Shabeer Ibrahim

Mobile: +974 3390-8540
Email: shabeeribm@gmail.com
Web: **linktr.ee/shabeeribm**
Skype: shabeeribm
Location: Qatar
Relocation: Open

Hands on Experience

- Cisco Identity Services Engine (ISE)
- Cisco Stealthwatch
- CarbonBlack Appcontrol
- CarbonBlack Response
- Cisco Umbrella
- Cisco Ironport
- Qradar SIEM
- Bluecoat Proxy SG
- Tenable
- Attivo BotSink
- Thinkst canary box
- Cisco ASA Firewall
- Palo Alto Firewall
- Incident Management
- Windows Forensics
- Memory Forensics

Domain Expertise

- Military
- Petroleum
- Banking
- US IT Recruitment

Professional Summary:

Cyber Security Engineer having experience with SIEM Solutions, Firewalls, Deception devices, Whitelisting devices, EDR solutions and other security devices

- Familiar with Cisco ISE, Cisco ASA and Palo Alto firewalls
- Familiar with EDR solutions like CarbonBlack response
- Familiar with monitoring devices like Qradar SIEM and Cisco Stealthwatch
- Excellent customer service skills and has experience in providing telephone, remote and email support to users.

Education and Trainings

- **B-Tech in ECE from MES CE, Kuttipuram**
- Implementing and Configuring Cisco Identity Services Engine (SISE) training
- CyberCrime Prevention training by MOI Qatar
- Attivo Network Administration training
- CB Response Training
- CB Appcontrol Training
- Tenable.sc scanning and Analysis training
- **SANS FOR508**: Advanced Digital Forensics, Incident Response, and Threat Hunting
- **SANS FOR572**: Advanced Network Forensics & Analysis

Certification

- GIAC Certified Forensic Analyst (GCFA)
- Palo Alto Networks Certified Network Security Administrator (PCNSA)
- Cisco Certified Network Associate (**CCNA**)
- Cisco Certified Network Associate (**CCNA Security**)
- Cisco Certified Network Professional (**CCNP R&S**)
- Certified Ethical Hacker (C|EH)
- Attivo Administration Fundamentals v4.2

PROFESSIONAL EXPERIENCE

CONFIDENTIAL, QATAR GOVT MAY 2016 – PRESENT

Title: Cyber Security (SOC) Engineer

- Performs real-time monitoring, security incident handling, investigation, analysis, reporting and escalations of security events from multiple log sources.
- Daily SOC operations also include log analysis and finding anomalies, designing new correlation rules, setting up dashboards, generating audit reports, fine-tuning existing correlation rules to reduce false-positives and responding to incidents.
- Perform vulnerability assessments, security testing, and work with operations and development teams on remediation and mitigation of findings and to produce and deliver a cyber security analysis report
- Manage network Security devices including firewalls and EDR solutions
- Development of use cases for Qradar SIEM and Cisco Stealthwatch and CB Response
- Making recommendations to management regarding security enhancements and improvements
- Creating and analyzing Annual maintenance contract and BoQ for security products
- Actively Blacklisting/Whitelisting third-party software programs which has vulnerabilities using Carbon Black Protection / Appcontrol
- Configuration, Troubleshooting and maintenance of Cisco Identity Services Engine (ISE)

PETROLINK DATA SERVICES LTD APRIL 2014 – APRIL 2016

Title: ICT Engineer

- Work as a part of 24/7 support team responsible for technical support at the network level: WAN and LAN connectivity, Firewalls / VPN / Active Directory / Servers and Security issues
- Manage and secure corporate mobile phones using Maas360 MDM
- Monitor the entire IT infrastructure using tools and manage system alerts and notifications and respond accordingly to resolve the issues.

CMC LIMITED, A TATA ENTERPRISE NOV 2013 – MARCH 2014

CS-Network Support Engineer

End Client : Reserve Bank of India, Cochin
Project : IDRBT Leased Line FM and AMC Project
[Support for Cisco Routing/Security Solutions]

NEWAGESYS SOLUTIONS PRIVATE LTD DEC 2010– NOV 2012

Sr Resource Specialist

CLERYSYS, INC DEC 2007– NOV 2010

System Administrator