

Security Best Practices for SCADA Networks and Process Management Systems

overview



Security Best Practices for SCADA Systems

Made Simple

The online security of SCADA networks and process management systems is critical for utility organizations to ensure that there is no disruption of service, process redirection, or manipulation of operational data that could result in serious disruption to the nation's critical infrastructure. The U.S. Department of Energy states that "actions are required by all organizations, government or commercial, to secure their SCADA networks as part of the effort to adequately protect the nation's critical infrastructure." In fact, online threats to SCADA systems may pose as much risk for potentially significant failure within a power generation system as a physical attack.

There are several business challenges for utility organizations in achieving the level of online security that meets security best practices for SCADA networks and process management systems, including:

- No formal definition of security requirements
- Lack of incremental security budget
- Absence of necessary security expertise
- Inability to easily deploy and manage required technology
- Need for company-wide employee education on security best practices

Internet Security Systems is prepared to help.

As a world leader in products and services that protect online assets, Internet Security Systems, Inc. (ISS) has demonstrated continued success helping utility organizations quickly and simply achieve security best practices to protect their process management systems.

Complete Solutions

from a Single Security Partner

Through its ADDME approach, ISS is uniquely capable of delivering a complete solution for SCADA systems that includes the assessment, planning, technology, deployment assistance, education and ongoing management that is needed to attain security best practices. ISS delivers a complete solution through:

- **X-Force® Professional Security Services** - An elite team of security professionals that partner with your organization to assess your current security posture and develop a complete roadmap for meeting security best practices.
- **Technology** - Comprises ISS' award-winning solutions spanning the network, server and desktop environments as well as vulnerability detection applications. ISS' SiteProtector™ central management application unifies configuration, deployment and data correlation for all of these agents.
- **Managed Services** - Provides around-the-clock protection for organizations lacking the time, expertise or appropriate internal resources to secure critical information. This comprehensive suite of services provides cost-effective, scalable security solutions through effective leverage of ISS' technology.
- **X-Force Security Intelligence** - ISS' leading group of over 40 security experts, dedicated to proactive counter-intelligence, research, development and public education against online threats, including those facing public organizations. The X-Force tracks the evolution of threats through its Global Threat Operations Center to make sure public organizations are aware of the latest cyber-risks.

The ISS Approach to Security Best Practices for SCADA Networks and Process Management Systems

In order to streamline security and help achieve security best practices for SCADA systems, ISS has developed a five-step process covering the complete security management lifecycle, including phases for Assessment, Design, Deployment, Management and Education (ADDME™). The ADDME process identifies and analyzes gaps in the current security state compared to requirements for security best practices. It then designs and implements solutions to close those gaps and ensure ongoing conformity.

The following phases are part of the ADDME process:

