# MATTHEW FONGER

Ellijay, GA (Open to Relocation) • (706) 889-3677 • fongerm05@gmail.com • linkedin.com/in/matthew-fonger

## SUMMARY

Cybersecurity analyst with hands-on experience in SOC monitoring, alert triage, malware analysis, and vulnerability management across multiple client environments. Security+ certified (DoD 8570/8140 IAT Level II), CySA+ certified (satisfies DoD 8140 CSSP-Analyst). BS in Cybersecurity; MS in progress at Georgia Tech. U.S. citizen, eligible for a Secret clearance, open to relocation.

## CERTIFICATIONS & CLEARANCE

- CompTIA Security+ (CE) — meets DoD 8570.01 / 8140 IAT Level II baseline requirement
- CompTIA CySA+ — meets DoD 8140 CSSP-Analyst baseline
- Clearance: U.S. citizen; eligible to obtain and maintain a Secret clearance
- Member, OWASP

## PROFESSIONAL EXPERIENCE

**Cybersecurity Engineer | GA Cyber Defense — Georgia** **Feb 2026 – Present**

Managed security services provider delivering SOC monitoring, incident response, and vulnerability management to 20+ client organizations.

- Monitor and triage security alerts across 20+ client environments using Cynet, Datto EDR, RocketCyber, and VSA X, investigating approximately 500+ alerts per week and escalating confirmed incidents with documented findings.
- Analyze suspicious file hashes and IP addresses using tools like VirusTotal, AbuseIPDB, IPQS, and Talos and deliver written analysis to client stakeholders.
- Perform forensic imaging and disk analysis with Autopsy to support incident investigations, reconstruct attack timelines from system artifacts and log data.
- Run recurring vulnerability scans with ConnectSecure across client networks, prioritizing findings by severity and tracking remediations to closure.
- Deploy, configure, and tune endpoint detection rules across client environments, validating agent coverage and reducing false-positive alert volume.

**Cybersecurity Intern | Shiloh — Georgia** **Nov 2024 – Mar 2025**

- Audited web-based services against established security standards, identifying and documenting 50+ vulnerabilities with prioritized remediation recommendations.
- Deployed security audit tooling to assess service configurations, implemented approved fixes with the engineering team, and re-tested to verify remediation.
- Hardened a production Linux VPS through configuration changes and access control tightening, closing identified attack surface.
- Evaluated company systems based on ISO 27001 and proposed changes to aid in compliance efforts.

**Digital Manager | 4thSoilVentures — Georgia** **May 2024 – Mar 2025**

- Provided technical support and troubleshooting for online platforms and end users; managed digital content operations and research.

## SECURITY PROJECTS & LABS

- SOC Investigation Simulations (LetsDefend and TryHackMe): Completed 20+ end-to-end investigations covering alert triage, log analysis, phishing analysis, and incident response, documenting each in ticket format consistent with SOC escalation workflow.
- Offensive & Defensive Labs (TryHackMe and LU): Completed 150+ rooms spanning network security, penetration testing, Windows and Linux forensics, and threat detection.
- Virtualized Security Lab: Built and maintain a multi-VM lab for exploit testing, malware detonation and analysis, and vulnerability assessment using Metasploit, Nmap, Burp Suite, and Wireshark; map observed techniques to MITRE ATT&CK.

## TECHNICAL SKILLS

**SIEM & EDR:** Splunk, Datto EDR, Cynet, RocketCyber, VSA X, Microsoft Defender

**Detection & Analysis:** Alert triage and validation, log analysis, IOC identification, network traffic analysis (Wireshark, TCP/IP), malware analysis (x64dbg), digital forensics (Autopsy), detection tuning

**Vulnerability Management:** Nessus, ConnectSecure, Nmap, Metasploit, Burp Suite

**Cloud & Frameworks:** Microsoft Azure, MITRE ATT&CK, Cyber Kill Chain, ISO 27001, CIS Controls, NIST CSF / 800-53

**Scripting & Languages:** Python, SQL, C++, HTML, Powershell

**Operating Systems:** Windows, Linux, macOS

## EDUCATION

**Georgia Institute of Technology** — Master of Science, Cybersecurity | Atlanta, GA Expected May 2027

**Liberty University** — Bachelor of Science, Computer Science (Cybersecurity) | Lynchburg, VA August 2025 | GPA 3.61