Samuel Graziano

samgraziano2002@gmail.com | 703-568-7424 | www.linkedin.com/in/Linked-in-SHG

PROFESSIONAL SKILLS

Operating Systems: Linux (Ubuntu, Debian, Kali), Windows Client, Windows Server, macOS, Cisco IOS
Languages and Tools: Python, KQL, PowerShell, Linux CLI, Splunk, Wireshark, PfSense, Suricata, Snort, YARA, Volatility (dlllist, malfind), Microsoft Defender, Autopsy, FTK Forensics Toolkit, FTK Imager, Cloud Platforms (Azure, AWS), Shodan, Cisco IOS, Switch Security, Diagnostics & Troubleshooting

EDUCATION

Old Dominion University **GPA: 3.86**
Cybersecurity, B.S. **08/2026**
Relevant Coursework includes: Cyber-Infrastructure & Technology, Computer Networking, Microsoft Security, Cloud Security, Linux Security, Network Security, Python Programming

Northern Virginia Community College **GPA: 3.5**
Cybersecurity, A.A.S. (Cum Laude) **05/2025**

Old Dominion University
Cybersecurity Certificate **03/2023**

PROFESSIONAL EXPERIENCE

Arcova **Tysons, Virginia**
Advanced Services Intern **06/2026 — Present**

- Used EasyDMARC, openSquat, and Gobuster to conduct an external reconnaissance assessment of internet-facing assets, identifying potential security weaknesses from an attacker's perspective.
- Utilized breach references, known domain-squatting risks, and Shodan intelligence to analyze external attack-surface data across DNS/DNSSEC configurations, exposed services, subdomains, login portals, technology stacks, and cloud assets; documented findings for validation and reporting.
- Supported an authorized purple team engagement by executing controlled adversary techniques aligned with MITRE ATT&CK.
- Evaluated security visibility and detection capabilities by simulating account and group discovery, RDP activity, policy and registry manipulation, external tool transfer, and credential-access techniques.
- Developed five hypothesis-driven threat hunts focused on post-compromise identity activity.
- Created and validated reusable Sigma and KQL detection queries to distinguish legitimate administrative behavior from potential privilege escalation and lateral movement.
- Identified unusual activity involving Windows utilities and recommended access reviews, visibility improvements, and continued monitoring based on least-privilege principles.
- Presented threat-hunting findings to security stakeholders; included documented investigation results, visibility gaps, and actionable detection and prevention recommendations.

Golfdom **Tysons, Virginia**
Sales and Service Associate **10/2023 — Present**
As a retail sales cashier, provides customers prompt and courteous checkout experience. Collaborates with teammates, regularly offers suggestions to improve retail operations, demonstrates excellent customer service and consistently receives positive feedback from both customers and managers.

Great American Restaurants **Fairfax, Virginia**
Server **03/2021 — 04/2022**
Main duties included familiarizing guests with daily specials, accurately taking food and beverage orders, properly timing multi-course meals, and fulfilling miscellaneous guest requests. Demonstrated a strong work ethic while providing exceptional customer service.