Cisco Security Remote Management Services for Intrusion Prevention Systems (IPS)

Today's threat landscape is dynamic and ever-evolving, with over 70,000 new threats surfacing per day. As threats and attacks become more sophisticated it is paramount to have the critical security expertise, security intelligence and proactive operational security management capabilities to ensure the safeguard of critical assets and infrastructure. To meet the challenge and remain ahead, enterprises must move away from basic monitoring and alerting to preventative mitigations based on actionable intelligence.

Cisco Remote Management Services for Security

Cisco® Remote Management Services (RMS) for Security provides 24/7/365 proactive threat monitoring and management services for advanced and emerging security technologies and network architectures. Utilizing a proven delivery methodology based on ITIL® while delivered within a co-managed framework, Cisco RMS for Security ensures operation excellence and complete customer control. Cisco RMS for Security provides a proactive, holistic approach to monitoring, managing and protecting critical network infrastructures ensuring business continuity. Built on an advanced, extensible Cisco Security Platform and embedded with real-time intelligence from Cisco Security Intelligence Operations, the Cisco RMS for Security architecture is a proven and unparalleled.

Cisco Security Intelligence Operations

Inform, Protect, Respond

Cisco Security Intelligence Operations (SIO) provides early-warning intelligence, threat and vulnerability analysis and proven Cisco mitigation solutions to ensure protection from new and emerging threats.

The Cisco Security Intelligence Operations (SIO) telemetry infrastructure consists of over 700k global sensors which continuously collect, analyze, classify and disseminate actionable security intelligence. The RMS Security Operations Center (SOC) incorporates this security intelligence combined with customer specific security analysis to proactively prevent and mitigate security threats and attacks for Cisco RMS Security customers.

The Cisco Security Intelligence Operations (SIO) includes:

- **Cisco Security Operations Center (SOC)**—Global team responsible for the monitoring, management and security of Cisco Security Remote Management Services customers
- **Product Security Incident Response Team (PSIRT)**—Global team responsible for the management, investigation and reporting of vulnerability information for Cisco products
- **Computer Security Incident Response Team (CSIRT)**—Cisco internal security incident and response team
- **Security Research Operations (SRO)**—A highly skilled security organization with deep security domain knowledge and expertise responsible for delivering security mitigations and remediations
- **IntelliShield**—Up to the minute actionable security intelligence, vulnerability analysis and threat identification
- **IPS Signature Team**—Expert team responsible for vulnerability research and the creation of Cisco IPS signatures
- **SenderBase**—Real-time global security telemetry data, threat analysis and reputation scoring

Cisco Security Services for Cisco IPS

Cisco Remote Management Services for Security provides a 24/7/365 industry leading, proactive and cost-effective solution for monitoring and management of Cisco IPS appliances and modules. Armed with the latest security intelligence and industry-level expertise the Security Operations Center (SOC) provides real-time surveillance in order to protect and prevent against attacks, malware, worms, and internet based attacks targeting critical business assets. Cisco Security RMS for IPS provides continuous proactive threat analysis, event classification, automated notifications, mitigation and reporting all accessible via a secure web portal. The continuous lifecycle of IPS policy reviews, signature updates, critical asset identification, signature tuning, and event analysis and classification are managed by Cisco security professionals. Two levels of service are available, which are designed to ensure each enterprise is provided the protection and required security operational scale.

Q&A Examples

Q. What is the service activation process of tuning and implementing IPS monitoring and management?

A. The service activation process for IPS includes an initial review of the current IPS policy, signature deployment, customer network traffic patterns, critical assets and applications. This information coupled with external security intelligence, analysis of events and customer architecture provides the baseline of the initial IPS security policy.

Q. How are IPS polices maintained and updated?

A. Security RMS conducts monthly reviews of all managed security devices and ensures that the applied policy is up to date with customer internal and regulatory policies and standards. Policy audits and reviews are shared with the customer to ensure that the corporate access control policy remains consistent and is updated as the business moves ahead. All Security RMS device or configuration changes follow the ITIL process and are conducted within the customer change control process ensuring complete visibility, accountability and audit traceability.

