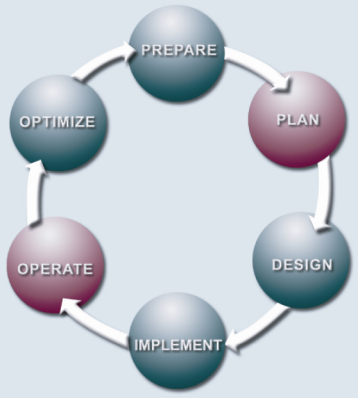
Cisco Security IntelliShield Alert Manager Service

Cisco Security IntelliShield Alert Manager Service provides a comprehensive, cost-effective solution for delivering the security intelligence organizations need to help prevent, mitigate, and quickly remediate potential IT attacks.

THE CISCO LIFECYCLE SERVICES APPROACH



The unique Cisco Lifecycle approach to services defines the requisite activities at each phase of the network lifecycle to help ensure service excellence. With a collaborative delivery methodology that joins the forces of Cisco, our skilled network of partners, and our customers, we achieve the best results.

Network Lifecycle Phases

- **Prepare**—Develop a business case for a technology investment
- **Plan**—Assess readiness to support proposed solution
- **Design**—Create a detailed design to address business and technical requirements
- **Implement**—Deploy new technology
- **Operate**—Maintain network health through day-to-day operations
- **Optimize**—Achieve operational excellence through ongoing improvements

SERVICE OVERVIEW

In mission-critical environments, IT security staff must take proactive steps to mitigate threats before they can impact the business. However, to take such steps, organizations need timely, accurate, and credible security intelligence. With thousands of threats and vulnerabilities reported each year and dozens of independent services reporting new issues, security personnel are constantly challenged to find the reliable appropriate intelligence they need to make fast decisions.

Cisco® Security IntelliShield Alert Manager Service filters through the myriad of alerts from reporting organizations to provide the strategic, targeted security intelligence customers can use to proactively respond to potential IT threats, mitigate risk, and increase business continuity. With this service in place, IT security staffs can spend less time combing through mailing lists and vendor Websites for new alerts, and focus on remediation and proactive protection within their own mission-critical networks.

CHALLENGE

Protecting the IT infrastructure from viruses, worms, and other threats has become increasingly difficult. The first step in securing the business network is understanding where vulnerabilities exist. This is because IT security personnel searching for accurate security intelligence face:

- **Too much data**—New threats may be reported by numerous public services and private organizations, hundreds of times each year.
- **Too many formats**—New threat alerts may be published by dozens of different sources, each in a different format, and each using a different process to identify, characterize, confirm, and report the problem.
- **Difficulty determining the importance of a new threat**—With so many independent bodies publishing alerts, security personnel can have a difficult time finding objective information about the credibility, urgency, and severity of a new threat report.
- **Difficulty tracking remediation status and progress**—Even when a security team has timely, reliable information about a new threat and the action that must be taken to address it, few organizations have systems in place to effectively track the status of remediation efforts.

The process of gaining reliable, relevant security intelligence becomes a labor-intensive, costly drain on an organization's IT security staff.

SOLUTION

Cisco Security IntelliShield Alert Manager Service is a threat and vulnerability alerting service that allows organizations to easily access timely, accurate information about potential vulnerabilities in their environment – without time-consuming research. The service provides a comprehensive, cost-effective solution for delivering the security intelligence organizations need to help prevent, mitigate, and quickly remediate potential IT attacks. Organizations using Cisco Security IntelliShield Alert Manager Service customize their portal by defining the unique networks, systems, and applications that make up their infrastructure, as well as criteria using a standardized risk rating system to determine the threats and vulnerabilities that affect them. The service then provides vendor-neutral intelligence alerts that are pre-filtered to deliver only the relevant information, arming security personnel with the intelligence they can use to take rapid action and protect critical systems. As a result, security personnel can work more quickly and efficiently, and more effectively prioritize remediation activities.

Cisco Security IntelliShield Alert Manager is an important component of the Cisco Self-Defending Network (SDN) strategy, which employs multiple layers of defense. It complements the Cisco security intelligence Website, http://www.MySDN.com, by providing more comprehensive, in-depth, and timely analysis of a broader range of threats and vulnerabilities. And, unlike antivirus solutions that focus only on network endpoints, Cisco Security IntelliShield Alert Manager provides a single, comprehensive clearinghouse for the latest threat and vulnerability information across the entire corporate IT domain.

