ANSHUMAN SINGH

+1(720) 546-3166 | Denver, CO | anshumans.work96@gmail.com | GitHub | LinkedIn | Medium | Portfolio

CYBER SECURITY SPECIALIST

SUMMARY

Innovative and results-oriented cybersecurity specialist with extensive experience safeguarding digital assets and ensuring regulatory compliance. Proficient in designing robust security frameworks, mitigating vulnerabilities, and implementing AI-driven solutions to combat evolving threats. Adept at leveraging cutting-edge tools and cross-functional collaboration to enhance threat intelligence and incident response capabilities. Open to relocation across the U.S. and committed to driving cybersecurity excellence for organizations of all sizes.

TECHNICAL SKILLS

Operating Systems: Windows Operating System, Windows Server Series, Linux Distributions, Cisco IOS, Mac Operating System, UNIX

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 (ADB), Cowrie

Programming & Scripting: Python, Bash, PowerShell, Java, JavaScript, C Programming, Kotlin

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), Federal Information Security Management Act (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 Management (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

CERTIFICATIONS

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

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 Analyst*, Infosys Ltd. (Nov 2019 - Jul 2022)*

- Monitored and analyzed network traffic and system logs using SIEM tools like Splunk to identify potential threats and ensure compliance with organizational security protocols.
- Managed a queue of ServiceNow tickets, ensuring timely resolution of security-related requests and incidents while maintaining detailed documentation for audit purposes.
- Conducted routine vulnerability assessments and supported security audits, identifying misconfigurations and recommending actionable remediation strategies.
- Documented incident details, performed root cause analysis, and assisted in containment and recovery processes as part of incident response efforts.
- Collaborated with IT teams to configure firewalls, intrusion detection systems (IDS), and endpoint protection tools, ensuring alignment with organizational security policies.
- 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 [URL].
- Delivered security awareness training to over 500 employees, reducing successful phishing attempts by 40% and fostering a security-conscious workplace culture.
- Designed and implemented automated scripts to streamline vulnerability scanning and reporting, reducing manual effort by 30% and improving report accuracy.

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%.
- **Enterprise Network Simulation**
  Designed virtual network architectures using Cisco Packet Tracer and Wireshark to simulate and test defenses against DDoS and On-path attacks, improving the resilience of test setups.
- **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.