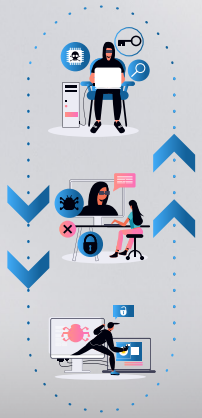

SAGA
new frontier group
GETTING CYBER SECURE WITH
PENETRATION TESTING SERVICE
Security
Operation
Service

The world is evolving, making information the most asset of today's businesses. Safeguarding it is becoming main goal for any organization. It's a key task of a good practice commonly called Cybersecurity - the practice of protecting networks, programs, systems and data from malicious attacks. The exponential growth of data, devices, processing power, algorithms, and networked systems, valuable assets for any business competing in the 21st century, comes with newer risks and vulnerabilities. Citing data security, infrastructure protection and cloud security as the fastest-growing areas of security spending. Organizations have many more challenges. These range from meeting statutory, contractual requirements, lack of control over operations by virtue of outsourcing /cloud services, poor visibility into value generated by the deployed security solutions etc.

„Hacks and data thefts, enabled by weak security, cover-ups or avoidable mistakes have cost companies a totalof nearly $4.4 billion and counting for The 12 biggest data breach fines, penalties, and settlements so far.Sizable fines assessed for data breaches since 2019 suggest that regulators are getting more serious about organizations that don't properly protect consumer data. Marriott was hit with a $124 million fine, later reduced, while Equifax agreed to pay a minimum of $575 million for its 2017 breach. Now, the Equifax fine has been eclipsed by the $1.19 billion fine levied against he Chinese firm Didi Global for violating that nation's data protection laws, and by the $877 million fine against Amazon last year for running afoul of the General Data Protection Regulation (GDPR) in Europe."



Today, there are more devices than people, and attackers are becoming more sophisticated and innovative. Common cyber-attacks are becoming cheap to conduct, inventiveness of the attackers almost has no limits. What's to gain for the attackers from cyber-attacks? Access to sensitive information or interrupting normal business processes.

Having a strong cybersecurity strategy offers a clear, detailed plan that standardizes security across an organization. It all starts with assessing your current security measures to help you better understand your current environment. That's why a strong cybersecurity approach is critical to defend against cybercrime.

SAGA
new frontier group

Moreover, governmental laws, applicable regulatory & compliance are to be strictly followed as per regulators are no more threatening but rather defining high priced fines and penalties for consumer data breaches:

According to Gartner, the impact of pandemic and the rapid acceleration of digital initiatives in a short time, forced organizations to control and manage disruptions to their business. As security and risk management leaders handle the recovery and renewal phases from the past two years, they must consider forward-looking strategic planning assumptions when allocating resources and selecting products and prioritizing services and initiatives. How do security and risk management leaders keep pace with the future of digital in a post-pandemic scenario?

Cybersecurity is now the number-one spend item on the technology investment list. In 2022, 88% of boards say cybersecurity is a business issue, not a technical one.

CIOs and senior IT executives must be able to communicate the risks, value and cost of cybersecurity to their board of directors. Boards want metrics, measurement and governance that will help protect against ransomware and other threats. Cybersecurity leaders require more versatile skills as security shifts from a technology-focused to a business-focused discipline. Communicating and influencing key stakeholders across the organization are key attributes in ensuring the success of a defensible security program.

Understanding your current state is a key path to improving security posture. How are you exposed? What and where are technological threats and risks? Are your technologies up to date? Are your security solutions and architecture providing proprietary defense whilst being effective as they should be? Where are the gaps or weaknesses that could leave you vulnerable? We can help you with the much-needed insight into the security stance of deployed technologies with a complete technical risk assessment, security scan and architecture review specific to the threat profile of your technology and market.

SAGA
new frontier group

SERVICE OVERVIEW

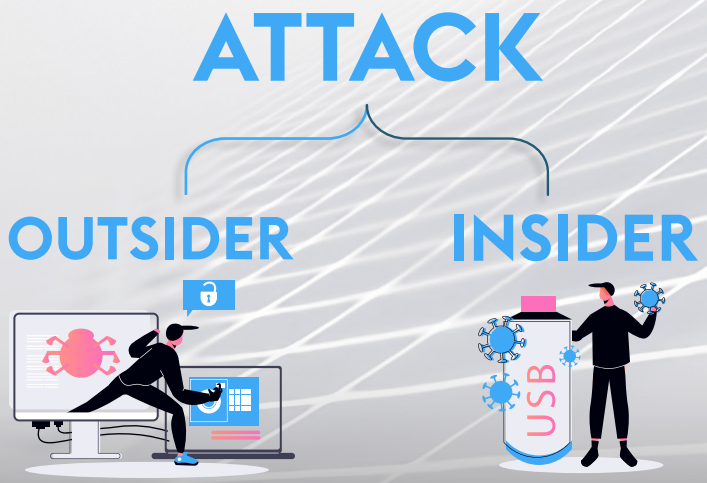
"A method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might."

