# Sistema de Monitoração, Análise e Respostas de Segurança da Cisco

## Cisco Security Monitoring Analysis and Response System

O Cisco® MARS (Sistema de Monitoração, Análise e Respostas de Segurança) é uma família de dispositivos de alto desempenho e escaláveis para gerenciamento, monitoração e mitigação de ameaças que permite utilizar com eficiência os dispositivos de segurança e rede, combinando a monitoração de eventos de segurança tradicional com inteligência de rede, correlação contextual, análise de vetores, detecção de anomalias, identificação de hotspots e capacidades de mitigação automatizadas. Combinando esses recursos, o Cisco Security MARS identifica com mais precisão e elimina os ataques à rede e, ao mesmo tempo, mantém a conformidade da rede.

## Principais benefícios

### Monitoração centralizada

O Cisco MARS fornece informações detalhadas sobre a infra-estrutura da rede, incluindo roteadores, switches, firewalls, concentradores de VPN e dispositivos de ponto terminal através de diversos registros de dispositivos, alertas e comunicações do NetFlow. Ele permite que o Cisco Security MARS processe as informações das ameaças até o endereço IP e MAC, e a porta de switch mais próxima, além de fornecer um caminho para ataque através da rede.

### Repositório de eventos central

O Cisco Security MARS serve como repositório central para todos os eventos gerados por dispositivos de segurança, como firewalls, servidores de autenticação, serviços de prevenção e detecção de invasão da rede, e servidores proxy. Os eventos de dispositivos de rede e os registros de estações de trabalho e servidores também são coletados. Todos os eventos coletados são inter-relacionados em tempo real.

### Redução de dados

O Cisco Security MARS pode reduzir milhões de eventos de segurança a alguns poucos incidentes de rede.

### Mitigação de ataque oportuna

O desempenho e a especialização do sistema permitem reconhecer e recomendar ações para redução dos ataques antes que eles consigam derrubar toda a rede.

**Figura 1. Implementação altamente escalável**

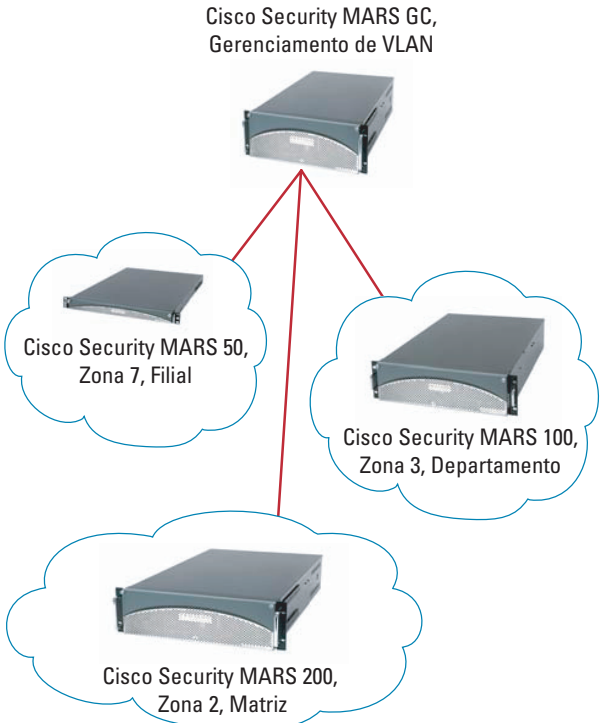
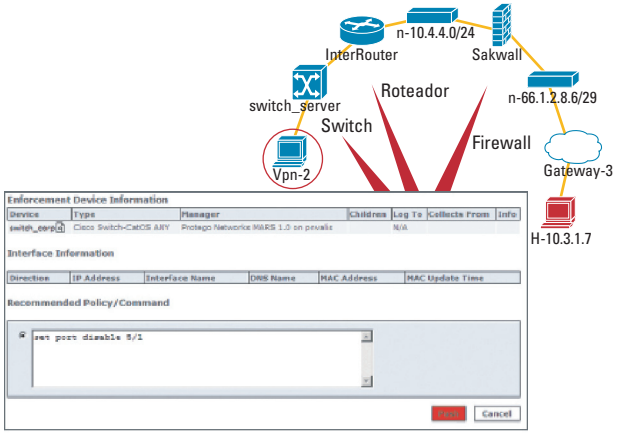
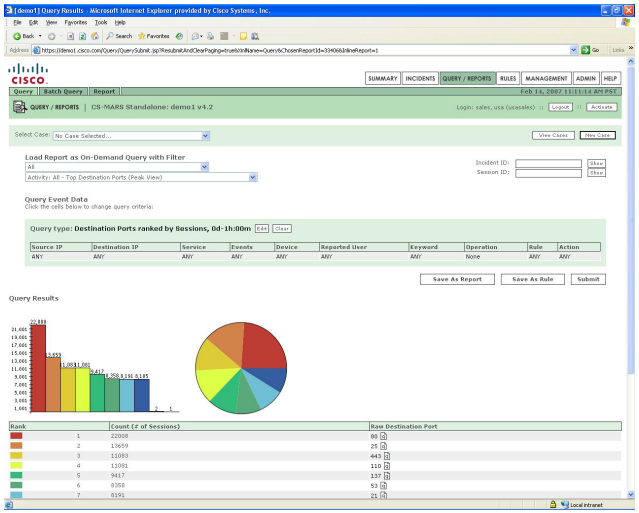



