Application Security Engineer

BPP Education is entering a new phase of its growth and evolution, attracting thousands more students each year and expanding into new verticals and new markets globally. The BPP Product & Technology (P&T) organisation is evolving rapidly, and driving transformation of its platforms, digital products and experiences, in order to help BPP Education scale and meet the growth of the business in the coming years.

We're looking for a talented application security engineer to help us build secure applications, systems and infrastructure alongside our products that delight and engage learners during their time studying with BPP and beyond, throughout their working lives.

As the **Application Security Engineer**, you will report to the Head of Cyber Security, providing technical leadership and expertise to identify, assess and mitigate security vulnerabilities and threats. This role is key as we transform BPP Education to become more customer centred, design and data informed, to build products that meet and exceed our users' needs across our education ecosystem.

Key responsibilities

- **Secure Coding:** Conduct code reviews, threat modeling, and mentor developers on security best practices.
- **Identity & Access Management (IAM):** Configure RBAC, MFA, and manage privileged access in alignment with compliance standards.
- **Cloud Security:** Support secure AWS configurations, enforce infrastructure-as-code policies, and assist in cloud architecture design.
- **Vulnerability Management:** Perform scans, coordinate remediation, and prioritize risks.
- **Collaboration:** Share findings, contribute to internal documentation, and run security workshops with cross-functional teams.

Essential Skills

- Proven experience as an application security engineer working in an agile environment.
- Good knowledge of application security concepts, secure coding practices and common vulnerabilities (e.g. OWASP Top 10).
- Strong understanding of threat modelling methodologies and practical experience in applying them to software systems.
  Hands on experience with security testing tools such as static / dynamic analysis and penetration testing tools.
- Proficient in development languages and frameworks such as Python, JavaScript, React, Node.
- Knowledge of security standards and frameworks (e.g. ISO27001).
- Excellent verbal and written communication skills.