



## DATA SHEET

# CISCO INCIDENT READINESS ASSESSMENT

**The Cisco® Incident Readiness Assessment service provides advanced preparation and planning to help you minimize the potential effects of network security threats and vulnerabilities.**

### Service Overview

To help protect your critical assets against security intrusions or disruption, you need to proactively assess the effectiveness of your network security and operations. Doing so enables you to identify weaknesses in your incident preparedness and to create an action plan for significantly reducing the costs of security incidents.

The Cisco Incident Readiness Assessment service employs the industry-leading Cisco incident management methodology to assess the effectiveness of your network to mitigate the effects of computer worm or virus outbreaks or denial-of-service (DoS) attacks. This assessment can help protect your business by alerting you to network and operational risks that leave your organization ill prepared to respond promptly and effectively to security intrusions.

The Cisco Advanced Services Network Security team combines expert network security research and industry-leading practices to help you be better prepared to withstand security intrusions. This offering:

- Helps minimize the risk of a successful attack by identifying known vulnerabilities and threats
- Provides an actionable plan to improve incident preparedness
- Reduces the time to resolution during a security incident by recommending improvements to incident management tools and techniques

Cisco Advanced Services engineers work closely with your staff to evaluate the effectiveness of your network security operations and infrastructure and then recommend improved practices, technologies, and tools needed to minimize the effects of security threats and vulnerabilities.

### Minimizing the Risk of a Successful Attack

The Cisco Advanced Services Network Security team begins with a review of operational practices and procedures in place to detect and respond to an incident. The Cisco methodology is based on current industry best practices, accepted security models such as International Organization for Standardization (ISO) 17799, and practical experience gained through Cisco involvement in securing large network environments. The team examines operational processes and policies to determine if effective incident detection, containment, and response procedures are in place.

During an assessment, Cisco engineers review your security network infrastructure to determine if it effectively and efficiently supports your organization's security requirements. The analysis performed includes:

- A review of overall network design to determine if it effectively isolates trusted internal networks and systems from intruder access and DoS attacks
- An analysis of network security infrastructure to determine how effectively new threat events are detected and controlled
- A review of the security design of selected platforms to determine if any functions they utilize might result in undesirable security exposures

A well-managed set of security management and monitoring tools, combined with well-documented incident response plans and procedures, is essential for defending against network threats. A review of your organization’s security management procedures and tools can determine if your operations staff has the necessary tools and procedures for effectively monitoring, detecting, and responding to anomalous traffic that can indicate the first signs of an attack.

Table 1 details the deliverables, activities, and benefits of the Cisco Incident Readiness Assessment service.

**Table 1 Deliverables, Activities, and Benefits of the Cisco Incident Readiness Assessment Service**

Deliverables and Activities	Benefits
Collect required operational, network, design, and management information <ul style="list-style-type: none"> <li>• Understand the operational procedures used to detect, contain, and respond to security incidents</li> <li>• Gather network architecture and device information, including scans of device configurations</li> <li>• Understand network monitoring tools and procedures</li> <li>• Gather information on attack mitigation tools design and strategy</li> </ul>	<b>Mitigates network security threats</b> <ul style="list-style-type: none"> <li>Finds and eliminates known vulnerabilities</li> <li>Minimizes the risk of a successful attack</li> <li>Limits damage caused by viruses , worms, and DDoS attacks</li> <li>Helps improve incident readiness and response procedures</li> </ul> <b>Improves productivity</b> <ul style="list-style-type: none"> <li>Improves the ability of network operations teams to prevent, detect, and respond to future threats</li> <li>Provides an actionable plan to improve incident readiness preparedness</li> <li>Reduces time to resolution with techniques to improve incident response</li> </ul>
Perform onsite interviews and design reviews Analyze data and statistics identifying incident readiness gaps <ul style="list-style-type: none"> <li>• Analyze network operations and procedures for incident readiness and response</li> <li>• Assess network security infrastructure design for typical classes of risk (for example, virus outbreaks, DoS attacks, etc.)</li> <li>• Review device configurations for security vulnerabilities</li> <li>• Review security management controls for incident monitoring and management</li> </ul>	<b>Reduces total cost of ownership</b> <ul style="list-style-type: none"> <li>Reduces risk of expensive and embarrassing downtime</li> <li>Takes advantage of investment in network and security infrastructure technology</li> <li>Helps lower operating costs through consistent deployment of operational policy and procedures</li> </ul>
Identify security gaps in operational processes, security infrastructure, and network security management tools and procedures	
Provide detailed recommendations for improving incident readiness and response policy, procedures, architecture, design, and configuration	
Present executive findings and recommendations	
Deliver detailed Incident Readiness report with analysis, findings, and recommendations	

**Cisco Difference: People, Process, Tools, and Partners**

Cisco Advanced Services for Network Security offers certified experts, in-depth technical knowledge, specialized tools and methodologies, and industry-leading security research labs to deliver high-quality network security services. Cisco consultants and engineers can help you minimize the risk to valuable business assets by working with your team to assess, design, implement, and help optimize network security solutions that are critical to managing the evolving information security threat.



### **Availability**

The Cisco Incident Readiness Assessment service is available globally. To obtain the most current information on how Cisco Advanced Services can help to improve your incident readiness and response capabilities, contact your Cisco representative.

Cisco Systems® offers various services programs to help accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you to protect your network investment, optimize network operations, and prepare the network for new applications to extend network intelligence and the power of your business.

### **For More Information**

For more information about the Cisco Incident Readiness Assessment service or other Cisco Advanced Services, visit [www.cisco.com/go/securityconsulting](http://www.cisco.com/go/securityconsulting) or contact your Cisco service account manager.

## CISCO SYSTEMS



### 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 Web site at [www.cisco.com/go/offices](http://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

Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0503R)

### Cisco Internal Use Only

Printed in the USA

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

Page 4 of 4