Omar **Chedid**

DevSecOps Engineer

(+1) 919-272-0294 | ochedid95@gmail.com | omarchedid.com/hire-me | omarchedid95 | omarchedid

Summary

I am a DevSecOps engineer located in the San Francisco bay area working at Cisco Systems - AppDynamics on securing cloud infrastructure. I'm currently on an H1B visa that is valid till 2022 and looking for new opportunities that can offer personal and professional growth.

Education

North Carolina State University

Raleigh, NC

Master of Science in Computer Science

2017 - 2018

.

American University of Beirut

Beirut, Lebanon

Bachelors of Engineering in Computer and Communications Engineering

2013 - 2017

Experience

AppDynamics

303 2nd Street, San Francisco, CA 94107

DevSecOps Engineer

Feb 2020 - Present

- Working with the techops and security teams on scanning, patching, and securing cloud infrastructure on **AWS**. We currently use Terraform, Ansible, Chef, and Jenkins to manage over 1,500 servers that span four global regions.
- Taking full ownership of developing an in-house vulnerability management system with **Node JS** (Express), **React JS**, and **SQL** to keep track of infrastructure vulnerabilities and 30 day SLA patch requirements. This was a full stack project (backend, frontend, containerization, infrastructure provisioning, and deployment) that I delivered in under two months. Read more about it here: https://omarchedid.com/projects/
- Used **Terraform**, **Ansible**, and **Jenkins** to spin up a scalable, reliable, and multi-region **Splunk** deployment on AWS. This project involved creating a cluster of indexers, heavy forwarders, VPC peers, and a cluster master.
- Worked extensively on reducing Splunk ingestion costs by automating AWS **ELB** access log ingestion from **S3** into Splunk on demand. This was done using Python and Jenkins.
- I'm an active member of the Cisco CATO (Cloud Authority To Operate) team which enforces SOC2 compliance requirements across the server farm.

Cisco Systems

3550 Cisco Way, San Jose, CA 95110

Software Security Engineer

December 2018 - Feb 2020

- Worked with a small team of 15 senior security engineers and architects on building the next generation cloud native firewall. The team functions like a startup and is extremely **agile**. Daily tasks include adding features to the control plane in **Golang**, writing build automation scripts with **Python** and **Jenkins**, and building system level test infrastructure using **Kubernetes** and **Ansible**. The development environment is completely containerized so I am constantly working with virtualization technologies such as **Docker** and **Vagrant**. This team uses **git** for version control.
- Worked on implementing high performance **GRPC** APIs using **protobuff** messaging for Go. Also worked on securing these APIs by setting up secure **TLS** channels using our internal **PKI** for certificate management.
- Joined the Snort3 **IDS/IPS** team for some time were I explored the Snort3 code base and got a chance to learn about the system architecture.
- Contributed to the ASA firewall source code in **C**. The features that I worked on were firewall clustering and high availability, GPRS tunneling, anti-replay, anti-spoofing, and location logging. This team uses **perforce** for version control.
- Did some hands on physical networking in the Cisco data center to bring up our **VmWare ESX** cluster. Gained experience setting up virtual machines on the cluster and networking virtual machines together to create a test bed. This is where I learned how to setup an **ACL** and **NAT** tunnels.
- Acted as the **scrum master** during the daily stand up meeting and have been practicing the agile methodology ever since I started working at Cisco.

Akamai Technologies

150 Broadway, Cambridge, MA 02142

Software Engineer

May 2018 - August 2018

- Worked with the network systems team on integrating the IP address management (IPAM) system with the router configuration manager (RCM) system. This involved the use of **Perl** and SQL scripting.
- Developed RESTful APIs in Python using the **Flask** framework that push and pull router **JSON** configuration files to and from Git repositories. Also wrote scripts that parse router configuration files and model configuration changes in a mysql database. After that, I created tests for the API resource in Python and used the mocking library to simulate back-end database interactions.
- Lastly, I developed Perl scripts that parse internet route registry (IRR) dumps and import internet routes into the IPAM database after verifying the validity of the routes.

North Carolina State University

1910 Entreprenur Drive, Raleigh, NC, 27606

Cybersecurity Researcher

September 2017 - December 2018

- What started as a grad school course project turned into three semesters worth of security research. Worked with Dr.Muhammad Shahzad on a paper called “Distributed Authentication Methods for ARP Cache Poisoning Mitigation”.