S. MARIMUTHU
Email-ID: msmuthu001@gmail.com
Contact No: +91 7418626948

Career Objective:

To succeed in an environment of growth and excellence. Earn a job, which provides me job satisfaction and help me achieve personal as well as the organization goals.

Certifications/Trainings

- ISO 27001:2013 Lead Auditor in Chennai
- CCNA Training Completed in Chennai
- DCM in Diploma Computer Management Course completed in Thiruvannamalai.

Summary

Having experience in Information Security domain for over 8 years. Understanding in Information Security Tools & operations, experience in IS-SIEM, VAPT and Malware Analysis.

- Hands on experience in IBM Qradar Tool for L2 Security Operation Center Analyst in 5 years.
- Hands on experience in Nessus, Burp suite and NMAP Tools for Vulnerability Assessment and Penetration Testing – VAPT in 1 year.
- Hands on experience in Malware analysis in 1 year.
- Hands on Experience in Identity Access Management Operations in 3 years.

Work Experience and Responsibilities:

The details of the various responsibilities that I have handled are listed below, in chronological order.

Company	Equitas Small Finance Bank – Head Office in Chennai.
Role	Assistant Manager Information Technology.
Period	October 2016 to Present – 5 Years.
Description	SIEM – L2 Security Operation Center Analyst / Vulnerability Assessment and Penetration Testing – VAPT /Malware Analysis.

Roles and Responsibilities.	**1. Handling L2 Security Operation Center Analyst.** • Support the day to day operations of the security operation center. • Utilize security operations standards to analyze and escalate security events. • Monitor and enforce security policy. • Develop solution for process automation wherever possible.

- Develop and maintain incident response management policies and procedures.
- Monitor public security advisories and alerts for information related to
  Threats and Vulnerabilities.
- Monitor/Tune/Support several security monitoring platforms (e.g. IPS/IDS, Next-gen Firewall, Anti-Virus/EDR, WAF, DDOS, Vulnerability scanners, Windows, Non-Windows and Network devices).
- Provide support for incident response and vulnerability management efforts.
- Drive efforts to improve and further built out the security monitoring tools.
- Create SOPs, Run books and Reports.
- Take part in root cause analysis and other fine tuning works.
- Escalate to L3 team wherever necessary.
- Fair knowledge of cyber security technologies such as SIEM, Firewall/NGFW, AV/EDR, WAF, Proxy, DLP and Active Directive.
- Performing both Internal and External security audit closure.
- Validate contributing and non-contributing log sources in SIEM.
- Fine tuning SIEM rule against threat.
- Knowledge on TCP/IP network traffic and event log analysis.
- Participate in SIEM-Qradar and Wincollect agent upgrade activity.
- Participate in SIEM-Qradar Architecture change.
- Day by day validate in Qradar health check such as EPS, CPU, Memory, Primary and Secondary Qradar console/event Collect, contributing/Non-contributing log sources and backup activities for service/system optimize.
- In-depth knowledge of phishing mail.
- Willing to work any shift (Day/Night/Weekend).
- Maintain knowledge of current security trends and be able to clearly communicate to the team.

2. VAPT(Vulnerability Assessment and Penetration Testing)
Period: September 2020 to Present – 1 Year.

- Performing L1 level support to Nessus, Burp suite and NMAP vulnerability scans for scanning activities.
- Nessus used for Infrastructure scanning.
- Burp suite used for Web applications scanning.
- NMAP used for Ports scanning.

Roles and Responsibilities:

- Proactively research and monitor security related information sources to aid in vulnerability discovery.
- Contact scans or pen tests to identify vulnerabilities or confirm compliance to security standards.
- Perform in-depth analysis of Vulnerabilities by correlating data from varies sources.
- Facilitate proactive remediation or mitigation of new vulnerabilities by collecting information from threat and vulnerability feeds, analyzing the impact /applicability to environment and communicating applicable vulnerabilities and recommended remediation actions to be impacted team.

	• Assist with routine compliance and audit functions to ensure regulatory scanning requirements are satisfied. • Provide input to leadership for enhancing the vulnerability management strategy. • Ability to develop and maintain metrics and reports on vulnerability findings and remediation compliance. • Manage and run vulnerability remediation campaigns. • Document remediation tasks to application and system owners. • Report finding to stakeholders as well as recommendation for remediation. • Track vulnerability from identification through to remediation using ticketing system. • Create standard and procedures for vulnerability management process. • Coordinate with different teams to perform regular patching and scanning.
	3. Malware Analysis. **Period: September 2020 to Present – 1 Year.** • Performing L1 level support to Malware analysis. **Roles and Responsibilities:** • Perform malware analysis for PE and Non-PE files. • Experience in knowledge of Security/Threat landscape for window/Linux and iOS platform • Strong knowledge of modern security problems. • Experience in analyzing large amount of data. • Strong capabilities in Microsoft products like offices Excel, Word, and PowerPoint.
Company	**Equitas Small Finance Bank – Head office in Chennai**
Role	**Senior Identity & Access Management Operations**
Period	September 2013 to October 2016 – 3 years
Description	Providing IT infrastructure support and Application Access provisioning and De-provisioning for an employees through Incident and Service Request tickets based on Industrial standard and agreed SLA.

Roles and Responsibilities	**Identity & Access Management Tasks**: • Work on User profiles, User groups, Security roles, Security Classes, Authorization Lists, Security Objects, Payment Authorization Groups, SharePoint Sites/License Management, Web UI Monitoring and Websitesunder various types of BAU, New Joiner, Mover & Resignation tickets. • Maintain critical application access and service accounts. • Creation/ Modification / Deletion of Users in more than 100 applications. • Investigate and Diagnose Issues. • Processing new hires/terminations based on the pre-requisites. • Maintain MIS for the IAM Team to submit daily/weekly/monthly reports. • Driving IAM Service Improvements • Reconciliation and Remediation Activities • Handling Bulk Requirements. • Create application Process Documents (SOPs). • Handling Internal and External audits. • Handling RPA project to single sign on.
	Area of Interest & Special Skills
	Area of Interest. • SEIM-Qradar • Nessus, Burp suite and NMAP • Anti-Virus- AV/EDR • Firewall, WAF, Proxy and DLP **Special Skills.** • Quick Learner and Self Motivated • Adoptable to work as a Team • Leadership Quality & Confident • Good MS office work skill.

Educational Qualification:

- Completed SSLC (State Board) in Government Hr. Sec. School in the year 2006
- Completed HSC (State Board) in Government Hr. Sec. School in the year 2008
- Completed BE – ECE in Sri Aravindar Engineering College in the year 2012

Personal Profile:

Name	:	S. Marimuthu.
Name of Father	:	K. Selvam.
Date of Birth	:	10.05.1991.
Gender	:	Male.
Nationality	:	Indian.
Languages Known	:	English & Tamil (Speak and Write).
Address	:	15/1, Aranganathan subway, Kaverinagar, Saidapet-15

Declaration:

I hereby declare that all the above statements are true and correct to the best of my knowledge.

Place :

Yours Truly,

Date :

(S.MARIMUTHU)