KG Hawes

Partners in Technology

VAPT

WWW.KGHAWES.COM | (866) 687-9006 | CONTACT@KGHAWES.COM

TOC

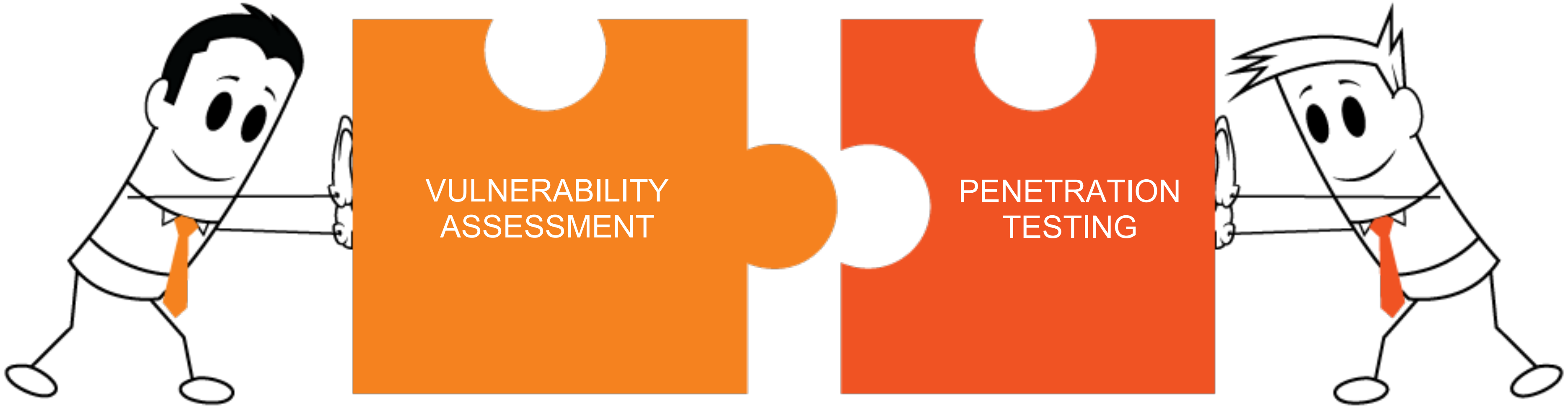
VAPT

Vulnerability Assessment & Penetration Testing

TOC

VAPT | Overview

NEXT: VAPT Process



VAPT: Vulnerability Assessment & Penetration Testing

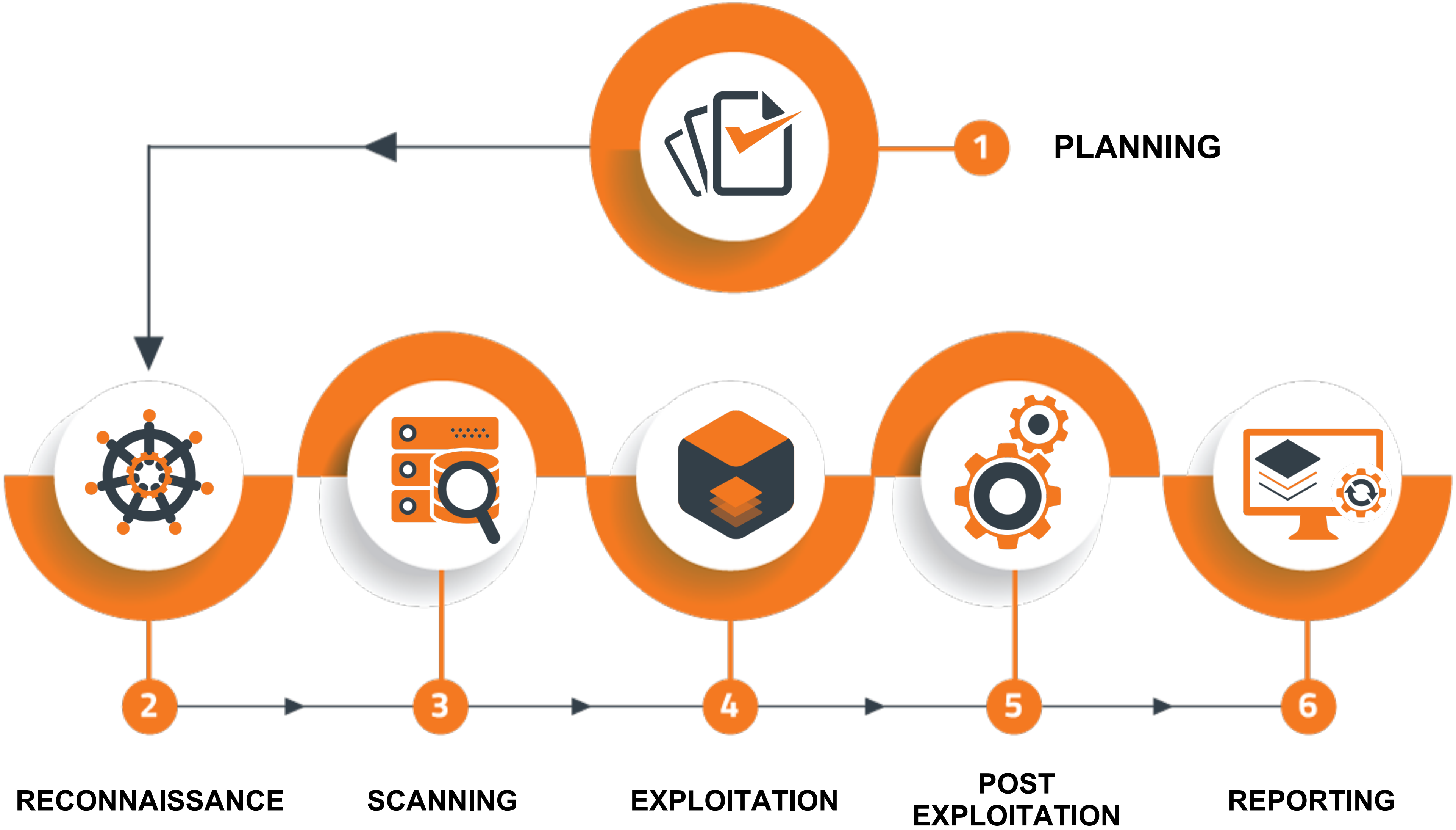
Though vulnerability assessments can be conducted without a penetration test, it is not recommended. Vulnerability testing involves the use of both manual methods and high-tech scanners to identify the security vulnerabilities in an organization's servers, applications and network devices. While it is useful for identifying a system's vulnerabilities, it will not differentiate between exploitable and non-exploitable vulnerabilities. For this you need...

Penetration testing attempts to exploit the vulnerabilities found in the vulnerability assessment.

TOC

VAPT | Process

NEXT: Step 1. Planning



TOC

VAPT | Step 1: Planning

NEXT: Step 2. Reconnaissance →

In this step, KG Hawes and your business will determine the scope of testing, and what the preferred strategy is going forward. This will include a questionnaire as well as your organization’s expectations and outcome goals.

TOC

VAPT | Step 2: Reconnaissance

NEXT: Step 3. Scanning →

This step denotes the act of gathering information about the host. The information encompassed will vary based on the scope determined in Step 1, but generally includes:

- Host's location,
- Type of server it's hosted on,
- Type of CMS platforms used,
- Version on which it's built,
- Programming software used, *and*
- Any other possible information about your system.

TOC

VAPT | Step 3: Scanning

NEXT: Step 4. Expoitation →

In this step, penetration scanners (both automated and manual) come into play. This phase determines:

- The type of server used,
- Its service version,
- The open ports left unclosed, *and*
- Any security loopholes that exist in an application through which cyber stalkers can infiltrate and exploit.

The difference between this and the reconnaissance stage, is that in reconnaissance, the information is taken passively (without hitting the host) while this phase has the host being hit and responded to (active scanning).

TOC

VAPT | Step 4: Exploitation

NEXT: Step 5. Post Exploitation

In this step, previously identified vulnerabilities, from Step 3, will be manually scanned. The exploitation phase of a penetration test focuses solely on establishing access to a system or resource by bypassing security restrictions.

