Skills Sheet

Cyber Security Analyst

Role overview: A Cyber Security Analyst is responsible for safeguarding your organisation's IT networks and computer systems. They monitor security measures, detect vulnerabilities and respond to cyber threats – ensuring the confidentiality and integrity of your digital assets.

DISCOVER

Step 1: Discover
- Sourcing
- Testing and matching
- Culture fit interview
- Candidate approval

Watch this video for a demo of shortlisting and interviewing candidates on *Potential*

TRAIN

Step 2: Train (avg 150 hrs)
- IT Fundamentals
- Networking Fundamentals
- Linux Fundamentals
- OSINT Fundamentals
- Cyber Security Analyst
- Cyber Awareness

CAPSTONE PROJECT

Step 3: Demonstrate
Capstone: SFIA level 3
Using the scenario provided, build an Incident Response Plan (IRP) to address cyber risks and neutralise threats.

Read more about Capstones

This Capstone is an example only and can be tailored to your organisation's needs.

DEPLOY

Step 4: Deploy
- Internal hiring
- Onboarding

GROW

Step 5: Grow
- Post deployment
- Capstone: SFIA level 4
- Capstone: SFIA level 5

Ready to take the next step? Get in touch at: potential@withyouwithme.com

Training pathway

Cyber Security Analyst

WITHYOUWITHME

Below is the recommended training for candidates to be job-ready as a Cyber Security Analyst. This suite of courses can be completed in as little as 150 hours.

Explore the full Cyber pathway

Duration: 3.5 hrs

IT Fundamentals

This course provides a great overview of the basics of IT, from hardware to security.

- Computers
- Hardware
- Working safely
- Operating systems
- Software applications
- Office suites
- Virtual machines
- Networks
- The Internet
- Cloud computing
- Internet of Things
- Security in IT

Duration: 4-6 hrs

OSINT Introduction

An introduction to OSINT (Open Source Intelligence), this course educates students on the impact publicly available information can have on individuals and organisations.

- Explain what Open Source Intelligence is and how it is obtained
- Understand the positive and negative paradigms of Open Source Intelligence
- Understand the base concepts of data considerations

Duration: 8-12 hrs

Networking Fundamentals

This course is designed to teach students how computer networks operate, from a small local area network to the wider internet.

- Network topologies
- Cable standards
- Wiring standards
- Media types
- Communication types
- MAC addresses
- Network devices
- Wireless technology
- OSI model
- TCP/IP protocols
- Wide Area Networks
- Virtual Private Networks
- Authentication protocols
- Routing protocols
- Firewalls
- Ports and network Address Translation
- Virtualisation

Duration: 100 hrs

Cyber Security Analyst

This course provides an understanding of how to implement technical requirements for the defensive and offensive protection of a computer network.

- Intro to cyber security
- Defence in depth
- Malware
- Cryptology
- Threat actors
- The SOC and the Tier 1 Analyst role
- Operating system security
- Analysing advanced threats
- Incident response
- SIEMs and network traffic analysis

Duration: 20 hrs

Linux Fundamentals

This course is designed to introduce the Linux operating system and provide instruction on basic administration

- Intro to Linux
- File system hierarchy standard
- The Linux command line
- Files & directories: Creating, managing, copying, moving & deleting
- Basic system administration
- Linux & the Cloud

Duration: 10 hrs

Cyber Introduction Bundle

Cyber Security Awareness

How to Protect your Data

What is Social Engineering?

Phishing Attacks

Ready to take the next step? Get in touch at: potential@withyouwithme.com

Training pathway

Red Team (Additional)

These courses are optional additions to the Cyber Analyst career pathway – depending on the needs of your organisation.

Duration: 30 hrs

Red Team Essentials (RTE)

In this course, students will learn how to:

- Design, plan and execute a penetration test using a provided standard testing methodology
- Research and investigate attack techniques and describe mitigations for them
- Provide a detailed report on penetration testing activities conducted within the Capstone project which highlights activities, results, issues encountered and the residual risk

Duration: 10 hrs

Red Team Operator
Windows Buffer Overflow

In this course, students will learn how to use Immunity Debugger, Mona Modules and msfvenom to create fully developed buffer overflow exploits in Python2 and Python3 for the Windows platform.

- Introduction & setup
- Spiking
- Fuzzing
- Finding the offset
- Bad characters
- Mona Modules
- Generating and using payloads

Duration: 50-80 hrs

Linux Privilege Escalation

In this course, students will learn beginner and intermediate privilege escalation and local machine lateral movement techniques.

- Enumerate, validate, and exploit privilege escalation vulnerabilities in GNU/Linux environments
- Identify and exploit insecure scripting for lateral movement and privilege escalation
- Provide a detailed report on privilege escalation activities within the Capstone project which highlights activities, results, issues encountered and the residual risk

Blue Team (Additional)

Duration: 50 hrs

Blue Team Essentials (BTE)

This course teaches students the fundamentals of cyber security theory and computer network defence, plus the elements that contribute to defensive operations.

- Networking concepts, protocols and network security
- Risk management processes
- Cyber security and privacy
- Laws, regulations, policies & ethics
- Threats and vulnerabilities
- Cyber defence and tools
- Network traffic analysis
- Incident Response Planning

Ready to take the next step? Get in touch at: potential@withyouwithme.com

Cyber Security Analyst

Capstone: SFIA level 3

WITHYOUWITHME

CAPSTONE PROJECT

A Capstone project is a practical exercise which enables students to demonstrate technical proficiency before stepping into a new role.

The final Capstone presentation is made to the employer or hiring manager and other relevant team members who may ask technical questions relevant to the person's new skill set.

Cyber Security Analyst
Capstone outline

Build an Incident Response Plan (IRP) to support a given scenario

Present the IRP assessment as a briefing to staff in the form of a short video presentation, including:

- Introduction
- Scope
- Demonstration
- Challenges
- Summary

SFIA skills tested

Information security
SCTY | Level 3

- Applies and maintains specific security controls as required by organisational policy and local risk assessments.
- Communicates security risks and issues to business managers and others. Performs basic risk assessments for small information systems.
- Contributes to the identification of risks that arise from potential technical solution architectures. Suggests alternate solutions or countermeasures to mitigate risks. Defines secure systems configurations in compliance with intended architectures.
- Supports investigation of suspected attacks and security breaches.

Information assurance
INAS | Level 3

- Follows standard approaches for the technical assessment of information systems against information assurance policies and business objectives.
- Makes routine accreditation decisions. Recognises decisions that are beyond their scope and responsibility level and escalates according.
- Reviews and performs risk assessments and risk treatment plans. Identifies typical risk indicators and explains prevention measures.
- Maintains integrity of records to support and justify decisions.

Penetration testing
PENT | Level 4

(If Red Team pathway is selected)

- Follows standard approaches to design and execute penetration testing activities.
- Researches and investigates attack techniques and recommends ways to defend against them.
- Analyses and reports on penetration testing activities, results, issues and risks.

Ready to take the next step? Get in touch at: potential@withyouwithme.com