Solutionlab 

Solutionlab 

Solutionlab shall provide you with access to a highly skilled team of consultants with significant experience in penetration testing. Solutionlab's team who has experience of working with a large number of security aware, international customers in many different fields. Our extensive international experience, as well as our strong presence in Eastern Europe gives us first-hand access to emerging information and trends concerning actual and upcoming threats.

Our wide range/types of penetration tests services, security assessments combined with our risk mitigation consultancy services, ensure that the needs of you will be fully covered.

- Vulnerability Assessment and Penetration Testing (VAPT)
  - Web application penetration test
  - Mobile application penetration test
  - Network penetration test
  - Compiled Application Penetration Test
  - . . .
- Compliance and Governance (GRC)
- Consulting and Managed technologies
- Education – awareness training

Solutionlab

Vulnerability Assessment and Penetration Testing (VAPT)

Vulnerability Assessment and Penetration Testing (VAPT) provides enterprises with a more comprehensive application evaluation than any single test alone. Using the Vulnerability Assessment and Penetration Testing (VAPT) approach gives an organization a more detailed view of the threats facing its applications, enabling the business to better protect its systems and data from malicious attacks. Vulnerabilities can be found in applications from third-party vendors and internally made software, but most of these flaws are easily fixed once found. Using a VAPT provider enables IT security teams to focus on mitigating critical vulnerabilities, while the VAPT provider continues to discover and classify vulnerabilities.

Industry leading tools provide automated discovery to uncover the potential vulnerabilities in your network and web applications	Assessment of your organization's exposure to vulnerabilities	Measurement of the risk and potential risk associated with the discovered vulnerabilities	In-depth report of the discovered vulnerabilities, along with remediation recommendations

Outcome: Better transparency and increased awareness of potential vulnerabilities and risks to the business

Reconnaissance of customer network and applications, mimicking the techniques used by an attacker	Assessment and identification of potential vulnerabilities are collected	Discovered vulnerabilities are measured and then exploited using real-world tools and techniques	In-depth report on the discovered vulnerabilities and which were successfully exploited, along with remediation recommendations

Outcome: Better transparency into potential threats and reduced effort by knowing which vulnerabilities can be exploited

