Sistema de supervisión, análisis y respuesta de seguridad de Cisco

Sistema de supervisión, análisis y respuesta de seguridad de Cisco

El Sistema de supervisión, análisis y respuesta de seguridad (MARS) de Cisco® es una línea de dispositivos escalables de alto rendimiento para la administración, supervisión y mitigación de amenazas que ayuda a los clientes a usar de manera más eficaz los dispositivos de red y de seguridad al combinar la supervisión de eventos de seguridad tradicional con inteligencia de red, correlación de contexto, análisis vectorial, detección de anomalías, identificación de hotspots y capacidades de mitigación automatizadas. Al combinar estas capacidades, Cisco Security MARS ayuda a las empresas a identificar y eliminar con precisión ataques contra la red y al mismo tiempo permite garantizar el cumplimiento de las políticas de seguridad de la red en todo momento.

Beneficios clave

Supervisión centralizada

Cisco Security MARS proporciona información detallada sobre la infraestructura de la red como routers, switches, firewalls, concentradores y dispositivos de puntos terminales mediante diversos registros, alertas y comunicación NetFlow. Esto permite a Cisco Security MARS procesar la información sobre amenazas hasta la dirección IP y MAC, y el puerto del switch conectado más cercano e indica la ruta del ataque a través de la red.

Depósito central de eventos

Cisco Security MARS funciona como un depósito central para todos los eventos generados por los dispositivos de seguridad tales como firewalls, servidores de autenticación, servicios de detección y prevención de intrusiones en la red, y servidores proxy. Se recopilan registros de eventos de dispositivos de la red así como registros de estaciones de trabajo y servidores proxy. Todos los eventos recopilados se correlacionan en tiempo real.

Reducción de datos

Cisco Security MARS puede reducir millones de eventos de seguridad a un puñado de informes de incidentes de red.

Mitigación oportuna de ataques

El sistema cuenta tanto con el rendimiento como con la capacidad de reconocer y recomendar la mitigación contra ataques antes de que éstos puedan afectar toda la red.

Figura 1. Implementación muy escalable

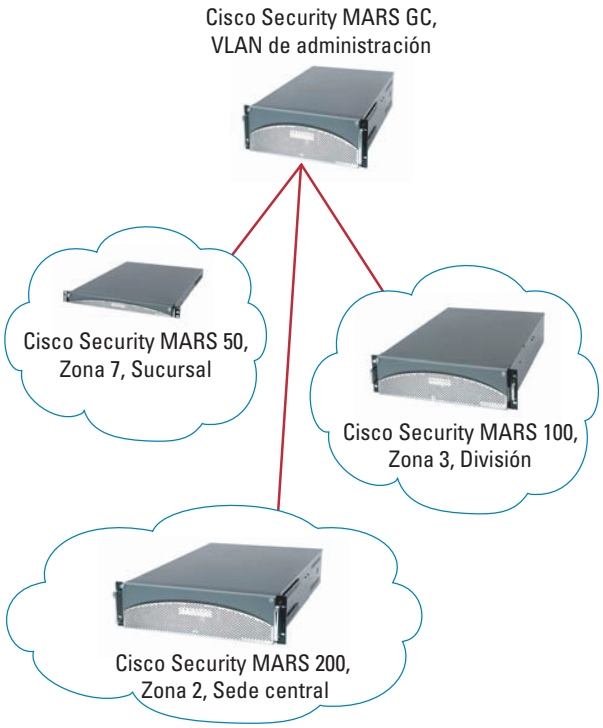
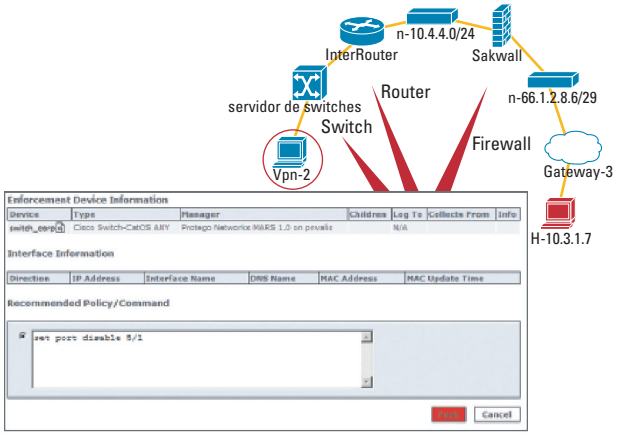
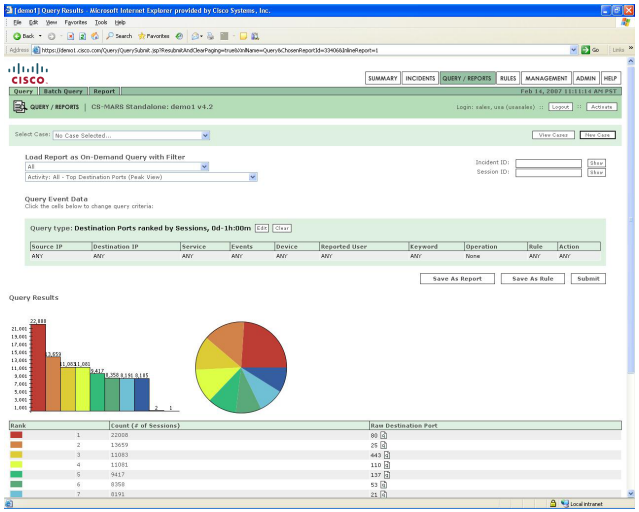


