AMALA XAVIER T

8129687929| amalaxavier97@gmail.com |www.linkedin.com/in/amala-xavier-t-1aa528154

Cyber Security Analyst with Proven ability to understand and follow incident response procedures in fast-paced environments. Proficient at training resources on alerting customers to possible malicious activity, resolving priority cases and creating reports that enable experts to modify security policies.

PROFESSIONAL EXPERIENCE

SOC Analyst – UST, Trivandrum 02/2022 – 10/2024

- To analyze, escalate, and aid in the remediation of critical security incidents, adhere to detailed processes and procedures.
- Monitoring security incidents in real time via the SIEM console, investigating the events, doing in-depth analysis, and mitigation.
- Create, update, and manage incident tickets with the help of ITSM tools like Jira & Service Now.
- Provides Threat Advisory Reports to all Stakeholders about new Vulnerabilities that are discovered globally which includes details on Vulnerability, Affected products, Workarounds , Solution and Steps to apply mitigation.
- Provide clear and accurate information to the next shift or team member to ensure a smooth transition of responsibilities.
- Document incidents, actions taken, and the outcomes for future reference. Prepare regular reports on security incidents, trends, and recommendations for improvement.
- Responsible for creating the weekly and monthly reports for governance meetings, and was a part of all governance meetings with stakeholders.

SOC Analyst Trainee - Cyberfort DigiSec Solutions Pvt Ltd, Chennai 08/2021 – 02/2022

- Monitoring and analysis of security events with the use of ELK, Wazuh and Rapid7 (SIEM Tools). Execution of SOC procedures Triage security events and incidents, detect anomalies, and report remediation actions and custom parse. Rules, Reports and Dashboards.
- To escalate the incident whenever the SLA's are not met and to monitor the health of the SIEM tool and assist SOC Analyst in incident workflow. To assist SOC team in incident detection and resolving and communicate with external teams in proper incident resolution.
- Worked on ISO 27001 Standards and Mapping ISO vs NIST and BCP vs DRP (UAE Client).

Analyst Security Operation Trainee – Skill Cube Pvt Ltd, Trivandrum 04/2018 – 10/2018

- Overview of Security Operations Center
- Introduction to SIEM Architecture and design of SIEM
- Deployment and configuration of SIEM
- Writing event correlation rules - Use cases

- Proactive vulnerability assessment
- Incident handling - detection and response & 3R Compliance - Retention, Rules & Reporting

EDUCATION

- **M.Sc. Cyber Forensics**
  Mahatma Gandhi University 2019 – 2021
- **B.Sc. Cyber Forensic**
  Mahatma Gandhi University 2015 – 2018

TECHNICAL SKILLS

- **SIEM Tools:**
  Azure Sentinel, Sumo logic, Splunk, Wazuh
- **EDR Solution:**
  Crowd Strike
- **Packet Analysis:**
  Wireshark, TCP Dump, N-map
- **Framework:**
  MITRE ATT&CK
- **E-mail Security**:
  E-mail Analysis, E-mail Authentication Protocol.
- **Data Recovery & Backup Tool:**
  Cyber Check
- **Steganography Tool:**
  Open-Stego

CERTIFICATIONS

- Sector Skill Council: NASSCOM Analyst Security Operation Centre.
- Microsoft - Security Operation Analyst Associate.
- Mile2 - Certified Security Principles.
- Oracle - OCI Certified Foundations Associate.
- arcX - Cyber Threat Intelligence 101.
- Sumo Logic Certified - Fundamentals.
- Sumo Logic Certified - Cloud SIEM Fundamentals.
- Google Chronicle Security - SIEM Fundamentals.

LANGUAGES

- English
- Malayalam
- Tamil
- Hindi