**CURRICULAM VITAE**

**AMOL DUBEY**

**Mob:** 7879454513

**E-mail:** [amoldubey1995@gmail.com](mailto:amoldubey1995@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:** |

* B.COM form G.S. College Of Commerce Jabalpur with 70% in the year of 2016.

|  |
| --- |
| **Summary** |

* 3+ years of overall experience as Security Analyst on Arc sight 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.
* Install and maintain security infrastructure for new threats, Assess threats, risks, and vulnerabilities from emerging security issues.
* Aggregating and Correlating the Logs and Configuring Reports, Queries, Rules, Filters, Dashboards, Real Time Alerts and Console Resource Operations.
* Comprehensive Knowledge on Implementation of ESM Components (Connectors, Console). Good Knowledge in Implementation of Smart Connectors.
* Provide 1st level of threat response for Security Event Management team at Security Operations Center (SOC).
* Motivated team player and can adapt and learn new technologies, tools and applications.

|  |
| --- |
| **IT Experience:** |

Working as Security Analyst at ‘Robomoto technologies private limited’.

Position : Security Analyst

Period : August 2018 to till the date.

|  |
| --- |
| **ArcSight ESM Security Analyst(AESA) Key Responsibilities:** |

* Monitor events, Log analysis and Investigate incident a daily basis.
* Regular health checks monitoring, and reporting.
* 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.
* Having idea on Implementation of smart connectors.
* Acquired extensive hands-on experience in network engineering & troubleshooting.
* 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.
* Worked in 24x7 Operational support.

|  |
| --- |
| **Arcsight Technical Skills:** |

* End device integration with Arcsight. (Base lining, Logging, Communication)-Entry Level.
* Implementation of Custom Queries, Filters, Rules, Active Channels, Dash Boards.
* Troubleshoot and resolve issue of Log Stoppage of different devices.
* SIEM Tools: ArcSight ESM, Splunk.
* Cisco Cybersecurity Essentials Certificate and NSE 1 Certificate.
* Post Graduation Diploma In Computer Application.

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

(Amol Dubey)