ICS

WE SECURE IT

VULNERABILITY
ASSESSMENT

A Step-by-Step Guide to Conduct a Vulnerability Assessment

PART OF

datef.it

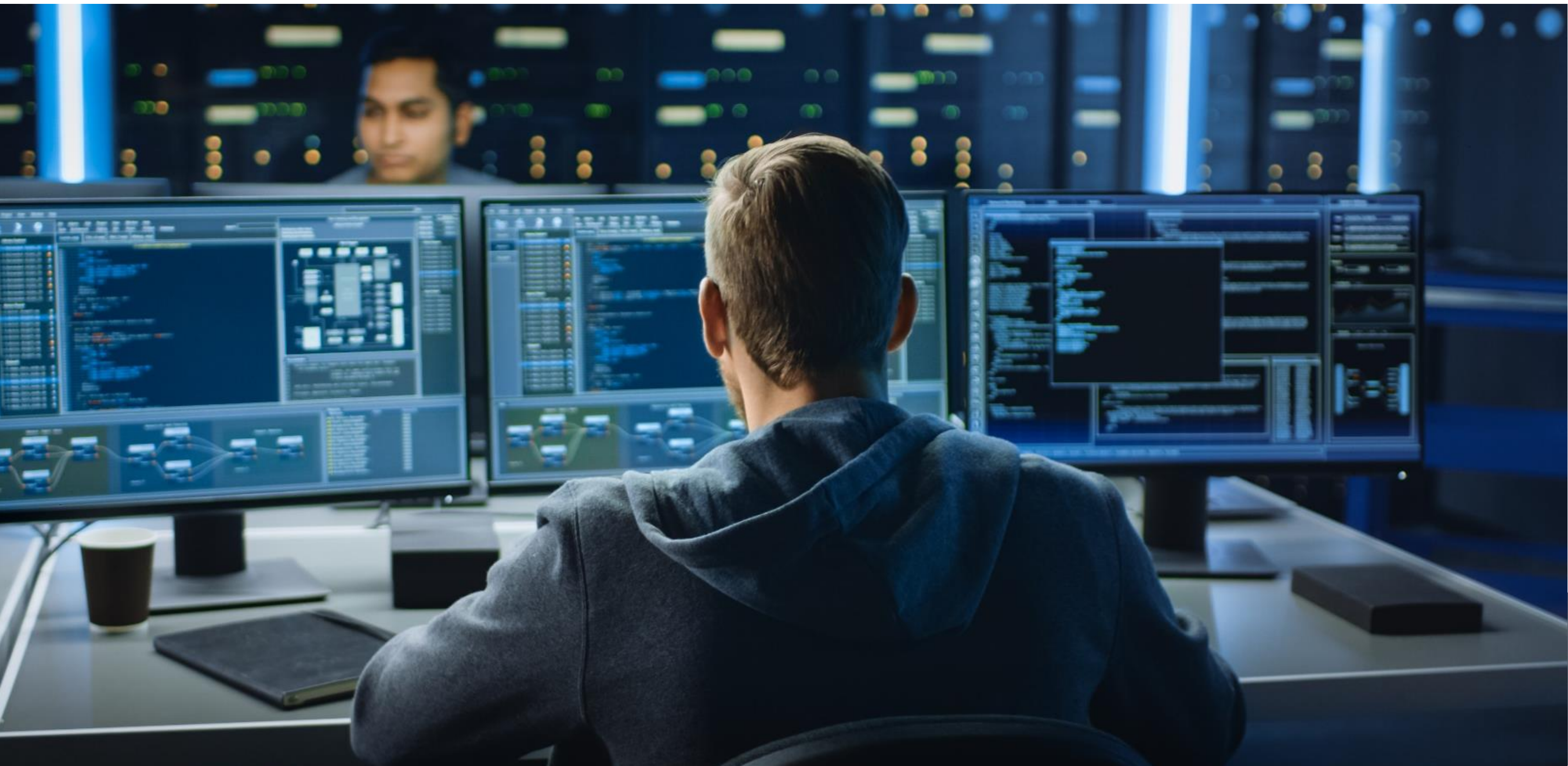
MOVE TOGETHER

SUMMARY

Over 23,000 new software vulnerabilities were identified and publicly published in 2020 alone. Numbers like this no longer raise eyebrows in the cyber security industry, as astounding as they may appear to the uninformed. Although no organization is likely to be targeted by all 23,000, it just takes one to inflict tremendous havoc.