**Figura 2. Otimiza investimento para minimizar**




*Automated Leveraged Mitigation*

**Figura 3. Relatórios Avançados**



### Conscientização de rede total

Utilizando as configurações completas de todos os tipos de dispositivos e sistemas da rede, o Cisco Security MARS integra o NAT/PAT (Network Address Translation/Port Address Translation) e informações de endereços MAC para identificar invasores, alvos e hotspots da rede em formato gráfico possibilitando uma reação rápida. Endereços pré e pós-NAT podem ser exibidos.

### Avaliação de vulnerabilidade integrada

O Cisco Security MARS determina se um possível ataque à rede é genuíno ou um falso positivo, reduzindo ainda mais o número de alarmes.

### Redução dos custos de implementação e operação

Após o *bootstrapping* e conexão à rede, o sistema identifica e mapeia a topologia. O sistema torna-se operacional em muito pouco tempo.

### Mitigação automática

O recurso de mitigação automática identifica os dispositivos de gargalo disponíveis ao longo do caminho do ataque e capacita o usuário a automatizar comandos apropriados dos dispositivos para mitigar a ameaça. Além disso, muitos atributos essenciais, como endereços MAC, nome de estação de trabalho do Windows, nome de usuário de VPN e primeira porta switch física de um ataque são automaticamente identificados. Os resultados podem ser usados para impedir ataques e minimizar danos com rapidez e precisão.

### Correlação inteligente dos eventos da rede

O Cisco Security MARS obtém inteligência de rede compreendendo a topologia e as configurações dos dispositivos roteadores, switches, ferramentas de análise de vulnerabilidade e firewalls, e criando um perfil do tráfego da rede. A função integrada de descoberta da rede do sistema cria um mapa da topologia com a configuração dos dispositivos e as políticas de segurança atuais, permitindo que o Cisco Security MARS modele os fluxos de pacotes na rede. Como o dispositivo não opera inline e usa muito pouco os agentes de software existentes, isso não afeta o desempenho da rede e do sistema.

### Análise do Netflow

O Cisco Security MARS coleta dados do NetFlow de roteadores que chegam a atingir uma velocidade de 300.000 fluxos por segundo. Os registros do NetFlow e do firewall são usados para analisar o uso da rede por cada estação de trabalho específica. Isso permite que os administradores detectem e reajam a anomalias, como a presença de vírus e worms.

