Infopercept
SECURE • OPTIMIZE • STRENGTHEN

CASE STUDY

CYBER SECURITY & RISK ASSESSMENT

LEADING BANK OF MIDDLE EAST

Overview

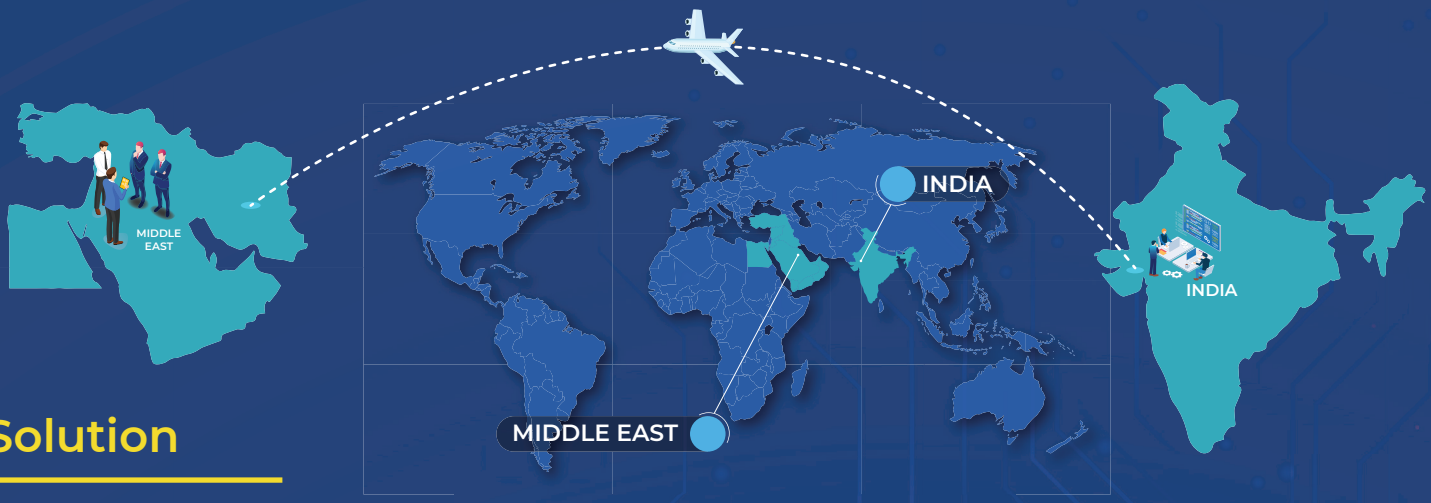
We have worked to minimize the vulnerabilities of a leading bank of Middle East serving a large customer base. The Bank already had expensive solutions and security network infrastructure in place. The bank had an intermediate security framework already in place to ward of potential cyber-attacks. But needed a to spin up a more proactive & robust Security Network.

Problem

The bank had invested exponentially in the Cyber Security infrastructure & already had an SOC & NOC, as well as established Security Plans in place. They also had an INFOSEC team to assess & monitor the overall security framework health. But were unable to efficiently utilize these security resources & assets.

The bank's security was already vetted by top industry names for years. But were still not able to achieve the outcome in terms of the security with regards to the overall investment incurred.

- The bank's security was already vetted by top industry names for years. But were still not able to achieve the outcome in terms of the security with regards to the overall investment incurred.
- A partner & someone already trusted and proven in the industry.
- Solid tech knowledge coupled with great service as this was going to be a marathon & not a sprint
- Using innovative technology, that is reliable & constantly evolving so as to not slow down the process if chasing false positives.
- A "one-stop shop" for vulnerability management, penetration testing in identifying risks.
- Value based service & an advisory partnership, so they can have the guidance while constructing the security network.



Solution

We met all of the criteria needed & were selected. Immediately we set out to build together a team of experienced cybersecurity experts having industry specific and sent them to on-site at the Bank's location in Central Asia. This Cybersecurity Assessment team consisted of:

- Tester & Researcher
- Application Security Expert
- Risk Assessment Expert

This team was subjected to Remote Governance & quality Review from our main office as & when required.

Once reaching the Bank's location in Middle East, our team initiated our patented 7 step process for security assessment & optimization along with our core philosophy of Understanding, Experience & Expertise. These 7 steps include:

- Goals & Scope
- Information Gathering
- Information Analysis & Planning
- Vulnerability Detection
- Attack & Penetration/ Privilege Escalation
- Result Analysis & Reporting
- Clean Up

After a thorough assessment of the Bank's security Network and available solutions we were able to ascertain that although the core banking was protected by a strong security framework. It was under performing due to a lack of proper integration and configuration & also because it was intermingled with other banking apps. Here we could also have suggested a new solution to be added in the bank's already burgeoning Security Solution basket be done with it.

Instead we decided to carefully optimize & fine tune the existing solutions so that they perform efficiently as they should be without costing the bank on another solution.

After recognizing the weak zones of the existing network we subsequently patched them up by Hardening, Optimizing & performing the right integration using the Existing Security Solution available to the bank.

Following our security optimization procedure and patching the vulnerabilities. Bank was able to more safely utilize its Core banking, including Net Banking, mobile banking as well as its internal transaction payment apps.

Helped the Bank to realize that safeguarding a particular Business-Critical zone without proper Network segmentation and the suitable integration won't be able to guarantee overall Network Security & Integrity.

We also shared and imparted our unique approach of SOS (Security Optimization Strengthen) for Cyber Security SOS.

As we believe in the adage of Prevention is better than cure. We want the organizations to be self-motivated & take proactive steps to better strengthen and optimize their Security framework periodically so as to mitigate the occurrence of cyberattack & threats in the business-critical zones.

For Businesses to continue their Operations uninhibited we recommend implementing Cybersecurity SOS for an Emergency SOS situation.

Infopercept

SECURE • OPTIMIZE • STRENGTHEN

Corporate Office:
Infopercept Consulting Pvt. Ltd.
H-1209, Titanium City Center, Satellite, Ahmedabad-380015.
India.

www.infopercept.com | Follow us on -