades que los afectan. El servicio proporciona alertas de inteligencia neutrales que están pre-filtradas para brindar solamente información relevante, armando al personal de seguridad con inteligencia que pueden usar para tomar rápida acción y proteger los sistemas críticos. Como resultado, el personal de seguridad puede trabajar más rápida y eficientemente y priorizar de manera más efectiva las actividades de solución de problemas.

El Security IntelliShield Alert Manager de Cisco es un importante componente de la estrategia de Red Auto-Defensiva (SDN, por sus siglas en inglés) de Cisco, la cual emplea múltiples capas de defensa. Complementa el sitio Web de inteligencia de seguridad de Cisco, http://www.MySDN.com, al brindar análisis más exhaustivo, profundo y oportuno de un amplio rango de amenazas y vulnerabilidades. Y, al contrario de las soluciones antivirus que sólo se enfocan en los bordes de la red, el Security IntelliShield Alert Manager de Cisco proporciona una cámara compensadora, única y amplia, para la más reciente información de amenazas y vulnerabilidades a través de todo el dominio corporativo tecnológico.

El Security IntelliShield Alert Manager Service de Cisco comprende cuatro componentes primarios:

- **El portal del Security IntelliShield Alert Manager de Cisco** funciona como la interfaz del cliente. El portal es seguro y completamente personalizable, permitiendo a las organizaciones recibir solamente información en redes, sistemas y aplicaciones específicas utilizadas por la organización. Las organizaciones también pueden configurar el portal para enviar notificaciones vía correo electrónico, localizador, teléfonos celular y dispositivos con capacidad SMS. Un canal SML en tiempo real también está disponible y permite a los clientes de Cisco integrar el contenido Security IntelliShield Alert Manager de Cisco en sus propias aplicaciones.
- **El Security IntelliShield Alert Manager de Cisco back-end intelligence engine** es la infraestructura que recaba información de amenazas y lleva cada nuevo reporte de amenazas y vulnerabilidad a través de un riguroso proceso de verificación, edición y publicación. Los expertos del Security IntelliShield Alert Manager de Cisco revisan y analizan cada amenaza para confirmar las características de la amenaza y la información de producto y crean una alerta en un formato estandarizado y fácil de entender. Cada amenaza es calificada de manera objetiva en términos de su urgencia, la credibilidad de la fuente y la severidad del ardid, permitiendo una comparación más fácil y un proceso de toma de decisión más rápido. Las nuevas amenazas y vulnerabilidades pueden actualizarse varias veces conforme evolucione la situación.
- **La base de datos histórica del Security IntelliShield Alert Manager de Cisco** es una de las más extensas colecciones de información pasada de amenazas y vulnerabilidad de la industria. La base de datos es investigable y tiene un índice completo, cuenta con información de los últimos seis años y contiene más de 1,700 fabricantes, 5,500 productos y 18,500 versiones distintas de aplicaciones.
- **El sistema de flujo de trabajo integrado del Security IntelliShield Alert Manager de Cisco** proporciona un mecanismo para rastrear las soluciones a las vulnerabilidades. El sistema permite a la gerencia de tecnología ver qué tareas están pendientes, a quién se le asignaron y el estatus actual de los esfuerzos de solución.

BENEFICIOS PARA EL NEGOCIO

El profesional de seguridad promedio invierte un mínimo de dos horas al día rastreando nuevas amenazas y vulnerabilidades, un total de más de 525 horas cada año solamente en actividades de investigación. Con el Security IntelliShield Alert Manager Service de Cisco, la tediosa y laboriosa investigación es conducida por los expertos en inteligencia del Security IntelliShield Alert Manager en beneficio del personal de seguridad de la organización, y los resultados se entregan directamente al personal de seguridad de tecnología cada día, sin datos superfluos que no se aplican directamente al ambiente de la organización.

Con el Security IntelliShield Alert Manager Service de Cisco, las organizaciones obtienen:

- **Uso más eficiente de los recursos del personal de seguridad**, dado que todas las alertas se entregan en un formato consistente y fácil de entender, y las organizaciones solamente reciben aquellas alertas que afectan su ambiente
- **Inteligencia de seguridad más oportuna y efectiva** a través de advertencias tempranas de forma proactiva acerca de nuevos ataques y vulnerabilidades de la tecnología
- **Análisis de alta calidad**, dado que cada alerta está personalizada, es objetiva, neutral y priorizada de acuerdo a un sistema estandarizado de calificación de riesgos
- **Solución más rápida a vulnerabilidades potenciales**, dado que muchas alertas incluyen un análisis IntelliShield de Cisco acerca de la amenaza con salvaguardas y procedimientos de derivación, así como enlaces a parches.
- **Protección continua contra amenazas y vulnerabilidades emergentes,** porque los clientes definen las redes, sistemas y aplicaciones que conforman su infraestructura y personalizan el criterio y los umbrales de riesgo para recibir notificaciones, asegurando que los clientes sólo verán la información que precisan.
- **Amplia información acerca de amenazas y vulnerabilidad**, incluyendo vulnerabilidades de seguridad, código malicioso y tendencias mundiales de seguridad que incluyen información histórica acerca de miles de fabricantes y productos

