

ANSHUMAN SINGH

720.546.3166 | Denver, CO | anshumans.work96@gmail.com | [GitHub](#) | [LinkedIn](#) | [Medium](#) | [Portfolio](#)

INFORMATION SECURITY ENGINEER

SUMMARY

Innovative Cybersecurity Engineer with a strong computer science and engineering foundation, specializing in designing and deploying secure systems to protect critical infrastructures. Adept at integrating advanced security solutions with engineering principles to enhance organizational resilience against modern threats. Experienced in automation, cloud security, and regulatory compliance, with a proven track record of implementing cutting-edge technologies and frameworks. Open to relocation across the U.S., committed to driving secure engineering practices and delivering impactful solutions.

TECHNICAL SKILLS

Operating Systems: Windows Operating System, Linux Distributions, Cisco IOS, Mac Operating System, UNIX, Parrot OS

PKI & Cryptography: Venafi, Keyfactor, Entrust, DigiCert, PKI Spotlight, SSL/TLS, Certificate Lifecycle Management, Cryptographic Key Management, PKCS Standards, Digital Signatures

Security Tools: Kali Suite, YARA, Nessus, Splunk, MITMProxy, Sigma, GNS3, Cisco Packet Tracer, Wireshark, Metasploit, Burp Suite, Snort, VMware, vSphere, Active Directory, Microsoft O365, Frida, Objection, Android Debug Bridge, Cowrie, DAST/SAST

Programming & Scripting: Python, Bash, PowerShell, Java, JavaScript, C Programming, RESTful API, Pandas, Matplotlib, Plotly, Numpy, Flask

Malware Analysis Tools: Process Explorer, CFF Explorer, Fiddler, Regshot, Process Monitor, Process Hacker

Cloud Security Platforms: AWS Tools, IBM Cloud, Microsoft Azure Security, Google Cloud Security, Google Cloud Platform (GCP), OpenStack, Cloud Access Security Brokers (CASBs), Endpoint Security, IAM, SIEM

Compliance & Regulatory Frameworks: GDPR, HIPAA, NIST, CISA, ISO 27001, SOC 2, CIS Controls, COBIT, SANS Top 20, OWASP Top 10, Cyber Kill Chain, MITRE ATT&CK, Payment Card Industry Data Security Standard (PCI DSS), FISMA

Core Cybersecurity Skills: Threat Intelligence, Incident Response, Vulnerability Management, Data Privacy, Log Analysis, Security Automation, Zero Trust Architecture, AI/ML in Cybersecurity, Digital Forensics, Networking

Networking: TCP/IP, IPv4, IPv6, SFTP, SSH, RDP, Load Balancing, DNS Resolution, Firewall (Cisco ASA, Palo Alto, Fortinet)

Identity & Access Management: SailPoint, Okta, CrowdStrike, Trend Micro, EDR Solutions, Sophos, CyberArk, Qualys

DevOps & Automation Tools: Ansible, Terraform, Kubernetes, CI/CD Pipelines, Git, GitLab, SVN, Artifactory, SonarQube, ELK Stack (Elasticsearch, Logstash, Kibana), Docker, OpenShift

Databases: MySQL, PostgreSQL, Microsoft SQL Server, MongoDB, Redis, Cassandra

Monitoring & Analytics: Zabbix, Nagios, Cacti, Datadog, SolarWinds, Google Analytics, Adobe Analytics

Project Management & Collaboration Tools: JIRA, Trello, Slack, Microsoft Teams, Confluence, Service Now, Remedy

EDUCATION

• **MS in Cyber Security & Privacy**, *New Jersey Institute of Technology* (2022 - 2024)

• **BTech in Computer Science & Engineering**, *Kurukshetra University* (2015 - 2019)

PROFESSIONAL EXPERIENCE

Cyber Security Specialist, *Rebecca Everlene Trust Company* (Aug 2024 - Present)

- Designed and implemented comprehensive cybersecurity policies and procedures across the organization, achieving full compliance with GDPR, CCPA, and FERPA standards.
- Spearheaded the deployment of Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA), reducing unauthorized access incidents by 30% and streamlining authentication workflows.
- Established and maintained an incident response framework, minimizing detection-to-resolution time for security breaches and reducing downtime by 20%.
- Partnered with IT and development teams to enforce secure software practices, aligning code reviews and deployments with OWASP Top 10 guidelines.
- Conducted regular threat assessments and vulnerability scans using Nessus and Burp Suite, mitigating over 85% of critical vulnerabilities and enhancing system resilience.
- Led company-wide security training initiatives, improving phishing detection rates by 40% and fostering a security-conscious culture.
- Monitored and analyzed network activity using Splunk, proactively identifying and resolving potential security breaches.
- Authored comprehensive compliance reports for internal and external audits, demonstrating improved security posture and achieving positive audit outcomes.

