LTIMindtree

CASE STUDY

Modernizing SOC for a Leading Financial Services Company in Africa

Improving Cyber Defense Protection by transforming existing SOC into a cognitive and autonomous SOC

Client

The client is a leading financial services company in Africa.

Challenges

As a long-standing client partner for the last 15 years, we understand their key business drivers impacting security. The key challenges they faced were as follows:

- Inadequate insights into critical vulnerabilities
- High number of false positive alerts
- Lack of operationalization of threat intelligence
- Lack of integration of asset management data into the SOC

LTIMindtree Solution

LTIMindtree enabled a holistic security view for the client and improved cyber defense maturity by redefining security operations and threat intelligence. We modernized their Security Operations Center (SOC) by enabling threat intel, content development, security orchestration, and automation across 36k+ assets.

Key Solution Highlights:

- Operationalized next-generation SOC with SIEM-based security, threat intelligence, IR automation with Security orchestration, automation and response (SOAR), Endpoint Detection and Response (EDR) security, SOC operations, and incident response
- Enabled content engineering driven by threat intelligence inputs and mapped to MITRE Framework
- Set up process to assess content coverage and enhancement based on live threat intel feed
- Created a customized playbook in SOAR leveraging threat enrichment sources and multiple third-party tools
- Performed daily analysis of critical vulnerabilities along with the availability of exploits and publish advisory
- Created and finetuned detection use cases on threat intel platforms
- Developed 16 Playbooks and created 10 SOPs
- Implemented priority intelligence requirements that include dashboards, rules, and disseminating actionable threat intel
- Published more than 21 threat intel reports and SOP developed for intel sharing and investigation of TI POV.

Business Benefits

LTIMindtree's intel-led, data-driven, automated response helped the client achieve the following key business outcomes.

- MITRE Technique IDs coverage improved from 36 to 59
- Improved threat detection efficacy (TDE)
- Improved intel-based TDE
- 70% of effort saved on malware, phishing, CrowdStrike, and Network Access Control (NAC) alerts incidents
- Rule finetuned to reduce false positive instances