IT Infrastructure and Security Engineer

Department:	Information Technology Services
Classification:	Level 8
Reports to:	Associate Director, ITS
Direct reports:	Not applicable

Who we are

The Victorian Tertiary Admission Centre Limited (VTAC) empowers, connects, and supports learners and providers to enable transparent and inclusive access to education. We aim to be a contemporary organisation that creates and delivers value for our stakeholders.

We act as a bridge between prospective students and Victorian universities, TAFE institutes and independent tertiary colleges. Each year we process around 83,000 applications for tertiary courses and issue a similar number of offers throughout the year on behalf of institutions. This includes the provision of information and enquiry services to applicants and schools.

VTAC also conducts the annual scaling of VCE results and the calculation of the Australian Tertiary Admission Rank (ATAR), including arrangements for International Baccalaureate students and interstate students.

Our IT Services department focuses on the maintenance and continuous improvement of infrastructure and systems. It supports applicant and institution service delivery and efficient data management.

Our values

Collaborative Excellence

- We work together with trust, openness and shared purpose to amplify our impact – valuing diverse perspectives, encouraging respectful dialogue and achieving more through collective effort.

Curious Thinking

- We embrace curiosity and life-long learning – questioning assumptions, taking considered risks, responding to change, exploring new ideas and seeking opportunities to grow, innovate and improve.

VICTORIAN TERTIARY ADMISSIONS CENTRE
VTAC LTD ABN: 19 667 966 038
A Level 7, 130 Lonsdale Street, Melbourne, VIC 3000
T +61 3 9926 1020
W vtac.edu.au

Inclusive Impact	• We create an environment where everyone feels valued, heard and empowered to contribute – championing equitable and accessible education, embracing difference, and ensuring our services and actions benefit all.

About the role

The Security Engineer is responsible for designing, building, and maintaining the security architecture of the organization's IT systems. This role ensures the confidentiality, integrity, and availability of data and systems through robust security designs and controls. The ideal candidate will possess deep technical expertise, a strong understanding of risk management, and a strategic mindset to align security initiatives with business goals.

Key responsibilities

Role-specific

- Develop and maintain enterprise security architecture frameworks and standards
- Design secure network, system, and application architectures to defend against evolving cyber threats.
- Collaborate with IT, DevOps, and software development teams to ensure security is embedded throughout the technology lifecycle.
- Conduct threat modelling, risk assessments, and architecture reviews of current and proposed systems
- Lead incident response planning and support forensic investigations when necessary.
- Protect services and applications from unauthorised and illegitimate access, from external and internal sources
- Operational management of security tooling including but not limited to, SIEM, EDR, Identity & Access Management and Cloud Security platforms.
- Monitor and analyse security alerts, logs, and events from various systems and applications to identify and respond to potential security threats or incidents.
- Investigate and perform in-depth analysis of security incidents, determining the root cause, impact, appropriate mitigation actions and future recommendations

- Develop and implement on premise, cloud and co-lo network security controls, including on boarding of security policies, standards, and guidelines for systems and applications
- Preparing documentation (drawings, diagrams, design notes, work instructions, test procedures and reports) in support security policies, standards, and guidelines for systems and applications.
- Conduct regular audits on systems to identify vulnerabilities, weaknesses and misconfigurations in the organisation's environment.
- Implement appropriate security controls including authentication controls, security best practices, SIEM detect and respond queries to continually improve VTACs security posture.
- Maintain secure authentication Identity & Access Management (IDAM) flows between on-prem and multiple cloud systems
- Management End-to- of multi-site network infrastructure across multiple locations including optimise network performance (VLANs, routing, QoS, segmentation) and implementing and maintaining secure network segmentation
- Continually improve the security knowledge, guidance and mentorship to employees by promoting a culture of security and driving security awareness.

Organisation-wide

- Ensure you are aware of and adhere to legislation and VTAC policy relevant to the duties undertaken, including Equal Employment Opportunity, supporting equity and fairness; Occupational Health and Safety, supporting a safe workplace; Conflict of Interest; and Privacy.
- VTAC expects staff to appropriately balance risk and reward in a manner that is sustainable to our long-term future, contribute to a culture of integrity and collaboration, and provide an environment that is safe, secure, and inclusive. Ensure you are aware of and adhere to VTAC polices relevant to the duties undertaken and the values of the VTAC. This is a standard which the VTAC sees as the benchmark for all its activities.

Key selection criteria

Education/Qualifications

The appointee will have:

- A Bachelor's degree in Computer Science, Software Engineering, Information Systems or a related field; or
- an equivalent combination of relevant experience and/or education/training such as:
    - Certified Information Systems Security Professional (CISSP)

- Certified Cloud Security Professional (CCSP)
- AWS/Azure Security Specialty
- SABSA, TOGAF, or other architecture frameworks
- GIAC certifications (e.g., GSEC, GDSA)
- Networking technologies – routers, switches, and routing protocols.

Knowledge and Skills

The successful candidate will possess all or most of the following requirements:

- 7+ years' experience in cyber security analysis, security operations, incident response, or related roles
- Experience managing security across multiple cloud environments
- In depth knowledge of the Microsoft security ecosystem (including Azure AD, Conditional Access, PIM, Defender, Defender 365, Sentinel etc.), Email Security platforms (Mimecast preferred), vulnerability and patch management, web filtering, firewalls, SIEM and endpoint protection.
- In depth experience with AWS environments including Solid working knowledge of AWS (EC2, VPC, IAM)
- Solid understanding of security, risk and control frameworks and standards including NIST Cybersecurity Framework, and ISO27001
- Strong understanding of Systems Engineering methodologies and tools such as ITIL
- Technical expertise in network security, system and cloud security knowledge, firewalls, intrusion detection, web application security, IoT Security, vulnerability scanning, and malware protection.
- Strong knowledge of common vulnerabilities and exploitation techniques.
- Practical experience with threat hunting, cyber security incident handling, and red teaming exercises.
- Knowledge of application security and implementation of security controls across the software development lifecycle
- Experience managing Palo Alto platforms (firewalls, policies, patching)
- Experience with web protocols and standards (TCP/IP, HTTP, SSL, and DNS)
- Networking technologies – routers, switches and routing protocols
- Demonstrated ability to work as an effective member of a team as well as being able to exercise substantial levels of independence, judgement and initiative

- Excellent communication skills, including the ability to prepare professional documentation for various audiences, advise and negotiate at high levels and maintain discretion in a complex environment
- Excellent problem-solving skills
- Knowledge of secure coding practices and DevSecOps principles

Soft Skills:

- Excellent communication skills with the ability to explain technical concepts to non-technical stakeholders.
- Strong problem-solving, analytical, and organizational skills.
- Proven leadership abilities and experience working across cross-functional teams.
- High level of integrity, professionalism, and attention to detail.

Other requirements

- Travel to other locations may be required.
- There may be a requirement to work additional hours from time to time.
- There may be peak periods of work during which taking of leave may be restricted.
- A current satisfactory Working with Children Check is required.