

---

# Cybersecurity

## From Zero to Hero

Mohammad Khreesha  
Cybersecurity Manager

<https://technawi.net>

# Whoami

- 13+ Years of IT & Infosec Experience.
- Cybersecurity Manager [at] Baaz Inc..
- Cybersecurity Trainer.
- OWASP Amman Chapter Leader.
- Youtuber, Blogger, & CTF Maker.
- CEH, CHFI, ECSA, LPT master, OSCP, CRTP, eCPPT, eCPTX, eWPT, eWPTX, eMAPT, ISO 27001 LI Certified.
- Top Arab Cybersecurity Social Media Influencer (2019, 2020, & 2021).





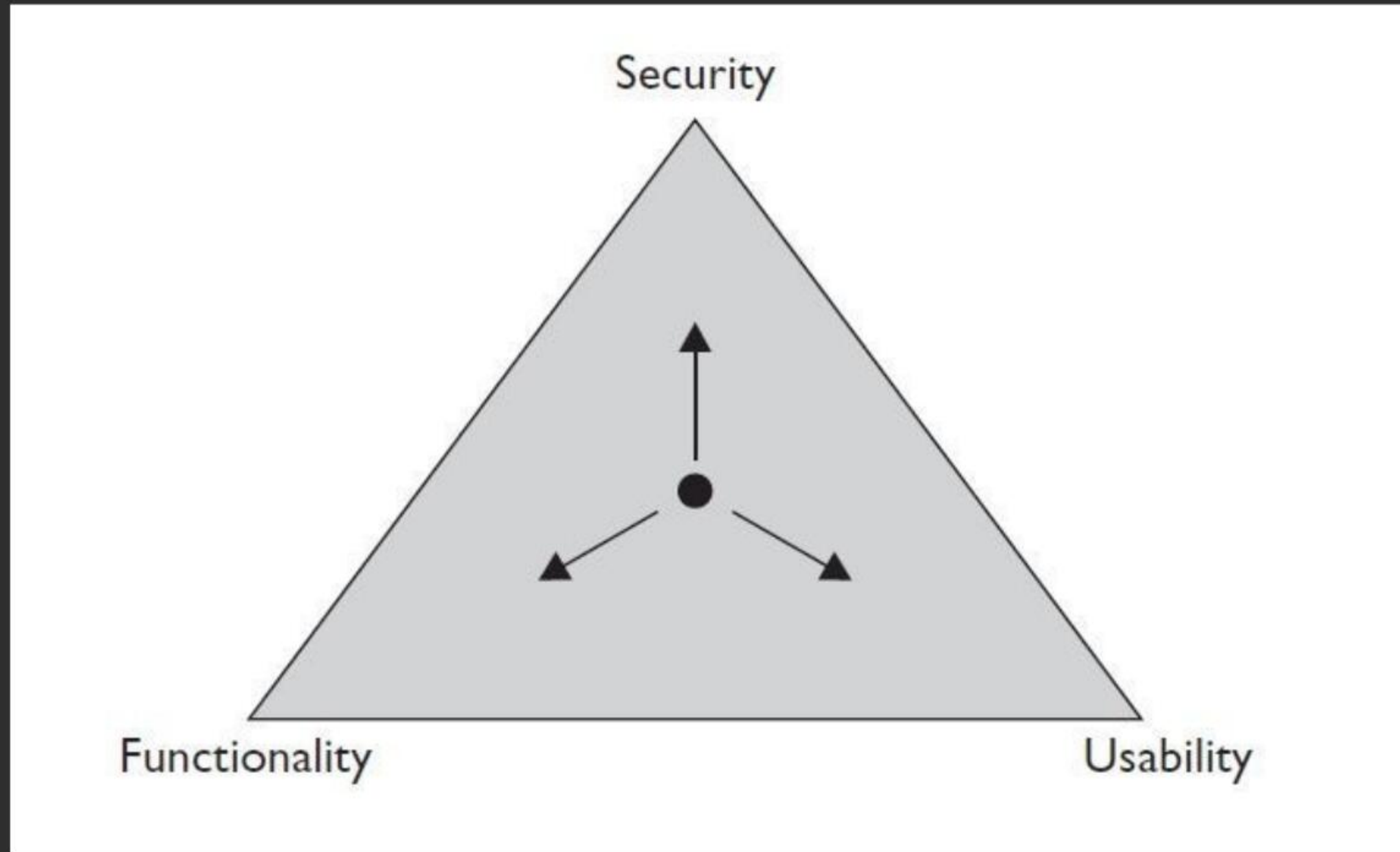
# Table of Contents

- Introduction to Cybersecurity.
- Cybersecurity Paths.
- Cybersecurity Skills.
