BRENNAN LEBLANC

Cybersecurity Professional | Seattle, WA | www.linkedin.com/in/brennan-leblanc-4619a51a9 | GitHub: Brennan-LeBlanc-spu

SUMMARY

Security Engineer with 2 years of specialized experience in vulnerability management, application security, and AWS cloud security. Established a NIST-compliant vulnerability management program at PRISIDIO that reduced critical vulnerabilities by 20% while strengthening cross-team collaboration. Proficient in secure AWS architecture design, IAM best practices implementation, and full-stack development using security-by-design principles. Seeking to leverage technical expertise and security background to protect critical infrastructure and sensitive data.

SKILLS

- Technical: Python, JavaScript, React, Rust, AWS Development, lambda, API's, Vulnerability Management, Vulnerability Scanning, Secure Coding Practices, Resource Management, Risk Management, Strategic Alignment, AWS Cloud Security, AWS Cloud Deployment, Incident Response, IAM Polices, Zero Trust, Compliance, Patch Management

- Google AI Essentials Certificate, Pursuing Security + from CompTIA and AWS Cloud Practitioner

PROFESSIONAL EXPERIENCE

PRISIDIO Cybersecurity Analyst | 08/2024 - Present

- Implemented vulnerability management program at Prisidio, creating 100% coverage of code assets, 20% reduction in Critical Vulnerabilities, enabling early detection of vulnerabilities, and reducing deployment delays by building SAST, SCA, IaC, and DAST Scanners into the CI/CD pipeline and release cycle.
- Integrated software development and architecture team with vulnerability management program, creating developer buy-in and reducing mobile risk by 30% by following Industry Standards with vulnerability remediation.
- Responded to one of the Websites going down after a faulty configuration of CAAs and got it back online by renewing SLL/TLS certificates and updating CAAs to allow for the CA authority to be accepted.

PRISIDIO Information Security Intern/Security Engineer/Software Engineer | 05/2024 - 08/2024

- Engineered and secured a full-stack threat feed website, implementing multiple security controls, including input validation, authentication, and secure API integrations
- Conducted comprehensive web application penetration testing, identifying and remediating 12+ critical vulnerabilities across company digital assets
- Architected and deployed secure AWS infrastructure using IAM best practices, S3 encryption, and security groups to maintain data confidentiality
- Developed both frontend (React) and backend (Node.js) components with security-by-design principles, including XSS protection and secure data handling

Strategic Alliance Consulting Cybersecurity Analyst Intern | 05/2023 - 12/2023 | Bellevue, WA

- Conducted research on generative AI and its implications on Phishing Scams.
- Architected Network Topology for Ethical Hacking for implementing Ransomware, testing the capabilities of Generative AI ability to generate malicious code in the form of Ransomware.
- Collaborated with senior security engineers to deploy Network Topology in AWS, creating an Ethical Hacking Environment and Successfully Implementing part of the Ransomware, encrypting 100% of user files in their directory.

EDUCATION

Bachelors in computer science | 06/2025
Seattle Pacific University - Seattle, WA