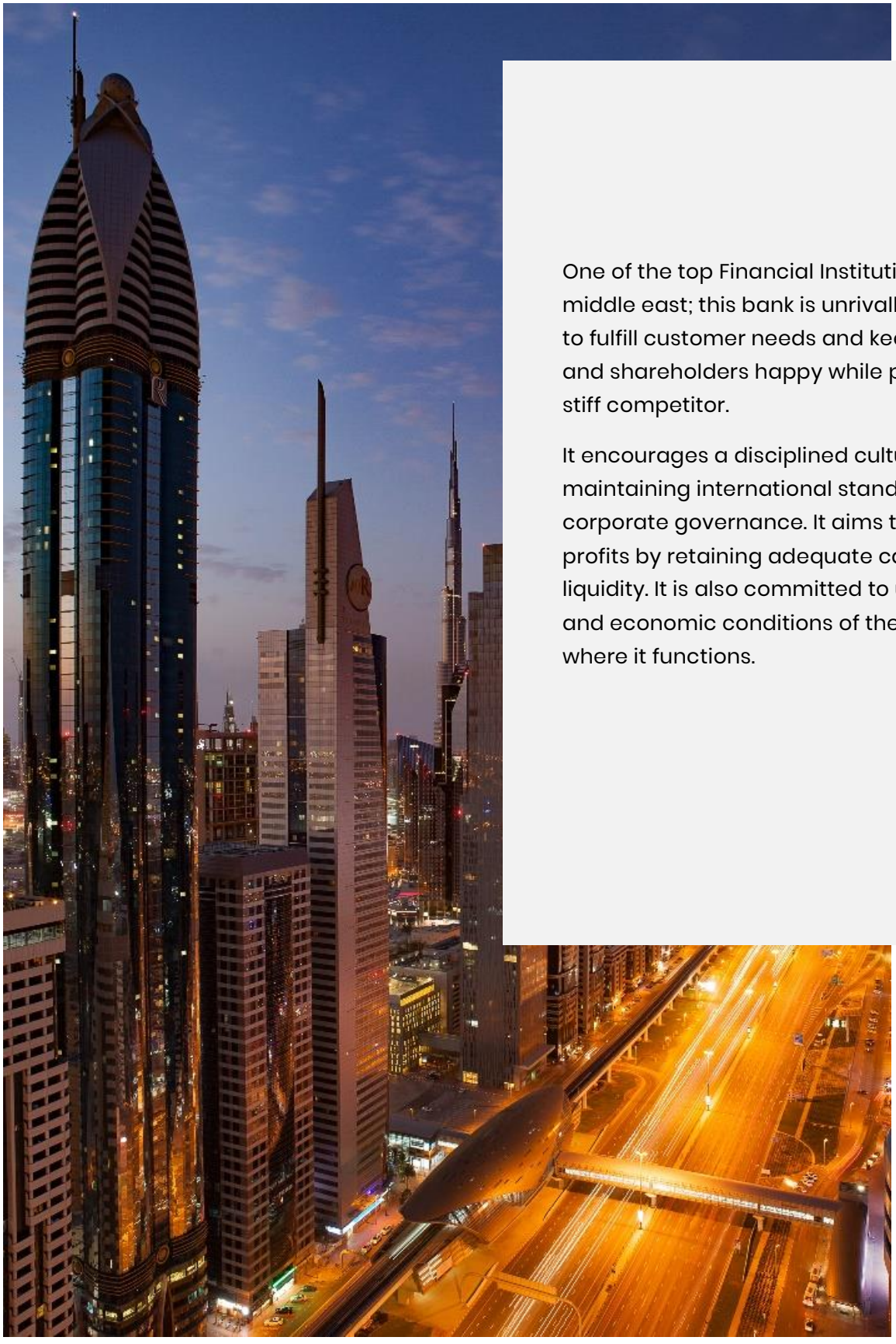
2021

CASE STUDY

Bank Security Optimization for Top Financial Institution in the Middle East

Infopercept

Introduction



One of the top Financial Institutions in the middle east; this bank is unrivalled in its ability to fulfill customer needs and keep employees and shareholders happy while proving to be a stiff competitor.

It encourages a disciplined culture while maintaining international standards of corporate governance. It aims to maximise profits by retaining adequate capital and liquidity. It is also committed to uplift the social and economic conditions of the communities where it functions.

The Problem

The *Chief Information Security Officer (CISO)* of the bank was well informed regarding security issues. He had done extensive research and had come up with top rated solutions for his company. These security solutions were vetted by **Gartner,** a global advisory and research firm, that provides information and tools to enable a company to improve its performance on critical activities. The problem was in integrating and implementing these solutions. A classic skill gap problem where there was a break in the link between solutions and their application.