- Cybersecurity Certificates.
- Cybersecurity Resources.
- Q&A.

# Introduction to Cybersecurity

- Cyber Security is the practice of protecting our electronic data by preventing, detecting, and responding to cyber attacks.
- Cyber Security effects on :
  - Political Systems
  - Countries Infrastructures ie. : Electric, Gas Stations, .... etc
  - Companies
  - You Privacy
  - ... etc
- This means that it affects your life

# Continue..







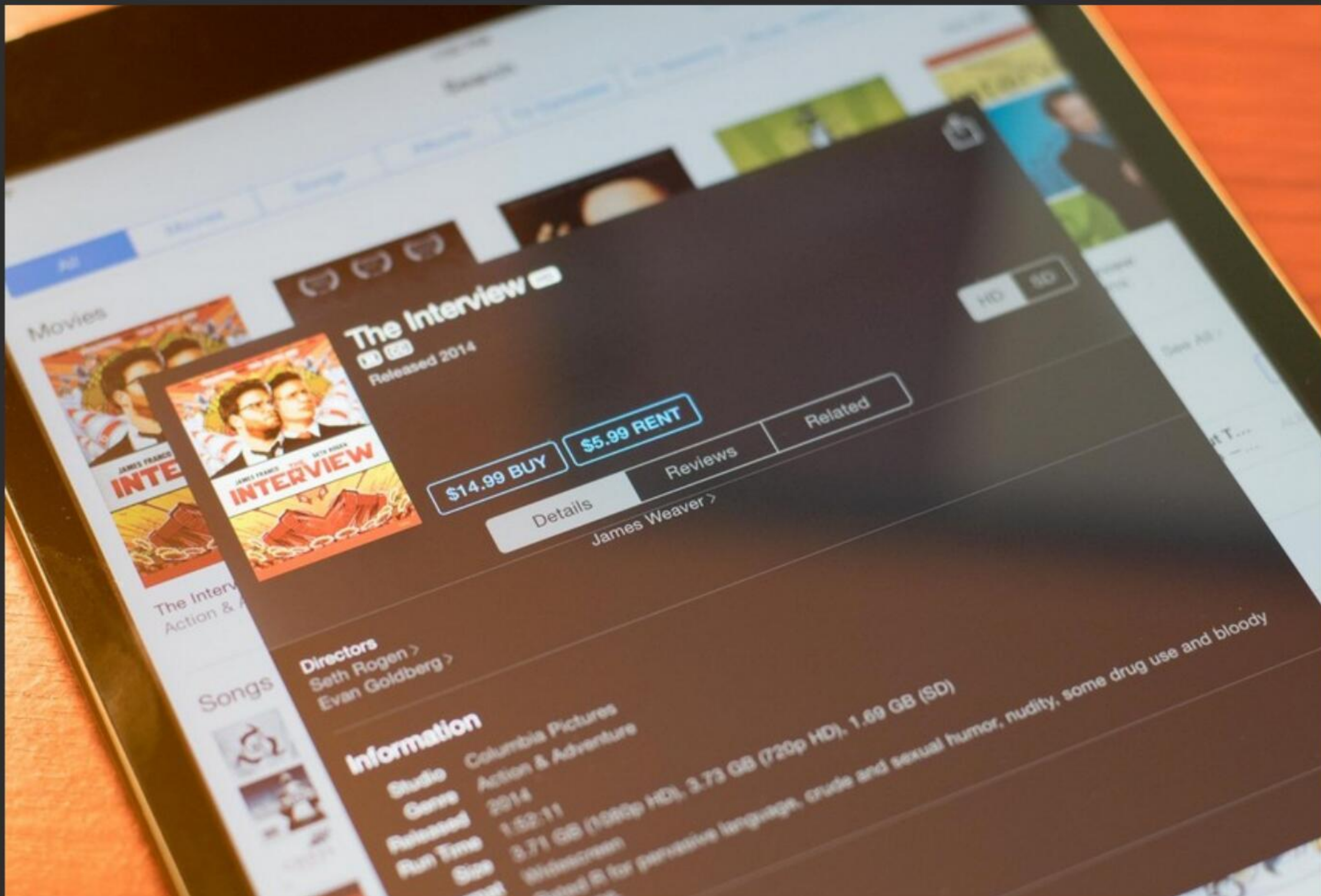
[https://en.wikipedia.org/wiki/Bob\\_Quick\\_\(police\\_officer\)](https://en.wikipedia.org/wiki/Bob_Quick_(police_officer))





