BABITHA BANAGANI

CYBER SECURITY ANALYST

DETAILS

Address – Amaravathi Nagar, Near M.R.Palli Circle, Tirupati, Chittoor, India, 517501

Date of Birth - 12th August 1997, Tirupati

Email ID – babithabanagani@gmail.com

Phone No - +91 8297465536

LinkedIn - https://www.linkedin.com/in/babitha-banagani-247b82245

Professional Summary

Cybersecurity Analyst with good exposure on multiple security technologies, worked different security platforms in SOC Operations with an experience in Event Monitoring, Vulnerability Management, Threat Intelligence, Analyzing Alerts, Malware analysis etc. A proven ability to assist with the day to day running activity of Cyber Security Operations having 2 years and 1 month of experience.

Employment History

HCL Technologies, Chennai – Cybersecurity Analyst (SOC Operations)

2020 — PRESENT

- Monitoring malicious activity by analyzing all priority alerts, investigating indicators of compromise of bad reputation (IOCs like Source IP, Destination IP, File Name, File Hashes, Domains etc.) and performing triage on alerts based on criticality and scope of threats from any abnormal behaviors, suspicious activities, traffic anomalies, unauthorized scanning etc.
- Performing endpoint analysis and preventing all malicious files, software by blocking/auditing/unblocking on **Endpoint Security** tools like Sophos,Trend Micro,Crowdstrike to reduce false positive alerts.
- Identifying, evaluating, prioritizing, and reporting on security vulnerabilities in systems by mitigating the vulnerabilities by making changes to the infrastructure or to the impacted system, upgrading and patching the operating system of a server, software to latest version on **Vulnerability Management** tools like Qualys.
- Analyzing data which catch abnormal behavior or potential cyberattacks on logs event on **SIEM** tools like IBM Qradar, Splunk etc., development of use cases based on client requirements, customized rules to capture and alert critical incidents, event validation & analysis and experience in log monitoring, filtering, report generation. Analyzing and reporting detailed information related on the Data loss prevention alerts, Detecting and preventing Intrusion attempts.
- Having Knowledge on Tcp/ip,WAN and LAN Concepts,Protocols,Firewalls.
- Responsible for creating daily/weekly/monthly security incidents report with standard procedures and managing customer SLAs for real time alerting, response and reporting.
- Responsible for creating incidents for different severity alerts and following up until the case is close with proper resolution by identifying rule modification to ignore the legitimate traffic.

TOOLS

- Vulnerability Management - Qualys Guard
- Endpoint Security – Sophos,TrendMicro, Crowdstrike Falcon
- SIEM – IBM Qradar
- Ticketing – ServiceNow,Demisto

CERTIFICATIONS

- Qualys Certified Specialist - Vulnerability Management

SKILLS

- Vulnerability Management
- Endpoint Security (EDR)
- Security Operations (SOC)
- SIEM
- Malware Analysis
- Risk Analysis
- Incident Response
- Threat Intelligence
- Team Communication

EDUCATION

Bachelor Of Technology (B.Tech), SVEW,JNTUA University, Tirupati – 72%

JULY 2014 — JUNE 2018

Electronics And Communication Engineering (ECE)

Intermmediate – Sri Chaitanya Junior College, Tirupati – 85.9%

June 2012 — APRIL 2014

MPC

School, Sri Adbhutha Vidyanikethan, Tirupati – 9.5 CGPA

MARCH 2011 — March 2012

SSC

DECLARATION

I hereby declare that the above written particulars are true to the best of my knowledge and belief. If provided an opportunity, I will utilize it with all my determination to be a committed professional dedicated to the cause of the organization.

Place: Tirupati BABITHA BANAGANI