Aakash Prasad

Boston, MA | prasad.aa@northeastern.edu | (781) 708-6994 | Website: https://skyseccoder.github.io/ | LinkedIn

EDUCATION

NORTHEASTERN UNIVERSITY, Boston, MA
College of Computer and Information Science, **GPA: 3.75/4.0** Graduated Aug 2018
Master of Science in Information Assurance and Cybersecurity

VELLORE INSTITUTE OF TECHNOLOGY, Tamil Nadu, India
School of Information Technology and Engineering, **GPA: 3.75/4.0** Graduated May 2016
Bachelor of Technology in Information Technology

TECHNICAL KNOWLEDGE

Language:	**Python, Bash, Go, JavaScript**
Operating System:	Mac OS, Windows, Kali Linux, CentOS, Ubuntu
Tools:	Wireshark, Aircrack-ng, Burp Suite, Metasploit, Nessus, ProDiscover, SANS SIFT, Sleuth Kit, Autopsy, Xplico, SIEM, Threat Stack, Splunk
Cloud/DevOps technologies:	AWS(Lambda, EC2, S3, EKS, Guard Duty, etc.), Terraform, Docker, Kubernetes, Helm, Jenkins, RDS(MySQL, Microsoft SQL), Scalyr, Git, New Relic, Grafana, Octopus, Bamboo, Datadog, Vault, Rancher, Fleet, Kubernetes

WORK EXPERIENCE

DraftKings, Boston, MA Jul 2020 - Present
Site Reliability Engineer

- Responsible for maintaining, monitoring, scaling and the uptime of DraftKings's production infrastructure.
- Cut monthly infrastructure costs by 10% or millions, and put controls in place to prevent infrastructure over expenditure.
- Worked with teams to better understand requirements and implement optimal solutions for deploying and maintaining infrastructure on premise and the cloud.
- Architected and implemented scalable CI/CD pipelines to deploy code faster and securely to meet business deadlines.
- Architected, maintained and implemented complex Kubernetes workloads from scratch in all DK SDLC environments.
- Secured cloud and datacentre systems to ensure state and regulatory compliance.

Validity Inc., Boston, MA Apr 2019 – May 2020
Infrastructure Security Engineer

- Designed and implemented an AWS IAM strategy, across multiple AWS accounts for employees and service users.
- Implemented a centralized logging architecture for all company AWS accounts.
- Created and operated several tools in Golang and Python in order to monitor production infrastructure, locate potential security vulnerabilities, identify and inventory critical assets(in AWS).
- Identified and remediated several security issues in Jenkins, AWS, Kubernetes, GitHub, EC2, S3, etc.
- Responsible for the auditing and remediating security issues of databases(SQL), network, system, container infrastructure.
- Coordinated with several teams to prioritize, execute and fix several security vulnerabilities and implement best practices.
- Evangelized security and organisational best practices across various teams in the organization.

Threat Stack, Boston, MA Sept 2018 – Apr 2019
Security Analyst (SOC)

- Performed threat hunting in several customer environments in order to detect and prevent ongoing attacks.
- Monitored system and AWS based environments in order to prevent overprovisioning and minimising attack surfaces.
- Performed penetrations tests on servers in order to detect ongoing attacks, provide recommendations and remediations.
- Worked with product and DevOps teams in order to improve the Threat Stack platform.

CERTIFICATIONS

Amazon Web Services Security Specialty Feb 2020
Issued Feb 2020 . Expires Feb 2023 – Credential ID: YV2N6GT1NBQ41EW6