DHANANJAY RATHOD

Email: Dhananjay.v.rathod@gmail.com **Contact number:** 9920223425

Information Security Engineer

*Information Security Analyst with 7 years experience in **security event analysis** and **network security.** Seeking a position which can provide **growth** & **excellence** and earn a job which provides **job Satisfaction**, **self-development** and also be involved in work where I can utilize skill and **creatively** involved with system that effectively contributes to the **growth of organization**.*

Technical Skills

- *SIEM – Qradar, Security Analytics, Archsight, RSA Envision*
- *WAF – Imperva, F5, Radware*
- *Firewall – Checkpoint, Juniper, Paloalto*
- *Fireeye APT – HX (EDR), NX, FX*
- *Device management, Forensic Investigation & Use case creations*

Soft Skills

- *Systematic work procedure*
- *Leadership and Decisiveness*
- *Self Confidence & self motivation*
- *Critical Thinking, Creativity and Probem solving*
- *Adaptability and Collaboration*

PROFESSIONAL EXPERIENCE

❖ **IBM India pvt. Ltd.** (February2020 to Current date)

- Client/Project: **Axis Bank Ltd. & Bank of Baroda**
- Working as a Technical Services Specialist (L2 – SOC & Network Security).

➢ Daily BAU activites:

- Incident Response: Providing expert analysis on critical incidents after L1 analysis.
  - Providing remediation to resolve existing incident & recommendation .
  - Implementing/Finetuning SIEM/EDR/WAF rules as per MITRE framework.
- Upgraded Qradar from 7.4.3 FP3 to 7.5.0 UP2 IF2.
- Worked on mitigation Log4j zeroday vulnerability and against Dragonforce attacker group.
- Troubleshooting issues related to VA Scans or log forwarding to SIEM tools.
- Closing points related to VA Scans, Web App. Security , internal and external audits.
- Implementation of Fireye HX for endpoint analysis and Participation in IDRBT cyberdrill.
- Implementing firewall change requests on PA, Juniper, Checkpoint, AWS& Azure Cloud setup.
- Implementing change requests on F5 LB/dns.
- Managing, generating and troubleshooting issues for SSL certificates and SSLV devices.
- Troubleshooting connectivity issues for firewall changes, load balancing, 2way ssl, vpn tunnels.
- Installation and troubleshooting issues for security devices in datacenter.
- Implementing/troubleshooting signature changes on IPS/WAF. Onboarding Applications on WAF .
- Integrating security devices and servers with Qradar.

➢ Tools/Technologies used:

- Qradar – SIEM, QNI, QRIF
- WAF – Imperva, F5, Radware
- SSL Visibility – Symantec, Radware
- QualysGuard
- Checkpoint Firewall
- Forcepoint DLP
- FireEye – NX, FX, HX
- IPS - Tippingpoint
- Smokescreen - WebDecoy
- Juniper Firewall
- Entrust (Certificate Generation)
- Arbor APS
- F5 – LTM / GTM
- NTP-Microsemi
- PaloAlto Firewall

❖ **Paladion Networks** (February2019 to Jan2020)

- Client/Project: **BNP Paribas**
- Working as an L2 Analyst in Security Monitoring Center(Incident Response).

➢ Daily BAU activites in Incident Response:

- **Analyzing IPS** for any anomalous activities from outside or within the network.
- **Analyzing WAF & Firewall logs** for any web-based attacks on public facing IP's.
- **Malware analysis** of files and **sandbox analysis** of files or URLs.
- Monitoring for any multiple **login failures patterns** in Databases, Servers and workstations.
- Monitoring **proxy logs** to check for any breach in daily upload/download limit and site access.
- Monitoring for any **critical commands execution** in databases.
- Creating **health check** and event count report for SIEM device and related tools.
- **Searching for any IOC's** from the received threat intelligence feeds.
- Monitoring for **DDoS** based network or application attacks.
- Creating Incident tickets and providing recommendation for the remediation of assigned incidents.

➢ Other activities:

- Participation in **Cyber drill**.
- Providing analysis and logs to internal CSIRT team.
- Checking perimeter devices to check for any recon activity or any possible threat.

➢ Tools used:

- ArcSight SIEM tool
- McAfee Advanced Threat Defence
- RSA Archer
- Recorded Future
- Soltra Edge

❖ **HCL Comnet** (May2018 to February2019)

- Client/Project: **State Bank of India**
- Working as an L2 Analyst in Security Operation Center (DAM).

➢ Daily BAU activites:

- Performing **integration of new databases** and maintaining the appliances, as well as **troubleshooting** occurred issues.
- Monitoring Database activities, setting alerts and raising incidents if suspicious activity found.
- Performing log & configuration **backup of DAM Policies**.
- Creating **dashboards and setting alerts** in RSA SA, and monitoring the same.
- Performing **weekly and monthly checks for DAM and SA devices**, for fine tuning.
- Incident response/management : Detecting, Analyzing/investigating and Acting on Incidents and providing recommendations to the affected team/departments.

➢ Tools used:

- Imperva DAM.
- RSA Security Analytics.
- RSA Archer.

❖ **HCL Comnet** (June2016 to May2018)

- Working as an L1 Analyst in Security Operation Center.

➢ Daily BAU activites:

- Incident response/management :
  - **Monitoring alerts** from various devices, performing analysis and generating reports.
  - Keeping track of latest updates from sources regarding **blacklisted IP's**.
  - Acting on Incidents and providing recommendations to the affected team/departments
- **Creating dashboard** and dashlets, **parsing logs** for unsupported devices.
- Checking **status of DAM DB Agents** and monitoring alerts.
- **Integrating new DB Servers** as per requirement.
- Ticketing tool- HP Service manager to **raise incidents**.

➢ Other activities:

- Providing analysis and logs to Incident Management team.

➢ Tools used:

- RSA Envision.
- HP Service Manager (Ticketing)

❖ **RTNS** (September2015 to June2016)

- Working as an L1 Analyst in Security Operation Center

Trainings/Certifications and Badges

- IBM Security QRadar Technical Sales Foundations - Level 100 (credly.com/badges/281d2dd5-775a-4694-b186-36e92a3a96c5)

- Cybersecurity IT Fundamentals Specialization (credly.com/badges/f840b1fa-b088-4317-b5ef-f8667a70ab24)

- Cybersecurity Compliance Framework & System Administration (credly.com/badges/e9b3f24a-88ef-4c3e-b12d-6234585396f7)

- Cybersecurity Roles, Processes & Operating System Security (credly.com/badges/ded0b74d-7791-4968-a96c-e0da8e80b49e)

- Network Security & Database Vulnerabilities (www.credly.com/badges/3695dfb6-cd4b-4235-bd3d-2ad8ee189895)

- Introduction to Cybersecurity Tools & Cyber Attacks (credly.com/badges/fa475339-ef32-44c2-a7e5-9c138d5d9b8f

- Think Like a Hacker (credly.com/badges/44061d4b-6b59-49d7-8cb8-15e04a8235e7)

- **Certified Ethical Hacker v9**: ECC73758489141

EDUCATIONAL QUALIFICATIONS

Degree	University		Percentage	Grade
SSC	Maharashtra State Board		77.07%	Distinction
Diploma in Electronics &Telecomm.	Maharashtra State Board of Technical Education	1st Year	73.44%	Distinction
		2nd Year	70.34%	Distinction
		3rd Year	80%	Distinction
B.E. in Electronics &Telecomm.	Mumbai University	2nd Year	52%	Second Class
		3rd Year	53.17%	Second Class
		4th Year	62.71%	First Class