Power Systems Security
Prevention and protection
Highlights
- Reduce the risk of business and data loss and consequences of a disruption in IT services
- Lower the cost of user administration and management
- Uncover exposures and administrative oversights
- Policy and standards analysis
- Audit and compliance reporting
- Create an environment for trusted computing

Security in an on-demand, complex world
Privacy and data protection are the responsibility of all. In a world where data is easily acquired, shared and stored (and potential data misuse is a concern) everyone must do their part to handle information in compliance with their company's requirements and values.

The cost of poor security practices
IBM research indicates security expenses are growing three times faster than IT budgets. Mounting regulatory and compliance mandates carry stiff government penalties and fines if ignored; ever-growing volumes of data tax infrastructures and control capabilities; customer records disappear with alarming frequency; and security breaches cost an average of $6.6 million per incident.

With the added pressure of a challenging economy, to compete effectively a business cannot tolerate any security exposures. From a minor breach like exposing one's password or major failure like the disclosure of client data, neither are acceptable and can result in new administrative procedures, a failed audit or lost business. Some circumstances could even lead to a lawsuit.

Security offerings
Engage the experts of IBM Systems Lab Services and Training to help uphold your company's commitment to privacy and data security. Our team has developed a multitude of offerings to address your specific security concerns and to help you fully leverage the security capabilities of your IBM PowerSystems™ environment.

Security Consulting and Risk Assessment
Consulting and Implementation Services
From help implementing a security feature to additional resources to supplement your staff, our Consulting and Implementation Services provide general and custom consulting. Our most popular services include:

- Password Elimination and Single Sign-on (SSO)
- Data and Tape Encryption
- Audit journal setup and analysis
- Security Assessments
- LDAP Workshop and Implementation Services
- RBAC Workshop and Implementation Services
- PowerSC Workshop and Implementation Services
- Breach Analysis
- Secure Communications
- Security Remediation
- IBM WebSphere® Application Server health checks

PowerSC Tools for IBM i
PowerSC Compliance Assessment and Reporting Tool for IBM i
Regular assessments are key to uncover hidden or incorrectly administered security issues. The PowerSC Compliance Assessment and Reporting Tool for IBM i provides information on the security administration of an IBM i system or across a number of IBM i systems. This tool collects more than 1000 pieces of statistical information including user profile administration, network configuration, operational configuration, system settings and more. That information is placed in one location for Security Administrator viewing thru a series of Web Query dashboards so that security compliance can be monitored “At
a Glance”. The PowerSC Compliance Assessment and Reporting Tool for IBM i can also produce an HTML formatted report of 50-plus pages in just two-to-20 minutes depending on the size of the user population. An easy to use interface is included to instrument the scoring of compliance against customer policy. This is the one tool you should not be without!

**PowerSC Security Diagnostics for IBM i**
Similar to the PowerSC Compliance Assessment and Reporting Tool for IBM i, the PowerSC Security Diagnostics for IBM is an exhaustive collection tool, often used during a security assessment to help document findings. It can also be purchased separately to enhance reporting ability. Statistics provided include detailed reporting of more than 70 areas on IBM i, an executive summary, top ten findings and mediation plan.

**PowerSC Privileged Access Control for IBM i**
Without careful control, privileged users can pose a risk to your system security. This tool enables the security administrator to reduce privileged accounts, with a mechanism to temporarily elevate privileges to users when needed. PowerSC Privileged Access Control is fully auditable and provides notifications when invoked. This allows compliance to industry guidelines on privileged users.

**PowerSC Secure Administrator for SAP on IBM i**
SAP provided administrator user profiles are often shared, leading to security exposures and ineffective auditing. PowerSC Secure Administrator for SAP on IBM i addresses this exposure by providing a secure and auditable mechanism enabling multiple SAP administrators to utilize the same SAP administrator user profile without sharing the profile itself.

**PowerSC Access Control Monitor for IBM i**
This tool monitors security deviations from specified application design. Monitoring compliance of libraries, objects, and authorization lists that are out of corporate security policy standards, data classifications, or other security related configurations. PowerSC Access Control Monitor for IBM i provides ad hoc or scheduled analysis and reporting.

