# CURRICULAM VITAE

## Atul thakre

**Mob:** 7019753218,9826457084
**E-mail:** atul10061993@gmail.com

## Career objective

To associate with an innovative and vibrant organization, allowing me to put my competencies to the best use, to add value to the organization and contribute to my overall growth as an individual.

## Academic Overview:

- Completed Bachelor of Engineering from sushila Devi Bansal College of Engineering mahow road, Indore affiliated to RGPV with specialization in Electronics and Communication (2012-2016) (CGPA-6.98).

## Professional Summary

- 5+ years of overall experience as Soc Analyst on Microsoft Azure Sentinel & ArcSight ESM.
- Real time monitoring of network security components and devices such as Firewall, Routers, System Application, Windows devices, UNIX devices, Web servers.
- Manage 24x7 operations at SOC, including event monitoring which includes incident detection, tracking and analyzing on real time basis, report generation.
- Create Log monitoring reports on daily, weekly, and monthly basis in order to maintain strict SLA adherence.
- Aggregating and Correlating the Logs and Configuring Reports, Queries, Rules, Filters, Dashboards, Real Time Alerts and Console Resource Operations.
- Provide 1st level of threat response for Security Event Management team at Security operation center (SOC).
- Motivated team player and can adapt and learn new technologies, tools, and applications.
- Good understanding of Azure sentinel and ArcSight architecture.
- Good Knowledge in network like TCP/UDP, OSI Model, three-way headshake, IP Address.
- Good Knowledge in network security devices like Firewall, IPS/IDS, Switch, Router,
- Good knowledge on DNS, DHCP and Active Directory.
- Good understanding of various SOC processes like monitoring, analysis and play books etc.

## IT Experience:

- Now working with L&T cloudfinity datacenter business from 20 March 2023 to till date as a assistant manager (SOC Monitoring).
- Complete working with NTT India Pvt Ltd**.** From 21 Feb 2022 to 20 Feb 2023 as a MS Engineer L1 (SOC).
- Complete Working with Unitel works wireless solutions Pvt Ltd. From 1 Aug 2019 to 20 Feb 2022 as a project coordinator (Network)

## Roles & Responsibilities:

- Deep dive analysis of triggered alerts using SIEM and other analysis tools like IP Void, Virus Total, MX Toolbox etc.
- Monitor events, log analysis, and Investigate incident a daily basis.
- Investigate Incidents using Channels/Dashboards/Events/Graphs/Annotations/Cases and Reports.
- Escalate issues as per the escalation matrix to the operation heads or senior authorities for faster and better resolution.
- Creating reports and monitoring dashboards in Sentinel.
- Participating in weekly SOC meetings to discuss about raised incidents.
- Creating the guest user access in the FortiGate firewall.
- Follow up with incident response team for remediation.
- Familiar with logger and command center for the Advance admin activity and license requirements.
- Hands on experience on the Incident Response activities like Malware analysis, Brute force analysis etc.
- Well-versed with complete event annotation, incident management, attack analysis.
- Perform Security SIEM Operational task - Analysis, Optimization, Filters, Active channels, Reports, Suggestion of fine tuning on existing rules.
- Drafting shift handovers.
- Worked in 24x7 Operational support.

## Technical Skills:

.

- SIEM Tools: Microsoft Azure Sentinel, ArcSight ESM, XSOAR.
- EDR: Crowd strike
- Firewall: Palo-Alto, FortiGate Firewall.
- Ticketing Tool: SNOW, BMC, ITSM.

## Personal details:

| | |
|---|---|
| Date of birth: | 10 Jun 1993 |
| Father's name: | Ramesh thakre |
| Mother's name: | khumeshwari thakre |
| Linguistic Abilities: | Hindi & English |

I hereby declare that the details furnished above are true and correct to the best of my knowledge.

(ATUL THAKRE)