

# INTRODUCTION TO OFFENSIVE & DEFENSIVE TECHNOLOGIES

KAMILIMU COHORT 9 – CYBERSECURITY



# TABLE OF CONTENTS

**01**

CHECK-IN

**02**

WORLD OF CYBER SECURITY PT.1

**03**

WORLD OF CYBER SECURITY PT.2

**04**

INTRO TO OFFENSIVE/DEFENSIVE  
TECHNOLOGIES

**05**

OFFENSIVE SECURITY - THE  
JOURNEY

**06**


DEFENSIVE SECURITY - THE  
JOURNEY

**07**

HANDS-ON LAB: OFFENSIVE  
(BREAKERS)

**08**

HANDS-ON LAB: DEFENSIVE  
(DEFENDERS)





How are you  
doing?



# The world of cyber security – fields

## Offensive security

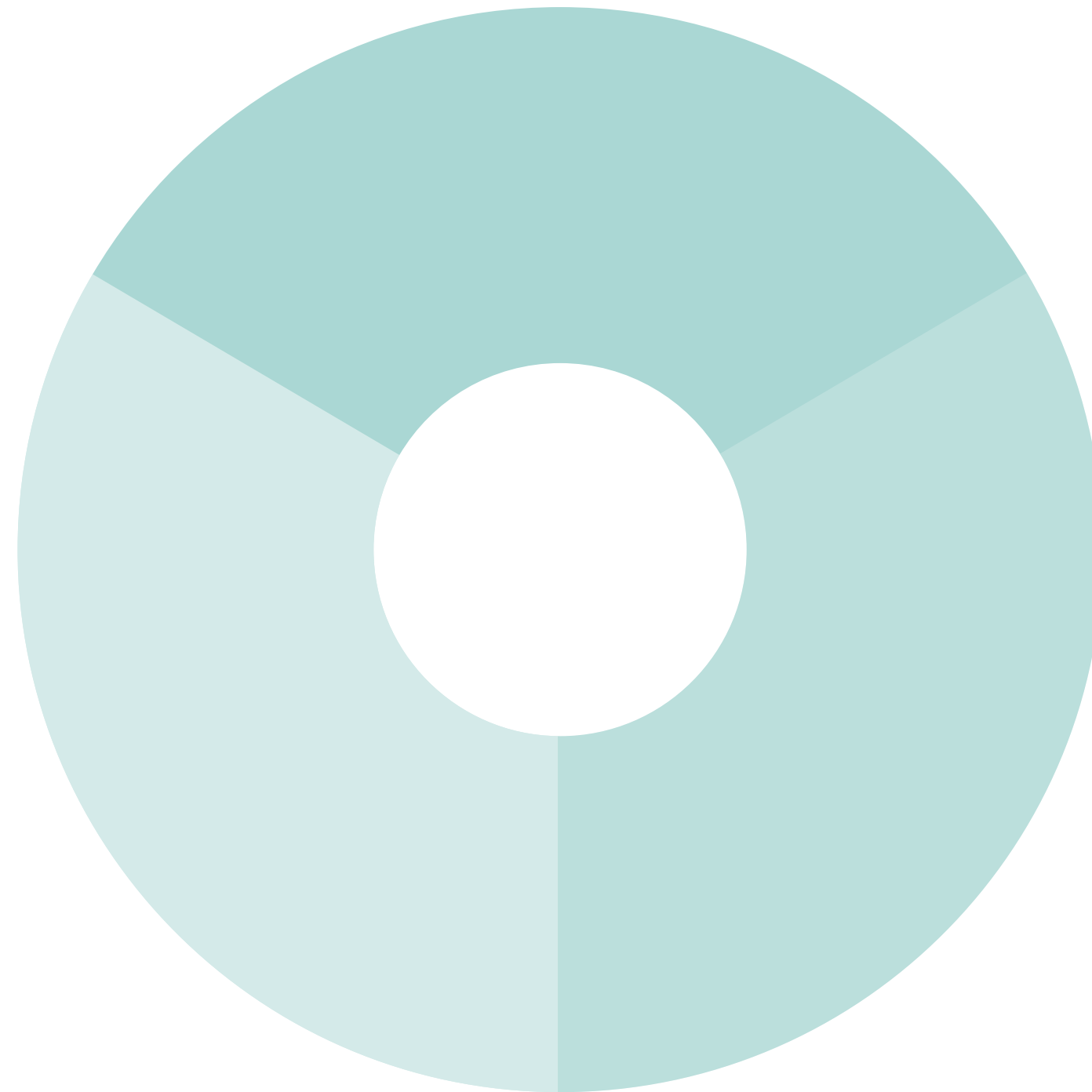


Also known as the “red team” or black/white/grey hackers. They work to find bugs in technology.

## GOVERNANCE (GRC)



A broad term capturing Governance (management), risk and compliance. What companies are expected to do by the law.



## Defensive security



Also known as the “blue team” or “purple team”. They work to protect against the “bad” guys in security.

## Forensics/Incident Response (DFIR)



This field deals with assessing what went wrong after an attack or “incident”.

