ANGELINA SANCHEZ

Cyber Defense Analyst | SOC Operations | Threat Detection | SIGINT

Orlando, FL | angelina305_386@yahoo.com | linkedin.com/in/asanchez01 | TS/SCI w/ CI Polygraph Eligibility

PROFESSIONAL SUMMARY

Cyber Defense Analyst with 6+ years of combined experience in SOC operations, cyber threat analysis, SIGINT, and incident response supporting classified and DoD environments. Experienced with Splunk, Elastic, Microsoft Sentinel, Trellix, ACAS/Tenable.sc, Tanium, and Qmulos. Holds CompTIA Security+ and CySA+ certifications; currently pursuing CISSP and an M.S. in Cybersecurity at Southern New Hampshire University.

CORE COMPETENCIES

SOC Operations & Incident Response • Threat Detection & Cyber Analysis • SIEM Detection & Tuning • Network Forensics & Traffic Analysis • IOC/TTP Analysis • Vulnerability Management • Classified Computing Environments • DoD Cyber Operations

PROFESSIONAL EXPERIENCE

Cyber Defense Analyst | Lockheed Martin - Orlando, FL **Feb 2026 - Present**

- Monitor and analyze cybersecurity alerts within a classified Security Operations Center to identify, validate, and escalate potential threats to mission-critical systems.
- Conduct incident investigations and network traffic analysis; document findings and support timely containment and mitigation actions.
- Develop and refine detection content while collaborating with cybersecurity stakeholders to improve threat visibility and defensive operations.

Cyber Defense Analyst | Leidos (supporting DISA) - Scott AFB, IL **May 2024 - Jan 2026**

- Monitored, analyzed, and correlated alerts across Splunk, Microsoft Sentinel, Elastic, and Trellix to identify malicious activity and support incident escalation across classified systems.
- Conducted cyber incident investigations and root-cause analysis; coordinated containment and mitigation with internal and external stakeholders, including DISA and USCYBERCOM.
- Developed and fine-tuned SIEM correlation searches, dashboards, and alerts to strengthen detection and prevention capabilities while maintaining awareness of adversary TTPs and vulnerabilities.

Cryptologic Technician | U.S. Navy Reserve - Various Locations **Mar 2021 - Present**

- Deliver signals intelligence (SIGINT) and digital network intelligence in support of national defense operations and cyber threat identification.
- Support intelligence reporting and ensure proper handling and dissemination of classified products in alignment with DoD INFOSEC and OPSEC standards.

EDUCATION

M.S. Cybersecurity | Southern New Hampshire University - Online **In Progress**

B.S. Criminal Justice, Homeland Security Emphasis | Florida Technical College - **Aug 2020**

CERTIFICATIONS

CompTIA Security+ ce - Active • CompTIA CySA+ ce - Active • CISSP - In Progress

PROJECTS & TECHNICAL DEVELOPMENT

Elastic SIEM Home Lab | - **Mar 2024**

- Deployed Elastic Stack SIEM with Kali Linux, configured Elastic Agents for endpoint monitoring, and created custom detection rules, dashboards, and alerts for threat visibility and response testing.

Verizon Cloud Platform Job Simulation | Forage - **May 2025**

- Used Python to assess cloud VPN design for redundancy, resiliency, and least privilege; presented application-security and risk-mitigation recommendations.

ADDITIONAL EXPERIENCE

Chenega CABS / Naval Air Warfare Center Training Systems Division - Administrative Assistant (2023) • Florida Department of Corrections / Volusia County Detention Center - Correctional Officer (2014-2022)