CYBALT™

**BANKING ENTERPRISE**
CASE STUDY

# Providing 24 X 7 Security Monitoring, Management and Response Services to a Leading Banking Enterprise

## INTRO:

One of the leading banking and financial services enterprise was looking for efficient and effective 24 X 7 security monitoring, management and response services. After a rigorous selection process, Cybalt™ was selected to provide the services, which eventually enabled the bank to perform their business in the most secured way.

## OBJECTIVES:

The Bank commenced operations in 1991, and has since grown to become one of the most respected and services focused banks in the region.

The Bank was encountering challenges of managing potential security threats from their increasingly popular next generation client touch points. Their business applications and customer portals enhanced customer experience and increased business convenience, but posed unique cyber security risks to the bank.

Hence, the enterprise needed greater visibility into transactions; streamline its cyber security processes and configurations. Moreover, the intended to instill a security mindset across their managerial structure.

## SOLUTIONS:

To arrive at a proper solution it was important to perform comprehensive Risk Assessment. It also included studying their entire IT infrastructure, architecture, various business flows, network layouts and baseline, applications, existing security threats through deep dive pen testing, knowing the processes and its on-ground implementation etc. Based on the initial efforts, a comprehensive plan was prepared to provide 24*7 security services, which mainly served to provide visibility, improved detection and response.

This detailed approach helped immensely to arrive at very effective detection mechanism ensuring minimum false positives. Response also improved with specific and detailed remediation steps. This was mainly done with help of industry standard i.e. MITRE attack framework. Specialized skillsets and processes were utilized to achieve needed SLA and always ahead of threats to ensure it doesn't impact the business.

Various awareness sessions were also conducted which helped the bank to strengthen the first line of defense. Ongoing blue teaming and red teaming sessions were conducted to continuously test Bank's preparedness to address vulnerabilities. This provided a significant boost to achieve necessary maturity.

## AT A GLANCE

### Challenges:

- Lack of threat and risk visibility
- Immature cybersecurity processes
- Ineffective configuration management
- Unavailability of cybersecurity skillsets

### Benefits:

- 24X7 Security monitoring and response to protect from threats
- Configuration baseline basis on risk assessment
- Streamlined policy and procedures for sustainability
- Efficient incident management program

## BENEFITS:

At the very outset, it provided enhanced visibility, which was very critical. Additionally, with an effective incident management process that included monitoring, detecting and response, Cybalt was able to secure overall threat landscape effectively. Cybalt team approached this project holistically and provided a long-term roadmap to increase the security posture of the client. This eventually helped the bank to achieve required security maturity level.