IntegraFin

Cyber Security Engineer

Division/Department	Information Technology
Reports to	Cyber Security Team Lead
Direct reports	None

Role Overview

The Cyber Security Engineer will help to design, develop, and mature the company's cyber security capability, including the selection, implementation, and management of security tools and technologies focused on detection, prevention, and analysis of security threats. They will assess risk, identify mitigating controls, create and review design artifacts, and support the creation, implementation, and maintenance of a robust cyber security framework in line with Integrafin's strategy and threats.

Individuals who are hands-on with security tools, technically experienced, and capable of making risk-based security decisions are ideal for this position. The candidate should be able to build relationships and collaborate effectively with the wider technology teams. Additionally, they must communicate security topics to non-technical, non-security, senior business stakeholders to enable strategic security decision-making. A self-starter is required for this role, and the successful applicant should demonstrate ownership and responsibility for resolving issues.

Key Areas of Responsibility

- Work with technology and business teams to deliver security processes, technologies and controls, acting as the authority on security related queries
- Define, design, implement, and maintain security solutions appropriate to the business' needs
- Create designs or review existing/proposed designs for services or applications to identify potential security issues. Where issues are identified look to resolve them using defined security patterns and security principles
- Support the definition, execution and continuous improvement of key cybersecurity processes including vulnerability & patch management, security incident response, security monitoring, endpoint security, identity and access management, network security, and cryptography
- Manage, deliver, and lead cyber security and cyber risk assignments, producing documentation, presentations, reports, recommendations, and design proposals to impact and steer business and IT design decisions
- Contribute to the development of cyber security standards, procedures and guidelines
- Contribute as a team member in projects and change initiatives aimed at increasing enterprise security capabilities e.g., identity and access management, centralised monitoring, etc.
- Provide security analysis and support throughout the organisation, ensuring security and governance requirements are met, and be proactive in the identification and remediation of security incidents

Education and Knowledge Requirements

Essential	Desirable
• Strong knowledge of security architecture patterns, design principles, and security controls • Knowledge of information technology compute, storage, networking, and identity components, how they are impacted by cyber threats and appropriate security controls to protect them	• A bachelor's or master's degree in computer science, Information Security, or a related field • Professional certifications such as Certified Information Systems Security Professional (CISSP), Certified Cloud Security Professional, Certified Ethical Hacker (CEH), or Certified Information

• Ability to design and document effective security controls aligned to business requirements using a risk-based approach • Familiarity with application attack tactics and techniques (MITRE Framework), security maturity models (OpenSAMM, C2M2), security frameworks (NIST CSF), security standards (OWASP, SANS Top 25), and regulations (GDPR, PCI-DSS) • Strong technical skills in modern technologies and methodologies including virtualisation, cloud computing, and serverless deployments • Strong technical skills including Azure, Microsoft Defender, M365 and firewalls • Ability to understand and comprehend the impact of decisions, balancing requirements and deciding between approaches • Experience of working effectively with a variety of stakeholders from different technology and business teams • Strong verbal and written communication skills • Must have the ability to work independently and take initiative	Security Manager (CISM) are highly desirable • Strong knowledge of Operating System security and system hardening concepts such as CIS Benchmarks • Experience in working with information security frameworks and regulatory requirements including ISO27001, NIST, PCI DSS, GDPR, Cyber Essentials • Experience of general IT Audit processes and conducting risk assessments • Experience in threat hunting, digital forensics or cloud security principles

Experience Requirements

Essential	Desirable
• Minimum of 2 years experience in a security engineer / analyst, role focusing on designing and implementing security solutions and managing security infrastructure • Previous experience in Financial Services environment	• Experience of ZeroTrust and cloud-native security principles • Experience in dealing with regulatory requirements specific to the Financial Services Industry

Attributes

- Total integrity, objectivity, accountability, and mature approach to the role.
- Strong intellect and analytical ability.
- Strong interpersonal and communication skills.
- Focused on delivery and task orientated.
- Ability to innovate and think out of the box to solve problems and evolve solutions

Competence Requirements

Working with others (Level C)

Works collaboratively with others to achieve common goals

Impact and influence (Level C)

Builds rapport, uses persuasion and influence to obtain support and buy-in for activities to the benefit of the business

Leadership (Level C)

Demonstrates an ability to drive, motivate and inspire both self and others to achieve goals

Developing self and others (Level B)

Develops self and others, showing a genuine interest in helping others reach their potential

Achievement orientation (Level C)

Works to achieve results and improve individual and company performance through what they do

Customer orientation (Level B)

Develops and maintains strong relationships with our customers and understands how this relationship is central to Transacts success

Relationship building (Level B)

Builds mutually beneficial, collaborative, long term relationships both internally and externally

Planning and organising (Level B)

Has ability to plan, organise and prioritise work

Innovation and continuous improvement (Level C)

Seeks and uses ideas to continually improve performance or themselves and the business

Analytical thinking and decision making (Level C)

Has ability to analyse, investigate and interpret information, issues and situations to make the right decisions in a timely manner

Financial and business awareness (Level C)

Understands what Transact does and the business environment in which it operates

Accountability

As a financial services company we are bound by various rules and regulations. In this role you are particularly accountable for these areas:

Compliance and Risk

- Adhere to all processes and deadlines as required by the Group Compliance department in line with regulations.
- Understand the risks, control and governance requirements for the group and flag and escalate risks and error within your remit.
- Comply with all internal policies and procedures.
- Comply with the Individual Conduct Rules.

Training and Competence *

All of our staff are expected to acquire and maintain the desired level of competence for their role which requires them to have the skills, knowledge and expertise needed to discharge the responsibilities of their role. This may include Continual Professional Development (CPD).

You are required to:

- Undertake all training required for your role.
- Attend and participate in internal training courses as required by your role.

- Undertake continual professional development relevant to your role.
- Continue to maintain technical knowledge and contribute to the development of the knowledge of other team members.

* For definitions, please see the T&C Guide