Walter Singleton

LinkedIn | 917-###-#### | waltersingleton.com | waltersingletonnyc@gmail.com | GitHub

Skills

- Wireshark | Nmap | KnowBe4 | FortiGate | Splunk | Microsoft Defender XDR | Alert Logic | Cortex XSIAM | CrowdStrike | Wiz
- Windows | macOS | Linux (Ubuntu/Kali) | Active Directory | EntraID | Google Workspace | Jamf | ServiceNow | Office 365 Suite
- Vulnerability Management | SIEM | EDR | MFA | IAM | Phishing Simulation | Firewall Rules | Threat Detection & Response

Experience

Cybersecurity Analyst — **The Home Depot** — *New York, NY, USA* — **9/2025 - Current**

- Investigated and resolved high-volume security alerts across North America using Palo Alto Cortex XSIAM improving response efficiency and supporting enterprise-scale incident detection for 500,000+ endpoints.
- Triaged the cybersecurity mailbox, identifying phishing and other malicious activity for escalation and remediation for 600,000+ associates
- Designed and tested Large Language Model (LLM) use cases to enhance alert analysis, IOC research, and file investigations.
- Built and optimized XQL queries to extract and correlate data from XSIAM datasets, enabling faster investigations for security incidents.

Information Security Analyst, Intern — **SUNY** — *Cobleskill, NY, USA* — **8/2024 - 06/2025**

- Improved network security by configuring firewall rules with FortiClient and Microsoft Defender, cutting unauthorized access by 40%
- Automated firewall address inputs with Python/PowerShell scripts, reducing manual effort by 50%.
- Enhanced cloud security by managing and supporting cloud-based applications (Azure), resulting in a 20% reduction in security incidents through proactive monitoring.
- Mitigated 100% of high-risk vulnerabilities in Active Directory and cloud using threat scanning and remediation.
- Monitored user behavior to detect risks, investigating and mitigating phishing and scam threats via mailbox quarantines.
- Led phishing simulations for 1200 users, lowering click rates by 25% and boosting awareness.

Information Technology Analyst, Intern — **Ford Foundation** — *New York, NY, USA* — **6/2024 - 08/2024**

- Streamlined IT operations by creating Standard Operating Procedures (SOPs) for future interns, increasing onboarding efficiency by 30%.
- Enhanced network infrastructure stability by troubleshooting and resolving connectivity issues, reducing downtime by 10%.
- Managed MDM (JamF) for secure access to mobile devices.
- Provided IT support in analytics, programming (Python), and data management, allowing an increase in administrative task performance.
- Managed A/V for 500+ events annually, preventing technical issues during high-profile meetings.

Tech Center Assistant — **Cobleskill Technology Services** — *Cobleskill, NY, USA* — **8/2021 - 05/2024**

- Resolved 100+ hardware and software issues per semester for students and faculty, improving satisfaction and device reliability.
- Improved IT ticket response by 15% through efficient request handling using Active Directory and TeamDynamix.
- Enhanced connectivity for 200+ users per semester by diagnosing and resolving Wi-Fi and system configuration issues.
- Increased faculty productivity by resolving application and driver issues across Windows and Mac platforms.

Education

Bachelor of Technology — **SUNY Cobleskill** — *Cobleskill, NY, USA* — **8/2021 - 12/2024**

- Major in Cybersecurity *(While completed Associates in Computer Information Systems)* ***3.8 GPA***

Projects

- **Password Generator:** Creator of Unique Password Generator using Diceware. Link to Website

Mentorship

- **Cybersecurity Club Vice President:** Responsible for mentoring and giving career advice to CS/Cyber students. Hosted internal Hackathons & CTF events.
- **Cybersecurity Tutor:** Automation Programming | Incident Response Methodologies | Career Advice | Professional Portfolio

Others

- **CompTIA Security+**: Certification that certifies user has knowledge and skills necessary to perform core security functions required of any cybersecurity role **(01/2025)**