Software Security

Ayman Hammouda

Information Security Consultant – Security Meter

WHO AM I ...!!

- 10+ Years in information Security Field

- Alexandria University

- ITI Graduate

- Operation Manager

- Ayman.Yousry@security-meter.com

- Ayman Hammouda

Agenda

- Introduction for Cyber-Security

- Security in Software Development

- Security Application Threats

- Secure Coding

Cyber Security

The act of securing computers, programs, data or networks from potential threats like undeliberate or deliberate data change, unauthorized access, or even destruction. Needless to say, all kinds of businesses that have use information technology need cyber security specialized workers especially those that have confidential data e.g. financial institutions, governmental bodies.

Why do we need Cybersecurity?

The New York Times

Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity

Hacks of OPM databases compromised 22.1 million people, federal authorities say

CNN politics — The Biden Presidency   Facts First   2022 Midterms

Russian hackers behind SolarWinds hack are trying to infiltrate US and European government networks

BLOG POST
OPERATION GHOSTSHELL:
NOVEL RAT TARGETS GLOBAL AEROSPACE AND TELECOMS FIRMS

OPTUS yes

Giant Optus Hack May Swallow a Quarter of Singtel Profits
- Fallout from security breach at phone company Optus grows
- Estimated bill could top $420 million, based on typical costs

Cybersecurity – National Focus

"Cyber power is revolutionising the way we live our lives and fight our wars, just as air power did 100 years ago. We need to build up our cyber capability so we can grasp the opportunities it presents while ensuring those who seek to use its powers to attack us and our way of life are thwarted at every turn," prime minister Boris Johnson.

Global Britain in a competitive age
The Integrated Review of Security, Defence, Development and Foreign Policy

"It is the policy of my Administration that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security." president Joseph Biden.

Executive Order on Improving the Nation's Cybersecurity
MAY 12, 2021 • PRESIDENTIAL ACTIONS

المادة 31
أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذي ينظمه القانون.

Cybersecurity Domains

Cryptography

Network Security

Security Operations

OT Security

Application Security

Security Strategy, Risk & Compliance

IOT Security

Digital Forensics

Cloud Security

Data Security

Incident Response

Malware Analysis

Identity and Access Mgmt.
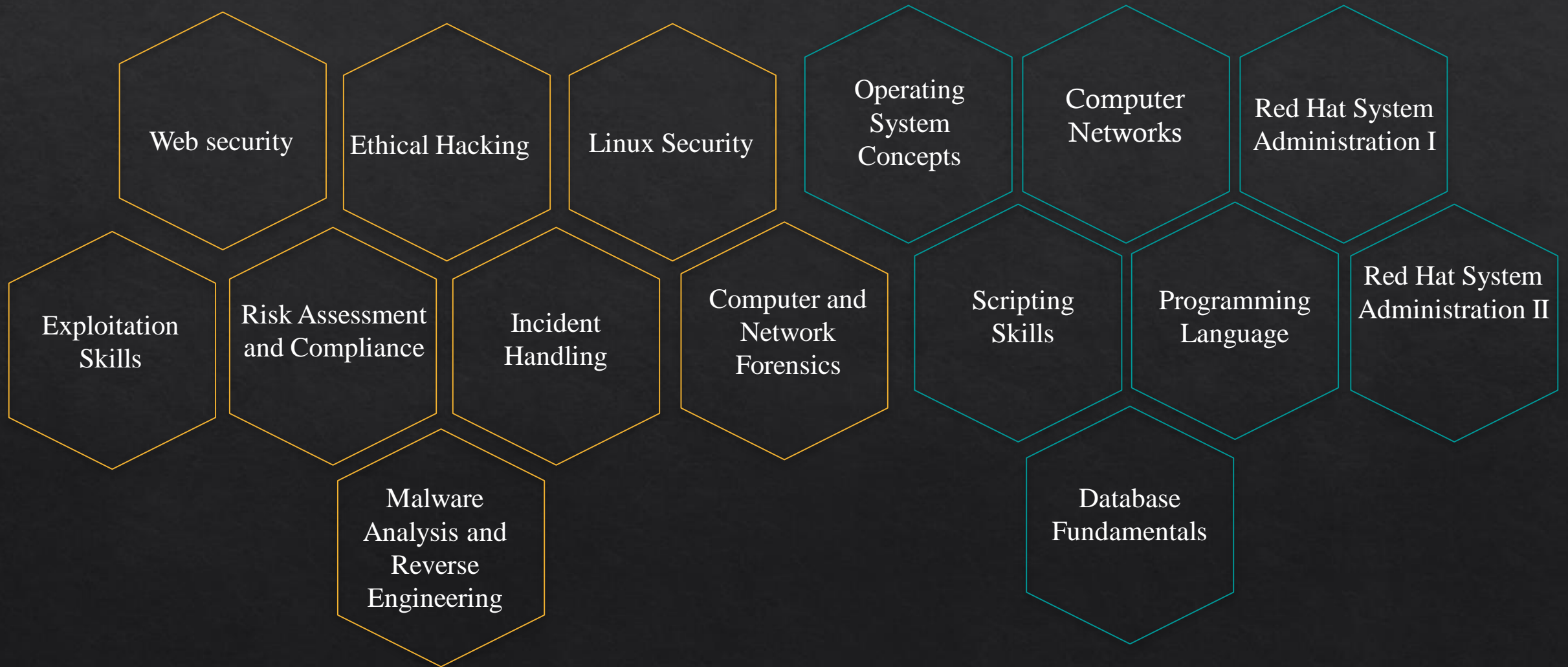
Systems/Host Security