https://www.ncsc.gov.uk/guidance/penetration-testing

Penetration testing service, (also called pen testing or ethical hacking), provides a systematic process of "real life" test of an exposure to known security vulnerabilities. It determines the extent to which it is susceptible to external / internal attacks. Penetration testing should be viewed as a method for gaining assurance in your organization's vulnerability assessment and management processes, not as a primary method for identifying vulnerabilities.

This type of security testing represents an efficient and tangible assessment of the security of information assets, communications, and control infrastructure. It focuses on network, application and system vulnerabilities an unauthorized user could exploit from inside and outside of the organization with varying levels of access and information.

Attack scenarios include the ability to view, steal, corrupt, modify, deny access to, or destroy corporate information assets as an "Outsider" with no knowledge of client's operations and as an "Insider" (employee, consultant, or business partner). Qualified pen testers perform automated and manual penetration tests, using proven techniques, methodologies, and tools to detect undesirable risk conditions.



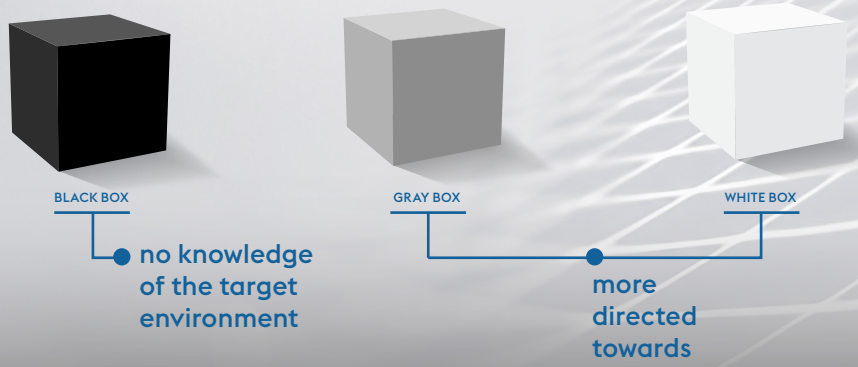
SAGA
new frontier group

A highly evolved and structured approach of penetration testing services is needed to examine the security functionality of systems within the scope of testing. All analysis are aimed to be conducted in non-disruptive manner in most cases to the organization, providing valuable insights on its security posture.

Depending on the depth of testing warranted and agreed by the organization, penetration testing service is delivered in many flavors in meeting their contractual, regulatory, or corporate governance requirements. It can be performed either from an external perspective (outsider's view) which involves analysis of publicly available information as a typical attacker would do. On the other hand, penetration testing from internal perspective tries to exploit vulnerabilities with privileges assigned to typical users of the environment.

The penetration testing can be further categorized into black box, gray box or white box depending on the purpose of the testing. Black box testing is performed with absolutely no knowledge of the target environment. Black box testing performed from an external perspective can provide the closest results to that of a real life hack attempt. It also provides very deep insight into the true security stance of the client. Gray and white box tests are more directed towards specific targets with either partial or full knowledge of the target and the environment in which it is working in.

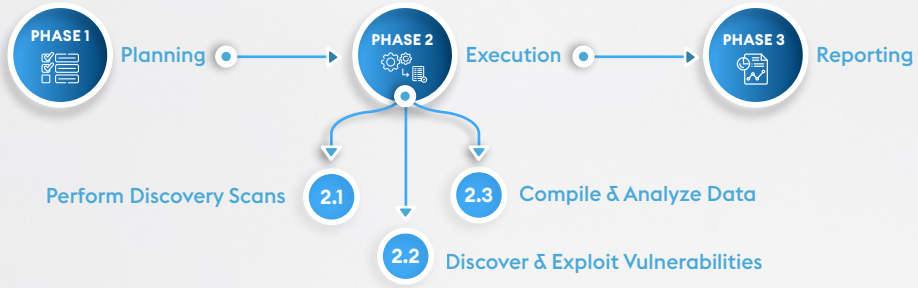
PENETRATION TESTING



SAGA
new frontier group

APPROACH & METHODOLOGY

In our approach conduct security assessments utilizing our SAVE methodology. The SAVE methodology is based on industry regarded best practices and standards to ensure each engagement is performed in an efficient, consistent, and thorough manner.