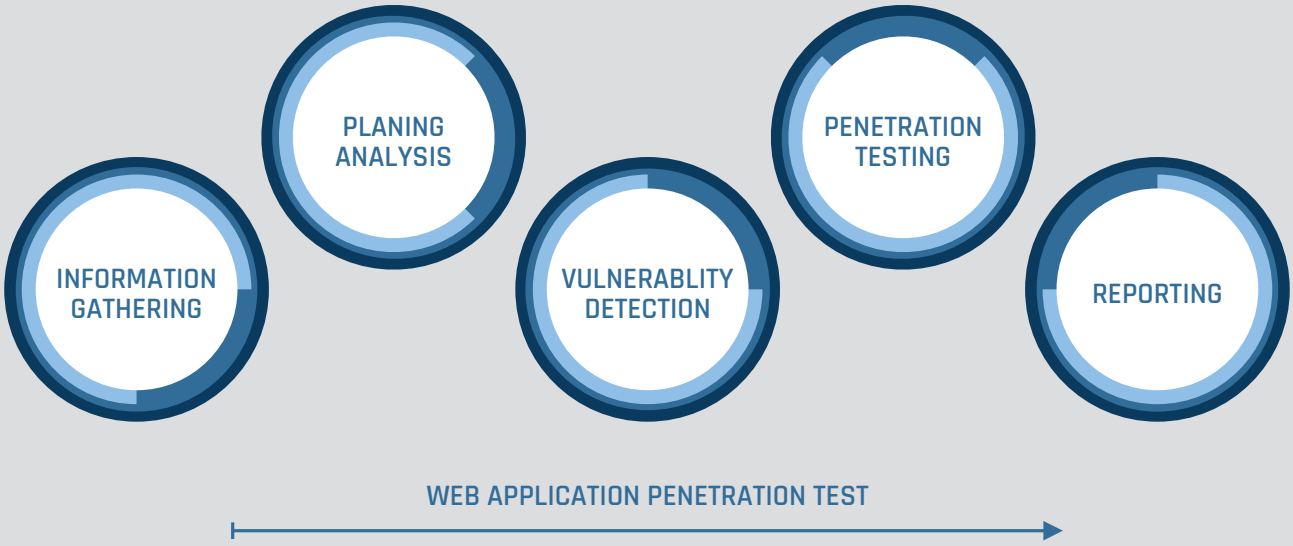
Solutionlab

Web application penetration test

Web applications are very common and omnipresent. They range from very simple static repositories to massive, complex, and dynamic structures, merging various technologies and information processing principles. Being Internet-exposed at the crossroads between users, technology platforms and backend database systems, modern web applications are susceptible to numerous attacks and need to be protected.

A security assessment will ensure that applications are secure in handling sensitive data, and do not allow unauthorised access to themselves or to their backend servers.

Our tests are geared towards finding issues within the applications, and educating developers to design and implement secure applications. The final report of the test that we deliver contains detailed recommendations to help developers patch the issues identified during the test. Where an issue cannot be immediately rectified, mitigation strategies will be presented, depending on the environment where the application is implemented.



Solutionlab

Mobile application penetration test

Mobile applications are becoming more and more popular as users expect to access services on demand through mobile platforms and devices. They now offer the power and functionality of traditional client computers, and are therefore susceptible to many of the associated risks, as well as new risks unique to these devices.

A security assessment will ensure that applications are secure in handling sensitive data, and do not allow unauthorised access to backend servers.

Our tests are geared towards finding issues within the application and educating developers to design and implement secure applications. The final report will contain detailed recommendations to help developers patch the issues identified during the testing. Where an issue cannot be immediately patched, mitigation strategies will be presented, depending on the environment where the application is implemented.

Solutionlab

Network penetration test

Penetration testing is an essential component for proving the potency of an organization's information security program. External & Internal comprises a security test from the Internet and from the internal network, whereby our security consultants test the security of the network with a view to identifying security issues that can be exploited by external and internal hackers and worms giving unauthorised access.

Both tests are critical to maintaining a well-secured network, and should be performed a minimum of once per year.

With our security test based on well-proven test methodologies, we review your business-critical IT systems to identify vulnerabilities that can be exploited by malware and hackers. The test can be performed at three levels, depending on the relevance of the systems covered by the scope of the test:

Level 1: A test at Level 1 indicates whether a system can withstand random and elementary attacks, which are typically performed by malware and amateur hackers.

Level 2: A test at Level 2 indicates whether a system can withstand targeted attacks that are typically performed by skilled or persistent hackers with a specific motive for wanting to attack you. A Level 2 test always includes a Level 1 test.

