swisspentest

Continuously 24/7 Risk Monitoring for Web- and Network applications

With several hundred fully automated security tests, the swisspentest platform offers comprehensive vulnerability detection for web applications. By continuously simulating attacks on a target, the scanning engine quickly and easily detects misconfigurations, vulnerable libraries and incorrect infrastructure hardening protocols.

The platform is available as an isolated container (SaaS) or containerized on Kubernetes (on-premise). By cloning a target efficiently and using a deep learning module to reduce false positives the best possible precision is achieved.

Key Features

International Standards

To provide accurate vulnerability analysis, the security scans were developed compliant with the OWASP Testing Guide and reports are generated according to Mitre A&ttack, CWE and CVSS standards. Popular vulnerabilities also get listed with their respective CVE identifier.

Infection Detection

Through a technological partnership with SWITCH, pattern matching can be used to quickly and effectively detect infections on a web application and prevent SEO poisoning or website defacements.

Portal

Monitored assets and scanning options can be administered via the central user interface of the swisspentest platform. In addition, all found vulnerabilities and legal risks are displayed with detailed descriptions and precise technical details. In addition, an extensive network topology map of registered assets is compiled and visualized.

The portal's comprehensive toolbox extends its functions to the areas of web usability and offers further useful web insights.

Use Cases

Current safety level at a glance

The clear presentation of the test results in diagrams and statistics enables an optimal assessment of the current security level of an infrastructure.

All non-intrusive security scans are performed on an infrastructure clone, which is frequently regenerated by efficient crawling of the target. This reduces the number of HTTP requests sent to a target and thus prevents overloading of the target website.

Development Life-cycle

- ✓ **Development Phase**
  With the help of the generated patch codes, security vulnerabilities can be closed quickly.
- ✓ **Test phase**
  During testing, the ***penetration test*** scanning mode can be activated, which has been built for aggressive intrusion.
- ✓ **Deployed phase**
  To ensure good usability, the scanning mode can be switched to ***vulnerability scan*** during the productive stage.

Additional features

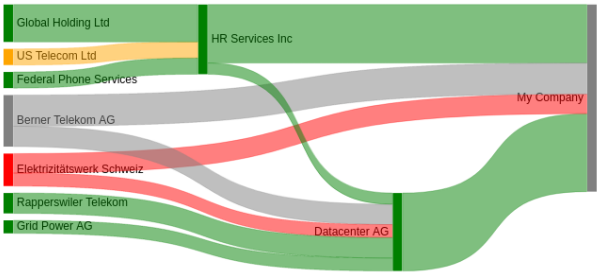
Threat Intelligence

The Threat Intelligence Engine scans the Deep Web for risks such as phishing attacks or mis-issued SSL/TLS certificates that are dangerous to your organization.

If a threat is found, an alert is issued, which can be manually analyzed and then escalated or closed.

Cyber Risk Supply Chain

With the "Cyber Risk Supply Chain" module, it is possible to record the 3rd party assets relevant for the service and to show their impact on the own company. Based on the inherited risk of identified vulnerabilities of the service provider and the exploitation impact defined for the respective service in the swisspentest, the risk can be modeled and graphically displayed.



Subcontractors of the 3rd parties can also be included as underlying resources. Risks, which normally remain hidden via a common subcontractor, thus also become visible. With the swisspentest Vulnerability Scanning Engine the cyber risk of the supplier is determined and continuously monitored. This gives you an overview of the supplier cyber risks visible on the internet at all times.

Internal Structure

Deep Learning Module

To avoid false positives, a deep learning module with TensorFlow is used.

The deep learning module consists of a modified LSTM network, which was trained using evaluated source codes of the Alexa Top 1000 and a specially developed loss function. The accuracy is further increased by using the t-SNE algorithm for feature selection.

Automated Selenium Testing

To enable the analysis of single page web apps, a Selenium Virtual Browsing module is available that crawls the event handlers of an application and indexes the requests. By establishing a proxy for the initiated traffic, all requests are accurately captured by this analysis. Found API calls are added to the attack vectors to be tested for injections or other possible manipulations.

In order to test the entire user flow process across multiple forms and not being blocked by input validators, input mappings can be used to map concrete input values to input fields.

Ticket System

Risks can be summarized via hash identifier, can be converted into a ticket and assigned to a user. The ticket is automatically closed by the scanning engine when the risk is no longer found. If it is detected again, the ticket is reopened automatically.

RESTful API

Through the comprehensive RESTful API, the scanning engines can be integrated into internal CI/CD pipelines or other applications. This integration is simplified by the available Swagger UI, through which the documentation of the RestAPI calls can be viewed and queries can be directly tested. For authentication, an API Access Token is used, which allows API access to a selected team.

Docker

Modeled as multiple microservices and Docker containerized, the kastsec platform behind the swisspentest can be deployed on premises as containers using Kubernetes or Docker Compose.

Platform Governance Mechanism

Through a comprehensive access management system, the users of each team can be individually equipped with various rights. This can protect sensitive data and ensure a separation of powers within the application.

The implemented block chain logging system ensures complete transparency by recording all user actions within the swisspentest platform. Therefore it is not possible for a user or an administrator to tamper with or delete log entries.