Why work in Cybersecurity?

- It is fun

- It pays well

- You sound cool

- You get to protect others

- Plenty of open jobs, all the time, every where

- And you can do many different things

Cyber Security Market

The following are the major employers for Cyber Security Engineers in Egypt:
- Enterprise Market "Banking, ISPs ..etc"
- Cyber Security Companies-Integrators
- Cyber Security Vendors

How to Start

Web security

Ethical Hacking

Linux Security

Operating System Concepts

Computer Networks

Red Hat System Administration I

Exploitation Skills

Risk Assessment and Compliance

Incident Handling

Computer and Network Forensics

Scripting Skills

Programming Language

Red Hat System Administration II

Malware Analysis and Reverse Engineering

Database Fundamentals

Core Technical Skills

Non-Core Technical Skills

Cyber Security Certificates

Professional Certification

- Security Plus+
- Certified Ethical Hacker
- SANS- GIAC / GSEC 504
- CCNA Security
- OSCP: Offensive Security Certified Professional
- Security Technologies Knowledge
- E-learning

Open Challenges & Resources

There are some good open resources that can be taken to improve your skills:

- CTF and Cyber Olympics
- Open Source Tool (Kali, Black Box)
- Online Challenges (root-me, Hacker one…etc.)
- Udemy, Corsera, Cybrary ..etc
- **Keep up to Dated**

