# CASE STUDY

## SHELL UNCOVERS CRITICAL SECURITY VULNERABILITIES THROUGH A CYBER ATTACK SIMULATION

### Client Background

Shell, a global group of energy and petrochemicals companies, has approximately 94,000 employees in more than 70 countries and territories. Shell is helping to meet the world's growing demand for energy in economically, environmentally, and socially responsible ways. It produces more than 3 million barrels of oil equivalent per day and has over 40,000 service stations worldwide. Shell's New Energies business pursues two main areas of opportunities: new fuels for transport, such as advanced biofuels, hydrogen, and charging for battery-electric vehicles; and power, including low-carbon sources such as wind and solar as well as natural gas.

### Business Challenge

After having experienced a cybersecurity incident, Shell Retail reached out to SoftServe to implement a Cyber Attack Simulation and Protection service to evaluate the current security posture and maturity of their IT organization. They decided to partner with SoftServe for the company's 25 years of experience building secure solutions, certifications success, and extensive expertise. SoftServe was asked to develop a plan to perform the following:

- Application security assessments
- Cloud security assessments (internal and external penetration testing)
- Social engineering simulation attacks

## Project Description

The cyber and social engineering attack simulation was conducted by the SoftServe team of certified ethical hackers, experts, and engineers. During the engagement, SoftServe's security experts used best practices and the most advanced guidelines and standards, such as OWASP Top-10 Web Application Risks and the NIST Framework for Improving Critical Infrastructure Cybersecurity.

During the engagement, SoftServe worked in close collaboration with Shell's internal IT team and leadership, including the CIO.

SoftServe recommended a black-box approach for external perimeter penetration testing. Black-box security testing is a method of software and infrastructure security testing in which the security controls, defenses and design of the infrastructure and applications are tested from the outside-in, with little or no prior knowledge of the application's internal workings. Essentially, black-box testing takes an approach similar to that of a real attacker.

Since black-box security testing does not assume or have knowledge of the target being tested, it is a technology independent method of testing. This makes it ideal for a variety of situations, particularly when testing for vulnerabilities that arise from deployment and configuration issues.

In addition, it offers the opportunity to encompass a wide test coverage with a very low false-positive rate when compared to other testing methodologies.

Based on the black-box penetration testing, the process was divided into ten stages:

1. Information gathering
2. Target discovery
3. Scanning and fingerprinting
4. Segregation of targets
5. Vulnerability identification
6. Vulnerability analysis
7. Penetration exploitation
8. Impact analysis
9. Mitigation strategies developments
10. Reporting

During this assessment following areas for testing were covered:

- On-premises equipment and employees
- Employee security and awareness
- Internal IT infrastructure
- Third party resources and providers
- External network perimeter
- Public facing web applications

## Value Delivered

The test uncovered a number of critical vulnerabilities that might have compromised sensitive data. The identified vulnerabilities were exploitable, and the risk posed was significant. SoftServe's security assessment helped Shell Retail prevent significant financial loss.

Within a short time span, SoftServe's team detected a range of defects and provided far-reaching recommendations with regard to internal controls, applications, and infrastructure.

SoftServe's security experts defined the most effective approach to eliminate all the identified vulnerabilities, improve key controls on external and internal infrastructure, and educate employees about security risks and the importance of testing internal security policies and procedures regularly.

---

**"SoftServe's team has the highest level of security expertise. After the security assessment which found critical vulnerabilities we decided to continue our collaboration to mitigate the risks. We have great confidence in SoftServe and highly recommend working with them."**

Alexander Shevchuk, IT Manager, Shell Retail.

# ABOUT US

SoftServe is a digital authority that advises and provides at the cutting-edge of technology. We reveal, transform, accelerate, and optimize the way enterprises and software companies do business. With expertise across healthcare, retail, media, financial services, software, and more, we implement end-to-end solutions to deliver the innovation, quality, and speed that our clients' users expect.

SoftServe delivers open innovation—from generating compelling new ideas, to developing and implementing transformational products and services.

Our work and client experience are built on a foundation of empathetic, human-focused design that ensures continuity from concept to release.

We empower enterprises and software companies to (re)identify differentiation, accelerate solution development, and vigorously compete in today's digital economy—No matter where you are in your journey.

Visit our **website**, **blog**, **Facebook**, **Twitter**, and **LinkedIn** pages.


**USA HQ**

201 W 5th Street, Suite 1550
Austin, TX 75703
+1 866 687 3588

**EUROPEAN HQ**

One Canada Square
Canary Wharf
London E14 5AB
+44 (0) 800 302 9436

info@softserveinc.com
www.softserveinc.com


softserve