L1 SOC ANALYST

Requirement: SOC SIEM Analyst
Job Location : Mumbai / Pune
Experience Range: 1 to 2 Years

Job Description**:**

The security analyst, Level 1, works within the SOC (Security Operations Centre) and is responsible for the monitoring of systems, investigating root causes, and coordinating with Level 2 and 3 engineers for analysis and response.

The security analyst works using log data as well as many security tools, and ticketing systems.

Primary Roles and Responsibilities:

Roles :

- Monitor alerts automatically generated by security systems
- Monitor threats and new attack techniques being disclosed in the wild
- Investigate events to determine if they are true events or false positives
- Create new ways to search for potentially suspicious events on systems
- Participate in projects to improve security monitoring toolkits as well as to improve defensive controls
- Provide different types of data to measure security and compliance

Required Skills:

1. Basic understanding of security concepts on networks, Window, Linux, web applications.
2. Basic understanding of networking concepts
3. Ability to multi-task under strict deadlines.
4. Professional and interpersonal skills.
5. Ability to work effectively and contribute within a team environment.
6. Experience with some security tools.
7.Experience in understanding and analysing various log formats from various sources.
8. Experience in analysing reports generated by SIEM tools.

Candidate profile

Experience/ Qualifications:

- 1 to 2 years of relevant experience.
- Bachelor's degree in Computer Science, Information Technology, Systems Engineering, or a related field.
- Relevant Security Certifications preferred (Security+, CEH etc.).
- Good oral and written communication skills to collaborate with the team.
- Should be willing to work in rotational 24/7 shifts -

Employment Type:Full Time, Permanent

Salary: As per Industry Standards

Role:System Security

Industry:IT-Software / Software Services

Functional Area:IT Software - Network Administration, Security