Cybersecurity Concepts – Threat, Vulnerability & Risk

Threat

Vulnerability

Risk

Cybersecurity Concepts – Threat, Vulnerability & Risk
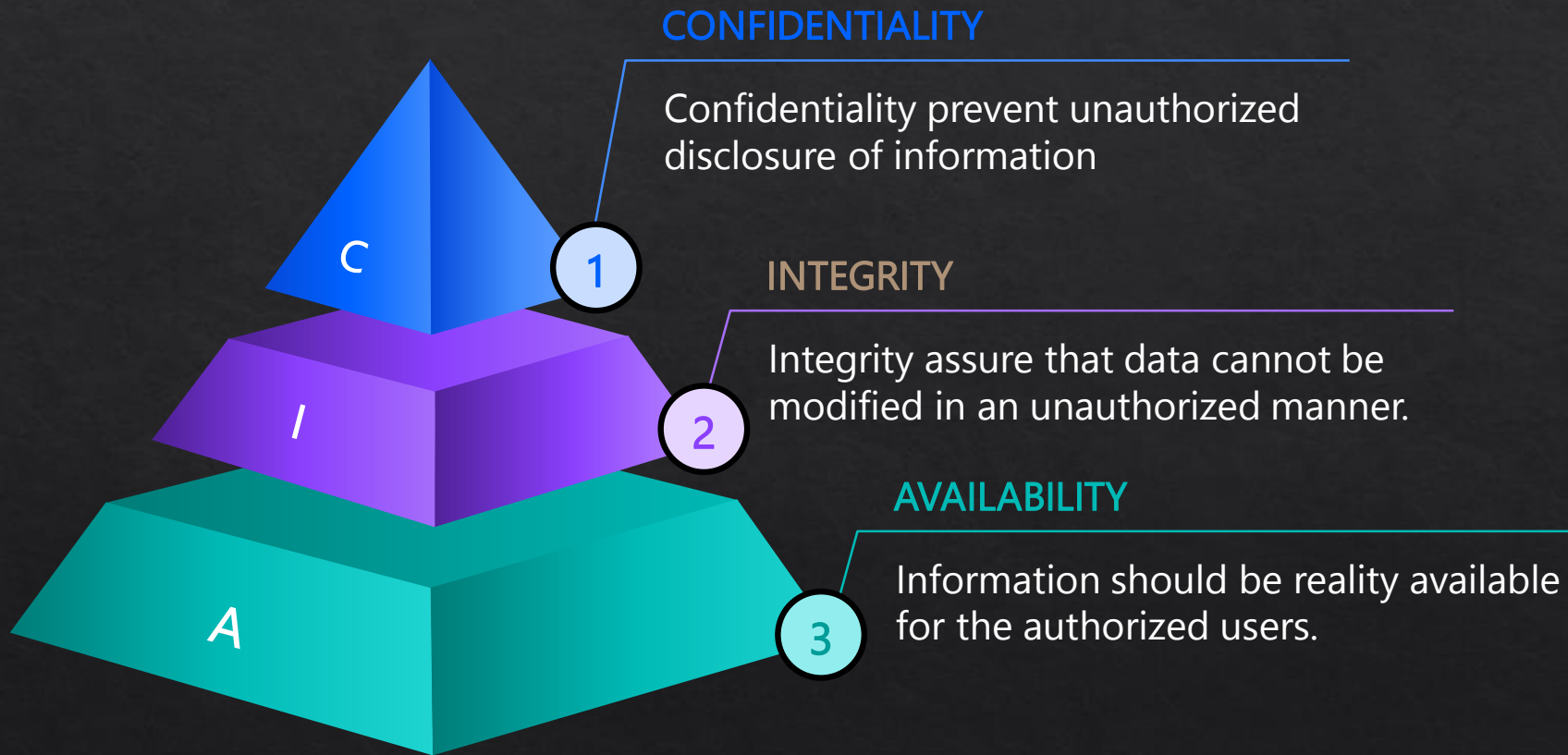
Threat   Vulnerability   Risk

Risk = Threat x Vulnerability

Cybersecurity Concepts – CIA Triad

CONFIDENTIALITY

Confidentiality prevent unauthorized disclosure of information

C

1

INTEGRITY

Integrity assure that data cannot be modified in an unauthorized manner.

I

2

AVAILABILITY

Information should be reality available for the authorized users.

