Position Description – Security Analyst, Cyber Operations

Position Details

Position Title: Security Analyst, Cyber Operations

College/Portfolio: Operations **School/Group:** ITS

Campus Location: Primarily based at Melbourne CBD campus, and the potential to work across other RMIT campuses as required.

Classification: HEW 7 **Time Fraction:** 1.0

Employment Type: Continuing

Reporting Line: Senior Manager – Cyber Security Operations

No. of Direct reports: Nil

RMIT University

RMIT is a global university of technology, design and enterprise, committed to creating transformative experiences for students and making a meaningful impact through research, innovation, and engagement. For more information on RMIT University follow the links below.

https://www.rmit.edu.au/about
https://www.universitiesaustralia.edu.au/university/rmit-university/
https://www.rmit.edu.au/about/facts-figures

Our campuses in Melbourne (City, Brunswick, Bundoora, and Point Cook) are complemented by international campuses in Vietnam and a centre in Barcelona, Spain. We proudly acknowledge the Woi Wurrung and Boon Wurrung peoples of the eastern Kulin Nation on whose unceded lands our campuses are located.

We are deeply committed to reconciliation and Indigenous self-determination, embedding these values throughout our policies, culture and structures.

https://www.rmit.edu.au/about/our-locations-and-facilities

Why Join RMIT?

Our people are at the heart of everything we do. At RMIT, we value innovation, collaboration and impact. Our values are the heart (durrung) of who we are and what we stand for at RMIT. They guide what we do, how we make decisions, and how we treat each other.

Inclusion **Imagination** **Integrity** **Courage** **Passion** **Impact**

Learn more about our values: https://www.rmit.edu.au/about/our-strategy/values

Organisational Accountabilities

RMIT is committed to the safety, wellbeing and inclusion of all staff and students. As a staff member, you are expected to comply with all relevant legislation and RMIT policies, including those related to: Equal opportunity, Occupational health and safety, Privacy and trade practices & Child safety standards:

Appointees are responsible for completing all required training and ensuring that they and their team members remain up to date on relevant compliance obligations.

Staff are expected to understand and support RMIT's child safe practices as part of their professional responsibilities. More about our child safety commitment: https://www.rmit.edu.au/about/our-locations-and-facilities/facilities/safety-security/child-safety.

Leadership at RMIT

At RMIT, leadership is not defined by position or hierarchy—it is a shared responsibility demonstrated by all staff, regardless of role or title. Leadership is grounded in our six core values, which guide and shape how we work together, make decisions, and create impact.

Effective leadership means consistently integrating these values into everyday actions and interactions, whether influencing a project outcome, supporting a colleague, or leading a team. All staff are expected to embody the principles of the *Be–Know–Do* Leadership Model:

Be – We are open and authentic, inclusive and empowering. We are purpose driven role models and communicators.
Know – We are self-aware, and understand our stakeholders, our sector and priorities.
Do – We set clear direction and expectations, we develop ourselves and others and promote mutual accountability to deliver results.

At every level, leadership at RMIT is about influence, contribution, and mindset. It is reflected in how we empower others, foster collaboration, and drive positive change through capability-building and alignment to strategic goals.

College/Portfolio/Group

The Operations Portfolio enables integrated, enterprise-wide delivery for best practice student and staff experience.

The Portfolio incorporates the following business units: Legal Services, Enabling Services Reform, Enterprise Projects and Business Performance, Data and Analytics, Finance, Procurement, Information and Technology Services, Health Safety and Risk, Property Services and the Office of the Chief Operating Officer.

The Portfolio houses key delivery functions across the staff and student journeys and enables overall experience for both groups. It is integral in bringing the RMIT strategy to life across the globe. Each of these functions supports the University's global operations directly and through its controlled entities.

Information and Technology Services provide RMIT with current and emerging technology systems and services. Our vision of unleashing technologies to enable great experiences for RMIT communities drives a proactive and leading-edge technology ecosystem that supports the University's commitment to lifelong learning.

Position Summary

The Security Consultant, Cybersecurity Operations is responsible for supporting the detection, investigation, and response to cybersecurity threats across RMIT's enterprise and cloud environments. The role focuses on triaging incidents from the SIEM, DLP, vulnerability management, patch compliance, and data protection initiatives.

Working as part of RMIT's Cybersecurity Operations, this role provides hands-on technical and investigative capability, assisting in the protection of RMIT's people, data, and systems.

Key Accountabilities

1. Incident Management and Response
   - Triage and investigate alerts from our SIEM, and EDR platforms.
   - Manage incidents escalated from Tier 1 SOC analysts, performing deeper technical investigation and coordination with relevant teams.
   - Classify and document incidents following the RMIT CISO Incident Response Framework (aligned to NIST SP 800-61).
   - Support forensic evidence collection, log analysis, and containment actions as required.
2. Data Protection and Governance
   - Review and investigate incidents generated by DLP, Information Protection Labels, and Data Governance policies.
   - Conduct triage of DMARC, spoofing, and phishing-related events, coordinating with the other teams.
   - Identify and recommend improvements to Microsoft Purview policies and governance configurations.
3. Vulnerability and Patch Management
   - Monitor vulnerability reports.
   - Track remediation activities and patch compliance across infrastructure and endpoint environments.
4. Security Engineering Support
   - Assist with maintenance of SIEM and SOAR data connectors, detection logic, and automation workflows.
   - Contribute to building detection use cases, dashboards, and playbooks.
   - Participate in testing and validating new integrations or security technologies before production rollout.
5. Continuous Improvement and Collaboration
   - Support post-incident reviews, root-cause analysis, and lessons-learned documentation.
   - Contribute to knowledge base and playbook updates.
   - Participate in tabletop exercises and security awareness initiatives.
   - Engage collaboratively with service owners, risk and governance teams, and the broader ITS community.

Essential

- Demonstrated experience in security operations, system administration, or incident response in a complex enterprise environment.
- Working knowledge of SIEM and SOAR platforms.
- Familiarity with DLP, Information Protection Labels, and Data Governance policies.
- Understanding of vulnerability and patch management processes.
- Strong analytical, troubleshooting, and communication skills.
- Knowledge of cybersecurity frameworks such as NIST CSF, CIS Controls, or ISO 27001.

Desirable

- Experience working with AWS or Azure security services (e.g. GuardDuty, CloudTrail, Security Hub).
- Proficiency in SIEM queries or scripting languages (PowerShell, Python).
- Understanding of network and endpoint security fundamentals.
- Relevant certifications (Microsoft SC-200, SANS GIAC, CompTIA Security+, or equivalent).

Personal Attributes

- Analytical thinker with a strong attention to detail.
- Team-oriented with the ability to collaborate across technical and non-technical stakeholders.
- Calm and methodical under pressure during incident response.
- Motivated to continuously develop cybersecurity skills and knowledge

Qualifications

Tertiary Education and a number of years relevant experience

Working with Children Check

Appointment to this position is subject to holding a valid Victorian Working with Children Check and other checks as required by the specific role. Maintaining a valid Working With Children Check is a condition of employment at RMIT.