Adan Lopez

San Dimas, CA
heyadanlopez@gmail.com | LinkedIn: adan-lopez-76947911 | Github: heyadanlopez-a11y

Education: Pasadena City College (2000-2001)
Certifications: CISSP, COMPTIA Security+,
Other Training: UCLA Project Management Extension, DoD Risk Management Framework
Other: Active DoD Secret Clearance
Languages: English and Spanish (fluent)

Experience

- **Cyber Risk Management:** Achieved measurable risk reductions every year with minimal investment or head count. Quantified the event likelihood (ARO) from sources like industry breach reports, FEMA/USGS National Risk Index, penetration test findings, and recent vulnerability scans. Modeled threats and mapped to assets and business dependencies, then quantified the potential impacts by translating to key profit drivers. Identified practical mitigations using existing tools or practices, to maximize ROI and accelerate risk resolution. Extracted impact calculations (SLE) from sources such as GDPR administrative fines, cyber insurance contracts, penalties from False Claims Act (FCA) violations, ISACA guidance, Verizon DBIR reports, lost defense contracts, and loss of EBITDA from business interruption. Allied with business managers to ensure my calculations (SLE) were based on the real-world and supported by data. Produced scope-limited assessments at the facility, system, and asset level, for rolling up to DoD risk reports. Streamlined risk registers, impact scoring matrices, RTO/RPO metrics, and qualitative risk heat maps to suit the culture and sophistication level of the specific organization.
- **Regulatory Compliance:** Consistently scored in the top 10 out of 57 Transdigm companies during multiple rounds of DFARS, NIST 800-171, CMMC, GDPR, and SOX assessments. Developed simple, no-fuss System Security Plans (SSP) which reduced the burden of compliance and were presented as a model to other business units. Identified gaps in the CMMC assessment practices of our 3rd party consultants, potentially saving the company $65k in failed certification assessments. Significantly reduced the scope of our CMMC assessment by implementing segmentation and strategic asset categorization, saving the company 5 figures in security tooling. Experienced mapping frameworks and merging into a single management tool/program to reduce duplication of work using Excel, Exostar, SAI360, and AuditBoard.
- **Supply Chain Risk (TPRM/SCRM):** Responsible for shared responsibility and risk assessment of third-party SOC providers, Microsoft/AWS cloud threats, cloud RMM and endpoint management, XML-integrated inventory management, API-integrated patch management, and many others. Partnered with Purchasing to implement a risk-based vendor onboarding process, vendor scorecards, and approved suppliers list. Performed NIST 800-171 assessments of suppliers. Identified and negotiated gaps in MSP service contracts to ensure security objectives and regulatory requirements are met. Performed supply chain threat modeling and risk mitigation measures to reduce potential blast radius of a supply chain breach. Leveraged SOC 2 Type 2 reports, ISO 27001, BitSight EASM, supplier interviews, supplier policies and procedures, and shared responsibility matrices to evaluate vendor security posture. Leveraged my experience with major supply chain incidents like SolarWinds, CrowdStrike, and Log4j.
- **SOC Management & Governance:** Implemented and managed internal SOC/SOAR operations utilizing cost effective solutions like AlienVault, SolarWinds LEM, Lepide, Netwrix, ExtraHop NDR, Qualys, Crowdstrike Falcon, Crowdstrike IDP, SentinelOne, Sumologic SIEM, MS Ops Mgr (MOM). Selected by corporate to join a committee evaluating SOC providers for 57 Transdigm

aerospace/defense companies. I evaluated shared responsibilities, SLAs and deliverables, across EDR, Patch Management (PM), Vulnerability Management (VM), and SIEM. I assessed performance of 3rd party SOC operations and metrics, such as signal coverage, threat analysis, incident mishandling, threat intelligence feeds, and detection rule effectiveness. I improved SOC metrics by using risk assessment, threat modeling, data inventory and classification, and business impact assessments (BIA), to identify gaps in SOC operations and ensure alignment to real-world business risks. Conducted penetration testing of ADCS and Active Directory that uncovered critical blind spots in SOC monitoring where attacks had gone undetected.