<https://www.businessinsider.com/biometric-fingerprint-password-hacking-2015-1>





[https://en.wikipedia.org/wiki/Sony\\_Pictures\\_hack](https://en.wikipedia.org/wiki/Sony_Pictures_hack)

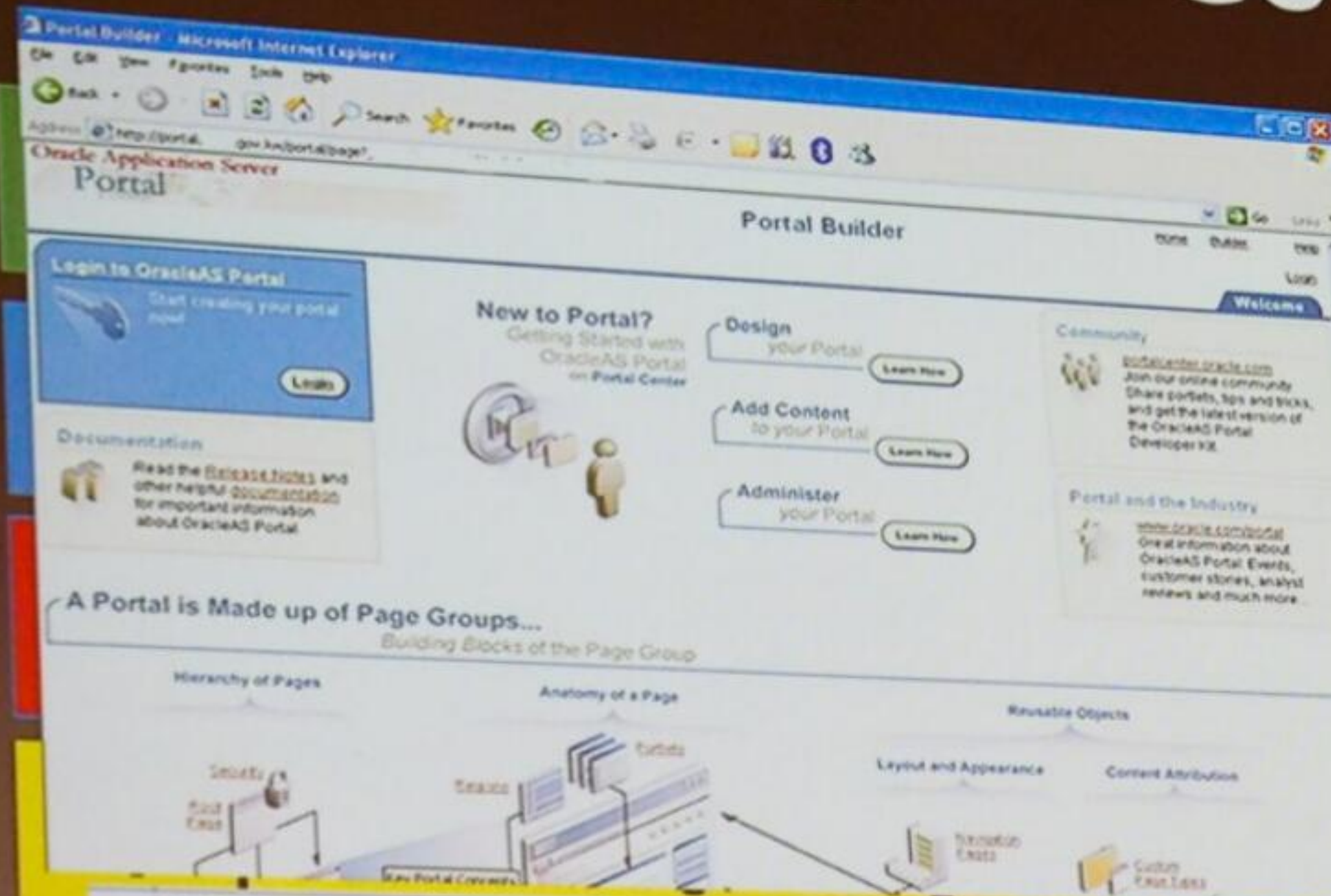




# Owning the Government



NO Bribes



## Ministry of Justice - Usernames & Passwords

Username	Password
amjad	ebz
blueman	f123
ebtehal	msh
fatma	shaik

## Ministry of Defence - Usernames & Passwords

Username	Password
mgholoum	mona
mbaqer	manal
ejaleel	entesar
sfalou	safwan
mmetwally	mohammed
Imohammad	layla
eshemary	eshemary
admin	admin
aghimlas	adlah
osama	osama

