C-104 Ramchandra Niwas, Plot 21-2
2, Sector – 12 A, Koparkhairane
Navi Mumbai MH 400709
E-mail: raghurajch@gmail.com
Mob: 9960524140/9930223071

Raghuraj Singh Chouhan

CISM, CCSP, CEH, CCNA, MCSA, ITIL

Objective Having obtained Global Certification and being a qualified CISM, CCSP, CCNA, MCSA, ITIL professional, I am looking forward to working in a challenging environment that provides opportunity to learn key technologies (Information Security) field, with focus on establishing and enhancing Information Security within an organization best of my capabilities.

Summary **Total Work Experience (16+ Years)**
Employer #1 : **HDFC Bank Ltd Mumbais**
Designation : Asst. Vice President (AVP) Cyber Security
Duration : **Jan 2018 to till date**

Job Profile : Project/Vendor/Resource Management, SIEM, SOAR, AIML, IR (Incident Response), Process Automation, Policy, Vulnerability Management, Security solution evaluation and Implementation, FPN (Funding Proposal Note), Budgeting, PO(Purchase Order), PoC (Proof of Concept) of Security Solution, Presentation, Cloud (AWS, GCP) Firewall, Algosec, Xypro, HP Nonstop , BASE24, zSecure (IBM Mainframe), Vision plus and Xygate SecurityOne, Database Activity Monitoring (DAM),), TCO, IT Audit.

Employer #2 : **Pricewaterhouse Coopers Pvt Ltd (PwC)**
Designation : Asst. Manager) Cyber Security
Duration : **Aug 2014 to Dec 2017**

Job Profile : IT Audit, Implementation of Security solution, Configuration review, hardening of Security devices, Gap assessment and closer, Project Management, VAPT, SIEM (RSA Envision, RSA SA, ArcSight, McAfee and QRadar), NIPS, IDS, Web Security, Nessus, Firewall (Checkpoint, Fortigate, Cisco ASA), NIPS, McAfee EPO, PIM (Arcos) Cisco ACS, Nmap, Backtrack, winscp, SSH putty, wireshark , CSM (Cisco Security Manager), HLD, LLD, , SIEM Use case, Leading project end to end, reviews of document, SoW, SOP, MBSS, Vulnerability assessment, IT Governance, reporting etc, NAC (Nevis,)Third Party Information Security Assessments

Employer #3 : **Capgemini India PVT ltd** (SOC)
Designation : Consultant (Sr. Security analyst)
Duration : **June 2011 to July 2014**

Job Profile :

Information Security Analysis :

- Addition/modification/removal of devices from RSA monitoring tools after regional security officer Approval.
- Creation/modification/removal of content (Rules, Reports and Dashboards) from RSA monitoring tools.
- User access management for RSA monitoring tools
- RSA tools' Backup activity, configuration, change activity, Upgrade, Update, tool health check etc.
- Perform the Vulnerability Scan through the Nessus security center with regional Nessus scanner.
- Report the latest vulnerability to the respective team for further action
- Raising the VA tickets based on Critical, High and Medium vulnerability.
- Analyzing critical security events occurring across the organization and maintaining decorum within organization.
- Integration of Window, Linux, SQL, Network and security devices with RSA Envision.
- Support all aspects of Security Information and Event Management initiative.
- Analyzing various Security events on RSA Envision case management, taking audit trials.
- Vulnerabilities management for security / Network /Servers / Host Devices and provide the solution to maintain their security from attackers, Providing Remediation and Action based on the Vulnerability detected and follow ups with the respective team.
- Handling Critical events driven SLA and OLA.
- Responding to day-to-day security requests relating to RSA Envision operations.
- Focused on IT risk Management Services, security services, Vulnerability management and assessment services.
- Review security device logs to analyze network traffic for suspicious/malicious activity.
- Creating Work Instruction for security related events and providing a feedback loop on simplifying the process and procedures.
- Log reviews and security forensic reviews.
- Investigating different types of malware with the help of different tools and sending it to the vendor for further investigation and then updating the signature database. Risk and Vulnerability Assessments.
- Scanning windows, Linux and network and Security devices using Nessus and preparing report accordingly.
- Threat detection and management by Nessus Scanning.

Tools:

RSA, Security Analytics, RSA Envision (ES 5060)4.1, Nessus Security center, Nessus 5.1,Tipping point SMS, Prolexic ddos mitigation , BMC Remedy, Putty, SysAid, ticketing tool and many more tools.

