Avinash Nutalapati

github.com/AvinashNutalapati • Portfolio: avinashnutalapati.github.io/AvinashCybersecPortfolio/

Summary:

- **Automated Security Testing Integration**: Led the integration of automated application security testing tools and technologies, significantly boosting efficiency and security posture.
- **Strategic Security Solutions**: Partnered with enterprise teams to devise and implement security solutions in line with Security Architecture, business objectives, technological requirements, and evolving threat landscapes.
- **Risk Assessment and Management**: Conducted comprehensive risk assessments for current and new services and technologies, identifying and addressing design gaps and risks, and proposing robust security enhancements.
- **Effective Risk Communication**: Specialized in conveying risk assessment results to information security stakeholders and business partners, establishing a reputation as a trusted advisor for informed risk management decisions.
- **Innovative Risk Posture Improvement**: Initiated and developed solutions for risk remediation or mitigation, markedly improving the organization's risk posture.
- **Strong Interpersonal Relations**: Fostered and maintained robust working relationships across the organization, crucial in the effective management of information risks.
- **Security Threat Intelligence**: Kept up-to-date with emerging security threats, constantly refining security architectures to counter potential risks.
- **Communication Skills**: Demonstrated exceptional communication abilities, adept at simplifying complex risks, solutions, and security concepts, and effectively facilitating group meetings and discussions.
- **Professional Experience**: Offers 5+ years of experience in information security management frameworks (IS027000, COBIT, NIST 800, etc.), augmented by a solid background in regulatory compliance.
- **Extensive Cybersecurity Experience**: Served as a Graduate Teaching Assistant at Northeastern University, focusing on Cybersecurity Foundations and Security Risk Management and Assessment. Managed a team of 6 TAs and co-created 7 cybersecurity projects.
- **Internship at JP Morgan Chase & Co.**: Functioned as an Internal Audit Analyst, executing a thorough Audit on SDLC, CI/CD Pipeline Technologies, and Tools. Produced 45 training videos for SDLC Controls testing, significantly reducing research hours for Tech Auditors.
- **Security Engineering Expertise**: Played a pivotal role at RapidSOS in Detection and Response, addressing parsing errors, developing real-time alert systems, and integrating cloud-based logging systems for enhanced security monitoring.
- **Advanced Scripting Proficiency**: Authored over 10 scripts using Python, PowerShell, and Bash to automate routine cybersecurity tasks, thereby boosting efficiency.
- **Leadership at Metmox Solutions**: As a Senior Security Analyst L3 and Training Lead, secured 2800+ devices, led CIRT investigations, and oversaw Vulnerability Management for over 100,000 assets.
- **Experience with Accenture**: Monitored and triaged security events for various Fortune 500 clients, developing advanced detection rules and integrating threat intelligence.
- **Project Expertise**: Showcased skills in Cryptography, SQL Injection, XSS, CSRF, and Buffer-Overflow attacks. Conducted a comprehensive SOC2 Readiness assessment as a Capstone Project.
- **Multilingual and Tool Proficiency**: Skilled in Python, Bash, JavaScript, PowerShell, among others. Experienced with various security tools like Splunk ES, QRadar, ELK Stack, and more.
- **Cloud and IT Audit Experience**: Familiar with cloud technologies (AWS, Azure, GCP) and proficient in conducting IT audits, including a Technology IT Audit during an internship at JP Morgan Chase & Co.

- **Certifications and Memberships**: Pursuing or holding certifications such as CISSP, CEH, CCNA, and active membership in ISC2 and ISACA.
- **Soft Skills**: Renowned for analytical thinking, exceptional communication, problem-solving capabilities, and meticulous attention to detail.

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.
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.
Certifications: CC – ISC2, CompTIA Sec +, CEH, CCNA, CISSP – Expected in 2024.
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
Northeastern University, **Khoury College of Computer Sciences 2023.**

Experience

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

- Undertaking Application Security Vulnerability Management process and enhancing it.

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 – Summer Intern 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 15+ SDLC, CI/CD Pipeline Technologies and Tools. Found a 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 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 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) –Unpaid Volunteer work, Hyderabad India

- Secured 2000+ Legacy Servers & 800+ Desktops by installing, maintaining EDR and Anti-Virus solutions while investigating alerts along with SOC team in our Global Fusion Center.
- Led investigations into CIRT calls finding patient zero's, root cause, containment, and forensics.
- Supervised 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 effectiveness3+ 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.

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

- Monitored, Investigated and Triaged Security events. Identified crucial, stealthy attacks with accuracy and precision.
- 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 (120+ 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 (750 GB/Day), collection rate, True positive and Log Thresholds.
- Curated 30+ SOPs for Incident Response and Threat Analysis. Leveraged Attack & MITRE TTPs.
- 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.

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.