SALT

Financial Services

Secure Your Financial APIs: Navigating Compliance and Threats

Overview: The financial services industry frequently faces the challenge of innovating without compromising on security standards. APIs play a vital role in open banking, payment processing, and customer engagement; however, they also bring considerable risks. This document highlights essential compliance requirements and security factors relevant to financial APIs, emphasizing the crucial role of API Posture Governance in navigating these challenges and ensuring continuous compliance..

Compliance Landscape:

- PCI DSS v4.0: Crucial for safeguarding cardholder information. This standard is particularly relevant for APIs processing payment card data, highlighting the importance of secure development, robust access controls, and effective vulnerability management to thwart fraud and data breaches. [Req. 2.2.7, 6.2.3, 6.2.4, 6.3.2]
- Open Banking and PSD2 (EU): Requires secure APIs for third-party access to customer accounts, enforcing Strong Customer Authentication (SCA) and secure communication protocols. [Article 30]
- NYDFS Cybersecurity Regulation (23 NYCRR 500): Mandates that financial institutions in New York State establish thorough cybersecurity programs, which encompass API security measures. [500.11]
- ISO/IEC 27001 & 27017: Establishes a framework for information security management, particularly within cloud settings, which is crucial for protecting sensitive financial data and ensuring continuity of business operations.
- MITRE ATT&CK Framework: Provides valuable insights into adversary tactics that target financial APIs, aiding organizations in understanding and mitigating potential attacks.

Key API Security Considerations:

- Strong Authentication and Authorization (OAuth 2.0, MFA).
- Secure Data Transmission (TLS, mTLS).
- Rate Limiting and Input Validation to prevent abuse.
- Continuous Monitoring and Logging for anomaly detection.
- Regular Vulnerability Assessments and Penetration Testing.
- Data Loss Prevention and Encryption.

How Salt Security Helps:

Salt Security offers a robust API security platform designed specifically for the finance sector and achieve compliance:

- API Discovery: Finds all APIs, including shadow and zombie versions, for thorough visibility.
- Posture Governance: Following API discovery, Salt Security automates the enforcement of security policies and compliance with financial regulations (e.g., PCI DSS, GDPR) using pre-built and custom rules. This ensures a consistent security posture across all APIs and simplifies compliance reporting.
- Vulnerability Assessment: Identifies API vulnerabilities, including flaws in business logic.
- Threat Detection: Guards against attacks such as credential stuffing and API abuse, safeguarding transactions and data.
- Data Security: Ensures visibility into sensitive financial data as it moves.

Conclusion:

Safeguard your financial assets and uphold customer trust by implementing a strong API security strategy. Salt Security provides essential tools to automate API security and posture governance, directly helping you achieve and demonstrate compliance with regulations like PCI DSS, PSD2, and NYDFS. For a deeper insight into API security compliance, we invite you to consult our detailed **API Compliance Whitepaper.**