

Sandeep Rajendiran

571-245-0611 | sandeep76575@gmail.com | [Linkedin](#) | [Github](#) | Fairfax, Virginia

TECHNICAL SKILLS

Languages: Java, Python, C, Golang, Typescript/React, SQL, JavaScript, PowerShell, Bash scripting
Security Tools: Metasploit, Nmap, Wireshark, Burp Suite, OWASP ZAP, SQLMap, Nessus, Kali Linux, Snort
Cloud & DevOps: AWS (EC2, S3, IAM, VPC, ECS, DynamoDB, Lambda, SQS, and Step Functions), Kubernetes, Terraform, Git
Cybersecurity: Web & Mobile Penetration Testing (VAPT), IDS/IPS, SIEM (Splunk, Sentinel), YARA, Sigma Rules, OWASP Top 10, LLM Security (Prompt Injection, Data Poisoning), CVE, MITRE ATT&CK framework, Red Teaming
Operating Systems: Windows, Mac, Windows Server 2019/2016/2012 R2, Linux & Unix (Ubuntu, Kali, Cent)

CERTIFICATIONS

AWS Certified Solutions Architect – Associate | AWS Cloud Practitioner | eJPT v2 | Google Cybersecurity Professional | PT1

EXPERIENCE

Security Engineer

June 2025 – Present

Bravent LLC

- Led the planning and compliance strategy for a **government-grade tool** that automated vulnerability scanning of 100+ web apps/APIs, aligning findings with **20+ federal frameworks** (e.g., NIST SP 800-53, FedRAMP, FISMA).
- Integrated **30+ scanning tools** (ZAP, Wapiti, Nikto, Lighthouse, SSLyze, WhatWeb) and developed a unified parser to normalize JSON/CSV findings, increasing reporting accuracy by **75%**.
- Mapped 5,000+ scan results to 300+ compliance controls across frameworks like **CMMC, ZTM, BOD 22-01**, reducing manual compliance workload by **65%** through automated logic mapping.
- Implemented full **OWASP Top 10 coverage** with deep web application testing to detect 200+ monthly vulnerabilities (injection, misconfigurations, access control flaws) and leveraged **Agentic AI** to dynamically prioritize findings, recommend remediations, and auto-generate compliance-ready reports, reducing triage time by 50%.

Software Engineer

Oct 2022 – Aug 2023

Accenture

- Led end-to-end **vulnerability assessments** and **penetration testing** initiatives, implementing robust security measures that mitigated potential risks. reducing security breaches by 50% and strengthening network resilience.
- Implemented and managed **Azure Defender for Cloud** and **Azure Sentinel**, refining **IDS/IPS** configurations that improved threat detection accuracy by 35% within three months, enhancing cloud security posture.
- Conducted security event monitoring and analysis within a SOC using **Splunk**; detected and analyzed threats, performed **root cause analysis (RCA)**, and contributed to improving containment workflows for accelerated incident response.
- Distinguished in IT Security and Security Incident Response, Security controls and **Endpoint Security**. Proficient in Risk Management and **Cloud Security**, with expertise in Access Management and Information Security.
- Developed comprehensive documentation detailing system configurations, **CI/CD** security integration and **security protocols**, which led to a measurable **30% increase in team compliance** with established industry standards and enhanced knowledge retention practices across departments.

PROJECTS

OpenIntel – OSINT Reconnaissance Framework | *Bash, Python, GCP*

- Developed a **modular OSINT tool** integrating **12+ APIs** (Shodan, IPStack, etc.), automating reconnaissance workflows and reducing manual effort by 70% across 500+ data points.

AI-Driven Threat Detection & Automated Security Response | *AWS CloudFormation, Terraform*

- Built a **serverless threat detection pipeline** using AWS GuardDuty, Lambda, and Lookout for Metrics, improving breach detection and response time by 40% via automated AI-driven actions.

EDUCATION

Masters of Science in Information Systems

George Mason University

Fairfax, VA

(Graduated) Aug 2023 - May 2025

Bachelor of Engineering in Computer Science

Anna University

Chennai, India

(Graduated) June 2018 - May 2022

ACHIEVEMENTS

- Discovered and reported critical security vulnerabilities, including **XSS, IDOR, SQL Injection** preventing potential financial losses exceeding **\$100,000**; earned recognition in **Indeed's Hall of Fame**, **Atlassian** and **Google VRP appreciation**.
- Strengthened organizational defenses against cyber threats by systematically documenting and reporting all identified **OWASP Top 10 vulnerabilities** via recognized bug bounty platforms like **Bugcrowd, HackerOne** and CTF competitions facilitated prompt responses from security teams.