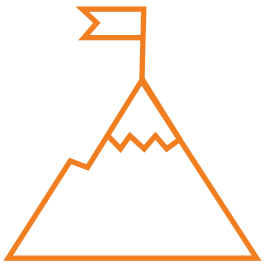
LTI
Let's Solve

A Larsen & Toubro Group Company

Case Study

Driving Cyber Defense Maturity for a Global HVAC Manufacturing Conglomerate with End-to-End Advisory, Implementation, and Operational Support

The client is a world leader in heating, air-conditioning, and refrigeration solutions, with proven history in driving innovation with new products and services that improve global comfort with efficiency and sustainability.



Business Challenges

- Blueprint for modernizing existing SOC to a next-gen SOC with the right level of technology integration, operationalization, and contextualization using cyber analytics
- PaloAlto XSOAR platform implementation, operationalization, and BAU support; automation of runbook/playbook, and building an active cyber defense operations center
- Implementation services such as security monitoring and incident response, and content engineering and development
- Staying a step ahead of adversarial activities by leveraging contextualized Threat Intelligence inputs and proactive Threat Hunt mechanism
- Making the existing security operations center robust enough to meet necessary compliance standards and conform to established NIST cybersecurity standards.

LTI Solution

Performed product security evaluation, devised smart manufacturing, building, refrigeration, transportation digital security strategy, and architecture design

Provided technical blueprint for setting up a digital SOC and supported building up a business case for monetization of digital SOC blueprint

Evaluated existing SOC capability and defined a next-generation active cyber defense blueprint and roadmap to evolve an integrated operational SOC model with security monitoring, intelligence, hunting, automation, and orchestration—including a product recommendation roadmap to move to the active SOC journey in the future for achieving NIST maturity of 3.9+

Provided next-gen cyber operations—AI/ML and cyber analytics-driven SIEM for 100k+ assets and 60k+users, with strict conformance to defined SLAs/KPIs, 24x7 monitoring, threat investigation, detection, and reporting services

Assisted customer in SASE/cloud security build, monitoring, and management, runbook/playbook automation, and content engineering for TI, TH, TD for building up next-gen active cyber operations

Identified emerging trends and attack methodologies based on investigations, internal/external threat feeds, and dark Web and open source intelligence; ensured cyber threat operations will be conducted daily to meet the evolving risk landscape

Developed new rules/customized existing rules-based on trends, attack methodologies, and emerging threats

Used referential data and complex rule sets to provide real-time fraud and loss prevention monitoring as applicable

Executed intrusion discovery/response by thorough analysis of threat feeds, vulnerabilities, and by formulation of hypothesis pattern and TTP detection

Business Benefits

Fewer cyber attacks and other malware infection and propagation due to enhanced resilience with the right level of technology integration, operations, and support	**Enhanced SOC efficiency and velocity** due to improved operational performance and efficiency with development of custom use cases, runbook/playbook automation, content engineering for Threat Intelligence, Threat Hunting, and Threat Detection for building up next-gen active cyber operation	**Keeping pace with cyber adversaries** as a result of enhanced velocity in responding to threats with infusion of contextual, noiseless and prioritized cyber threat intelligence reports	**Increase efficiency with operationalization of 9k+ use cases** for Intelligence and Purple team-driven threat hunting, development, and operationalization of identified new rules, and creation/fine-tuning of use cases and correlation rules	**Reduced cost of operation** for threat intelligence services due to sharing of threat intelligence across a broad pool of users

Info@lntinfotech.com