**Tabela 1. Linha de produto Cisco Security MARS**

| Modelos de controlador local | Eventos/seg[1] | NetFlows/seg | Armazenamento | Unidade de rack | Tipo de controlador global | Potência |
|---|---|---|---|---|---|---|
| Cisco Security MARS 20R (CS-MARS-20R-K9) | 50 | 1.500 | 120 GB (não-RAID) | 1 UR x 16 pol. | GC, GCm | Autoswitch 300W, 120/240V |
| Cisco Security MARS 20 (CS-MARS-20-K9) | 500 | 15.000 | 120 GB (não-RAID) | 1 UR x 16 pol. | GC, GCm | Autoswitch 300W, 120/240V |
| Cisco Security MARS 50 (CS-MARS-50-K9) | 1.000 | 30.000 | 240 GB RAID 0 | 1 UR x 25,6 pol. | GC, GCm | Autoswitch 300W, 120/240V |
| Cisco Security MARS 100e (CS-MARS-100e-K9) | 3.000 | 75.000 | 750 GB RAID 10 de troca ativa | 3 UR x 25,6 pol. | GC, GCm | Autoswitch de 500W de dupla redundância, 120/240V |
| Cisco Security MARS 100 (CS-MARS-100-K9) | 5.000 | 150.000 | 750 GB RAID 10 de troca ativa | 3 UR x 25,6 pol. | GC, GCm | Autoswitch de 500W de dupla redundância, 120/240V |
| Cisco Security MARS 200 (CS-MARS-200-K9) | 10.000 | 300.000 | 1.000 GB RAID 10 de troca ativa | 4 UR x 25,6 pol. | GC, GCm | Autoswitch de 500W de dupla redundância, 120/240V |
| Cisco Security MARS 110R (CS-MARS-110R-K9) | 4.500 | 75.000 | 1.500 GB RAID 10 de troca ativa | 2 UR x 27 ¾ pol. (P); 3,44 pol (A); 19 pol. (L) | GC2 | Autoswitch de 2x750 W de dupla redundância, 120/240V |
| Cisco Security MARS 110 (CS-MARS-110-K9) | 7.500 | 150.000 | 1.500 GB RAID 10 de troca ativa | 2 UR x 27 ¾ pol. (P); 3,44 pol (A); 19 pol. (L) | GC2 | Autoswitch de 2x750 W de dupla redundância, 120/240V |
| Cisco Security MARS 210 (CS-MARS-210-K9) | 15.000 | 300.000 | 2.000 GB RAID 10 de troca ativa | 2 UR x 27 ¾ pol. (P); 3,44 pol (A); 19 pol. (L) | GC2 | Autoswitch de 2x750 W de dupla redundância, 120/240V |

| Modelos de controladores globais | Modelos aceitos | Máximo de conexões | Armazenamento | Unidade de rack | Potência |
|---|---|---|---|---|---|
| Cisco Security MARS GCm (CS-MARS-GCm-K9) | Cisco Security MARS 20R/20 & 50 apenas | 5 | 1 TB RAID 10 de troca ativa | 4 UR x 25,6 pol (P); 19 pol. (L). | Autoswitch de 2x500 W de dupla redundância, 120/240V |
| Cisco Security MARS GC (CS-MARS-GC-K9) | Cisco Security MARS 20R/20, 50, 100e/100, 200 | Não restrito | 1 TB RAID 10 de troca ativa | 4 UR x 25,6 pol. | Autoswitch de 2x500W de dupla redundância, 120/240V |
| Cisco Security MARS GC2 (CS-MARS-GC2-K9) | Cisco Security MARS 110R/110 & 210 apenas | Não restrito | 2 TB RAID 10 de troca ativa | 2 UR x 27 ¾ pol. (P); 3,44 pol (A); 19 pol. (L) | Autoswitch de 2x750 W de dupla redundância, 120/240V |

No segundo trimestre de 2007, o Cisco Security MARS liberará modelos de dispositivos atualizados. Esses novos dispositivos são os modelos 110R, 110, 210 e GC2 . Os novos modelos fornecerão mais recursos de desempenho e armazenamento. Esses novos modelos usarão software versões 5.2.4 e superior, enquanto o 20R, 20, 50, 100e 100, 210, GC e GCm continuarão a usar as versões de software 4.x. A paridade dos recursos gerais será mantida entre os releases 4.x e 5.x, incluindo (mas não limitado) suporte a dispositivo, suporte a assinaturas, correções de problemas e recursos não afetados por diferenças de hardware das duas plataformas.

[1] Eventos por segundo: Máximo de eventos por segundo com uma correção dinâmica e todos os recursos ativados.