If you're wondering how likely you are to be harmed by one of these flaws, an IBM study found that scanning for and exploiting vulnerabilities will be the most common attack vector in 2020 (35 percent of attacks), surpassing phishing attacks.

Hence, this paper explains the importance and purpose of a Vulnerability Assessment in order to prepare your company from common attacks.



WE SECURE IT

WHAT?

What is a Vulnerability Assessment, and how does it work?

We all make mistakes as people, and because software is developed by humans, it is bound to have flaws. While many defects are innocuous in nature, some turn out to be exploitable vulnerabilities, jeopardizing the system's usefulness and security. This is when a vulnerability analysis is useful. A vulnerability assessment is an examination of vulnerabilities in IT systems at a certain moment in time with the goal of detecting the system's flaws before hackers gain access.

PURPOSE?

What is a vulnerability assessment's purpose?

There's a significant difference between believing you're exposed to a cyberattack and understanding precisely how vulnerable you are, since you can't avoid it unless you know how you're vulnerable. The purpose of the vulnerability assessment is to close this gap. A vulnerability assessment examines one or more of your systems and provides a thorough report. This report may then be used to address the issues discovered in order to prevent security breaches.

Furthermore, a rising number of businesses rely on technology to run their everyday operations, yet cyber dangers such as ransomware may bring your organization to a standstill in an instant. Because it is well recognized that prevention is preferable than treatment, cyber security is becoming increasingly important, and solutions to ensure its resilience are in high demand. More SaaS clients, for example, are requesting frequent vulnerability assessments, and having proof of security testing may help you create more business.

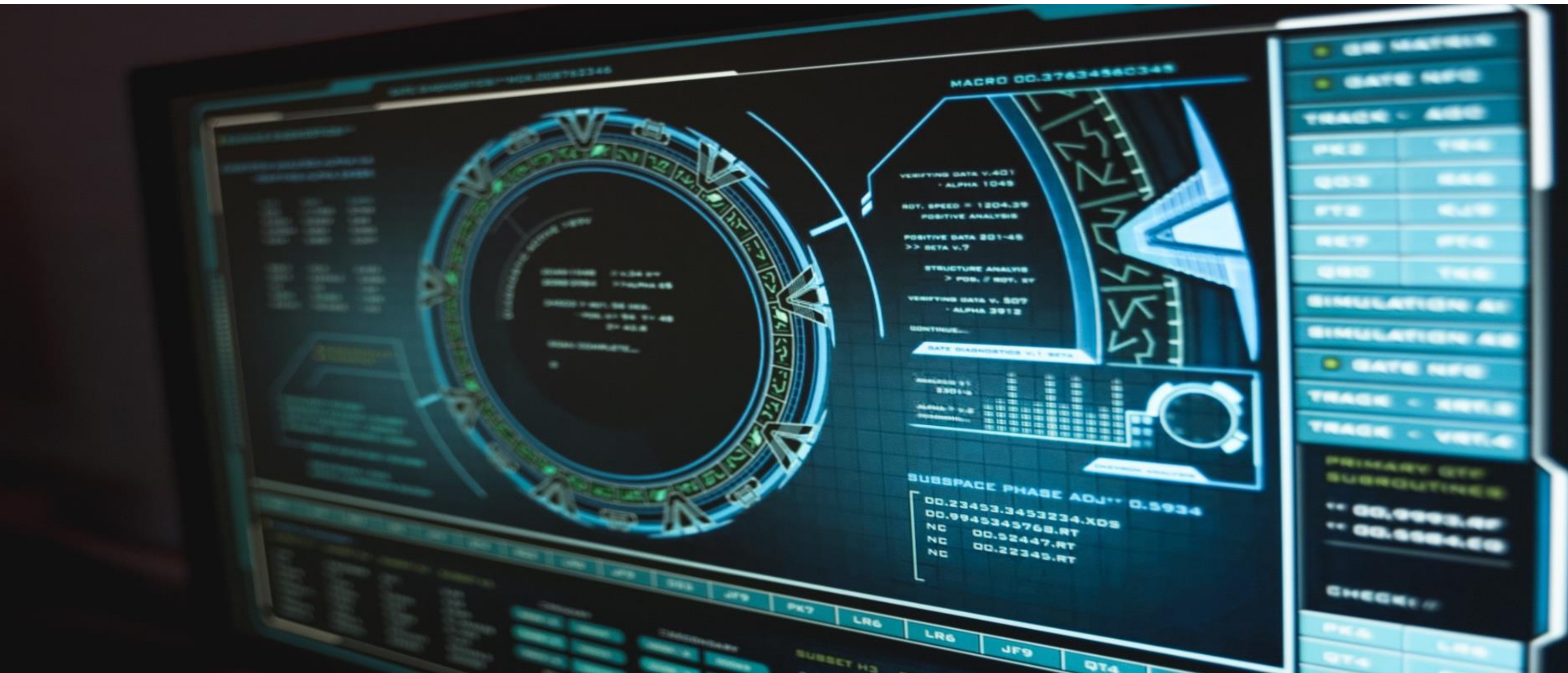
.

