

Raaghav Devgon

Boston, MA | (857)919-7245 | devgon.r@northeastern.edu | Github:/raaghavd|

Linkedin: <https://www.linkedin.com/in/raaghav/>

Availability: Dec '21

EDUCATION

Northeastern University,

Khoury College of Computer and Information Science

Candidate for a Master of Science in Computer Science

Related Courses: Information Retrieval, Privacy Engineering, Software Vulnerabilities and Security

Boston, MA

Dec 2021

GPA: 3.89

DR. APJ Abdul Kalam Technical University

Bachelor of Technology in Computer Science Engineering

Related Courses: OOPs, Data Structures, Databases, Software Engineering, Cryptography

Jun 2017

TECHNICAL KNOWLEDGE

Languages: Java, C, C++, C#, Python, JavaScript.

Databases: MySQL, PostgreSQL.

Web: HTML, CSS, PHP, ReactJS.

Certifications: IBM Blockchain Essentials, IBM Cloud Essentials, Currently studying for CIPT.

Tools: ElasticSearch, ELK stack, QRADAR, Arcsight, vSphere, vRealize, Docker, Sci-kit learn, Git, Axonious, KnowBe4, JIRA, Falcon Sandbox, Phantom, Mimecast, Metasploit, Splunk, Darktrace, Demisto, Active Directory, Wireshark, Nmap, Nessus, Metasploit, BurpSuite, SQLMap, Hashcat.

Skills: Threat Modelling, OWASP Top 10, SAML, OAuth, NIST, ISO, PCI DSS, HIPAA, Penetration Testing.

WORK EXPERIENCE

Kolberg Kravis Roberts and Co .

Cybersecurity Analyst Co-op

New York City, NY

Jul 2020 - Jan 2020

- Investigated events and incidents using tools such as SIEM, E-mail security gateway and sandboxes to perform efficient event triage, incident response and closure.
- Developed and refined playbooks for automation in SOAR platforms, improved efficiency and throughput of analysis by 85%.
- Created SIEM alerts for suspicious processes based on Windows event logs, DNS, Firewall, MFA, AD etc., in support of event triage and threat hunting.
- Refined process of creation of service accounts by building a service management tool.
- Tuned threat detection process for Managed Security Service Provider improving accuracy of alerts by 94%.
- Conducted third party vendor assessments and reviewed SOC2 reports.

IBM

Security Consultant

Bangalore, India

Dec 2017 - Apr 2019

- Trained in SIEM and Endpoint security tools such as: QRADAR, Symantec Endpoint protection.
- Monitored security events from various SOC entry channels (Logs, Tickets) using LogInsight.
- Established daily security incident and vulnerability management processes, safeguarded corporate data and technology platform components from known threats.

PROJECTS

Differentially Private Recommendation System

May 2020 - Jun 2020

- Added laplace noise to dataset to strengthen anonymity of data whilst querying and generated a privacy preserving system.
- Tools used: MovieLens dataset, Python and Sci-Kit Learn.

Search Engine: Built with Elastic Search

Jan 2020 - Feb 2020

- Allowed users to perform topical search on indexed data.
- Indexed a total of 120,000 links in Elastic Search ranked using PageRank algorithm.

Plagiarism Detector: Source Code plagiarism detector

Oct 2019 - Nov 2019

- Implemented a unique hash algorithm based on AST in Java to calculate amount of plagiarism between two or more source codes.

RESEARCH

Analysis of Privacy Issues Related to Business Networking Services

June 2020 - Current

- Recipient of Northeastern University's "Pathway To PhD" grant, Mentored by Tamara Bonaci.
- Objective to research adversarial employer behaviour on professional social networks. The goals are to understand scope of nefarious employer behaviour on these networks; threat modelling of adversary and proposing changes to UX design of platform.

Analysis of encryption and lossless compression techniques for secure data transmission

Jan 2019

- Selected for publication in IEEE ICCS 2019 conference, Singapore; Co-author.