



## **SENIOR MANAGER: INFORMATION & CYBER SECURITY**

(Payclass PG (13,5))

### **Enterprise Infrastructure Services**

### **Information & Communication Technology Services**

The Information Security team is responsible for protecting the confidentiality, availability and integrity of the University of Cape Town's information and information systems.

The Enterprise Infrastructure Services Division seeks to appoint a Senior Manager to lead the Information Security Team while retaining the responsibility for the practical application of cyber operations. This role will suit candidates that are self-motivated, proactive, that can work under pressure and who have demonstrated experience in stakeholder management and who can lead a team of security analysts through the effective identification, response, and recovery process for cyber incidents.

#### **About you:**

- Do you have experience leading and managing operational information and cyber security service delivery and experience working in cyber security operations?
- Do you have proven experience acting as the escalation point for all security incidents that require attention and timely responses?
- Can you effectively manage security incidents, ensuring the appropriate process is followed from start to finish e.g., Coordinate response, triage and escalation of security events affecting information assets and activities within a Computer Incident Response team?
- Do you have experience in reviewing defining and reviewing new SIEM use cases, run books that provide guidelines for analyzing and responding to specific threats related to the new use case
- Are you looking to take your cyber security skillset to the next level, leading and developing others?
- Do you possess excellent interpersonal skills, with the ability to communicate with staff at all levels?
- Can you build effective working relationships with internal and external stakeholders?

If the answer to these questions is yes – we want to hear from you!

#### **Requirements for the job:**

- Relevant qualification at NQF level 7 (e.g. Degree in Computer Science, Information Systems (information and/or security domain as major) or similar)
- Advanced certifications such as CISM, CISSP or CASP which are current
- 10 years experience in Information technology (Enterprise infrastructure)
- A minimum of 5 years in an information and cyber security role - 3 years must be experience in a senior management role at team management level or higher
- Demonstrated experience and understanding of project and program management

#### **Technical requirements for the job:**

- Hands-on experience and proficiency in analyzing high volumes of logs, network data (e.g., NetFlow, FPC), and other attack artifacts in support of incident investigations
- Expert in incident handling and digital forensic processes
- Knowledge of Data Loss Prevention, Data Replication, and Disaster Recovery Systems.
- A deep understanding of Technology Security risks and mitigating solutions
- Strong knowledge ISO27001/2 Cybersecurity Framework
- Knowledge of legal, regulatory, and privacy requirements
- Knowledge of Centre of Internet Security Standard (CIS), COBIT 2019 and NIST frameworks

- Proficiency in three or more of the following: Anti-Virus, IDS/IPS, Full Packet Capture, Host Based Forensics, , and/or PKI
- In-depth knowledge of architecture, engineering, operations, use case definition and playbook automation in at least one enterprise SIEM platform (e.g., SIEMonster, QRadar, Splunk)
- Demonstrable knowledge of and experience in two or more of the following: network security, computer security (Windows, Mac, and Linux), application security, and cloud security

**Non-Technical requirements for the job:**

- Proven ability to work under stress in emergencies, with the flexibility to handle multiple high-pressure situations simultaneously
- Excellent written and verbal communication skills with the ability to form effective working relationships with other staff and stakeholders
- Confidence communicating technical cyber security risks, incidents and threats to non-technical staff and stakeholders
- Determination and tenacity to drive service and security improvements across the business and the ability to assess the effectiveness of control measures and make improvement suggestions
- Ability to work well under minimal supervision
- Analytical thinking and problem-solving skills
- Attention to detail when delivering technical documentation, policies, and procedures

*The annual remuneration package, including benefits, is negotiable between **R1,137 499** and **R1,338 233** depending on experience and qualifications.*

*Hybrid work arrangements can be negotiated.*

**An application which does not comply with the following requirements will be regarded as incomplete and not considered.**

To apply, familiarize yourself with our website at [www.icts.uct.ac.za](http://www.icts.uct.ac.za), then e-mail the following documents in a single pdf file to: [icts-jobs@uct.ac.za](mailto:icts-jobs@uct.ac.za)

- UCT Application Form (download at <http://forms.uct.ac.za/hr201.doc>)
- **Personal statement, up to 1,000 words**, you should set out in your statement why you are interested in this role and provide examples of where your skills and experience meet the requirements for this role as detailed in the advert .
- Curriculum Vitae (CV).

The document should be named according to the following guidelines: **Reference Number, Senior Manager Information and Cyber Security Services, Surname, First Initial.**

*Only short-listed candidates will be contacted and may be required to undergo competency assessments.*

**Telephone:** 021 650 1673                      **Website:** [www.icts.uct.ac.za](http://www.icts.uct.ac.za)

**Reference number:** E231049                      **Closing date:** 17 November 2023

*"UCT is a designated employer and is committed to the pursuit of excellence, diversity, and redress in achieving its equity targets in accordance with the Employment Equity Plan of the University and its Employment Equity goals and targets. Preference will be given to candidates from the under-represented designated groups. Our Employment Equity Policy is available at [www.uct.ac.za/downloads/uct.ac.za/about/policies/eepolicy.pdf](http://www.uct.ac.za/downloads/uct.ac.za/about/policies/eepolicy.pdf). "*

UCT reserves the right not to appoint