CHIRAG DEWAN

chirag0728@gmail.com | (919) 771-7668| LinkedIn | GitHub | Portfolio

SUMMARY

Security engineer with 3+ years of experience in offensive security research, cloud security, and detection engineering. Background in zero-day vulnerability discovery across ICS environments, ML-powered fraud detection, and cloud-native security architecture. Specializing in AI/ML security with active research in behavioral threat detection for AI platforms and cloud workload anomaly detection.

PROFESSIONAL EXPERIENCE

Software Engineer II – Vulnerability & Detection Engineering, GM Financial |Dallas, *TX* **Mar '25 - Present**

- Engineered ML-powered fraud detection pipeline processing $10M+ in monthly transactions across AWS and Azure, correlating PyTorch behavioral scoring with custom Splunk detection rules to prevent $450K+ in losses
- Designed and enforced zero-trust cloud architecture across AWS and Azure, reducing security misconfigurations by 85% through automated policy enforcement and continuous posture monitoring
- Built Python CLI automation tool integrating ServiceNow and Active Directory via OAuth 2.0, automating four AD group operations and reducing manual provisioning workflows from hours to minutes
- Deployed and managed cloud infrastructure through Terraform across Azure environments as part of the CCOE, enforcing standardized security configurations and infrastructure-as-code best practices
- Mentored 4+ junior engineers on vulnerability assessment workflows, detection rule development, and security automation, accelerating team detection engineering maturity

Offensive Security Researcher, RTX/RTX BBN | *Aurora, CO & Boston, MA* **Jun '23 - Feb '25**

- Discovered 8 zero-day vulnerabilities in ICS protocols through fuzzing and differential packet reverse engineering, developing weaponized proof-of-concept exploits for coordinated disclosure
- Built AI-driven intrusion detection system analyzing firmware telemetry to identify anomalous behavior across embedded networks, expanding detection coverage for previously unmonitored attack surfaces
- Delivered offensive security briefings to DoD stakeholders, directly shaping zero-trust research strategy and funding priorities
- Conducted reverse engineering of embedded firmware and proprietary ICS protocol implementations using Ghidra and IDA Pro, identifying undocumented functionality exploitable for remote code execution
- Built custom detection signatures and network-level indicators of compromise from zero-day research, enabling defensive teams to identify exploitation attempts across monitored environments

Senior Cybersecurity Intern, RTX | *Aurora,CO* **May '22 - Dec '22**

- Built automated threat triage tools supporting ICS-focused detection operations and vulnerability assessment workflows

Information Security Intern, Reata Pharmaceuticals | *Dallas,TX* **May '21 - Aug '21**

- Led incident response during an active organizational breach, conducting investigation and introducing centralized logging capabilities to establish forensic visibility

PROJECTS

PARALLAX — Privacy-Preserving Threat Detection for AI Platforms |Github **Feb '26**

- Designed five-tier behavioral detection framework identifying model distillation attacks on AI platforms without inspecting user content, achieving 100% detection with 0% false positives across 1.5M simulated events
- Built weighted scoring engine analyzing 9 behavioral signals (request velocity, timing regularity, token ratios, session patterns) with tiered privacy escalation and human-in-the-loop authorization gate
- Developed real-time analyst dashboard with per-account compute cost estimation, behavioral fingerprint visualization, and automated case triage recommendations

KESTREL — Cloud-Native AI Workload Anomaly Detection | **Mar '26**

- Building multi-cloud detection engine targeting compromised AI workloads including GPU hijacking, unauthorized model training, and anomalous inference patterns across AWS and Azure
- Implementing MITRE ATLAS-tagged detection rules for AI infrastructure abuse in containerized environments with pluggable cloud provider adapters
- Designing modular detection architecture supporting cross-platform threat correlation and automated alert enrichment

TECHNICAL SKILLS

Security Tools: Splunk, ELK Stack, Ghidra, IDA Pro, Metasploit, Burp Suite, YARA, Sigma, Nessus, Wireshark, Nmap
AI/ML: PyTorch, TensorFlow, LangChain, Hugging Face, Scikit-learn, CrewAI, RAG, Pandas, NumPy
Cloud & Infrastructure: AWS, Azure, Kubernetes, Terraform, Docker, Redis, Kafka
Languages: Python, Rust, C/C++, Java, SQL, Bash, TypeScript, Golang
Certifications & Courses: SANS SEC504; SANS SEC560; AWS Security – Specialty; CRTO; CySA+; Security+; AWS Solutions Architect – Associate; Terraform Associate; Splunk Cybersecurity Defense Analyst; SecAI+; OSCP (In Progress)

EDUCATION

Bachelor of Science in Computer Science - Arizona State University | GPA: 3.74; Summa Cum Laude **Aug '19 - May '23**