Turkish Journal of Computer and Mathematics Education *Vol.13 No.02 (2022), 1185 - 1188*
Research Article

Financial Data Security and SIEM: Protecting Sensitive Financial Information in Banking and Fintech Systems

ShivaDutt Jangampeta
Senior Manager of Security Engineering
JPMorgan Chase
Plano, USA
shivadutt87@gmail.com

ABSTRACT

Financial Technology (Fintech) companies thrive on data security and trust. Customers willingly entrust these organizations with their valuable personal and financial information. Failure to preserve this trust could erode the very foundation they rely on to conduct their business. Robust cybersecurity measures and solutions have become a necessity in an era where many fintech organizations are increasingly embracing digital transformation. SIEM solutions use multiple data security monitoring tools and effortlessly fit in the fintech environment. This paper reviews the importance of SIEM systems in fintech space.

Keywords – Security Information and Event Management (SIEM), Financial Technology (Fintech), Next-gen SIEM.

Introduction

For everyone living in the modern digital era, data is everything. For businesses, money is their focus. When you fail to protect your money, someone will steal it. Thus protection of data is not just a compliance checkbox but a requirement for a business to survive and prosper [1]. Essentially, data protection involves robust security measures and solutions to safeguard sensitive financial data from constant security threats.

Financial Technology (Fintech) has revolutionized the finance industry with exemplary solutions, including advanced payment, lending, mobile banking, and financial management methods. However, whereas fintech has improved financial accessibility and efficiency, it has brought security risks that need to be addressed to ensure sustained growth. Therefore, in the increasingly evolving fintech space, cybersecurity plays an essential role in guaranteeing integrity, privacy, trust, and availability of digital financial services.

A. Innovative cybersecurity solutions for Fintech companies

Fintech companies rely on innovative cybersecurity solutions such as cloud computing, artificial intelligence (AI), Blockchain, and big data analytics. While these advanced technologies enhance financial accessibility and holistic business operation, they present potential cybersecurity risks. For instance, cloud computing escalates data confidentially challenges; artificial intelligence and big data require robust data protection to secure customer data; and blockchain requires an appropriate

implementation to block unauthorized access.

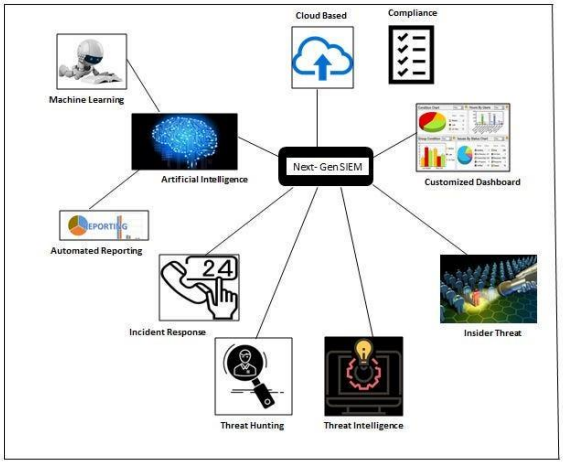

Fig. 1. Features/benefits of Next-gen SIEM tool

B. SIEM Cybersecurity for Fintech Companies

Recently, the demand for next-gen SIEM cybersecurity solutions in the finance industry has become increasingly apparent. Traditional SIEM solutions have become obsolete: they cannot address evolving and new security threats across sophisticated heterogeneous environments. Consequently, businesses are looking for robust SIEM systems to enhance their security posture. Fintech enterprises should secure their data from a wide spectrum of security threats. With a vast wealth of valuable data, digital assets, payment systems, as well as user data at risk, these businesses are lucrative targets for a broad variety of cyber-attacks, including phishing attacks, data breaches, DDoS attacks, fraud, etc. Modern Next-gen SIEM cybersecurity solutions prevent all these cyber threats as they offer robust platforms that enable constant monitoring, identification, and real-time mitigation of security events. These advanced SIEM solutions go beyond standard query functions and log management to provide top-in-class threat identification while guaranteeing compliance with industry-specific regulations.