Employer #4 : **Bank of America** ICC (Information Control Center)
Designation : Sr. Engineer Information Security (SOC)

Duration : **Aug 2009 to June 2011**

Job Profile :

Information Security Event Analysis:

- Analyzing critical security events occurring across the organization and maintaining decorum within Bank of America, Countrywide Financial and Merrill Lynch and other acquired firms in terms of Information security.
- LOBRA (Line of Business Risk Assessment) and Emergency LOBRA.
- Malware analysis through 41 Anti-virus and Anti-malware engines.
- Focused on IT risk Management Services, Application security services, Vulnerability management and assessment services.
- Analyzing various Security events on ArcSight case management, taking audit trials.
- Handling Critical events driven SLA and OLA.
- Creating Work Instruction for security related events and providing a feedback loop on simplifying the process and procedures.
- Providing Internal trainings to team on various critical security events and managing case in ArcSight.
- Generating events manually for the security related issues which are need to be adhered by SLA.
- Managing and working on Security event Lifecycle from the creation of events to closure.
- Generating reports and taking audit on that.
- Working with various teams such as firewall teams, Desktop teams, proxy team, etc in setting up different security rules and addressing security issues.

- Working on IDS and IPS indirectly, understanding the signatures, updating the signature database time to time.
- Monitoring of traffic flow on critical e-commerce servers via Arbor dashboard.
- Investigating different types of malware with the help of different tools and sending it to the vendor for further investigation and then updating the signature database. Risk and Vulnerability Assessments.
- Information Security Review's.

Tools :

- Arc Sight 5.0.1 SIEM, Remedy, simslogger (Linux based server), wireshark, Arbor, snoop portal (for IDS / IPS analysis), Nessus, Nmap, Backtrack, winscp, SSH putty, Tectia and many intranet based tools used for Threat management

Employer #5 : HCL COMNET
Designation : Sr. Engineer Information Security (**Reserve Bank of India**) SOC
Duration : February 09 to June 09

Employer Profile :

The activities of the company focused – Utilities, Banking and Telecom, among others. In the area of services the HCL covers the entire range of communication and computing systems (Hardware and Software's) ranging from leased lines, radio links, terminal equipment.

Clients: Reserve Bank of India (Datacenter)

Job Profile:

- As an Information Security Eng. at Reserve Bank of India (Client), Maintaining the security and security Components in datacenter. Maintaining the security set up that includes Checkpoint NGX R62, Nokia IP 1220, Eventia Reporter, Smart view monitor, IPS 4240, FWSM, ISDM, Switches 3550, 3560, Symantec Antivirus 10.2, HIDS 5.1, Maintaining and configuring of Firewalls, rules, routes and VPN policies.

- Maintaining the security set up that includes Checkpoint NGX R62, Nokia IP 1220. Event management, Incident management, Access rights management and Configuration change management, Report Generation and analysis for Network threat management and mitigation using IDS and Firewall.

- Monitoring and analyzing IDS events, signature and signature engine up gradations, Monitoring/ analyzing Firewall reports at Eventia Reporter like blocked and access connections reports and all as well as Checkpoint real logs and Symantec HIDS 5.1 reports.

- Monitoring Symantec Antivirus 10.2 both 32 bit and 64 bit updates and user definition at Server, Managing backup strategy weekly and monthly, fine tuning of all security devices, Co-ordination with Network and System Engineers.

Employer # 6 : Network Solutions (**An IBM Company**).
Designation : Network Security Engineer. (Oriental Bank of Commerce) SOC
Duration : February 07 to 8th February 09.

Employer Profile :

The activities of the company focused – Utilities, Banking and Telecom, among others. In the area of services the NetSol covers the entire range of communication and computing systems (Hardware and Software's) ranging from leased lines, radio links, terminal equipment and PCs to Powerful servers to meet user requirements.

Client: Oriental Bank of Commerce (Datacenter) SOC

Job Profile:

- As a member of Orientals Bank Network Security Team (Client), Maintaining the security and security Components in datacenter. Maintaining the security set up that includes Checkpoint, CSMARS, CSA, CSM, ACS, PIX 535, PIX 525, 515E IPS (V6.0) 4215, Maintaining and configuring of firewalls, rules, routes and VPN policies.

- Event management, Incident management, Access rights management and Configuration change management, Report Generation and analysis for Network threat management and mitigation using CSMARS and VMS. Analyzing security of severs in coordination with System Engineers using CSA, up gradation of latest signature and engine in IPS and CSMARS.

- Co-coordination the NOC engineers and FMS engineers from all over India for any network related problem. Managing backup strategy for Device configurations, raw data (PIX SYSLOG massages and IPS events), reports and logs for future analysis, Update managements for Devices in SOC setup and inventory maintenance.

