Justin Goncalves

IT System Administrator

: **857-407-9412**
: **justingoncalves34@gmail.com**
: **Boston, MA**
: **https://www.linkedin.com/in/justingoncalves/**
: **https://justingoncalves34.github.io/Cybersecurity_Journey/**

For a detailed overview of my background, cybersecurity projects, certifications, and skills, please visit my GitHub portfolio

Projects, Activities, and Virtual Internships

Virtual SOC Environment Project (September - October 2024)
- Established a **Virtual Security Operations Center (SOC)** using **Microsoft Azure** and **Sentinel**, with real-time monitoring and incident response.
- Monitored over ***7.6 million events*** and nearly ***6,000 alerts***, optimizing threat detection and incident management through custom alert rules.
- Analyzed attack patterns and adjusted incident response strategies to enhance the efficiency of monitoring processes to reduce false alerts.

Telstra Cybersecurity Virtual Experience Program (September 2024)
- Simulated work experience as a Cybersecurity Analyst and Engineer on Telstra's ***Security Operations Center (SOC)*** Team.
- Managed the incident response lifecycle, including triaging malware attacks, and documenting postmortem reports to enhance response strategies.
- Engineered and implemented a firewall using a custom ***Python*** script to block malicious traffic.

Commonwealth Bank Intro to Cybersecurity Program (August 2024)
- Served as a Cybersecurity Generalist on the Commonwealth Bank Fraud Detection and Response team.
- Analyzed and visualized data using ***Splunk*** to identify fraud patterns.
- Managed a phishing and malware incident using the Incident Response Lifecycle, and authored a detailed incident report.
- Conducted penetration testing and recommended remediation strategies.

PwC Switzerland Cybersecurity Job Simulation Program (August 2024)
- Worked as a Cybersecurity Analyst on PwC's Digital Intelligence Team.
- Conducted risk assessments and developed layered security strategies.
- Wrote reports on network segmentation and firewall configurations, and delivered presentations on risk management strategies to stakeholders while recommending network security improvements.

InfoSec Data Handling Security Assessment Project
- Analyzed data-handling procedures for confidentiality, integrity, and availability in compliance with ***NIST SP 800-53*** Guidelines.
- Recommended security controls, encryption protocols, and access authorization measures to improve secure data handling.

Work Experience

Operations Manager/IT System Administrator
Digit Web Solutions - Remote | (Dec 2023 - Present)
- Led a team of developers and engineers to deliver custom web solutions for clients, optimized workflows for operational efficiency, and ensured client satisfaction.
- Managed IT operations, including system administration, technical support, web hosting, network security, and incident response.

Freelance Web Developer
Remote | (April 2021 - Dec 2023)
- Developed secure, responsive websites using HTML, CSS, JavaScript, and frameworks like React, with a focus on performance and cross-browser compatibility.
- Implemented security features, including HTTPS, SSL certificates, and secure payment gateways, while optimizing site performance and SEO.

Certifications

- **CompTIA Security+**, (2024)
- **ISC2 Certified in Cybersecurity,** (2024)
- **Google Cybersecurity Professional**, (2024)
- **Qualys Vulnerability Management Detection and Response (VMDR)**, (2024)
- **Qualys Cybersecurity Asset Management (CSAM)** (2024)
- **Qualys Vulnerability Management Scanning (VMS)** (2024)
- **U.S. Department of Homeland Security National Incident Management System (NIMS)**
  - IS-100.C, IS-200.C, IS-700.B, IS-800.D, IS-230.E, IS-860.C, IS-906, IS-915, IS-916, IS-1300, IS-2500

Skills

Frameworks
NIST CSF (SP 800-53, 800-61, 800-171) | OWASP
CIS Controls | PCI DSS | HIPAA | GDPR | NIMS
SOC 1/SOC 2 | ISO/IEC 27001 | MITRE ATT&CK

Tools/Technologies
Splunk | Qualys | Wireshark | Burp Suite | Metasploit
TCPDump | Chronicle | Azure + Sentinel

Security Operations & Monitoring
SIEM Tools | Threat Hunting | Log Analysis
Intrusion Detection/Prevention Systems (IDS, IPS)

Core Competencies
Incident Detection and Response | Cryptology
Vulnerability Management | Risk Assessment |
Network Security | Identity and Access Management

Programming/Scripting
Python | SQL | Bash/Shell Scripting | HTML 5 | CSS

Education

University of Massachusetts - Dartmouth, MA
Finance Major | (2019-2020, (2022-2023)
Relevant Coursework: Business Statistics, Financial Modeling, Operations Management, Risk Management, Project Management

Boston Latin School - Boston, MA
High School Diploma (2019)
#1 Ranked high school in Massachusetts at the time of my graduation.