Justin Goncalves

Boston, MA (Willing to Relocate/Travel)
(857) 407-9412
justingoncalves34@gmail.com

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

EXECUTIVE SUMMARY:

Certified cybersecurity professional with expertise in vulnerability management, incident response, and SIEM tools. Proven success in safeguarding assets, optimizing IT systems, and delivering secure, scalable solutions. Recently accepted into the SANS Technology Institute's Cyber Immersion Academy, to further my education and advance my skills.

CERTIFICATIONS:

- **CompTIA Security+ CE,** (2024)
- **ISC2 Certified in Cybersecurity (CC),** (2024)
- **Google Cybersecurity Professional**, (2024)
- **Qualys Certified Specialist Certifications** (2024)
  - Vulnerability Management Detection and Response (VMDR), CyberSecurity Asset Management (CSAM), Vulnerability Management Scanning (VMS)
- **U.S. Department of Homeland Security National Incident Management System (NIMS)**, (2024)
  - 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

EDUCATION & TRAINING:

SANS Technology Institute

Cyber Immersion Academy ***(February 2025 - 2026)***

- Selected for a prestigious and intensive cybersecurity program with courses designed to provide hands-on experience in offensive and defensive security techniques.
- Anticipated completion of industry-leading certifications such as GIAC Security Foundations **(GFACT)**, GIAC Security Essentials **(GSEC)**, and GIAC Certified Incident Handler **(GCIH)**.

University of Massachusetts Dartmouth

North Dartmouth, MA ***(2019 - 2020, 2022-2023)***

- Some education with a concentration in Finance and Financial Operations
  - Completed Coursework Included: Calculus, Business Statistics, Macro-Economics and Micro-Economics, Operations Management, Principles of Accounting, Financial Modeling, Investment Analysis, Financial Markets
  - Umass Dartmouth Economics Club, (2022)
  - Umass Dartmouth Cyber Security Education Club (CSEC), (2022)

SKILLS:

Tools/Technologies: Splunk, Qualys, Microsoft Azure + Sentinel, Wireshark, Burp Suite, Metasploit, TCPDump, Google Cloud Platform
Frameworks: NIST CSF (SP 800-53, 800-61, 800-171), OWASP Top 10, CIS Controls, PCI DSS, HIPAA, GDPR, NIMS, SOC 1/SOC 2, ISO/IEC 27001, MITRE ATT&CK
Core Competencies: Incident Detection and Response, Cryptology, Vulnerability Management, Risk Assessment, Network Security, Identity and Access Management (IAM), Governance, Risk, and Compliance (GRC), Security Engineering
Security Operations: SIEM Tools, Cloud Security Monitoring, Threat Intelligence, Log Analysis, IDS/IPS, Penetration Testing
Programming/Scripting: Python, SQL, Linux, Bash/Shell Scripting, HTML 5, CSS

LABS, PROJECTS, AND PROGRAMS:

AIG Cybersecurity Engineering Program

- Served as an Information Security Analyst on the AIG Information Security Team, conducting research and infrastructure analysis to draft a detailed remediation plan for impacted teams.
- Crafted an advisory email to notify the Product Development team of the vulnerability, risks, impacts, and actionable remediation steps.
- Developed and executed a **Python**-based brute-force script to decrypt a ransomware-encrypted file during a simulated attack, showcasing technical proficiency in incident response and encryption methodologies.

Virtual SOC Environment Project

- Established a cloud-based Security Operations Center (SOC) using **Microsoft Azure and Sentinel**, delivering real-time threat detection and incident response capabilities for 2 Virtual Windows Servers.
- Monitored **7.6 million security events** and implemented custom KQL alert rules to enhance detection and resolution efficiency.
- Conducted threat intelligence analysis, refining incident response strategies and identifying attack vectors for improved monitoring.

Telstra Cybersecurity SOC Experience Program

- Led Telstra's Security Operations Center (SOC) Team as a Cybersecurity Analyst and Engineer.
- Managed the Incident Response Lifecycle, triaging malware attacks and documenting procedures for strategic improvement.
- Engineered and implemented a custom **Python** firewall rule to block traffic exploiting the **Spring4Shell** vulnerability **(CVE-2022-22965)**, bolstering defenses.
- Collaborated with SOC teams to develop actionable insights for enhanced incident response planning.

Commonwealth Bank Intro to Cybersecurity Program

- Served as a Cybersecurity Generalist on the Commonwealth Bank Fraud Detection and Response team.
- Analyzed and visualized data using **Splunk** to identify fraud patterns and enhance incident detection monitoring.
- Managed simulated phishing and malware attacks using the Incident Response Lifecycle and developed security awareness training aligned with **ACSC** best practices.
- Conducted penetration testing on web applications, identifying critical vulnerabilities and recommending remediation strategies.

PwC Switzerland Cybersecurity Program

- Worked as a Cybersecurity Analyst and Consultant on PwC Switzerland's Digital Intelligence Team.
- Conducted risk assessments, uncovering critical vulnerabilities and recommending mitigation strategies aligned with frameworks like **NIST CSF and ISO-27001**.
- Authored detailed security reports, outlining solutions such as network segmentation and enhanced security architectures.
- Provided tailored recommendations to improve clients' compliance posture and risk management frameworks.

Cybersecurity Incident Response Project (NIST CSF)

- Executed an incident response plan for a Distributed Denial of Service (DDoS) attack using the **NIST Cybersecurity Framework**, improving threat mitigation.
- Strengthened network defenses by recommending updated firewall settings, monitoring systems, and network segmentation.
- Conducted a comprehensive post-incident analysis, identifying vulnerabilities and recommending long-term improvements to strengthen the organization's security posture.

WORK EXPERIENCE:

Operations Manager/IT Systems Administrator

Digit Web Solutions, Remote/WFH, Full-Time ***December 2023 - Present***

- Managed web hosting services for 30+ clients, ensuring optimal website performance, uptime, security, and seamless functionality through DNS, SSL certificates, and email configurations.
- Led a talented team of Software Engineers, Web Developers, Data Analysts, and Graphic Designers to deliver high-quality projects on time and within budget.
- Oversaw and led the deployment of web development projects, software solutions, business automations, and internal IT infrastructure, ensuring scalability, security, and efficiency.
- Designed and implemented scalable IT infrastructure, including network systems and cloud-based solutions, while establishing robust data backup and disaster recovery plans.
- Optimized internal workflows to enhance operational productivity, improve client satisfaction, and streamline processes for software licensing and hardware procurement.
- Conducted IT risk assessments, implemented security controls, and trained team members and clients on cybersecurity best practices to safeguard sensitive information and digital assets.

Freelance Web Developer

Independent Contracting, Remote/WFH ***April 2021 - December 2023***

- Collaborated with clients to gather requirements, define project scope, and deliver tailored web solutions. Designed, developed, and deployed responsive, user-friendly websites tailored to client requirements, managing client domain registration and hosting services.
- Integrated various third-party tools and APIs to implement custom website features, analyze performance and metrics, optimize functionality, and deliver a seamless user experience.
- Specialized in identifying and troubleshooting technical issues while implementing robust solutions to maintain website functionality, enhance security, and ensure reliability.
- Created comprehensive documentation for website updates and trained clients on content management systems, ensuring long-term usability and operational independence.