Phase 1: Assessing the current level of information security

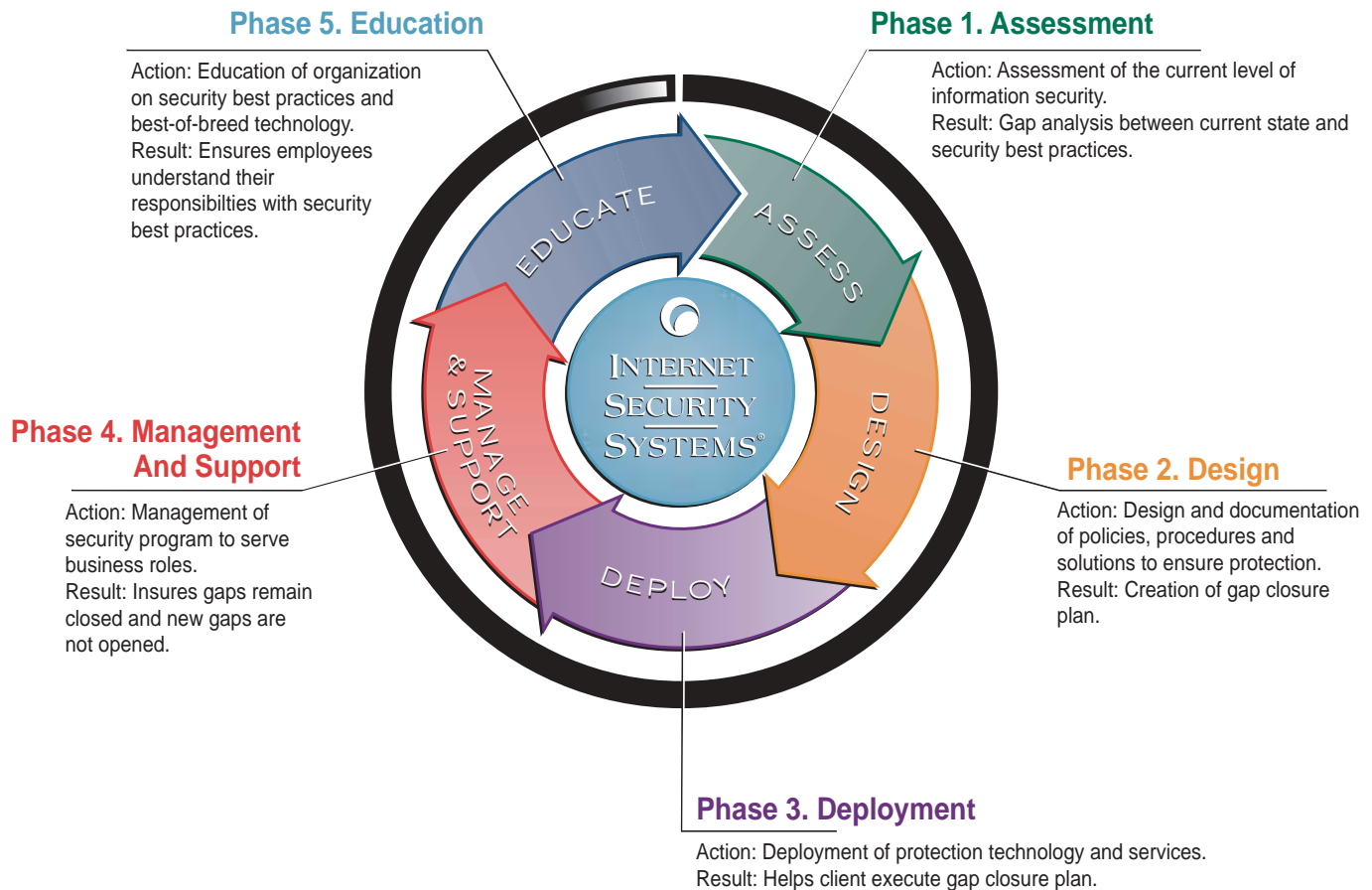
Phase 2: Designing and documenting policies, processes and solutions to ensure protection

Phase 3: Deploying protection technology and services

Phase 4: Managing the security program to serve business goals

Phase 5: Educating the organization on security best practices

The ISS Approach to SCADA Networks And Process Management Systems



Get Started Today!

Internet Security Systems offers organizations a single source for planning, expertise and technology that addresses security best practices for SCADA networks and process management systems. By partnering with ISS, your organization benefits from the best security intelligence and technology in the world, freeing your resources to focus on core business issues and functions.

For more information about the five-step ADDME process and ISS' technology products and services, please visit www.iss.net/products_services/market_solutions/index.php or contact us at 888-901-7477.



INTERNET SECURITY SYSTEMS®

6303 Barfield Road • Atlanta, GA 30328 • Tel: 404.236.2600 • Fax: 404.236.2626 • www.iss.net

About *Internet Security Systems*

Founded in 1994, Internet Security Systems (ISS) (Nasdaq: ISSX) is a pioneer and world leader in software and services that protect corporate and personal information from an ever-changing spectrum of online threats and misuse. Internet Security Systems is headquartered in Atlanta, GA, with additional operations throughout the Americas, Asia, Australia, Europe and the Middle East. For more information, visit the Internet Security Systems Web site at www.iss.net or call 888-901-7477.

Copyright © 2004, Internet Security Systems, Inc. All rights reserved worldwide.

Internet Security Systems, the Internet Security Systems logo, Proventia, SiteProtector, System Scanner and Wireless Scanner are trademarks and service marks and Database Scanner, Internet Scanner, X-Force and RealSecure are registered trademarks, of Internet Security Systems, Inc. Other marks and trade names mentioned are the property of their owners, as indicated. All marks are the property of their respective owners and used in an editorial context without intent of infringement. Specifications and content are subject to change without notice.