DIGITALL

PEN TESTING

CHALLENGE

In an increasingly digital world, safeguarding critical infrastructure and protecting digital assets are paramount concerns for businesses and organizations.

Ensuring the security of these assets is not only a matter of protecting sensitive information but also of complying with regulations and safeguarding the company's reputation, thus the common questions companies ask themselves more and more are:

Is my critical infrastructure at risk?

Does my IT comply with regulations?

Are my digital assets well protected?

Is my company's proprietary data safe right now?

What would happen to my company's reputation if the company is compromised?

DIGITALL'S SOLUTION

Our wide spectrum of penetration test options across various domains, including Web, Mobile, API, Network, and more ensure that every aspect of your digital infrastructure is thoroughly evaluated in regards of security weaknesses. We offer:

Highly qualified, certified, and experienced ethical hackers who are dedicated to ensuring your digital safety.

Pre-defined packages for a quick start and predictable budgeting.

Tailor-made options that fit the level of testing that aligns with your specific requirements and risk tolerance.

DIGITALL

WHAT YOU GET

Detailed report on discovered vulnerabilities and security hardening recommendation:
- Executive summary
- High-level risk details
- Summary of findings
- Detailed technical information
- Classification of vulnerability
- Name of vulnerability
- Discovery information
- Threat & impact
- Affected software
- Evidence of vulnerability
- Conclusion & mitigation recommendations

KEY BENEFITS

- Risk awareness
- Compliance
- Reveal hidden and unknown vulnerabilities and flaws
- Increased cyber security maturity level

WHY DIGITALL

- Highly trained ethical hackers
- Various security certifications at company and team level
- Experienced cyber security team of 60+ experts
- 360 degrees IT company with holistic expertise in secured digitalization
- Proven methodology – OWASP, NIST SP 800-115, ISSAF

DIGITALL

PEN TESTING PACKAGES

WEB APPLICATION PENETRATION TEST

Websites and online portals are some of the most exposed public internet resources companies have nowadays. Testing them for security issues through our Web Application Penetration Testing service ensures that the applications are resilient, or at least, that companies know where potential weaknesses are, so they can work on fixing them. We believe in the strength of engineering and science and use the OWASP framework as a basis for our tests, enriching them with additional attack types.

WHAT WE DO

- Information gathering
- Configuration and deployment management testing
- Identity management testing
- Authentication testing
- Authorization testing

- Session management testing
- Input data validation testing
- Error handling
- Cryptography
- Business logic testing
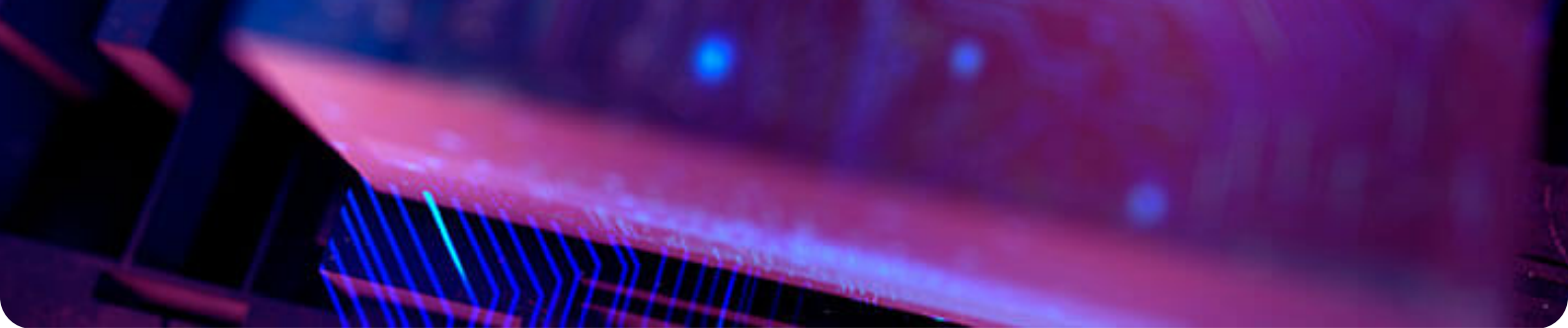- Client-side testing

SCOPE

1 x Web application

penetration test including external network penetration test & retest

10 DAYS

ONE-SIZE-FITS-ALL

MOBILE APPLICATION PENETRATION TEST

Mobile applications are the most dynamically developing apps and it doesn't look like this will change soon. We help businesses ensure that their mobile apps are secured by conducting a comprehensive assessment of all their components. All areas of security considerations are based on an industry-recognized best practice and standard – OWASP Mobile AppSec Verification Standard (MASVS).

WHAT WE DO

- Configuration analysis
- Analysis of static changes
- Discovery of third-party vulnerabilities
- Dynamic analysis
- Behavioral analysis
- Vulnerabilities detection
- Backend vulnerability analysis

SCOPE

1 x iOS and Android
mobile application penetration test & retest

5 DAYS

ONE-SIZE-FITS-ALL

API PENETRATION TEST

In today's interconnected digital landscape, APIs play vital role in data exchange and functionality between applications. However, they also pose significant security risks if not properly tested and secured. Our API penetration testing service ensures that your APIs are hardened and respectively your data and systems are protected from potential threats.

WHAT WE DO

- Authentication and Authorization Testing
- Input Validation and Data Integrity Checks
- Security Configuration Review
- Testing for Authorization Bypass
- Sensitive Data Exposure Checks
- API Rate Limiting and Throttling
- Business Logic Testing
- Error Handling and Exception Testing
- Security Misconfiguration Assessment
- API Documentation and Endpoint Analysis

SCOPE

1 x API
endpoint penetration test & retest

8 DAYS

ONE-SIZE-FITS-ALL

DIGITALL

INTERNAL PENETRATION TEST

Internal Penetration Testing helps to identify how far an attacker can move laterally through a network once an external breach has occurred or - based on their internal access - what is within reach. We use a cycled approach with testing, identification, documentation, retesting and final reporting for maximum efficiency.

WHAT WE DO

- Information gathering
- Identification of security mechanisms
- Identification of services
- Exploitation of vulnerable services
- DNS configuration and NW scanning
- Network sniffing
- Social engineering

SCOPE S
UP TO 50 HOSTS AND 5 NW
segments test & retest

5 DAYS

SMALL

SCOPE M
UP TO 500 HOSTS AND 20 NW
segments test & retest

15 DAYS

MEDIUM

SCOPE L
UP TO 1000 HOSTS AND 50 NW
segments test & retest

20 DAYS

LARGE