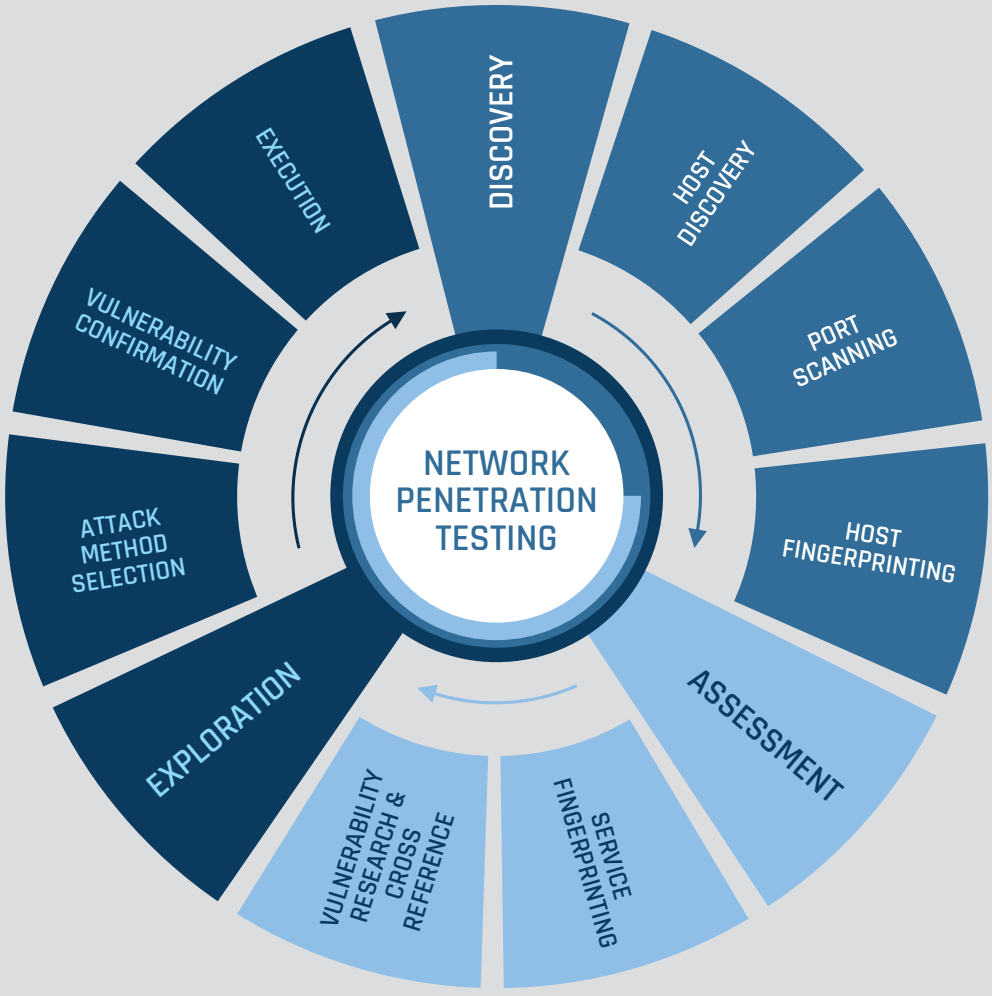
Level 3: A test at Level 3 shows whether a system can withstand targeted attacks with insider knowledge, which is typically performed by skilled or persistent hackers with detailed insight into your systems, configurations, and workflows.

In connection with our security testing, we offer a range of optional services including: inspection of firewall rules, tests of web services, security inspection of web code, and tests of payment processes on websites.

Solutionlab

We use automated tools, as well as manual and creative tests (for Level 2 and 3 tests). For the manual tests, we use our comprehensive test case database as the starting point, which contains descriptions of the latest methods hackers use to exploit vulnerabilities. As part of our testing, we test how vulnerable your systems are for Denial of Service attacks.

After the execution of the test, you will receive a security report that documents the test results and provides you with an accurate status of IT security in the systems we tested, including an indication of your level of security. The report consists of an executive summary with conclusions, and a technical review of the vulnerabilities we have identified and prioritized. The report also contains suggestions so that your employees or outside contractors can begin to address the identified vulnerabilities. We personally review the report with you.



Solutionlab

Compiled Application Penetration Test

Examines non-web-based software from the same perspective as an attacker – without access to the source code, but with all the tools which an attacker will use to discover and exploit the flaws in your application. It is based on a high-level methodology which is iterative, with a focus on analysing and understanding the target from a business perspective before any attacks are planned and executed.

One of the main differences from many other penetration tests is that the big picture is considered, and relevant considerations, such as how attackers may disrupt a business by targeting its brand, are included where this makes sense. It incorporates deep intelligence gathering from public sources as one of its main components. The information gathered as part of it is analysed and used to plan and execute targeted attacks. These are prioritized according to security risk areas and critical assets of the business that is being tested in order to maintain a relevant test focus from a business perspective.

