POSITION DESCRIPTION

Manager and Cyber Engineer

POSITION DETAILS

Position Title	Cyber Security Engineering Manager
Classification	7015495
Position Number	NEW
School/Office	Digital Services / Security & Digital Operations
Division	Division of Operations

POSITION PURPOSE

The Manager and Cyber Security Engineer leads the strategic development and operational delivery of cyber engineering capabilities across the University. This role ensures the design, implementation, and optimisation of security controls and platforms (build, integration, automation, and run) across hybrid cloud and on-prem environments, enabling the University to maintain a resilient and compliant cyber posture aligned to NIST CSF 2.0 (with ISO/IEC 27001 and ISM where applicable). The position contributes to institutional strategy through expert leadership in security engineering (e.g., IAM/PAM, EDR/XDR, SIEM/SOAR, WAF/DDoS, DLP/CASB), threat mitigation, control automation, and reliability engineering with measurable control effectiveness (e.g., asset/log coverage, MTTD/MTTR, patch SLAs).

It also plays a key role in embedding security-by-design and by-default principles into engineering patterns, guardrails, and reference implementations for enterprise platforms, ensuring that cyber risk is addressed early and systematically through threat modelling, hardened baselines/golden builds, IaC policy-as-code, and MITRE ATT&CK–informed detections integrated with SOC/IR playbooks. The role partners with Enterprise Architecture for pattern approval and standards, while owning the implementation, integration, and operationalisation of controls.

KEY ACCOUNTABILITIES

- Lead and manage cyber security engineering operations to deliver secure, scalable and resilient platforms across the University (build, integrate, automate, run).
- Develop and implement a control-led security engineering roadmap aligned to NIST CSF 2.0 and relevant standards (ISO/IEC 27001; ISM where applicable).

- Design, deploy and harden core security technologies, including next-generation firewalls, IDS/IPS, WAF/CDN, EDR/XDR, SIEM/SOAR, DLP/CASB and PKI.
- Standardise automation and Infrastructure-as-Code (golden builds, baselines, guardrails/policy-as-code) across cloud and on-prem.
- Continually uplift resilience and efficiency through tuning, simplification and removal of single points of failure.
- Lead, coach and develop principal and specialist engineers; maintain a clear RACI with SOC/IR.
- Collaborate with internal stakeholders and external partners to ensure alignment of engineering solutions with business needs and EA-approved patterns (implementation and operationalisation owned by this role).
- Ensure compliance with cybersecurity standards and legislation, demonstrating control effectiveness via agreed KPIs/KRIs (e.g., coverage, configuration compliance, MTTD/MTTR, patch SLAs).
- Monitor emerging threats and technologies, providing expert advice on control selection, tuning and decommissioning grounded in MITRE ATT&CK.
- Embed secure-by-design practices across infrastructure and platform lifecycles (threat modelling, hardening standards, change control).
- Maintain robust detection and logging frameworks to support high-quality monitoring and response (coverage and fidelity expectations, runbooks/playbooks).
- Provide engineering oversight for major infrastructure and cloud initiatives, ensuring secure implementation, testing and effective handover (runbooks, support models, KPIs).

QUALIFICATIONS, EXPERIENCE AND SKILLS

- Postgraduate qualifications in Cybersecurity, Information Technology, or a related field, or demonstrated equivalent experience.
- Extensive experience in security engineering and platform operations within complex organisations (hybrid cloud and on-prem).
- Proven ability to lead high-performing technical teams and deliver strategic outcomes.
- Deep knowledge of cybersecurity frameworks, threat intelligence, and secure platform design.
- Strong stakeholder engagement and communication skills, including the ability to influence at senior levels.
- Demonstrated capacity to manage complex projects and drive innovation in cyber operations.
- Strong understanding of secure network architecture, zero trust models, and hybrid/cloud security design.
- Hands-on experience deploying and maintaining enterprise-grade security platforms (e.g., SIEM, SOAR, EDR, IAM).

Technical Proficiency

- Proficiency in scripting or automation tools (e.g., Python, PowerShell, Terraform) to improve engineering workflows.
- Working knowledge of cloud security platforms (AWS, Azure) and associated native security controls.
- Demonstrated ability to design and manage secure logging, monitoring, and alerting systems with defined coverage and quality targets.

Desirable

- Certifications such as CISSP, CISM, SABSA, or relevant cloud security certifications (e.g., AWS Security Specialty, Azure Security Engineer Associate).
- Experience contributing to sector-wide security forums or collaborative cyber initiatives (e.g., AHECS, AARNET).
- Understanding of DevSecOps practices and integration of security into CI/CD pipelines.

KEY RELATIONSHIPS

This position reports to: Director, Cyber Operations
This position supervises:

- Principal Cyber Engineer
- Specialist Firewall Engineer
- Specialist Cyber Engineers

Key internal relationships:

- Chief Digital & Information Officer
- Cyber Security Assurance and Operations (CSAO)
- ITDS Leadership Team
- Risk, Legal, and Governance Units
- Academic and Research Units

Key external relationships:

- Cybersecurity vendors and service providers
- Sector forums (e.g., AHECS, AARNET)
- Regulatory bodies and compliance partners

CHALLENGES

- Leading cyber security engineering initiatives in a rapidly evolving threat landscape.
- Balancing strategic priorities with operational demands across a multi-campus and international footprint.
- Ensuring compliance with complex and changing cybersecurity regulations.
- Driving innovation while managing constrained resources and legacy systems.
- Maintaining a high signal-to-noise ratio in detections (reduce false positives, improve alert precision and triage quality).

OCCUPATION SPECIFIC CAPABILITY SET

SFIA

SFIA Capability	Code	Level	Rationale
Information security	SCTY	6	Leads design and implementation of secure digital infrastructure; ensures alignment with regulatory and risk frameworks.
Solution architecture	ARCH	5	Consulted on patterns and guardrails; partners with Enterprise Architecture while owning implementation/integration and run.

Innovation	INOV	6	Identifies and implements new technologies to strengthen cyber posture and operational effectiveness.
Systems integration and build	SINT	6	Owns integration of security platforms, telemetry, and control guardrails across hybrid environments at enterprise scale.
IT infrastructure	ITOP	6	Directs the secure configuration, operation, and evolution of University-wide infrastructure.
Security administration	SCAD	**6**	Sets policy-as-code, golden builds, configuration standards; delegates operational execution and assures compliance.
Incident management	USUP	**5**	Engineers high-fidelity detections and logging; supports SOC/IR with playbooks and platform fixes.
Leadership	LEDR	6	Sets direction, establishes standards and KPIs/KRIs, coaches principals/specialists, manages vendors and budgets.
Stakeholder relationship management	RLMT	5	Builds strong cross-functional and external partnerships to align cyber engineering with business priorities.

UNIVERSITY EXPECTATIONS

The University expects that all employees are aware of, and comply with legislation and Western's policies and procedures relevant to the position, including but not limited to:

→ Code of Conduct
→ Work Health and Safety and Wellbeing Management System
→ Enterprise Agreement or Award
→ Anti-discrimination principles, Equal Employment Opportunity and staff and student equity.

Approved by:
Date: