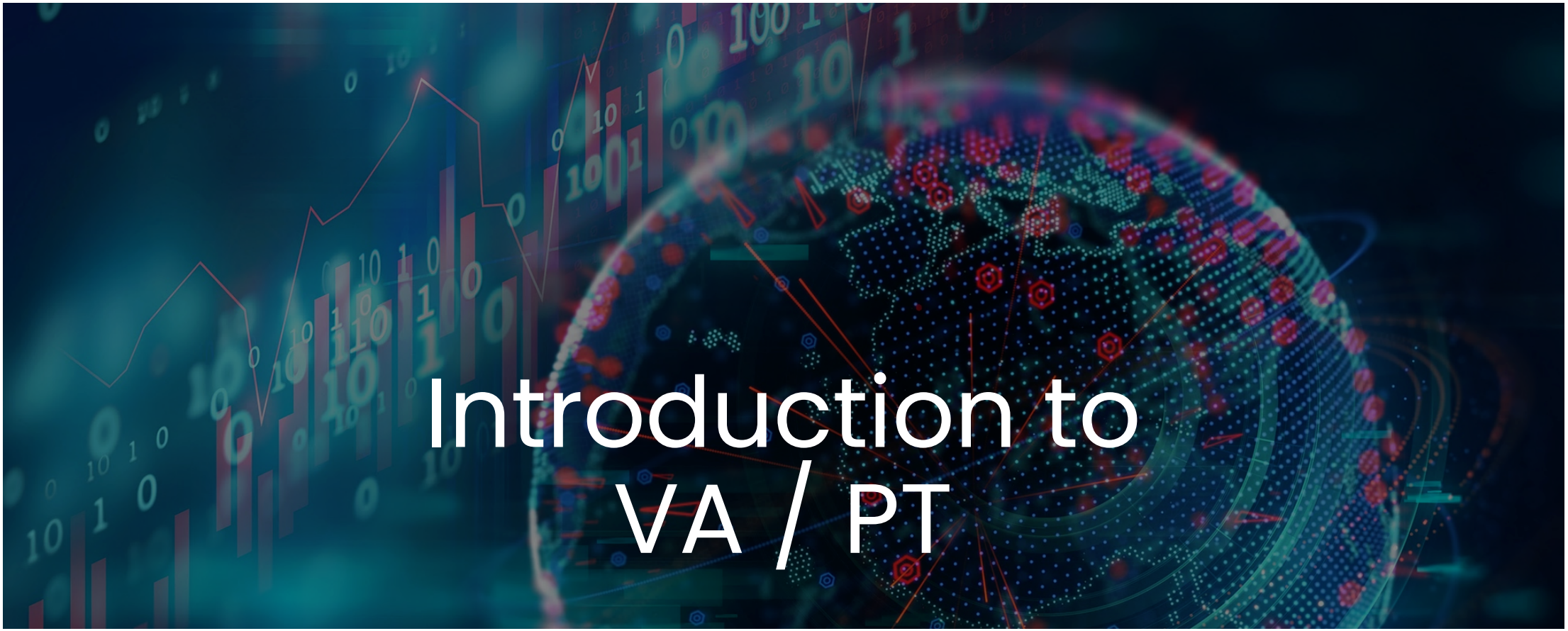


Introduction to VA / PT

DYNAFENSE
CYBER SECURITY

Picture credits: https://eda.europa.eu/what-we-do/capability-development/cyber

AGENDA

WE WILL COVER

00 **Introduction**

01 **What is VA / PT?**

02 **Similarities and Differences**

03 **Types of PT**

04 **Practice**

DYNAFENSE CYBERSECURITY

INTRODUCTION

Experienced cybersecurity and risk professionals

Cybersecurity penetration testers and security assessors who sees the big picture yet precise enough to pick up the minutiae.

Focused on cyber risks faced by organisations today

We understand your business.
We understand the cyber risks you face.

Bespoke assessment approach and recommendations

One size does not fit all. We curate and apply our techniques and tactics according to the industry and risk profile.

Conduct bespoke security research

We perform bespoke security research on the business IT equipment, software and tools used by both management, operational staff and IT staff.

Say Hong TAN

Founder & Director

Tel: +65 8717 7537

FOUNDER

INTRODUCTION

Experienced cyber security assessor and risk management professional.

Holds Chartered Accountant (Singapore), CREST, ISACA certifications.

Led teams on banking-related regulatory reviews and assessments, including IT controls testing.

Advised and implement various data privacy and IT security frameworks for clients in variety of industries.

Received Singapore Government and MINDEF Bug Bounty tokens as appreciation for identifying vulnerabilities.

