RAMKUMARAMALRAJ   
**ramkumar33.ra@gmail.com · 380-269-9929** [**linkedin.com**](https://www.linkedin.com/in/ramkumar-amalraj) **·** [**Portfolio**](https://ramontheweb.github.io/portfolio/)

Experience  
**2022-2024  
Junior DevOps,** Taylor Software Systems

* Designed, install, configure and support internal and customer facing servers, network devices and firewalls.
* Automation of routine tasks building Python pipelines and Bash scripting to reduce error-rate and increase task efficiency.
* Development, deployment and monitoring of Pandas data pipelines and log parsing using regex, as well as grok patterns in Elastic environments.
* Maintenance of CI/CD pipelines using Jenkins and integration of Docker for application containerization, ensuring consistent deployments across any environment.
* Created documentation of processes and configurations to improve company knowledge base and ease-of-maintenance for continued development and usage after end of contract.

Education  
**2022-2024  
Bachelors of Information Sciences (Cyber Security),** Sheridan College

* Designed, deployed, and secured server environments using firewalls (Cisco ASA, pfSense), IDS/IPS (Snort), and SIEM tools (Wazuh).
* Visualizing information and concepts using technical reports & network diagrams to communicate, document and report findings.
* Analyzed network threats (malware, DDoS) and applied NIST CSF & MITRE ATT&CK frameworks for risk mitigation.
* Studied malware samples in C (Ghidra) to identify payload delivery mechanisms and persistence mechanisms (registry modifications, rootkits) in lab environments.
* Development of Python scripts for task automation. (Network scanning, Log analysis)

**2018-2021  
CST. Information Systems Analyst,** Sheridan College

* Diverse program involving working with many different frameworks, languages, and technologies with real time practice in different lab environments simulating real world scenarios.

Technical Skills, Certifications, Project

* **Languages**: Python, Bash, PL/SQL, PowerShell, UNIX Shell, C++.
* **Toolkit**: Docker, Wireshark, Metasploit, Snort, Ghidra,
* **Frameworks:** Elastic (ELK, Wazuh), MITRE ATT&CK,,.NET
* **Certifications:** CompTIA SEC+, A+. Network+, CISSP (Studying)
* **Online Projects:** [**leetcode**](https://leetcode.com/u/vahaes33/) **,** [**tryhackme**](https://tryhackme.com/p/ramkumar33.ra)**, github**