CAREER OPPORTUNITIES

Job Description:
Information Security Architecture & Engineering Lead UK

WELCOME TO PCI PAL

PCI Pal is a leading provider of SaaS solutions that empower companies to take payments securely, adhere to strict industry governance, and remove their business from the significant risks posed by non-compliance and data loss. We are integrated and resold by some of the worlds' leading business communications vendors, as well as major payment service providers.

We are currently looking for a Information Security Architecture & Engineering Lead to join our UK team.

THE OPPORTUNITY:

The Information Security Architecture & Engineering Lead forms the technical heart of PCI Pal's Information Security function. The role owns cloud architecture review, DevSecOps and secure SDLC practice, security automation and tooling, and security architecture strategy for the organisation, replacing reactive, post-deployment triage with design-stage security input across Engineering, Product and Pre-Sales.

YOU WILL BE RESPONSIBLE FOR:

Cloud Security & Architecture

- Own architecture review and sign-off for all new AWS production changes, including network segmentation, IAM design, and KMS/secrets management etc.
- Threat-model new cloud services and workloads before go-live, rather than reviewing them after deployment.
- Own remediation design, not just triage, for CNAPP and associated cloud security service findings, including closing current findings based upon risk classification and associated requirements.
- Set forward-looking security architecture patterns and guardrails ahead of Engineering's roadmap, not behind it.

DevSecOps & Secure SDLC

- Own CI/CD security gates and Infrastructure-as-Code scanning (e.g. SAST and successor tooling), working jointly with Development Team.
- Develop and maintain security automation, integration and validation tooling using Python and C#/.NET, with appropriate use of PowerShell, Bash and relevant APIs/SDKs.
- Review security-relevant application code and engineering patterns, and produce proof-of-concept code, test harnesses and remediation examples where required.
- Provide secure SDLC guidance to the Engineering function through the central advisory model, design reviews, sign-off gates, and scheduled sessions.
- Extend coverage into container and API security as the function's remit grows (Phase 3 of the deployment plan).

AI & Emerging Risk

- Provide technical engineering support to the AI Security & Governance function for LLM/model security testing (OWASP LLM Top 10 etc.), including scripted test harnesses and repeatable validation tooling, where execution capacity is needed.
- Support technical validation of AI/cloud vendor control claims (e.g. redaction testing, data flow verification) where risk warrants it, alongside AI Security & Governance.

Central Advisory to Engineering, Product & Pre-Sales

- Provide the technical security voice in customer-facing pre-Sales conversations and Product design discussions, on a scheduled and on-request basis.
- Maintain the design review calendar and RACI agreed with Engineering, Product and Pre-Sales, explicitly a central advisory relationship, not a placement or embedded model.
- Lead joint threat-modelling cycles for major product changes.

Governance & Reporting

- Provide technical risk input into Information Security GRC's risk register and Statement of Applicability, rather than GRC compiling technical risk independently.
- Report progress against the Target Operating Model roadmap to the Information Security Project Manager & CISO.

WE WANT TO HEAR FROM YOU IF YOU:

Essential

- Demonstrable and considerable experience in cloud security architecture (AWS essential and Azure), including IAM design, network segmentation, and secrets/KMS management.
- Hands-on DevSecOps experience: CI/CD pipeline security, Infrastructure-as-Code scanning, and policy-as-code.
- Strong hands-on software development and scripting capability, including Python and C#/.NET, with the ability to read, review and write secure production-quality code; familiarity with PowerShell, Bash, REST APIs and common software development tooling.
- Experience building security automation, API integrations, test harnesses or internal engineering tools, using source control, peer review, testing and secure coding practices.
- Experience threat-modelling applications and cloud workloads at the design stage, not just reviewing them after deployment.
- Working knowledge of PCI DSS v4.0.1 and ISO/IEC 27001:2022; familiarity with ISO/IEC 42001:2023 is an advantage.
- Experience triaging and remediating findings from a CNAPP or cloud security posture tool.
- Experience providing technical oversight to an offshore or distributed engineering team, including runbook design and quality assurance.
- Strong stakeholder communication skills, able to advise Engineering, Product and Pre-Sales credibly.
- Extremely strong documentation skills.

Desirable

- Experience with AI/LLM security testing (OWASP LLM Top 10, prompt injection, model/vendor risk assessment).
- Familiarity with the Microsoft 365 E5 security stack (Entra ID, Defender for Endpoint, Intune), given PCI Pal's existing Zero-Trust investment.
- Container/Kubernetes security experience.
- Familiarity with additional engineering languages and ecosystems used in cloud-native environments, such as JavaScript/TypeScript, Java or Go.
- Relevant certification: CISSP, CCSP, AWS Certified Security Specialty, or equivalent.
- Experience operating within a PCI DSS Level 1 service provider or merchant environment.
- Prior experience transitioning a function from reactive/operational delivery to an architecture- and engineering-led model.

CAREER OPPORTUNITIES

IN RETURN WE OFFER:

- 25 days holiday, rising to 28 days per annum with length of service
- Medical, dental and optical insurance cover
- Option to either work in our Ipswich office, or from home (or both!)
- An exciting and flexible working environment surrounded by friendly and committed co-workers
- Electric Vehicle Scheme incentive
- “Work from anywhere” 2 weeks per year policy
- Reward, benefits and wellbeing hub (offering support, discounts, cashback and savings)
- Training and development opportunities
- Ad-hoc team events, incentives and competitions

TALK TO US:
If you have any questions or want to find out more, we’d love to hear from you.

Please contact the Recruitment Team recruitment@pcipal.com