



## At the Heart of Security Management

## Securing IT Assets from Continually Evolving Threats

### CASE STUDY

#### Synopsis

In a complex business environment, effective monitoring and reporting of security incidents requires deep understanding of a variety of requirements—from regulatory mandates and knowledge of security controls to the ability to secure IT assets from various threats. A global financial enterprise found this capability in us. They entrusted us with providing a security incident tracking and reporting system that reduced their operational risks. Today, as their Security Incident and Event Monitoring (SIEM) vendor, we continue to deliver new ideas and more value, ensuring their security incident monitoring and management processes are strengthened.

#### About the Client

A global financial enterprise, the client has more than 53,000 employees, and offers retail and

commercial banking services to customers in over 40 countries.

#### Business Challenge

Given the background of various security incidents and failed security monitoring initiatives, the client realized it was imperative to

- ◆ strengthen the security system, process, and operations from cradle to grave
- ◆ comply with regulatory norms
- ◆ overcome skill challenges that were coming in the way of leveraging technology.

For one, there were no backend facilities to process the information. The client also wanted foolproof supervision in an affordable and non-intrusive manner, increased credit rating, and reduced downtime.

## Our Solution

Given the customer-centric nature of the incident management process, we understood the strategic importance and business impact of a new and improved version of the security incident tracking and reporting system upon the client's operations. We helped the client deploy an enterprise-wide SIEM solution that enabled them to:

- ◆ Strengthen security incident monitoring and management processes and measures
- ◆ Set up a cradle-to-grave security monitoring and reporting environment with architecture spanning redundant systems, applications, and networks
- ◆ Use cost-effective 24x7 dual shore operations for business continuity—with services including tooling administration, vulnerability scanning and assessment, penetration testing, user access management, and machine state monitoring
- ◆ Customize agent (tool interfaces for application) development for Sybase, Oracle, SQL, Banker's Automated Clearing System (BACS), and several other business applications
- ◆ Customize crystal reports as per their specification

Our trained and skilled staff used tools and processes to provide a workflow-based solution that recorded footprints at each level of security

investigation. We also provided VPN connectivity that facilitated remote monitoring for the client.

## Delivering More Value

We deployed a 24X7 monitoring system that monitored services from offshore/onsite locations.

- ◆ **More Improvements:** With our solution, the client improved and strengthened their security incident management processes and measures, thus reducing operational risks. We also improved the client's overall audit rating, thus allowing them to free up their blocked money.
- ◆ **More Alignment:** We successfully aligned new business initiatives with the security operations center in the planning phase—mitigating risks.
- ◆ **More Savings:** The costs involved in complying with regulatory norms dropped through our offshore-onsite approach to execution.
- ◆ **More Satisfaction:** We reduced the downtime and revenue loss due to malicious or non-malicious activities—improving customer experience and brand equity. The regulators were also satisfied with the implementation.
- ◆ **More Efficiency:** The minimum involvement of internal resources in daily operations ensured that they were free to focus on strategic activities.

## The NIIT Technologies Advantage

Relying on our monitoring system, the client not only gets regular alerts that notify of malicious activity but can also recognize attack types and prevent issues before they begin. Our tools and processes further helped them handle and escalate security issues to the concerned department.

The successful implementation of our solution gave confidence to the client leading them to implement the solution in three more countries in which they operate.