Solutionlab

Network Device Security and Configuration Assessment

The assessment of network devices and server configuration in the network segment, configuration of network equipment and security tools supporting is the process of identifying weaknesses in security controls to ensure security comprehensiveness. This assessment is performed using administrative access to network servers and devices. The focus of this assessment is to perform a configuration and ruleset review.

On inspection of your set of firewall rules, we identify vulnerabilities which a hacker or malware may be able to exploit to penetrate your firewall. The test requires that we receive your firewall rules and a network diagram which illustrates where the firewall is placed. We then thoroughly, manually and with tools, scrutinise your firewall rules – line by line – and use our security knowledge to identify security breaches in the configuration of your firewall. The security reviews will be performed according to methodologies described in the OSSTMM testing guides, NIST Technical Guide to Information security testing and assessment, and our own methodologies based on our experience with security reviews and tests.

Solutionlab

Virtualisation Assessment

Virtualisation of your server environment has been implemented, and you are reaping the numerous benefits associated with being able to run more virtual servers on significantly fewer physical servers. You enjoy a better overview, more straightforward administration, enhanced flexibility and scalability, and a better operating economy, but have you given sufficient thought to security?

Virtual server environments are generally more dynamic than physical server environments, because of which such environments carry greater security risks in terms of accessibility, data integrity and confidentiality of information on IT systems.

We test your virtual server environment with automatic tools and by means of manual/creative tests. Through internal tests, we also can check the hardening of your systems and the patch status for the operating system and virtualisation software.

We compare the test results with best practice, based among other things, on recognised security guidelines from the National Institute of Standards and Technology (NIST). We then document the test results in a report which is personally presented to you. The report contains general recommendations for remedying any security issues discovered in the server environment.

Solutionlab

Remote Access Assessment

A review of the VPN/RAS endpoints is done to ensure that they are configured in line with industry best practices, and have been securely deployed. We advise to do a comprehensive VPN assessment that looks at all possible attack vectors. When we perform a thorough VPN assessment, it is critical that we can review the network.

Penetration testing of a VPN is rather straightforward, and regardless of the type of VPN, there are some steps we will perform:

1. Scan open ports and fingerprinting.
2. Exploit known vulnerabilities.
3. Operate default user accounts.

Database Assessment

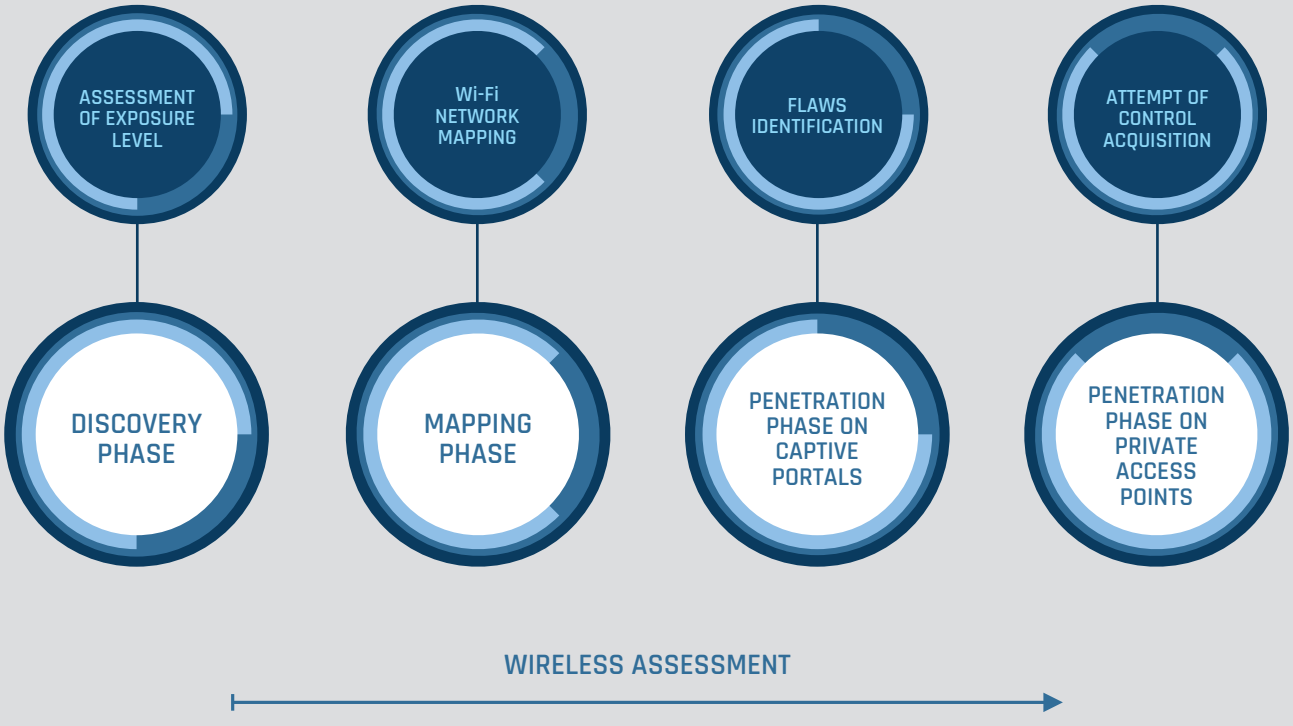
A full review will be undertaken of the database structure, user privileges, patching policy, and configuration leading to a formal report with recommendations for mitigating any vulnerabilities found.