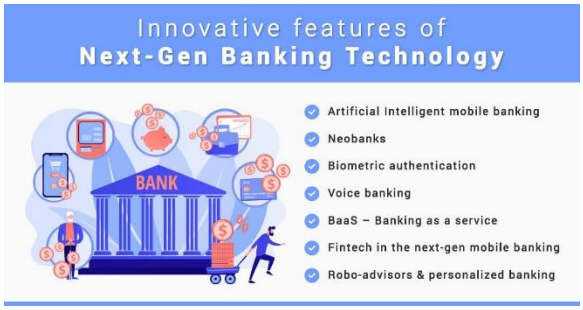

Fig 2. Advanced features of Next-gen Banking Technology

Significance of Advanced Next-gen SIEM Cybersecurity Solutions

***A.* Addressing emerging challenges in the Fintech environment**

Financial institutions are faced with an evolving threat landscape and increasing operational complexity that sabotages their information security, compromises valuable data, and upsets their service delivery. As a result, these companies have a mandate to implement advanced cybersecurity tools to guarantee

comprehensive protection of their sensitive data against emerging and evolving threats. Next-gen SIEM solutions address security gaps like:

i) Cloud threat detection gaps

Whereas cloud-powered solutions offer flexibility and scalability, they also pose significant security risks to Fintech companies. For example, cloud misconfigurations, inadequate access controls, and unprotected interfaces can result in the divulgence of sensitive data. Contemporary security threats go beyond data centers, networks, BYODs, edge, etc. thus security teams often encounter visibility gaps or a high number of false positives. Next-gen SIEM solutions address these problems and leverage advanced tools like AI and ML analytics to project, identify, prevent, and mitigate security incidents across complex IT environments.

ii) Insider risk management

High-fidelity SIEM cybersecurity tools enable proactive internal threat identification and mitigations. These solutions process and analyze huge volumes of data from different sources to spot anomalies, unusual behaviors, and patterns. These tools contextualize the information with employee sentiment information to correctly prioritize internal risks.

*iii)*Cybersecurity talent gap

Advanced SIEM cybersecurity solutions address the cybersecurity talent gap by optimizing the efficacy of SOC experts. The tools leverage AI and ML algorithms to automate the threat identification process and configure pre-defined rules that immensely minimize response times to new and evolving security threats, enabling SOC teams to promptly examine, analyze, and respond to potential threats before they become substantial data breaches.

iv) Rebalancing standard SIEM spend

If traditional SIEM systems are deeply rooted within an organization's security operation, ripping them can be a hassle thus it is recommended to augment them. However, running multiple SIEM systems can be costly and at the same time unnecessary [2]. Fortunately, next-gen SIEM solutions offer consumers cost relief by reducing ingestion costs for traditional SIEMS. The advanced tools offer surprising flexibility regarding data storage options and allow businesses to explore different security data lake options.

B. Excellent financial service capabilities

Advanced SIEM systems are characterized by multifaceted capabilities in managing intricate cybersecurity environments specific to the fintech industry. They are:

(i) Flexible architecture

Next-gen SIEM solutions offer fintech businesses tremendous flexibility in terms of embracing different security data lakes, customizing ML-based models, as well as hosting and data ingestion options.

(ii) Seamless Data ingestion

These tools offer an immensely streamlined approach to data consumption, enabling efficient collection and investigation of security data. As a result, the overall cybersecurity posture of fintech businesses is bolstered.

(iii) Advanced ML analytics

ML-based Next-gen SIEM solutions enable proactive threat detection and mitigation, enabling fintech organizations to secure their IT infrastructures against new and evolving security threats.

(iv) Contextualized Risk Scoring and Prioritization

These advanced SIEM solutions offer contextualized risk scoring and prioritization, enabling fintech businesses to focus on significant security incidents and allocate adequate resources for mitigation.

Conclusion

The uptake of advanced SIEM tools by fintech companies improves their cybersecurity postures by enhancing security system flexibility, streamlining data consumption, offering ML-based analytics, and contextualizing risk scoring and prioritization. This enables them to proactively identify, prevent, and respond to potential security threats; securing their sensitive information from threat actors.

References

[1] Medium , SIEM and Financial Industry., Cybersecurity Manual., 2019.
[2] Finsec, Cybersecurity in financial sector infrastructures from SIEM probes to risk assessment and mitigation with a use case walkthrough, 2020.