Job dashboard for emerging role – Ethical Hacker

ESTIMATED TIME HORIZON:
Short-term*

Contents
Section Top

Trends impacting this role

- AI & Analytics
- Cybersecurity
- Changing Public/ Client Expectations
- Cloud Computing

Responsibilities of the role

This job role is responsible for performing security assessments for clients and advanced penetration tests on clients' computers (primarily network penetration testing, web application vulnerability assessment, etc.). This requires familiarity with the infrastructure of the organisation, business operations and assessment of risks. Job holders will ensure that there is proper governance and controls put in place to help clients detect vulnerabilities, pre-empt these attacks and help them strengthen their systems.

Job Tasks

- Scan software environment for vulnerabilities and upon finding any, explore potential risks and vulnerabilities and mitigate these security risks
- Perform regular monitoring of security systems and evaluate reverse engineering malware to determine the threat level

- Perform research via open-source and dark-web channels on the targeted system or user identified to ethically hack and keep abreast of the latest threats and vulnerabilities
- Provide advice on complex security test data analysis to support security vulnerability assessment processes, including root cause analysis
- Incorporate emerging security and risk management trends, issues, and alerts in penetration testing and ethical hacking activities

- Advise clients on security issues, including explanation on the technical details and how they can remediate the vulnerabilities in the systems
- Deliver quality client services and manage client expectations

- Monitor project progress, manage risk and ensure key stakeholders are kept informed about progress and expected outcomes
- Develop new and innovative strategies to identify issues within the security systems

Skills Analysis

Technical Skills (TSC) Required

- Audit and Compliance
- Cyber and Data Breach Incident Management
- Cyber Forensics
- Cyber Security
- Cyber Risk Management
- Cloud Computing
- Data Analysis
- Digital Forensics
- Digital Technology Environment Scanning
- Forensic Data Analytics
- Financial Analysis
- IT Governance
- IT Standards
- Network Security
- Programming and Coding
- Project Execution and Control
- Professional Skepticism and Judgment
- Risk Assessment
- Security Assessment and Testing
- Security Governance
- Security Strategy
- Stakeholder Management
- Strategy Implementation
- Test Planning
- Threat Analysis and Defence
- Threat and Vulnerability Management
- Threat Intelligence and Detection

Critical Core Skills Required

- Communication
- Creative Thinking
- Digital Fluency
- Problem Solving
- Sense Making
- Transdisciplinary Thinking

* Estimated timeline of demand for emerging job roles (Short-term: Current to 2 years | Medium-term: 2 to 5 years)

Sources: 1. Glassdoor – Job Postings for Information Security Consultant (Penetration Tester) | 2. Cybersecurity Education Guide – Ethical Hacker

Understanding how the dark web works safeguards data-hungry businesses – The Ethical Hacker

Tan Soon Siang

Director, Risk Advisory,
Deloitte Singapore

> “ *Ethical Hacking is also one of the best ways to learn about the technology or system you are hacking*

Soon Siang started his career in Deloitte’s Cyber Risk team as an intern and what keeps this passion alive over the past decade is the dynamic nature of the work where adaptability and problem solving are required. He finds satisfaction in safeguarding the cybersecurity posture of his clients. Hence, he decided to pursue a career in this field after completing his Computer Science degree and is now a Director.

Share with us how your role as an ethical hacker has changed over the years

“In the past, ethical hackers mainly test servers and websites. With the emergence of **new technology platforms** such as mobile applications, cloud platforms and Internet of Things (IoT) devices, the **scope of work** for an ethical hacker has **expanded**,” shares Soon Siang. He explains that as accounting practices move towards digitalisation, there has been a rise in cyber attacks and crimes are becoming more sophisticated. Hence, accounting practices need to ensure that the large amount of data that their clients have entrusted them with are kept safe. “There needs to be **proper governance and controls** to help clients **detect vulnerabilities, pre-empt these attacks and help them strengthen their systems**,” illustrates Soon Siang.

He also shares that technology tools have also enabled them to improve their existing processes and drive productivity. “We used to review server configurations line by line manually and now with emerging technologies like **Intelligent Automation**, the scripts automate this process and flag out anomalies. This saves around 70% of our time! The time savings have definitely benefitted my team immensely, allowing them to focus their effort on identifying vulnerabilities in more complex systems, bringing greater value-add and efficiencies to our clients,” added Soon Siang.

What does an ethical hacker do in his day-to-day job?

“There is no typical day for us! Our work ranges from testing operational technology systems to ensure that they meet regulatory requirements of Critical Information Infrastructure (CII), to simulating hacking activities on body cameras/IoT smart devices to pre-empt any possible attacks,” explains Soon Siang. He also shares with much enthusiasm of his experiences in scanning ports in companies’ systems to detect vulnerabilities, attempts to evade intrusion detection systems and performing network traffic analysis. Soon Siang adds that he will then discuss the findings with his clients after the testing. “The key is to **simplify these technical findings and convey the risk and impact to clients concisely**,” explains Soon Siang.

Advice to practitioners who are keen to explore a career in ethical hacking

“Stay curious, stay passionate and never stop learning!,” shares Soon Siang. He emphasised the importance of being **proactive in learning** such as through participating in online hacking challenges and taking up professional certifications such as Offensive Security's Penetration Testing and CREST Certification.