Sienna Brookes Senior Application Security Engineer

New York, NY · sienna.brookes@gmail.com · +1 212-555-0148 · linkedin.com/in/siennabrookes

PROFILE SUMMARY

- **Senior Application Security Engineer** with **7 years** in AppSec, now owning **threat modeling and code scanning** for a **cloud security platform** used by large enterprises, after 3 years securing **fintech money movement**.
- Hands-on with **Go** and **TypeScript** code, custom **Semgrep** rules and **CodeQL**, **Burp Suite Professional**, **Snyk** and Dependabot, and GraphQL and REST API testing in **Postman**.
- Deep expertise in **multi-tenant isolation**, **STRIDE threat modeling**, **custom SAST rules** and **API authorization**, mapped to OWASP ASVS Level 2 so findings line up with what customers ask about in security reviews.
- Works with the **platform, data pipeline and frontend teams**, the detection team and compliance, and chairs the **weekly design review** where new services get their security sign-off.
- Coaches newer AppSec engineers, runs the **security champions program**, and keeps the **Semgrep rule library** that every new service picks up on its first day.

TECHNICAL SKILLS

Languages & Frameworks:	Go, TypeScript, React, Node.js, Python, GraphQL
SAST & Code Scanning:	Semgrep (custom rules), CodeQL, GitHub Advanced Security, Gitleaks
DAST & Pentest Tools:	Burp Suite Professional, Postman, Nuclei, OWASP ZAP
SCA & Supply Chain:	Snyk, Dependabot, Syft, CycloneDX, Sigstore Cosign
Threat Modeling & Standards:	STRIDE, attack trees, OWASP ASVS (Level 2), OWASP API Security Top 10, CWE
Auth, API & Crypto:	OAuth 2.0, OpenID Connect, JWT, SAML, mTLS, AWS KMS
CI/CD, Cloud & Bug Bounty:	GitHub Actions, Kubernetes, Docker, AWS, Jira

EDUCATION

NYU Tandon School of Engineering — **B.S. in Computer Science** — Brooklyn, NY · Sep 2015 to May 2019

OffSec — **OSWE certification** — New York, NY · Mar 2023

WORK EXPERIENCE

Wiz (Google Cloud) — **Senior Application Security Engineer** — New York, NY · Apr 2022 to Present

- Ran **STRIDE** threat models on new cloud connectors and APIs with a focus on tenant boundaries, getting high-risk design changes agreed before coding started on **95%** of them.
- Wrote **62 custom Semgrep rules** for Go patterns that break tenant scoping, like a database query with no tenant filter, and ran them on every pull request across 90+ services.
- Fixed authorization on **48 GraphQL and REST endpoints** by moving tenant checks into shared middleware, closing the cross-tenant access bug class an outside pentest found in 2023.
- Set fix deadlines by severity for pentest, scanner and customer-reported findings, and cut the median time to fix a critical finding from **18 days to 5**.
- Wrote the security champions playbook that **6 product groups** now use to run their own first-round design reviews, and mentored 3 AppSec engineers through their first year.

Betterment — **Application Security Engineer** — New York, NY · Jul 2019 to Mar 2022

- Reviewed **Ruby on Rails** code for deposits, withdrawals and transfers, finding **23 money-movement bugs**, including a race condition that allowed a double withdrawal.
- Rolled out **Snyk** across 120 repos with an upgrade policy for critical packages, cutting open critical dependency vulnerabilities from 85 to **7** in 9 months.
- Tested the iOS and Android app APIs with **Burp Suite** before each major release, finding **11 high-severity issues**, mostly broken object level authorization on account endpoints.