Piyush Pote

8144098786 | piyush.pote@outlook.com | Linkedin

Cyber Security Analyst| Vulnerability Management| Penetration Tester| SOC Analyst

SUMMARY

Cybersecurity Analyst with 2+ years of experience in various cyber security domains such as penetration testing, SOC operations, and threat intelligence, with a proven track record of reducing vulnerabilities by 30% and streamlining incident response times. Skilled in leveraging security tools like Qualys, Microsoft Defender, and Splunk for proactive threat detection and endpoint protection.

WORK EXPERIENCE

Merck Sharp and Dohme LLC — Rahway, New Jersey

Cybersecurity Analyst, ITRMS(Associate) — June 2023 – August 2023

- Automated CVE asset retrieval and vulnerability scan results via API integration using python scripts for EDR tools Qualys, Wiz, and Microsoft Defender, cutting mitigation time by 30% and enhancing asset visibility by 10%.
- Developed a Python-based Linux Vulnerability Management System with MongoDB integration, automating CVE triage and reducing critical vulnerability response time by 20%.
- Designed interactive dashboards for periodic review ensuring real-time vulnerability tracking and remediation, increasing cross-team engagement and accelerating potential vulnerability identification by 20%.
- Monitored and enforced security policies using Active Directory, ensuring adherence to best practices for access control and data protection, leading to a 15% improvement in security compliance across critical systems.
- Conducted daily CVE research and prioritization using Splunk, ensuring proactive threat mitigation aligned with zero trust principles for enhanced risk management.
- Assisted in real-time incident response by identifying Indicators of Compromise (IOCs) and generating detailed threat intelligence reports, reducing incident resolution time by 25%.
- Collaborated with Incident Response teams to perform security log analysis and threat hunting, leveraging SIEM tools like Microsoft Sentinel and Splunk.

ERSEGMENT — Mumbai, India

Penetration Tester, Red Team(Full-time) — April 2021 – June 2022

- Executed penetration tests and security assessments for 20+ clients, creating test cases and documentation to bolster security postures and ensure regulatory compliance.
- Led Vulnerability Assessment and Penetration Testing on government websites, identifying OWASP Top 10 vulnerabilities, mitigating critical issues improving system security by 20%.
- Executed security assessments using Nessus scans and tailored penetration strategies, identifying and exploiting system weaknesses, resulting in a 30% increase in security and improving clients' threat detection capabilities.
- Developed a Capture The Flag (CTF) challenge for interns, incorporating OWASP Top 10 vulnerabilities and tools like Burp Suite and OWASP ZAP, to enhance company's penetration testing training program.
- Demonstrated advanced penetration testing skills using techniques like privilege escalation, network pivoting, and exploit development, earning a global ranking of #532 on Hack The Box and improving threat detection capabilities.
- Specialized in Linux system security and web application vulnerability assessment, ranking in the top 5% on TryHackMe, gaining proficiency with Metasploit, Wireshark, and SQLmap.
- Aligned security practices with NIST, GDPR and ISO 27001 standards, conducting regular audits and policy updates, enhancing compliance and audit-readiness across multiple client environments.

SDG-RAIT — Mumbai, India

Security Engineer, Backend Team(Intern) — April 2020 – November 2020

- Implemented OWASP Top 10 controls for web application security and conducted threat modeling for the client's company website, enhancing overall system security by 25%.
- Integrated automated security scanning tools (OWASP ZAP, SonarQube) into the CI/CD pipeline, resulting in a 30% reduction in security vulnerabilities and improved development workflows.
- Led security testing procedures using Burp Suite and Nessus, identifying and mitigating critical flaws across key systems.
- Developed and enforced API security policies, implementing robust authentication and authorization mechanisms with OAuth 2.0 and JSON Web Tokens (JWT), strengthening data protection and access control.

CERTIFICATIONS & SKILLS

Certifications: CompTIA Security+ Certification (SY0-701), EC-Council Certified Ethical Hacker (CEH V11), ISC2 Certified in Cybersecurity (CC)

Security Tools: Qualys, Wiz, Microsoft Defender, Entra ID, Intune, Sentinel, Splunk, Crowdstrike Falcon, Wireshark, Nessus, Burp Suite

Programming Languages: Python, C++, Java**,** Javascript

Skills: PowerBI, MongoDB, Docker**,** Azure, Cloud Security Controls, Active Directory, IAM, Firewall Management, Incident Response, Data Loss Prevention, Metasploit, **Currently pursuing OSCP+.**

EDUCATION

Pennsylvania State University — **University Park, Pennsylvania**

Master of Science in Cybersecurity Operations and Analytics (3.8 GPA) — May 2024

Research Work: Securing the Smart: Exploring Optimal Defense Strategies Against Man-in-the-middle Attacks in IoT Networks.