Avinash Nutalapati

Boston, MA • (617) 516-3444 • avinash.nutalapati@gmail.com
• linkedin.com/in/avinash-nutalapati/ • GitHub • Portfolio

Experience

Application Security Engineering Co-Op January 2023 – May 2023
RapidSOS, NewYork

- Led **vulnerability management** and application security assessments, achieving a 50% reduction in detection time of vulnerabilities in **SAST, DAST** - API Security in the **CI/CD** pipeline.
- Developed and executed security testing methodologies, including proof of concepts using **Python**, for over 20 vulnerabilities to communicate with **developers** enhancing the security posture.
- Utilized STRIDE for **threat modeling** to conduct Tabletop exercises identifying residual Risks.
- Resolved 30+ Log Parsing issues in **ELK** stack and **AWS** CloudTrail integrations streamlining **SOC** Operations. Created Multiple New Use Cases to identify Threats as required by Business.

Senior Security Analyst | Deputy Lead, Training Lead June 2021 - April 2022
Metmox Solutions, Hyderabad, India

- Managed vulnerability analysis & **remediation** across platforms, aligning with **OWASP Top-10** using Qualys. Spearheaded **EDR and Anti-Virus** integrations to create higher visibility into digital assets.
- Conducted executive-level reporting and documentation on security policies, SOC reports, and control gaps. Applied **cloud security** and **IAM** best practices in AWS reducing unauthorized access incidents.

Senior Application Development Analyst May 2018 - Mar 2021
Accenture Security, Bangalore, India

- Excelled in **Threat Intelligence** Analysis and **Incident Response**. Refined over 120 correlation and detection rules in **SIEM (Splunk)**, significantly enhancing alert responsiveness and accuracy.
- Monitored, Investigated and **Triaged Security events** and identified crucial, stealthy attacks of APT's and State Sponsored groups. Expertly integrated **Attack and MITRE TTP** frameworks for deep dives.
- Identified critical security vulnerabilities through proactive **Threat Hunting** activities using tools like Shodan and Google Dork, along with deep dives into the Dark Web.

Skills

Languages: Python, **Bash**, JavaScript, **PowerShell**, Groovy Script, SQL, HTML.
Security Tools: Splunk ES, QRadar, ELK Stack, **Semgrep**, Palo Alto, **Qualys**, Microsoft Defender.
Cloud Security: AWS Security Hub, **Azure** Security Center, **GCP** Security Command Center.
Certifications: CISSP (Expected Mar 2023), ISC2 Certified Security Professional.
Technology Audit: **JP Morgan Chase & Co. Internship**, SOC2 Readiness - Capstone Project.

Projects

Splunk Home Lab Setup Jan 2019 – Mar 2019

- Established a Splunk Home Lab environment using Docker to simulate real-world data analytics scenarios, enhancing skills in data ingestion, search processing, and visualization.

Security Risk Assessment (*Audit, Protocols, Compliance, SANS Policy*) Jan 2022 – Mar 2022

- Conducted risk assessments and proposed controls aligning with **NIST-800-53, ISO-27001** standards.

Achievements

- Captured the flag **winner** in Hack Harvard 2022. Demonstrated skillset in **Web Application security.**

Education

Master of Science in Cybersecurity | Northeastern University