If there are any findings which are determined to be false positives, then these are eliminated, so that only actual issues are accounted for.

Web Applications

Mobile Applications

Networks

APIs

TOC

VAPT | Step 5: Post Exploitation

NEXT: Step 6. Reporting →

Once the testers have gained access to their target (as described in Step 4 Exploitation), they will attempt to gain greater access to your organization's systems. A few examples are listed below of what a tester may attempt to post exploit. They may:

- Access sensitive data stored within the exploited system, and/or
- See what additional systems the exploited network can provide (if the network was accessed), and/or
- Maybe the exploited system is part of a domain that can be used to exploit other systems, etc.

TOC

VAPT | Step 6: Reporting

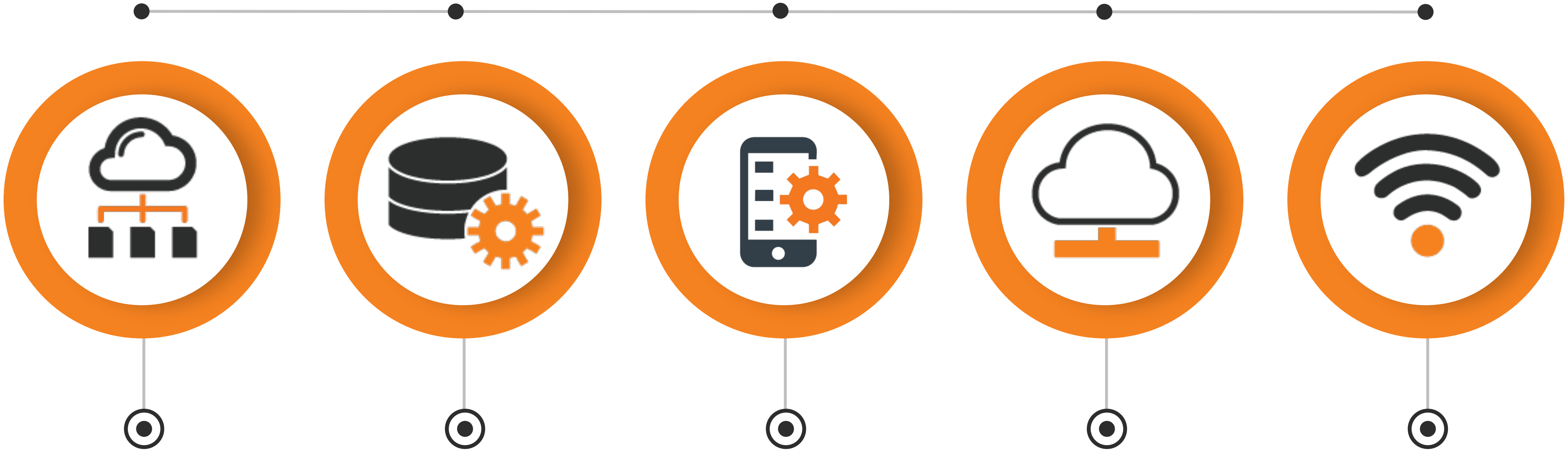
NEXT: Scanners Used

This is the final step of our VAPT process. Identified issues are tracked, listed in terms of their vulnerability’s severity ratings, through CVE, and a complete report is given to your company. This report will include precise details on actual issues and our recommendations on how to address (remediate) them.

TOC

VAPT | Scanners Used

NEXT: Methods Used



Network-based scans are used to identify possible network security attacks and vulnerabilities in wired or wireless networks.

Database scans can be used to identify the weak points in a database so as to prevent malicious attacks, such as SQL Injection attacks.

Application scans can be used to test websites in order to detect known software vulnerabilities and misconfigurations in web applications.

Host-based scans are used to locate and identify vulnerabilities in servers, workstations and other network hosts.

Wireless Wi-Fi network scans usually focus on points of attack in the wireless network infrastructure.

TOC

VAPT | Methods Used

NEXT: Step 6. Tools Used →

WHITE BOX

Testing method in which internal structure, design and implementation of the item being tested **is known** to the tester.

