Rajendra Mahesh Oak

Contact No.: +91 8080254390/7977345576 **E-Mail:** rajendraoakster@gmail.com

Career Summary

Focused SOC Specialist & Info Sec professional with 6.5 years of progressive expertise in information security, security operations & Technical support. Leverages expertise in security software and products to build solid IT security infrastructure Genuine team player committed to managing Operations and projects flawlessly while contributing to business objectives. Excellent Communication and interpersonal skills with hands on experience on a wide range of security Technologies.

Profile Snapshot

- Certified Ethical Hacker v9 Certification with 89.6%
- CISCO Certification of CCNA with 86.3%.
- IBM Qradar – SIEM
- Brand Monitoring – RSA (Anti Fraud Command Centre)
- Hyper Scale SIEM– DNIF (Netmonastery Product)
- IBM Guardium - DAM
- Vulnerability Management (Qualysguard/Nessus)
- Endpoint Security – McAfee Suite (Gateway,EPO,DLP)
- Brand Monitoring (RSA- anti fraud command centre)
- Cyber threat intelligence (IOCs & Patching)
- A thorough professional with a proactive attitude, capable of thinking in and out of the box, generating new solutions and ideas for the team and company.
- Experience in Information Security domain, worked on different flavors and versions of technology.
- Extensive experience in installation, administration, maintenance & troubleshooting.

Domain Interest

- **Cyber Security**
- **Information Security**
- **Audit**

Industry / Areas Worked

- **Cyber Security (SOC)**
- **Network Operation center**

Professional Background

Company Name : ***Reserve Bank Information Technology Pvt Ltd***

Tenure : **December 2021 to till date**

Profile : **SOC Specialist**

Responsibilities

- Managed SIEM/DAM Integration process to integrate critical Payment DB servers (RTGS/NEFT) as well as Non-Payment Servers. Also integrated Network Security Devices.
- Fine Tuning of SIEM use cases to reduce the false positive of incident alerts.
- Maintained documentation of security and disaster recovery policies andprocedures.
- Ensure all Threat intelligence IOCs received from various TI sources (Cert-IN, NCIIPC, IB Cart) has been blocked on priority on all security solutions.
- Ensure all latest vulnerabilities and zero day attacks CVE IDs are patched/blocked on respective security solutions on immediate basis.
- Proactively monitoring of RSA - Anti Fraud Command Centre (brand monitoring) to take down of phishing/malicious websites.
- Directed vulnerability assessments or analysis of information security systems.
- Evaluated performance indicators to assess security control quality.
- Provided technical support related to security product installation and use.
- Incident Management for Security Operations Centre.
- Review alerts raised by the SIEM, analyze the events and classify them.
- Ensure tickets are logged in the IT ticketing system.
- Follow up on closure of the tickets with the relevant stakeholders.
- Report on exceptions, highlight delays in incident closure.

- Assist in developing SOC vision, align to business, and build a roadmap to achieveit.
- Ensure that all servers, key applications, networking devices, security devices are integrated with SIEM solution.
- Ensure that all attacks on RBI information system are detected and managed.
- Undertook IPS Fine-tuning project for limiting the noise over the Security infra and proper implementation of required rules and policies for IPS signature blocking/Whitelisting.

Company Name : **Netmagic Solutions (NTT Global Communications Company)**

Tenure : **March 2018 to December 2021**

Profile : **Senior Engineer – Security Practice**

Responsibilities

- Responsible for providing L2+ support to security infrastructure hosted in Netmagic Datacenter and customers Datacenter
- Investigating Security incidents within the organization and providing Investigation reports and recommending corrective measures.
- Conducting Quarterly Vulnerability Assessment of customer Infrastructure.
- Configuring and Managing Web Application Firewalls such as Imperva, monitoring Web attacks and fine tuning policies.
- Analyzing logs and determining feasibility of the use cases to be implemented as per the customer requirement using the SIEM tools.
- Creating co-relation rules, designing and implementing use cases, reports & dashboards on SIEM
- Providing yearly/quarterly cyber audit data and close necessary points
- Prepare monthly/quarterly governance PPT and conduct meeting to discuss customer requirements
- Configuring and sharing daily, weekly & monthly reports
- Managing endpoint security with McAfee threat prevention (EPO/DLP)
- Upgrading/migrating customers SIEM & WAF tools
- Managing DR Drills at NCDEX trading commodity as per SEBI standards

