alletec

Strengthening Cybersecurity for India Operations of a Leading Asian Bank

Security Information and Event Management (SIEM)

Business Overview

A prominent international bank, headquartered in Bangladesh, has been steadily expanding its footprint across India. Focused on offering high-quality banking services to exporters, importers, and retail customers, the bank is registered as a foreign bank in India. Despite operating with a limited capital base, the bank has rapidly grown in last couple of years by maintaining strong connection with Vostro-banks, valued customers and stakeholders. With operations spread across few locations in India, the bank is committed to modernizing its operations and strengthening its technology infrastructure to match its pace of growth.

Business Challenges

As part of its technology modernization initiative, the bank made a strategic decision to host its core banking systems and applications on the cloud. While this move offered scalability and agility, it also introduced critical cybersecurity challenges, including:

- A need to **continuously protect cloud-hosted infrastructure and applications** from cyber threats
- The requirement to **collect and monitor logs** from all systems, applications, and devices in a centralized manner
- The goal of enabling **real-time threat detection, identifying compromised users, and detecting behavioral anomalies**
- A need to **reduce manual processing** of security logs, ensure better compliance, and enhance visibility into security operations

Alletec's Approach and Solution

The Bank partnered with Alletec, a trusted cybersecurity expert, to address these challenges. Alletec began by assisting the bank in securely provisioning its systems and applications on the cloud, establishing a robust foundation for their digital operations. Following this, Alletec's cybersecurity experts conducted a thorough assessment of the bank's environment and recommended the implementation of an intelligent **Security Information and Event Management (SIEM)** solution based on Microsoft technology - specifically, **Microsoft Sentinel.**

The implemented solution focused on:

- **Log aggregation from all systems, applications, and users**
- **Advanced threat intelligence and analytics** to detect anomalies and potential breaches
- **Real-time event correlation** to detect compromised users and unusual behavior
- Creation of **automated policies** to monitor violations and respond proactively

Impact and Results

- Enhanced security operations efficiency
- Faster and automated incident response
- Improved threat detection accuracy
- Over **50% reduction in manual effort**
- Better compliance and SLA adherence

By replacing manual log processing with an AI-driven enterprise SIEM platform, Alletec **enabled the bank to analyze 100% of logs**— dramatically improving the accuracy of threat detection and enabling the timely identification of security violations and better enforcement of security policies.

The implementation of SIEM solution for log management and correlation helped us achieve security and data compliance.

Alletec's Role in Driving Cybersecurity

Alletec has emerged as a trusted cybersecurity partner for BFSI organizations navigating digital transformation. For this bank, Alletec not only provisioned a secure cloud infrastructure but also enabled enterprise-grade cybersecurity by implementing Microsoft's SIEM solution tailored to financial compliance and risk management.

With continuous monitoring, AI-based threat detection, and policy automation, Alletec helped the bank elevate its cybersecurity posture, reduce operational risk, and build resilience in a dynamic regulatory and threat landscape.

USA
5605 North MacArthurBlvd.,
Ste 1000, Irving, Texas 75038

Canada
181 Bay Street, #1800,
Toronto, Ontario, M5J 2T9

Kenya
The Westwood, Vale Close off
Ring Road Westlands, Nairobi

India
A-1, Sector - 58
Noida - 201 301