# RISHAB KHARIDHI

**Phone:** 650-336-5122 / 720-569-5152 **Email:** rishab.kharidhi@gmail.com **LinkedIn:** linkedin.com/rishab-kharidhi **GitHub:** rishabkharidhi

## WORK EXPERIENCE

**Security Engineer** Aug 2020 – Present

Amazon Web Services (AWS) – Security Hub New York, NY

- Designed, built and maintained security controls and frameworks utilizing Python, for the AWS Service Security Hub, adhering to industry standards such as AWS Best Practices, PCI DSS, CIS and NIST.
- Conducted thorough code reviews for controls developed to ensure compliance with industry standards.
- Provided technical support as On-Call to customers, collaborating with cross-functional teams to fix bugs.
- Contributed to the release of public-facing security controls for customer use, including the development of an internal tool using Python to automate the process for customer-facing documentation.

**Security Engineer** Aug 2020 – Present

Securonix Jersey City, NJ

- Spearheaded high-pressure POCs resulting in a 20% increase in team's revenue, by collaborating with cross-functional teams to create end-to-end MITRE ATT&CK compliant threat models and policies, ensuring customer satisfaction and auditing quality to maintain regulatory requirements, also performed initial event triage and threat hunting by adopting STRIDE to mitigate security risks.
- Improved time efficiency by 50% in preparation and maintenance of POCs by automating and scripting tools.
- Designed and set up 800+ use cases on average per POC to demonstrate anomalies such as beaconing, enumeration, insider threat, account misuse, credential sharing, endpoint malware, fraud, etc.

**Threat Research and Development Intern** Aug 2020 – Present

Webroot, An Open-text company Broomfield, CO

- Reverse engineered malware using static/dynamic analysis, developed modules for PE file disassembly, YARA scanning, and containerized dependencies to reduce effort by 30% to reproduce consistent scalable builds.

## PROJECTS

**Web Application Security and Development:** Independent Study

- Performed threat analysis of a lab-based web application and executed XSS, SQL injection, request forgery.
- Have been involved in CTFs and hacking challenges weekly on websites such as tryhackme (top 7% in world).

**Software Exploits, Anti-RE detection and Mitigation:** Nov 2019

- Analyzed windows and Linux applications to evaluate vulnerabilities and constructed scripts to exploit functions in C to perform overflow attacks. Used IDA & IDA Python to detect and mitigate anti-re techniques.

**Forensic Data Carver Tool:** Mar 2019

- Developed a Python tool to aid in forensic analysis to extract and recover files from within a filesystem hex dump. The tool implemented finite state machines and improved the efficiency of existing tools by 8%.

## EDUCATION

**Master of Science, Cybersecurity: University of Colorado Boulder, CO** GPA: 3.9/4.0 May 2020

Graduate Teaching Assistant – **Digital Forensics, Penetration Testing**, Recipient of **William E. Rapp Fellowship Award**

## TECHNICAL SKILLS

**Cryptography:** Symmetric and Asymmetric encryption, Digital Certificates, Hashing, PKI, Stream and Block Ciphers
Application Security: Threat Modelling, STRIDE, OWASP Top 10, NIST Framework, Mitre ATT&CK Framework
**Network Protocols:** TCP, IP, TLS, IPSec, DHCP, DNS, HTTPS, VPN, Firewalls, Snort
**Programming/Scripting Expertise:** Python, PHP, C, C++, SQL, HTML, x86, Java, Bash/Shell, PowerShell, Golang
**Tools:** IDA Pro, Windbg, Ollydbg, GDB, PPEE, Burpsuite, Metasploit, Sleuthkit, Docker, NMAP, Wireshark, Splunk
Domain Expertise and Coursework: Reverse Engineering, Privacy Analysis, Policy, Differential Privacy, K-Anonymity, Privacy Assessments, Secure Code Audit, Data masking, Data obfuscation
**AWS Services:** Security Hub, EC2, Lambda, Cloudformation, S3, Directory Services, EMR, EKS, Cloudwatch, IAM