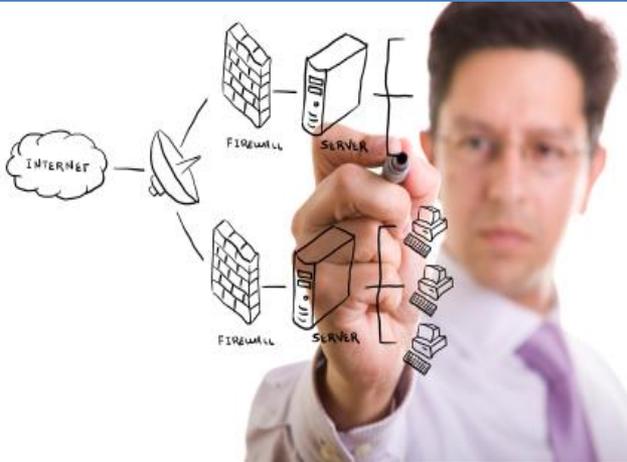# AIX Systems Security Hardening Services for IBM Power Server

An outsider's perspective can bring unexpected value to your organization

TLC

Skills and expertise to help you increase the business value from your Power Systems Investment.

This workshop shall study host based security highlighting importance of AIX security features including TE and TCB setup, EFS implementation, system wide file permissions, RBAC, system authentication database including user's profiles. Identify a list of unnecessary installed file sets that are considered as a threat to overall security and TCP/IP in general.

With an in-depth understanding of technology infrastructure along with hands-on experience gained through working on critical issues in key industries of the IT marketplace, TLC is committed to providing you with top-end consulting services and solutions to meet your unique business challenges.

As an option, this workshop can also be combined with Gap Analysis Workshop based on IT capabilities domains including Governance, Risk and Compliance, Security Intelligence and Analytics, Identity and Access Management, Data Security, Application Security and Infrastructure Security.

For additional details on other workshops, please visit: https://www.tlcpak.com/techwrkshp.html

About this services and Key Business Challenges –

Security threats are often thought of as activities originating from external organizations, and traditionally firewalls and DMZs have been used to set up protection to make corporate environment secure. Historically, computer forensic data has constantly shown that intrusions occur most often of the times within an enterprise. Cleartext passwords, for example, are still a common practice within the corporate network

Generating IBM AIX security reports should reflect the current security model overview of your system, and these reports can then be presented to managers or audit to show how your AIX system is managed with regards to security.

This workshop shall produce an audit security snapshot of your system enables organizations to produce the effectiveness of your security controls to ensure that security is managed properly on your AIX servers running business mission critical applications. It also demonstrates the standard security policy that you are currently adopting.

Following are the components that will be part of this workshop:

- Execute a planning session with client's IT team to gather initial data on the installed systems

- This service includes a detailed analysis of 1 LPARs running clients business mission critical applications.

- Collect all the necessary snapshots in a separate JFS2 filesystem.

- Record changes after executing different AIX tools and commands.

- Securing the Base Operating System and provide high level information about how to protect the system.

- Understand, explore and recommend clients common security setup including authentication, authorization, confidentiality, privacy, integrity, and availability by considering AIX best practices methodologies.

- Securing the Base Operating System and provide high level information about how to protect the system.

- A set of AIX systems wide utilities will be used to explore clients existing environment that helps in identifying and reducing security hazards.

- You will be informed for taking necessary actions to implement TLC findings and recommendations that includes the installation of AIX fixes, firmware and microcodes.

- Provide up to two of your personnel with basic skills instruction on the administrative tasks performed during this service.

- Present summary to client's senior executive management with suggestions and recommendations.

- At the completion of this service, a detailed report shall be presented to the client.

During this workshop, following areas of AIX operating system will be reviewed.

- Studying 10 critical steps to security compliance
- Analysis of system wide security configuration files
- Study system-wide critical logs
- Identifying operating system gaps
- Users and systems related securities
- Deep dive study of TCP/IP configurations files
- Cron related security issues
- System recovery procedures
- And much more
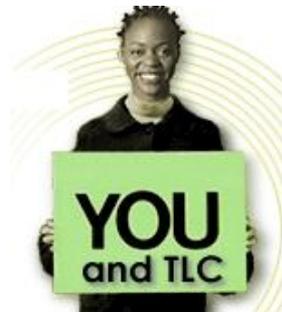
Workshop Code: WS303

For additional information please write to:
info@tlcpak.com