

Moira Lopez

Cybersecurity Consultant

CONTACT DETAILS

📞 555-555-555

✉️ moiralopez7@gmail.com

📍 San Diego, CA

CORE SKILLS

- SIEM Best Practices
- Data Loss Prevention
- Systems Administration
- Cloud Infrastructure Controls
- Cybersecurity Consultation
- NIST/CIS/COBIT Frameworks
- Vulnerability Assessments
- Intrusion Detection

PROFESSIONAL PROFILE

Dedicated Cybersecurity Consultant with enterprise-level experience in designing, configuring, and managing security infrastructure devices, such as firewalls, SSL VPNs, secure web gateways, IPSs, and app firewalls. Ability to calculate the impact of adverse events by assessing clients' security controls, business continuity strategies, disaster recovery plans, and system threats within cloud environments. Adept at information gathering, planning, and execution of network security migration and upgrade projects.

CAREER SUMMARY

Jan 2018 - Present

IAP Worldwide Services, San Diego, CA Cybersecurity Consultant

Outline

Determine critical security weaknesses that pose vulnerabilities, for a leading provider of global logistics, facilities management, and technical services that solves public/private sector customers' most demanding business challenges.

Key Responsibilities

- Develop strategic roadmaps to devise and implement secure solutions that reduce risks and improve the overall cyber resilience of technology assets and IT controls.
- Gather requirements and advise customers on product/services through solutions that mitigate threats and support governance programs for transformational change.
- Conduct demonstrations, proofs of concept, and presentations to client stakeholders.
- Provide subject matter expertise in third-party risk management and automate security processes and tools to review controls for cloud-based applications.
- Draw up cost estimates for any needed defense upgrades and pinpoint potential integration issues for IT project managers.
- Deliver complex services, including project plan management, architectural design, system integration, and knowledge transfer activities.
- Perform assigned audit engagements related to confidentiality, integrity, information protection, and data availability.
- Secure end-to-end IPsec connections using Active Directory Certificate Services to drive risk remediation or changes from previous audit for existing suppliers.
- Coach IT personnel towards expertly understanding network concepts/protocols, such as RIP, BGP, OSPF, MPLS, STP, VRRP, WCCP, Load Balancing, and WAN Acceleration.

Key Achievements

- Outlined an incident response plan that minimized breaches by 70% for 100+ clients.
- Optimized efficiency by 40% by creating awareness campaigns and training materials for staff on best practices related to email, web browsing, and social media usage.
- Boosted client satisfaction levels by 60% due to providing ongoing support and responding to requests from users regarding account access issues, password resets.