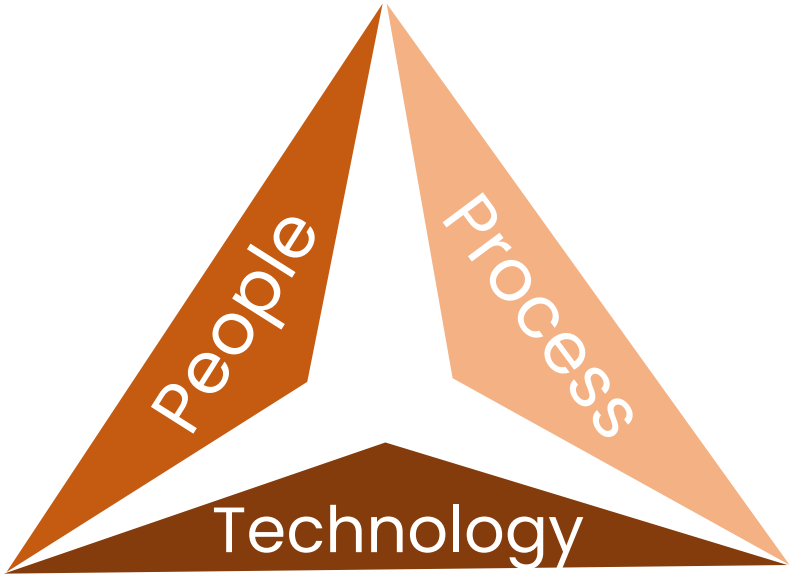
INFORMATION SECURITY

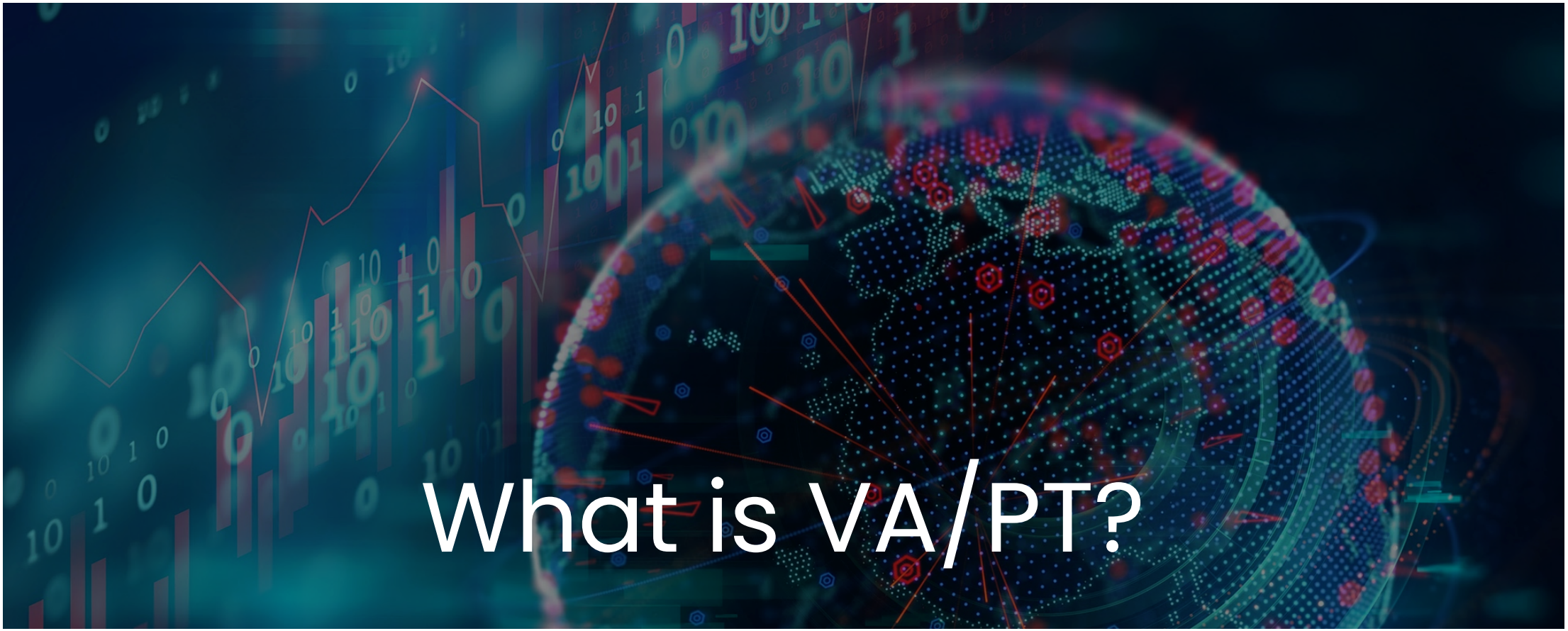
INTRODUCTION

CIA Triad

CYBER SECURITY

INTRODUCTION





What is VA/PT?

DYNAFENSE
CYBER SECURITY

Picture credits: https://eda.europa.eu/what-we-do/capability-development/cyber

MAS Monetary Authority of Singapore

中华人民共和国个人信息保护法

（2021年8月20日第十三届全国人民代表大会常务委员会第三十次会议通过）

PCI DSS COMPLIANT

PCPD HK PCPD.org.hk 香港個人資料私隱專員公署 Office of the Privacy Commissioner for Personal Data, Hong Kong

保障、尊重個人資料私隱

Protect, Respect Personal Data Privacy

ISO/IEC 27001

INFORMATION SECURITY MANAGEMENT

Who requires VA/PT?

HIPAA Health Insurance Portability and Accountability Act

NIST National Institute of Standards and Technology U.S. Department of Commerce

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

Characteristics

VA VS PT

- Breadth
- Non-Intrusive approach
- List oriented
- Systematic approach
- Applies both automated and manual tests
- Good to know programming languages
- Prioritised list of vulnerabilities and associated assets

- Depth
- Intrusive approach
- Goal oriented
- Less structured approach
- Predominantly relies on manual tests
- Must know programming languages
- Step by step exploitation reproduction

TOOLS USED IN VA

VULNERABILITY ASSESSMENTS

OpenVAS by Greenbone

Open Vulnerability Assessment Scanner

SSLyze

& Custom tools…

TOOLS USED IN PT

PENETRATION TESTS

PortSwigger

cobaltstrike
by HelpSystems

Fiddler

uncover

hex-rays

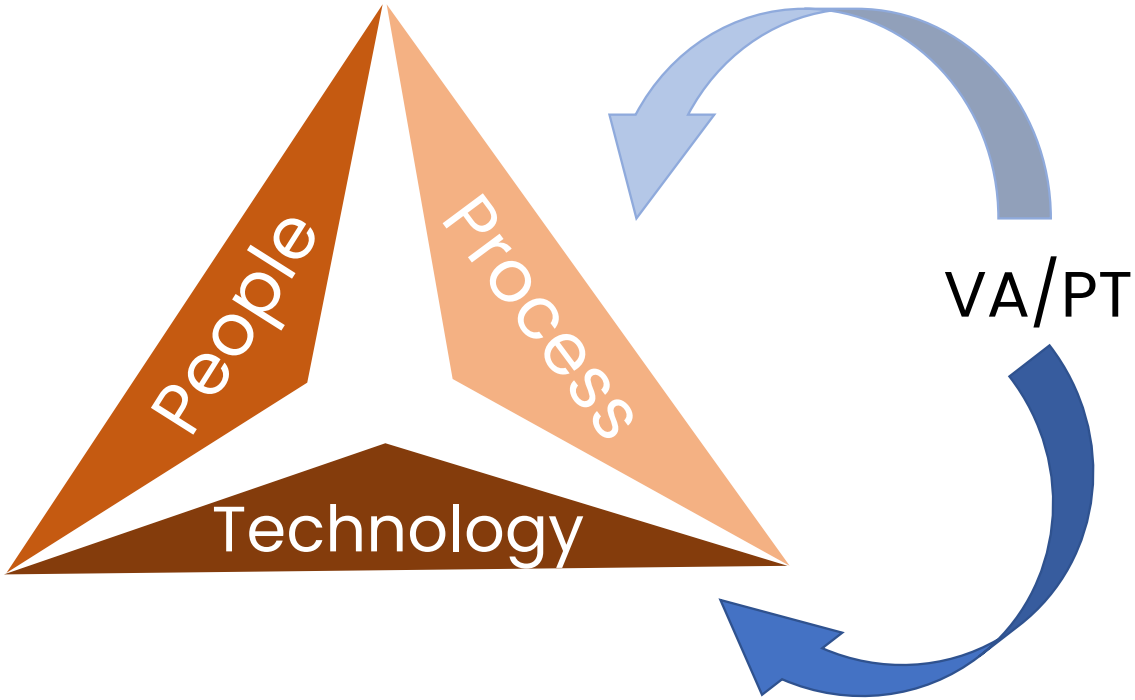
FRIDA

MOBSF

& Custom tools...

WHAT DO VAs/PTs test?