# Sistema de Monitoração, Análise e Respostas de Segurança da Cisco

### Correlação contextual

A correlação contextual usa inteligência de rede para agrupar vários eventos de segurança e comportamento de rede através de limitações NAT nas sessões e identifica incidentes válidos aplicando regras de correlação definidas pelo usuário e pelo sistema a várias sessões. O Cisco Security MARS é fornecido com um conjunto completo de regras predefinidas, freqüentemente atualizadas pela Protego, que identificam a grande maioria dos cenários de ataques compostos, ataques de dia zero e worms. Uma estrutura de definição de regras gráficas simplifica a criação de regras personalizadas definidas pelo usuário para qualquer aplicativo. A Correlação Contextual reduz consideravelmente os dados de eventos não-processados , facilita a priorização de respostas e maximiza os resultados das medidas preventivas implementadas.

### Arquitetura de alto desempenho e escalável

O Cisco Security MARS captura eventos com uma rapidez de até 10.000 por segundo em uma única caixa. Quando a necessidade se estende além de uma única caixa, o Cisco Security MARS Global Controller pode ser implementado no ponto central. O Global Controller agrega os incidentes dos controladores locais individuais. O controle local é responsável pela maior parte do trabalho nesta arquitetura e, portanto, obtém-se um aumento de desempenho praticamente linear a cada controlador local implementado.

## Especificações de hardware

- Dispositivos montáveis em rack de 19 pol. para fins específicos; UL, FCC, CE e VCCI aprovados
- Sistema operacional fortalecido com segurança, com a maioria dos serviços de rede desativada
- Duas interfaces 10/100/1000 Ethernet e DVD-ROM com mídia para recuperação
- Armazenamento: RAID 0 para Cisco Security MARS 50; RAID 10 de troca ativa para Cisco Security MARS 100, 200 e Global Controller (GC)
- Potência de 500 watts (W) compartilhando carga redundante; autoswitch de 120/240 volts para os modelos 100e/110R e superiores

## Relatório de conformidade e investigação em tempo real

O Cisco Security MARS oferece uma estrutura de análise fácil de usar que simplifica o fluxo de trabalho de segurança convencional, automatizando a atribuição de casos, investigação, escala, notificação e anotação para operações diárias e auditorias especializadas. Ele pode reproduzir graficamente os ataques e recuperar os dados dos eventos armazenados para analisar eventos anteriores. O sistema oferece total suporte a consultas especiais para esforços de data-mining (extração de dados) em tempo real e subseqüentes. O Cisco Security MARS traz inúmeros relatórios predefinidos para satisfazer os requisitos operacionais e auxiliar nos esforços de conformidade com as regulamentações, incluindo SOX, GLBA, HIPAA, FISMA e Basel II. Um gerador de relatório intuitivo permite modificar mais de 100 relatórios padrão ou gerar uma quantidade ilimitada de novos relatórios para: planos de ação e correção, incidentes e atividades de rede, postura de segurança e auditoria, além de relatórios por departamentos e, formatos de dados, tendências e gráficos. O sistema também fornece relatórios em lote e por e-mail.

## Administração

- Interface da Web segura (HTTPS), administração por função, trilha de auditoria de usuário completa
- Escala de incidentes, fluxo de trabalho e notificação por e-mail, pager, syslog e SNMP (Simple Network Management Protocol)
- Gerenciamento hierárquico do Cisco Security MARS GC de vários dispositivos Cisco Security MARS
- Suporte a atualizações: suporte de dispositivo, novas regras e recursos
- Dados de incidentes e dados não-processados compactados são armazenados continuamente em arquivo do NFS (Network File Sharing) off-line

## Consulta e Relatórios

- A GUI oferece suporte a diversos padrões e consultas personalizadas
- Mais de 100 relatórios populares: administrativos, operacionais e de regulamentações
- Geração de relatórios intuitivos para relatórios personalizados ilimitados
- Formatos de dados, gráficos e tendência que oferecem suporte a HTML e exportação de CSV
- Sistema de relatórios: especial, em lote, por modelo e com encaminhamento por e-mail

## Identificação da topologia

- Camada 3 e Camada 2: roteadores, switches, firewalls
- IDS de rede: componentes e dispositivos
- Descoberta manual e agendada
- SSH, SNMP, Telnet e comunicações específicas de cada dispositivo
- Arquivo semente, em vez de descoberta