TAC Security

Information security Manager

Cyber Security Business | Experience:3-5 Years

Key Skills:

VAPT, OWASP, Pentesting, Source code review, Vulnerability assessment, Web application security, Network security review, Network architecture review, Configuration review, Process review, Multi tasking, Time management , Team handling, Cryptography, Malware , SIEM Solutions, SPLUNK. Security intelligence threats and threat actors. Strong Analytical and Problem-Solving Skills., Good knowledge of Security devices and it's functioning

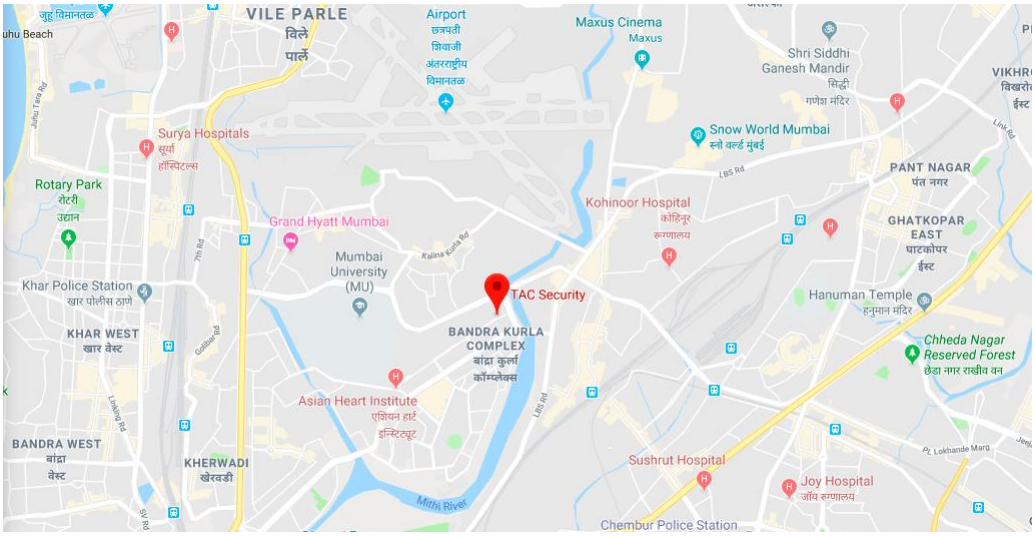
Key Responsibilities:

- To perform network penetration testing both for external and internal networks. Assessments involved information gathering, port scanning, operating system fingerprinting, service fingerprinting, vulnerability scanning, manual verification of vulnerabilities and reporting. Performed exploitation of vulnerabilities as part of penetration testing activities.
- To design and implement security systems to protect a company or organization's computer networks from cyber attacks, and help set and maintain security standards.
- To use advanced analytic tools to determine emerging threat patterns and vulnerabilities.
- To identify potential weaknesses and implement measures, such as firewalls and encryption.
- Liasoning with stakeholders in relation to cyber security issues and provide future recommendations.
- To assist with the creation, maintenance and delivery of cyber security awareness training for colleagues.
- To give advice and guidance to staff on issues such as spam and unwanted or malicious emails.
- Responsible for monitor SIEM Dashboards and SIEM administration, Management and fine-tuning or Health monitoring of SIEM solution.
- Responsible for team & vendor management, overall use of resources and initiation of corrective action where required for Security Operations Centre.
- Ensure incident identification, assessment, quantification, reporting, communication, mitigation and monitoring
- To perform mitigation with the help of asset owners.
- To Perform threat management, threat modelling, identify threat vectors and develop use cases for security monitoring.
- 24/7 Security Monitoring & Alerts with Faster incident response, remediation and monitor and respond to 'phishing' emails and 'pharming' activity.
- To create and implement Use-cases/content for process enhancement and better security.
- To Ensure all the integrated devices are sending logs without fail.
- To Ensure all rules and reports are working as expected.
- Scripting languages such as python & PowerShell.

Preferred Qualification:

- B. Tech, M. Tech, BCA, MCA, B.SC, M.SC- Computers.
- Certification in CEH
- . Certification in OSCP, ISO 2001, PCI-DSS, CCSP (Preferable)

Location:



- **Mumbai, INDIA**

  #13, 1st Floor, Pinnacle Corporate Park, Near Trade Tower

  Bandra Kurla Complex (BKC), Bandra East, Mumbai, Maharashtra 400051

To learn more about TAC Security, visit: **www.TACSecurity.com**

TAC Security, Inc.
99 Wall Street, #554 New York NY 10005,
New York, New York 10005, US

TAC InfoSec Private Limited
World Tech Tower, Plot C-203 4th Floor,
Industrial Area, Sector 74, Mohali, Punjab
160055

About TAC Security

TAC Security is a leading and trusted cyber security consulting partner that specializes in securing the IT infrastructure and assets of the leading enterprises and governments globally.

TAC Security protects ₹1 Trillion transactions every year through it's Artificial intelligence (AI) based Vulnerability Management Platform ESOF (Enterprise Security in One Framework)

TAC Security