RISKS

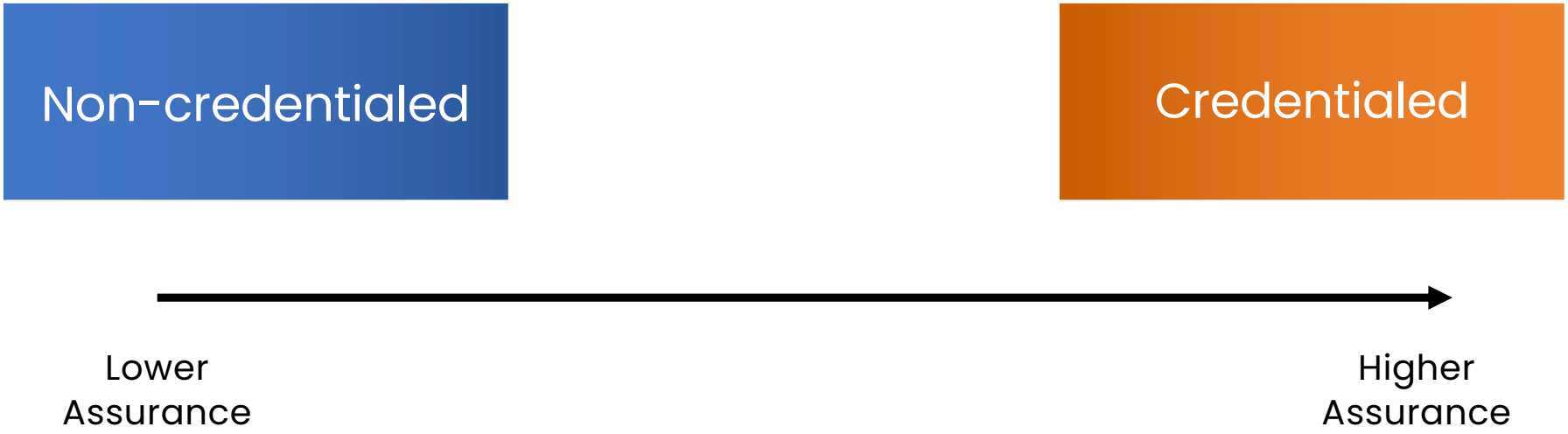


DYNAFENSE
CYBER SECURITY

Picture credits: https://eda.europa.eu/what-we-do/capability-development/cyber

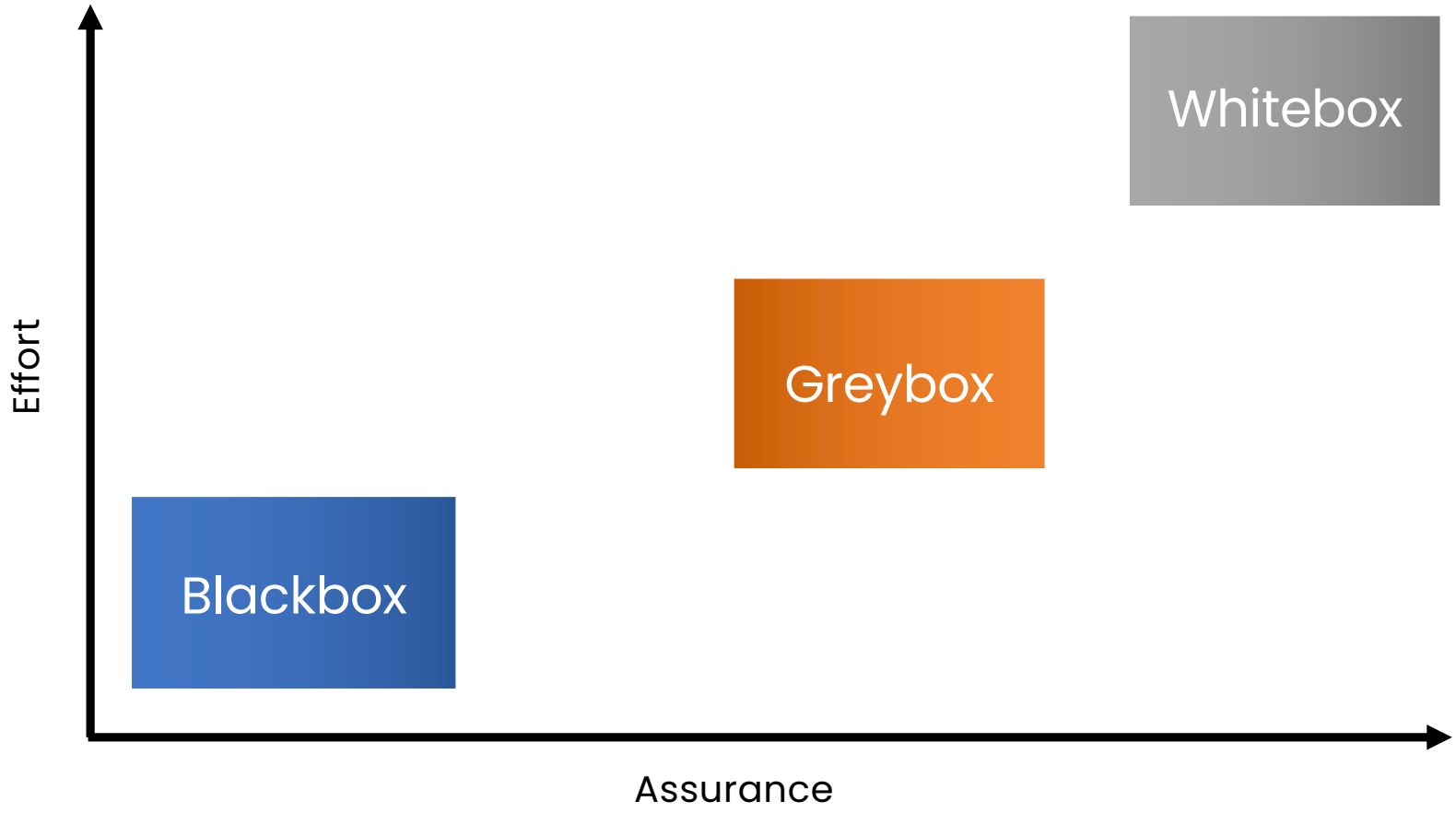
VULNERABILITY ASSESSMENTS

ASSURANCE



PENETRATION TESTS

ASSURANCE



DYNAFENSE
CYBER SECURITY

Picture credits: https://eda.europa.eu/what-we-do/capability-development/cyber

Quiz #1

POP QUIZ

VA/PT

What is getting tested – People, Process, Technology

A. People, Process
B. Process, Technology
C. People, Technology

Point in time vs Over time

- Is a Vulnerability Assessment considered a Point-in-Time test or Over time test?
- Similar for Penetration Testing.

