Avinash Nutalapati

Dallas, Tx | 6175163444 | github.com/AvinashNutalapati
Portfolio: avinashnutalapati.github.io/AvinashCybersecPortfolio/
LinkedIn: linkedin.com/in/avinash-nutalapati/

Summary

A highly adept Senior Security Professional with a master’s degree in Cybersecurity from Northeastern University, I bring a powerhouse blend of experience and technical prowess across security domains. Proven at industry leaders like Accenture, JP Morgan Chase & Co, Discover and Cigna, I've led high-impact initiatives in Security Operations and real-time threat analysis. Most recently, I spearheaded a centralized vulnerability management process at Discover, streamlining incident response and boosting security posture. With a proactive mindset, investigative expertise, and a cloud-focused skillset, I'm eager to elevate Amazon’s security operations, driving robust defenses and futureproofing their expansive digital landscape.

Skills

Languages: Python, Bash, JavaScript, PowerShell, Groovy Script, SQL, HTML.
Security Tools: Splunk ES, QRadar, ELK Stack, Tanium, Palo Alto, Qualys, Symantec DCS, Carbon Black, Microsoft Defender for Endpoint, Identity, Office and Cloud, Active Directory, Okta, Semgrep and Proofpoint, Contrast, Nexus IQ, SonarQube, Nexus, ArmorCode.
Open-Source Tools: Kerberos, Wireshark, Nmap, BurpSuite, Metasploit, IDAPro, Curl, JTR, Hashcat, OpenSSL, Tcpdump, pfsense, Docker and Nikto.
Operating Systems: Linux, Kali Linux, Ubuntu, Unix, ios and Windows.
Cloud: VPC, EC2, S3, POD Security - Kubernetes, IAM, Vault, CloudTrail in Azure, AWS and GCP.
Technology IT Audit: JP Morgan Chase & Co. Internship, SOC2 Readiness - Capstone Project.
Frameworks: HIPAA, PCI-DSS, COSO, CIS 18, NIST-800-53, ISO-27001, GDPR.
Security Skillset: Firewall, IDS/IPS & DLP. TCP/IP, UDP, HTTP, HTTPS, TLS/SSL & DNS. OWASP Top10 (Web/API). VAPT.
Memberships: ISC2, ISACA – New England Chapter.
Soft skills: Analytical, Problem-Solving, Effective verbal communication skills, Stakeholder Management, Attention to Details, Time Management, Critical Thinking, Security Mindset, Team Collaboration, Adaptable, Focused, Accountable, and helpful.

Education

Master of Science in Cybersecurity, Khoury College of Computer Sciences
Northeastern University, Boston, 2023.

Bachelor of Technology in Electronics and Communications
Sreenidhi Institute of Science and Technology, Hyderabad, India, 2018.

Experience

Vulnerability Analyst – L8 Senior Mar 2024 – Present
Discover Financial Services – Riverwoods, IL

- **Monitored and triaged application security events**, enhancing organizational security by identifying and analyzing advanced attacks. Proficient in incident response and security engineering.
- **Proficient in coding** with Python, PowerShell and Bash, strengthening application security frameworks through effective code maintenance and review. Supported integration of advanced security tools for enhanced vulnerability management.

- **Led investigations into application security incidents** to strategically improve threat intelligence and response capabilities. Competent in remediating real-world security threats.
- **Established a centralized application vulnerability management process**, integrating over 5 security tools to streamline detection and management, complemented by automated Jira ticketing for rapid response.
- Created baselines for application security policies and streamlined Zero-day VM process with the infrastructure vulnerability management team.

Information Protection Senior Advisor Feb 2024 – Mar 2024

The Cigna Group | Technology Security Evaluations – App Sec – Bloomfield, CT

- Evaluated multiple App Sec TSEs as an advisor to provide approval for Code based New/Existing projects to make sure the project is secured and any Riks are Accepted/Mitigated.

Graduate Teaching Assistant | Khoury College September 2022 – December 2023

Northeastern University | Foundations of Cybersecurity | Security Risk Management and Assessment.

- Directed 6 TAs, oversaw 3 weekly lab sessions, and co-developed 7 cybersecurity projects, while actively contributing to the **Security Risk Management and Assessment** course in Grading and Student Mentoring.

Internal Audit Analyst June 2023 – August 2023

JP Morgan Chase & Co. | Chief Technology Office – Legacy West Plano, TX

- Collaborating with the CTO team to conduct 1 comprehensive Audit on the **45+ SDLC Controls**, CI/CD Pipeline Technologies and Tools. Found **few gaps** in the newly suggested controls and recommended changes.
- Created 45 **short training videos** for SDLC Controls testing to reduce 30+ research work hours of each Tech Auditor with the goal of more accurate and less-time consuming auditing.

