CISCO SECURITY MONITORING ANALYSIS AND RESPONSE SYSTEM AT–A–GLANCE

CISCO SECURITY MONITORING ANALYSIS AND RESPONSE SYSTEM

The Cisco® Security Monitoring Analysis and Response System (MARS) is a family of high-performance, scalable appliances for threat management, monitoring, and mitigation that helps customers to make more effective use of network and security devices by combining traditional security event monitoring with network intelligence, context correlation, vector analysis, anomaly detection, hotspot identification, and automated mitigation capabilities. By combining these capabilities, Cisco Security MARS helps companies to accurately identify and eliminate network attacks while maintaining network compliance.

KEY BENEFITS

Centralized Monitoring

Cisco Security MARS provides detailed information about the network infrastructure including routers, switches, firewalls, VPN concentrators, and endpoint devices through a variety of device logs, alerts, and NetFlow communication. This enables Cisco Security MARS to process threat information down to the IP and MAC address and the nearest attached switch port, and provides the attack path through the network.

Central Event Repository

Cisco Security MARS serves as a central repository for all events generated by security devices, such as firewalls, authentication servers, network intrusion detection and prevention services, and proxy servers. Network device events as well as workstations and servers logs are also collected. All collected events are cross-correlated in real time.

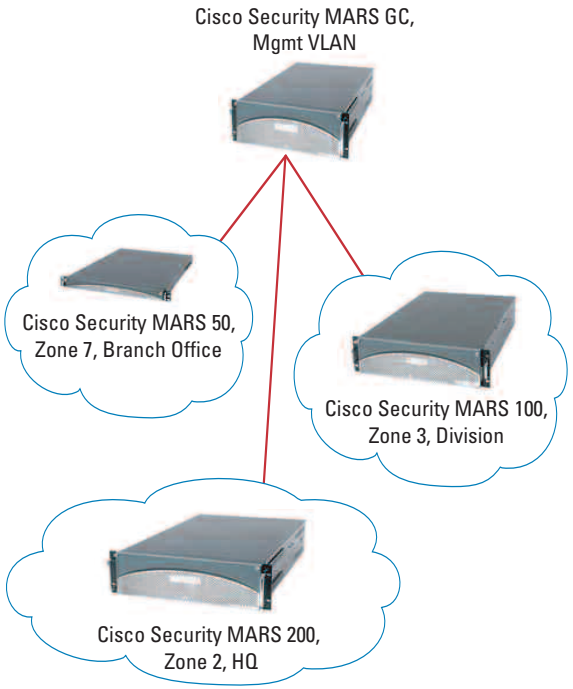
Data Reduction

Cisco Security MARS can reduce millions of security events to a handful of actual reported network incidents.

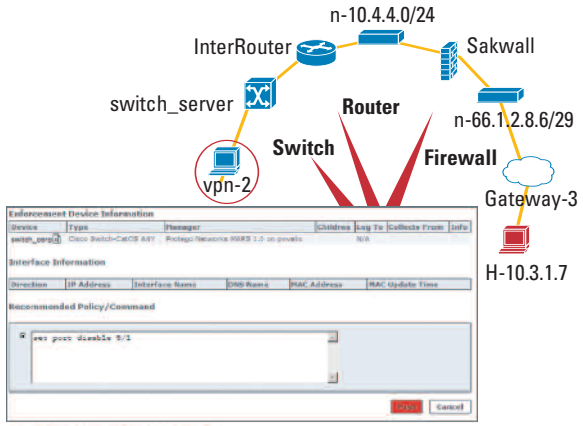
Timely Attack Mitigation

The system has both the performance and the built-in expertise to recognize and recommend mitigation for attacks before they can bring down an entire network.

Highly Scalable Deployment



Leverage Investment to Mitigate



Automated Leveraged Mitigation

Advanced Reporting

Compliance and Operational Management Reporting

End-to-End Network Awareness

Using the full configurations of all types of network devices and end systems, Cisco Security MARS integrates Network Address Translation/Port Address Translation (NAT/PAT) and MAC address information to identify attackers, targets, and network hot spots in graphical form for quick action. Pre- and post-NAT addresses can be displayed.

Integrated Vulnerability Assessment

The Cisco Security MARS determines whether a possible network attack is genuine or a false positive, further reducing the number of alarms and the time needed to take action.

Reduced Deployment and Operational Cost

After bootstrapping and connecting to the network, the system discovers and maps the topology. The system becomes operational in a very short period of time.

Automatic Mitigation

The automatic mitigation capability identifies available choke-point devices along the attack path and empowers the user to automate appropriate device commands to mitigate the threat. In addition, many essential attributes, such as MAC addresses, Windows workstation name, VPN username, and first-hop physical switch port of an attack are automatically identified. The results can be used to quickly and accurately thwart attacks and minimize damage.

CISCO SECURITY MONITORING ANALYSIS AND RESPONSE SYSTEM AT–A–GLANCE

Network-Intelligent Event Correlation

Cisco Security MARS obtains network intelligence by understanding the topology and device configurations from routers, switches, vulnerability analysis tools, and firewalls, and by profiling network traffic. The system's integrated network discovery builds a topology map containing device configuration and current security policies. enabling Cisco Security MARS to model packet flows through your network. Because the appliance does not operate inline and makes minimal use of existing software agents, it does not affect network or system performance.

