RISHAB KHARIDHI

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

WORK EXPERIENCE

Security Engineer Apr 2022 – Present
Amazon Web Services (AWS) – Security Hub New York, NY

- Developed and maintained security controls using Python, creating backing AWS Config rules to evaluate various AWS services, in compliance with leading industry standards, such as AWS Best Practices, PCI DSS, CIS, NIST.
- Evaluated and tested the developed security controls and config rules by writing unit tests using MagicMock.
- 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 documentation, developing of an internal automation tool.
- Performed region testing of security controls utilizing CloudFormation to deploy AWS infrastructure,config rules.

Security Engineer Aug 2020 – April 2022
Securonix, SIEM & UEBA Jersey City, NJ

- Spearheaded high-pressure POCs resulting in a 20% increase in team's revenue, by creating end-to-end MITRE ATT&CK compliant threat models and policies, to ensure customer satisfaction and auditing quality to maintain regulatory requirements. Performed initial event triage and threat hunting by adopting STRIDE methodology.
- 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 May 2019 – Dec 2019
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.

Linux Systems Administration: Mar 2019 – Apr 2019

- Set up a corporate network for 20 employees on Linux machines, configuring DHCP, DNS, and web servers.

Forensic Data Carver Tool: Mar 2019

- Developed a Python tool to aid in forensic analysis to extract and recover files from within a filesystem dump.

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
AWS Services: Security Hub, EC2, Lambda, Cloudformation, S3, Directory Services, EMR, Cloudwatch, IAM, Config