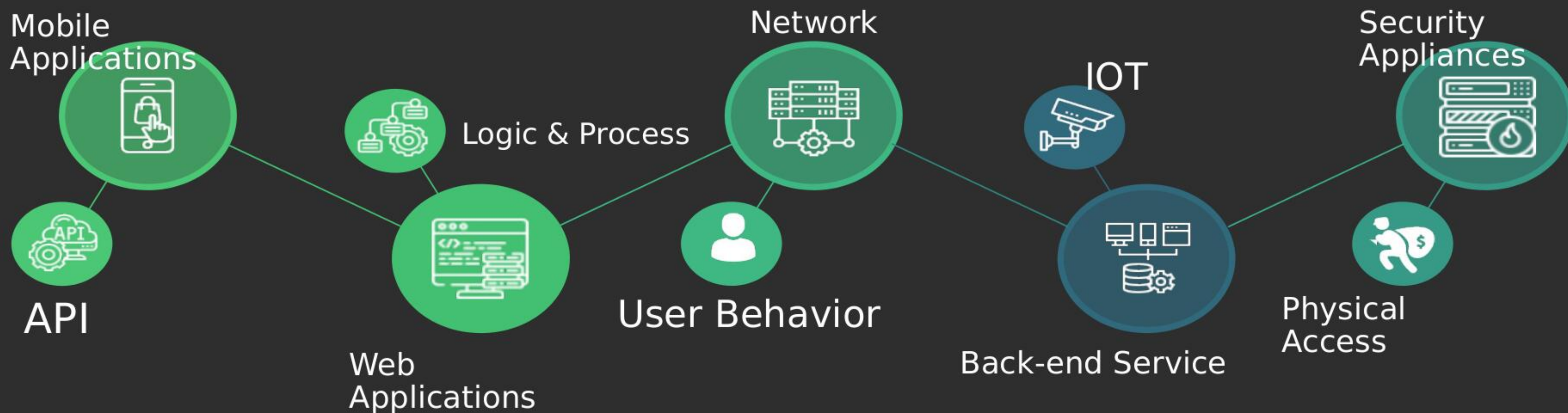
## Database Schema

- ☒ DEVELOPMENT
  - ☐ master
  - ☐ tempdb
  - ☐ model
  - ☐ msdb
  - ☐ pubs
  - ☐ Northwind
  - ☐ \_NEW
  - ☐ Finance\_Emp\_Affairs
  - ☐ CAREER
  - ☐ Comp\_ \_Affairs
  - ☐ COMP\_REG
  - ☐ Emp\_Evaluation
  - ☐ PHONES
  - ☐ ect\_clients
  - ☐ new\_printers
  - ☐ Contracts\_Dept
  - ☐ Contracts
  - ☐ Planning
  - ☐ QualityControl

<https://www.youtube.com/watch?v=m1lhGqNCZIA>



# Complete Security





# Cybersecurity Paths

- Defensive (Blue Teaming)
  - Security Operation Center
  - Security Architecture
  - DFIR
  - Threat Hunting
  - Threat Modeling
- Offensive (Red Teaming)
  - Pentesting
  - Source Code Review
  - Threat Emulation
- Governance & Management
  - Policies
  - Procedures
  - Compliance



# Security Operation Center (SOC)

- Budget on Prevention vs on Detection
- While Prevention is Ideal, Detection is a MUST!
- Better Visibility
- SOC Analysts are those who :
  - Detect.
  - Analyze.
  - Respond to..
  - Report on..
  - And Prevent, cyber security incidents.



# Continue..

- SOC Job Titles:
  - Intrusion Detection Analyst
  - SOC Analyst / Engineer
  - CERT Member
  - Cyber Threat Analyst
- SOC Jobs Certificates :
  - EC-Council Certifications (CEH, CSA, CTIA, ECIH)
  - CompTIA Certifications (Security+)
  - SANS GIAC Certifications (GSEC, GCIH, GCIA, GMON)
  - ISC2 Certifications (SSCP)





# Incident Response

- Methodology:
  - Preparation, Identification, Containment, Eradication, Recovery, Lesson Learned.
- Certifications Related to IR Jobs:
  - EC Council Certifications (ECIH)
