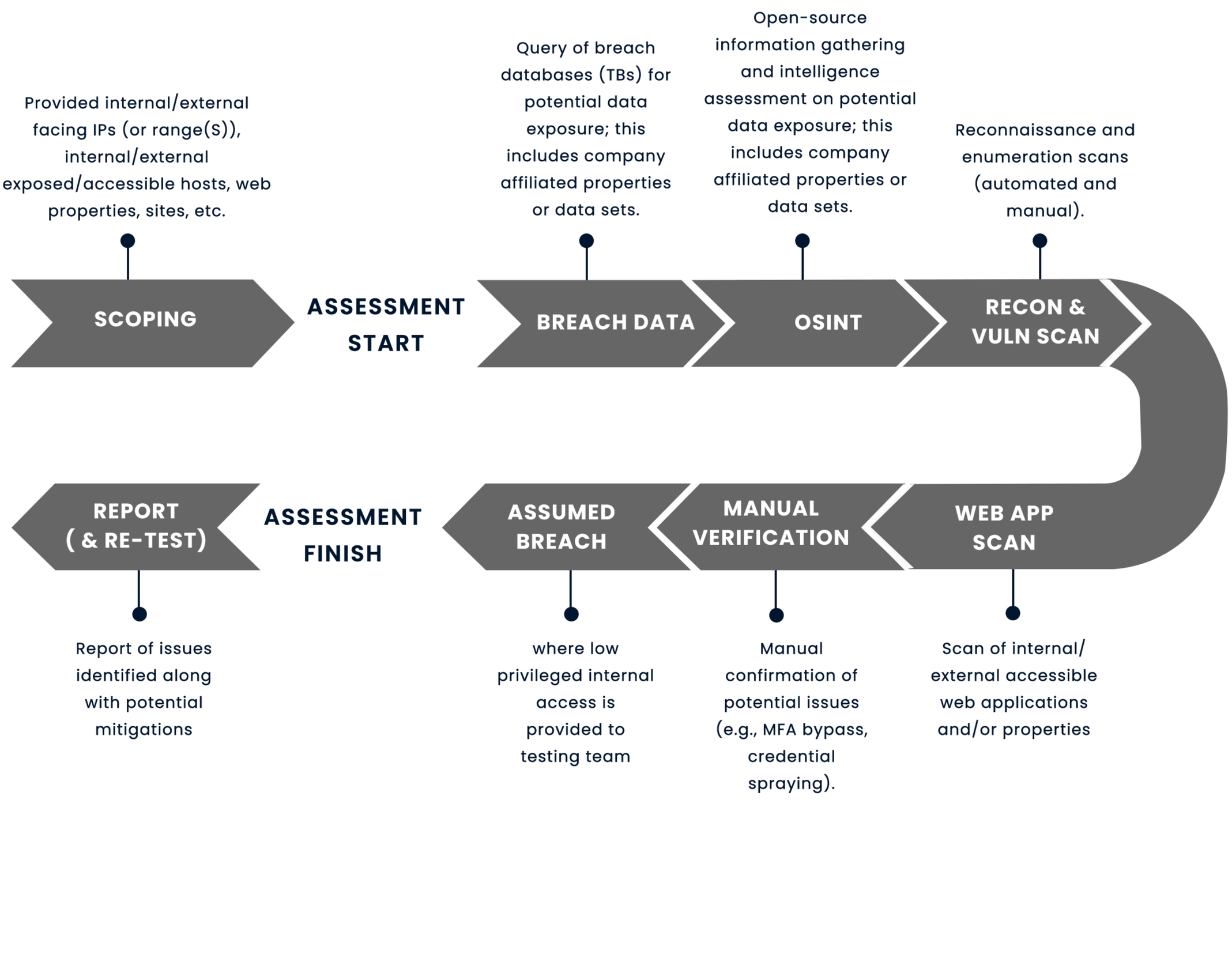
PENTESTING-AS-A-SERVICE

“Helping businesses to identify the vulnerabilities in their IT Infrastructure”

Penetration Testing, aka Pen Testing, is a simulation of a real-world cyber-attack. Penetration Testing-as-a-Service helps you discover the weaknesses in your IT infrastructure by simulating an attack on a computer system or network from external and internal threats. Bluetooth-Attacklates the me tools, know-how, and methodologies malicious hackers use. The difference between a real attack and simulation of a real-world cyber-attack is that a real attack vanishes your business within minutes. Still, Penetration Testing attacks find vulnerabilities in a controlled system, helping you discover and fix problems before an attacker does. The output is a comprehensive report identifying where to close security holes and how to improve security posture.