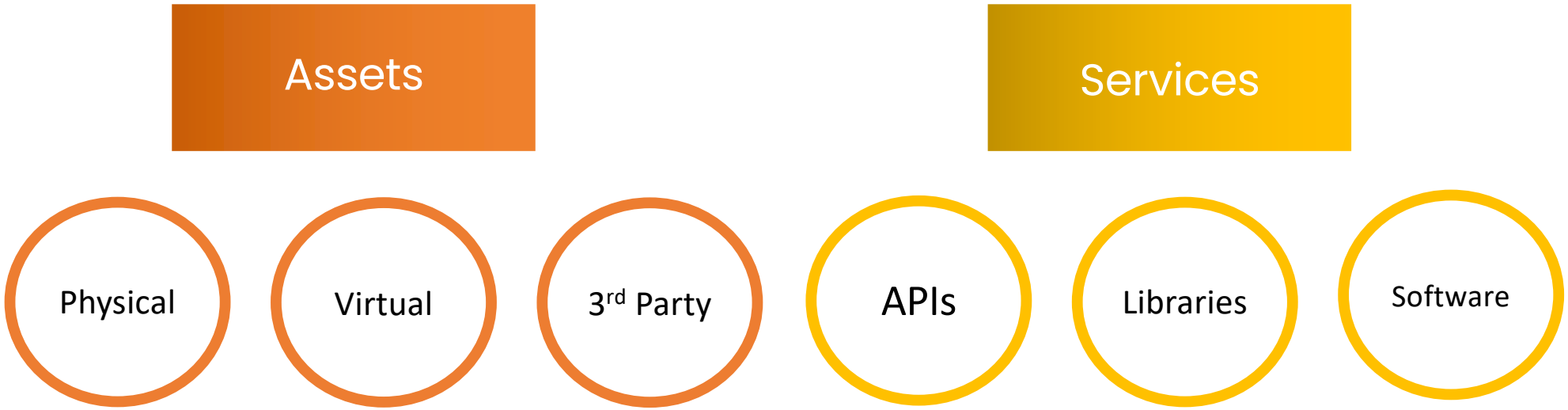
Where are VAs/PTs applied to?

DYNAFENSE
CYBER SECURITY

Picture credits: https://eda.europa.eu/what-we-do/capability-development/cyber

WHERE ARE VAs APPLIED TO?

ASSETS & SERVICES



Firewalls
Mobile phones
Servers
IoT
Load balancers
Routers
Desktops
Laptops
Network switches
Wireless access points

Middleware
Applications
Mobile apps
Mobile operating systems
Databases
Operating systems

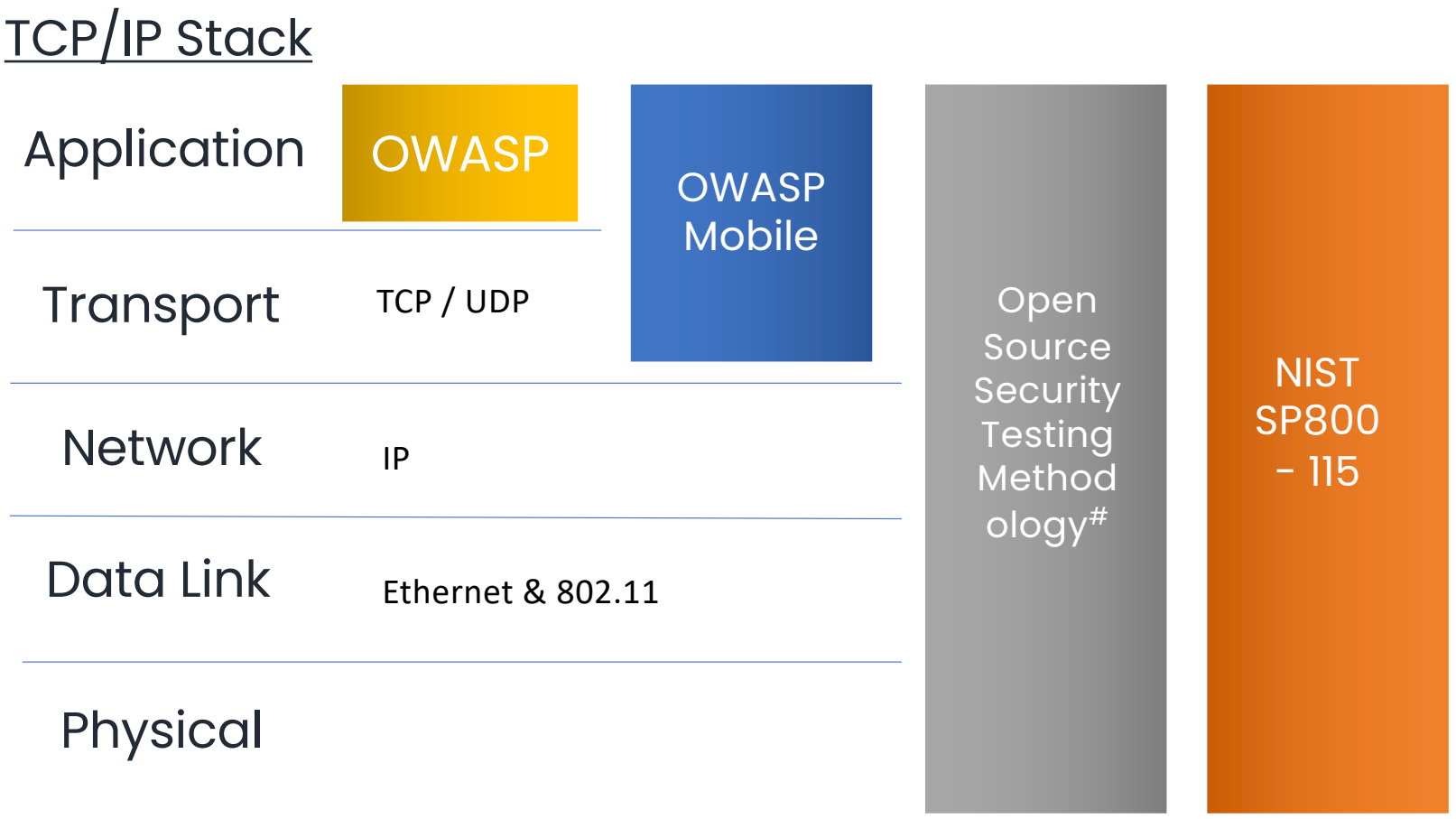
TYPES OF VAs

ASSETS & SERVICES

- Operating System
- Databases
- Application Servers
- Network / Network devices
- Wireless networks

