LTI
Let's Solve

A Larsen & Toubro Group Company

Case Study

End-to-End Managed Security Services for Leading Insurance Company

Client

Our client is a leading provider of comprehensive suite of solutions ranging from traditional life insurance, annuity reinsurance, to acquisition support, which solves complex balance sheet needs based in the US.

Challenges

- The client was looking for a roadmap to improve its overall cybersecurity posture.
- They did not receive reliable and up-to-date threat intelligence from dedicated internal and external resources on a regular basis.
- Furthermore, a formal process to develop threat models, aggregated list of threats, threat actors, and threat motives was not established.
- Access requests were managed through a paper-based process. As a result, a centralized view of access provisioning requests was not in place.
- Access to the office wired network was not restricted, allowing unauthorized devices to establish a connection with the organization's internal network.
- The client's users have local administrator privileges on laptops and workstations, allowing them to install software and administer the operating system without any restrictions. They were looking for a privilege access management solution.
- Vulnerability management was handled by another vendor and there wasn't enough visibility on remediation progress, risk posture.
- There was a need of a process which would ensure remediation efforts are focused on truly critical and high priority vulnerabilities as per the client's environment before moving onto lower priority vulnerabilities.
- They had several business partners and were looking for a B2B VPN tunnel solution to their partner networks.

LTI Solution

- Developed a well-defined project-plan & roadmap for implementation of multiple cybersecurity solutions for the client.
- Implemented Securonix SIEM solution, which receives comprehensive threat intelligence feed from third-party vendors. Based on these feeds, threat models were defined. All NSRE-ingested logs are compared against these threats model and any violations are immediately flagged for action or remediation.
- In addition, threat models were created specific to the client environment, which ensured any anomalies or unusual traffic was immediately detected. Furthermore, behavior-based detection was also implemented (UEBA).
- Saviynt and accompanying operating/monitoring processes were implemented to enforce IAM standards across the enterprise.
- BeyondTrust and accompanying operating/monitoring processes were implemented to properly manage privileged accounts. Local admin privileges would be disabled through this BeyondTrust PAM implementation.
- Established a well-defined vulnerability management process and associated SOPs. These were built after numerous discussions with the client and customized to their environment.
- Established a process to contextualize vulnerabilities' criticality – based on the asset's criticality, location of the asset, security controls, etc. This ensured prioritization of remediation efforts.
- Deployed a Network Access Control solution using Cisco ISE. This ensured detection of any rogue devices connecting to the network among other access control policies.
- Successfully designed and implemented a B2B VPN tunnel solution to the partner networks of the client.

Business Benefits

Improved the overall cybersecurity posture of the client by the implementation of several security solutions.

Customized threat models and UEBA functionality of SIEM ensured optimum usage of security monitoring by focusing on events of interest.

Helped channelize remediation efforts on vulnerabilities, which are truly critical for the client's environment.

SOPs were drafted and constantly updated – resulting in a more streamlined problem-solving capability. This, in turn, reduced the overall time to resolve the incidents.

Reduction of false positives on SIEM has ensured efforts are utilized appropriately on true positives, thereby increasing the overall productivity.

A fully functional B2B VPN tunnel solution with the client's partner networks, ensuring a secure and smooth communication.

LTI (NSE: LTI) is a global technology consulting and digital solutions company helping more than 400 clients succeed in a converging world. With operations in 31 countries, we go the extra mile for our clients and accelerate their digital transformation with LTI's Mosaic platform enabling their mobile, social, analytics, IoT and cloud journeys. Founded in 1997 as a subsidiary of Larsen & Toubro Limited, our unique heritage gives us unrivalled real-world expertise to solve the most complex challenges of enterprises across all industries. Each day, our team of more than 33,000 LTItes enable our clients to improve the effectiveness of their business and technology operations and deliver value to their customers, employees and shareholders. Find more at **http://www.Lntinfotech.com** or follow us at **@LTI_Global.**

info@lntinfotech.com