Solutionlab

Wireless Assessment

Many companies increasingly make use of wireless networks to the benefit of both their employees and eventual guests that will need an internet connection. A relevant question arises however. Is the wireless network sufficiently secured against hacker attacks at the same level that the company has secured its wired network?

A hacker does not have to be physically located in your company to hack into your wireless network and from there further into your internal network with confidential data. Everything he needs is wireless equipment and a hole in your wireless security. Our team delivers straight talk about the security in your wireless network.



Solutionlab

Social Engineering

Hackers' working methods are becoming more and more sophisticated. To an increasing extent, today's hackers are professional hackers that employ a broader spectrum of methods, such as social engineering, by which the company's employees are duped into surrendering confidential information.

We test the company's employees based on different scenarios that are adapted to the needs of the company in question. For example:

Phishing attacks. Our team sends emails to employees under the pretence that they should open an attached file or click on a link. Attached files result in a malicious, though controlled code being run on the client's machine, for example: via Java, Office, PDF, etc. If the computer is not correctly patched, it may be possible to assume control of an employee's PC and use it as a steppingstone to take control of other machines on the internal network. Links are designed to get employees to log onto false websites with their username and password, or to submit confidential information concerning the IT systems. The wording of the emails we send out or the text which appears on the false websites is always tailored to the needs of the company in question.

Impersonation. We may contact employees pretending to be calling from e.g. a telemarketing bureau or the company's internal IT department's helpdesk in order to get the employee to perform specific actions and/or reveal sensitive information. There are plenty of possibilities, with the options chosen being adapted to your company's internal procedures.

Social network services. The team uses social networks such as Facebook, Twitter, and LinkedIn to obtain information about employees and the company to thereby acquire confidential data.

In-person tactics that can be used to collect information about the targeted systems to help identity attacks vectors and targets

Develop a relationship with the target

Utilizing the collected information and relationships to breakdown the target

Identifying social engineering strategies that can be utilized in cybersecurity

Solutionlab

Cloud security review

As organizations have moved more and more critical applications, workloads, and services to the cloud, we could help them review their overall cloud strategy and architecture from a best practices and security point of view. We offer security testing appropriate for all levels of complexity – from simple security reviews of cloud hosted virtual machines, to deep-dive assessments of cloud-native applications.

Solutionlab

The vulnerability assessment

The networked environment is not static – new systems are introduced, laptops come in and out of the network, new software and upgrades get installed regularly.

