Avinash Nutalapati

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

Education

Master of Science in Cybersecurity
Northeastern University, **Khoury College of Computer Sciences,** Boston, MA. Jan 2022 - Dec 2023

Technical Skills

Languages: Python, Bash, JavaScript, PowerShell, Groovy Script, 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 and Proofpoint.
Open-Source Tools: Kerberos, Wireshark, Nmap, BurpSuite, Metasploit, IDAPro, Curl, JTR, Hashcat, OpenSSL, Tcpdump,pfsense and Nikto. **Operating Systems**: Linux, Kali Linux, Ubuntu, Unix, Windows.
Cloud: VPC, Docker, Cluster Engine, EC2, S3, POD Security - Kubernetes, IAM, Docker, Vault, CloudTrail in Azure, AWS and GCP. **Certifications**: CC – ISC2, CISSP – Expected by Dec 2023.
Technology Audit: JP Morgan Chase & Co. Internship, SOC2 Readiness - Capstone Project (Sponsored).

Experience

Graduate Teaching Assistant | Khoury College September 2022 – December 2023
Northeastern University | Foundations of Cybersecurity | Security Risk Management and Assessment, Boston, MA

- Directed 6 TAs, oversaw 3 weekly lab sessions, and co-developed 7 cybersecurity projects.
- Contributed to Security Risk Management and Assessment course in Grading and Student Mentoring on evaluating Risk to propose controls on HIPAA, PCI-DSS, COSO, CIS 18, NIST-800-53, ISO-27001, GDPR.

Application Security Engineering Co-Op January 2023 – May 2023
RapidSOS | Location Services for 911 – Police, EMS, IAR

- Performed vulnerability scans using ZAP – Jenkins and updated results on 3 internal URLs, resulting in a 50% reduction in the average time to detect vulnerabilities as part of SAST/DAST - API Security in CI/CD pipeline.
- Developed proof of concepts (POCs) using Python for over 30 discovered vulnerabilities in CISA reports, enabling the development team to efficiently address potential security concerns and reduce the overall risk.
- Utilized industry-standard threat modeling methodologies like STRIDE to assess risks within different systems.

Senior Security Analyst L3 (Specialist) | Deputy Lead, Training Lead June 2021 - April 2022
Metmox Solutions (Now Achieve Cybersecurity) Hyderabad, India | Client: Stryker Orthopedics – Michigan

- Led 1/3rd of cross-functional projects and teams in establishing DevSecOps practices within SDLC. Revamped Playbook, Documented Security Policies/Processes/Procedures, and analyzed 100's SOC Reports.
- Tested 3 PoC and Managed 10+ Third Party Security Technologies across 10+ platforms and products. Supervised Vulnerability Management (100,000 assets). Expert knowledge of OWASP Top10 (Web/API).
- Accomplished Security of 2000+ Legacy Servers and 800+ Desktops. Troubleshooted for server stabilization and infrastructure performance 90%+ (Procmon) related issues with Windows Legacy Operating Systems.
- Investigated 10+ reported critical vulnerabilities, provided information of Version/Patches, Exploitation Likelihood, Impact and Risk. Strong understanding of TCP/IP, UDP, HTTP, HTTPS.

Senior Security Delivery Associate L1-L2 May 2018 - May 2021
Accenture | Managed Security Services | Multiple Clients - USA

- Monitored, Investigated and Triaged Security events. Developed correlation and detection rules (80 Use Cases) to improve alerting in Threat Landscape as part of L2 Incident Response. Performed Phishing Analysis.
- Drafted weekly technically detailed reports on status of the SIEM to include metrics on number of logging sources (750 GB/Day), log collection rate, True positive and server performance. Presented to clients in brief.
- Established and Curated 30+ standard operating procedures for the administration, content management, change management, patch management, and Life-Cycle management of the SIEM/Log Management in CSIRT Team.
- Analyzed potential Cyber Kill Chain threats, leveraging Attack & MITRE TTPs in 40+ incident responses.

Achievements

Hack Harvard 2022 (Assembly AI, Python)

- Won capture the flag (CTF) event at Hack Harvard 2022 conducted by Snyk.