

JOHN SOMANZA

818-746-0972 | Johnbsomanza@gmail.com

johnsomanza.com | linkedin.com/in/john-somanza | github.com/JohnSomanza | youtube.com/@JohnBSomanza

EDUCATION

Bachelors of Science, Cybersecurity and Information Assurance

Western Governors University, 2025 (Expected)

CERTIFICATIONS

CompTIA Security+, CompTIA Network+, CompTIA A+, Google Cybersecurity Specialization, ISC2 CC, Cybersecurity Analyst (LeveldCareers), Google IT Support Specialization, Qualys VMDR

PROJECTS

Project: Implementing a SOC and Honeynet in Azure

Source: github.com/JohnSomanza/Cloud-SOC-Honeynet

Platforms and Technology Used: Azure Virtual Machines, Microsoft Sentinel (SIEM), Log Analytics

Project: Developing a Help Desk Ticketing System with osTicket

Source: github.com/JohnSomanza/osTicket-Prereqs

Platforms and Technology Used: osTicket, Azure Virtual Machines

Project: Demonstrating a Vulnerability Management Lifecycle in Azure

Source: github.com/JohnSomanza/Qualys-Vulnerability-Management

Platforms and Technology Used: Qualys, Microsoft Azure

Project: Securing RDP Using Duo MFA

Source: github.com/JohnSomanza/Securing-RDP-With-MFA

Platforms and Technology Used: Microsoft Azure (Windows Server 2019 Virtual Machine), Remote Desktop Protocol (RDP), Cisco Duo Security RDP

Project: Running Active Directory on VirtualBox

Source: github.com/JohnSomanza/Active-Directory-On-VirtualBox

Platforms and Technology Used: Active Directory, VirtualBox, Powershell

Commonwealth Bank Introduction to Cybersecurity Job Simulation on Forage - August 2024

- Completed a job simulation involving the role of a cybersecurity generalist, specializing in fraud detection and prevention for Commonwealth Bank's Cybersecurity team
- Developed skills in building data visualization dashboards using Splunk to uncover patterns and insights in historical customer data, aiding in fraud detection
- Demonstrated the ability to respond effectively to cybersecurity incidents, including notifying relevant teams, collecting information, containing and stopping attacks, and aiding in recovery efforts
- Enhanced security awareness expertise by designing infographics promoting best practices for secure password management, following Australian Cybersecurity Centre advice
- Acquired practical experience in penetration testing, assessing the security of web applications, identifying vulnerabilities, and providing recommendations for remediation to bolster cybersecurity defenses

EXPERIENCE

Company: Log(N) Pacific

August 2024 - Present

Title: Cyber Security Support Technician (Intern)

- Implement secure cloud configurations using Azure Private Link, Network Security Groups, Microsoft Defender for Cloud, and Azure Regulatory Compliance for NIST 800-53, PCI DSS, and HIPAA/HITRUST, resulting in a **97.5%** reduction in security incidents over the same time interval
- Automated Log Analytics Workspace and Microsoft Sentinel integration using Python/KQL, leading to the development of 10 advanced SIEM dashboards and workbooks, enhancing real-time threat detection and response efficiency
- Troubleshoot and support Microsoft Azure services, including Microsoft Sentinel (SIEM), Virtual Machines, Azure Monitor, and Azure Active Directory

Company: PCI Consultants Inc.

Jan 2024 - Feb 2024

Title: Sr. Data Entry Clerk

- Critical role in inputting sensitive information with precision and confidentiality
- Proficient in maintaining data integrity and accuracy, while also adept at identifying patterns and anomalies within datasets was another responsibility
- Possess strong analytical skills and attention to detail, crucial for detecting potential security breaches or irregularities in data

SKILLS AND TECHNOLOGIES

Software: Microsoft Azure (Azure Sentinel, Entra ID), Nessus, Duo, VirtualBox, Qualys, Splunk Enterprise, osTicket

Areas of Expertise: Active Directory, SIEM, Incident Response, Identity and Access Management, NIST 800-53, Network Security Groups, Firewalls, Access Control Lists (ACLs), Virtual Machines, Virtual Networks, Cloud Computing, Windows 10/11, Remote Desktop Protocol (RDP), Multi-Factor Authentication (MFA), VMDR