INTELIGENCIA DE SEGURIDAD ACTUALIZADA

El Security IntelliShield Alert Manager Service de Cisco es pionero en soluciones de inteligencia de seguridad en el mercado. El equipo de investigación del Security IntelliShield Alert Manager de Cisco opera las 24 horas del día, los siete días de la semana, para ofrecer a las organizaciones inteligencia actualizada, así como análisis a profundidad y validación de amenazas altamente confiable.

Sin embargo, el Security IntelliShield Alert Manager Service de Cisco es mucho más que sólo un servicio de alerta. La solución incrementa los esfuerzos de analistas internos de seguridad al brindar inteligencia de seguridad concisa e intuitiva para ayudar a las organizaciones a tomar mejores decisiones y mitigar riesgos más efectivamente. Con el Security IntelliShield Alert Manager de Cisco, las organizaciones tienen inteligencia de seguridad más oportuna, efectiva y exhaustiva y una mayor habilidad para defender su negocio proactivamente que antes.

A diferencia de otros procesos y servicios de inteligencia de seguridad, el Security IntelliShield Alert Manager Service de Cisco proporciona:

- **Reportes de inteligencia con gran amplitud y alcance**, incluyendo avanzada información y análisis de soluciones avanzadas
- **Reportes concisos y fáciles de entender**, con cada variación y actualización de una amenaza consolidada en un solo reporte, fácil de leer, en vez de ofrecer docenas de reportes separados de cientos de páginas
- **Una amplia variedad de opciones de entrega para los reportes**, incluyendo un mecanismo integrado de notificaciones que rápidamente entrega la información correcta a las personas adecuadas vía correo electrónico, localizador, teléfono celular y otros dispositivos con capacidad SMS.

POR QUÉ SERVICIOS DE CISCO

Cisco Systems y sus partners brindan un amplio portafolio de servicios y soporte de punta a punta que puede ayudarle a mejorar el costo total de propiedad de la red, así como la agilidad del negocio y la disponibilidad de la red para así incrementar el valor empresarial y el retorno en inversión de su red.

El enfoque del Lifecycle Services de Cisco define el conjunto mínimo de actividades requeridas, por tecnología y complejidad de red, para ayudarle a desplegar y operar exitosamente tecnologías Cisco, así como para optimizar el desempeño a través del ciclo de vida de su red. Este enfoque puede ayudarle a conseguir una red de alto desempeño, integrar tecnologías avanzadas, bajar costos operativos y mantener la salud de la red a través de las operaciones cotidianas.

PARA OBTENER MÁS INFORMACIÓN

Para obtener más información acerca del Security IntelliShield Alert Manager Service de Cisco, visite http://www.cisco.com/go/intellishield o contacte a su representante de cuenta local o a su partner de seguridad Cisco.

Cisco Services.
Making Networks Work.
Better Together.

Oficinas Centrales Corporativas
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Oficinas Centrales en Europa
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Oficinas Centrales en las Américas
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Oficinas Centrales en Asia Pacífico
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 317 7799

Cisco Systems tiene más de 200 oficinas en los siguientes países y regiones. Las direcciones, números telefónicos y de fax están listados en el sitio de Cisco en www.cisco.com/go/offices.

Alemania • Arabia Saudita • Argentina • Australia • Austria • Bélgica • Brasil • Bulgaria • Canadá • Chile • China PRC • Colombia • Corea • Costa Rica • Croacia • Dinamarca • Dubai, UAE • Escocia • Eslovaquia • Eslovenia • España • Estados Unidos • Filipinas • Finlandia • Francia • Grecia • Hong Kong SAR • Hungría • India • Indonesia • Irlanda • Israel • Italia • Japón • Luxemburgo • Malasia • México • Nueva Zelanda • Noruega • Países Bajos • Perú • Polonia • Portugal • Puerto Rico • Reino Unido • República Checa • Rumania • Rusia • Singapur • Sudáfrica • Suecia • Suiza • Tailandia • Taiwán • Turquía • Ucrania • Venezuela • Vietnam • Zimbabwe

XX/LW XXXXX

Impreso en los EEUU.

C00-00000-00 07/06