Data Protection & Privacy Researcher, NJIT Ying Wu College of Computing (Sept 2022 - Jun 2024)

- Led a research initiative utilizing machine learning and natural language processing techniques to detect privacy violations in Android healthcare applications, assessing data sharing practices and retention policies.
- Performed comprehensive GDPR compliance audits for healthcare applications, identifying critical vulnerabilities and implementing AI-driven solutions to enhance data privacy.
- Audited and analyzed over 10,000 Android apps using tools like Frida and ADB, improving secure coding practices with GitHub Copilot and reducing compliance errors by 25%.
- Engineered AI-powered methodologies to evaluate the compliance of consent notices with GDPR requirements, uncovering discrepancies in data sharing and retention disclosures.
- Designed Python-based automated vulnerability assessment scripts, reducing manual analysis time by 60% and enabling faster and more accurate threat detection.
- Collaborated with cross-functional research teams to address emerging privacy challenges, successfully integrating solutions into active projects.
- Applied threat modeling techniques to preemptively identify and mitigate risks in application development, safeguarding sensitive data against breaches.
- Mentored graduate students on secure software development practices and regulatory compliance, cultivating a new generation of privacy-focused developers.

Cyber Security Engineer, Infosys Ltd. (Nov 2019 - Jul 2022)

- Automated security workflows using Python and Bash scripting, reducing manual vulnerability scanning efforts by 40% and supporting a team of 10 analysts across global environments.
- Designed and implemented RESTful APIs to integrate security tools (e.g., Nessus, Burp Suite) into CI/CD pipelines, reducing deployment testing time by 30% and streamlining security validation across 100+ monthly deployments.
- Developed scalable pipelines using Python (Pandas, NumPy) and visualization tools (Matplotlib, Plotly) to analyze 10GB+ daily network log data, automating threat detection reporting, and enhancing detection accuracy.
- Led a team of 7 engineers to design and deploy a modular DDoS mitigation framework, achieving 50% faster recovery times in simulated attack scenarios.
- Contributed to full-stack development of analytics dashboards using React (JavaScript) and Flask (Python), providing real-time monitoring for incident response teams and reducing investigation times by 25%.
- Enhanced CI/CD pipelines by integrating automated code review tools (SonarQube) and dynamic application security testing (DAST), reducing vulnerabilities detected in pre-deployment testing by 35%.
- Improved system configurations for firewalls and IDS (Cisco ASA, Palo Alto, Snort) as part of a company-wide initiative to align with industry standards, increasing threat detection rates by 25%.

CERTIFICATIONS

- **AWS Certified AI Practitioner** (Amazon Web Services, Sept 2024) [[URL](#)]
- **CompTIA Security+** (CompTIA, Dec 2024) [[URL](#)]

KEY PROJECTS

- **GDPR Compliance in Android Apps** [[URL](#)]
Analyzed privacy and compliance violations in Android healthcare apps using ML and NLP models with tools like Frida, Objection, Scikit-learn, and ADB, identifying GDPR compliance issues in 70% of cases.
- **Open Source Intelligence (OSINT) Gathering** [[URL](#)]
Developed a Python-based tool integrating Recon-ng, theHarvester, and Shodan to automate data collection and visualization for cybersecurity assessments, reducing manual effort by 50%.
- **Automated Threat Detection System** [[URL](#)]
Created an AI-powered framework using Python and GPT-3 API to detect and respond to network threats in real time, reducing detection time in simulated environments by 40%.
- **Honeypot Deployment and Threat Analysis with ELK Stack** [[URL](#)]
Deployed an SSH honeypot with Cowrie and integrated it with an ELK Stack to capture, analyze, and visualize real-world cyberattacks, enhancing proactive threat detection capabilities.
- **Defense Mechanisms Against DDoS Attacks** [[URL](#)]
Authored and presented a research paper on Distributed Denial-of-Service (DDoS) attacks and defense mechanisms, analyzing attack trends and innovative mitigation strategies, published in IGI Global.