Gustavo Salazar
(408)-202-8177
Gussalazar2525@gmail.com

Professional Summary

Cybersecurity professional with hands-on experience in incident response, vulnerability management, security monitoring, and endpoint/cloud security operations across both manufacturing and Department of Defense environments. Proven ability to analyze security events, manage SIEM/EDR alerts, harden systems, and support compliance frameworks. Known for strong analytical thinking, clear communication, and cross-team collaboration. Seeking to contribute to GILLIG's Security Operations Center by applying advanced security monitoring and investigative skills.

SOC Analyst | Gillig LLC | January 2026 – Present

- Investigate and triage security alerts using CrowdStrike Falcon, escalating and documenting findings for CCI and IT leadership.
- Utilize Qualys for vulnerability management, including deployment of recurring monthly patches and compliance scans.

Service Desk Technician | Gillig LLC | May 2024 – December 2025

- Support incident response activities by collecting endpoint artifacts, reviewing detections, and validating remediation steps.
- Deploy, configure, and manage Intune MDM, securing laptops, iPads, and mobile devices across the organization.
- Performed account provisioning, identity troubleshooting, and system access in support of Microsoft 365 and Active Directory environments.

Information Systems Security Manager | United States Air Force | May 2021 – May 2024

- Led cybersecurity operations in alignment with DoD Risk Management Framework (RMF), significantly improving system security and compliance readiness.
- Conducted security incident investigations, performed log reviews, and coordinated mitigation strategies with other IT teams.
- Delivered cybersecurity training to 800+ personnel, strengthening organizational cyber hygiene and user awareness.
- Improved enterprise vulnerability posture by approximately 85%, rising 76 positions in ANG security rankings through enhanced scanning, patching workflows, and remediation oversight.
- Recommended and implemented secure hardware/software solutions to enhance endpoint and network security posture.

Information Systems Specialist | United States Air Force | October 2019 – April 2021

- Engineered secure configurations for enterprise hardware/software, improving endpoint reliability and reducing technical vulnerabilities.
- Provided advanced troubleshooting for user devices, network connectivity, and secure computing environments.

- Supported deployment and validation of new equipment and applications, ensuring compliance with security requirements.

Vulnerability Management Technician | United States Air Force | October 2016 - September 2019

- Conducted vulnerability scans and audits, identifying and remediating system weaknesses across multiple network domains.
- Produced detailed reports on risk findings and remediation progress for leadership review.
- Participated in on-call rotations supporting rapid security incident handling.

Client System Administrator | United States Air Force - Deployment | July 2018 - February 2019

- Provided system administration for mission-critical LAN/WAN and virtual client environments.
- Managed privileged user access and group policy configurations in Active Directory.

Education

- Bachelor of Science – Business Administration, Management Information Systems – (Graduating May 2026) | San Jose State University
- Associate of Science - Cybersecurity | Moorpark College
- Associate of Science - Information Systems Technology | Community College of the Air Force

Certifications

- CompTIA Security+
- ISACA Certified Information Security Manager - CISM

Security Clearance

- DoD National Top Secret/SCI

Technical Skills

- **Security Tools:** CrowdStrike Falcon, Qualys, Intune MDM, Varonis, DISA STIGs, DoD RMF
- **Platforms:** Microsoft 365 Security, Azure AD / Entra ID, Active Directory
- **Security Domains:** Incident response, SOC monitoring, vulnerability management, endpoint security, log analysis
- **Systems:** Windows OS, LAN/WAN infrastructure, virtualization environments

Professional Approach

- Strong investigative and analytical mindset
- Ability to translate security findings into business impact
- Clear and concise communicator during high-pressure incidents
- Experienced working across cross-functional IT, cybersecurity, and operations teams
- Highly adaptable, mission-focused, and effective under pressure