**PowerSC Network Firewall for IBM i Exit Points**
This tool simplifies the addition and removal of point definitions for users on IBM i. Exit points are a provision of the IBM i operating system that lets some system functions perform additional checking and validation through user-created programs. The tool currently includes programs for managing exit points for FTP, ODBC, JDBC, File Transfer, Host Servers, DRDA/DDM, REXEC, CLI and RMTCMD. Additional exit point programs can be added. This easy-to-use interface lets a security administrator define which users are allowed through the exit point, and an audit journal record is created whenever a user accesses it.

**PowerSC Audit Reporting for IBM i**
User activity and system/application auditing is a requirement for most companies. The PowerSC Audit Reporting Tool simplifies the task of viewing entries in the IBM i security audit journal. It provides flexibility and a statistical view of the number of entries occurring in each journal entry. The security administrator can select an entry by date, time or type, drill down for details and optionally print or send an output file. The tool includes features for managing journal receivers, reporting on special authorities, monitoring for the entries defined in the PowerSC Network Firewall for IBM i Exit Points and a report scheduler.

**PowerSC Certificate Expiration Manager for IBM i**
Certificates are valid for a specific time range, typically one year, and expiration becomes more complex when more services require them. PowerSC Certificate Expiration Manager for IBM i is a java-based tool that simplifies cross-platform certificate expiration management by maintaining a log of all expiration activities and sending notice via email. An easy-to-use configuration GUI is included to manage XML settings.

**PowerSC Password Validation Tool for IBM i**
Despite warnings, one-in-five users choose a non-compliant password to protect their identity. We’ve developed a program to validate and ensure passwords meet company and industry recommended rules and guidelines. The tool also lets the security administrator establish a dictionary of excluded terms, to further tighten password security.

**PowerSC Single Sign On (SSO) Suite for IBM i**
Password and user profile management is often challenging. Users often have different passwords for each system or application they access; they have multiple user registries, and so on. The PowerSC Single Sign On (SSO) Suite for IBM i has several tools that provide an effective alternative to manual configuration and reducing help desk costs. The following are available individually, with or without services:
- PowerSC SSO Suite for Domino includes Domino synchronization and DSAPI Plug-ins.
- PowerSC SSO Suite for EIM includes EIM CL Commands, EIM Populator, EIM Management Utility, EIM Based Password Reset, EIM Based CRTUSERPRF, and Windows AD Profile Synchronization.
- Password Synchronization Tool
- Single Sign On for SAP

**PowerSC Encryption Suite for IBM i**
Application developers are required to meet data security standards and protect critical data. PowerSC Encryption Suite for IBM i simplifies the implementation of cryptographic capabilities. Several tools are available to provide procedures and techniques to simplifying the implementation while using IBM i Operating System capabilities. The following are available individually:
- Cryptographic Services APIs
- Cryptographic Coprocessor
- Cryptographic Support (CR1) Emulator Tool
Security Services for AIX

IBM PowerSC Services for AIX
A suite of new IBM AIX® features address security issues common to Cloud and Virtual Data Center environments. PowerSC features include Trusted Logging, Trusted Network Connect and Patch Management, Security and Compliance Automation and Trusted Boot. Services include training and guidance to easily implement these features.

Role Based Access Control (RBAC) Services
UNIX systems are built around the "superuser" or "root" concept. Root access can create security problems on an AIX system by allowing a privileged user the ability to perform any task and view or modify any file on the system. Root is also the most targeted user account for hackers. One of the best ways to eliminate security dangers created by excessive root access is by implementing RBAC. AIX 6.1 Enhanced RBAC is the most secure and sophisticated method to delegate traditional root access to non-root users. Our RBAC services provide the necessary training and guidance for getting your RBAC implementation underway.

LDAP Implementation Services
Provides full technical and hands-on implementation and training to deploy LDAP, LDAP replication, LDAP failover and SSL integration for centralized user management of AIX partitions with IBM Tivoli® Directory Server or Microsoft Active Directory Server.

