ROHIT BANKOTI

[redacted] [redacted]

Accomplished and certified IT security professional with experience assisting organizations successfully complete enterprise-wide security projects.

Experience in finance, technology, healthcare, telecom industries and a proven track record of streamlining security processes, design and implement efficient security solutions, lead and assist multi-disciplined, multi-national teams in achieving security efficiency.

Professional Qualifications:

Degree	Bachelor of Technology (Computer Science [redacted])
CGPA	6.36/10
Institute	**University Institute of Engg. & Tech. (MDU), Rohtak**

Academic Qualifications:

- Completed XII standard from **Hamdard Public School** (CBSE) in [redacted] with 79%
- Completed X standard from **Amrita Public School** (CBSE) in [redacted] with 81%

CERTIFICATIONS

- Sophos Certified Architect for UTM by RED Education.
- Sophos Certified Engineer for Endpoint, MDM, Email protection, Encryption.
- GFI (Languard, FAX maker, Mail essential & Cloud, Endpoint security
- CEH version 7 training from net hub.
- ECSA (E-council) 412-79 complete training from net hub.
- Smooth Wall Certified engineer and Operator Certified.
- McAfee certified for McAfee VSE, EPO, Mobile Management, HIPS and Mail.
- Symantec Partner certification and Advanced Threat Protection.
- Certified Information Security and Ethical hacking (C.I.S.E) from innobuzz.
- Infowatch (DLP) training on endpoint and network level.
- Qualys Vulnerability Expert.
- C++ and .NET certification from Aptech, South Extension (Delhi)

Professional Synopsis:

Currently:-

Working with Mckinsey & Company, Gurgaon, India as Security Engineer.
- Mainly working with ATP projects.
- Anti-phishing program
- Other Operations

2015 to 2016 with CSC (Computer Science & Corporation), Noida
- Sandboxing and Malware clean-up process
- Identify Malware Domain and Phishing Attack vector.

- **Dec 2014 to Aug 2015 with ASIT, Delhi as Security Consultant.**

Working as UTM, SIEM, MDM and DLP architect.
•UTM: Cyberoam, Fortigate, Sonicwall.
•Endpoint Software: McAfee, Symantec, Eset, Kaspersky.
•Vulnerability Scanner: GFI languard, Nessus.
•Web Proxy: Barracuda, Untangle, squid.
•SIEM: Splunk, Arc sight.
•IDS/IPS: SourceFire NGIPS, Threat Track.
•WAF: Astaro, Barracuda
•Mobile Device Management: Mass360, McAfee (EMM).

Worked security and Auditing of Company like Desein Indure, PVR group, NEWS Channel (India TV/Live India) and more

- **June 2012 to Nov. 2014 with Satcom InfoTech Pvt Ltd. (Distributor Firm) , Sarita vihar (Delhi) as Technical Consultant for North-India region.**

DUTIES & RESPONSIBILITY: Installation, management and troubleshooting.

- UTM: Sophos (Astaro), Smoothwall, Kerio.
- Endpoint Software: Sophos, Vipre, McAfee.
- Encryption : McAfee (safe boot),Sophos(Utimaco), WinMagic, Kaspersky.
- Email Security: Sophos(Pure Message), Mcafee, GFI Mail Essentials, Kerio connect.
- Moblie Device Management: Sophos(SMC), Mass 360, McAfee(EMM),GFI MDM.
- Vulnerability Scanner: GFI languard, Nessus.
- Web Proxy: Smothwall(SWG), GFI(Web Monitor), Barracuda.
- SIEM: McAfee, Splunk, GFI Events Manager.
- IDS/IPS: SourceFire NGIPS.

Other: GFI Mail Archiver, GFI Fax Maker, **Threat Track sandbox**, Infowatch DLP.

Client List: AMTEK Auto, Matrix, Birla Soft, MIND, Dainik Jagran, Prime bank (Bangladesh), Exide battery (W.B.), MIT (pune), Rockland Hospital and more.

Network Security

- Network Engineering including Infrastructure Firewalls, UTM, DMZ Architecture, VPN Remote Network Access, Site to site VPN, WAF, Messaging & Email Security, Web Content Filtering, Access Control, IDS/IPS, Wireless protection etc.
- Network Infrastructure including Scope/Size/Requirements; Through Hands-on Deployment / Delivery /Implementation.
- Advice and Lead Client in the Network Security technology. Domain providing Infrastructure technical assessments, Discovery, Design, Architecture and Implementation.

Endpoint Security

- Install and maintain Enterprise Security infrastructure including Anti-Malware, Anti-Spyware, IPS/IDS, log management, and Vulnerability assessment.
- Hands on remediation of malware/virus that were not automatically handled and utilized various security tools to either prevent or remediate security problems.
- Implemented and maintained data loss prevention for incident and risk.
- Encryption (POA/PBA, AES256, key management, data recovery, email and mobile).

Mobile Device Management

- Device: Android, BlackBerry, Apple IOS, Window mobile/phone and more…
- (Compliance Status, Policy enforcement over different medium, Security over apps/device/calls/message/email, encryption, cloud storage, passcode, location, device wipe, restrictions, Wi-Fi & VPN etc.)

Threat / Intelligence Analyst

- Knowledge of attack vectors, threat tactics and attacker techniques.
- Strong understanding of Microsoft Windows SYS Internals
- Deep understanding of incident response, practices and processes
- Static, Dynamic and Network Analysis tools
- Familiarity with intrusion detection systems (e.g., snort) and tools (e.g., tcpdump, Wireshark)

Working with Python and Perl interpreter for endpoint and network for customization.

Also Presales experience including POC, SOW, SOP, RFI, RFP, and Technical Demonstrations, formal Technical Sales Presentations and Leading Technical Workshops, etc.

Strengths

- I am self-driven, responsible, and optimistic and believe in innovations.
- Strong determination is the built in trait of my personality, abilities to lead any team and mutual cooperative person.
- Familiarity with Information Security regulations - HIPAA, ISO/IEC 27000, and PCI DSS.
- Wide knowledge of information security principles and practices and ability to manage independently.

Personal Details:-

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
Nationality -	Indian
Languages -	Hindi, English

(Rohit Bankoti)
[redacted]

[redacted]