INDUSTRY TESTING METHODOLOGIES

YOU SHOULD KNOW



Old

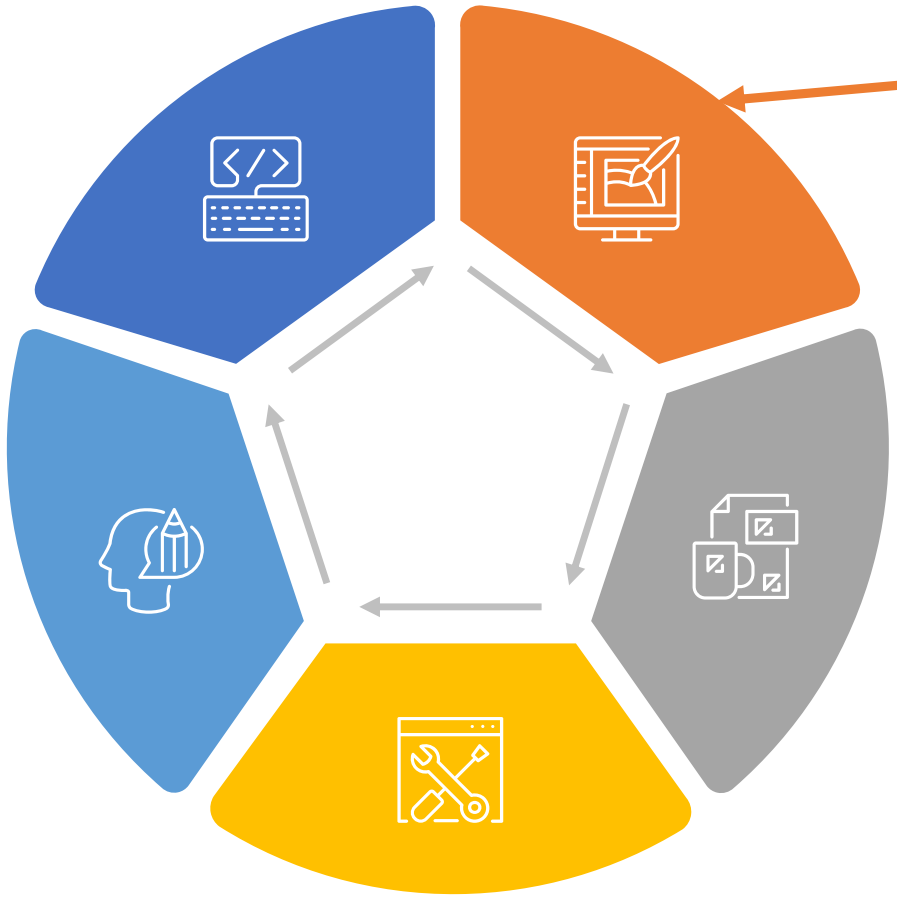
Understanding the VA process

DYNAFENSE
CYBER SECURITY

Picture credits: https://eda.europa.eu/what-we-do/capability-development/cyber

VULNERABILITY ASSESSMENT

PROCESS FLOW



1. Planning

Determine assets for the VA, applicable timeline and no-go IP addresses

2. Vulnerability Asst

Perform VA on in-scope assets, Highlight immediately if Critical or High vulnerabilities were detected

3. Triage

Classify vulnerabilities based on asset and its severity levels.

4. Report

Deliver results in the form of a VA report

5. Remediation

Remediate to lower risk. Reduce, Accept, Transfer.

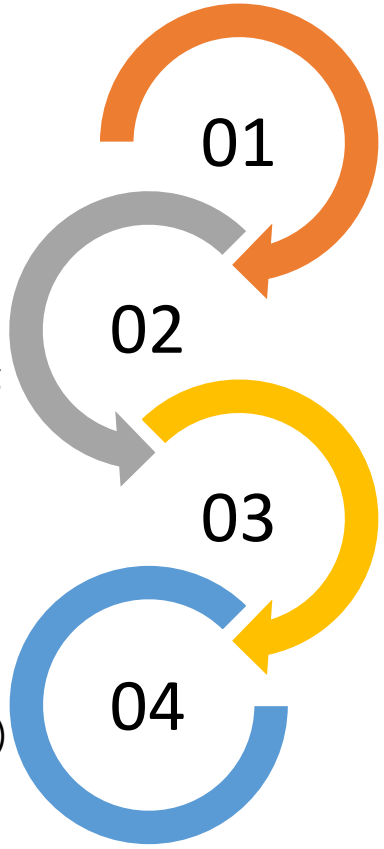
Understanding the PT process

DYNAFENSE
CYBER SECURITY

Picture credits: https://eda.europa.eu/what-we-do/capability-development/cyber

PENETRATION TESTING

PROCESS FLOW



Planning

Determine what assets are in-scope for the PT, applicable timeline and no-go IP addresses

Information collection

Perform reconnaissance on the in-scope IP addresses, determine services, underlying operating system, etc.

Penetration

Perform PT on in-scope assets, Highlight immediately if Critical or High vulnerabilities were detected

Report and clean up

Deliver results in the form of a report. Remove or highlight implants (eg stored XSS) if need be.

Vulnerability Scoring Systems

DYNAFENSE
CYBER SECURITY

Picture credits: https://eda.europa.eu/what-we-do/capability-development/cyber

Common Vulnerability Scoring System Version 3.0 Calculator

Hover over metric group names, metric names and metric values for a summary of the information in the official CVSS v3.0 Specification Document. The Specification is available in the list of links on the left, along with a User Guide providing additional scoring guidance, an Examples document of scored vulnerabilities, and notes on using this calculator (including its design and an XML representation for CVSS v3.0).

Vu ems

Base Score

Select values for all base metrics to generate score

Attack Vector (AV)

Network (N) | Adjacent (A) | Local (L) | Physical (P)

Attack Complexity (AC)

Low (L) | High (H)

Privileges Required (PR)

None (N) | Low (L) | High (H)

User Interaction (UI)

None (N) | Required (R)

Scope (S)

Unchanged (U) | Changed (C)

Confidentiality (C)

None (N) | Low (L) | High (H)

Integrity (I)

None (N) | Low (L) | High (H)

Availability (A)

None (N) | Low (L) | High (H)

eu/what-we-do/capability-development/cyber

VPR Key Drivers

You can view the following key drivers to explain a vulnerability's VPR.

Note: Tenable does not customize these values for your organization; VPR key drivers reflect a vulnerability's global threat landscape.

Key Driver	Description
Age of Vuln	The number of days since the National Vulnerability Database (NVD) published the vulnerability.
CVSSv3 Impact Score	The NVD-provided CVSSv3 impact score for the vulnerability. If the NVD did not provide a score, Nessus displays a Tenable-predicted score.
Exploit Code Maturity	The relative maturity of a possible exploit for the vulnerability based on the existence, sophistication, and prevalence of exploit intelligence from internal and external sources (e.g., Reversinglabs, Exploit-db, Metasploit, etc.). The possible values (**High**, **Functional**, **PoC**, or **Unproven**) parallel the CVSS Exploit Code Maturity categories.
Product Coverage	The relative number of unique products affected by the vulnerability: **Low**, **Medium**, **High**, or **Very High**.
Threat Sources	A list of all sources (e.g., social media channels, the dark web, etc.) where threat events related to this vulnerability occurred. If the system did not observe a related threat event in the past 28 days, the system displays **No recorded events**.
Threat Intensity	The relative intensity based on the number and frequency of recently observed threat events related to this vulnerability: **Very Low**, **Low**, **Medium**, **High**, or **Very High**.
Threat Recency	The number of days (0-180) since a threat event occurred for the vulnerability.

