Summary	
Department	Digital & Innovation- Cyber
Sub Department	Cyber Security- Cyber Defense
Job Title	Analyst/ Associate/ Sr. Associate/Consultant/ Sr. Consultant
Location	UAE- Dubai & Abu Dhabi
Experience	0-5 years

About Us

Known for being a great place to work and build a career, KPMG provides audit, tax and advisory services for organizations in today's most important industries. Our growth is driven by delivering real results for our clients. It's also enabled by our culture, which encourages individual development, embraces an inclusive environment, rewards innovative excellence and supports our communities. With qualities like those, it's no wonder we're consistently ranked among the best companies to work for. If you're as passionate about your future as we are, join our team.

KPMG Lower Gulf (the UAE member firm of KPMG International) offers a comprehensive compensation and benefits package. KPMG is an affirmative action-equal opportunity employer. KPMG complies with all applicable local laws regarding recruitment and hiring. All qualified applicants are considered for employment without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, disability, protected veteran status, or any other category protected by applicable federal, state or local laws.

About the practice

Digital & Innovation- Cyber – KPMG helps clients' identity and mitigate risks while discovering new opportunities to create value. Our end-to-end risk services span across all domains across financial services, health care, Oil & Gas and government entities ranging from managing strategic risks in the C-Suite to improving board oversight as well as balancing financial and environmental policies to addressing cyber threats.

Platform / Market Offerings – Cyber Security and Defense

- Our flexible, pragmatic and independent approach to managing cyber security means that we work with organizations – from network to boardroom – to address constantly changing threats. We ensure that our clients can continue to take advantage of the benefits of digital business without worrying about the potential pitfalls.
- While every organization's needs are different – and we tailor our approach accordingly – KPMG offers a range of services that cover the three critical elements of effective and agile cyber security: Aware, Prepare & Respond.

Job Purpose

- Lead projects in cyber security across technical engagements including vulnerability assessment and penetration testing.
- Play subject matter specialist role in presenting observations, description, severity, risk and optimized mitigation controls to the client based on the assessments
- Have good communication and project management/ reporting skills for client engagements across working along or leading small project teams

Roles and Responsibilities

Candidate should have deep experience across the following technical sub-domains with proven expertise (as applicable) along with out of the box thinking ability

- **Application Security**
  - ✓ Expertise in performing thorough application security engagements across **Web applications, APIs, thick clients and mobile applications** (as applicable) and deep knowledge across both black box and grey box penetration testing- using manual testing and automated scanners
  - ✓ Ability to identity and present threats along with providing optimized recommendations as per client environments.
  - ✓ Should be able to understand written code across common languages (Java, C, PHP etc.) to perform white box security testing (**Source code review**) – using a combination of manual and automated tools
  - ✓ Should be familiar with tools including but not limited to Burp Suite, Nessus, Acunetix, Net Sparker, SQLMap etc.
- **Network Security**
  - ✓ Exposure to performing thorough infrastructure/network vulnerability assessment and penetration testing (including real-world exploitation) for internal and external environments- using manual testing and automated scanners over wired and wireless configurations across IT/OT and IoT Networks (as applicable)
  - ✓ Should hold strong basic concepts in network and how to optimize tools and scripts to perform scanning and exploitation as per client environments
  - ✓ Should be familiar with network vulnerability assessment and penetration testing technologies and tools including but not limited to Nessus, Nmap, OpenVas, NeXpose and Qualysguard etc.
  - ✓ Ability to fine-tune/ develop attack scripts using powershell, python based on client environments to execute agreed attack scenarioss
- **Network Architecture and Configuration Review**
  - ✓ Knowledge in understanding network architecture with a combination of network diagrams as well as on-site reviews from security perspective
  - ✓ Ability to read configuration files of network devices (across switches, routers, firewalls etc.) using mix of automated tool based report and manual inspection
- **Red Teaming/ Social Engineering**
  - ✓ Candidate should have knowledge across frameworks such as CREST, MITRE etc., and be able to explain red teaming concepts and attack vectors for environments
  - ✓ Ability to comprehend a client network and setup social engineering infrastructure to perform relevant assessments.
- **Preferred knowledge across emerging technologies**

✓ It is preferred that candidate have some basic knowledge across any emerging technology across OT/IoT/ Blockchain/ SecDevOps and Cloud technologies etc. (as add-on)

Person Specifications	
Education	Graduation/ Post graduation in computer science/ engineering
Desired Certifications	CEH/ OSCP/OSCE/ GWAPT/LPT/GMOB/ESSA/CISSP and other relevant certifications'
Skills and Abilities	1. Excellent written and communication skills 2. Ability to work in a collaborative team environment/ lead smalls teams on projects 3. Familiarity with scripting language (powershell, python etc.) 4. Good presentation and reporting skills in technical and business language 5. Project management skills 6. Flexible to travel (if needed)

Mode of interview	
Technical Round	• Initial round with assessment on technical questions and communication skills assessing fitment • Live coding and penetration testing round to demonstrate practical skills
Managerial Round	• Managerial round to assess soft skills and attitude and scenario based questions
Final Director/Partner round (as applicable)	• Final round with techno-managerial and soft skills assessment