

## Education

California Polytechnic State University (Cal Poly), San Luis Obispo (SLO)

B.S. Computer Science, concentrating in Security

Graduation: June 2021

## Work Experience

Software Development Engineer Intern (Security), *GoDaddy* (Remote) June 2020—Present

- Automated processes for on-demand analysis/reporting of CVE exploit exposure of potentially-affected machines within GoDaddy's infrastructure.
- Utilized Mitre ATT&CK's STIX implementation to relate techniques, tactics, and mitigations with relevant CVE exploits and their supporting classifications/weaknesses in Go.
- Created a Go library to retrieve detailed information for CVEs, CPEs, and CAPECs using APIs for NIST and CIRCL.
- Enriched IP and domain-related IOCs using Shodan data for internal team tools.

Junior Security Operations Center Analyst, *Cal Poly* (SLO) October—June 2020

- Triaged student, faculty, and staff-submitted phishing emails and suspicious user account network activity for blue-team tasks.
- Achieved proficiency in Splunk by creating alerts, advanced dashboards, and workflows and completed Splunk Fundamentals I.
- Automated a Python script to parse, enrich, and normalize email files and IOCs to streamline daily analysis processes.

Threat Research Intern, *BlackBerry Cylance Inc.* (Irvine, CA) June—September 2019

*Stuart McClure — CEO Executive Circle Summer Internship Program*

June—September 2018

- Developed an advanced automation framework to validate and test team-developed EDR rules against malicious and trusted binaries, and integrated it into the team's Jira workflow.
- Created an EDR rule validation tool using Python for team usage and to validate consumer submissions.
- Contributed towards mitigating the MITRE ATT&CK Framework and secured high-priority company deals with custom EDR rules.
- Learned advanced static and dynamic malware analysis skills and techniques and Metasploit hacking skills.
- Enriched malicious hashes with family classification data using VirusTotal and internal APIs.

## Skills

Security Automation	Splunk	Malware Analysis	x86 Reverse Engineering
Python	C	Go	Regex
REST APIs	Python Flask	Web Scraping	Metasploit
pfSense	VLANs	Firewall Administration	Computer Networking
BASH/ZSH	vim	git	L <sup>A</sup> T <sub>E</sub> X
VMware	Docker	systemd	

## Projects

White Hat Malware Lab

- Personally-developed lab environment for teaching static/dynamic malware analysis techniques to club members.
- Allows for club research on malware attacks, antivirus bypasses, reverse-engineering training, and Kali Linux/Metasploit ethical penetration-testing teaching and practice.
- Powered by VMware ESXI, Python Flask, pfSense, and CrowdStrike Hybrid Analysis.

## White Hat Cybersecurity Club (SLO)

- Malware Tech Team Lead – Project founder and leader of a 20+ member team. Fall 2019—Present
- SysAdmin – Administrator of lab server, networking, and custom CTF infrastructure. Spring 2019—Present
- Webmaster – Developer/Maintainer of club website (<https://thewhitehat.club>). Spring 2018—Spring 2019
- Gave technical talks on Virtualization Security, Malware Analysis, Web Server Security, Security Question Security.

## Relevant Coursework

Computer Security	Wireless Security	Programming Languages
Computer Networks	Systems Programming	Computer Architecture
Operating Systems	Intro to Computing with Security	Technical Writing