DIFFERENCE?

Vulnerability Assessment and Penetration Testing (VAPT)

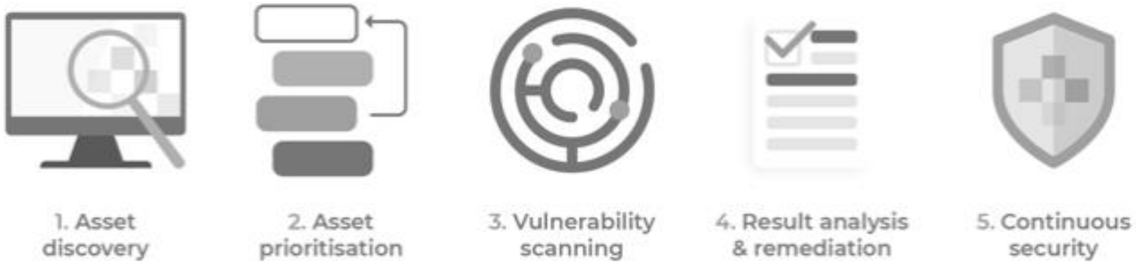
Vulnerability assessments and penetration testing are often confused. Many security firms provide both, and the distinctions between them are sometimes muddled.

Looking at how the heavy lifting in the test is done is the greatest way to identify the difference between these two products. An automated vulnerability assessment is one in which a technology performs all of the work and provides a report at the end. Penetration testing, on the other hand, is a manual procedure that relies on a penetration tester's expertise and experience to find vulnerabilities in an organization's systems.



HOW?

How to Conduct a Vulnerability Analysis



You may do a vulnerability assessment using the following stages if you have the necessary tools:

1. Asset Discovery

To begin, you must first determine what you want to scan, which is not always as straightforward as it may appear. A lack of visibility into an organization's digital infrastructure and linked devices is one of the most prevalent cyber security issues.

The following are some of the reasons behind this:

- Smartphones, laptops, and other **mobile devices** are intended to detach and rejoin often from the workplace, as well as from employees' homes and other remote places.

- **IoT Devices:** IoT devices are part of a company's infrastructure, although they're mostly connected to mobile networks.

- **Cloud-based Infrastructure**: Cloud service providers make it simple to set up new servers as needed without the requirement for IT support.

We'd all like to work in a well-organized company, but the reality is often more chaotic. Simply keeping track of what various teams are putting online, or altering, at any one time can be difficult. It's difficult to protect something you can't see, therefore this lack of sight is a concern. Fortunately, the finding part of the process may be automated to a great extent. Some contemporary vulnerability assessment technologies, for example, may identify cloud-based infrastructure by performing discovery on public-facing systems and connecting directly to cloud providers.

