

PRANAY PRABHAT

SOC Analyst-Fraud Prevention/Information Security

CONTACT:



+91 9896546063



pran4y@gmail.com



www.linkedin.com/in/pran4y/



https://pran4y.github.io

ADDRESS:



Sector 21

Gurgaon

Delhi NCR, Haryana - 122016

CERTIFICATION:



Security Information & Event Management

Sai Acuity Institute of Learning Pvt Ltd, **Udemy**

TOOLS:



SIEM

Splunk



Ticketing

JIRA



EDR

CrowdStrike Falcon

EDUCATION:



B.Tech. (2017)

Electronics & Communication Engineering
Delhi Institute of Technology & Management
DCRUST, Murthal, Sonapat



12th (2013)

S.R.C. Inter College, BSEB
Katihar, Bihar



10th (2011)

H.S.N. High School, BSEB
Katihar, Bihar

OBJECTIVE:

Looking for an active role of SOC Engineer/SOC Analyst in an organization, where I can use my knowledge and skills to detect and defend against attacks and threats that help drive company growth with improved security.

EXPERIENCE:

❖ SOC Analyst-Fraud Prevention/Information Security

Teleperformance Global Service Private Limited (Jan'20, Jun'21 – **Currently Working...**)

Here, I'm working with events and incidents as they come in. I'm responsible for:

- >Constantly monitor and assess incoming events and incidents to promptly identify potential infiltration attempts within organization system.
- >Analyze system logs, identifying patterns that could indicate security threats.
- >Collaborating with another team (IT, Network, server) to resolve security incidents & improve overall security, escalate validated and confirmed incidents to SOC Lead, actively participate in compliance Meeting/Audits.

❖ Associate

IGT Solutions Pvt. Ltd. (Mar 2019 - Oct 2019)

I supported daily operations and collaborated with team members to achieve goals, ensuring efficient workflow and contributing to overall project success.

❖ Fraud Analyst

Quattrro Processing Services (Nov'17 – Nov'18)

I was responsible for the whole process of Data extraction and Deployment. Investigation on issues which was occurring while processing those data.

SKILL:

- » Good understanding on network concept including OSI Model IP Classes, IP Addresses, Ports and protocols, & Malware
- » Solid Knowledge on Security Concept and Servers like AAA, CIA, Encryption, DNS, Hashing, DHCP
- » Familiar with Cyber Kill Chain Framework & Good Knowledge of Cyber Attack (Zero Day, Syn Flood, DOS & DDOS, Brute Force, Spoofing etc.)
- » Understanding on Security solution like Firewall, IPS/IDS, and Endpoint Security Solutions like AV/DLP
- » Knowledge of SIEM (**>Splunk**), writing on Queries, Creating Report, Dashboard. Analyzing of Phishing Email reported by the Internal End User.
- » Knowledge of Incident Response Life Cycle.
- » Acknowledging and rising tickets on validated incidents.
- » Monitoring and analyzing the logs which are triggered 24*7 and conduct investigation on them.