Don Brightson

Security & Software Engineer

Portfolio: www.donbrightson.tech | Email: dbrightson78@gmail.com
Github: github.com/dbrightson | LinkedIn: linkedin.com/in/donbrightson
Address: Chennai, Tamil Nadu, India | Contact: +91 9884054579

Summary

Security Engineer with strong background in incident response, malware analysis, forensic investigations, and threat detection. Experienced in scripting (Python, Bash), log analysis, and automating security workflows across hybrid cloud environments (AWS/GCP). Integrated ML models with Azure Sentinel for anomaly detection, and developed real-time dashboards for SOC visibility. Contributed to an open-source interactive graph analytics platform as part of a virtual software engineering experience at J.P. Morgan. Passionate about root-cause analysis, defending distributed systems at scale, and driving measurable operational improvements.

Education

Sri Muthukumaran Institute of Technology, Chennai, India (Sept 2020 – June 2024)
Bachelor of Engineering - Computer Science & Engineering (GPA: 8.12/10)

Skills Summary

- **Programming Languages:** Python (Expert), Java, JavaScript, SQL, C++
- **Security Concepts & Tools:** Security Automation, IAM Principles (SAML, OAuth, OIDC), Risk Assessment (CVSS), Vulnerability Management, Secure Coding (OWASP), SIEM (Azure Sentinel), Network Security (TCP/IP, DNS), System Hardening, Basic Burp Suite
- **Frontend:** ReactJS, NextJS, HTML, CSS, TypeScript
- **Backend & DevOps:** NodeJS, ExpressJS, MongoDB, Firebase, MySQL, REST APIs, CI/CD Concepts, Agile Methodologies, Microservices Architecture
- **Cloud & Platforms:** Google Cloud Platform (GCP), AWS (EC2, S3, IAM, CloudTrail, Lambda, CloudWatch, VPC), Docker, Kubernetes, Git, Postman, Linux
- **Core CS & Soft Skills:** OOPS, Data Structures, Algorithms, AI/ML Concepts, Analytical Thinking, Communication, Problem-Solving

---

Achievements

- **1st Place - Bot Brains Battle 2024, IIT Bhubaneshwar:** Engineered a real-time AI algorithm for robotics decision-making under high-pressure scenarios.
- **Top 15 Project - Naan Mudhalvan Competition 2023:** Developed an AI-based real-time legal chatbot recognized by the Tamil Nadu Chief Minister for innovation.

Work Experience

Flipkart – Associate Security Engineer (May 2025 – Present)

- Integrated machine learning algorithms (LOF, Isolation Forest) with Azure Sentinel SIEM for proactive threat detection and incident response optimization.
- Developed an online assessment platform and ATS that handled 40,000+ applications, saving 100+ hours/month.
- Built real-time SOC and security monitoring dashboards for IAM, endpoints, servers, and networks, improving monitoring efficiency by 30% and reducing response time by 25%.

Flipkart – Information Security Trainee (Nov 2024 – May 2025)

- Automated security workflows with Python, enhancing SOC efficiency in vulnerability assessments and compliance checks.
- Aided in drafting and enforcing hardening policies to improve system resilience and enterprise-wide compliance.
- Proposed optimizations that reduced project costs by 10% and saved analysts 5+ hours/week through automation.
- Practiced risk assessment and vulnerability prioritization in a large-scale hybrid cloud environment.

J.P. Morgan (Virtual Experience) – Software Engineer (July 2024 – Sept 2024)

- Participated in a virtual internship focused on software engineering fundamentals and data-driven UI design.
- Improved a React-based stock price visualization dashboard to handle real-time API updates and client-side rendering performance.
- Resolved feature bugs and optimized user interactions to deliver a cleaner, more interactive financial analytics platform.

Projects

Voice of Justice – AI-Assisted Legal Consultation

- Developed a multi-platform legal chatbot increasing consultation efficiency by 40%.
- Implemented JWT-secured auth, integrated real-time lawyer databases, increasing user engagement by 25%.
- Built a web scraper to aggregate legal data dynamically, enhancing data quality and UX.

Context-Aware DLP – Semantic - First Data Loss Prevention System

- Built a real-time DLP engine using FastAPI and sentence-transformers to semantically detect PII, secrets, credentials, and financial/medical data in free-text inputs.
- Trained a logistic regression model on 300+ examples with nlpaug-based data augmentation, achieving high recall with low false positives across domains.
- Developed an interactive web interface using React, TypeScript, and TailwindCSS for inline content inspection and feedback submission.
- Integrated a feedback loop to flag and retrain on false positives/negatives, enabling continuous learning and context adaptation.
- Outperformed traditional DLP (regex/keyword-based) by 40% in detecting hidden sensitive content during comparative benchmarks.