TYPES OF PTs

ASSETS & SERVICES

- Web / Mobile Applications
- Application Servers
- Operating System
- Databases
- Network / Network devices
- Wireless networks
- VoIP
- Hardware appliances (Door control systems, CCTV, etc)

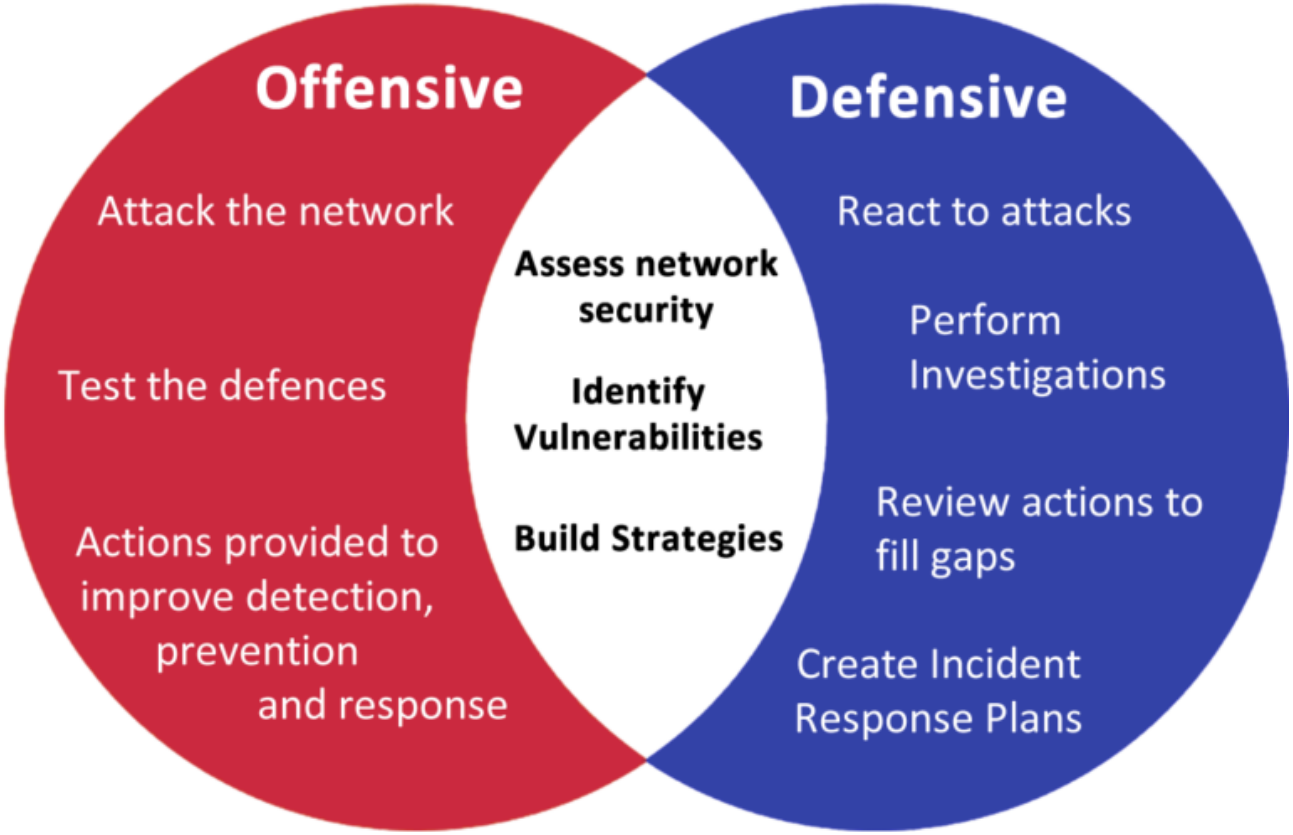
What's after VA/PT?

DYNAFENSE
CYBER SECURITY

Picture credits: https://eda.europa.eu/what-we-do/capability-development/cyber

RED TEAM vs BLUE TEAM

STEP UP



Picture credits: https://www.pentestpartners.com/penetration-testing-services/purple-teaming/

* Teams

Step up

Picture credits: https://www.pentestpartners.com/penetration-testing-services/purple-teaming/

DYNAFENSE
CYBER SECURITY

Picture credits: https://eda.europa.eu/what-we-do/capability-development/cyber

Quiz #2

POP QUIZ

A. The company is preparing for an IPO. As part of the requirements, a pre-IPO due diligence assessment requires a VA to be performed by an independent third party.

An IT Director furiously insists the VA performed three months ago on the company's cyber assets is still valid and wants to submit the same report so he will not need to ask for additional budget from the COO.

Is the IT Director correct?

B. What's Vulnerability Management?

Quiz #3

POP QUIZ

You've started on a PT engagement on a client's Internet facing web service.

Right before the PT engagement ends, you managed to locate a vulnerability in the above web service, divulging all the user Personally Identifiable Information (PII).

What do you do next?

a. Record the steps to exploit the vulnerability for inclusion into the final PT report.
b. Extract as much user PII as possible for verbatim inclusion into the final PT report, as evidence of work done.
c. Inform the client of the vulnerability.