A

3

Cybersecurity Concepts – AAA

◈ Authentication

◈ Authorization

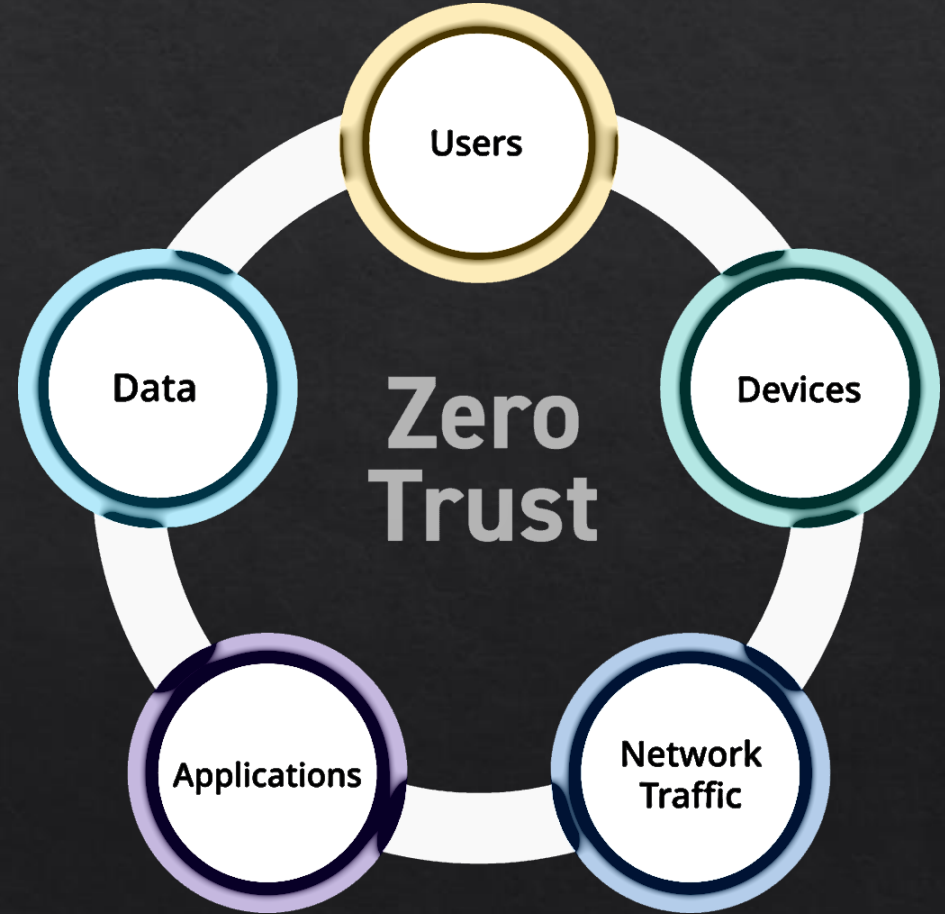◈ Accounting

Authentication