Clients: Bajaj Allianz (Datacenter) Pune

Job Profile:

- Worked at Nortel firewall 5600, PIX Firewall (515E, 525), Checkpoint, Alteon switch Firewall, configuration of PIX firewall with as per user requirement giving access and NAT, PAT with public IP, Group policy and access rules creation with direction, policy pushing as per CPU utilization and VPN id creation at VPN contivity box.

- Implementation of Lease Line and ISDN (BRI & PRI), MPLS lines Commissioning & Lease line & ISDN lines. Along with WAN configuration, Routing protocols: OSPF Configuration on Cisco Routers (1700, 1800, 2500, 2800, 2600, and 3600), Switches (1912, 1924, 2950, 3550, and 3560 [L3]) and creating VLAN and inter-VLAN routing. Along with static routing, access-list. Designing of IP scheme as per user at branch.

- Managing & maintain the network uptime as per clients SLA, The work involves Network Handling, Solving problems related to Internet connection (Lease Lines, ISDN lines) Configuration of Routers, Switches, Modems. Router maintenance, replace hardware card & software like IOS. Co-ordinate with other region engineers for any new commissioning, shifting, up gradation.

Employer # 7 : Engicon System
Designation : System Engineer

Job Profile:

- Installation of Operating System, Hardware & System Administration to look after assembling and installation of PC's as well as maintenance of PC's and Printers at customer site, Networking and Troubleshooting.

- Solving problems related with Internet connection (Lease Lines, ISDN lines), Modem, Routers, Hubs, and Switches.

Technical Skills

- Configuration of Cisco Routers, Switches (1912, 1924, 2950, 3550, 3560 [L3]) and creating VLAN and inter-VLAN routing. Along with practical knowledge of routing protocols like RIP / OSPF.

- Good knowledge of Leased lines, ISDN, PRI, MPLS CH E-1 also involved in commissioning of Lease Circuits from BSNL and other service provider.

Planning & Designing

- Design a LAN, WAN IP Addressing scheme to meet design requirements, select an appropriate Routing Protocol based on user requirements, Simple Internet work using Cisco technology, Develop an Access-list to meet user specifications & choose WAN Services to meet customer requirements.

Implementation & Operation

- Configure Routing Protocols given user requirement such as RIP, IGRP, EIGRP, OSPF, Configure IP addresses, subnet masks & gateway addresses on routers and hosts, Configure a Router for additional administrative functionality, Switches with VLANs, Implement a LAN, Perform an initial configuration on a Router, Perform an initial configuration on a Switch, Implement Access-list & simple WAN Protocols such as PPP, HDLC.

Computers Skills:

Platforms : Windows 2016, 2012, Windows9x, Windows 2000, 2003 Server, Wi n xp, 2007 2008, MS-DOS, Linux, CentOs.
Packages : MS-Office.

Academic/Professional Profile:

- Pursuing **CISSP** (Certified Information System Security Professional)
- **CISM** (Certified Information Security Manager)
- **CCSP** (Cisco Certified Security Professional Certification).

- **ITIL V3** (Information Technology Infrastructure Library)
- **CCNP** Routing (BSCI) 642-801.
- **CCNA** (Cisco Certified Network associate 640-801) **ISCO ID: CSCO10922700**
- **MCSA** Microsoft Certified System Administrator (MCSA+ADS)

CCSP:-

- **SND** (Cisco Certified Securing Network Devices) with **1000/1000**
- **MARS** (Cisco Certified Monitoring Analysis and Response System) with **980/1000**
- **SNRS** (Cisco Certified Securing Network with Cisco Routers and Switches) with **1000/1000**
- **SNPA** (Cisco Certified Securing Network with PIX Firewall and ASA) **988/1000**.
- **IPS** (Cisco Certified Implementing Cisco Intrusion Prevention Systems) **953/1000**.

Education:

- MBA (Senior Management Program) from Indian Institute of Management Culkata (IIMC)
- M.Com. from DAVV Indore, M.P.
- B.Com from Barkatullah University, Bhopal MP.

Personal Profile:

Fathers Name	:	Shri G.S. Chouhan
Nationality	:	Indian
Passport	:	**K8952995**
Language Known	:	English, Hindi, Marathi.
Marital Status	:	Married
Permanent Address	:	Ramchandra Niwas, Plot 21/22, Sect. 12 A, Koparkhairane Navi Mumbai 400709

I declare that the above information is correct according to best of my knowledge

(Raghuraj Singh Chouhan)