1 PLANNING

The planning phase of the penetration testing project is designed to define the boundaries of the project, define tasks involved in the project, the resources and time required, and project schedule for the engagement team. The methodology determines high-level scope during initial planning. This initial scope statement identifies deliverables required to meet the goals and objectives. It also defines the logical boundaries and baselines in terms of a baseline model (logical scope). Once the project starts, the methodology confirms initial scope and refines it to specify its remaining dimensions.

2 EXECUTION

The actual assessment of the target environment will take place in this phase of the project. The execution phase is split into multiple sub phases each of which is explained in sections below. The combination of tools and techniques which greatly depend on the scope of the project and the type/category of testing chosen by the client.

Phase 2.1 – Perform Discovery Scans

The goal of the discovery scanning stage is to gain as much information as possible about the target environment. The discovery scan will be carried out before any automated tools or manual hacking techniques are used. Efforts will be made to discover

mated tools or manual hacking techniques are used. Efforts will be made to discover and enumerate the following information at a minimum:
- All possible information about the target organization such as its subsidiaries/parent company, locations, key stakeholders etc
- Technical information such as DNS servers, MX handlers and any other information available publicly
- Range of IP addresses, IP addressing schemes, internal network segments and maps, Privileged user details etc

Phase 2.2 – Discover & Exploit Vulnerabilities
A host of tools and techniques will be employed at this stage to discover the vulnerabilities within the target environment. The information obtained in the preceding stage will be crucial to the success of this stage. Once the discovery of vulnerabilities concludes, attempts will be made to exploit the same using additional tools and techniques. This will be done in a manner that the exercise provides a “real life” test of the security posture of the organization.

Phase 2.3 – Compile & Analyze Data
The completion of the Exploit stage provides the data needed to create the final report and recommendations. All data which was obtained will now be sorted and initial recommendations drafted. The results of the Exploit phase need to be summarized and categorized. Technical recommendations result from weaknesses in system configurations and settings. Procedural recommendations result from the administrations of systems, over all architecture and policy. These two types of recommendations need to be defined. Enterprise-wide recommendations will be developed based on patterns of findings resulting from the detailed recommendations.

REPORTING

The final reports which will be the deliverables of the project will be submitted to the organization and this will also act as a concluding step. The deliverables need to go through a co-development effort with the client before they are submitted. The reports will summarize the detailed recommendations developed in the preceding stages and present management with a report documenting the overall security weaknesses in the organization. The report will be the final deliverable to the client.

KEY BENEFITS

What should a penetration testing report tell you? We are certain of one thing as conclusion – Pen Testing should become an undetachable part of organizations security culture. Reducing the cyber-attack surface is essential in discovering security gaps and closing them off before opportunistic threat actors find a way through them. By regularly conducting security testing one can be assured that solutions and protective measures provide confidence whilst staying up to date and in accordance to internal policies, laws, rules and regulations safeguarding business and continuity of processes in place. Reoccurring security testing by 3rd party experts can keep confidence in the picture that protection, controls, and compliance are on the highest level.

SAGA
new frontier group

To protect yourself, you should regularly conduct security testing to:

Ensure your existing security controls are effective.

Gain insight on inadequate or improper configurations

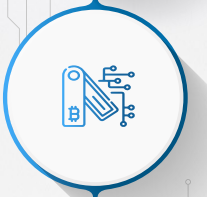
Test new software and systems for bugs; (example: identifies broken access control, with incorrect or incomplete authentication mechanisms, as the leading API exposure)

Support your organization's compliance with security and other relevant privacy laws or regulations (e.g., PCI DSS, HIPAA,GDPR)

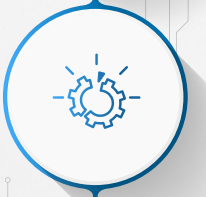
Identify apps and systems that are impossible to secure or modernize (End-of-Support / End-of Life)

In merges & acquisitions security testing can help in due diligence stage to gain more information and better insights on cyber risks

Identify security flaws so that you can resolve them or implement appropriate controls



Be aware on known and unknown hardware or software flaws



Identify operational weaknesses i n processes or technical countermeasures

Assure customers and other stakeholders that their data is being protected avoiding the hefty costs and penalties of a data breach

Have the ability to improve an organization's revenues by highlighting redundant services, inefficient processes, and so on

SAGA
new frontier group

saga.rs