Authorization

Accounting

AAA
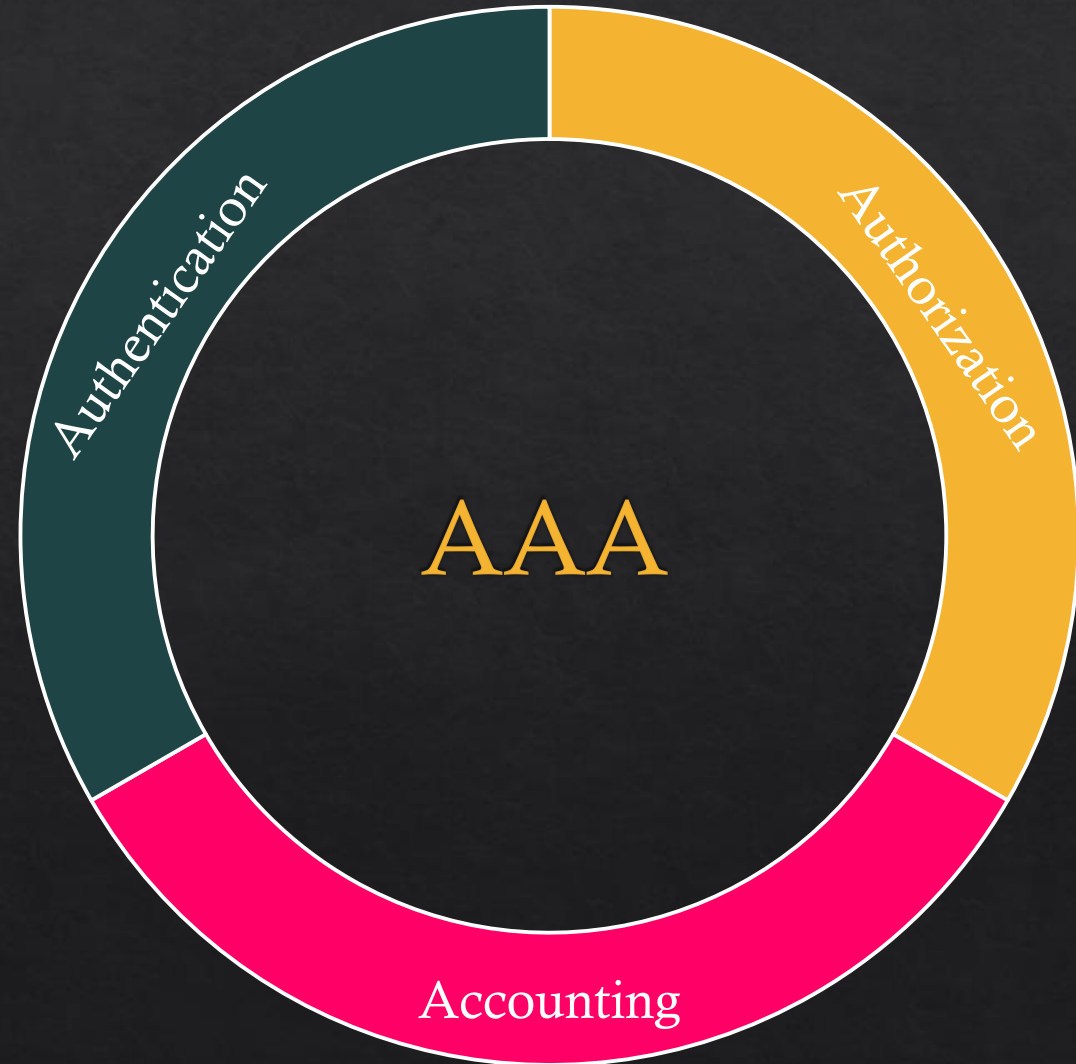
Cybersecurity Concepts – Least Privilege, Need to Know & Segregation of Duties