DO YOU KNOW?

- **363 high-risk vulnerabilities with CVSSv3 10.00** and RCE access were found in 2022
- **Fixing a critical vulnerability** took companies **193.1 days** on average in 2021(AppSec Stats Flash - Year in Review)



TYPES OF PENETRATION TESTING SERVICES

- **External Penetration Testing**

Securing internet-facing assets such as web, mail, and FTP servers is a huge concern. An attacker is always drawn to the company's assets that are accessible over the internet. Hence, knowing your perimeter weaknesses is critical before threat actors attempt to exploit them. Our external Penetration Testing helps identify vulnerabilities in internet-facing infrastructure, enumeration & exploitation.

- **Internal Penetration Testing**

Isolating and securing the assets in the internal network is another challenge for any organization. Imagine a case where the attacker somehow gets into your network or the threat actor is one of the internal members. It will not take long for him to infect the whole network and cause a MAJOR security breach. Internal Penetration Testing assists in answering the questions such as how far an attacker can infiltrate the network and what sensitive resources an attacker can access, assuming the attacker is already inside your network.

- **Wireless Penetration Testing**

The entry point for a malicious actor can be your insecure wireless networks like Wi-Fi or Bluetooth network. Wireless Penetration Testing helps identify the vulnerabilities in the wireless network that an attacker can exploit to become an uninvited guest in a network and keep an eye on all sensitive communications without revealing his presence.

- **Web Application Penetration Testing**

If an attacker successfully breaks into the web application or server, he may also gain access to sensitive information and other applications. Web Application Penetration Testing helps apply remediation against undiscovered vulnerabilities and make sure source code is as per the best practices.

- **Mobile Application Penetration Testing**

Mobile applications are increasing with the increase in the count of smart devices. However, a vulnerable mobile application may affect not only the organization but the users too. A single bug or vulnerability can cause data theft, including the user’s personal information. Our performs comprehensive mobile penetration testing to identify such security and privacy issues.

- **DoS and DDoS**

Sometimes, a threat actor attempts to crash a service or a server by sending a significant number of data packets from a single device or various devices. A good counter strategy for such attacks must be implemented in the environment. Our tests the performance of such vulnerable servers by conducting simulated Denial-of-Service (DoS)/Distributed Denial-of-Service (DDoS) to help you formulate the counter strategies and prepare you for Cyber Warfare.

- **Social Engineering Assessment**

People are the most vulnerable assets in any organization. Hence, organizations must conduct Social Engineering Assessments to test human vulnerabilities and train their employees, so they don’t fall prey to attackers. Our Social Engineering Assessment helps you test employees and associated security policies to identify the weakest link in the security strategy.

Typical Length of Engagement 1 – 4 weeks

HOW OFTEN DO YOU TEST IT INFRASTRUCTURE FOR VULNERABILITIES

It is recommended to conduct Pentesting at least twice a year to stay current with vulnerabilities and potential threats. The frequency of testing can vary depending on a number of factors, including:

- **Company size:** larger companies may require more frequent testing to ensure the security of a larger infrastructure.
- **Potential exposure to attack vectors:** companies with a higher risk of attack, such as those handling sensitive data or operating in a regulated industry, may require more frequent testing.
- **Industry:** different industries may have specific regulations or compliance requirements that require more frequent testing.
- **Infrastructure type/size:** the complexity and size of a company's IT infrastructure can also impact the frequency of testing.
- **Industry-specific regulatory environment:** Companies operating in a regulated industry, such as healthcare, finance, and government, may have specific regulatory requirements that mandate more frequent testing.

It is always a good practice to review and update the company's security posture and conduct a risk assessment to determine the most appropriate frequency of testing.

CONTACT US

CONTACT US NOW!

+1.612.532.5539 mohammed@archlightsolutions.com www.archlightsolutions.com