Q. What is the process for deploying new IPS signatures?

A. A customer defined standard change management process is created during the initial service activation for all managed security devices. All new signatures are reviewed and tested leveraging the Cisco RMS Security early adopter network to ensure that signatures are accurate and applicable for the customer environment. All changes follow the customer defined change control process and are documented, submitted, approved, tracked and visible within the Cisco RMS Security portal.

Cisco Security Remote Management Services for Intrusion Prevention Systems (IPS)

Cisco RMS Monitoring and Management Services for IPS

Table 1. Cisco RMS Deliverables for either Monitoring or Management Services for Intrusion Prevention Sensor (IPS)

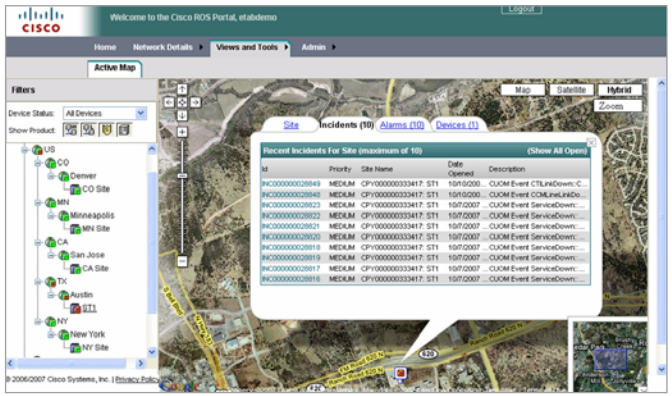
Features	Deliverables	Monitoring Standard	Management Enhanced
Management Readiness Assessment	· Initial policy and configuration assessment, network traffic analysis, critical asset identification and application pattern monitoring	✓	✓
	· Service activation, portal account creation and notification profile definition	✓	✓
Incident Management	· 24/7/365 proactive ITIL based incident monitoring, classification and automated lifecycle notification of security events, raised thresholds and device alarms	✓	✓
	· Incident investigation and diagnosis detailed security incident analysis and classification (Benign, Attack, Denial of Service, Malware, Misuse, Reconnaissance, Suspicious traffic)		✓
	· 24/7/365 resolution and restoration of security incidents and fault or performance violations on managed security devices. Direct access to Cisco Certified Security expert analysts and engineers.		✓
Problem Management	· Analyze incident trends to identify patterns or systemic conditions or problems and root cause		✓
Change Management	· 24/7/365 access to certified security experts for changes to resolve an incident or problem, changes to respond to a critical vulnerability and standard changes to resolve known error	✓*	✓
Advanced Security Event Correlation	· Identify suspicious patterns based on multi-dimensional, correlated data enhancing security visibility by grouping together disparate security events across the network.	✓	✓
	· Embedded IntelliShield security intelligence	✓	✓
Security Reporting Suite	· Comprehensive on demand IPS security reporting suite	✓	✓
	· On-demand IPS performance and trending dashboard		
Web Security Portal	· Incident drill down and investigation, Intellishield Applied Mitigations, device inventory, software version, serial number and host information and active map	✓	✓

*Customers purchase a block of hours that are used for executing Elective Changes. The amount of hours purchased may vary by contract.

Unparalleled Visibility: Control and Reporting

The Cisco Security RMS secure multi-factor authentication portal provides a single pane of glass into the status of the network security infrastructure, security event drill-down as well as performance and security reporting. The in-depth reporting dashboard provides on-demand reporting requests for trending, data analysis and security situational awareness.

Figure 1. Cisco Security RMS Portal



The in-depth security reporting suite for IPS provides unparalleled visibility into security events, trends and high-level CXO reporting needed to satisfy compliance requirements. The following reports are available for the Cisco Security RMS Services for IPS.

Intrusion Prevention Blocked Attack Reports

- Top Blocked Attacks by Signature
- Top Blocked Attacks by Sensor
- Top Source Blocked Attacks
- Top Destination Blocked Attacks
- IPS Signature Severity

Intrusion Prevention Summary Reports

- Top Fired Signatures/Signature Severity
- Top Attacker Source
- Top Attacked Destinations
- Signature Severity Summary by Sensor
- Top Fired Signatures Severity

For More Information

For more information about Cisco Security Remote Management Services, visit www.cisco.com/go/rms or contact your local account representative.

C96-705533-00 04/12