MOHAMMED ZAHEER

CONTACT

Address : Vellore, TN 632001

Phone : +91-7418704202

Email : zaheermohammed410@gmail.com

SKILLS

- Risk Management
- Vulnerability Assessment
- Compliance
- Threat Hunting
- Email Security
- Penetration Testing
- Report Writing
- Embedded Linux Security
- ARM exploitation and security
- Docker container security
- ISO 21434
- SAEJ3061
- API security
- Mobile Security
- Python
- Bash Scripting

EDUCATION

Bachelor of Engineering : Electrical, Electronics Engineering Technologies, 06/2016
Anna University - Vellore
Percentage - 76%

High School Diploma : 05/2012
Voorhees Higher Seconday School - Vellore
Percentage - 71%

SSLC, 05/2010
Voorhees Higher Secondary School - Vellore
Percentage - 82%

CERTIFICATIONS

- EC Council - Certified Ethical Hacker

PROFESSIONAL SUMMARY

Passionate cyber security professional with more than 5 years of experience in Automobile Cyber Security (**Threat Analysis and Risk Assessment, Threat Modeling, Security Concept Development, Implementation of Security Concepts**) and IT Cyber Security (**Security Monitoring, Threat Hunting, Vulnerability Management, VAPT**).

Never give up person with **positive frame of mind**. Eager to work as a team and contribute to team success through hard work, attention to detail and excellent organizational skills. Self-Motivated to learn, grow and excel in Automotive Cyber Security.

WORK HISTORY

Cybersecurity Engineer, 05/2022 to Current
Magna Electronics - Pune, India
Project - Fisker and Stellantis ADAS

- Working in ADAS projects
- Covering entire cybersecurity lifecycle of the project following ISO21434
- Eastablishing the automated process vulnerability management in compliance with the ISO21434: Clause 8 - Continual Cyber Security Activities
- Written Incident response management process and implemented the process
- Working with software & systems teams to implement functionalities incorporating cybersecurity concepts
- Working along with manufacturing team to assist them on production security, key management
- Working in blackduck software composition analysis tool to scan the software binaries post build

Senior Software Engineer - CyberSecurity, 03/2021 to 05/2022
Valeo India Private Limited - Chennai, India
Project - Daimler Telematics Control Unit

- Lead the project in collaboration with customer and adhere to their timelines, following agile methodologies
- Performed preliminary risk analysis based on the RFQ documents provided by the customer
- Have done the Threat analysis and Risk assessment using stride model.
- Wrote the Damage scenarios with respect to the road user perspective leveraging the key aspects such as financial, operational, safety, privacy
- Accommodating the UNECE threat references in the risk assessment and in lining with UNECE WP29, UN R155(CSMS) cyber security
- Written the security concepts or security fixes for the identified threats
- Delivered the required security concepts to the customer at mentioned timeline

- Advanced Android Application Exploitation- TheHacktivists

COURSES

- Cisco Certified Network Administrator
- Practical Ethical Hacking - Pursuing

- Managing and writing complex security requirements on IBM DOORS utilizing DOORS attributes
- Writing V2X related security requirements
- In lining with software teams throughout the Project Lifecycle
- Involved in key aspects during the implementation of software
- Working knowledge on ISO 21434 and SAE J3061
- Assisting team on error corrections and on streamlining the risk assessment process

IT-Analyst -SOC- Vulnerability Management, 01/2019 to 03/2021
Lennox India Technology Center - Chennai, Tamilnadu

- Performed Manual and Automated Security Testing for Web Application & Web Services
- Planning, Conducting and reporting Vulnerability and risk assessment of applications
- Ensuring the security coverage for all the applications of organization
- Identification of Injection, Business logic, Authentication, Session Management, etc.
- Related flaws in applications and encasing attack scenarios and associated risk to business
- Risk associated with vulnerability explained to the project team for better.
- Provided mitigation for the identified application vulnerabilities and worked with the project team for the remediation.
- Understanding in data privacy and data security regulatory requirements or framework such as HIPAA, GDPR, NIST, HITRUST, SOC II, etc.)
- Working knowledge and exposure of IT Governance, Risk Management, and Compliance practices
- Communicate any potential risks or guidance, to the Division, with regards to GDPR (from Article 29 Working Party, or Capita Group Data Protection Officer)
- Provide recommendations to the Division, on Data Protection related initiatives or awareness campaigns
- Have streamlined the infrastructure vulnerability assessment process and designed the architecture
- Performing vulnerability scans on the servers and other network devices via Nexpose from Rapid 7 & Nessus from Tenable
- Prioritizing the vulnerabilities identified, Create Remediation Projects with Incident Ticket and assign it to Stake Holders for Remediation.
- Evaluate Risk to Perform Upgrade, Apply Patch & to Remediate Configuration Vulnerabilities.
- Performing PCI scans every quarter and submitting the report to external auditor for compliance
- Validate the Closure with the Scheduled Scan.
- Involved in ensuring the disaster recovery and business continuity plans are up-to-date and exercised periodically. Produce all documentations related to conducted DRPs.
- Having a knowledge in performing internal active directory pentesting
- Hands on experience in webapplication testing tools like burpsuite, sqlmap, Netsparker and webinspect

IT Analyst - SOC, 04/2018 to 01/2019
Lennox India Technology Center - Chennai, Tamilnadu

- Monitor the organization's network for security threats & investigate security violations
- Performing Attack-Based threat hunting and Data based threat hunting in SIEM

- Sound Knowledge in social engineering attacks
- Analyzing email related threats such as Phishing, Social engineering & Scam's
- Conducting phishing and scam simulations with self defined tools to spread awareness among users
- Creating quarterly trend report on phishing and scam
- Organizing and Implementing the information security awareness program's
- Having knowledge in windows active directory attacks
- Linux suspicious events monitoring and root cause analysis
- Azure security center, Active directory monitoring & root cause analysis
- O365 email security monitoring
- Creating use cases on various platforms such as Linux, Windows, DLP, Firewall in SIEM
- Expertise in various security tools like Palo Alto UTM, Varonis - Endpoint Threat Detection, McAfee ePO, Cimtrak FIM, Barracuda SPAM Filtering FW and SkyHigh CASB

Process Executive, 12/2016 to 03/2018
Infosys - Chennai, Tamilnadu

- Working in Security Incident and Event Monitoring SIEM platform – Security Analytics
- Working in FireEye and GRA Tool
- Monitoring various event sources for possible intrusion and determine the severity of threat
- Hauling Ad hoc report for various event sources and, customized reports and scheduled reports as per requirements
- Monitoring security incidents from multiple devices such as Symantec Antivirus, Check Point Firewall, NIPS, AD, Bluecoat, Cisco switch and Cisco ACS
- Monitor RSA SA dashboards to keep track of real time security events, health of end point devices
- Collecting the logs of all network devices and analyze the logs to investigate the suspicious activities
- Investigate the security logs, mitigation strategies and Responsible for preparing Generic Security incident report
- Analyze the Malware with tools like sysinternals
- Creating daily/weekly/monthly reports for baselines on critical incidents