

# Selwin George Murzello

155 Callodine Ave, Buffalo, NY, 14226

📞 716-228-7487 ✉ [selwinge@buffalo.edu](mailto:selwinge@buffalo.edu) [in linkedin.com/in/selwin-murzello](https://www.linkedin.com/in/selwin-murzello)

## Technical Skills

---

**Security Skills/Frameworks:** Web Application & Network Penetration testing, Cloud Security Audit, Threat Modelling, Infrastructure security Audit, Secure Configuration review, SIEM-Security information and event management, Security Architecture, NIST, SOC2, PCI-DSS

**Tools:** Wireshark, Metasploit, Nmap, Burp Suite, Snort, Splunk, Nessus

**Languages:** Python, Java, C, C++, HTML/CSS, SQL, Bash/Shell Scripting

## Education

---

**University at Buffalo, The State University of New York**

**August 2023 – December 2024**

*Master of Science: Engineering Science (Cyber Security)*

*Buffalo, New York*

**University of Mumbai**

**June 2019 – April 2022**

*Bachelor of Science: Information Technology*

*Mumbai, India*

## Experience

---

**Vice President Cyber, CyberSmithSecure Pvt Ltd**

**June 2022 – January 2023**

*Mumbai, India*

- Led high-impact projects involving SOC 2 and NIST frameworks, significantly advancing the company's security posture and compliance.
- Directed enterprise-level vulnerability assessments and penetration testing, driving improvements in network and application security.
- Played a key role in vendor selection processes for Zero Trust implementations, influencing major strategic decisions regarding cybersecurity technologies.

**Business Executive, CyberSmithSecure Pvt Ltd**

**October 2020 – May 2022**

*Mumbai, India*

- Managed and innovated cloud security auditing on platforms including AWS, ensuring robust security configurations and compliance with best practices.
- Collaborated closely with IT and strategy teams to align cybersecurity measures with organizational objectives and technological advancements.

**Cyber Security Intern, CyberSmithSecure Pvt Ltd**

**September 2019 – September 2020**

*Mumbai, India*

- Developed foundational cybersecurity skills, focusing on modern technologies and techniques such as Vulnerability Assessment and Penetration Testing, which prepared me for advanced roles in cybersecurity architecture.

## Projects

---

**Splunk Data Analysis for Cybersecurity Enhancement** | *Splunk, firewall logs, system event logs*

**April 2024**

- Integrated various datasets to create a comprehensive view of the organization's security landscape.
- Improved risk mitigation by providing actionable insights and recommendations based on data analysis.
- Reduced incident response time by 30% through automated alerting and streamlined investigation processes.

**Digital Forensics Traffic Flow Evaluation** | *Wireshark, NetworkMiner*

**March 2024**

- Utilized Wireshark for real-time and offline packet capture, decoding various network protocols to inspect content, headers, and metadata. Conducted detailed protocol analysis to identify deviations from expected norms, helping in detecting misuse.
- Identified and leveraged NetworkMiner to extract files, metadata, and host information from captured network traffic. Traffic flow visualization to uncover malicious activities and trace attacker movements.

**Security Hardening and Incident Response** | *VMware vSphere, pfSense, MariaDB, Wireshark, Nmap* **December 2023**

- Demonstrated exceptional proficiency in incident response, swiftly resolving cybersecurity incidents to minimize impact. Implemented stringent security measures to harden systems, reducing vulnerabilities by 35%.
- Ensured full compliance with the 18 CIS Critical Security Controls, showcasing a thorough understanding of industry-standard security practices.

## Certifications / Achievements

---

- Certificate of Cloud Security Knowledge (CCSK), Cloud Security Alliance (CSA).
- Managed executive board and ran weekly meetings to oversee the progress of Managed Security Services.
- Represented SUNY Buffalo and secured a top-10 ranking in a defensive security competition, effectively defending against real-world cyber attacks and completing various tasks to enhance essential cybersecurity skills.