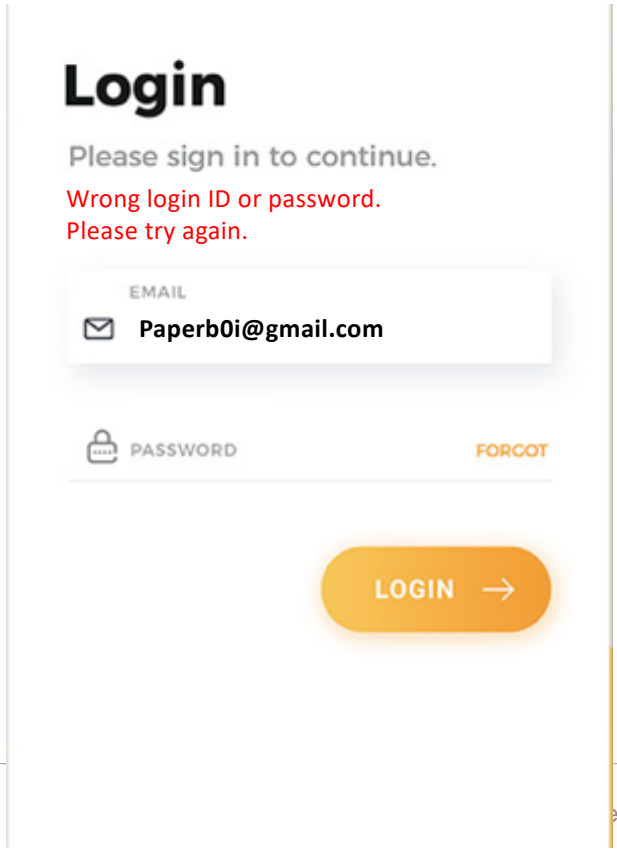
Quiz #4

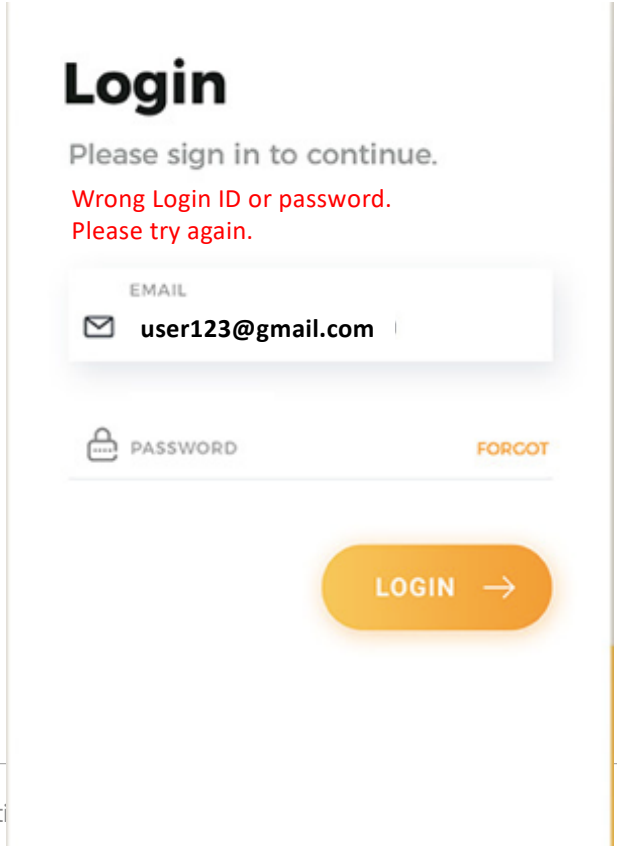
POP QUIZ

You've come to the completion of a PT engagement and concluding with the last few tests.

You've typed in a valid username and invalid password.

The web service returned this





You've typed in an invalid username and invalid password.

The web service returned this

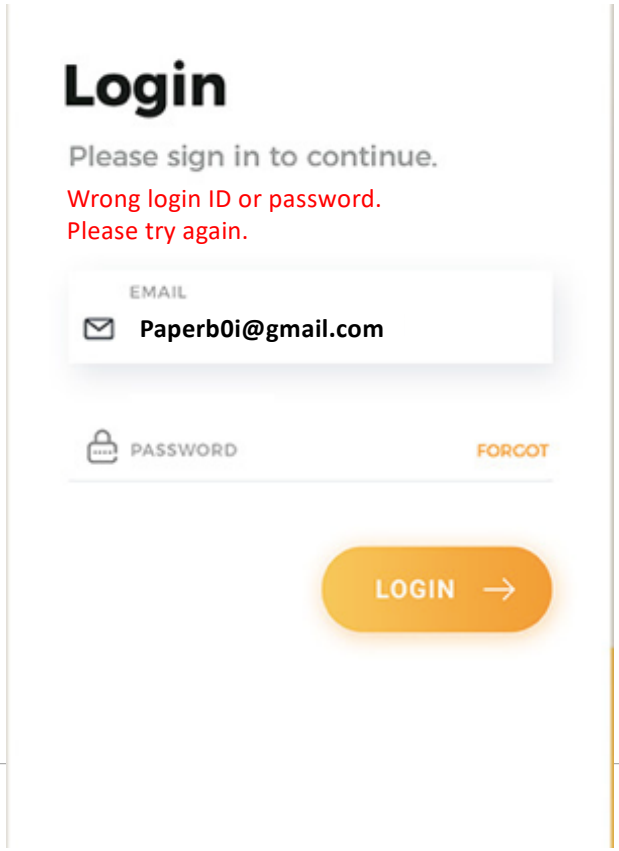
Quiz #4

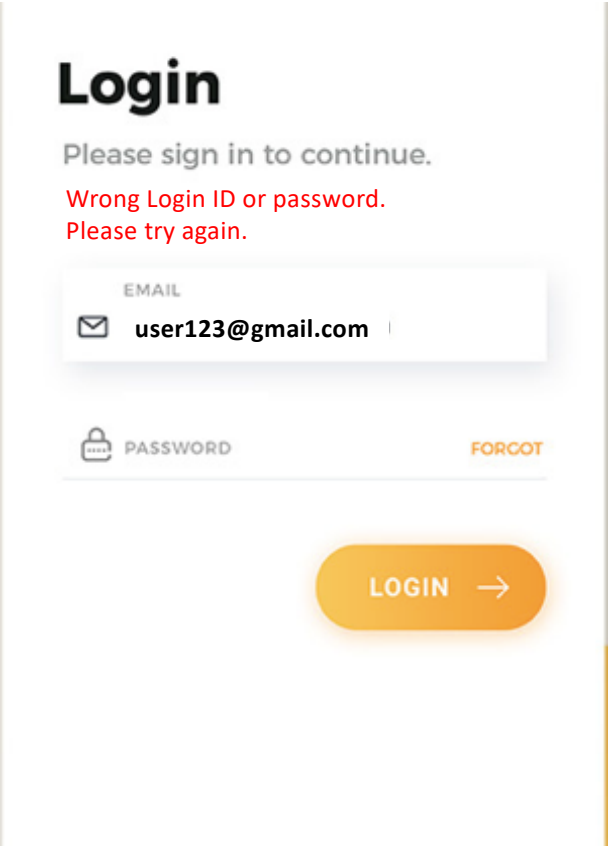
POP QUIZ

i. What class of weakness is this?

a. Cross Site Scripting (XSS)
b. Account enumeration weakness
c. Account spoofing weakness
d. Cross Site Request Forgery (CSRF)

ii. How can this weakness be exploited?





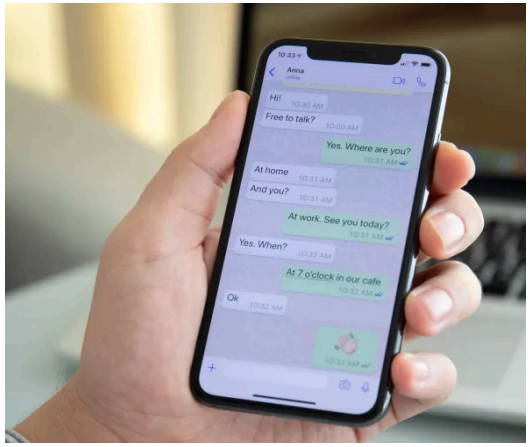
DYNAFENSE
CYBER SECURITY

Picture credits: https://eda.europa.eu/what-we-do/capability-development/cyber

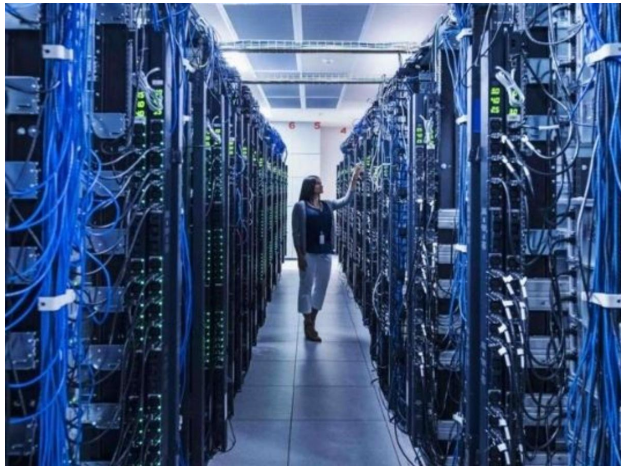
HOW DO DEVICES TALK?