Regularly scanning the network environment for software vulnerabilities and abnormal activity is paramount to network security and is an important PCI objective, which requires a quarterly network scan. It ensures that network administrators keep track of activity that could introduce new exposures. Scanning often uncovers new exposures introduced by updates, new systems, new software, or other changes to the environment.

Solutionlab

Compliance and Governance (GRC)

In today's cyber security landscape, ensuring compliance and good governance is more important than ever. Our experienced and fully qualified Risk Management and Governance team will assist you in reaching and maintaining compliance to standards and regulations such as: ISO 27001, PCI DSS, GDPR, SWIFT, NIST Cybersecurity Framework, CIS Controls, EBA Guidelines on ICT and security risk management to ensure that you are in line with best practice frameworks.

Results will be presented in a business focused report where the client's current maturity level will be rated, followed by recommendations on how to reach the advised target maturity level. The report will also contain high-level findings, identification of threat actors, and likely attack scenarios. We offer the following services:

- CISO and information security team as a service
- DPO (Data Protection Officer) as a service
- Cyber Security Assessment
- PCI DSS
- SWIFT
- Corporate Governance

Solutionlab

Consulting and Managed technologies

Our consultant will provide a high-level consultancy to improve your cyber security maturity. The consultancy gives you a tangible view of where your strengths and weaknesses are, and prioritisation to address them. Additionally, you can quickly see your current and desired maturity rates – all in a format that is easily presentable to the board.

Our consultants have been instrumental in providing reasoned advice and support in delivery of technical solutions, policies and procedures, and cyber and information risk management strategies. All of these aim to reduce the risk of cyber-attacks that are faced by their business.

Our team's delivered consultancy services include global practice, and this is supported where required by the technical skillset provided by our Penetration Testing and Managed Technologies services which incorporates threat intelligence function.

With our security team, the client can get Managed Technologies Services for Network and End-Point Monitoring. By means of the Network Traffic Analyzer, we define infected workstations inside the client network, even with encrypted traffic. AI technologies / Machine Learning, which constantly adapt to a client-specific network, will detect any small deviations from normal.
For example: an employee who becomes too active outside of his normal hours, or if a system administrator has gone rogue, etc. So, with an endpoint agent, we can see even more down to the core processes on a PC, and do machine learning on that too. Therefore, we can see if any of the key parameters are unusual compared to normal activity – both in terms of time of day or week, amount of data, type of device, type of software, recipient, etc. We do also capture ALL raw data, as well as encrypted data. It is then possible to decrypt, to do deep level forensics after a cyber incident if needed.

Our team integration with cloud service providers /partners is also welcomed.

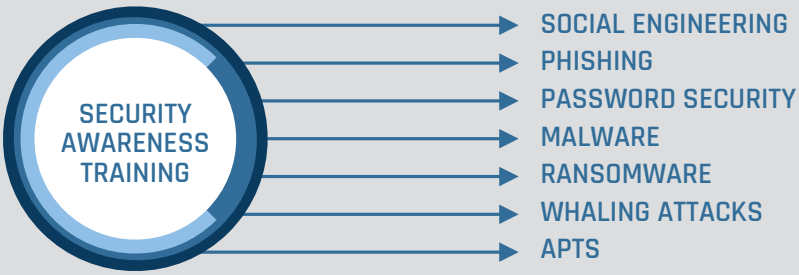
Solutionlab

Education – awareness training

We believe that a holistic and systematic approach to awareness training is the most effective solution. If the individual employee's security awareness needs to be increased, it should be seen as a cultural change throughout the organisation. For this to succeed, a focused and systematic effort is required.

We offer awareness training on several levels ranging from an entire course based on your specific business goals and desires, as well as training that is specifically adapted to various employee groups within your company, to a single presentation where we meet with management or employees, and talk about the current threat landscape, based on your specific industry. We offer the following awareness solutions:

- Cybersecurity awareness training
- GDPR training
- Training for Developers
- PCI DSS Training



Solutionlab 

Contact our security advisory team on **sec@solutionlab.net**