CURRICULAM VITAE

Jagathish S Micheal
+971547431001/+971562938829
jegathish88@gmail.com

Objective

Motivated and enthusiastic System & Network security Analyst professional with 12+ years of experience. My areas of expertise include System, Network Security & SOC Lead and on-site technical support involving Security tools. I would like to pursue a challenging career and strive for more challenging role to acquire knowledge and achieve higher grounds in the ever growing and innovative field of Security.

Core Competencies

- Security Monitoring & Thread Detection
- Incident Response & management
- Forensic Evidence Analysis
- Qualys Vulnerability Scan tool
- Forcepoint Email Security
- Forti Sandbox
- Sentinel one (EDR)
- Symantec Endpoint Security
- TrendMicro Deep Security
- Splunk Enterprise security
- Mime cast Email Security
- Knowbe4 Training Tool
- Cyber Insurance
- Reblaze Web security
- IBM QRadar
- Azure Sentinel

Educational Qualification

- **B. Tech (I.T.)-Anna University-India**
- **CCNA (R & S) Certified**
- **MCSE Certified**
- **Fortinet NSE (Level 2)**
- **Cyber Security Professional (U.S Council) Certified**
- **Splunk Master Architect (Training).**
- **CyberArk Certified Trustee.**
- **SOC Analyst (Training)**
- **CISSP(Training)-Infosec**

Professional Experience

Role: **Snr SOC Analyst**
Organization: **Smart Dubai Pulse (DU), Dubai**
Duration: **Feb-2023 to till Date**

This role involves leading a team of cybersecurity professionals, coordinating incident response activities, and ensuring the effectiveness of security monitoring and threat detection measures. Maintaining the organization's security posture and mitigating potential risks.

Responsibilities:

- Proactively monitor and analyze security alerts generated by Azure Sentinel to identify potential threats and security incidents.
- Investigate security incidents, perform root cause analysis, and recommend remediation actions to mitigate risks.
- Develop and fine-tune Azure Sentinel playbooks, queries, and detection rules to enhance detection capabilities.
- Collaborate with cross-functional teams to ensure timely incident response and resolution.
- Conduct regular reviews of Azure Sentinel configurations and policies to maintain optimal performance and compliance with security standards.
- Developed and maintained custom dashboards, workbooks, and reports in Azure Sentinel to provide stakeholders with actionable insights into security posture and threat landscape.
- Utilize security tools and technologies to detect and investigate potential security incidents.
- Participate in tabletop exercises and incident response drills to test and improve incident response procedures
- Identify opportunities for automation and optimization to improve efficiency.
- Ensure compliance with industry regulations, standards, and internal security policy
- Contribute to security governance initiatives, risk assessments, and audits.
- Assist in the development and implementation of security policies, procedures, and controls.
- Prepare and present reports on SOC performance, incident metrics, and trends.
- Maintain accurate documentation of security incidents, investigations, and actions taken.
- Provide clear and concise communication regarding incident findings and recommendations.
- Conduct regular assessments and audits of security controls and systems.
- Coordinate and oversee the organization's response to major security incidents or breaches.
- Communicate effectively with senior leadership and provide regular status updates on SOC operations.

Role: **Snr SOC Analyst**
Organization: **Eros Group, Dubai**
Duration: **Oct-2012 to Feb-2023 (10 +years)**

Responsible for installation, maintenance of network Security systems and various SIEM tools. To design, analyze and provide technical support with a Security limit. Incident response, forensic investigation. Monitoring security alert from varies security systems**.** Vulnerability analysis and desktop central patch management system handling.

Responsibilities:

- Keep up to date with the latest security and technology developments.
- Research/evaluate emerging cyber security threats and ways to manage them.
- Plan for disaster recovery and create contingency plans in the event of any security breaches.
- Monitor for attacks, intrusions and unusual, unauthorized, or illegal activity.
- Test and evaluate security products.
- Design new security systems or upgrade existing ones.
- Use advanced analytic tools to determine emerging threat patterns and vulnerabilities.
- Identify potential weaknesses and implement measures, such as firewalls and encryption.
- Investigate security alerts and provide incident response.
- Monitor identity and access management, including monitoring for abuse of permissions by authorized system users.

- Link with stakeholders in relation to cyber security issues and provide future recommendations.
- Generate reports for both technical and non-technical staff.
- Maintain an information security risk register and assist with internal and external audits relating to information security.
- Monitor and respond to 'phishing' emails and 'pharming' activity.
- Assist with the creation, maintenance, and delivery of cyber security awareness training for colleagues.
- Give advice and guidance to staff on issues such as spam and unwanted or malicious emails.
- Alien Vault USM alarm monitoring, incident response, incident investigation.
- Splunk installation and dashboard creation, Enterprise security.
- Organization cyber insurance.

Role: Engineer-IT System and Network
Organization: Vasanth TV Pvt Limited, India
Duration: Sep 2010 to 3rd Oct 2012 (2 years)

As a network Engineer being an In charge taking responsibility for overall activities in a project having expertise into Execution, Maintenance, Management from the worker and meeting to the Customer Requirements as a Consultant.

Responsibilities:

- Manage Domain environment for two sites through remote support. (Team Viewer, VNC).
- Manage shared folder and devices through permission.
- Mail Clients configuration backup &Troubleshooting. (MS Outlook).
- Local and Network Printer configuration, troubleshooting.
- Internet & LAN configuration, troubleshooting.
- Software troubleshooting update and patch installation.
- Manage Antivirus (Symantec).

References upon Request