Sergio D. Andrade

808-780-7526
serigo.andrade.one@gmail.com
www.linkedin.com/in/sergio-andrade-one

PROFESSIONAL SUMMARY

An experienced professional with an extensive background in cybersecurity, threat hunting, analytic development, digital forensics, knowledge management, information technology (cloud services, servers, client systems, intrusion detection (network/host), firewalls, networking, endpoint detection), training, office organization (process improvement, manpower etc.), as well as extensive leadership and managerial experience in a variety of organizational sizes and functional areas. I enjoy staying informed on cybersecurity news and the latest research utilizing various platforms such as SANS Internet Storm Center, Black Hills Information Security, various security vendors and researchers as well as podcasts such as “Darknet Diaries”.

Security Clearance: Top Secret/SCI – “Continuous Evaluation” enrolled (2022)

PROFESSIONAL EXPERIENCE

Position: Cyber Intrusion Analyst, Leidos GSMO-II ***2021 – Present***
DISA Pacific Defensive Cyber Operations, Joint Base Pearl Harbor-Hickam, HI
Scope: Performs attack sensing and warning by leveraging cyber security tools, tactics, and techniques to hunt for and report distributed, long-term, coordinated, low-visibility, network-based attacks across customers' networks and to identify possible unauthorized activity. Conducts retrospective analysis of historical data to aid in identifying trends and potential predictive measures by modifying intrusion detection rules and correlation searches. Conducts threat hunting operations to identify anomalous activity based on OSINT and leading-edge security research. Provided training on threat hunting, alert analysis and triage, and analysis process and methods. When appropriate, will recommend network and/or system configuration updates in response to changes in the threat environment.
Primary Tools: Splunk (SIEM) Enterprise Security, Cisco Firepower, Palo Alto, Menlo, Open Sensor Platform (OSP) BluVector, ELK Stack, Kibana (SIEM), Zeek, Elastic, Suricata (IPS/IDS), Snort (IPS/IDS), Logstash, Network Flow Data (SiLK), McAfee Endpoint Detection, Tanium, Wireshark, VirusTotal, Domain Tools Iris, Arbor (Internet Access Point), Authentic8 (SiLO), AnyRun, Shodan, Endace (PCAP), CyberChef and various OSINT tools.

Position: Information Security Manager, Intelligence Directorate **2019 - 2020**
Headquarters, Pacific Air Forces, Joint Base Pearl Harbor-Hickam, HI
Scope: Pacific Air Forces (PACAF) lead for the Intelligence Community (IC) Information Security and Industrial Security programs; provided guidance, policy, training, awareness, and support to 19 subordinate command organizations throughout the Pacific theater of operations. As manager of the PACAF IC Information Security program; provided oversight of security incidents, containment, sanitization, and reporting to the Air Force IC SCC and coordinated clean-up efforts with subordinate units throughout the theater. Oversaw the Security, Education, Training and Awareness (SETA) program and produced awareness materials, tracked training, and provided outreach support to subordinate organizations. Manages the IC Industrial Security program for Joint Base Pearl Harbor-Hickam and reviewed, validated, and coordinated contractor access requirements to SCI data, systems, and facilities.

Position: Operations and Personnel Manager **2013 - 2018**
Headquarters, Pacific Air Forces, Joint Base Pearl Harbor-Hickam, HI
Scope: Managed and advised leadership on manpower utilization and employment for 15 offices and 102 employees. Oversaw knowledge management strategy and established processes to support collaboration and knowledge flow to subordinate units throughout the Pacific region. Administered $1.8M contract expansion project; identified support requirements, met with senior leaders, and developed knowledge management strategy timeline.

EMPLOYMENT HISTORY CONTINUED:

Deputy Technical Director | Joint-Base Langley-Eustis, VA	2012 - 2013
Network Operations Manager | Joint-Base Langley-Eustis, VA	2010 - 2012
Systems Administrator | Special Duty	2005 - 2010
Client Systems Tech | Davis-Monthan AFB, AZ	2001 - 2005
Access Database, HTML developer | Aviano AB, Italy	1998 - 2001
Administrative Tech | Araxos AB, Greece	1997 - 1998
Administrative Tech | McClellan AFB, CA	1993 - 1997

EDUCATION
Bachelor of Science Degree, Network Security | University of Advancing Technology (2017)
US Air Force Management and Leadership courses (2020,2013, 2012, 2006 &1996)

RECENT TRAINING
Elastic Training (Zeek, Logstash, Elastic and Kibana) (ID: C73108) (2022)
Splunk Boss of the SOC Competition Participant (Mar & Aug 2021)
Splunk 7.x Fundamentals (2021)
Tanium (2021)
Black Hills Information Security Threat Hunting & Packet Decoding (2021)
MITRE ATT&CK CTI (2021)
Autopsy Digital Forensics (ID: 621arby4rz) (2020)

CERTIFICATIONS
GIAC GSOC (Exp: 2026)
CompTIA CySA + (Exp: 2024)
AWS Certified Cloud Practitioner (Exp: 2024)
EC-Council Certified Network Defender (Exp: 2023)
CompTIA **Security +** (Exp: 2024); **Network +** (Exp: 2024) and **A+** (2009)
Microsoft Certified Systems Administrator (Completed Coursework - 2006)