Ashish Dev Choudhary

Tucson, AZ | ashishdevchoudhary@gmail.com | LinkedIn: ashishdev13 | GitHub: Ashishdev13

Professional Summary

SOC Analyst with hands-on experience in real-time security monitoring, incident triage, and threat detection across SIEM platforms and endpoint security tools. Proficient in Python-based automation, OSINT-driven threat intelligence, and MITRE ATT&CK-aligned TTP analysis. Eager to apply blue team expertise and strong investigative skills to strengthen SOC operations and reduce organizational risk.

Technical Skills

Languages: Python, Java, C, JavaScript, HTML, SQL.
Frameworks: CSF, COBIT, ISO 27001, Pandas, NumPy, Scikit-learn, OpenCV, Git, Docker, AWS, Azure.
Core Skills: SIEM, Incident Response, Threat Intelligence, Threat Hunting, Malware Analysis, Network Security Monitoring, Log Analysis, Endpoint Security, OSINT, Vulnerability Management, Cloud Security, IPS, IDS, Information Security.
Certifications: ICCA | eJPT | CompTIA Security+

Professional Experience

Cybersecurity Fellow (Reviewer), Handshake AI – San Francisco, CA **Sep 2025 – Present**

- As **Reviewer**: Auditing and refining prompt-response pairs, ensuring accuracy, safety, and consistency across cybersecurity-focused LLM projects.
- Providing structured feedback to trainers, improving research quality and maintaining high standards across submissions.
- As **Trainer**: Developed domain-specific prompts and evaluated LLM outputs to enhance correctness and model alignment.

UG Cybersecurity Research Assistant, University of Arizona – Tucson, AZ **Jan 2026 – May 2026**

- Identified and classified injection, access control, and misconfiguration vulnerabilities across 200+ LLM-generated configurations.
- Built a Python pipeline combining static analysis, rule-based scanning (Semgrep/Bandit), and LLM reasoning to detect injection, access control, misconfiguration, and crypto flaws.
- Designed a critique-based evaluation framework to assess LLM-generated code/configurations against OWASP Top 10 vulnerabilities.

Junior Security Operations Analyst, CyberEyeAW – Sierra Vista, AZ **May 2025 – Aug 2025**

- Monitored and analyzed more than 100 weekly security incidents, enabling real-time response and safeguarding sensitive data with a 99% resolution rate.
- Conducted vulnerability assessments and applied mitigations that reduced system exposure by over 70%.
- Collaborated with SOC teams and enhanced threat detection capabilities using tools such as ThreatLocker, improving response time by 30%.

Cyber Intelligence Intern, CogMac – New Delhi, India **May 2024 – Aug 2024**

- Leveraged OSINT tools to identify and document 25+ common adversary TTPs, informing updated incident response playbooks that improved threat mitigation strategies and were adopted by 7 teams.
- Investigated more than 50 cybersecurity risks in hardware and financial transaction systems, contributing to a 30% reduction in incident response time.
- Automated Python-based data pipelines, saving 40 hours per month and increasing efficiency by 25%.

Projects

Decoy & Honeypot Deployment Assistant github.com/Ashishdev13

- Built an automated honeypot deployment script that cut setup time by 70% and boosted simulation efficiency.
- Captured and logged over 500 unauthorized access attempts in controlled environments for detailed TTP analysis.

OSINT Reconnaissance Automation Tool github.com/Ashishdev13

- Built a modular Python reconnaissance framework supporting WHOIS, DNS analysis, subdomain discovery, email harvesting, tech fingerprinting, port scanning, and automated HTML report generation.
- Reduced manual OSINT collection time by automating multi-source intelligence gathering for threat actor profiling and digital forensics workflows.

Education

University of Arizona, BAS in Cyber Operations, Minor in Computer Science **Aug 2022 – May 2026**

- **GPA:** 3.5/4.0 (Dean's List, Highest Academic Distinction)
- **Coursework:** Active Cyber Defense, Cyber Threat Intelligence, Cyber Investigations and Forensics, Web Development, Operating Systems, Cyber Warfare, Violent Python.