TCP/IP PROTOCOL

Client



Server



Application Layer

Transport layer

Network Layer

Data Link Layer

Application Layer

Transport layer

Network Layer

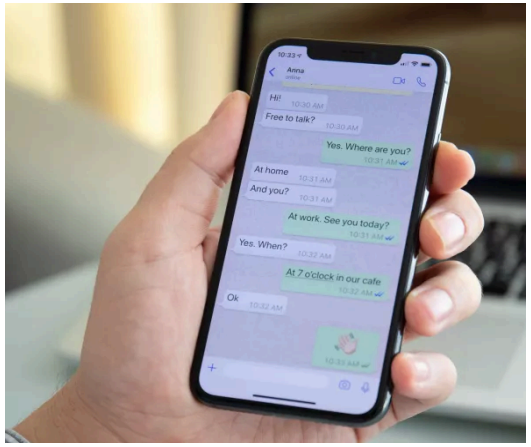
Data Link Layer

Physical Layer (Transfer Medium)

HOW DO DEVICES TALK?

TCP/IP PROTOCOL

Client

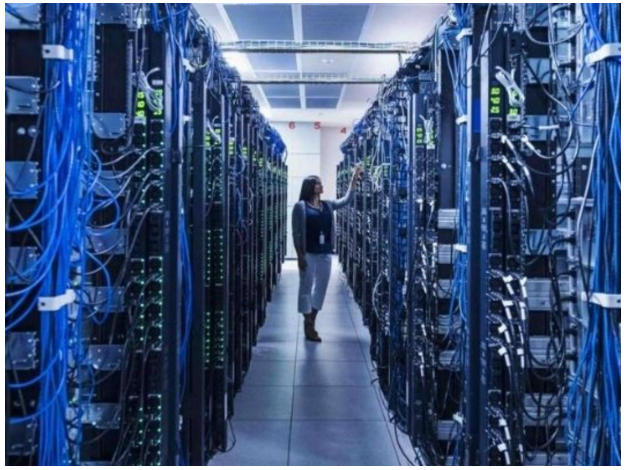


HTTPS

TCP Port: 48293

IP: 192.168.1.49

Server



HTTPS

TCP Port: 443

IP: 66.11.48.54

IPv4 and IPv6

TCP/IP PROTOCOL

TCP	UDP
Ports: 1 - 65535	Ports: 1 - 65535
Connection Oriented	Connectionless

VULNERABILITY ASSESSMENT DEMONSTRATION #1

Using Nessus Professional

NARRATIVE

DEMONSTRATION #1

You are helping your IT Security Engineer to perform a credentialed VA on a newly commissioned IT asset. It is a Windows Server running on a Dell R740.

This was hardened by the vendor before deploying into the production environment.

You need to run a credentialed VA scan to make sure there are no High or Medium findings.

The Windows Server's ip address is 192.168.1.21

PENETRATION TEST #1

Using nmap

NARRATIVE

PENETRATION TEST #1

A newly commissioned Window Server was configured and deployed into the office IT operations.

The owner of the business (Jimmy Yeung) somewhat knows IT security and such prefers to DIY the Windows Server security himself.

He is often away from office.

You, the ever-helpful employee, decided to perform your own security assessment (PT) of the Windows Server after getting his permission.

The Windows Server's ip address is 192.168.1.21

You also know there is a default administrative account created by Windows upon setup called Administrator.

NARRATIVE

PENETRATION TEST #1

Provide details on the users found in the Windows Server.

nmap

PENETRATION TEST #1

Nmap or Network Mapper is a tool used to detect services on servers.

It is very configurable with multiple options. Most common options below

-sS – Send TCP SYN probes

-sU – Send UDP probes

-Pn – Assume all hosts are online (No ping)

-n – Never do DNS resolution

-sV - Probe open ports to determine service/version info

-O - Enable OS detection

-A - Enable OS detection, version detection, script scanning, and traceroute

nmap

PENETRATION TEST #1

Nmap format

```
C:\Users\user> nmap -sS -sU -Pn -n 192.168.1.21
-oA tgt-192-168-1-21
```

Hints

-sS – Send TCP SYN probes

-sU – Send UDP probes

-Pn – Assume all hosts are online (No ping)

-n – Never do DNS resolution

-oA – output results to file name

Nmap format

```
C:\Users\user> nmap –A –Pn 192.168.1.21 –oA tgt-192-168-1-21-all
```

Hints

-sS – Send TCP SYN probes

-sU – Send UDP probes

-Pn – Assume all hosts are online (No ping)

-sV - Probe open ports to determine service/version info

-oA – output results to file name

-A - Enable OS detection, version detection, script scanning, and traceroute

Nmap format

```
C:\Users\user> nmap –sS -sU –Pn –p1-65535
192.168.1.21 –oA tgt-192-168-1-21-all-ports
```

Hints

-sS – Send TCP SYN probes

-sU – Send UDP probes

-Pn – Assume all hosts are online (No ping)

-p – Test these ports

-oA – output results to file name

-O - Enable OS detection

-A - Enable OS detection, version detection, script scanning, and traceroute

hydra

PENETRATION TEST #1

Hydra is a tool used to test credentials against a service or services (aka brute-force accounts.) This is akin to continuously inserting keys into a lock and checking each key one at a time.

It is very configurable with ability to test a number of services, for example, smb – commonly use for shared folders in Windows environment

ssh – Secure shell, commonly used in Unix environments

rdp – Remote desktop

hydra -l <account name> -P <password list> 192.168.1.21 rdp

-l : *LOGIN NAME* -P : PASSWORD LIST

PENETRATION TEST #2

Data Exfiltration

NARRATIVE

PENETRATION TEST #1

A newly commissioned Window Domain Controller was configured and deployed into the IT operations.

HR also requested for their own Windows Server to store PnC HR data.

You, the new IT Security Engineer hire, are tasked to perform a security assessment of the Windows Servers after getting the COO's permission.

NARRATIVE

PENETRATION TEST #2

The Windows Domain Controller's ip address is 192.168.1.31

The HR Windows server's ip address is 192.168.1.32

You also know there is a default administrative account created by Windows called Administrator.

You found Press Releases on the web, written by Company's Corporate Comms staff. At the end of the Press Releases, you noticed the email addresses were in the format of
[firstname][lastname]@Company.com

NARRATIVE

PENETRATION TEST #2

You googled more and found three of the Company's HR staff had posted their own profiles on LinkedIn. They are:

Sam Yang (HR Executive),

Fish Low (Asst HR Director) and

Apple Lim (HR Director)

PENETRATION TEST #2

How many usernames can you test to login to the Windows Server?

What are the potential Windows Server usernames you can test against?

Nmap format

```
C:\Users\user> nmap –A –Pn 192.168.1.32 –oA tgt-192-168-1-32-all
```

Hints

-sS – Send TCP SYN probes

-sU – Send UDP probes

-Pn – Assume all hosts are online (No ping)

-sV - Probe open ports to determine service/version info

-oA – output results to file name

-A - Enable OS detection, version detection, script scanning, and traceroute

NARRATIVE

PENETRATION TEST #2

Provide details on the users found in each of the Windows Server (if applicable).