# Positive Technologies secures the digital future of leading MENA insurance group

**Background**

Founded in 1964, Qatar's first domestic insurance provider has evolved into a cornerstone of the Middle East and North Africa (MENA) region's financial universe. From safeguarding critical industries like energy, marine, aviation, and health to delivering tailored insurance solutions, the company has built a reputation as a trusted partner in region.

As part of its forward-looking vision, the insurer has embraced digital transformation, rolling out online platforms and mobile applications to streamline services and enhance customer experiences. Yet, this leap into the digital age comes with a double-edged sword: the other side a heightened exposure to an ever-growing threat of cyberattacks.

In the MENA region, financial services and insurance firms are under siege, with **43% of cyberattacks targeting financial institutions** and ransomware incidents surging **30% over the past year alone**. For insurers, the stakes are especially high. Handling vast amounts of sensitive data and relying on interconnected systems makes them prime targets for breaches, fraud, and operational disruption. For this company, securing its digital infrastructure wasn't just a precaution—it was a business-critical necessity to safeguard customer trust and ensure resilience in the face of evolving threats.

**Challenge**

As the company prepared to launch a new suite of digital applications, it faced the critical challenge of identifying and addressing vulnerabilities in its application code before deployment. Weaknesses such as outdated frameworks, insecure APIs, and insufficient encryption posed serious risks. These flaws could lead to data breaches, financial fraud, or reputational damage. In an environment where cybercriminals continuously evolve their tactics, even a single oversight could have devastating consequences.

The complexity of modern insurance operations further heightened the stakes. Digital applications must integrate seamlessly with legacy systems to maintain efficiency, but this interconnection also broadens the attack surface. A breach could expose sensitive customer data or disrupt financial transactions, eroding trust and stability. With financial

institutions in the MENA region among the top targets for cyberattacks, the insurer urgently needed a thorough cybersecurity assessment to address these vulnerabilities.

**Solution**

Faced with these challenges, the insurer turned to **Positive Technologies**, a global leader in cybersecurity trusted by more than **4,000 organizations**. Known for its **expertise in vulnerability management and penetration testing**, Positive Technologies was well-prepared to deliver a comprehensive cybersecurity assessment tailored to the unique demands of the insurance group.

The assessment began with advanced instrumental scanning and web application security tests designed to uncover vulnerabilities across the company's systems. Positive Technologies used a **black-box testing methodology to mimic real-world cyberattacks**, identifying potential weak points in the application infrastructure. This process revealed how attackers might exploit vulnerabilities such as **SQL injection, cross-site scripting (XSS)**, and **misconfigured access controls**.

Beyond detecting code-level flaws, the assessment delved deeper into the security of APIs, encryption protocols, and the integration points between the insurer's applications and legacy systems. These areas represented some of the most significant risks. Studies have shown that **APIs are responsible for the vast majority of application-related security incidents** in the financial sector. By focusing on these high-risk areas, Positive Technologies helped the insurer fortify its applications and ensure resilience against even the most sophisticated threats.

**Outcome**

The assessment uncovered critical weaknesses that could have left the insurer exposed, including **outdated libraries**, **weak authentication protocols**, and **insecure API configurations**. Armed with this information, Positive Technologies worked hand-in-hand with the insurer to implement targeted fixes. Security patches were applied, encryption standards were bolstered, and access controls were tightened. These actions didn't just plug the gaps—they significantly reduced the company's risk exposure in areas most vulnerable to modern cyberattacks.

For the insurer, the transformation was immediate. Applications that once carried hidden risks were now fortified and ready for deployment, offering the company a newfound confidence in its ability to withstand emerging threats. Identifying and eliminating vulnerabilities early in the development process also saved valuable time and

resources, avoiding the chaos of last-minute fixes and costly delays. Even more importantly, the insights gained from the assessment have reshaped the company's cybersecurity strategy, ensuring that every future digital initiative is built on an unshakable foundation of security.

**Conclusion**

Positive Technologies helped the insurance group go beyond addressing vulnerabilities by equipping them to face down with confidence the growing cybersecurity challenges of the MENA region. Through identifying and remediating risks unique to the insurance sector, the company safeguarded sensitive customer data and bolstered its reputation as a secure and innovative service provider.

This partnership highlights the impact of taking a proactive approach to cybersecurity. As cyberthreats become increasingly sophisticated, collaborations like this offer a critical advantage for organizations undergoing digital transformation. For the insurance group, the work with Positive Technologies was not just about resolving immediate issues. It marked a pivotal step toward embracing a secure and confident digital future, with systems fortified and customer trust firmly intact.