The Cisco Security IntelliShield Alert Manager Service encompasses four primary components:

- **The Cisco Security IntelliShield Alert Manager portal** serves as the customer interface. The portal is secure, and completely customizable, allowing organizations to receive only information on the specific networks, systems, and applications used by the organization. Organizations can also configure the portal to push notifications via email, pager, cell phone, and SMS capable devices. A real-time XML feed is also available that allows Cisco customers to integrate Cisco Security IntelliShield Alert Manager content into their own applications.
- **The Cisco Security IntelliShield Alert Manager back-end intelligence engine** is the infrastructure that collects threat data and takes each new threat and vulnerability report through a rigorous verification, editing, and publishing process. Cisco Security IntelliShield Alert Manager experts review and analyze each threat to confirm the threat characteristics and product information and deliver the alert in a standardized, easy-to-understand format. Each threat is objectively rated on urgency, credibility of source, and severity of exploit, allowing for easier comparison and faster decision making. New threats and vulnerabilities may be updated several times as a situation evolves.
- **The Cisco Security IntelliShield Alert Manager historical database** is one of the most extensive collections of past threat and vulnerability data in the industry. The fully indexed and searchable database extends back six years and contains over 1,700 vendors, 5,500 products, and 18,500 distinct versions of applications.
- **The Cisco Security IntelliShield Alert Manager built-in workflow system** provides a mechanism for tracking vulnerability remediation. The system allows IT management to see which tasks are outstanding, to whom the task is assigned, and the current status of all remediation efforts.

BUSINESS BENEFITS

The average security professional spends a minimum of two hours per day tracking new threats and vulnerabilities – totaling more than 525 hours spent each year solely on research activities. With Cisco Security IntelliShield Alert Manager Service, tedious, time-consuming research is conducted for an organization's security staff by Cisco Security IntelliShield Alert Manager intelligence experts, and the results are delivered directly to IT security personnel each day – without extraneous data that does not apply directly to the organization's environment.

With the Cisco Security IntelliShield Alert Manager Service, organizations gain:

- **More efficient use of security staff resources**, since all alerts are delivered in a consistent, easy-to-understand format, and organizations receive only those alerts that affect their environment
- **More effective, timely security intelligence** through proactive early warnings about new attacks and technology vulnerabilities
- **Higher-quality analysis**, since each alert is customized, objective, vendor-neutral, and prioritized on a standardized risk rating system
- **Faster remediation of potential vulnerabilities**, since many alerts include Cisco IntelliShield analysis of the threat with recommended safeguards and workarounds, as well as links to patches.
- **Continuous protection against emerging threats and vulnerabilities,** because customers define the networks, systems, and applications that make up their infrastructure and customize the criteria and risk thresholds for receiving notifications, assuring customers only see the information they need.
- **Comprehensive threat and vulnerability information**, including security vulnerabilities, malicious code, and global security trends that include historical information about thousands of vendors and products

UP-TO-THE-MINUTE SECURITY INTELLIGENCE

Cisco Security IntelliShield Alert Manager Service is pioneering security intelligence solution in the marketplace. The Cisco Security IntelliShield Alert Manager research team operates 24 hours a day, seven days a week to bring organizations up-to-the-minute intelligence, as well as in-depth analysis and highly reliable threat validation.

However, Cisco Security IntelliShield Alert Manager Service is much more than just an alert service. The solution augments in-house security analysts' efforts by delivering concise, yet insightful security intelligence to help organizations make better decisions and more effectively mitigate risk. With Cisco Security IntelliShield Alert Manager, organizations have more timely, effective, and comprehensive security intelligence – and greater ability to proactively defend their businesses – than ever before.

Unlike other security intelligence processes and services, Cisco Security IntelliShield Alert Manager Service provides:

- **Extraordinary breadth and depth in intelligence reporting**, including advanced remediation information and analysis
- **Concise, easy-to-understand reports**, with each variation and update of a threat consolidated into a single, readable report, instead of delivering dozens of separate reports totaling hundreds of pages
- **A wide variety of delivery options for reports**, including an integrated notification mechanism that quickly delivers the right information to the right people via email, pager, cell phone, and SMS capable devices.

WHY CISCO SERVICES

Cisco Systems® and its partners provide a broad portfolio of end-to-end services and support that can help you improve network total cost of ownership, business agility, and network availability to increase your network's business value and return on investment.

The Cisco Lifecycle Services approach defines the minimum set of activities needed, by technology and by network complexity, to help you successfully deploy and operate Cisco technologies and optimize their performance throughout the lifecycle of your network. This approach can help you to achieve a high-performance network, integrate advanced technologies, lower operational costs, and maintain network health through day-to-day operations.

FOR MORE INFORMATION

For more information about the Cisco Security IntelliShield Alert Manager Service, visit http://www.cisco.com/go/intellishield or contact your local account representative or your Cisco security partner.

Cisco Services.

Making Networks Work. Better Together.

Corporate Headquarters
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

European Headquarters
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

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Website at** www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

XX/LW XXXXX

Printed in the USA

C00-00000-00 07/06