Abhishek Mishra

S/O BK Mishra (HM), Kendriya Vidyalaya Ramgarh cantt.
Jharkhand
India

E-mail: abhi.cybersec2812@gmail.com
Phone: 08980565844

OBJECTIVE

"To work in a firm with a professional work driven environment where I can utilize and apply my knowledge, skills of Cyber Security by which i can provide security to the Organization's infrastructure (Data/information) and make Company Proud and achieving organizational goals."

WORK EXPERIENCE

Gateway Technolabs Pvt Ltd — Jan 2018 — Jan 2019

SOC Analyst

- Hands-on Practice on Splunk,Secdo, Cylance, Crowd strike (EDR), SIEM, CEHv9, CHFIv9, Wireshark, Nmap, Vulnerability management.
- Skilled in creating & executing security policies, plans, & procedures for the network .
- Knowledge of developing and implementing risk response strategies with senior business and technology risk managers for the coordination and execution of fraud prevention & cyber security initiatives.
- Gained exposure in various aspects of cyber security including computer network attack, computer network defense, computer network reconnaissance, cyber forensics, and cyber intelligence collection and analysis.
- Incident Handling.
- Having knowledge of many other Security Tools. Performed risk analyses to identify appropriate security countermeasures.
- Monitored computer virus reports to determine when to update virus protection systems.
- Monitored social media and online sources for industry trends.
- Devoted special emphasis to punctuality and worked to maintain outstanding attendance record, consistently arriving to work ready to start immediately.

eCLINICALWORKS India Pvt Ltd — Feb 2019 — present

SOC Analyst

An EC Council - **Certified Ethical Hacker(CEHv9)** & **Computer Hacking and Forensic Investigator(CHFIv9)** with 4+years of experience in Cybersecurity as SOC Analyst.

I am currently working in eCW (eClinicalWorks) & responsible for :-

- Monitoring Alerts and Events.
- Handling Incidents.
- Monitoring Splunk Enterprise Alerts and Events.
- Monitoring Sophos EDR and helping L1 analyst to triage the alert accordingly.
- Performing Investigations with help of MS Sysinternals Tools and others.
- Performing risk analysis to identify appropriate security countermeasures.
- Monitored computer virus reports to determine when to update virus protection systems..
- Performing Malware analysis when required.
- Monitoring social media and online sources for security trends.
- Monitoring and performing scan for Vulnerabilities with Nexpose.

- Checking CISCO Firepower IDS/IPS logs.
- Knowledge of TCP/IP
- Performing QA on incidents.
- Software Approval process.
- O365 security alerts.
- Analyzing Microsoft defender for Cloud (Azure Portal) alerts.

QUALIFICATIONS

- CEHv9 (EC Council)
- CHFIv9 (EC Council)
- Incident Response & Advavanced Forensics (Cybrary.it)
- Crowdstrike tech.partner (Crowdstrike University)

EDUCATION

BE (ECE) Sept 2010 — Jan 2015

Vidya Vikas Institute Of Engineering & Technology (VVIET),Mysore

INTERESTS

- Threat Detection & Incident Response Activities
- Malware Analysis
- Exploring new Tools
- Singing

REFERENCES

https://www.linkedin.com/in/abhishek-mishra-42894015a/