GRAY BOX

Testing method performed with **limited information** about internal functionality of the system. Gray-box testers have access to the design documents along with information about requirements.

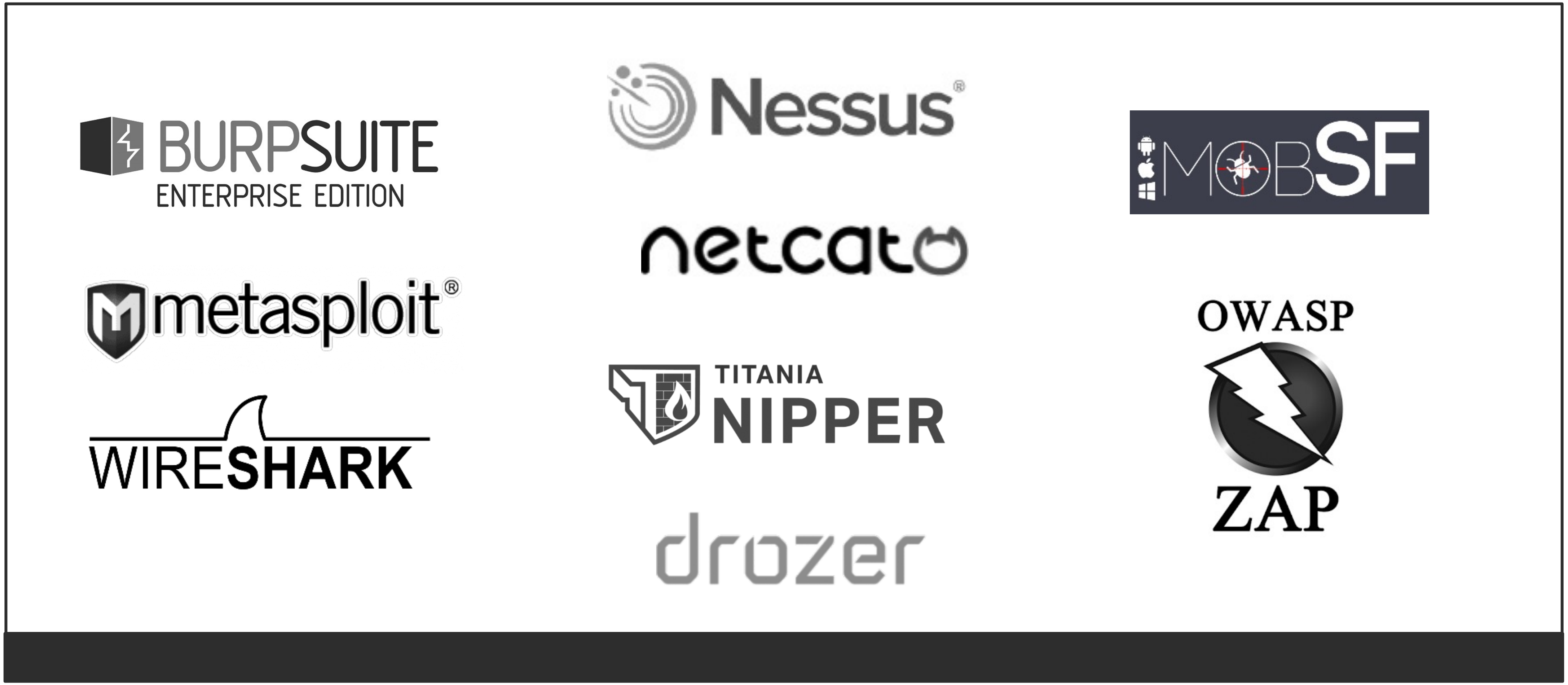
BLACK BOX

Testing method in which internal structure, design, implementation of the item being tested is **not known** to the tester.

