AIX Systems Security Hardening Services for IBM Power Server

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

TLC
Enterprise IT Professional Services

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.

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

www.tlcpak.com

About this services and Key Business Challenges

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.

Securing your environment model presents a challenge. Successful companies recognize that their security infrastructures need to address the business challenge. Most of them are not aware of the types of attacks that malevolent entities can launch against their servers and can plan appropriate defenses both internally and externally.

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 two of your LPARs (1 x Database Server and 1 x Application Server) running clients business mission critical applications.
- Collect all the necessary snapshots in a separate JFS2 filesystem and 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 followed by a detailed report.

Optional Services – Gap Analysis Workshop

As an option, this service 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.

Biggest Dilemma

Most of the global clients do not pay serious attention considering operating system security as a first line of defense to monitor.

People are building layers of securities revolving over Databases and Applications and leaving the underneath OS vulnerable.

Act today to prevent a breach tomorrow

75%

of organizations say they have significant cyber risk exposure

Workshop Code: WS310

For additional information, call for presentations or write to us at: info@tlcpak.com

Opportunities are made, not found