# David Huang

dshcodes@pm.me | dshphoto.me | github.com/dave-sh

## EDUCATION

**Georgia Institute of Technology**
*M.S. Cybersecurity* — *May 2027*

**University of Florida**
*B.S. Computer Science* — *Graduated*

**Certifications:** AWS Certified Solutions Architect – Associate, HackTheBox Certified Web Exploitation Specialist
**Publication:** Multi-beam Beamforming-based ML Algorithm to Optimize the Routing of Drone Swarms

## SKILLS

| | |
|---|---|
| **Languages:** | Python, Java, C/C++, JavaScript, Go |
| **Security Tools:** | Ghidra, IDA Pro, x64dbg, gdb, DynamoRIO, Yara, Splunk, Metasploit, Wireshark, BurpSuite, pwntools, MITRE ATT&CK, Snyk |
| **Tools:** | Git, Docker, Kubernetes, Linux, GitLab CI/CD, Rundeck, StackStorm, Azure SSO/RBAC |
| **AWS Services:** | EC2, RDS, S3, Lambda, SNS, SQS, Aurora, VPC Configuration |

## EXPERIENCE

**NVIDIA**
*Site Reliability Engineer Intern* — *Aug 2026 – Present*
- Built a Python CLI that manages ~900 servers through Rundeck, with JSON output for scripting, as a faster alternative to the web UI.
- Implemented Azure SSO login for the CLI in place of manual API key retrieval, tying every action to an individual user identity and making it auditable.
- Captured the production StackStorm server configuration and built a reproducible Docker image pipeline with GitLab CI/CD, replacing manual SSH-based config changes; migrated the deployment to Kubernetes.
- Modified open-source StackStorm to support Azure SSO, replacing a shared user account, and implemented RBAC for least-privilege access with actions attributable to individual users.

**Microsoft**
*Security Research Intern* — *May 2026 – Aug 2026*
- Built a sandboxed dynamic-instrumentation tool in C/C++ using DynamoRIO, automating runtime behavioral analysis of Go malware.
- Developed a binary-diffing tool to de-obfuscate Garble-protected Go binaries, recovering ~50% of statically linked libraries under default settings.
- Reverse engineered Go malware samples with IDA Pro and x64dbg; wrote technical reports that fed detection engineering and threat intelligence.

**New York Stock Exchange (Intercontinental Exchange)**
*Application Security Analyst* — *Dec 2025 – May 2026*
- Conducted penetration testing across web and internal applications using SAST, DAST, and SCA tooling; produced reports with proof-of-concepts, root cause analysis, and remediation guidance.
- Owned end-to-end management of the HackerOne bug bounty program, overseeing triage, researcher communication, and remediation tracking.

**Splunk (Cisco)**
*Software Engineer Intern* — *Jun 2025 – Aug 2025*
- Built Python and Go automation for incident response on infrastructure and application monitoring, including a Splunk dashboard with equivalent functionality at 99% lower data volume.
- Automated previously manual incident response playbooks by developing diagnostic tools, reducing mean time to resolution (MTTR) by 5–10 minutes per incident across 4 common alert types.

**Self-Employed (Contract)**
*Software Engineer* — *May 2024 – Jan 2025*
- Reviewed and improved the security and code quality of a PHP Laravel codebase and its documentation.
- Implemented an EC2 AMI-based restore process (1.5 hours faster per instance) and decoupled the application and database layers for security, stability, and scalability.