  - SANS GIAC Certifications (GCIH, GCIA, GCFA, GREM)



# Digital Forensics

- Law and Order of Information Security
- Digital Evidences are extremely Volatile
- Chain of Custody (Continuity of Evidence)
  - Evidence has been (Gathered, Processed, handled and stored) without alteration.
- Job Titles :
  - Computer Crime Investigator
  - Insider Threat Analyst
  - Law Enforcement
  - Digital Investigation Analyst
- Certifications :
  - EC Council Certifications (CHFI)
  - SANS GIAC Certifications ( GCFE, GCFA, GREM)
  - eLearnsecurity (eCDF)



# Governance & Management

- Governance determines who is authorized to make decisions.
- Governance: doing the right thing
- Management: doing things right.
- Jobs : CISO, Security Manager, Security Director

Management	Governance
Implementation	Oversight
Authorized to make decisions	Authorizes decision rights
Enforce policy	Enact policy
Responsibility	Accountability
Project planning	Strategic planning
Resource utilization	Resource allocation



# Security Audit

- It is a manual or systematic measurable technical assessment of a system or application.
- Usually the audit will be against standards, benchmarks, best practice and framework or process.
- Jobs : Auditor, Lead Auditor, Audit Manager
- Some of the standards in security the audit is happening against it:
  - ISO 27001 ( ISMS – Information Security Management System)
  - PCI DSS (The Payment Card Industry Data Security Standard)
  - HIPAA (Health Insurance Portability and Accountability)
  - ISO 22301 business continuity management system (BCMS)



