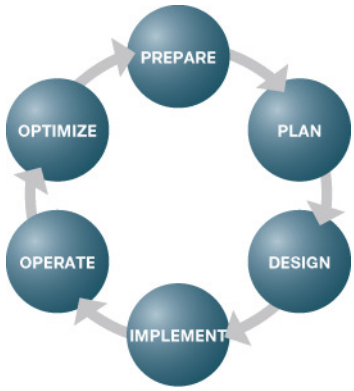
Cisco Security IntelliShield Alert Manager Service

The Cisco® Security IntelliShield Alert Manager Service provides a comprehensive, cost-effective solution for delivering the security intelligence organizations need to 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 affect the business. 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, applicable intelligence they need to make fast decisions.

The Cisco Security IntelliShield Alert Manager Service filters through the multitude 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 these services in place, IT security staff can spend less time looking through mailing lists and vendor Websites for new security threats; instead, they can focus on remediation and proactive protection within their own mission-critical networks.

Challenge

Protecting the IT infrastructure from the latest threats and vulnerabilities has become increasingly difficult. This is because IT security personnel face:

- **Too much data**—New threats may be reported by numerous public services and private organizations, thousands 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 may 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.

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

Solution

The 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 the Cisco Security IntelliShield Alert Manager Service customize their portal by defining the unique networks, systems, and applications that make up their infrastructure, and by defining 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 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 can more effectively prioritize remediation activities.

The Cisco Security IntelliShield Alert Manager Service is an important component of the Cisco Self-Defending Network and Threat Control and Containment strategies, which employ multiple layers of defense. The Cisco Security IntelliShield Alert Manager Service provides comprehensive, in-depth, and timely analysis of a broader range of threats and vulnerabilities. Unlike antivirus solutions that focus only on network endpoints, the service provides a single, comprehensive clearinghouse for the latest threat and vulnerability information across the entire corporate IT domain. To view examples of IntelliShield Alert Manager content, visit the Cisco Security Center (www.cisco.com/security), which provides around-the clock threat and vulnerability information, Cisco IPS signature documents, security news, and actionable intelligence to help improve your security.

The Cisco Security IntelliShield Alert Manager Service encompasses the following components:

- **The IntelliShield Alert Manager Web 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 send notifications using e-mail, pager, cell phone, and SMS-capable devices. A real-time XML feed is also available that allows Cisco customers to integrate IntelliShield Alert Manager content into their own applications.
- **The 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 intelligence 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 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 over six years and contains more than 1700 vendors, 5500 products, and 18,500 distinct versions of applications.
- **The 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.
- **The IntelliShield Alert Manager vulnerability alerts** use the Common Vulnerability Scoring System (CVSS) industry-standard rating system. Organizations also have access to a CVSS calculator that provides the ability to adjust and personalize scoring metrics to generate a more accurate reflection of their individual environments.
- **The IntelliShield Threat Outbreak Alert** covers the latest data regarding web-based threats and malicious e-mails, including spam, phishing, and botnet activity. This new alert is an effort to continually enhance the value of the service we deliver and provide customers with valuable content to stay current with the evolving threat landscape.
- **Cisco IPS Signature information is correlated** and available in the IntelliShield Alert Manager alerts. Organizations have access to perform targeted searches to display Cisco IPS Signatures associated with different threats to ensure they have the most up-to-date intelligence.
- **Cisco Services for IPS customers** have access to the Cisco Security IntelliShield Alert Manager search access feature.

Business Benefits

With the Cisco Security IntelliShield Alert Manager Service, tedious, time-consuming research is conducted for an organization's security staff by IntelliShield Alert Manager intelligence experts. Results are delivered directly to IT security personnel within minutes based on their chosen criteria—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.** 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.** The service delivers proactive early warnings about new attacks and technology vulnerabilities.
- **Higher-quality analysis.** Alerts are customized, objective, vendor-neutral, and prioritized on a standardized risk rating system.
- **Faster remediation of potential vulnerabilities.** Many alerts include analysis of the threat with recommended safeguards and workarounds, as well as links to patches.
- **Continuous protection against emerging threats and vulnerabilities.** Customers define the networks, systems, and applications that make up their infrastructure and customize the criteria and risk thresholds for receiving notifications. As a result, customers only see the information they need.

- Comprehensive threat and vulnerability information. This includes security vulnerabilities, malicious code, and global security trends that contain historical information about thousands of vendors and products.Up-to-the-Minute Security Intelligence

The IntelliShield Alert Manager research team operates 24 hours a day, 7 days a week to bring organizations up-to-the-minute intelligence, in-depth analysis, and highly reliable threat validation.

The 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 IntelliShield Alert Manager, organizations have more timely, effective, and comprehensive security intelligence—and greater ability to proactively defend their businesses—than ever before.

The 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 by e-mail, pager, cell phone, and SMS-capable devices

Why Cisco Services

Cisco and its partners provide a broad portfolio of end-to-end services and support that can help improve business agility, network availability, and the total cost of network ownership to increase a 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 successfully deploy and operate Cisco technologies and optimize their performance throughout the lifecycle of the network. This approach can help to achieve a high-performance network, integrate advance technologies, reduce 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 the Cisco Security Center at http://www.cisco.com/security or contact your local account representative or your Cisco security partner.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-385193-01 3/09