- **Vulnerability Management:** Held up as a model for sister companies by layering Nessus for endpoints, Bitsight for public-facing attack surfaces, and Secure Score for cloud assets, and integrating them into a single cohesive strategy of continuous monitoring. Eliminated frequent, unnecessary fire-fighting by developing risk-based vulnerability metrics which were informed by real business drivers, dependencies, and assets, rather than depending solely on limited metrics like CVSS, KEV, or LEV. Achieved major efficiencies by applying guidelines (CIS Benchmarks, OWASP) to reduce attack surface (least functionality) on core platforms (Azure, Active Directory, VMware), shifting from reactive remediation to strategic and enduring vulnerability reduction.
- **Identify Access Management (IAM)**: Modernized and hardened privilege access in MS Entra ID with a tiered administrative model and elimination of standing privileges (JIT via PIM). Implemented a privileged user “scorecard” to identify critical accounts and apply stricter controls, like approval-based escalation, host/IP-bound login, and real-time login alerts. Converted service accounts from password to “managed”, key-based authentication with automated rotation, and reduced access (least privilege), eliminating risks associated with unmanaged service accounts. Automated user access reviews by restructuring group and access roles to align with granular job functions, and changing the naming structure to clarify the access associated with each role, resulting in no-touch access report distribution, and transfer of access review ownership to proper data owners within the organization. Implemented lifecycle management, SSO/SAML, Netwrix PAM, passwordless auth, FIDO2, Windows Hello, passkey, Entra ID conditional access, risk-based adaptive evaluation, ADP HRIS automated provisioning via SCIM, segregation of duties on audit logs, device posture assessment, and API key rotation/vaulting.
- **Information System Security Manager for classified DoD systems:** I received DoD commendations, achieved excellent audit results with minimal corrective actions, and managed the classified systems to NIST 800-53 standards single-handed for 3 years.
- **Incident Response:** Saved the organization multiple times by responding appropriately and effectively to contain major outbreaks like Hafnium and Log4J before they became a reportable breach. Being grounded in hands-on incident response, my IR strategy prioritizes frequent testing, rapid containment, and out-of-band business continuity of critical business functions. I leverage high quality tabletop exercises as a continuous improvement tool as well as a training tool. Experience standing up minimally-viable IR plans rapidly, to satisfy customer or regulatory requirements for companies who are still early in their journey.
- **Cloud Governance:** Managed hybrid cloud security and reduced cloud risk by 20% by improving cloud posture (CSPM) with external pen testing, BitSight EASM, Maester, Prowler, and Qualys CSPM. Managed data sovereignty compliance with GDPR, ITAR, and CMMC. Developed a shared responsibility matrix for our cloud vendor. Scanned cloud assets like Teams, virtual machines, and Sharepoint against CIS benchmarks. Restricted external data sharing via email and unauthorized clouds with Purview, by combining data classification tags and DLP policies, with Defender for Cloud Apps (CASB) policies. Developed procedures for secure API configuration/access, key management, managed identities, and Azure Storage Accounts. Mitigated misconfiguration risks by implementing change control, change monitoring, and periodic audits. Hands-on experience securing SSO, SAML, OAuth, OIDC, passkeys, Azure RBAC, AWS

EC2 web servers, AWS VPC networks, S3 buckets, VPN gateways, elastic IPs, and DNS records.

- Managed access packages, external identities, and external organizations in Azure B2C (CIAM)
-
- **Industrial Security (IoT/OT): 20 years of experience managing risk and reducing attack surface related to** IIoT/IoT devices like NC machines, data collection/acquisition devices, PLC controllers, Schneider Electric power control systems, refrigeration sensors, RFID inventory management, CCTV, door access controllers, badge readers, digital signage, handheld barcode terminals. Enabled effective risk management of IoT/OT assets by implementing asset discovery and classification tags, and mapping them to key business operations (inventory, shipping, part quality, etc.) Reduced risk by baselining IoT/OT network traffic and applying anomaly detection with NDR. Assessed vulnerabilities in our physical security including guard monitoring, badged access systems, video surveillance, perimeter barriers, automated gates, and turnstiles.
- Artificial Intelligence and Large Language Models: Risk
- Perplexity, notebook LM, Gemini Gems

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:	2000 to 2018
Description:	Aerospace, IT architecture/engineering, GRC lead, help desk supervisor