PayPal

Title Manager, Application Security

Primary Job Responsibilities PayPal is the leading, secure way to pay and be paid. PayPal customers trust that their transactions and private information are secure because of the high standards of security enforced for PayPal technology. The application security program is designed to ensure that any software developed or acquired meets these stringent standards while enabling rapid innovation to meet customers' ever-changing needs.

The manager of the application security program will be responsible for:

1. Integrating security tools, standards, and processes into the product life cycle (PLC).
2. Ensuring that developers and QA personnel are trained with the appropriate level of security knowledge to perform their daily activities.
3. Improving and supporting application security tool deployments including static analysis and runtime testing tools.
4. Improving and maintaining secure development standards.
5. Supporting the incident response and architecture review processes whenever application security expertise is needed.
6. Managing annual penetration testing services, including both expert consulting and managed services.
7. Providing manual penetration testing and standards gap analysis services to internal business and technology partners.
8. Managing application framework and perimeter security improvement projects.
9. Supporting Vendor Security activities to ensure 3rd-party software and development meets PayPal security standards.
10. Integrating threat modeling practices into the product life cycle.
11. Providing security requirements for test-driven design.
12. Producing metrics reporting the state of application security programs and performance of development teams against requirements.

Job Requirements Successful candidates will be security evangelists who can translate security concepts into language that is meaningful to many audiences, including business and technical leaders and individual contributors. Candidates must be able to approach application security from the perspective of risk management and avoid purely academic thinking about software security. Demonstrable ability to influence decision-making processes at all levels of a large organization will be critical to success.

Candidates must have strong leadership skills and be effective managers of highly technical individuals.

Candidates must have excellent verbal and written communication skills, including experience speaking in public forums and writing/contributing to technical publications.

Candidates should be familiar with waterfall and agile development processes and have experience integrating secure development practices into both models.

The ideal candidate has experience writing and testing web applications and web services in the following programming languages: C/C++, Java, and JavaScript. The candidate should have familiarity with a variety of development and testing tools, including: Eclipse, GIT, GCC, JIRA, Subversion, Maven, ClearQuest/Case, Silk, FindBugs, HP/Fortify SCA, IBM AppScan, and HP WebInspect

Candidates must be able to explain all vulnerabilities and weaknesses in the OWASP Top 10, WASC TCv2, and CWE 25 to any audience, and discuss effective defensive techniques.

Candidates must have experience managing $1M+ budgets and planning multi-year roadmaps.

Familiarity with industry standards and regulations including PCI, FFIEC, SOX, and ISO27001 is desired.

Education Bachelors degree or higher in Computer Science preferred