◈ Least Privilege

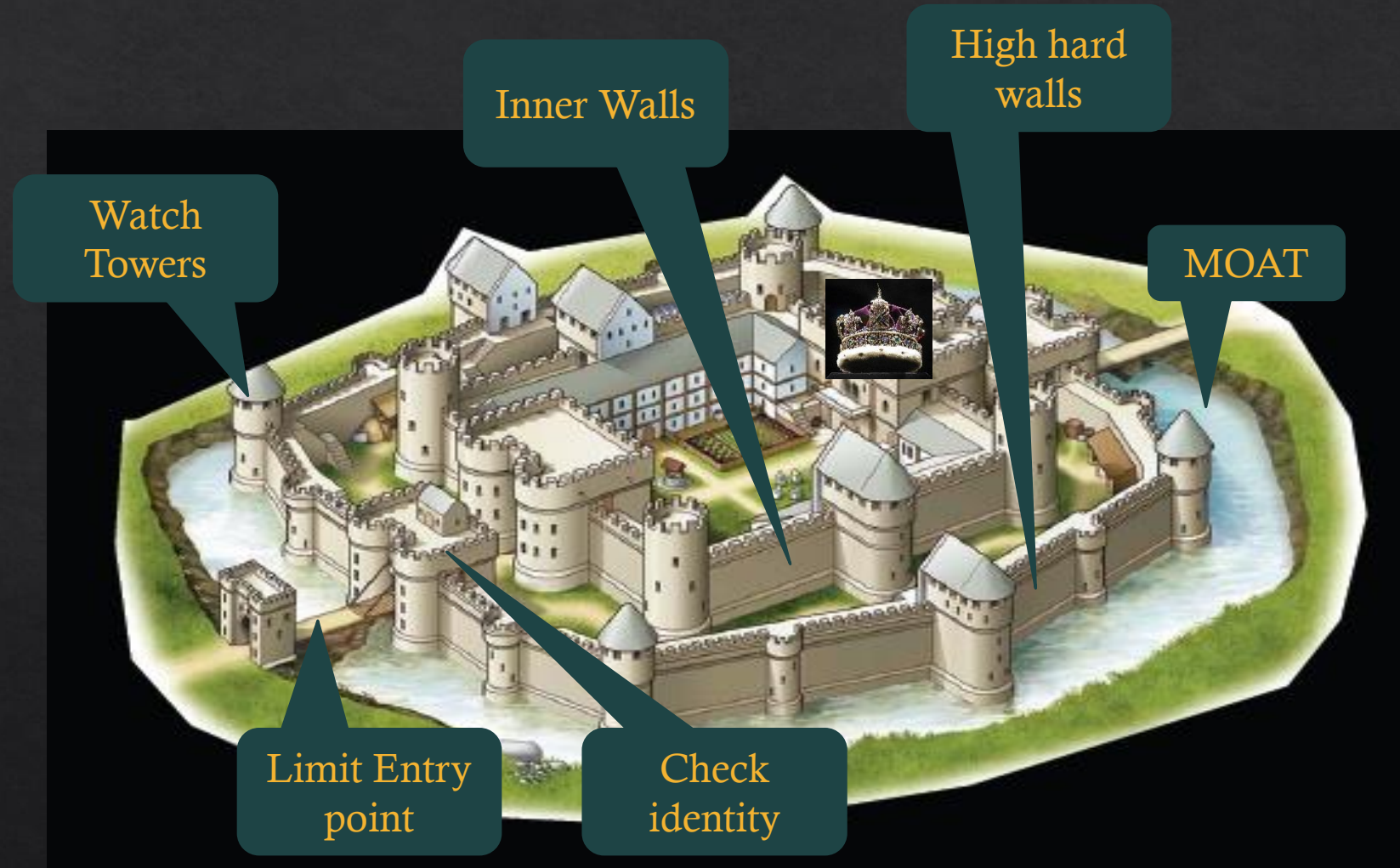◈ Need to Know

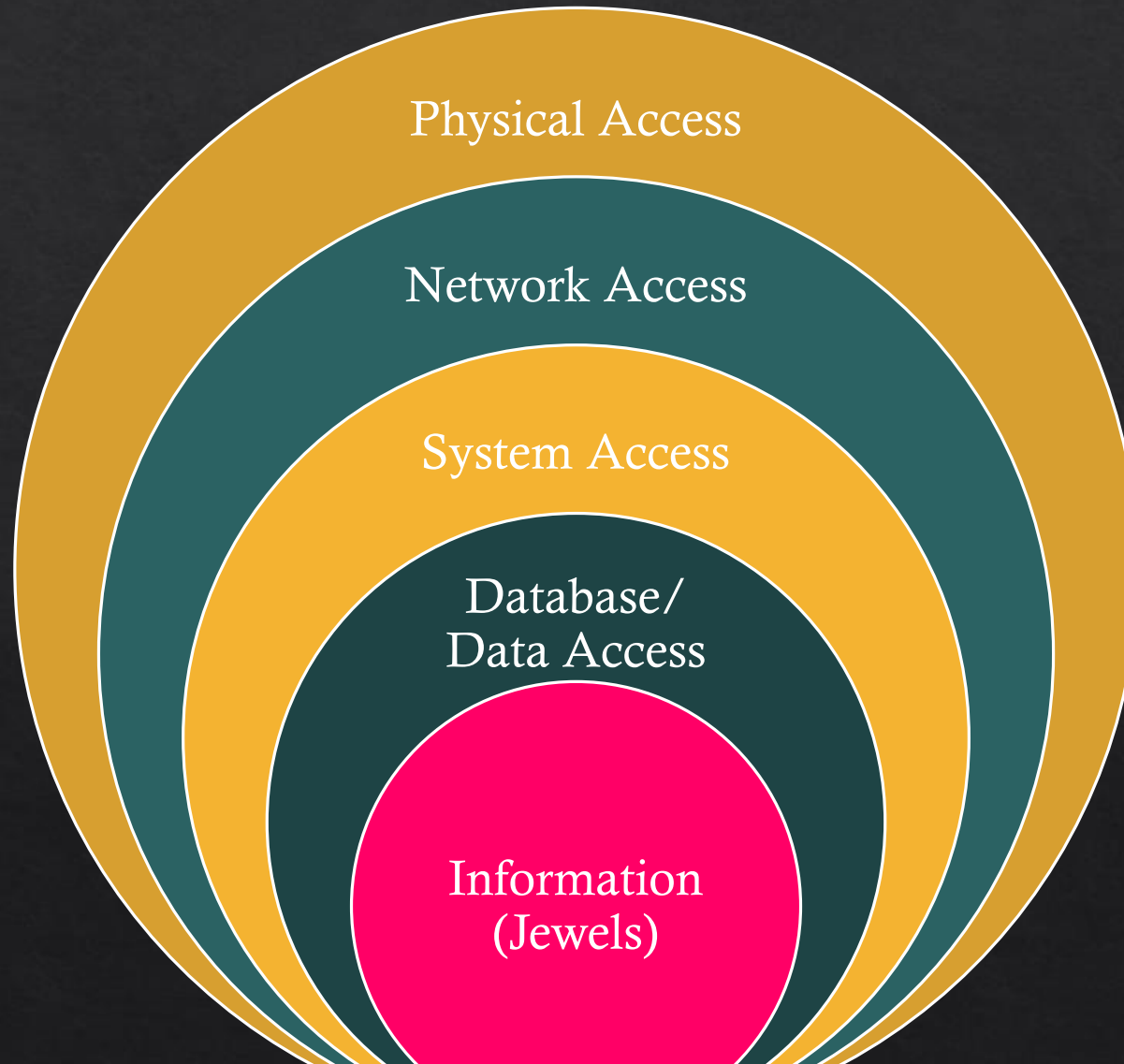◈ Segregation of Duties

Cybersecurity Concepts – Zero Trust

◈ Redefine the Perimeter

◈ Implement Least Privilege

◈ Never Trust, Always Verify
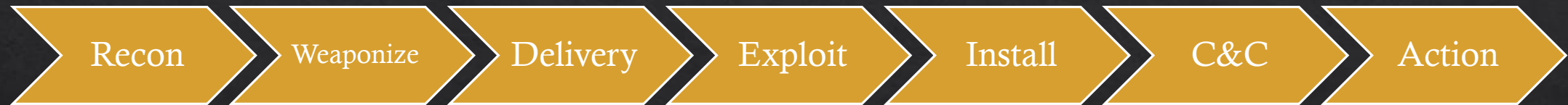
◈ Assume Breach

Concept – Defense in Depth

Concept – Defense in Depth

Physical Access

Network Access

System Access

Database/
Data Access

Information
(Jewels)

Concept – Kill Chain

Recon → Weaponize → Delivery → Exploit → Install → C&C → Action

RECONNAISSANCE   DELIVERY   INSTALLATION   ACTIONS ON OBJECTIVES

WEAPONIZATION   EXPLOITATION   COMMAND & CONTROL (C2)

Remember the Kill Chain

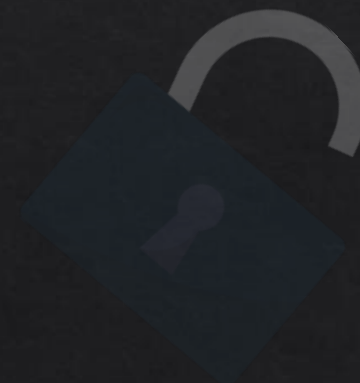| Recon	Weaponize	Delivery	Exploit	Install	C&C	Action

Lie Mislead Divert Deceive Obfuscate Disrupt Delay

Thanks

Questions ?