# Risk Assessment

- It is the process of understanding and responding to factors that may lead to a failure in the confidentiality, integrity or availability of an information system.
- Security Risk Assessment can be implemented base on different standards and approach like: ISO 27005/ ISO 31000 / NIST / Cobit 5 for risk.
- Jobs : Risk Assessor, Risk Officer, Risk Manager



# Pentesting

- Exploits security vulnerabilities in web-based applications, networks and systems.
- They use a series of penetration tools – some predetermined, some that they design themselves to simulate real-life attack.
- Responsibilities :
  - Perform formal penetration tests
  - Design and create new penetration tools
  - Web, Mobile, Network, IoT, SCADA, ...etc.
  - Help the customer fix the vulnerabilities.
  - Social Engineering.
  - PT is not about zero-days.

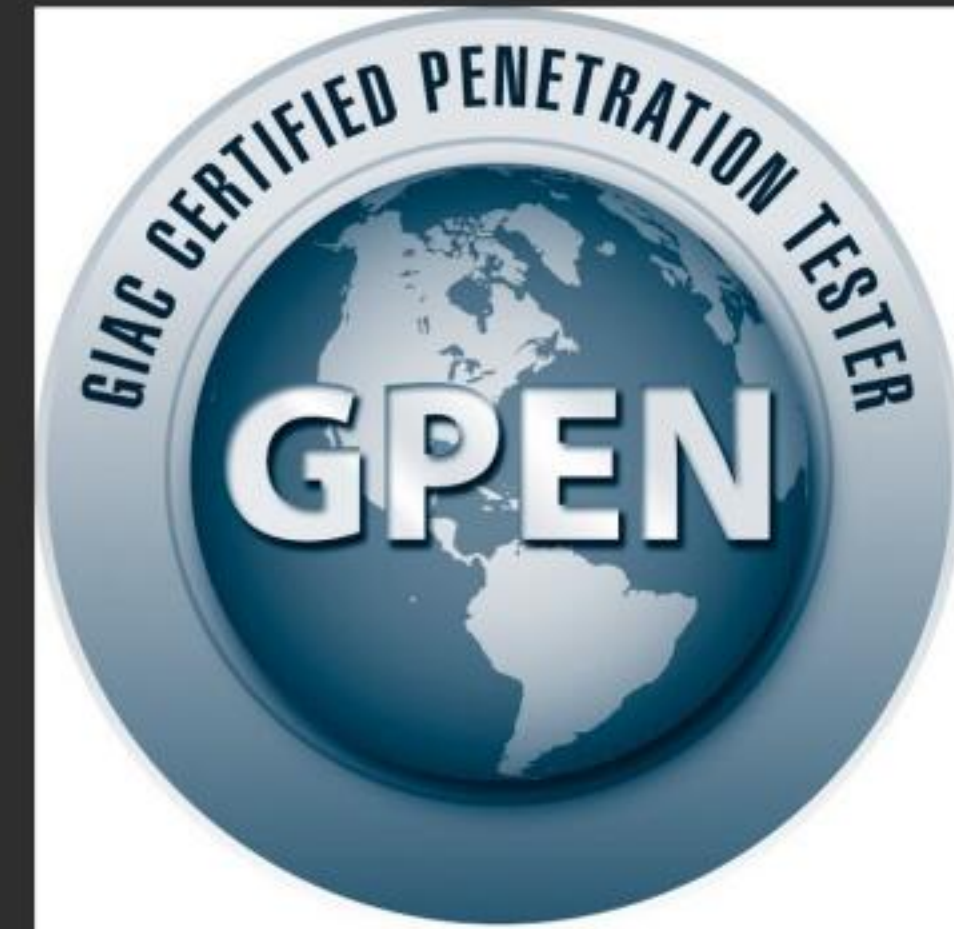
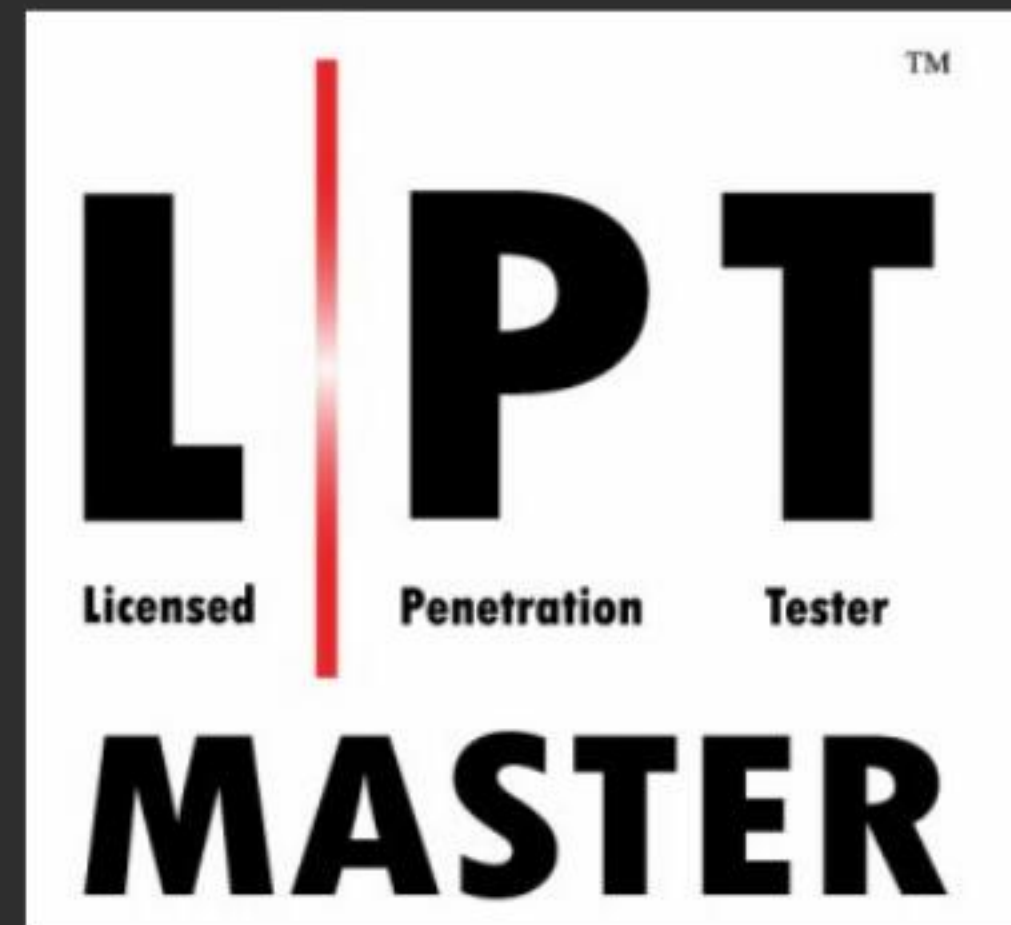


# Continue..

- Skills :
  - Computer Skills
  - Networking Skills
  - OS Skills (both Windows & Linux)
  - Infosec knowledge
  - Programming Skills
  - CTF Competitions



# Continue..





# Golden Rule

**“The best way to learn new things in your field is to teach them to others”**



# Any Questions, Comments or Concerns?

## Thank you!

Website : <https://www.technawi.net>

Linkedin : <https://www.linkedin.com/in/mohammad-khreesha-97b324a2/>

Twitter: @banyrock

Facebook : <http://www.fb.com/khreesha>

Youtube : <https://www.youtube.com/technawidotnet>

Email: [khreesha@technawi.com](mailto:khreesha@technawi.com)