**Company Name:** Panacea InfoSec Pvt. Ltd.

**Job Location:** Delhi

**Profile- SOC Analyst**

The Security Operation Centre (SOC) Information Security Analyst is the first level of monitoring in the SOC. The position monitors and responds to security events from managed customer security systems as part of a team on a rotating 24 x 7 x 365 basis.

**Core Responsibilities**

* The security analyst monitors security events from the SOC entry channels (SIEM Console), based on the security event severity, escalate to customer as appropriate to perform further investigation and resolution.
* Recommend enhancements to SOC security process, procedures and policies.
* Participate in security incident management processes.
* Works as part of a team to ensure that corporate data and technology platform components are safeguarded from known threats.
* Communicate effectively with customers, teammates, and management.
* Provide input on tuning and optimization of security systems.
* Follow ITIL practices regarding incident, problem and change management.
* Document and maintain customer build documents, security procedures and processes.
* Staying up to date with emerging security threats including applicable regulatory security requirements.

**Qualifications**

Ideal candidates will have as much of the following,

* A Bachelor's Degree / Diploma in a relevant area of study with a preference for Information Security, Computer Science or Computer Engineering.
* 1-2 years previous Security Operations Centre Experience in conducting security investigations.
* Detail oriented with strong organizational and analytical skill.
* Strong written communication skills and presentation skills
* Good knowledge of IT including multiple operating systems and system administration skills (Windows, Unix).
* Basic understanding of security incident management, malware management and vulnerability management processes.
* Strong understanding of networking principles including TCP/IP, WAN’s, LAN’s and commonly used Internet protocols such as SMTP, HTTP, FTP, POP, LDAP.