Figura 2. Aprovechamiento de la inversión para mitigación



Automated Leveraged Mitigation

Figura 3. Generación de informes avanzados



Conciencia de red de extremo a extremo

Al utilizar las configuraciones completas de todos los tipos de dispositivos de red y sistemas terminales, Cisco Security MARS integra la información sobre traducción de direcciones de red/traducción de direcciones de puertos (NAT/PAT) e información sobre direcciones MAC para identificar atacantes, objetivos y hotspots de la red en forma gráfica, lo que permite adoptar medidas en forma oportuna. Se pueden visualizar direcciones pre y pos NAT.

Evaluación integrada de vulnerabilidades

Cisco Security MARS determina si un supuesto ataque de red es genuino o un positivo falso, lo que reduce aún más la cantidad de alarmas y el tiempo necesario para adoptar medidas.

Menores costos de implementación y operación

Después de inicializarse y conectarse a la red, el sistema descubre la topología y genera un mapa. El sistema queda operativo en muy poco tiempo.

Mitigación automática

La capacidad automática de mitigación identifica dispositivos de embudo a lo largo de la ruta de ataque y permite al usuario automatizar los comandos de dispositivos apropiados para mitigar la amenaza. Además, muchos atributos esenciales, como direcciones MAC, nombre de estación de trabajo de Windows, nombre de usuario de red VPN, y puerto de switch físico de primer salto se identifican automáticamente. Los resultados pueden usarse para evitar ataques en forma rápida y precisa a fin de reducir al mínimo los daños.

Correlación de eventos con inteligencia de red

Cisco Security MARS obtiene inteligencia de red al comprender la topología y las configuraciones de los dispositivos de routers, switches, herramientas de análisis de vulnerabilidades y firewalls, y al generar perfiles del tráfico de la red. La capacidad de descubrimiento integrada del sistema genera un mapa de la topología de la red que contiene la configuración de los dispositivos y las políticas de seguridad actuales, lo que permite a Cisco Security MARS crear modelos de flujos de paquetes a través de la red. Debido a que el dispositivo no opera en línea y hace un uso mínimo de los agentes de software existentes, no afecta el rendimiento de la red ni del sistema.

Análisis Netflow

Cisco Security MARS recopila datos NetFlow de los routers con una rapidez de hasta 300.000 flujos por segundo. Los registros de NetFlow y firewall se utilizan para analizar el uso de la red hasta la estación de trabajo específica. Esto permite a los administradores detectar y tomar medidas contra anomalías, como la presencia de virus y gusanos.

