SECURITY ANALYST

(Payclass 12;12 Month Contract)

Information & Cyber Security Team

ENTERPRISE INFRASTRUCTURE SERVICES

INFORMATION & COMMUNICATION TECHNOLOGY SERVICES (ICTS)

UCT is seeking talented Information Security Analysts, to join Information and Cyber Security team. 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:

- Monitoring the university's network for information and cybersecurity anomalies
- Handling the entire lifecycle of your assigned security incidents from detection to resolution and root cause analysis
- Planning and implementing information and cybersecurity measures to protect computer systems, networks and data.
- Providing input to disaster recovery plans
- Performing risk assessments and recommending information and cybersecurity controls and technical measures (e.g., firewalls, data encryption)
- Recommending information and cybersecurity enhancements
- Developing and implementing information security related processes, systems, and services through project work
- Providing technical leadership for one or more information and cyber security systems and/or service components
- Contribute and participate in information security awareness drives and campaigns
- Develop and maintain security policies and procedures
- Engage with infrastructure, application support, and development teams to ensure security best practices
- Review existing and new technology architecture for data privacy and protection compliance
- Review existing and new technology to ensure it adheres to corporate information security standards.
- Work with information security engineering to ensure all security tools are deployed
- Educate and promote secure software development lifecycle
- Assess current technology architecture for vulnerabilities, weaknesses and for possible upgrades or improvement
- Assist with Ad hoc duties from time to time
- Assist with Projects as allocated by line manager

Qualification and experience required for the contractor role:

- Relevant qualification at NQF level 7 and
- 10 years' experience in enterprise ICT applications and infrastructure of which 5 years must be relevant current technical hands-on experience

Skills and competencies required

- Knowledge of (or at least a strong interest in and exposure to) information security concepts and technologies such as IDS, and endpoint security products, SIEM and SOAR platforms, web application firewalls, network security, computer security, digital forensics and vulnerability management methodology and tools
- Experience in handling the entire lifecycle of your assigned security incidents from detection to resolution and root cause analysis
- Knowledge and experience in implementing and configuring enterprise antivirus solutions (server and Desktop)
- Exposure to specialized IR processes such as reverse engineering, red/blue team exercises, forensics and investigations of data exfiltration and lateral movement
- System Administrator knowledge and working experience in Windows/Linux environments
- Fundamental knowledge and experience with Vulnerability and Patch Management within an Enterprise environment
- Experience providing security architecture guidance to systems administrators and developers
- Understanding of information security frameworks (e.g., ISO, NIST) and digital forensic methodologies and possible shortcomings they may have.
- Confidently and professionally interview/question users to determine or confirm root cause
- Communicate effectively with response and business partners
- Experience in providing status updates to executives and stakeholders in non-technical terms encompassing risk, impact, containment, remediation, etc
- An autonomous / self-managed work style

Advantageous Skills

- Scripting and basic programming in PowerShell and Python.
- Building and monitor SIEM alerting and dashboards.
- Current Industry-recognized certifications e.g., Security+, CEH, CISA, CISSP, OSCP
- Working understanding of applicable legislation (security and privacy)
- Relevant NQF 8 qualification and/or experience in Higher Education is advantageous

The annual remuneration package, including benefits, is negotiable between R906 943 to R1 066 991, depending on experience and qualifications.

Flexible Work conditions are available

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)
- Personal statement, up to 1,000 words, you should set out in your statement why you're interested in this role and provide examples of where your skills and experience meet the requirements for this role as detailed in the advert and job description
- Curriculum Vitae (CV)

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

Telephone:	021 650 3012	**Website:**	www.icts.uct.ac.za
Reference No:	E22995	**Closing Date:**	13 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*** "

UCT reserves the right not to appoint.