Henry Asare Principal Application Security Engineer

Boston, MA · henry.asare@gmail.com · +1 617-555-0192 · linkedin.com/in/henryasare

PROFILE SUMMARY

- **Principal Application Security Engineer** with **15 years** in financial services AppSec, now running the **application security program** for a **life insurer's** customer, agent and policy systems across **1,100 developers**.
- Hands-on with **Java**, **C#** and Python code, **Checkmarx** and Semgrep scanning, **Burp Suite Professional**, **Snyk** and Black Duck, and **HashiCorp Vault** for application secrets.
- Deep expertise in **AppSec program design**, **SAST tool consolidation**, **risk-tiered design review** and **regulated-industry controls** like NYDFS Part 500 and PCI DSS 4.0, with progress tracked in OWASP SAMM.
- Works with the **CISO**, engineering VPs, **internal audit** and the risk office, and presents the AppSec scorecard to the **technology risk committee** every quarter.
- Chairs the **AppSec architecture council**, wrote the company's secure SDLC standard, grew a **security champions network** of 70, and has mentored 6 engineers into senior roles.

TECHNICAL SKILLS

Languages & Frameworks:	Java, Spring Boot, C# / .NET, Python, TypeScript, Kotlin
SAST & Code Scanning:	Checkmarx, Semgrep, CodeQL, Veracode, Gitleaks
DAST & Pentest Tools:	Burp Suite Professional, Burp Suite DAST, OWASP ZAP, pentest vendor management
SCA & Supply Chain:	Snyk, Black Duck, CycloneDX, SLSA, NIST SSDF
Threat Modeling & Standards:	STRIDE, PASTA, OWASP ASVS (Levels 2 and 3), OWASP SAMM, PCI DSS 4.0, NYDFS Part 500
Auth, API & Crypto:	OAuth 2.0, OpenID Connect, SAML, mTLS, HashiCorp Vault, Azure Key Vault
CI/CD, Cloud & Bug Bounty:	Azure DevOps, GitHub Actions, Azure, AWS, Bugcrowd, ServiceNow

EDUCATION

Carnegie Mellon University — **M.S. in Information Security** — Pittsburgh, PA · Aug 2009 to May 2011

WORK EXPERIENCE

John Hancock — **Principal Application Security Engineer** — Boston, MA · Apr 2018 to Present

- Built the AppSec program for **1,100 developers** across 5 business lines, with a secure SDLC standard mapped to OWASP ASVS and NIST SSDF that internal audit now tests against.
- Consolidated 3 SAST tools into **Checkmarx** and Semgrep in Azure DevOps pipelines, cutting licensing spend by **31%** while every repo moved to a scan on each merge.
- Set fix deadlines by severity and a monthly scorecard for engineering VPs, cutting the median time to fix a critical application finding from **42 days to 9**.
- Started a design review board for new customer and agent apps, reviewing **85+ designs** a year with a risk-tiered **STRIDE** process so low-risk changes skip the full review.
- Rolled out **CycloneDX** SBOMs and Snyk policy gates for customer-facing apps, cutting the time to find every app using a newly disclosed vulnerable library from 2 weeks to **4 hours**.

MFS Investment Management — **Senior Application Security Engineer** — Boston, MA · Jul 2011 to Mar 2018

- Ran manual code review on **Java** and C# trading and advisor portal apps, finding **64 high-severity bugs** over 6 years, mostly injection and access control flaws.
- Scoped and managed yearly outside pentests on **12 client-facing apps**, retesting every fix in Burp Suite before closing the finding with the vendor.
- Moved the advisor portal from custom login code to **SAML** single sign-on with MFA, closing all **5 session management findings** from the previous pentest.