Sourabh Bhagwat

Associate Consultant

PERSONAL INFORMATION

Email
sourabhb445@gmail.com

Mobile
(+91) 7838974143

Total work experience
12 Years 0 Month

KEY SKILLS

Proof Point

Crowdstrike

Vulnerability Management

certified ethical hacker

Arbor

Ddos

SIEM

Log Analysis

Information Security

Security Monitoring

Security Analysis

Firewall

DDos

Cisco amp

Security Operations Center

McAfee Antivirus

OTHER PERSONAL DETAILS

PROFILE SUMMARY

Working with HCL Technologies Ltd. as a Associate consultant global cyber Security project in Soc team. Managing multiple Security technologies and incident response. Completed CEH training & Certification from EC council. I am interested to work in security operations, (SIEM), Soc team,cyber security domain.

EDUCATION

2008 — B.Sc
Devi Ahilya Vishwa Vidhyalaya (DAVV), Indore

2004 — XIIth
Hindi

2002 — Xth
Hindi

WORK EXPERIENCE

Apr 2022 - Present — Associate Consultant
Hcltech
Associate consultant in SOC team working on GSOC Project.

Mar 2021 - Mar 2022 — administrator security
Microland
As a Security Administrator I am responsible for managing and administration of DC-SOC operations and maintenance of various security Appliances. proficient in SIEM, Soc, cybersecurity, EDR, mcafee Epo and other Soc and network security tools.

Dec 2020 - Mar 2021 — Technical security
Hitachi Systems Micro Clinic
technical security field engineer

Jun 2017 - Nov 2020 — Information Security Engineer
Acpl Systems Pvt Ltd
Strong knowledge and experience in security events monitoring and operations. Investigating and creating case for security threats and forwarding it to onsite soc team for further investigation and action. Creating daily weekly and monthly analysis report for any security threats and send it to the all divisional team for further investigation. Performing log analysis & analysing the crucial alerts at immediate basis.

City Gurugram

Country INDIA

LANGUAGES

- Hindi
- Marathi
- English

Preparing reports on daily basis as per the client request preparing knowledge base and use cases. Preparing security documents and templates for escalations. Data source integration and Creating watchlist & alarms,reports on ESM for related IOC's. writing parsers. Prepare device health reports on daily basis. Communicate with McAfee TAC team for better fine tuning with SIEM. Upgradation the SIEM as required. hotfix updation. Responsible for any issue related to the SIEM appliance (hardware or software) take proper follow-up with McAfee TAC hardware team and close the case earliest.

Apr 2013 - May 2017

Network and information Security Engineer

Wipro Infotech

As a Network and information Security Engineer I have experience working with various network security appliances like switches,router, firewall , SIEM etc....

Projects

365 Days

Heromotocorp DC SOC

I am working in Centralized DC-SOC Team and responsible for providing Security monitoring services and incident response also Administration and Day to day operational task of various Security Devices tool like MacAfee SIEM, Cisco AMP, Dark trace, McAfee ePO, Big Fix. Coordinating with various TAC vendors and troubleshooting the issues. Coordinating with location team and follow ITIL framework (Incident, Problem, and Change). Weekly and Monthly SOC MIS Report Creation and presentation with Client.

1249 Days

IOCL Gurugram

it is a centralised data centre in Gurgaon for managing all divisions and soc engineers working 24*7 in SOC and Administration of network security and cyber security domain. I am responsible for mcafee siem administration configuration upgradation installation and reporting to the client on priority.

COURSES & CERTIFICATIONS

- CNSS (Certified Network Security Specialist) by International Cyber security Institute)
- Intel certified product specialist (Mcafee SIEM)
- CEH
- splunk fundamentals
- Insightvm Certified Administrator