Durga Janardhana Anudeep Betha

Cyberseurity Engineer | (240) 630-1574 | betha.anudeep@gmail.com | linkedin.com/in/anudeep-betha/ | Marylan

EDUCATION

University of Maryland College Park CGPA: 3.97
Master of Engineering, Cybersecurity Aug 2022 - May 2024 (Expected)
Relevant Coursework: Network Security, Secure Coding for Software Engineering, Secure Software Testing and Construction, Digital Forensics and Incident Response, Penetration Testing, Cloud Security, Information Assurance, Secure Tools for Information Security, Hacking of C Programs & UNIX Binaries, Networks and Protocols.

WORK EXPERIENCE

International Business Machines(IBM) Remote
Security Engineer Nov 2020 – Aug 2022

- Remediated critical security vulnerabilities including Tenable Nessus and OpenText FOD vulnerabilities, which prevented attacks like SQL Injection, Cross-Site Scripting, and Cross-Site Request Forgery with a 100% success rate.
- Actively engaged in the security incident response process, employing CVE for vulnerability identification and CVSS evaluations to determine the impact of vulnerabilities and guide their remediation within web applications.
- Implemented automated security CI/CD pipelines using tools like Jenkins and seamlessly integrated them with Sonatype Nexus which ensured that each code commit triggered automated scans, effectively reducing the time to detect and remediate potential vulnerabilities in the SDLC of the business-critical applications.
- Conducted manual security code reviews and penetration testing on critical web applications, restful APIs to identify vulnerabilities, which aided in the discovery of previously undetected security gaps in authorization mechanism.

International Business Machines (IBM) Bangalore, India
Security Intern Jan 2020 – Jun 2020

- Executed comprehensive vulnerability assessments on critical web applications using industry-leading tools, like Burpsuite, and Metasploit, contributing to the identification and mitigation of security risks.
- Applied application security testing (SAST and DAST) methodologies, utilizing tools such as OWASP ZAP, Snyk, and Nikto to scrutinize web applications for potential vulnerabilities to prevent known cyber-attacks.
- Contributed to incident handling procedures for security breaches by actively participating in response activities such as triaging alerts, gathering evidence, and documenting findings, which provided valuable hands-on experience in real-world security incident management.

PROJECT EXPERIENCE

SIEM Enhancement Project(Splunk) using MITRE ATT&CK Framework:

- Conducted a comprehensive analysis of existing security controls and historical attacks within the organization, categorizing them based on the MITRE ATT&CK Framework to identify potential blind spots.
- Implemented targeted improvements to the SIEM system by designing and deploying new correlation rules aligned with MITRE ATT&CK techniques, enhancing the detection and response capabilities against advanced threats.

Secure Financial Management System and Web Application Security Automation:

- Developed a secure financial management web application, emphasizing secure code development practices to protect Personally Identifiable Information (PII) and Payment Card Industry (PCI) data.
- Programmed DetectX, a Python-based command line tool, to automate the identification of SQL Injection and Cross Site Scripting Vulnerabilities in web applications, using Regular Expression pattern matching in server responses.

TECHNICAL SKILLS

Security: Secure Code Analysis(SAST, DAST, SCA), Incident Response, Web Application Security, Penetration Testing, DevSecOps, Threat Modeling, Email Security, Network Protocols (HTTP, DNS, TCP/IP), Vulnerability Management, Malware Analysis, API Security, Risk Assessment, EDR, MDR, DLP, XDR, IDS/IPS, OWASP Top 10, Bug Bounty.
SIEM Tools & Operating Systems: Splunk, QRadar, Linux, Windows, MacOS.
Languages: Python, PHP, Java, C++, C#, .NET Core, SQL, HTML, CSS, JavaScript, Bash Scripting, PowerShell.
Security Tools: Burpsuite, Metasploit, Nmap, SonarQube, Fortify On Demand, Nessus, ZAP, Qualys, Nikto, Snort, Wireshark, NetCat, Ghidra, Snort, Microsoft Defender(EDR), Snyk, Veracode, Microsoft TMT.
Digital Forensics: Volatility, Autopsy.
Cloud Technologies & Frameworks: Amazon Web Services, Azure, MITRE ATT&CK & D3FEND, Cyber Kill Chain.
Web Development: Git, HashiCorp Consul and Vault, Angular, MongoDB, JSON, Restful API, SpringBoot, ELK Stack.
Certifications: Azure Fundamentals (AZ-900), In pursuit of OSCP and AZ-500.