Job title: Security Architect	Location: GIBRALTAR, VIENNA, UK
Function: Product and Tech Reports to: Lead IT Security Architect	No. of direct reports: None No. of non-direct reports: None
Budgetary responsibility:	NGR/P&L:

Purpose of role

We're Entain. Powered by our very own technology and building products that push boundaries, Entain is home to a global family of more than 25 well-known brands and over 24,000 people, but we all play for the same team. When we win, we win together.

Our vision is to be the world leader in betting, gaming and interactive entertainment by bringing moments of excitement into people's lives. We will achieve this through our focus on sustainability and growth, driving change in the fast-paced world of entertainment.

As the Security Architect, you will play a pivotal role in shaping the security landscape of our organization, leveraging your expertise to assess risks, devise strategic security frameworks, and guide the implementation of effective security controls. With a keen focus on proactive risk management and continuous improvement, your primary objective will be to architect secure systems, ensuring that they are resilient to cyber threats and compliant with industry regulations and best practices.

In addition to designing secure systems, you will be responsible for assessing security-related network changes. This includes evaluating proposed modifications to our network infrastructure and configurations, communications between applications, access for third parties, and other network-related aspects. Your expertise will be instrumental in mitigating risks associated with network changes and maintaining the integrity and resilience of our network environment.

Key responsibilities

- Assess the security posture of new applications and services being implemented within the business, recommend appropriate safeguards, including cloud-native security controls and configurations.
- Leverage your deep understanding of both technical architecture and business flows to ensure that security measures are seamlessly integrated into our systems, including cloud infrastructures and containerization techniques such as Kubernetes.
- Collaborate with the security team and other stakeholders to develop a comprehensive security strategy that aligns with business objectives and regulatory requirements.
- Thoroughly review proposed changes to network infrastructure, configurations, protocols, application communications, and access for third parties, including those related to cloud infrastructures. Identify potential security implications and ensure changes adhere to established security standards and best practices across all environments.
- Stay up to date with the latest security trends, technologies, and best practices, and apply this knowledge to design and implement robust security measures.
- Possess a comprehensive technical perspective, delving into the intricacies of the business architecture and processes to ensure a holistic understanding.
- Evaluate the security aspects of newly introduced applications, conducting thorough assessments to guarantee alignment with security standards.
- Provide diligent scrutiny and approval for the deployment of new services in our production environments, maintaining a vigilant eye on security implementations.
- Conduct regular reviews of existing configurations to uphold the required level of security, adapting as necessary to evolving threats and challenges.

- Undertake security reviews as requested, particularly for integrations and other dynamic organizational requirements, ensuring a robust and adaptive security posture. Conduct risk assessments to identify potential security weaknesses, and develop mitigation plans to address them effectively.
- Foster close collaboration with Security Analysts to maintain a comprehensive understanding of security architecture and posture on both ends, promoting a unified approach to security management.

Occasional Responsibilities:

- Support on Security Incidents investigations and management.
- Collaborate with the Incident Response team to develop and test incident response plans.

Specialist skills and experience

The role requires a team player with strong technical foundations, hands-on information security skills, attention to detail and good problem-solving skills.

Essential

- At least two years' experience in a similar Information Security position. Proven experience as an architect, preferably in information security or cybersecurity.
- Attention to detail, good problem-solving skills and decision making
- Autonomous, self-organized, flexible, proactively taking initiative
- Familiarity with containerization technologies and container security concepts
- A thorough understanding of the security threat landscape, significant risks, technical developments and directions
- Experience in reviewing, assessing and defining security requirements based on risk appetite, international standards, compliance requirements and internal risk frameworks
- Very good ability to translate and accurately communicate security and risk implications across technical and non-technical stakeholders.
- Experience with designing and implementing security solutions, including on-premises, cloud-based, and containerization technologies, in a large-scale environment.
- Solid understanding of security frameworks, risk management, regulatory and industry standards (e.g., ISO 27001, PCI-DSS, NIST, GDPR).
- A thorough understanding of the current security threat landscape, significant risks, technical developments, and directions.
- Proficiency in cloud infrastructures in AWS, GCP, and/or Azure, preferably with a high level of expertise in one or more of these platforms. / Knowledge of cloud computing platforms (AWS, Azure, GCP) and their security principles.
- Proficiency in container security concepts and containerization technologies such as Kubernetes.
- Outstanding knowledge of the technical foundations behind networking, operating systems, and applications / Strong understanding of networking concepts, protocols, and architectures:
    - Networking protocols such as TCP/IP, SMTP, SSH, RDP.
    - Proficiency in operating systems (Windows, Linux, etc.) and familiarity with their security features including endpoint security solutions
    - Linux, Windows Operating Systems
    - Understanding of network firewalls, reverse / forwarding proxies, load balancers, Web Application Firewalls (WAFs) and VPNs.
    - Understanding of encryption techniques, cryptographic protocols, and key management.
- Experience in reviewing, assessing, and defining security requirements based on risk appetite, international standards, compliance requirements and internal risk frameworks.
- Strong communication, and interpersonal skills. Very good ability to translate and accurately communicate security and risk implications across technical and non-technical stakeholders.

Desired:

- In possession of industry certifications such as CISSP, CISM, GDSA, OSCP, or similar qualification.
- Experience in crafting and evolving enterprise security strategies, driving ongoing program development to ensure robust security posture maintenance.
- Online Gaming security experience

Competencies / behaviours

- Decision-making skills. Ability to quickly analyse, provide guidance and decide on the best solution based on the on the information at hand.
- Stakeholder engagement: Builds effective working relationships.
- Collaboration: Communicates effectively with a positive impact
- Analytical thinking: Thinks critically, providing well-reasoned insights.
- Agility: Quickly adapts and remains flexible while managing risks
- Acts with integrity: Takes ownership and does the right thing.

Diversity and equal opportunities:

As a global employer, Entain is committed to providing a safe, fun, and inclusive culture where our people feel like they truly belong.

We are a multicultural business that values, celebrates and respects individual differences, so whatever your sexuality, gender, gender identity, ability, age, race, religion, or belief, you will have a voice here, and the space to do your best work.

Our diverse internal networks provide the support for you to express your views and make a positive difference.