Executive Leadership Series

TLC
Education & Training
Services

The Role of Secure API Strategy for Open Banking System

1DAY

Workshop

- CXO's
- Business Executives
- Technology Executives
- Application Developers
- Cybersecurity Professionals
- Digital Leaders
- Project Managers
- Strategic Planners

The Role of Secure API Strategy for Open Banking System

Skills and expertise to help you increase your knowledge in the field of digital technologies

TLC
Education & Training Services

About this workshop

We are on a mission to transform the senior business executives and technology leadership teams on the potential knowledge on enterprise architecture and digital emerging technologies with a on point agenda that they have nothing to lose but everything to gain.

This one-day workshop is exclusively designed to unfold essential key areas of Open Banking and the implications of platform business models in the Banking and Financial Services industry.

During this workshop, executives will learn an understanding of open banking framework including platform models, digital ecosystem; API architecture and pillars of the Open Banking transformation, insights on global market trends from regulatory frameworks around the world to favorable business momentum for new entrants and incumbent strategies to build resilience, tools to comprehend and analyze opportunities and risks of any Open Banking project as well as practices to structure it's operational and technological aspects.

In a nutshell, the role of BOD's, business executives and technology leaders in open banking includes emphasizing strategic vision, risk management, technology adoption, customer-centricity, collaboration, and change management.

The biggest challenge is to **understand and focus on** "what customers want, how they want it, and how a bank can organize to secure their web-based services"

Target Audience

- CXO's, Business and Technology Leaders, Application Developers, Digital Leaders, Business Analysts, Project Managers, Enterprise Architects, Strategic Planners.

Open Banking and the Critical Role of API Security: Open banking has transformed the financial landscape, and API security plays a pivotal role in ensuring its success. Let's delve into the critical aspects:

APIs in Open Banking: APIs (Application Programming Interfaces) are at the core of open banking functionality. They enable financial institutions to standardize how they create and connect to an ecosystem of providers, facilitating the exchange of financial data. Banks provide access to their proprietary APIs, allowing fintech providers and third-party developers to access financial data. This collaborative approach fosters partnerships rather than competition among stakeholders.

Security Challenges: While open banking APIs address parameters like encryption, authentication, and authorization, they still face challenges. APIs interact with various services under the open banking umbrella, each with its unique logic. Financial institutions may have hundreds or thousands of APIs, making it difficult to standardize authorization implementation.

Heightened Risk: Open banking's reliance on APIs makes them prime targets for cyberattacks. Gartner predicts that API attacks and breaches will double by 2025. To protect against these threats, financial institutions must adopt robust API security measures that go beyond basic protocols. This includes threat detection, monitoring, and response strategies.

In summary, securing APIs is critical for maintaining consumer confidence, protecting data, and ensuring adherence to regulatory requirements in the dynamic landscape of open banking.

Unit 1 – Open Banking – A New Era in Banking Industry

- Problems and Challenges with Traditional Banking.
- What kind of problems holds banks back to step up to open banking?
- Understand API, what are API used for, and how are APIs implemented.
- Open Banking defined and Open Banking Regulatory Framework in Pakistan.
- Opening the data to 3rd parties creates opportunities for Consumers.
- The Three main objectives of Open Banking.
- The Role of API's in Bundling and Unbundling – The Concept.
- Securing the API Attack Surface – The bigger Challenge.
- How does Open Banking work and the Relationship between AISP & PISP.
- Open Banking Business Models and High-level Open Banking Architecture.
- Types of APIs, API Framework and types of open banking API Specifications.
- Understand Variable Recurring Payments (VRPs).
- Open banking payments vs other payment methods.
- Strong Customer Authentication.
- A High-Level Open Banking Framework.
- Enrolling with OB as a Third Party Providers & Technical Service Providers.
- Unit 1 Assessment.

Unit 2 – The Role of Secure APIs Strategy for Banking

- API Evolution Creates New Activities for Business and IT Leaders.
- Differentiating between Microservices and APIs Components.
- What is an API Strategy – Understand your IT Environment
- The key challenge in developing and implementing API strategy.
- Common vulnerabilities present in commercial software.
- New API Top 10 categories of vulnerabilities.
- Banking API Strategy Implementation Steps – The Four Key Pillars.
- How banks can benefit from the API-based approach?
- Types of API Strategies for Banks and their Use-cases.
- Top Objectives and Monetization Strategies of API Adoption.
- End-to-end API Management Lifecycle.
- Eleven steps in accomplishing successful API Management in Banking.
- Platform Capabilities and Deployment Options.
- API Exposures and Connections.
- Incorporate security into the development processes.
- Types of API Security Incidents and their Impacts.
- Why attacks continue despite Security Solutions are in place.
- Types of API vulnerabilities that are of greatest concern.
- Using 9-Types of API Testing – A Recommended Path.
- Knowing Security Capabilities an API Gateway should Provide.
- The best practices for API Security in open banking.
- The Banking Future Stack and Architecture.
- Cloud Web Application & API Protection – WAAP is way forward.
- Unit 2 Assessment.

