Adan Lopez

1469 Cypress St.
San Dimas, CA 91773
(714) 240-4496
heyadanlopez@gmail.com
LinkedIn

Qualifications

Citrus Community College (1999-2001)
Secret/SAP Clearance
Fluent in Spanish
ICS2 CISSP certification
COMPTIA Security+ certification
ICD-705 SAP/DoD Risk Management Framework (RMF) certificate

Employment History

Company: Kirkhill, Inc., Brea CA
Title: IT Manager
Date: 2018 to present
Description: Aerospace, team of 5, manage GRC, ISSM for DoD classified networks.

Company: Hartwell, Placenta CA
Title: IT System Administrator
Date: 2010 to 2018
Description: Aerospace, IT architecture/engineering, GRC lead, help desk supervisor.

Experience

- **Project Management:** Managed a $5m ERP replacement from Unix to AWS Govcloud. Delivered on time and under budget, despite lack of dedicated team, 40% team turnover, and unexpected Covid lockdowns.
- **ISSM for classified DoD systems:** Rescued program from suspension, restored ATO, and resumed shipments of product by developing SSP, NIST 800-53 procedures, and securing VHF impedance testing systems and NLR Arch radio frequency testing of low-observable materials, single-handed and in 90 days. COMSEC Responsible Officer, responsible for managing TACLANE, TEMPEST, and encryption systems.
- **Assessment Scope Reduction:** Reduced CMMC assessment scope and significantly reduced costs by analyzing scoping guidances, categorizing assets, diagraming data flows, and implementing strong flow control limitations to support reduced scope.
- **HITRUST and NIST CSF:** Identified significant improvements in cybersecurity posture by leveraging HITRUST and NIST CSF frameworks to bolster the CMMC controls.
- **Oversight of 3rd Party Assessors:** Prevented unnecessary costs due to improper 3rd party CMMC assessments by identifying inaccurate interpretation of control language

- **Risk Management:** Achieved significant risk reduction, improved business alignment, established risk lifecycle management (NIST 800-30), integrated security seamlessly into processes, mapped business dependencies to Mitre ATT&CK, ensured feedback to DRP/IR/budget, and fostered a strong risk culture.
- **Supply Chain/Cloud Service Providers:** Established supply chain risk management. Leveraged SOC II, Bitsight EASM, supplier interviews, and shared responsibility matrixes. Responded to and mitigated breaches like Solarwinds, CrowdStrike, and Log4J. Assessed compliance with CMMC, DFARS, GDPR, and SOX.
- **SOC operations:** Selected to help evaluate SOC MSSPs for 50+ Transdigm companies and standardize the SLA across the group. Evaluated shared responsibility matrixes, proposed services and deliverables across PM, VM, SIEM, and SOC. Assessed SOC operations, signal coverage, threat analysis, incident mishandling, and IOC effectiveness.
- **Incident Response:** I develop IR plans and lead table-top testing. I lead the threat response team and assist with analysis of logs, TTPs, anomalies, packet captures, drill-downs and pivots of threat graphs. I investigate signs of lateral movement, propagation, beaconing, privilege escalation, impossible travel, or anomalous program or script executions.
- **Azure IaaS/PaaS Security:** Implemented hybrid cloud and cloud risk reduction (30% improved score in Bitsight EASM) by leveraging shared responsibility matrixes and hardening with OWASP and CIS Benchmarks. Established secure processes for API configurations, key handling, managed identities, SSO, SAML/OATH, passkeys. Implemented token binding, adaptive/continuous evaluation, Azure RBAC, and JIT/PIM.
- **M365 Security:** Ensured secure transition to Exchange Online, Sharepoint, Teams and Azure VM migration. Designed secure vnet/subnet/NSG architecture. Segmented and hardened Azure resources. Hardened Exchange and Teams sharing and collaboration settings and implemented Purview DLP.
- **Vulnerability Management:** Achieved a major reduction in vulnerability by integrating Tenable Nessus, Bitsight EASM, MS Secure Score (Defender for Cloud), and Extrahop NDR in a multi-layered VM strategy. Managed pentesting and hardening of Windows, Active Directory and Vmware (SCAP/STIG, OWASP, CIS Benchmarks, Intune, SCCM).
- **Industrial Environments:** Reduced attack surface from IIoT/IoT devices (NC/PLC, environmental, RFID, digital signage, POS, logistical/inventory) via segmentation and port filtering. Oversight of guard monitoring, physical security assessments, badged access control systems, security cameras, and perimeter barriers such as automated gates and turnstiles.
- **Security Architecture/Engineering:** Re-architected IP subnetworks to support segmentation of user traffic from backend traffic and virtually eliminate lateral movement. Implemented tiered network segmentation for PAWs, and tiered administrative privileges in Active Directory.