softScheck

Thinking Security beyond Penetration Testing

As the threat landscape evolves, every organization needs to constantly review, evaluate, and manage the impact of these new risks. In line with this requisite, softScheck developed its security testing process (sSTP) in order to enable organizations to identify security loopholes, thereby prevent their systems from an attack (exploit) and avoid the occurrence of similar confrontations. Since its inception in 2001 as a security research Information Security Institute, softScheck has always been a research-driven security testing company with one goal: promotion of software security from inception to completion and in compliance with recognized industry guidelines such as ISO27034 & Microsoft Security Dev. Lifecycle.

Prof. Dr. Hartmut Pohl, CEO

Besides classical penetration testing offered by the ISO 27034-based Security Testing Process, softScheck also provides ISO 2700x, German IT security baseline, along with OWASP, CWE, SANS, NIST, PTES, OSSTMM and such other best practices of various security assessments. The company is also a proud audit partner for the security testing certification of TÜV Saarland and DEKRA, both Germany-based, global testing, certification, inspection, and training providers.

While every organization continues to lament about attacks on IT systems, little has been done to eliminate the vulnerabilities that are exploited to set an attack in motion. softScheck's core competency lies in providing a comprehensive Security Testing as a Service that is mapped directly from the softScheck sSTP, securing everything from software, firmware, apps and systems, to networks, servers, blockchains, and smart contracts.

The process involves security by design, which implies providing a security architecture review of the software and network system. Moreover, threat modeling involves identification of potential vulnerability of the system architecture. This is followed by Static Source Code Analysis that implies the static identification of vulnerabilities on source code level. A combination of a manual and an automatic solution, Static Source Code Analysis focuses on finding errors in authentication, authorization, security configuration, and session management along with logging, data validation, error handling, and encryption of data.

softScheck's Penetration Testing involves an authorized simulated attack on a computer system, which is performed to evaluate the level of security of the system. This test is performed in order to identify the vulnerabilities as well as the strengths of the system. The company's penetration testing process also includes the potential for unauthorized parties to gain access to the system's features and data, as well as strengths, enabling a full risk assessment to be completed. From a fuzz testing standpoint, softScheck's Fuzzing encompasses a dynamic analysis that emphasizes testing the executable, compiled programming code, eliminating the need for a source code(Black Box). "softScheck uses around 50 fuzzing tools as per requirement for the smooth functioning of the process from more than 300 tools, which are effective in diagnosing different vulnerabilities," says Prof. Dr. Hartmut Pohl, CEO, softScheck.

softScheck takes pride in their Red Team Services, which does not limit itself to the scope allowed by the conventional penetration test. Besides focusing on the core features of the testing process, the team also addresses the drawbacks arising from the same. The major objective of a Red Team Assessment is not just to identify vulnerabilities in the security system; it also assesses the client organization's detection and response capabilities. Through wireless methods, external methods, and social engineering, the team gleans sensitive information in the most dexterous way possible and emulates malicious elements such as Advanced Persistent Threat (APT), which try to avoid detection. softScheck prescribes a Red Team Assessment only to organizations with mature security programs."With our Red Team as a service, the security maturity of an organization will further be tested to reach its highest maturity," extols Pohl.

With an aim to extenuate malicious threats from the security landscape, softScheck is currently focusing on the advancement of their products and disseminating them among their target audience. ACO