



IBM Managed Security Services

Intrusion Prevention Service



Hackers not welcome

Your Web page has been altered, confidential data has appeared on multiple external Web sites, and you are unsure when or how this security breach occurred. You have been hacked! As you investigate, you are told that there is evidence that the hacker has been inside your critical systems for an extended period. Could you have known? Why were you not informed?

Prevent and detect unauthorized activities

Most companies do not have enough information – with enough lead time – to prevent attacks from hackers, viruses and worms but can only respond after the fact. Armed with advanced warning, however, these same companies can proactively defend their corporate assets. IBM provides our customers with advisories and alerts to help prevent, mitigate, and/or remediate security threats before those threats can impact your business.

IBM's Intrusion Prevention Service monitors your network for malicious activity 24x7x365. Our trained professionals at IBM's Security Operations Center (SOC) investigate and alert your security professionals or other designated staff when suspicious activity occurs via an escalation policy created for you. This IBM team

will work closely with your business to recommend and coordinate a timely response for professional, efficient handling of any suspicious activity. In the event of an incident, incident management services are available to our customers. IBM can assist you in properly responding to and management of any security related incident. Intrusion prevention dramatically reduces the response time for dealing with an unwanted intrusion, thus reducing the potentially harmful consequences, reducing costs and lowering risk.

Identify network intrusions as they happen

Sensors are placed at critical points in your network that intelligently analyze the packet activity to detect actual or attempted intrusions of the network, breaches of security, or misuse of the network. Whether inside or outside of the DMZ, these passive network sensors allow for maximum coverage and zero network performance impact. IBM compares suspicious activity against constantly updated profiles of known risk events, such as multiple password rejections, buffer overflow attempts, denial of service and other attack signatures.

Rely on our experience

IBM Global Services - comprising the largest professional security community in the world - offers broad experience and a proven track record of successful engagements. IBM can help reduce your risk and exposure in today's interconnected world by leveraging our extensive intellectual capital and best practices models to develop superior security and privacy programs.

- ✚ *Ranked #1 IS outsourcing services provider, worldwide and in the U.S. (Source: IDC, September 2003)*
- ✚ *Ranked highest in reputation, innovation and quality personnel among worldwide outsourcing providers. (Source: Ross Research, July 2003)*
- ✚ *Most preferred outsourcing provider in Asia-Pacific region. (Source: Gartner customer study, June 2003)*

Benefit from a team approach

IBM Global Services and our Business Partners combine the complementary strengths, skills and resources of multiple organizations in providing value-added services and solutions. By collaborating, we can offer you an array of benefits including enhanced solution technology, increased customer satisfaction, enhanced productivity and improved Return on Investment.



© Copyright IBM Singapore 2005
Printed in Singapore
07-05
All Rights Reserved

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.