Neeraj V

Senior Application Security Engineer / Senior Product Security Engineer

Currently working as Application Security Engineer with 4 **+ years of experience** in Cyber security domain with a domain knowledge in **Security Operations Center, Cyber threat Intelligence and Application Security** . Skillful in conducting penetration testing & technical reviews. In depth knowledge in Vulnerability management and assessment, Threat hunting and Red team areas.

mailtoneerajv@gmail.com | 9496831569 | Kerala, India | linkedin.com/in/n33rajv

SKILLS

Web Application VAPT | Network VAPT | API VAPT | SAST | DAST | SCA | SDLC | Thick Client VAPT

Active Directory Pentesting | Windows Privilege Escalation | Mobile Application VAPT | Linux Privilege Escalation

Threat Hunting | Threat Modelling | Incident Response | Secure Coding | DevSecOps | Azure | Cloud Security

WORK EXPERIENCE

Senior Application Security Engineer
Happiest Minds Technologies

10/2023 - Present *Bangalore*

Working in Client Side

Achievements/Tasks

- Implementing DevSecOps & Building a High-Impact AppSec Team for a Fortune 500 Company.
- Developed and implemented a comprehensive framework for the AppSec team, establishing processes and procedures for effective security integration throughout the development lifecycle.
- Championed a shift-left approach to security, integrating threat modeling (IriusRisk) early in the development process and throughout the CI/CD pipeline for proactive vulnerability identification and mitigation.
- Authored comprehensive Standard Operating Procedures (SOPs), Statements of Work (SOWs), and standards to ensure consistent and efficient security practices across the organization.
- Leading the selection and deployment of SAST (Coverity) and DAST (Whitehat) tools for automated application security testing, ensuring scalability and efficiency within the environment.
- Implementing IAST (Seeker) for real-time security monitoring and vulnerability detection, focusing on continuous improvement and proactive risk mitigation.
- Deploying SCA (Black Duck) solutions for effective open source software dependency management and risk mitigation, ensuring compliance with industry standards within the client organization.
- **TOOLS: IriusRisk, BlackDuck, Seeker, Coverity, SRM (CodeDx), WhiteHat**

WORK EXPERIENCE

Application Security Engineer
H&R Block

07/2020 - 09/2023 *Trivandrum, India*

Achievements/Tasks

- Perform Web, Mobile, Thick client and API Vulnerability Assessment and Penetration Testing (VAPT) based on OWASP standards and testing guides and provided comprehensive reports.
- Successfully integrated the SAST, DAST and SCA approach into the organization's DevSecOps framework.
- Expert in delivering the vulnerability readout calls to provide walkthroughs over the identified security issues and help development team with necessary fixes based on the technology stack.
- Collaborated with cross-functional teams including developers, architects,and project managers to ensure that security requirements were integrated throughout the software development lifecycle.
- Manage security risk software vendor relationship to improve use of automated security risk assessment tools.
- Develop SOP documents, prepare technical checklists for various penetration testing requirements.
- Support the bug bounty program.
- Established the Security Developer Champions program within the organization.
- Developed and maintained security dashboards and metrics to track security performance and identify areas for improvement.
- **TOOLS: Burp Suite Pro, Kali Linux, Burp Suite Enterprise, SonarQube, Sonatype, Invicti Netsparker, Metasploit, Nmap Wireshark, Nikto, SQLmap, Postman, Dirbuster, Hashcat, John the ripper.**

Cyber Threat Intelligence Analyst
H&R Block

04/2020 - 06/2020 *Trivandrum, India*

Achievements/Tasks

- Identify cyber threats, trends and new developments in cyber threat landscape by analyzing raw intelligence and data.
- Understand the lifecycle of cyber threats, attacks, attack vectors, and methods of exploitation; conduct trending and correlation of cyber intelligence for the purposes of attribution, threat modeling and establishing strategic countermeasures.
- Experience with a wide variety of open-source and/or vendor-supported intelligence and cybersecurity tools and technologies to detect and act upon external cyber threats to the organization.
- Synthesize large quantities of complex threat information, distilling it to the most critical issues and draws accurate conclusions, before relaying the threat intelligence to appropriate stakeholders.
- Actively monitoring Dark web sites for organization related sensitive data.
- **TOOLS: MISP, FlashPoint, Maltego, Avalon, FSISAC, Spiderfoot, Shodan, TorBot**

Security Operations Center Analyst
H&R Block

01/2020 - 03/2020 *Trivandrum, India*

Achievements/Tasks

- Monitor real-time security events on SIEM (LogRhythm) console and Event Analysis, Investigating and mitigation.
- Perform threat hunts across the network by relying on in-depth knowledge of SOC tools and techniques, leveraging indicators of compromises from incidents and security events to determine scope of breaches and potential impact.
- Working on assign ticket queue and Understanding and exceeding expectations on all tasked SLA commitments.
- Create and maintain weekly and monthly operational reports.
- **TOOLS: LogRhythm, Crowdstrike falcon, The Hive, Microsoft ATP, Paloalto, Qualys Scanner, Rapid7 InsightVM**

EDUCATION

MSc in Computer Science with specialization in Cyber Security
Indian Institute of Information Technology and Management Kerala (IIITMK)

07/2018 - 08/2020 *Trivandrum, Kerala*

Details

- CGPA : 8.63

EDUCATION

Bachelor Of Technology in Civil Engineering
TKM COLLEGE OF ENGINEERING

07/2013 - 08/2017 *Kollam. Kerala*

Details

- CGPA: 7.68

CERTIFICATES

Practical Ethical Hacking - The Complete Course (03/2021)
TCM Security

Microsoft Certified Azure Security Engineer (AZ-500) (In Progress)
Microsoft

Introduction to FIN6 Emulation Plans (02/2021)
AttackIQ

National Eligibility Test (NET) (12/2019)
UGC

Offensive Security Certified Professional (OSCP) (In Progress)
Offensive Security

Foundations of Purple Teaming (02/2021)
AttackIQ

Certified Network Security Specialist (CNSS) (07/2020)
ICSI (UK)

PROJECTS

Integrating Bro with SIEM for Security Operations Center (01/2020 - 05/2020)

Detection and analysis of Wormhole attack in IoT Network using Cooja and Foren6 (06/2019 - 11/2019)

Network Intrusion Detection using Machine Learning (01/2019 - 04/2019)

TOOLS

Operating System Kali linux, Parrot OS, Windows, Whonix, Tails, Tracelabs VM

LANGUAGES

English
Full Professional Proficiency

Hindi
Full Professional Proficiency

Malayalam
Full Professional Proficiency

Tamil
Full Professional Proficiency