# The world of cyber security – channels

**IOT security**

**API security**

**Web/mobile security**

**Network security**

**Blockchain security**

**Quantum security**

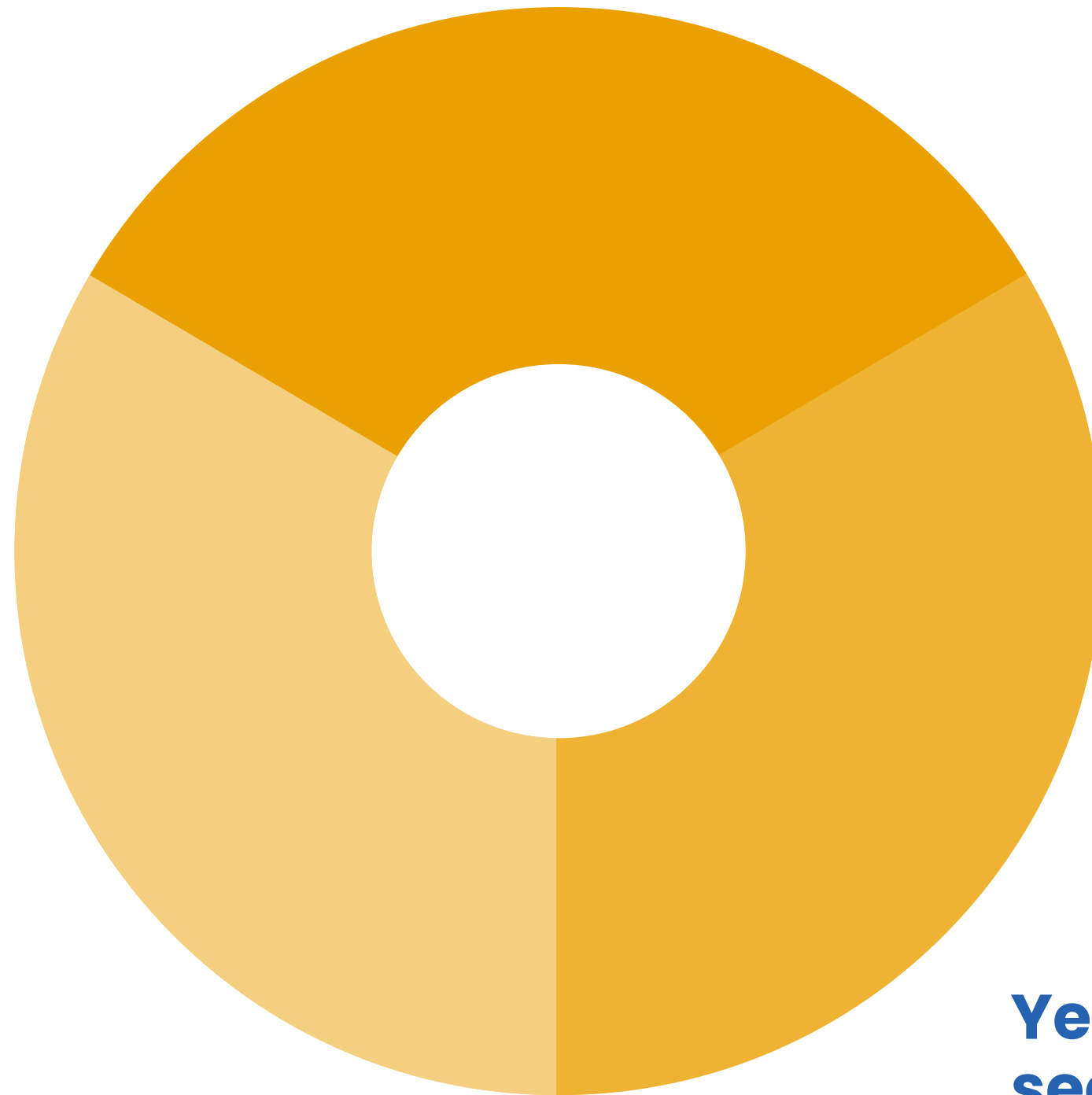
**Wireless security**

**Hardware security**

**Enterprise security**

**Cloud/AI/ML security**

**Yet to be found... security**





A close-up, low-angle shot of a computer keyboard with blue backlighting. The keys are dark, and the light creates a strong glow around the edges of the keys. The focus is sharp on the keys in the foreground, showing details like the 'TAB' key with its arrow icons and the 'CAPS LOCK' key. The background keys are blurred, creating a sense of depth.

# Offensive & Defensive technologies

How do you “break” “channels”?

&

How do you protect your assets from being broken?

# Offensive security

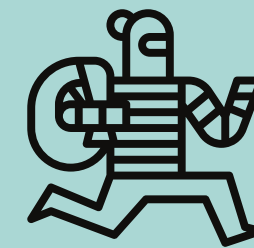
Generalized pathway



## Reconnaissance/Information gathering

How do you know where you are and what is available for attack?

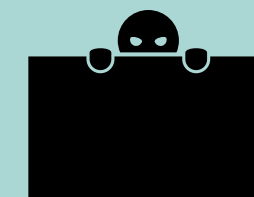
**Tools:** nmap, wfuzz/gobuster/dig/ping etc.



## Exploitation

Find and attack weaknesses identified within the asset.

**Tools:** burpsuite, hydra, metasploit, netexec



**Post exploitation** – cover your tracks, hide, etc.

Most actors will try and ensure they are not caught in this stage. Another aspect here is also reporting “white hat” for hackers.

**Tools:** AMSI bypass, etc.



### **Detection/Information gathering**

Finding the breach and assessing logs and data for how this was done.

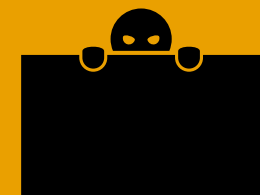
**Tools:** SIEM, Wireshark, EDR tech, IDS/IDP



### **Analysis & containment**

Understand the full scope of the breach and isolate the system/app.

**Tools:** Forensics tools, VirusTotal, ACL (block lists)



### **Treatment, recovery and restoration**

Locking down the malicious activity and removing it from systems.

**Tools:** backup and restore tooling etc.

# Defensive security

Generalized pathway



# Playground: Breakers

Offensive security  
lab: *Offensive  
Security Intro*



# Playground: Defenders

Defensive security lab:  
*Defensive Security intro*



# Bonus playground: Active Directory

Active Directory lab:  
breachingad



# Thank you!

QUESTIONS?