2. Asset Prioritization

The second question is whether you can afford to perform a vulnerability assessment on everything once you know what you have. In an ideal environment, you would do a vulnerability assessment on all of your systems on a regular basis. Vendors, on the other hand, frequently charge per-asset, thus prioritization might help when budgets can't cover all of the company's assets.

Here are some examples of areas that you might want to prioritize:

- Servers that are accessible over the internet
- Customer-facing software
- Databases holding confidential data

It's worth mentioning that the following are two of the most prevalent routes for bulk or untargeted attacks:

It's worth mentioning that the following are two of the most prevalent routes for bulk or untargeted attacks:

- Systems that are connected to the internet
- Laptops for employees

3. Vulnerability Scanning

Vulnerability scanners are programs that look for known security flaws and give instructions on how to repair them. Because these flaws are frequently disclosed publicly, there is a wealth of knowledge on susceptible software. This information is used by vulnerability scanners to discover insecure devices and applications in an organization's infrastructure. Initially, the scanner sends probes to systems in order to identify:

- Ports are open, and services are operating.
- Versions of software
- Setting up the configuration

The scanner may frequently discover several known vulnerabilities in the system being tested based on this information.

Furthermore, the scanner sends specialized probes to discover unique vulnerabilities that can only be tested by providing a safe exploit that verifies the vulnerability exists. Common vulnerabilities like as 'Command Injection' or 'cross-site scripting (XSS)', as well as the usage of default users and passwords for a system, may be detected using these sorts of probes.

The vulnerability scan might take anything from a few minutes to many hours, depending on the infrastructure you're analyzing (and, in particular, how large any websites are).

4. Result Analysis and Remediation

The scanner generates an evaluation report when the vulnerability scan is completed. Consider the following while reading this report and making remedial plans based on it:

> **The severity** of a possible vulnerability should be labeled by a vulnerability scanner. When preparing for repair, prioritize the most serious vulnerabilities first, but don't ignore the others indefinitely. It's not unusual for hackers to combine multiple minor flaws into a single attack. A competent vulnerability scanner will provide you a schedule for when you should resolve each problem.
>
> **Vulnerability Exposure:** Keep in mind that not all vulnerabilities are found on public-facing systems. Internet-facing systems are more likely to be attacked by any random attacker browsing the internet, thus they should be addressed first. After that, any employee computers with susceptible software should be prioritized. Furthermore, any systems that contain highly sensitive data or might have a negative impact on your organization may need to be prioritized above others.

5. Continuous Cyber Security

A vulnerability scan is a snapshot of the vulnerabilities in an organization's digital infrastructure at a certain moment in time. New installations, configuration modifications, newly found vulnerabilities, and other variables, on the other hand, can swiftly expose the business to risk. As a result, rather of treating vulnerability management as a one-time event, you should treat it as a continuous activity.

Because software development introduces numerous vulnerabilities, the most forward-thinking software development firms incorporate automated vulnerability assessments into their continuous integration and deployment (CI/CD) pipelines. This helps them to find and correct flaws in software before it is deployed, eliminating the risk of exploitation and the requirement to build and distribute fixes for vulnerable code.

ICS
WE SECURE IT

ICS SERVICE

The ICS Vulnerability Assessment Service

ICS offers a vulnerability assessment that scans your infrastructure for a variety of vulnerabilities. It's intended to save you time by doing proactive security checks, monitoring network changes, and synchronizing cloud systems, among other things. ICS provides a final report detailing the flaws and providing actionable remedial recommendations by being PCI DSS compliant, allowing you to identify and repair vulnerabilities before they are exploited by hackers.

