Brennan LeBlanc

Cybersecurity Analyst at Prisidio

E 206-484-5065 brennan.leblanc.cs@gmail.com q https://github.com/Brennan-LeBlanc-spu

Seattle, WA Portfolio: https://brennan-leblanc-spu.github.io/

SUMMARY

As a Cyber Security Analyst at Prisidio, I leverage my skills in full stack

development and cloud computing to enhance the security of web. applications. I have experience in architecting and implementing responsive Front end using React.js, engineering scalable backend infrastructure on AWS, and managing full deployment pipelines. I also have a strong background in cybersecurity, having worked as an InfoSec Intern at Prisidio and focusing on MDR and Pen-testing with the SAC team. I am passionate about staying updated with the latest technologies and trends in the field, and I am always eager to learn new skills and take on new challenges.

EXPERIENCE

Cybersecurity Analyst

Prisidio

10/2024 - Present Remote

Digital Vault Company

- Implemented and built SAST, SCA, and DAST vulnerability management programs at Prisidio, creating 100% coverage of code assets.
- Integrated security scanning into the CI/CD pipeline, enabling early detection of vulnerabilities and reducing security-related deployment delays by 50%.
- Led the integration of software development and architecture teams with a vulnerability management program, creating Shift left by Design.
- Implemented a risk-based prioritization framework that aligned remediation efforts with business impact, optimizing security resource allocation and reducing overall organizational risk exposure.

Information Security Intern

Prisidio

06/2024 - 09/2024 Remote

Digital Vault Company

- 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

Cybersecurity Analyst Intern

Strategic Alliance Consulting

06/2023 - 06/2024 Bellevue, WA

IT and Security Consulting Company

- Conducted research on generative AI security applications, creating proof-of-concept tools to enhance threat detection capabilities
- Architected and deployed secure AWS infrastructure using IaC principles, implementing defense-in-depth strategies and compliance controls
- Collaborated with senior security engineers to develop client-facing security assessment reports and remediation recommendations

CERTIFICATIONS

Google AI Essentials from Coursera

TCP/IP Deep Dive for Ethical Hackers from Chris Geer

EDUCATION

BA in Computer Science

Seattle Pacific University

10/2021 - 06/2025 Seattle, WA

PROJECTS

Vulnerability Management Program - Prisidio

10/2024 - Present Remote

My project was to create Prisidio's Code Analysts Vulnerability Management program.

- Implemented multiple SAST, SCA, DAST, and Infrastructure Code Scanners.
- Created Policies and Procedures within the development to create a Shift Left by Design based on Industry Standards.
- Patch management based on vulnerabilities found by the scanners

Full Stack Threat Feed Website - Prisidio: https://github.com/Brennan-LeBlanc-spu/GeekFood.net

06/2024 - 09/2024 Remote

As part of my internship at Prisidio, I was tasked with leading the Full Stack Development of a Threat Feed Website

- Developed Front-End in React and back-end in Python.
- The architecture was done with AWS resources (API Gateway, Lambda, DynamoDB. etc.)
- Pen-tested website and remediated vulnerabilities found in the website.

Ethical Hacking, Generative AI Research - SAC

06/2023 - 06/2024 Bellevue, WA

My project was to research the extent of Generative AI's ability to create malicious code

- Create AWS Environment/Infrastructure for Ethical Hacking.
- Created Malicious Code (Ransome Ware) that effectively encrypts 100% of the victim's files within their directory.

EXPERIENCE

Software Engineer Electronics Co-Lead

Seattle Pacific University Baja Racing

10/2022 - 10/2024 Seattle, WA

Baja Racing Team

- Architected and developed a full-stack car dashboard application using TKinter, Python, and SQLite, providing real-time vehicle performance metrics for race drivers
- Engineered hall effect sensor systems to precisely measure axle speed and RPM with 98% accuracy, enabling critical race performance data collection
- Implemented a high-definition backup camera system with a custom interface, enhancing driver visibility and improving safety during competition maneuvers
- Led a team of 5 electronics engineers, coordinating project timelines and technical specifications while meeting all competition deadlines
- Collaborate cross-functionally with mechanical and chassis teams to integrate electronic systems with physical vehicle components

PROJECTS

Baja Racing Car Dash - SPU Racing

https://github.com/Brennan-LeBlanc-spu/bajaGUI

10/2022 - 10/2024 Seattle, WA

Built Baja Racing Car Dash

- Displayed Speed, RPMs
- Secured and stored Speed and RPM data in SQLite
- Analyzed Data from SQLite to make decisions on how the car was going to be build.
- Built Front-End Display in TKinter
- Calculations and distribution done in python
- Network and Electrical Topology for wiring in Car

What Color – SPU CapStone

https://github.com/What-Color-SPU/What-Color- spu/bajaGUI

10/2024 - 5/2025 Seattle, WA

Android App to help colorblind individuals and others pick out their closet

- Implemented Secure Coding Practices
- AWS Architecture
- Semgrep for scanning

Rust Parser – SPU

https://github.com/Brennan-LeBlanc-spu/Rust_Parser

10/2023 - 11/2023 Seattle, WA

- Developed a custom syntax analyzer in Rust that parses and validates programming language structures. Implemented lexical analysis and recursive descent parsing techniques to efficiently process source code tokens. The project demonstrated proficiency in compiler design principles, advanced data structures, and Rust's memory-safe programming paradigm.
- Engineered a robust parser that accurately identifies and validates syntactic structures
- Leveraged Rust's ownership model and pattern matching to create efficient, memory-safe code
- Implemented error handling mechanisms to provide meaningful feedback for syntax errors
- Applied computer science theory to create a practical programming tool
- Collaborated with peers and instructors through Git version control