Security Engineering | Detection and Response January 2023 – May 2023

RapidSOS | New York | Location Services for 911 – Police, EMS, IAR

- Identified and resolved over 20 distinct parsing errors in log data, enhancing the accuracy.
- Developed Use-Cases to generate real-time alerts in slack from ELK.
- Integrated **AWS S3 CloudTrail** logging into the **ELK Stack (Kibana)** AWS daily to monitor and identify potential security threats in cloud infrastructure. Performed Error Check of **JSON** documents in ELK.
- Developed 10+ scripts using **Python, PowerShell, and Bash** to automate routine cybersecurity tasks, increasing efficiency.
- Monitored CI/CD Pipeline security issues & **Jenkins deployment** to increase resilience, BCP and Disaster Recovery of SaaS applications.
- Performed vulnerability scans using **OWASP ZAP** – Jenkins and updated results on 3 internal URLs to detect vulnerabilities as part of **SAST, DAST - API Security** in CI/CD pipeline.
- Threat Modelling using **STRIDE** within **SDLC**. Participated and lead contributor in tabletop exercises.

Senior Security Analyst L3 (Specialist) | Deputy Lead, Training Lead June 2021 - April 2022

Metmox Solutions (Now Ultraviolet Cybersecurity), Hyderabad India

- Secured 2000+ Servers & 800+ Desktops by installing, maintaining **EDR** and **Anti-Virus** solutions while investigating alerts along with SOC team in our **Global Fusion Center**.
- Established **Vulnerability Management** (100,000+ assets) with Vulnerability Assessment and Penetration Testing. Coordinated non-production environment simulations with Red Team.
- Investigated reported critical vulnerabilities, provided information of Version/Patches, Exploitation Likelihood, Impact and Risk to FastTrack **remediation and mitigation** strategies.

- Tested installation, performance and effectiveness **3+ PoC of Security Tools** for organizational needs.
- Communicated effectively with multiple security vendors including **Microsoft** to resolve issues related to security tools on a high priority and provide required exclusive awareness **trainings to New Hires**.
- Coordinated with **Third Party Security Risk Assessments** and **New Project Risk Assessments**.
- Troubleshooted **server stabilization** and infrastructure performance using Procmon like tools to make sure of security issues. Performed Threat Hunting activities in Shodan, Google Dork and Dark web.
- Developed 20+ **Dashboards in Splunk** to automatically track VP level **weekly metrics** reports.

Senior Security Delivery Associate L1-L2 | Shift Lead May 2018 - Mar 2021
Accenture | MSSP – Security Operations Center | Multiple Fortune 500 Clients.
Bengaluru/Hyderabad India

- Keen eye for **Network Log analysis** and pattern/trend identification. Developed Dashboards to identify anomalies to enhance Network Security and block potential IOC's.
- Expertise in **log correlation** and windows event id analysis to identify bad vector behaviors.
- Developed and **fine-tuned** correlation and detection **rules** (250+ Use Cases) to improve alerting in SIEM.
- Finetuned integration of threat intelligence effectively for reducing false positives by 20%.
- Performed **Email Phishing Analysis**. Excelled in detailed PDF malware analysis.
- Drafted weekly technically detailed reports on status of the SIEM to include metrics on number of logging sources (7500 GB/Day), collection rate**, False positives and Log Thresholds**.
- Curated 30+ **SOPs** for **Incident Response and Threat Analysis**.
- Spearheaded the integration of **Microsoft Sentinel** for real-time security analytics, advanced AD Security strategy for 150+ groups with **SOAR** process to enhance cloud security.
- Identified critical security vulnerabilities through proactive **Threat Hunting** activities using tools like Shodan and Google Dork, along with deep dives into the Dark Web.

Projects

Cryptography (*Python, C, Sodium Library)* July 2022 - July 2022

- Implemented 2-Way Encryption, SHA 256/512, MD5, Hashing, MAC, Digital Sign and PKI.

SQL-Injection, XSS, CSRF Buffer-Overflow, HTTP Smuggling (*HTML, Bash)* June 2022 - June 2022

- Scripted 15+ web attacks including Web Cache Deception and 2+ Buffer-Overflow.

Time Complexity attacks Side Channel (Python, Burp Suite) May 2022 - May 2022

- Replicated Time Complexity attacks by calculating server response time to guess user's passwords.

Security Risk Assessment (*Audit, Protocols, Standards, Compliance, SANS Policy)* Jan2022 - Mar2022

- Evaluated Risk to propose controls on HIPAA, PCI-DSS, COSO, CIS, NIST 800-53, ISO-27001, GDPR.

Splunk Home Lab Setup

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

SOC2 Audit – Capstone Project

- Successfully executed a comprehensive SOC2 Readiness assessment as a Capstone Project with Mobile Heartbeat, a subsidiary of HCA demonstrating in-depth understanding of Audit process.