ANCHAL RAHEJA
(CISSP | OSCP | GCFA | GCFR | GCIH)
anchalraheja3@gmail.com | (469) 970-8414 | Austin, TX
linkedin.com/in/anchalraheja github.com/anchalraheja credly.com/users/anchal-raheja

SUMMARY

Security Engineer with deep expertise in detection engineering, incident response automation, and AI-powered systems for security operations. Builds production LLM-driven platforms and Python-based automations for security workflows, operates global-scale SIEM and SOAR infrastructure, and leads large-scale, high-severity incidents in close partnership with legal and business stakeholders.

WORK EXPERIENCE

Senior Security Engineer, Amazon **Feb 2022 – Present**

- Led end-to-end incident response and security investigations across Amazon Stores, Prime Air, Whole Foods, and fulfillment centers, analyzing host and network telemetry for high-severity incidents.
- Led incident response efforts for third-party security breaches, partnering closely with Legal, Privacy, and Business stakeholders to assess impact, guide containment decisions, and support risk and disclosure workflows.
- Led the architecture and deployment of an AI-driven incident response system using Python and LangChain, reducing manual investigation time by ~4 hours per incident through multi-agent analysis of host, network, and historical incident data.
- Designed and implemented automated SOP and response documentation generation using an internal knowledge management framework, improving consistency and analyst effectiveness during incident response.
- Built and launched internal AI systems for security operations, enabling teams to leverage LLMs, custom security agents, and local RAG pipelines with federated authentication and access controls.
- Integrated AI agents with Splunk via Model Context Protocol (MCP) to provide contextual SPL query generation, detection analysis, and direct alert triage within existing SIEM workflows.
- Led an enterprise-wide Splunk consolidation initiative, migrating distributed Splunk environments into a centralized platform supporting 3,104 sites across 7 business units and 6 global regions with zero customer impact.
- Delivered $205,195 in annualized cost savings through SIEM infrastructure consolidation while maintaining enterprise-scale security monitoring and alerting.
- Designed, deployed, and maintained highly available SIEM and SOAR infrastructure as code, developing Python-based integrations and automation workflows that reduced incident response time by over 85%.
- Conducted continuous risk assessment and remediation for backend services operating across 70,000+ AWS accounts.
- Presented AI-driven security operations and incident response innovations at multiple internal Amazon forums, influencing adoption across security teams.

Security Engineer, Apple **Jun 2021 – Feb 2022**

- Threat modeling and performing architectural risk assessments of internally developed applications and systems.
- Perform technical reviews of Security Advisories and other communications related to vulnerability disclosure and remediation.
- Conduct network, cloud, infrastructure, and application penetration tests to identify and/or validate vulnerabilities and attack chains.
- Developed Python-based tools to enhance pentesting engagements.

Cloud Security Engineer, Amazon **Jan 2021 – Jun 2021**

- Triage/assess security issues and engage with internal service teams to ensure timely remediation of issues, escalating internally as necessary to ensure appropriate levels of urgency and engagement.
- Acts as a subject matter expert (SME) for AWS security services like IAM, SAML, KMS, CloudTrial, Config, CloudHSM, ACM, Inspector, GuardDuty,and Macie.
- Experienced with Lambda, creating Cloud Watch alarms, configuring ELB and WAF for various use cases.
- Providing Security best practices and architecture on AWS environment, assist with API/SDK related issues within customer architectures.
- Designing and delivering security solutions in Cloud infrastructure based on Cloud security standards, governance, and control practices.

Information Security Engineer II, Copart **Dec 2017 – Jan 2021**

- Trained team of 10 engineers to establish Threat Hunting program based on ATT&CK MITRE framework.
- Developed a Python-based threat intel-gathering software to enrich SEIM and correlation rules.
- Proven technical experience in windows forensics, memory forensics, and malware analysis.
- Developed Python-based SOAR tool to reduce incident response time from 2hrs to 10 mins.
- Developed security procedures, use cases, and enhanced security event logging process.
- Performed threat analysis of inbound network and host alerts, identified vulnerabilities, and recommended corrective measures.