Tabla1. Línea de productos de Cisco Security MARS

Modelos de controlador local	Eventos/ Seg.[1]	NetFlows/ Seg.	Almacenamiento	Unidad de bastidor	Tipo de controlador global	Alimentación
Cisco Security MARS 20R (CS-MARS-20R-K9)	50	1500	120 GB (no RAID)	1 RU x 16 pulg.	GC, GCm	300W, 120/240V selección automática
Cisco Security MARS 20 (CS-MARS-20-K9)	500	15.000	120 GB (no RAID)	1 RU x 16 pulg.	GC, GCm	300W, 120/240V selección automática
Cisco Security MARS 50 (CS-MARS-50-K9)	1.000	30.000	240 GB RAID 0	1 RU x 25,6 pulg.	GC, GCm	300W, 120/240V selección automática
Cisco Security MARS 100e (CS-MARS-100e-K9)	3000	75.000	750 GB RAID 10 de intercambio inmediato	3 RU x 25,6 pulg.	GC, GCm	500W redundante doble, 120/240V selección automática
Cisco Security MARS 100 (CS-MARS-100-K9)	5000	150.000	750 GB RAID 10 de intercambio inmediato	3 RU x 25,6 pulg.	GC, GCm	500W redundante doble, 120/240V selección automática
Cisco Security MARS 200 (CS-MARS-200-K9)	10.000	300.000	1.000 GB RAID 10 de intercambio inmediato	4 RU x 25,6 pulg.	GC, GCm	500W redundante doble, 120/240V selección automática
Cisco Security MARS 110R (CS-MARS-110R-K9)	4.500	75.000	1.500 GB RAID 10 de intercambio inmediato	2 RU x 27 3/4" (P); 3,44" (Al); 19" (An)	GC2	2x 750 W redundante doble, 120/240V selección automática
Cisco Security MARS 110 (CS-MARS-110-K9)	7.500	150.000	1.500 GB RAID 10 de intercambio inmediato	2 RU x 27 3/4" (P); 3,44" (Al); 19" (An)	GC2	2x 750 W redundante doble, 120/240V selección automática
Cisco Security MARS 210 (CS-MARS-210-K9)	15.000	300.000	2.000 GB RAID 10 de intercambio inmediato	2 RU x 27 3/4" (P); 3,44" (Al); 19" (An)	GC2	2x 750 W redundante doble, 120/240V selección automática

Modelos de controlador global	Modelos compatibles	Conexiones máximas	Almacenamiento	Unidad de bastidor	Alimentación
Cisco Security MARS GCm (CS-MARS-GCm-K9)	Cisco Security MARS 20R/20 y 50 solamente	5	1 TB RAID 10 de intercambio inmediato	4 RU x 25,6" (P); 19" (An)	2x 500 W redundante doble, 120/240V selección automática
Cisco Security MARS GC (CS-MARS-GC-K9)	Cisco Security MARS 20R/20, 50, 100e/100, 200	Actualmente sin restricción	1 TB RAID 10 de intercambio inmediato	4 RU x 25,6 pulg.	2x 500W redundante doble, 120/240V selección automática
Cisco Security MARS GC2 (CS-MARS-GC2-K9)	Cisco Security MARS 110R/110 y 210 solamente	Actualmente sin restricción	2 TB RAID 10 de intercambio inmediato	2 RU x 27 3/4" (P); 3,44" (Al); 19" (An)	2x 750 W redundante doble, 120/240V selección automática

En el segundo trimestre de 2007, se lanzarán al mercado modelos de dispositivos actualizados de Cisco Security MARS. Estos dispositivos nuevos son los modelos 110R, 110, 210 y GC2. Los nuevos modelos proporcionarán mayores capacidades de rendimiento y almacenamiento. Estos nuevos modelos usarán versiones de software 5.2.4 y superiores, mientras que los modelos 20R, 20, 50, 100e, 100, 210, GC, y GCm continuarán utilizando versiones de software 4.x. Se conservará la paridad general de características entre las versiones 4.x y 5.x, como (entre otras) la compatibilidad de dispositivos, compatibilidad de firmas, correcciones de fallas y características no afectadas por las diferencias de hardware entre las dos plataformas.

[1] Eventos por segundo: Cantidad máxima de eventos por segundo con correlación dinámica y todas las características habilitadas.

