Truong Dinh

931-206-1129 | ddinh1@usf.edu | Tampa, FL
linkedin.com/in/tdinh123 | github.com/tdinh-dev-sec-scientist | truongd-portfolio.netlify.app

EDUCATION

University of South Florida Tampa, FL
Bachelor of Science in Cybersecurity | **GPA: 4.0/4.0** Expected May 2028
- **Coursework:** Network Security, Operating Systems, Cryptography, Penetration Testing, Advanced Database Systems, Data Structures

CERTIFICATIONS, COMPETITIONS & PROGRAMS

- **CompTIA Security+ (SY0-701)** (Oct 2026) | **Google Cybersecurity Professional Certificate** (Aug 2025)
- **HTB SOC Analyst Job-Role Path** (Oct 2026) | **Bellini Mentorship Program**, USF (inaugural cohort mentee)
- **HTB Certified Defensive Security Analyst (CDSA)**, intermediate level – 7-day practical exam and report taken Nov 2026, result pending
- **Dragos CTF 2026 (ICS/OT) – solo, perfect score** (28,600/28,600) among 1,000+ teams; 48-hour forensics incl. Modbus/BACnet PCAPs

TECHNICAL SKILLS

Cloud & Security Engineering: AWS (IAM, S3, CloudTrail), Boto3, Terraform, CIS Benchmarks, least-privilege IAM, threat modeling
DevSecOps & Supply Chain: GitHub Actions, Docker, Checkov, OPA/Rego (Terraform, Kubernetes), Syft/Grype (SBOM), Cosign, pytest
Detection & SOC: Wazuh (SIEM), Splunk (SPL), Suricata IDS, Sysmon, Windows Event Logs, MITRE ATT&CK, incident response
Systems & Networking: Active Directory, Linux, OPNsense, VMware; TCP/IP, IPv6, DNS, DPI, Wireshark, Scapy, Nmap
Languages & Data: Python, Bash, PowerShell, SQL, C, Java; pandas, scikit-learn, TensorFlow

CYBERSECURITY PROJECTS

NetWatch SOC – Network Detection & Response Platform | *Python, PostgreSQL, Flask, Docker, Suricata, Splunk* May 2025 – Present
- Detected **6/6 held-out real attacks vs Suricata's 3/6** (ET Open rules; 6 attacks, 82 host-hours) at 1.0 vs 26.7 false alerts/host-hour.
- Engineered a Python IDS: byte-signature DPI (21 protocols), **18 detectors** across 16 MITRE ATT&CK techniques, **392 tests** in CI.
- Replayed 31M real packets (CSE-CIC-IDS2018); fixed 5 detection-logic bugs (no threshold tuning), cutting false alerts **375 to 1.1 per host-hour**.
- Correlated alerts into incidents (662 to 167, **75% reduction**); wrote a Splunk HEC forwarder with a dashboard and 5 scheduled alerts.

Vorrin – AWS Security Auditing & Guardrails Platform | *Python, Boto3, Terraform, Checkov, OPA/Rego, GitHub Actions* Dec 2025 – Present
- Built a read-only AWS misconfiguration auditor (Python, Boto3): 14 checks (11 CIS v3.0.0-mapped) across IAM, S3, and CloudTrail; detected **25/25 labeled misconfigurations** with 0 unexpected findings on 98 fixture cases.
- Enforced least privilege in code: a runtime guard blocks any AWS API call outside a declared read-only allowlist; the scanner's IAM policy is generated from that allowlist and CI fails on drift.
- Shift-left guardrails: Checkov, OPA/Rego, Syft/Grype SBOM vulnerability gating, Cosign signing; **1,456 tests**, 86% branch coverage.

Wazuh Detection Engineering Lab | *Wazuh, Sysmon, Active Directory, OPNsense, Suricata, Atomic Red Team* Aug 2026 – Present
- Built a segmented 5-VM home SOC (OPNsense/Suricata, Server 2025 DC, Win 11, Wazuh, Kali) with Sysmon and 4688/4104 logging via GPO.
- Emulated 15 attacks mapped to MITRE ATT&CK (Atomic Red Team, Nmap, SMB brute force); wrote **23 custom rules** and a Suricata decoder, closing **11 gaps** where default rules missed, mislabeled, or under-rated activity.
- Gated rules behind **78 engine test cases** (22 on real events) in Wazuh 4.14.8 on every push; boundary-tested thresholds and renamed binaries.
- Wrote 4 alert investigation cases (timeline, disposition, impact, remediation) in the style of a SOC analyst.

BOTSv3 Incident Response Investigation | *Splunk, SPL, Sysmon, AWS CloudTrail* Aug 2026 – Sep 2026
- Traced a PowerShell Empire intrusion (UAC bypass, backdoor admin, HTTPS C2) and S3 ACL changes across 2.8M Boss of the SOC v3 events.
- Extracted **8 IOCs**, mapped **13 ATT&CK techniques**, and wrote **5 detection queries** from the confirmed findings.

RESEARCH EXPERIENCE

Undergraduate Security Researcher – "The Invisible Tunnel" Dec 2025 – Aug 2026
IPv6 Covert Channel Detection | *Python, Scapy, scikit-learn, TensorFlow* | Advisor: Dr. James Church Austin Peay State University
- Built a PoC IPv6 C2 channel (Python, Scapy) in Destination Options PadN that evaded BPF, Snort, and DPI in a testbed (CVE-2024-38063).
- Wrote a stateless RFC 8200 rule with **0 false positives on 1M real MAWI IPv6 packets**; showed adaptive mimicry evades aggregate detection.
- **Authored a preprint** (Zenodo, doi.org/10.5281/zenodo.23029268); **2nd Place, STEM**, APSU Research Symposium; TN Posters at the Capitol.

EXPERIENCE

Computer Science Teaching Assistant Jan 2026 – May 2026
Austin Peay State University, CS & IT Department Clarksville, TN
- Diagnosed **200+ Java defects** for 30+ students in 2 hours/week of office hours, coaching debugging and core OOP/data-structure concepts.
- Graded assignments and labs, ran review sessions, and wrote study materials for an intro programming/OOP/data-structures course.

Peer Leader, Honors Program Jul 2025 – Dec 2025
Austin Peay State University Clarksville, TN
- Led **15 course sessions** for a 30-student Honors cohort as student-faculty liaison; published **16 weekly cybersecurity-awareness posts**.
- Mentored all 30 students one-on-one as their go-to contact for support and growth; coordinated with the professor on course delivery.