- Developed a Python-based application that performs automated identification, assessment, and vulnerability research of external corporate facing assets.
- Architected solution to provide MFA, credential scanning, private repo enforcement for non- enterprise GitHub Account.
- Automated AppLocker verification and validation for over 15,000 assets in the US and EU reducing the time from 3mo. to 8hrs.
- Launched password cracking campaign and cracked 60% hashes over a period of 48hrs.
- Created and fine-tuned Cisco Umbrella policies for the US, UK, and EU complying with GDPR.
- Deployed and validated Umbrella and CrowdStrike for 10,000 assets.
- Performed both Dynamic Application Security Testing (DAST) and Static Application Security Testing (SAST), filtering out false positives.
- Assessing the risk for discovered vulnerabilities and prioritizing them for developers.
- Developed POC's for vulnerabilities, explaining the root causes to management.
- Reduced application deployment time from Dev to Production by 30% and remediated SQL Injection, Buffer Overflows, XSRF, and misconfigurations.

Graduate Research Assistant, UTA **Aug 2017 – Aug 2018**

- Developed machine learning based early-stage malware detection techniques using hardware performance counter with a 99.13% detection rate.
- Built Python tool to collect over 4,000 malware samples for building signatures based on hardware performance counters.

Full Stack Dev, Computer Sec Club, UTA **Aug 2016 – Jan 2017**

- Developed Flask based web app with member login, team events, and educational videos for the club.

Business Development Associate, BYJU's **Jan 2016 – Jul 2016**

- Architected an energy-efficient task offloading system with distributed computing power as well as privacy protection.
- Ported data onto the cloud to solve security and energy consumption problems.

Application Intern, Aricent **May 2014 – Jun 2014**

- Reviewed and Assisted with security policies, procedures, standards, and guidelines.
- Developed asset request management system.

TECHNICAL SKILLS

AI	: LangChain, LangSmith, Strands
Programming	: Python, PowerShell, C, C++, PHP
Web Technology	: HTML5, CSS, XML, JavaScript, Flask, Bootstrap, Django
Security Tools	: CrowdStrike, Cylance, Endgame, Mimecast, NMap, Wireshark, BurpSuite, Appspider, Checkmarx, Nessus Tenable, Metasploit, Umbrella, Sumologic, Volatility, Fortinet, Splunk, SOAR

OPEN-SOURCE PROJECTS

Nessus Report Generator **Python, Selenium**

- Created a custom application that reduced vulnerability technical and executive reporting by 95% for over 4000 systems through automation.

Recon-X **Python, AWS, REST API, NMap**

- Developed a Python tool that validates the organization's external-facing assets, which included domain names, IP addresses, open ports, and geo-locations by fetching and correlating results from Shodan, Google Dorks and performing NMap scans.

Bot Shield **Python, Sumologic, Incapsula**

- Developed custom application to query API for a malicious IP address and perform automated analysis and blocking via WAF.
- Analysis was done using SIEM data analyzed against public blacklist repo and feeding the results to WAF.

Ride Share **Python, MySQL, Bootstrap**

- Developed a web application during a 24-hour hackathon which connects people having the same destination
- Application was developed during the Houston Flood to assist those in need of transportation.

CERTIFICATIONS

- GCFR - GIAC Cloud Forensics Responder
- GCIH - GIAC Certified Incident Handler Certification
- CISSP - Certified Information Systems Security Professional
- OSCP - Offensive Security Certified Professional
- AWS Cloud Practitioner
- GCFA - GIAC Certified Forensics Analyst
- CEH - Certified Ethical Hacker

PUBLICATION AND PRESENTATIONS

- Manage Your Attack Surface on a Budget **BSides Las Vegas 2021**
  https://www.youtube.com/watch?v=PGrdEqU_V4c
- Malware Early-Stage Detection Using Machine Learning on Hardware Performance Counters
  https://rc.library.uta.edu/uta-ir/bitstream/handle/10106/27675/RAHEJA-THESIS-2018.pdf

EDUCATION

The University of Texas at Arlington **Aug 2018**
Master of Science in Computer Science **(GPA: 3.87)**
Thesis -Malware Early-Stage Detection Using Machine Learning on Hardware Performance Counters

Manipal University Jaipur **Jun 2016**
Bachelor of Technology in Computer Science (**GPA: 3.5**)