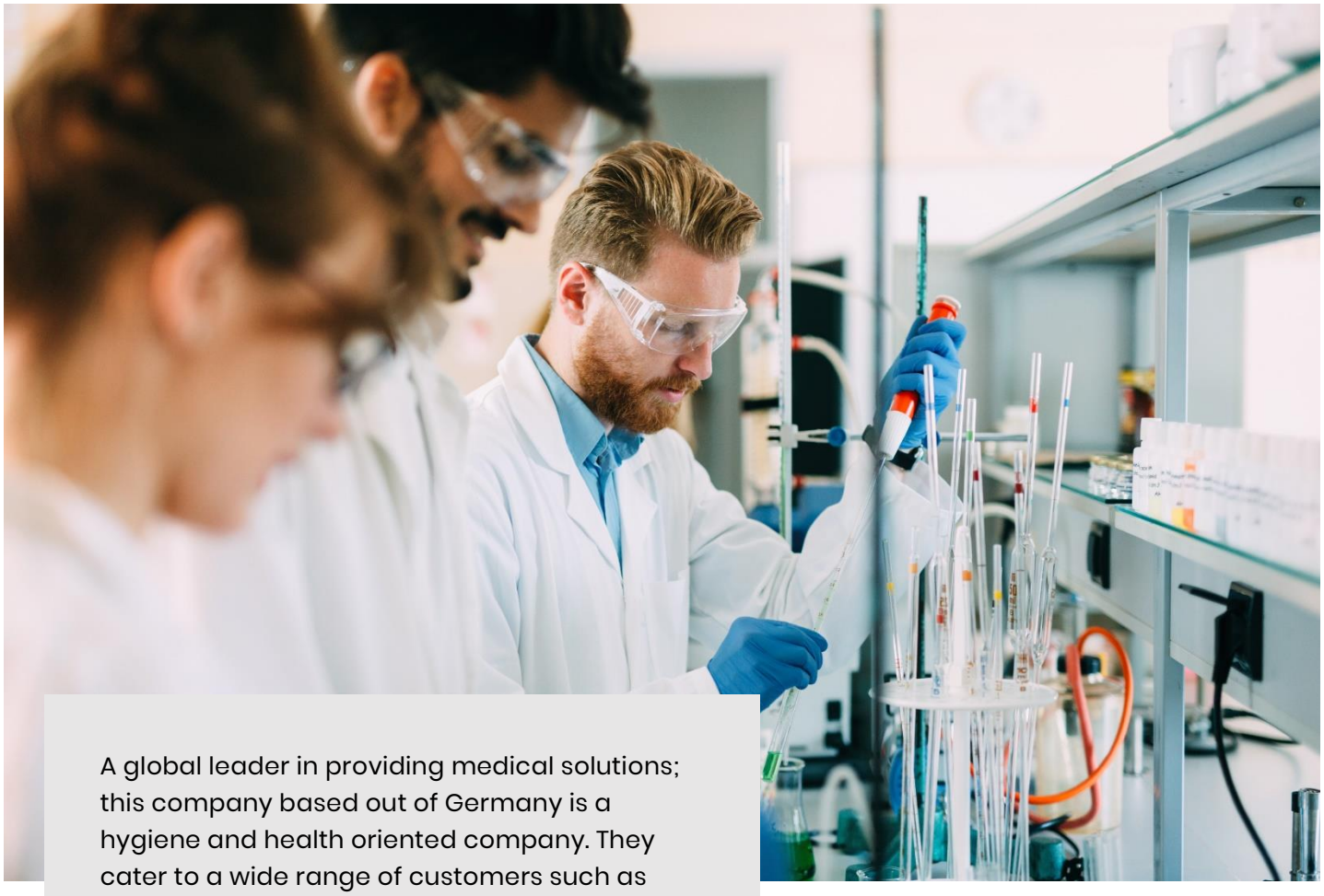
2021

CASE STUDY

Improving Security Posture of a leading German Pharma Company

Infopercept

Introduction



A global leader in providing medical solutions; this company based out of Germany is a hygiene and health oriented company. They cater to a wide range of customers such as online retailers, medical care distributors, and health care facilitators, hospitals, pharmacies etc. They provide a comprehensive package of services, products, and solutions. As they invest heavily in research and development, the CISO was keen on developing a strong security posture for the company's network systems and data systems.

Infopercept, a recognized name in the field of cyber security, is known for its diligent efforts in providing *customized solutions* based on the requirement of the clients. It does an in-depth assessment of security before arriving at a strategy.

The Problem

In the case of the global medical company, Infopercept was well aware of the serious nature of the data. A vast amount of **sensitive data** such as those **pertaining to clinical trials,** or **formulae of new medicines, vaccines etc.** are stored on the network. Considering that a lot of confidential data is at stake, Infopercept took extreme care and precaution while evaluating the systems network.

Solution:

Infopercept came up with a *variety of solutions* to beef up the network security. It launched an **Offensive Strategy** as a part of its **Offensive Security Practices; a proactive approach that uses continuous offensive techniques.**

Infopercept sent across a **Red Team** to scrutinize the network. The IT professionals who constituted the team simulated the actions of their real-life adversaries in order to identify the vulnerabilities and test their ability to detect and respond to real-life threats. Infopercept further did a complete review of the application source code to check for anomalies.

Phishing Exercise

Phishing exercise was taken up as part of the scrutiny. A number of malicious emails were sent to the staff to gauge their responses to phishing attacks.

Vulnerability Assessment and Penetration Testing (VAPT)

VAPT was done which involves vulnerability scanning to help classify security risks and provides services to mitigate them.

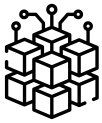
Application Security

Application Security was done to fix vulnerabilities at the application level in hardware and software processes. It is often indicated that a majority of security violations happen at this level.

DevSecOps

DevSecOps is a revolutionary idea that integrates the working of the developers with the IT team to produce outstanding results in securing the network and infrastructure.

Breach and Attack Simulation (BAS)



As a security validating feature, the BAS system helps organizations in identifying, testing, and measuring its security posture across different environments.

Continuous Automated Red Teaming (CART)

CART plays a significant role, where all older traditional methods have failed, in consistently testing and launching safe attacks. This is the need of the hour due to the dynamically changing attack surface and its poor visibility.

Learnings:

The team was able to identify a number of vulnerable areas which required immediate remediation. A *number of loopholes* were found in the internal as well as external applications. They were able *to break through the admin privileges* with ease and were able to gain access to their data systems. Even some of the *password files were not encrypted*, leaving the entire system exposed. In no time, the **Red Team** was able to penetrate into their core area of work and research.

Thus they have to be dealt with early on, to prevent them from becoming serious security breaches.

A debriefing was done with the CISO and the IT team appraising them of the measures taken and the strategies that need to be undertaken in the future to ensure the complete protection of their network security.

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

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