SureVector Analysis

The SureVector Analysis feature helps enable broader management scope, faster investigation, and increased response time. With SureVector Analysis, administrators can visibly and accurately trace the attack path, obtain details on the raw events that precede the incident, and pinpoint the source of the anomalous and attack behavior. As a result, a more complete and accurate analysis can be completed in real time, and thus the attack can be subverted.

Netflow Analysis

The Cisco Security MARS collects NetFlow data from routers as quickly as 300,000 flows per second. NetFlow and firewall logs are used to analyze network usage down to the specific workstation. This allows administrators to detect and take action against anomalies, such as the presence of viruses and worms.

Context Correlation

Context Correlation uses network-level intelligence to group multiple security events and network behavior across NAT boundaries into sessions and identifies valid incidents by applying system and user-defined correlation rules to multiple sessions. Cisco Security MARS ships with a full complement of predefined rules, frequently updated by Protego, that identify a majority of blended attack scenarios, day-zero attacks, and worms. A graphical rule-definition framework simplifies the creation of user-defined custom rules for any application. Context Correlation significantly reduces raw event data, facilitates response prioritization, and maximizes results from deployed countermeasures.

High-Performance and Scalable Architecture

Cisco Security MARS captures events as quickly as 10,000 per second on a single box. When the requirement extends beyond a single box, the Cisco Security MARS Global Controller can be deployed at the central site. The Global Controller aggregates the incidents from the individual Local Controllers. The local control does most of the work in this architecture and therefore near-linear incremental performance is realized with each Local Controller deployed.

Cisco Part Number (Protego Models)	Performance		Storage	Form Factor	Power Supply
	Events per Second	NetFlows per Second			
CS-MARS-20-K9	500	15,000	120 GB (non-RAID)	1 RU x 16 in.	300W
CS-MARS-50-K9	1000	30,000	240 GB RAID 0	1 RU x 25.6 in.	300W
CS-MARS-100E-K9	3000	75,000	750 GB RAID 10 Hot swappable	3 RU x 25.6 in.	500W dual redundant
CS-MARS-100-K9	5000	150,000	750 GB RAID 10 Hot swappable	3 RU x 25.6 in.	500W dual redundant
CS-MARS-200-K9	10,000	300,000	1 TB RAID 10 Hot swappable	4 RU x 25.6 in.	500W dual redundant
Cisco Part Number (Protego Global Controller Models)	**Distributed Monitoring**		**Storage**	**Form Factor**	**Power Supply**
	Models Supported	Maximum Connections			
CS-MARS-GCM-K9	From MARS 20 or 50 only	5	1 TB RAID 10 Hot swappable	4 RU x 25.6 in.	500W dual redundant
CS-MARS-GC-K9	Any	Not restricted	1 TB RAID 10 Hot swappable	4 RU x 25.6 in.	500W dual redundant

Cisco Security MARS 20

Cisco Security MARS 50

Cisco Security MARS 100e

Cisco Security MARS 100

Cisco Security MARS 200

Cisco Security MARS GC

CISCO SECURITY MONITORING ANALYSIS AND RESPONSE SYSTEM AT–A–GLANCE

HARDWARE SPECIFICATIONS

- Purpose-built, 19-inch rack-mountable appliances; UL, FCC, CE, and VCCI approved
- Security-hardened OS; with most network services disabled
- Two 10/100/1000 Ethernet interfaces; DVD-ROM with recovery media
- Storage: RAID 0 for Cisco Security MARS 50; RAID 10 hot swappable for Cisco Security MARS 100, 200, and Global Controller (GC)
- Redundant load sharing 500-watt (W) power; 120/240-volt autoswitch

REAL-TIME INVESTIGATION AND COMPLIANCE REPORTING

Cisco Security MARS boasts an easy-to-use analysis framework that simplifies conventional security workflow, providing automated case assignment, investigation, escalation, notification, and annotation for daily operations and specialized audits. It can graphically replay attacks and retrieve stored event data to analyze previous events. The system fully supports special queries for real-time and subsequent data-mining efforts. Cisco Security MARS offers numerous predefined reports to satisfy operational requirements and assist in regulatory-compliance efforts including Sarbox, GLBA, HIPAA, FISMA, and Basel II. An intuitive report generator can modify the more than 100 standard reports or generate new reports for an unlimited means to build: action and remediation plans, incident and network activity, security posture and audit, as well as departmental reports—in data, trend, and chart formats. The system also provides for batch and e-mail reporting.

ADMINISTRATION

- Secure Web interface (HTTPS), roles-based administration, full user audit trail
- Incident escalation, workflow, and notification through e-mail, pager, syslog, and Simple Network Management Protocol (SNMP)
- Cisco Security MARS GC hierarchical management of multiple Cisco Security MARS appliances
- Automated, verified updates: device support, new rules, and features
- Continuous compressed raw data and incident archive to offline Network File Sharing (NFS) storage

QUERY AND REPORTING

- GUI supports numerous default and customized queries
- More than 100 popular reports: management, operational, and regulatory
- Intuitive report generation for unlimited customized reports
- Data, chart, and trend formats support HTML and CSV export
- Report system: special, batch, template, and e-mail forwarding

TOPOLOGY DISCOVERY

- Layer 3 and Layer 2: routers, switches, firewalls
- Network IDS: blades and appliances
- Manual and scheduled discovery
- SSH, SNMP, Telnet, and device-specific communications
- Seed file instead of discovery

205314.J_ETMG_LF_6.05