CASE STUDY

SYSTEMSOFT TECHNOLOGIES™

Cyber Security Assessment

STATE DEPARTMENT OF HEALTH AND HUMAN SERVICES

Nowadays, volatile and dynamic threats and changing regulations are real for organizations doing business. For many, it's challenging to keep the security of your IT tools updated and controls properly configured.

What works best is striking the right balance between security and compliance with progress. You can do this by evaluating the risk and vulnerabilities of your IT infrastructure.

Ultimately, you want to stay secure and compliant, while lowering your risk profile. That way, you can focus on higher value-added activities to grow your organization.

Here's a case study about how an organization in the healthcare industry successfully evaluated its network, applications and overall security posture.

Situation

To meet healthcare privacy and security standards regulated by the Affordable Care Act (ACA), a state-sponsored administrative entity of the Department of Health and Human Services (DHHS) required Minimum Acceptable Risk Standards for Exchanges (MARS-E) compliance of its provider portal. Doing so ensures the confidentiality and integrity of protected health information (PHI) and personally identifiable information (PII) of patients. System Soft Technologies was selected as an independent, third-party assessment team, because of its expertise and certifications with U.S. and State DHHS' privacy and security policies and procedures.

Strategy

System Soft's team of advanced IT-certified security experts helped in the implementation of the following certifications for vulnerability testing:

- Certified Information Systems Security Professional (CISSP) for a broader view of network and application security
- Certified Information Systems Auditor (CISA) for ensuring and validating compliance requirements
- Certified Common Security Framework Practitioner (CCSFP) for providing best practices and remediation techniques for vulnerabilities
- Certified Ethical Hacker (CEH) for system and application vulnerabilities, testing against threat actors and cyber criminals
- Offensive Security Certified Professional (OSCP) for best practices in vulnerability testing

In addition to advanced IT certifications, System Soft conducted infrastructure penetration (PEN) testing and security testing of web applications and used its custom, proprietary security tools (developed in Python) to find various web vulnerabilities.

System Soft followed a strict seven-stage process based on National Institute of Standards and Technology (NIST) guidelines, which allows for a measurable, repeatable and defensible processes. These included:

1. Identifying the existing state of security.
2. Carrying out comprehensive assessments per the industry-leading compliance standard.

3. Performing vulnerability and web penetration (PEN) testing across infrastructure and web applications to identify gaps.
4. Reviewing high-level system architecture and design to identify gaps and provide recommendations to improve the overall security posture of the program.
5. Finding gaps in IT security governance and assessment of patching methods.
6. Communicating the technical security assessment findings and aligning with the business impact.
7. Providing a plan of action and milestone guidance for gaps remediation.

Outcome

Through advanced IT assessments based on NIST security controls and guidance, along with customized controls based on the client's business needs, System Soft assisted the state government entity to identify security gaps, associated risks and infrastructure weaknesses, as well as mitigate information security threats.

Remediation guidance was also provided to close security gaps during a two-month period. This helped the state-sponsored administrative entity for the DHHS to achieve compliance ahead of schedule and adhere to MARS-E approved control implementation.

To ensure continued protection from vulnerabilities and threats, System Soft provided assessment reports and documentation for ongoing maintenance and steps for periodic self-assessments.

Conclusion

When considering a third party security provider, it is important to look for a company with end-to-end security services and solutions and trusted advisors who can help you navigate the ever-changing cybersecurity landscape to ensure you have maximum threat protection and comply with regulatory requirements.

If you have questions about enhancing your security posture and achieving compliance, contact **System Soft** today.

Discover More about our solutions and services.