SANDEEP JAYASHANKAR

Product and Cloud Security Architect

Contact

Phone
443 845 4288
E-mail
sandeep.jayashankar@gmail.com

Skills

Application & Product Security
Cloud & Container Security
API & Mobile Security
Secure SDLC & DevSecOps
Threat Modeling & Security Architecture
Penetration Testing & Red Teaming

Awards

PayPal Spot Awards:
- implementing SPLC for 25 critical CORP apps
- operationalizing app remediation at scale
- log4j remediation triage and strategy

PayPal Key Talent Award
- implementing scalable Azure DevSecOps

Protiviti iAchieve Award
- Critical Role in Medical Device Testing

Education

Master of Science
Information Security
Johns Hopkins University-Baltimore, MD

Bachelor of Engineering
Electronics and Communications
Sir M. Visvesvaraya Institute of Technology - Bangalore, India

Certifications

Offensive Security Exploitation Expert
Offensive Security Web Expert
Offensive Security Certified Expert
Offensive Security Certified Professional
GIAC Mobile Device Security Analyst

Affiliations

Advisory Board member - EC-Council
Editorial Board member - ISSA Journal
Editorial Reviewer - ISACA Journal

A seasoned security architect with two decades of practical experience in **application, product, and cloud security**, with a primary objective to **operationalize organizations to reduce security tech debt**. A Technologist with a strong background as a **Software Developer** and a **Red Teamer**, with exposure to both **offensive** and **defensive** cybersecurity programs, with a penchant to adopt proactive approach to threat landscape.

Work History

Security Architect

SoFi, *Philadelphia, PA (2022-04 to Current)*

- Worked on creating AWS Technical Security Standards, and enabled enforcement of evaluated cloud security policies, both as proactive and reactive security control.
- Led Security Design, Architecture and Threat Modeling activities for SoFi's Banking, Credit Card, and other critical products/functions, and identified critical design defects and security loopholes.
- Drove Product Security Strategy roadmaps and improvements on programs including Bug Bounty and SAST.
- Led security improvements on Developer Environment, formulated a security risk matrix to help prioritize incoming review requests, and performed threat modeling on mission critical applications.
- Assisted in evaluating security posture during a critical merger, and formulated roadmap improvements post-merger.

Lead Application Security Architect (Engineer)

PayPal, *Philadelphia, PA (2017-05 to 2022-04)*

- Established **PayPal's Mergers and Acquisition Product Security program** and evaluated 7 (seven) oncoming organization's app and cloud/container security posture, while formulating roadmaps to inculcate PayPal's security standards and requirements in all phases of their product life cycle.
- Directed **PayPal's Product Security** program for enterprise and BU environments with primary objective to enable security automation, support zero trust architecture, and implement cloud migration guardrails.
- Advanced "**Paved Road**" or "**Secure Default**" Initiative to scale application security efforts and remediation strategy by providing secure development frameworks, environments, and security tools as part of CI/CD.
- Incorporated PayPal's **API security strategy** to implement authorization and access control, identify business logic abuse cases, and engineered PayPal's microservices security with Service Mesh architecture.
- Operationalized **container** and **application scanning** as part of PayPal's CI/CD framework and created streamlined remediation/waiver process to reduce bottlenecks in product deployment process.

Security Manager - Application and Mobile Security

Protiviti, Inc, *Philadelphia, PA (2014-01 to 2017-04)*

- Spearheaded **Application and Mobile Security practice** and its transformation initiative by bringing in significant enhancements to proposed testing frameworks, methodologies, and remediation strategies.
- Accomplished Protiviti's novel end-to-end service capability for evaluating **API, mobile, and IoT devices**, provided reusable process and tech frameworks on Secure SDLC, surpassing **$1.5 million** in net revenues.
- Developed **penetration testing** and **red teaming** exercises with defined end goals to demonstrate attack vectors that penetrate perimeter defenses, gain total control of CDE/PHI zones to exfiltrate data.
- Supervised, mentored, and developed a team of **penetration testers, red teamers,** and **application security engineers**, building from 4 engineers to a 22 strong team.

Principal Application Security Engineer

Financial Industry Regulatory Authority, FINRA, *Rockville, MD (2011-03 to 2013-12)*

- Led **Application Security Assessments program** handling 150 applications, performing security requirements review, application architecture and design review, threat modeling, secure code reviews, automated and manual penetration testing, and WAF policy reviews.
- **Reviewed and illustrated critical-risk vulnerabilities** to information security steering committee, discussed vulnerability remediation efforts with application and business stakeholders.
- Collaborated to develop **application risk rating matrix** for work prioritization and determining scope for penetration testing and source code assessments
- Configured and fine-tuned **FINRA's WAF** by monitoring for attack patterns and helping development team with interim remediation for detected vulnerabilities, and creating regex rule sets to block real-time attacks

Senior Software Developer, Security

Social Security Administration, *Woodlawn, MD (2010-04 to 2011-03)*

- Developed a new version of HSPD 12 PIV Card Management platform that provided administrators to full-fledged Identity and Access Management platform.

Public Speaking and Publications

- Evaluating Container Security with ATT&CK Framework – PayPal #TechTalk (Nov 2020)
- Runtime Analysis on Mobile Applications – OWASP Philadelphia Chapter (Feb 2017)
- Android Application Penetration Testing – OWASP Philadelphia Chapter (June 2016)
- Implementing Granular Access Definitions in Log Records – SAPUB (Oct 2020)
- Demystifying Tokens for Securing Enterprise APIs – ISSA (June 2020)
- Adopting MITRE ATT&CK Framework – PenTest Magazine (May 2020)
- 6 ways HTTP/3 benefits security – CSOOnline Magazine (July 2020)