synera

Innovations that shape future

**Solutions for:**

- Business and corporations
- Government organizations and agencies
- IT and cybersecurity companies

# Software Vulnerability Analysis

The number of vulnerabilities identified in application software is growing every year. In order to prevent possible attacks by intruders, it is necessary to identify and eliminate these vulnerabilities in time. To effectively solve this task, SYNERA.CONSULTING recommends regular software security analysis using modern tools.

Early detection of vulnerabilities in software development saves resources (financial, time, human). SYNERA.CONSULTING recommends a comprehensive approach, including expert analysis and tools, improving the speed and quality of checks.

**Security checks are recommended for all types of off-the-shelf software, as well as libraries and embedded modules, including:**

- Desktop software
- Web applications
- System-wide software
- Open Source

Inspection tools include a variety of software suites: scanners, static and dynamic analyzers, and phasers.

Static analysis detects vulnerabilities in source code before it is executed, while dynamic analysis detects vulnerabilities in a running application related to its functioning and environment. Fuzzing testing detects errors caused by incorrect or random data.

**Step 1**
**Source Data Analysis**

- Gathering software artifacts: source code, executables, docs, and development process evidence.
- Analyzing software design, technical docs, and development process evidence.
- Creating a list of potential vulnerabilities.

**Result:**
description of the project perimeter.

**Step 2**
**Develop a study design**

- Selection and customization of security testing tools.
- Drawing up a test plan with specification of test dates and methods.
- Preparation of test environments: build and runtime.

**Result:**
a deployed research testbed and an approved work plan.

**Step 3**
**Conduct safety audits**

- Conducting security audits using expert methods.
- Conducting instrumental security checks using scanners, static and dynamic analyzers.
- Conducting fuzzing-testing.

**Result:**
a list of found vulnerabilities.

**Step 4**
**Report preparation**

- Data Analysis.
- Conclusion.
- Report with recommendations for vulnerabilities.

**Result:**
a report with a list of found vulnerabilities and recommendations for their elimination.

# Security Analysis

To create a reliable cybersecurity system, it is very important to assess the potential capabilities of attackers and verify their ability to breach the organization's defenses.

**SYNERA.CONSULTING** offers a security analysis to objectively assess the security of the existing infrastructure and provide recommendations for its modernization.

**SYNERA.CONSULTING** consultants conduct the analysis as a systematic and comprehensive project, including vulnerability analysis and assessment of information security tools. In the process, threats and vulnerabilities are identified, their potential threat is assessed, weaknesses in protection systems and software are identified, and an objective assessment of the current level of protection is made.

## The objects of analysis can be:

- Wireless networks
- External perimeter
- Internal corporate network
- Information systems
- Customer's data infrastructure
- Web applications
- Mobile applications

At the final stage of the security analysis project, consultants develop recommendations on how to eliminate the identified vulnerabilities and modernize the infrastructure.

**Step 1**
**Identify vulnerabilities**

- Survey of the organization's infrastructure.
- Gathering information from available sources about known vulnerabilities.
- Compiling a list of vulnerabilities relevant to the customer's infrastructure.

**Result:**
security analysis plan.

**Step 2**
**Security Analysis**

- Development of penetration testing scenarios.
- Conducting penetration testing.
- Determination of attack vectors considering confirmed vulnerabilities.

**Result:**
confirmation of exploitation of identified vulnerabilities.

**Step 3**
**Report and Recommen-dations**

- Compilation of the list of information infrastructure components compromised during the works.
- Preparation of a list of identified vulnerabilities that lead to the realization of unacceptable events.
- Assessing the risks of exploitation of the identified vulnerabilities.

**Result:**
analytical (for management) and technical (for specialists) reports on security assessment and recommendations for improving the information infrastructure of the organization.

# Penetration Testing (Pentest)

To ensure a resilient cybersecurity posture, assessing the potential capabilities of attackers and validating their ability to compromise an organization's defenses is paramount.

**SYNERA.CONSULTING** offers penetration testing services, conducting them as systematic and comprehensive projects that encompass vulnerability analysis and evaluation of information security tools.

> Throughout this process, we identify threats and vulnerabilities, assess their potential impact, pinpoint weaknesses in protection systems and software, and provide an objective appraisal of the current security level.

## The scope of pentesting:

- Networks
- Web & Mobile Applications
- Operating Systems
- Databases
- Physical Security
- Social Engineering
- Cloud Services

At the conclusion of the penetration testing project, our consultants formulate recommendations for mitigating the identified vulnerabilities and modernizing the infrastructure.

**Step 1**
**Information collection**

- Assessment of the organization's infrastructure.
- Collecting data from various sources regarding recognized vulnerabilities.
- Compiling a list of vulnerabilities that are specific to the customer's infrastructure, identified through scanning processes.

**Result:** a list of relevant vulnerabilities.

**Step 2**
**Verification of the vulnerability list**

- Manual verification of vulnerabilities identified during automated scans.
- Attempts to exploit identified and verified vulnerabilities.
- Manual identification of vulnerabilities and flaws in applications, including third-party components.
- Search for flaws and vulnerabilities contained in applications that enable attacks on the Customer's infrastructure and its customers.

**Result:** penetration test plan.

**Step 3**
**Conducting a pentest**

- Developing penetration testing scenarios.
- Conducting penetration testing.
- Determination of attack vectors considering confirmed vulnerabilities.

**Result:** confirmation of exploitation of identified vulnerabilities.

**Step 4**
**Report and Recommen-dations**

- Compilation of the list of information infrastructure components compromised during the works.
- Preparation of a list of identified vulnerabilities that lead to the realization of unacceptable events.
- Assessing the risks of exploitation of the identified vulnerabilities.

**Result:** analytical (for management) and technical (for specialists) reports on security assessment and recommendations for improving the information infrastructure of the organization.

# Why us?

- We reduce time and costs
- We use a flexible approach
- We bring measurable planned business results
- We guarantee fast and transparent cost calculation
- We have many years of experience

synera.global