CASE STUDY

SECURITY OPERATIONS CENTER SERVICES FOR THE LARGEST SOUTHEAST ASIAN BANK

Achieved enterprise-wide security monitoring, incident reporting using a single platform.

Client Background

The client is one of the largest banks in Southeast Asia offering a gamut of banking and financial services to its customers. The client has different business units, each with their own IT and development teams, who share a common platform for certain banking applications. To build a better fortress and ensure safety from cyberattacks, like the biggest cyberattacks of 2016 that impacted various banks and financial institutions, the client wanted to test and improve its security posture. The key objectives of the client included:

- Building a Security Operation Center (SOC) service for enhancing the overall cybersecurity capability.
- Ensuring round-the-clock SOC service Service for Asia's leading nationalized bank.
- Providing Security Information Event Management (SIEM) tool training to the customer Security Team for dashboard creation and report management.

Xoriant Solution | Key Contributions

The client needed a strategic approach in real-time threat analysis and event response to tackle its everyday banking cyber security infrastructure issues. Xoriant was chosen as a fully managed security operations service provider considering our security expertise, training in latest threats and counter measures, insights on latest tools, technology to deliver end-to-end security management for applications and infrastructure. Our key contributions for the client included:

KEY BENEFITS

- Reduced risks of customer network being compromised with an improved response time security events.
- Enabled SOC team to effectively spot potential network vulnerabilities and address them before they become critical using threat monitoring.
- Helped achieve and maintain compliance with applicable International and Federal regulations.
- Improved thread identification and response time by ensuring a consolidated single point threat reporting hub.

- Operationalized the existing security tools and technology investments in client environment with support of expert team of analysts to provide real-time threat analysis and event response.
- Developed new rules and alerts to address new threats and increase operational efficiency with a collaborative approach between research and operations teams.
- Monitored each client device round the clock using a Logcollector (Sentinel) device installed at customer data center to collect and forward logs from each client device to ELK in cloud.
- Generated alerts with monitoring system for device network reachability state change (up/down), availability state change or threshold reached via SNMP polling, syslog events based on severity or custom alerting criteria, SNMP trap events based on severity or custom alerting criteria.
- Acknowledged alerts received by Xoriant SOC team, logged a Trouble Ticket within 30 minutes for the alert and executed alerting analysis activities.
- Generated notifications for alerts and sent to the customer's e-mail or phone in accordance with the customer contact list based on the following criteria – device type, alert severity, day incident date and time, escalation list.

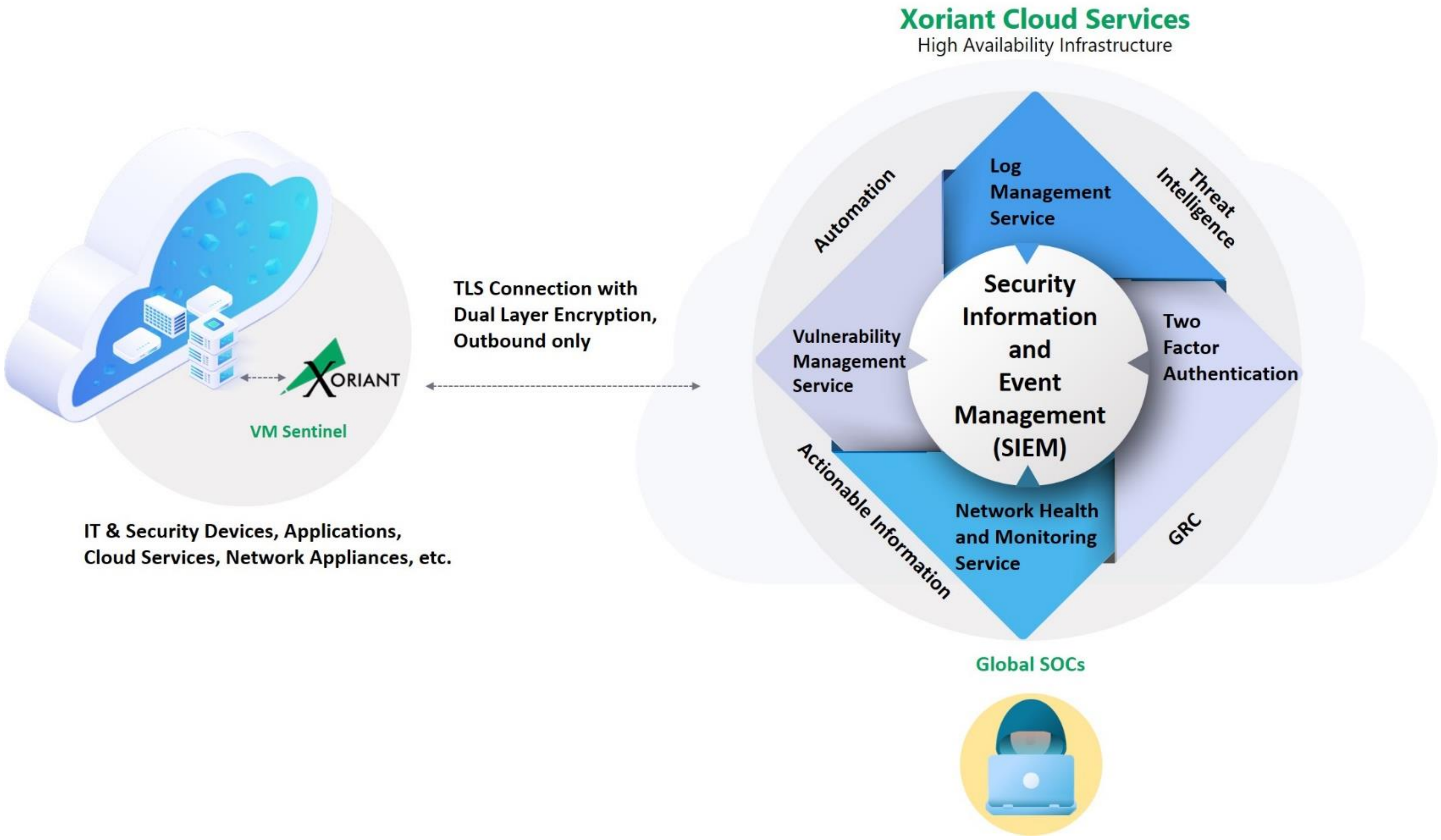
KEY BENEFITS

- Achieved global enterprise-wide security monitoring, incident and health improvisation reporting under a single platform.
- Provided detailed remediation steps to customer IT team to detect existing flaws and prevent future attacks.
- Reduced total cost of ownership by providing cost-effective SOC services.

Client Testimonial

> *Xoriant Security Team implemented Rules and Alerts mechanism based on ELK running on secured cloud platform. It reduced identification of security gaps and our customer overall security alert analysis time by 50%.*

Architecture Diagram


Xoriant Cloud Services
High Availability Infrastructure
XORIANT
VM Sentinel
IT & Security Devices, Applications, Cloud Services, Network Appliances, etc.
TLS Connection with Dual Layer Encryption, Outbound only
Log Management Service
Vulnerability Management Service
Security Information and Event Management (SIEM)
Two Factor Authentication
Network Health and Monitoring Service
Automation
Threat Intelligence
Actionable Information
GRC
Global SOCs

Technology Stack

Elastic Logstash | Kibana | GCP Cloud |Third-Party Ticketing Tools