TOC

VAPT | Tools Used

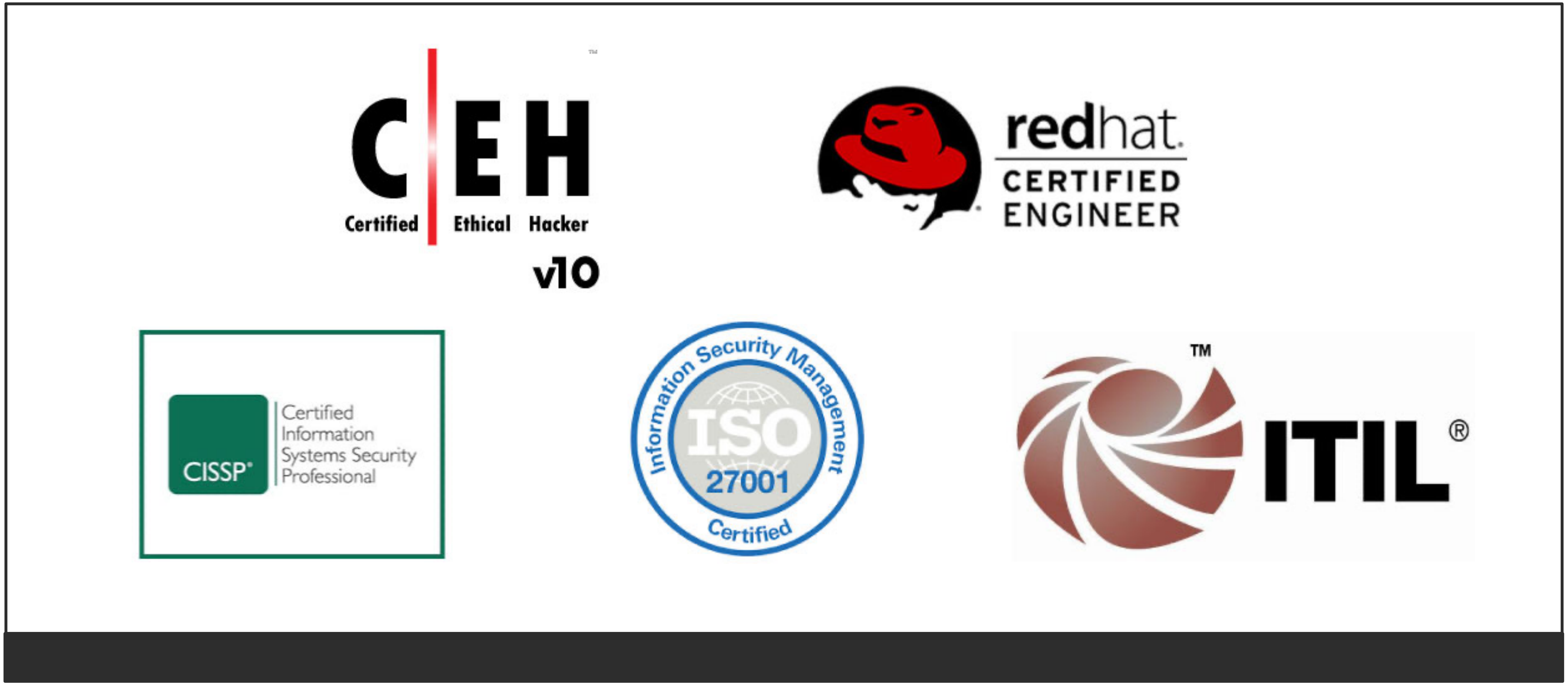
NEXT: Certifications



TOC

VAPT | Certifications

NEXT: Remediation



TOC

REMEDIATION

After the VAPT

(Separate Service)

TOC

AFTER THE VAPT | Remediate & Mitigate

NEXT: Other Services

The next step after a **VAPT** is to address the found vulnerabilities.

How you proceed depends upon the type of vulnerabilities found.

Vulnerability

REMEDIATE

Vulnerability can be removed (software patches, upgrades, etc.)

MITIGATE

Vulnerability can be minimized (configuration setting change).