Company Name : **Softcell Technologies LTD**
Tenure : **April 2016 to October 2017**
Profiles : **Security Engineer**
Project : **HDFC Bank (PCI-DSS)**
Responsibilities

- Handling Vulnerability Assessment, reporting Vulnerabilities to the concerned team and working towards its remediation.
- Hands on experience on Vulnerability Management tool – **QUALYS GUARD**.
- Working on highly critical and pressure based zone of HDFC's PCI-DSS Security project, coordinating with cross product and cross functional team for maintaining security levels at peak and eliminating maximum security threats as per Banking standards.
- Working knowledge on McAfee proxy, URL Categorization/URL ticketing whitelisting/blacklisting that contain malicious and could create security exploit in the domain such as RANSOMWARE, ADWARE etc.
- Working knowledge on **GLOBALSCAPE EFT v7.3.6 /7.3.7 / 7.4.2,** user creation/deletion, key mappings, assigning rights and troubleshooting issues related to files transfer through FILEZILLA & WINSCP in SFTP upon which bank's day to day operational tasks have major dependency.
- Conducting DR Drills pertaining to various security applications & products.
- Analyzing event logs while troubleshooting accessibility of any applications.
- Coordinating with global OEM teams for security related issues, their timely fixes minimizing business risk.
- Preparing various month end & quarter end security reports such as audit reports, capacity planning, vulnerability assessments, daily checklists, etc.
- Indulging in monthly Bank meetings for technical & operational improvement areas.
- Working knowledge on Nessus and Qualys guard

Certifications& Trainings

Academic Credentials

- **2014** B. Com from Mumbai University with 60.14%
- **2011** 12th from V.K.Krishna menon College, Maharashtra State Board with 55%
- **2009** 10th from Wamanrao muranjan vidyalay Maharashtra State Board with 76.76%

IT Proficiency

NETWORKING

- Network topologies, OSI Model
- Internet, intranet, routing protocols, VPN
- Different network methods like LAN, MAN, WAN, WLAN, TCP/IP architecture
- Familiar with routers, bridges and other networking devices
- Good knowledge of networking protocols, DMZ, SFTP

CISCO (Certified CCNA (640-802) 863/1000)

- Vlan, ACL, BGP, CISCO IOS
- RIP, RIP v2, PPP, HDLC, PAP, CHAP
- OSPF, EIGRP, Link state protocol, CDP
- Good Switching and routing knowledge
- IPv4, IPv6 and sub-netting knowledge, frame relay

- **CEH v9 Trained**
  - Nessus and NMAP
  - Wireshark and metasploit
  - Malware Threats
  - SQL injection & scanning networks.

- **SOFTWARE & COMPUTER SKILLS**
  - Windows/Linux Proficient skills in Windows 10, 8, 7, XP and Ubuntu / RHEL
  - Computer Skills MS Office (Word/ Power-point/ Excel/Outlook), PC Hardware & support skills.

Additional Training

- **Institute Name** : Nettech India.
  Training Undertaken : CCNA (640-802)
  Location : Thane

- **Institute Name** : Quik-Quest Institute of Knowledge
  Training Undertaken : CEH (certified Ethical Hacker)
  Location : Thane

- **Institute Name** : CMS Institute.
  Training Undertaken : Hardware H+ & Networking N+
  Location : Thane

Personal Dossier

- Date of Birth: 5th January, 1994
- Languages Known: English, Marathi & Hindi
- Gender: Male
- Marital Status: Married
- Nationality: Indian
- Home Town: Mumbai –Mulund (400082)
- Interest and Hobbies: Playing football, cricket
- Profile :www.linkedin.com/in/rajendra-oak