Sistema de supervisión, análisis y respuesta de seguridad de Cisco

Correlación de contexto

La correlación de contexto usa inteligencia a nivel de red para agrupar en sesiones múltiples eventos de seguridad y comportamientos de red entre fronteras NAT e identifica incidentes válidos mediante la aplicación a múltiples sesiones de reglas de correlación definidas por el usuario y del sistema. Cisco Security MARS viene con un completo conjunto de reglas predefinidas que Protego actualiza con frecuencia y que identifican la mayoría de los escenarios de ataques combinados, ataques de día cero y gusanos. Un marco gráfico de definición de reglas simplifica la creación de reglas personalizadas definidas por el usuario para cualquier aplicación. La correlación de contexto reduce significativamente los datos sin procesar de eventos, facilita la asignación de prioridades y maximiza los resultados de las contramedidas implementadas.

Arquitectura escalable y de alto rendimiento

Cisco Security MARS captura eventos a una velocidad de hasta 10.000 eventos por segundo en un solo dispositivo. Cuando se debe usar más de un dispositivo, puede implementarse en el sitio central el controlador Cisco Security MARS Global Controller. Global Controller recopila los incidentes de cada uno de los controladores locales. Como el control local hace la mayor parte del trabajo en esta arquitectura, se logra un incremento casi lineal del rendimiento con cada controlador local implementado.

Especificaciones del hardware

- Dispositivos de 19 pulgadas construidos para fines específicos y montables en bastidor; con aprobaciones UL, FCC, CE y VCCI
- Sistema operativo con seguridad reforzada; con la mayoría de los servicios de red inhabilitados
- Dos interfaces 10/100/1000 Ethernet; DVD-ROM con medios de recuperación
- Almacenamiento: RAID 0 para Cisco Security MARS 50; RAID 10 de intercambio inmediato para Cisco Security MARS 100, 200 y Global Controller (GC)
- Distribución de carga redundante de 500 vatios (W); selección automática de 120/240 voltios para los modelos 100e/110R y superiores

Investigaciones e informes de cumplimiento de normas de seguridad en tiempo real

Cisco Security MARS cuenta con un marco de análisis fácil de usar que simplifica el flujo de trabajo de seguridad convencional, al automatizar diversas funciones como asignación de casos, investigación, escalamiento, notificación y anotación para operaciones diarias y auditorías especializadas. Puede reproducir gráficamente los ataques y recuperar los datos de eventos almacenados para analizar eventos anteriores. El sistema es totalmente compatible con consultas especiales sobre esfuerzos de minería de datos en tiempo real y subsiguientes. Cisco Security MARS ofrece diversos informes predefinidos para satisfacer los requisitos operativos y ayudar a cumplir la normativa vigente como SOX, GLBA, HIPAA, FISMA y Basilea II. Un generador intuitivo de informes permite modificar los más de 100 informes estándar o generar informes nuevos para fines ilimitados como: planes de acción y solución, informes de actividad de la red e incidentes, informes sobre posición y auditoría de seguridad, además de informes departamentales: en formatos de datos, tendencias y gráficos. El sistema también permite generar informes por lotes y por correo electrónico.

Administración

- Interfaces Web seguras (HTTPS), administración basada en funciones, registro completo de auditoría de usuarios
- Escalamiento de incidentes, flujo de trabajo y notificación mediante correo electrónico, buscapersonas, registro de sistema y el Protocolo simple de administración de redes (SNMP)
- Administración jerarquizada de Cisco Security MARS GC de múltiples dispositivos Cisco Security MARS
- Admite actualizaciones: compatibilidad con dispositivos, nuevas reglas y características
- Archivo comprimido continuo de datos no procesados e incidentes se almacena fuera de línea en un servidor NFS

Consultas e informes

- La interfaz gráfica de usuario permite realizar diversas consultas predeterminadas y personalizadas
- Más de 100 informes populares: informes de administración, operación y de cumplimiento de la normativa vigente
- Generación intuitiva de una cantidad ilimitada de informes personalizados
- Los informes con formato de datos, gráficos y tendencias pueden exportarse en formato HTML y CSV
- Sistema de informes: especiales, por lotes, plantillas y envío por correo electrónico

Descubrimiento de topología

- Capa 3 y 2: routers, switches, firewalls
- IDS de red: tarjetas y dispositivos
- Descubrimiento manual y programado
- Protocolos SSH, SNMP, Telnet y comunicaciones para dispositivos específicos
- Archivo de semilla en vez de descubrimiento