

Pradeep Kumar
Security Analyst in Infosys - Career Contour

Hyderabad, Telangana, Telangana - Email me on Indeed: [indeed.com/r/Pradeep-Kumar/96485546eadd9488](https://www.indeed.com/r/Pradeep-Kumar/96485546eadd9488)

WORK EXPERIENCE

Security Analyst in Infosys

Career Contour -

March 2015 to Present

Security incident and event management (SIEM) is the process of identifying, monitoring and analysing security events or incidents within a real-time IT environment. It provides centralized view of the security scenario of an IT infrastructure

EDUCATION

B- Tech

Jawaharlal Nehru Technological University - Hyderabad, Telangana

SKILLS

Splunk, Network Security, Arc sight (2 years), SIEM (2 years), McAfee ESM (1 year)

ADDITIONAL INFORMATION

Technologies: McAfee SIEM, Arc sight, HP Service manager.

Description:

Security incident and event management (SIEM) is the process of identifying, monitoring and analysing security events or incidents within a real-time IT environment. It provides centralized view of the security scenario of an IT infrastructure.

Roles and Responsibilities:

- Have Experience in device integration, alarm creation in ESM.
- Having Experience on analysing FIREWALL events.
- Checking health status for all devices in ESM.
- Working in Offshore SOC team, Monitoring of SOC events, detecting and preventing the Intrusion attempts.
- Hands-on experience monitoring the SIEM tool.
- Provide level 2 supports to manage SIEM components.
- Creating reports as per client requirement.
- Analysing daily, weekly and monthly reports.
- Creating case for the suspicious issue and forwarding it to Onsite SOC team for further investigation.
- Monitoring the events on SIEM tool.
- Creating the tickets in ticketing tool.

<https://www.indeed.com/r/Pradeep-Kumar/96485546eadd9488?isid=rex-download&ikw=download-top&co=IN>
<https://www.indeed.com/r/Pradeep-Kumar/96485546eadd9488?isid=rex-download&ikw=download-top&co=IN>

- Finding false positive, fine tuning and escalating Security events.