Bharat Ram Pandey
Email: brpandey45@gmail.com
Mob: +91-8319569007

CAREER OBJECTIVE:

Diligent Cyber Security Specialist proficient in online security research, planning, execution, and maintenance. Adept at training and educating internal users on relevant cyber security procedures and preventative measures. Specialize in network monitoring, security software installation, and working to prevent cyber-attacks, especially in business and corporate settings.

TOTAL WORK EXPERIENCE:- Total Experience of 7+ Years Security & Network domain.

EDUCATIONAL QUALIFICATION:-

- Bachelor of Engineering (Electronics and Communication) with 64.2% from RGPV Bhopal.
- Higher Secondary with 62.6% from M.P. Board Bhopal.
- High School with 84.1% from M.P. Board Bhopal

Additional Expertise: -

- Experience in SIEM tools :- ArcSight & RSA Netwitness.
- Experience in Cortex XSOAR – Incident Management.

Experience Summary:-

Organization: Inspira Enterprise limited
Designation: Senior Security Analyst
From December 2022 to Present

JOB PROFILE:-

- Monitor security events and logs such as Proxy logs, IPS/IDS events, Firewall Active Directory , Antimalware events, Web Application Firewall (WAF), Endpoints security to maintain situational awareness
- Investigate malicious Phishing emails, domain and IP's and recommend proper blocking based on analysis.
- RSA Netwitness SIEM infrastructure & direct the functions, processes, and operations of the SOC and ensures policies and procedures are followed.
- Ensure SLA compliances, process adherence, process improvement to meet operational objectives.
- Develop and maintain an incident response management program that includes incident detection, analysis, containment, eradication, recovery and chain of evidence / forensic artifacts required for additional investigations.
- Ability to work directly with customers to ensure not only resolution management but also customer satisfaction.
- Creation of reports, dashboards, metrics for SOC operations and presentation to Management.
- Analysis User and Entity Behavior Analytics and raised alerts if required.
- Ability to priorities and drive to results with a high emphasis on quality.
- Monitor the security events of critical systems (e.g., e-mail servers, database Servers, web servers etc.) and changes to highly sensitive computer security Controls to ensure appropriate system administrative actions, investigate and Report on noted irregularities with the help of RSA SIEM.
- Responsible for new implementations or upgrades to existing systems.
- Monitoring security events which is from IDS/IPS, proxy logs, AV, firewalls etc.
- Providing support to SOC Analyst personnel utilizing the SIEM to respond to security incidents and events.
- Assists in the investigation and remediation of security incidents using SIEM technology, reports, and pattern analysis.
- Directing and supporting persons to contribute to the effectiveness of the information security management system.
- First point of contact within the departments for incident/weakness reporting. If a user has reported an incident/weakness.
- Regularly updating the SOPs

- Creation content like Correlation Rules, Query, Report, Dashboards etc
- Creating Custom parsers.

Previous Organization: Aujas Cyber Security limited
Designation: Senior Consultant
From Feb 2022 to December 2022

JOB PROFILE:-

- Integration of new devices with RSA Netwitness such as Windows, Linux, CISCO Firewall, Routers, Switches etc.
- Creation content like Correlation Rules, Query, Report, Dashboards etc.
- Performing Real-Time Monitoring, Investigation, Analysis, Reporting and Escalations of Security Events from Multiple log sources.
- Monitor events, log analysis, and Investigate incident on daily basis.
- Investigate Incidents using /Dashboards/Events/Graphs/Cases and Reports.
- Escalate issues as per the escalation matrix to the operation heads or senior authorities for faster and better resolution.
- Acquired extensive hands-on experience in network engineering & troubleshooting.
- Hands on experience on the Incident Response activities like Malware analysis, Brute force analysis etc.

Previous Organization: EMS Management Services Pvt. Ltd.
Designation: Security Analyst
From Sep 2017 to Feb 2021

JOB PROFILE:-

- Installing ArcSight Connectors (Windows, Syslog Connectors)
- Integration of new devices with ArcSight such as Windows, Linux, CISCO Firewall, Routers, Switches etc.
- Upgradation of ArcSight Connectors.
- Doing the troubleshooting if connector cache log.
- Creation of ArcSight content like Correlation Rules, Query, Report, Dashboards etc.
- Performing Real-Time Monitoring, Investigation, Analysis, Reporting and Escalations of Security Events from Multiple log sources.
- Monitor events, log analysis, and Investigate incident on daily basis.
- Regular health checks, monitoring, and reporting.
- Investigate Incidents using Channels/Dashboards/Events/Graphs/Annotations/Cases and Reports
- Escalate issues as per the escalation matrix to the operation heads or senior authorities for faster and better resolution.
- Acquired extensive hands-on experience in network engineering & troubleshooting.
- Hands on experience on the Incident Response activities like Malware analysis, Brute force analysis etc.
- Worked in 24x7 Operational support.
- Motivated team player and can adapt and learn new technologies, tools, and application.

Previous Organization: - Ananya Manpower Solutions Pvt. Ltd.
Designation: - Project Engineer
From Nov 2015 to Aug 2017

JOB PROFILE:-

- Experience of working in L1 support and real time environment, alarm monitoring of issues and provide immediate solutions..
- Good knowledge of installation, provisioning, commissioning, system/ integration of various Telecom equipment's
- Rfi and Atp survey..
- Fault Analysis, Alarm Clearance, Corrective and Preventive action to reduce fault rate and improve network availability.

Training and certification:-

- Fortinet NSE1 and NSE2 certified.
- Qualys vulnerability management certified.
- CEH V11.

ASSETS TO COMPANY:-

- Excellent interpersonal skills.
- Strong determination to grow in an organization.
- I believe to work in team.

STRENGTHS:-

- Quick learner & Implementer.
- Ability to interact with clients and customers.
- Interested to prove excellent in all activities by commitments.
- An effective and innovative team controller.

PERSONAL DETAILS:

Date of Birth	**:** 12-11-1990
Nationality	**:** Indian
Marital Status	**:** Married
Languages Known	**:** English, Hindi
Address	**:** Sai Niwas sector -20 Belapur Navi Mumbai.

DECLARATION:
I hereby declare that all the above-mentioned information is true to the best of my knowledge.
Place: Navi Mumbai (Bharat Ram Pandey)