They were on the lookout for a partner who would be able to bridge the gap and secure the data and infrastructure of the bank. They were keen on partnering with a *Managed Security Services Provider (MSSP),* who would have the skill and expertise to handle critical and sensitive information.

Infopercept was the unanimous choice when it came to providing world class managed security solutions.

Infopercept - An Undisputed Global Managed Cyber Security Services Provider

Infopercept has in the past provided cyber security solutions to a number of companies where the data was extremely confidential. With its highly efficient and competent team members and its mastery over the techniques and skills required, Infopercept was confident of fulfilling the security concerns of the bank.

True to its word, Infopercept, using its prowess over Offensive Security Strategies, was able to tackle the vulnerabilities in the network. This investigation necessitated checking the perimeter, network, endpoint, application, and database of the entire virtual landscape.

Solution:

Infopercept decided to take the benefits offered by the Open Source Software (OSS) tools in its investigation. Due to its high-quality software & hardware, integrated management, low costs, scaling and consolidating features, etc. Open Source Software is sought after by most enterprises to manage their various business needs.

Infopercept devised the following strategies to provide a total cyber security solution:

- As in any defense system, *securing the perimeter* was the primary focus. This was done using *Open Source Tools* that offer cloud based securities and advanced firewalls in order to safeguard the networks.
- *Implementation of firmware*, which acts as the interface between software and hardware, was undertaken. This provided significant competitive advantage to the security posture of the devices. Moreover, it also took care of the device security and updates by managing it centrally from a cloud based platform.
- *System Hardening* that encompasses the hardening of applications, database, server etc. was part of the Infopercept team's method to secure the peripheral network.
- *Cyber security benchmarking*, a technique which involves identifying the problem areas needing improvement, and tracking the changes over time, was another tactic used by the Infopercept team. Using the *CIS benchmark tools*, Infopercept was able to safeguard the network systems against cyber thefts.
- *Security Information and Event Management (SIEM)* that enables users to respond to threats in real time was used with the help of *Splunk*. Splunk acts as a centralized logging management tool both in proactive and reactive security. There were only 30 data sources to start with, by the time the Infopercept team had worked on it, there were 250+ data sources. They further built 300+ use cases and alerts. These use cases helped the users in performing tasks on the website.
- Endpoints or entry points are often the most vulnerable to attacks hence *endpoint patch management* was done. This was done using *Carbon Black*. This cloud-based endpoint security software ensured the detection and prevention of malicious attacks on the endpoints. Virtual agents that use artificial intelligence to provide automated guidance and solutions were installed. Asset mapping or threat mapping was done where all the assets such as phones, laptops, network, applications etc. were assigned risk scores to identify the level of threat. The number of assets escalated from 600 at the beginning to 1500 towards the end of the operation.
- *Application security* makes sure that the code or data within the app is not stolen at the application level. This was done using *Imperva WAF* which essentially protects web applications from online attack. This again is a cloud-based application that acted as a firewall and helped prevent layer attacks and zero day threats. It also enabled the blocking of DDOS attacks.
- Another important proactive measure taken by the Infopercept team was to ensure the *hardening of the operating systems* such as Linux and Windows. For instance, in Linux systems, a large number of components are assembled thus increasing the complexity and surface, which makes the system extremely vulnerable. *Server Hardening* which constitutes a set of disciplines and techniques was introduced as an integral part of improving the security. More than 100 controls were suggested and implemented.

Benefits:

The Infopercept team with its expertise was able to successfully implement the solutions provided by the CISO of the bank. Apart from bridging the gap between solutions and their applications, Infopercept used a number of open source software and tools, and cloud-based applications to further strengthen the security of the network. It provided a number of proactive measures for use in the future, given the sensitive and confidential nature of data stored in the bank. Due to its vast experience in the past of dealing with highly critical information, the Infopercept team was able to significantly improve the posture of the network much to the satisfaction of the bank.

About INFOPERCEPT

Infopercept's vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners' cybersecurity and accreditation needs.

Our specialized core team comprises of experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, are abreast of the latest trends and security innovations; ensuring that you always get the best security approach & solutions for your specific business needs, exactly the way you want it to be.

Imprint
© Infopercept Consulting Pvt. Ltd. 2021

Publisher
H-1209, Titanium City Center,
Satellite Road,
Ahmedabad – 380 015,
Gujarat, India.

Contact Info
M: +91 9898857117
W: www.infopercept.com
E : sos@infopercept.com

Global Offices

UNITED STATES OF AMERICA
+1 516 713 5040

UNITED KINGDOM
+44 2035002056

SRI LANKA
+94 702 958 909

KUWAIT
+965 6099 1177

INDIA
+91 9898857117

Infopercept