Opportunities are made, not found

Executive Leadership Series

The Role of Secure API Strategy for Open Banking System

Skills and expertise to help you increase your knowledge in the field of digital technologies

TLC
Education & Training Services

Open Banking Regulatory Framework in Pakistan

On February 1, 2020, United States Agency for International Development (USAID) has published a final report on "**Regulatory Framework for FinTech's in Pakistan**" under the project name of "**USAID Small and Medium Enterprise Activity (SMEA)**" with their suggestions and recommendations.

As a lead regulator on financial matters, State Bank of Pakistan (SBP) **perceived internationally driven open banking regulations** as a "CANDO" regulations.

The Securities and Exchange Commission of Pakistan (SECP) regulates other financial components as well as company registrations.

The final report addresses methods to catalyze and bootstrap the development of an emerging financial technology ('fintech') ecosystem in Pakistan.

The report also addresses the regulatory trilogy of who, what, and how of regulation including recommendations on new policy frameworks and approaches in line with evolving open banking best practices worldwide.

Though the delivery of financial services is dominated by local banks in Pakistan, there is a low use of accounts and non-cash payments which presents a humongous business opportunity for new entities known as FinTech's.

Confronting API Security in the New Open Banking Era

FinTech's are now challenged to provide innovative services by integrating a new business models to provide extended set of services that are currently not addressed by traditional banks and other large officeholders in Pakistan.

In a nutshell, the new financial services model using emerging technologies will reshape country's financial and technology ecosystem by creating network effects of increased competition, more choice for consumers, higher operational efficiencies, and improved financial inclusion.

The Three Key Points for Secure API Strategy

The Role of Secure API Strategy for Open Banking is crucial in the digital era. Here are key three points.

APIs and Open Banking: APIs constitute 31% of all web traffic and have facilitated services like banking transactions, remote check deposit, and GPS-assisted ATM locations.

Regulatory Standards: The European Union's Payment Services Directive (PSD2) enforces secure API usage, emphasizing strong customer authentication (SCA) and secure communication standards.

API Security Best Practices: Collaborate with partners, invest in intelligent technologies, and prioritize threat detection and response strategies.

Open banking APIs revolutionize the financial sector, enabling secure data exchange among banks, FinTech firms, and third-party providers. These APIs streamline connections, offering unparalleled convenience, speed, and security for customers accessing banking products. To protect open banking, institutions must adopt robust API security solutions that leverage AI and ML to identify attacks and safeguard opportunities driven by APIs.

Workshop Summary

The significance of attending **Open Banking and API security workshop**:

The Role of Secure API Strategy for Open Banking System Workshop:

- This course delves into the engine underneath financial platforms, focusing on the software infrastructure and API security behind OB.
- Key Learning Points:
  - **Understanding APIs**: Learn about the construction of Application Programming Interfaces (APIs).
  - **Integration of API Tools**: Explore how API tools and resources are integrated into high-value open banking solutions.
  - **Internet Security Management**: Assess open banking's internet security management and authentication.
  - **API Implementation Success**: Evaluate the success of API implementations and understand the testing and running processes.

API Security as a Limiting Factor or Accelerator:

- Integrating security into an OB solution is vital for winning customer trust.
- Gain insights into how security can either hinder or accelerate an OB strategy.

In summary, attending courses, workshops, and industry events enhances your knowledge, keeps you updated, and empowers you to contribute effectively to the evolving landscape of open banking and API security.

The Role of Senior Business and Technology Management in Securing API Security

Senior business management plays a crucial role in API security. Below are some key aspects:

1) **Strategic Alignment:** Leadership must recognize API security as a strategic business priority, integrating it into broader business objectives and risk management strategies. They should encourage a company-wide security mindset, where every employee understands the importance of API security and their role in maintaining it.
2) **Culture and Awareness:** Senior management should foster a cybersecurity conscious culture by promoting security awareness and training programs. Encouraging employee accountability for security practices and integrating security considerations into business processes is essential.
3) **Governance and Lifecycle Management:** Establishing a governance framework to manage the entire lifecycle of APIs is critical. This includes defining API specifications, versioning, documenting, testing, deploying, and retiring APIs. Implementing a structured API lifecycle management process ensures that security measures are incorporated from the early stages of development and throughout the entire lifecycle.

In summary, senior business management's active involvement in API security ensures alignment with business goals, promotes security awareness, and establishes robust governance practices to safeguard APIs.

Detailed Information

Course Code	: TN488
Course Duration	: 1 Day Workshop
Course Location	: TLC, Online, and Customer On-site.
Terms & Conditions	:100% payment in advance.
Course Deliverable	: Comprehensive Student Guide and Course Certificate

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

Opportunities are made, not found

Executive Leadership Series

We look forward serving you as one of your trusted education and training services partners.

www.tlcpak.com