Case Study

Vulnerability Management for Leading US-based Reinsurance 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

- Vulnerability management which includes, infrastructure (1500 assets) and applications (25) spread across multiple locations and hosted on the cloud platform as well.
- Perform Grey box application security testing on external exposed apps.
- Lack of visibility on key items such as vulnerability remediation, overall risk posture.
- Need for 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.
- Need a more flexible and customizable vulnerability management solution.
- Need visibility on how compliant its systems were to CIS and other benchmarks or standards.
- The solution must meet compliances for NYDFS, HIPAA & CISA/NIST defined PC/VA standards.

LTIMindtree Solution

- Qualys-based Hybrid Solution with cloud agents and scanners. Cloud agent-based scanning provided more flexibility in terms of scanning and reporting frequencies.
- Qualys virtual scanners were deployed to scan infrastructure where cloud agents were not supported.
- Periodic interactions with end-customer to review and discuss on vulnerability remediation progress.
- Process defined to contextualize vulnerabilities as per the client's environment, asset's criticality, placement of the asset, etc. This ensured remediation efforts are prioritized and focused appropriately.
- Policy compliance solution was deployed using Qualys, which ensured periodic reporting of compliance status, tracking remediation, and eventually improving the overall compliance posture.
- Qualys CSA module for AWS-specific misconfigurations, PC and policy hardening, threat management, and IOC-based threat hunting were implemented, and soon in consideration to expand to EDR and stack functions.

Business Benefits

Comprehensive vulnerability management covering the applications, infrastructure based on their CIA requirements, on-premise and cloud assets without any blind spots.

Systems adhering to the compliance requirements for the financial institution. All faults being taken in account and duly fixed with timelines.

Very minimal false positives due to the use of agent-based solution, which increased the operational efficiency. Patching teams fixing the real vulnerabilities that pose threat to the client.

45% reduction in false positives in first year, with ongoing transitions in IT service.