AIX Identity Management with ITDS
The best form of identity management for AIX systems is implemented using LDAP directory services. LDAP can save a great amount of time, effort, and energy by simplifying the task of supporting users and groups as a business grows. This type of centralized management allows you to remove the need of synchronizing passwords and accounts for users and groups across multiple AIX systems. This service provides an on-site workshop that will equip the customer with all the essential elements needed to deploy LDAP directory services using IBM’s Tivoli Directory Server (ITDS).

Pass-through Authentication with MSAD and ITDS
For most AIX customers, PTA provides the perfect solution for centralized password and user/group management of AIX systems. Using PTA, when AIX systems are configured as LDAP clients pointing to an ITDS LDAP server, ITDS provides the PTA mechanism to redirect authentication requests to a different LDAP server, in this case MSAD. This PTA service offering assists in the configuration of AIX users to use a single Windows network login password for both their Windows desktops and AIX systems.

AIX Auditing Workshop
The AIX Auditing subsystem provides comprehensive recording of security-related AIX events that can be used to alert you about potential or actual violations to the system security policy. This workshop provides the know how to track user activities critical to preventing, detecting or minimizing the impact of a security breach. The implementation of auditing allows thorough tracking, alerting, and analysis if something goes wrong.

Encrypted File System (EFS) Workshop
Safeguarding the data of a company is one of the most important security goals for any company. A hacker frequently aims to steal data that is stored within a company’s data center. Many companies expose themselves to high risk due to failing to utilize a data-centric security approach. As described by the Jericho Forum, a company shouldn’t solely depend on perimeter security for their security. Learn how AIX’s EFS can be used as part of a data-centric security approach that can protect important data residing on JFS2 file systems.
Who We Are
IBM Systems Lab Services and Training develops and deploys solutions across IBM systems offerings. Our team of experts are well-versed in product knowledge and platform specific hardware and software solutions for clients and IBM Business Partners. In addition to skills honed in IBM development labs, our consultants bring experience gleaned from thousands of worldwide engagements, development to implementation.

The Lab Services mission
Our mission is to help accelerate the adoption of new IBM products and offerings and maximize the performance of client systems. Our consultants leverage their relationships with IBM labs to build deep technical skills and bring the latest technology to our clients and partners.

We can help with smarter computing
Leverage our experience and knowledge to address the challenges of demands for service, inflexible infrastructures, tight budgets and incomplete, unreliable data. We collaborate with IBM service organizations like Global Technology Services, Global Business Services, Sales and Distribution, Software Group as well as IBM Business Partners.

Lab Services tools
Many of our solutions were built in response to customer requirements to fill product gaps, or a request to further enhance our products. They range from easy-to-install tools and utilities to more complex solutions; the latter often includes a services component intended to provide technical training and implementation services so clients and business partners can acquire and maintain mission critical skills.

How are these offerings acquired?
The utilities described here are offerings provided by IBM Systems Lab Services and Training and—unless noted otherwise—packaged as part of a consulting services engagement. Offering consists of the software license and maintenance, as well as planning, design and implementation services.

Pricing
Contact an opportunity manager to confirm requirements, define the scope of work, develop a services proposal and determine pricing.

Power Services
We offer services in all aspects of managing Power Systems environments, including installation, migration, porting, platform management, consulting and training. Take advantage of our always-current knowledge of products and solutions for virtualization, high availability, high performance computing and server consolidation.

For more information
Learn more about IBM Power Systems Security and related services. Contact stgls@us.ibm.com or visit:

ibm.com/systems/services/labservices

For a complete view of IBM Systems Lab Services-developed software services and tools, visit:

ibm.com/developerworks/systems/LabServicesTools

© Copyright IBM Corporation 2012
IBM Corporation
Route 100
Somers, NY 10589
Produced in the United States of America March 2012
IBM, the IBM logo, ibm.com, AIX, Power Systems, Tivoli and WebSphere are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

This document is current as of the initial date of publication and may be changed by IBM at any time.

Not all offerings are available in every country in which IBM operates.