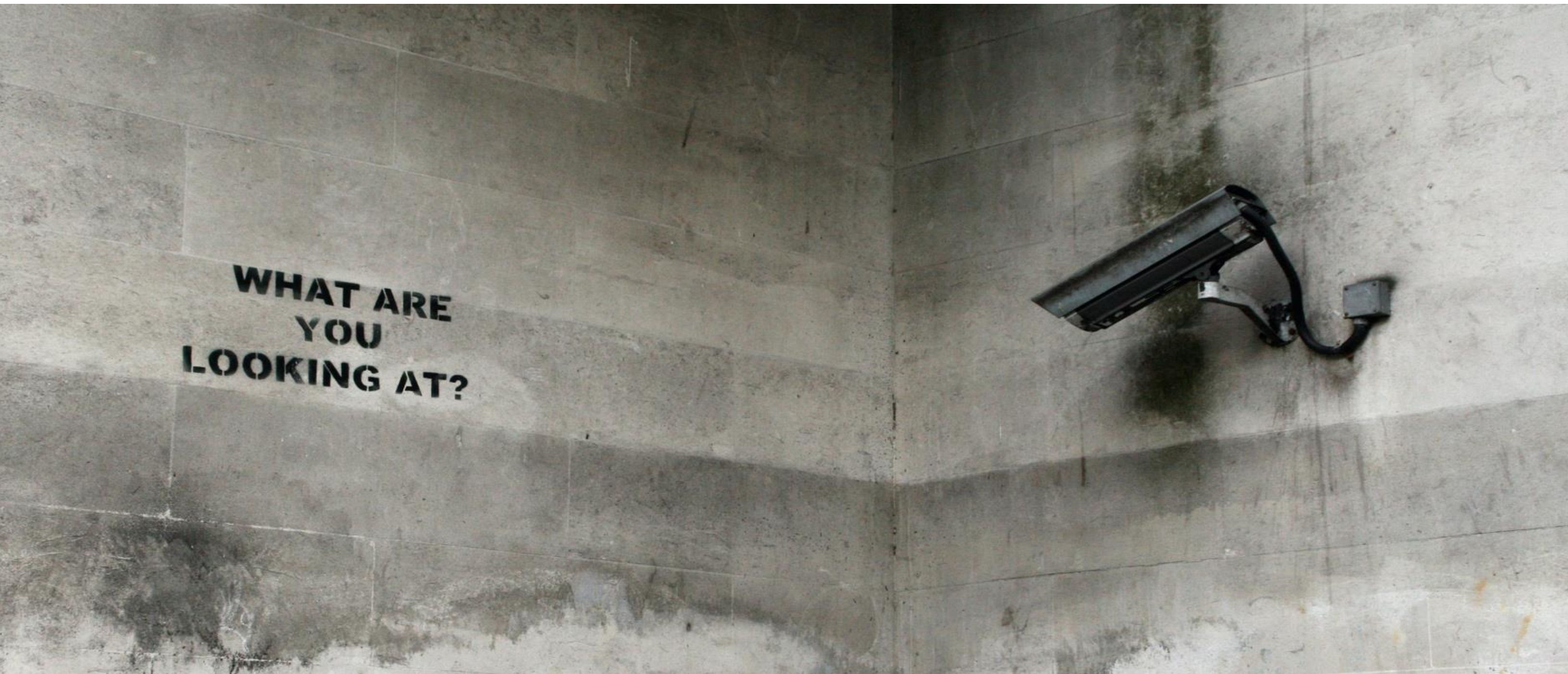
ICS
WE SECURE IT

CONCLUSION

To sum up,

a good cyber security posture necessitates regular vulnerability evaluations. Because of the vast number of vulnerabilities and the complexity of the ordinary firm's digital infrastructure, a corporation is nearly certain to have at least one unpatched vulnerability that puts it at risk. Finding these flaws before an attacker does might be the difference between a successful attack and an expensive and humiliating data breach or ransomware assault.

One of the best things about vulnerability assessments is that they can be done easily and even automated. You can significantly reduce your cyber security risk by investing in the proper technologies and doing frequent vulnerability scans.



WE SECURE IT

ABOUT ICS

Industrial Cyber Security is part of the Datef Group and provides highly effective cybersecurity solutions that medium and large enterprises rely on. We provide our clients with targeted assessments, as well as technical, organizational, and cultural approaches to mitigate risks and attack surfaces, and optimize our clients' resources.

Our team includes experienced and highly qualified cybersecurity experts who provide our clients with effective cybersecurity strategies with a proven cost-benefit balance.