| | | | |
|---|---|---|---|
| **Job Title:** | SOC Expert - OpenText SIEM & SOAR | **Years of Experience:** | 5-8 Years |
| **Department** | Technical | **Position Type:** | Full Time |
| **Location:** | Noida | **Date posted:** | |
| **Package:** | 10-12 Lacs | | |

**Job Description**

**Position Overview:**

The SOC Expert with expertise in OpenText SIEM and SOAR is responsible for monitoring, analyzing, and responding to security incidents within the organization. This role involves leveraging OpenText's Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solutions to ensure the security and integrity of the organization's information systems.

**Key Responsibilities:**

- **Security Monitoring and Incident Response:**
  - Monitor security alerts and events using OpenText SIEM.
  - Investigate and respond to security incidents promptly.
  - Perform in-depth analysis of security incidents and develop response strategies.
- **SIEM & SOAR Management:**
  - Configure and maintain OpenText SIEM and SOAR platforms.
  - Develop and implement use cases, correlation rules, and automated workflows.
  - Ensure the SIEM and SOAR systems are updated with the latest threat intelligence feeds.
- **Threat Hunting and Analysis:**
  - Conduct proactive threat hunting activities to identify potential security threats.
  - Analyze network traffic, logs, and other data sources to detect and mitigate threats.
  - Collaborate with the threat intelligence team to enhance detection capabilities.
- **Incident Documentation and Reporting:**
  - Document all security incidents and actions taken in detail.
  - Prepare and present incident reports to management.
  - Provide recommendations for improving the organization's security posture.
- **Collaboration and Communication:**
  - Work closely with other SOC team members and departments to coordinate responses to security incidents.
  - Provide guidance and training to junior SOC analysts.
  - Communicate effectively with stakeholders regarding security incidents and responses.

**Qualifications:**

- **Experience:**
  - Minimum of 5 years of experience in a SOC environment or a related cybersecurity role.
  - Extensive hands-on experience with OpenText SIEM and SOAR platforms.
- **Technical Skills:**
  - Proficiency in configuring and managing SIEM and SOAR solutions.
  - Strong knowledge of cybersecurity principles, threat vectors, and attack methodologies.
  - Experience with log analysis, network traffic analysis, and endpoint security.
  - Familiarity with scripting languages (e.g., Python, PowerShell) for automation purposes.
- **Soft Skills:**

- Excellent analytical and problem-solving skills.
- Strong communication and interpersonal abilities.
- Ability to work effectively under pressure and in a fast-paced environment.
- Detail-oriented with a high degree of accuracy.

**Desired Attributes:**

- Proactive and self-motivated.
- Ability to adapt to evolving threats and security landscapes.
- Strong organizational skills and the ability to manage multiple tasks simultaneously.
- Commitment to continuous learning and professional development.

**How to apply-**

Interested candidates are invited to submit their resume along with a cover letter detailing their relevant experience and motivation to **contact@pmspl.net.**