EXPERIENCE

Dataprise Remote
Cybersecurity Engineer (DFIR) Jan 2025 - Present

- Contribute to ransomware incidents by spinning up secure jump boxes, isolating systems, performing forensics, rebuilding and decrypting servers, and applying hardening controls.
- Monitor thousands of endpoints with CrowdStrike Falcon & SentinelOne, triaging anomalies in real time and driving rapid remediation.
- Deploy MFA enterprise-wide and improve SonicWall and FortiGate configurations after incidents, tightening network and identity defenses.
- Perform disk & memory forensics on compromised hosts, delivering evidence that guides remediation actions and future preventive strategy.

MIT Lincoln Lab Lexington, MA
Cyber Forensics Analyst (Co-op) Feb 2024 - Aug 2024

- Conduct forensic imaging, remote data collection, and analysis on over 200+ lab devices to support investigations.
- Insider Threat Program: Continuously monitor activities of employees and conduct detailed 90-day reviews via Splunk for departing employees, enhancing security and compliance.
- Research and compile Cyber Threat Analysis reports for executive leadership, highlighting key vulnerabilities and risks specific to the industry.

Minnesota Computer System, Inc. St. Cloud, MN
Jr. System Administrator Apr 2022 - Jan 2024

- Accomplished a 15% reduction in system downtime as measured by incident tracking, by diagnosing and resolving complex hardware and software issues.
- Configured and managed Active Directory and Office 365, including provisioning 100+ user accounts and implementing role-based access controls.
- Mitigated malware and other security threats by rapidly implementing containment & cleanup procedures.

Trace Labs Remote
Volunteer OSINT Analyst Mar 2020 - May 2020

- Utilized advanced OSINT tools to gather critical intelligence on real-world missing persons cases.
- Demonstrated the ability to work independently with minimal oversight and direction.

EDUCATION

Master of Science in Cybersecurity New York, NY
New York University Sep 2025 - May 2027

SKILLS & CERTIFICATIONS

Languages: Python, JavaScript, Bash, PowerShell, C/C++
Technologies: Crowdstrike, SentinelOne, Splunk, Pentesting tools, Cellebrite, EnCase, FTK, Axiom, MacQuisition/Digital Collector, Paladin, Oxygen, ServiceNow,Elasticsearch, ConnectWise, Binalyze
CompTIA Security+