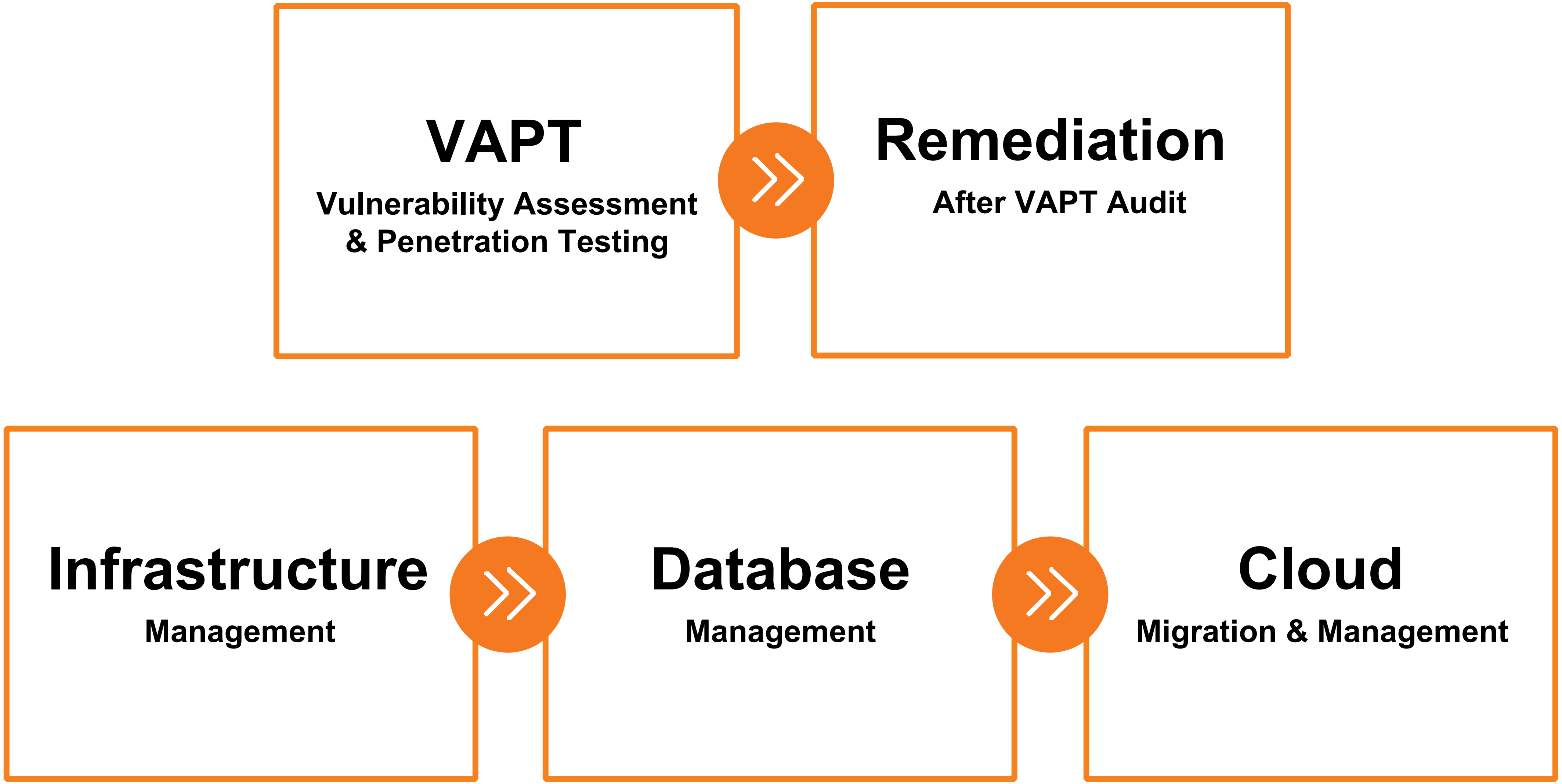
TOC

WWW.KGHAWES.COM | (866) 687-9006 | CONTACT@KGHAWES.COM

OTHER SERVICES

TOC

VAPT | Other Services



VAPT

Vulnerability Assessment & Penetration Testing

Remediation

After VAPT Audit

Infrastructure

Management

Database

Management

Cloud

Migration & Management

TOC

Contact Us

KG Hawes

Partners in Technology

✉ contact@kghawes.com

☎ 866.687.9006

https://kghawes.com

Executive / Corporate
12204 SE Mill Plain Blvd, Vancouver, WA 98684

Operations / Development
400 International Way, Suite #300 Springfield, OR 97477