CANBERRA CYBER HUB

DIGITAL SKILLS ORGANISATION

Closing the Cyber Skills Gap

Work-Integrated-Learning Pilot

POWER SKILLS BOOTCAMP - CYBER SECURITY ANALYST (ENTRY-LEVEL)
COMMENCING 17 APRIL 2023

AT A GLANCE

The Cyber Security Work-Integrated-Learning pilot has been co-designed with cyber security employers to bridge the gap between tertiary education and the skills employers need in the workplace and develop a pipeline of work-ready employees to cyber employers, fast. The following provides details of the components of the program.

THE OPPORTUNITY

An intensive and immersive training program of 4 weeks @ 28 hours a week to rapidly develop:

- Fundamental technical knowledge and skills needed to accomplish work-integrated learning tasks with confidence from the start of the internship.
- Professional skills to negotiate the complexities of interpersonal interactions at work, organise tasks and collaborate across teams.
- Work-integrated digital skilling, particularly to work within a company culture, and how to make the most of the experience and secure a job.
- Workplace health and safety understanding to meet workplace requirements.
- Connections with employers to ensure program requirements are met.
- Confidence and motivation to be successful in the internship program and beyond.

THE DETAIL

CompTIA Security+ Industry Certification (part of the Power Skills Bootcamp - self-paced)
The CompTIA Security+ training provides the core knowledge required for the cyber-analyst role and commences prior to the boot camp. Topics covered include:

- Access Control and Identity Management: fundamental concepts including authentication, authorisation and access control.
- Network Security Fundamentals: security function and purpose of network devices and technologies.
- Compliance and Operational Security: appropriate incident response procedures.
- Cryptographic Concepts: assessment tools and techniques used to discover security threats and vulnerabilities.

Critical Core Skills - Soft Skills (Human Skill) development (part of the Power Skills Bootcamp)
The program is aimed at developing both the technical and core skills required to effectively complete work-integrated projects and be productive in the workplace. The following critical core skills will be developed from bootcamp and throughout the program.

- Problem-solving skills outcome is being able to resolve (both proactive and reactive) problems.
- Communication skills which involve giving and receiving different kinds of information.
- Critical thinking skills which relate to recognising building and determining the importance of arguments and ideas.
- Decision-making focuses on evaluating; forming opinions of alternatives and experimenting to solidify validity of decisions.
- Creative thinking skills enable the ability to find new and innovative ways to perform tasks and improve processes and/or develop new approaches.
- Teamwork skills are the ability to work effectively with others during conversations, projects, meetings or other collaborations

STACKABLE MICROCREDENTIALS

During the pilot, interns will undertake one day per week of formal learning delivered flexibly with a blend of face-to-face and online learning sessions. For the remaining four days they will undertake work-integrated learning in the workplace.

1

Microcredential 1 - Cyber Core

This is an introduction to Cyber Security and provides the fundamental skills for those entering the Cyber Security Workforce. This includes:

- Information security is the fundamentals of protecting information and information systems from unauthorised use.
- Security Infrastructure focuses on the protection of infrastructure to limit vulnerability and to recommend remediation or mitigation.
- Security Operations identify groups' key applications prioritise and respond to security threats using workflows and automation.

2

Microcredential 2 - Cyber Assessment

Focuses on the strategies that can be implemented to assess cybersecurity measures and strategies to protect its information and systems from cyber threats. This includes:

- Digital Forensics is the process of using techniques and tools to identify, examine and analyse risks and threats.
- Threat Intelligence is the planning, collecting, analysing and disseminating of information that poses a threat to applications and systems
- Vulnerability Assessment is a systematic review of security weaknesses in an information system.

3

Microcredential 3 - Cyber Development

Develops the skills to implement policy, procedures and processes that will build and maintain cyber-security capabilities within an organisation. Topics covered include:

- Penetration Testing is the simulation of a cyberattack that tests a computer system, network, or application for security weaknesses.
- Software development/ programming/ testing – develop and test software components.

4

Microcredential 4 - Cyber Governance

This microcredential will deliver skills in developing, implementing and evaluating frameworks to ensure information and systems are secure. Topics include:

- Cyber Strategy defines the approach to cyber security. This includes vision, mission statement, and alignment with organizational policies, direction, and goals.
- Risk Management is the process of identifying, evaluating, and mitigating risks to an organisation's information and systems.

SUMMARY

Closing the Cyber Skills Gap - Work-Integrated-Learning Pilot is a comprehensive and flexible program designed to equip interns with the necessary skills to work as a Cyber Analyst. The program covers a range of both technical and soft skills. The pilot is delivered through a combination of classroom learning, online self-paced learning and work-integrated learning.