TECHNICAL SPECIALIST: CYBER SECURITY

(Payclass 11)

ENTERPRISE INFRASTRUCTURE SERVICES
INFORMATION & COMMUNICATION TECHNOLOGY SERVICES

UCT is seeking a talented Information Security Engineer/Technical Specialist, to join the UCT Information and Cyber Security team and CSIRT. This is a role which plays a critical part in ensuring that UCT derives value from its investment Information and Cybersecurity and reports to the Senior Manager Information and Cybersecurity Services in the Enterprise Infrastructure Services division.

Successful applicants will be responsible for evaluating and strengthening the security posture through continuous vulnerability, incident handling and security assessments. If you have the skills and are excited by all things cyber, then keep reading.

Responsibilities include:

- **Threat and Vulnerability Analysis** – Identifying potential security risks and weaknesses.
- **Incident Detection and Response** – Investigating security alerts, documenting incidents, and taking action against cyber threats.
- **Security Infrastructure Management** – Configuring and deploying security tools to protect an organization's network.
- **Disaster Recovery Planning** – Preparing strategies to mitigate damage from cyberattacks.
- **Threat Hunting** – Proactively searching for hidden threats that may have bypassed traditional security measures.

Qualification and experience required:

- **Relevant qualification at NQF level 7** in a relevant discipline such as Computer Science or Information Systems
- **7 years' experience in enterprise ICT applications and infrastructure** of which 3 years must be relevant current hands-on technical experience in cyber security
- **Threat Detection & Analysis** – experience in and understanding of cyber threats, malware, and attack vectors.
- **Incident Response** – expert level experience in investigating security breaches and mitigating risks.
- **Network Security** – experience in and knowledge of firewalls, intrusion detection systems, VPNs, network flow interpretation and monitoring.
- **Log Analysis** – experience and ability to analyze logs for anomalies and security incidents.
- **SIEM Tools** – experience with Security Information and Event Management (SIEM) platforms like Splunk, QRadar or preferably SIEMonster.
- **Programming & Scripting** – Familiarity with Python, PowerShell, or Bash for automation.
- **Working understanding of information security frameworks** (e.g., ISO, NIST) and digital forensic methodologies and possible shortcomings they may have. Working understanding of applicable legislation (security and privacy)

Soft Skills Required

- Critical thinking and problem-solving skills
- Excellent written and spoken communication skills
- Experience in and ability to provide status updates to executives and stakeholders in non-technical terms encompassing risk, impact, containment, remediation, etc.
- Ability to work within a team and across different departments
- An autonomous / self-managed work style
- Ability to prioritize and manage work under pressure
- Ability to coach and mentor junior colleagues
- A strong customer service ethic

Advantageous Skills

- Current Industry-recognized certifications e.g., Security+, CEH, CISA, CISSP, OSCP
- Experience in Higher Education is advantageous

The annual remuneration package, including benefits is R784 833 to R923 330 per annum, depending on experience and qualifications.

To apply, please e-mail the below documents in a **single pdf file** to: icts-jobs@uct.ac.za

- UCT Application Form (download at http://forms.uct.ac.za/hr201.doc)
- Cover letter, and
- Curriculum Vitae (CV)

An application which does not comply with the above requirements will be regarded as incomplete and not considered.
Only shortlisted candidates will be contacted and may be required to undergo a competency test.

Reference: E26102 **Closing date:** 23 January 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.hr.uct.ac.za/hr/policies/employ_equity*** "

When you apply for a position at UCT, we collect your personal information to assess your application, communicate with you, and coordinate interview logistics. Information such as race, gender, nationality, and disability status is used to support our Employment Equity obligations. We also verify your references, qualifications, conduct criminal and, for certain roles, credit checks. For more information about how the University of Cape Town uses personal information and your rights, please email popia@uct.ac.za.

The University reserves the right to extend the closing date for applications if deemed necessary and reserves the right to make no appointment.