Luis López

Contact Information

+1 514-449-3634 | luis.lopez@loxi.ca | https://www.linkedin.com/in/luislopez/

Summary

Cyber Security Professional with 10+ years of expertise in designing, implementing, and managing robust security solutions. Proven track record of leading technical teams and driving successful security initiatives in complex environments. Strong knowledge of industry best practices, compliance regulations, and emerging cyber threats.

Technical Skills

Cloud Security: GCP, AWS, MS Azure
IAM: Ping Identity (ForgeRock Directory Services, ForgeRock Identity Management, ForgeRock Access Management), SailPoint IIQ, CyberArk
Security Tools: StackRox, Brinqa, Rapid7 Nexpose, Nessus, OpenVAS, Qualys, AlienVault USM, MISP
Practices: DevSecOps, Vulnerability Management, Incident Response, Risk Management, Security Architecture
Platforms: Kubernetes
Operating Systems: Linux (Ubuntu, Debian, RedHat)

Professional Experience

Solution Architect – Cyber Security | BDC | September 2024 – Present

- Responsible for the security posture of applications and technical infrastructure by driving security in the design and development process.
- Develop and validate security requirements, and drive successful completion of security evaluation and testing.
- Create solutions, supporting current and foreseeable changes due to new technical or business requirements.
- Ensure solutions are functionality appropriate, technically sound, well-integrated, and support reuse within the existing ecosystem.
- Develop solution architecture by collaborating with Business units, Enterprise Architecture, Development, Security, and Operations.
- Provide value-added, professional advice to the Lead Solution Architect, Senior management team, and business partners.

Key responsibilities include:

- Translate business requirements into long-term architectural solutions for the business with aim to ease the sharing of consistent information between lines of business.
- Integrate into project teams as a cybersecurity solution architecture expert.
- Guide and propose technological solutions that meet business needs while aligning with IT strategies.
- Lead and/or participate in the design of solution architectures and associated artifacts, ensuring alignment with security policies, standards, and best practices.
- Advise teams regarding security risks and drive mitigation approaches.

Selected projects:

- Identity and Access Management: Implemented and maintained Customer, Workforce, and Partners identities lifecycle management using Ping Identity platform (ForgeRock Directory Services, ForgeRock Identity Management, ForgeRock Access Management).
- Identity Governance and Administration: Designed and implemented SailPoint IIQ with emphasis on access certification and job roles management.
- Privileged Access Management: Integrated CyberArk with IAM/IGA processes to fulfill audit and compliance requirements.

Cloud Security Architect – Cyber Security Engineering | EY | April 2022 – August 2024

- Spearheaded the design and technical implementation of solutions, focusing on cloud security architecture across GCP, AWS, and MS Azure, for client engagements and internal projects.

Key responsibilities included:

- Led cloud security assessments, supported cloud implementations, and handled technical escalations from current engagements.
- Provided hands-on consultancy services to clients following cloud security assessments.
- Identified and pursued business opportunities to expand market presence (i.e., produced RFP responses, formulated go-to-market strategies for new products or services, defined operational KPIs).

- Contributed to people-related initiatives such as recruitment, career coaching, and technical training to enhance staff key skills.

Selected client-facing engagement experience:

- Detailed assessment and architecture design for Data and Analytics solution in MS Azure (leveraging Synapse and PowerBI) to support digital transformation and improve security, privacy and compliance posture at an air ambulance service and medical transport non-profit organization operating at the provincial level.
- Technical project management for the expansion of a SaaS-Based Endpoint Privilege Management (CyberArk EPM) solution to enhance service and coverage, securing additional endpoints and enforcing least privilege without disrupting business at a Canadian financial service cooperative that is also the largest federation of credit unions in North America.
- Assessment for potential security compromise and vulnerability management program optimization covering definition, and documentation of the remediation process, including metrics dashboards in PowerBI, for Operational Technology environments at an electricity transmission and distribution utility serving a Canadian province.
- Customer Identity and Access Management (CIAM) migration from an on-premise in-house built solution to a PAAS provider (Auth0) for a large provincial corporation with commercial activities related to online gambling.
- Identification and remediation of cybersecurity issues related to the data storage unified platform for analytical consumption purposes (running in MS Azure Cloud) at a major retailer in the Canadian market.

Security Professional – Client Engineering | IBM | June 2021 – March 2022

- Worked with colleagues and technical leaders on the customer side to ensure security and compliance requirements were integrated into Minimum Viable Solutions (MVS).

Responsibilities included:

- Led DevSecOps practices and embedded security directly into development practices and CI/CD pipelines.
- Provided hands-on expertise with security practices across infrastructure, applications, and networks.
- Assisted clients in solving challenges and finding the proper balance between enabling and security in relation to the client’s organization and ecosystem.

Selected projects:

- Integration of Open Source threat intelligence sharing platform (MISP) with Security Orchestration and Response platform for electric power generation utility.
- Automation for vulnerability remediation activities in cloud-native production environments at a financial organization.

Cloud Security Architecture Lead | SAP CX | January 2018 – June 2021

- Executed technical hands-on and organizational leadership to foster a security-conscious culture.
- Ensured that technical decisions aligned with business objectives and were implemented effectively with stakeholder participation.

Duties/Initiatives:

- Led the rollout of the runtime protection tool for the commerce platform containers (StackRox), including defining the risk assessment process for application security in Kubernetes.
- Integrated regulatory aspects (e.g., GDPR, PCI-DSS, SOC, NIST) into technical reasoning.
- Developed comprehensive security architectures aligned with technical, business, and compliance initiatives (i.e.: privacy by design) to be delivered as product features and defined KPIs to measure the efficiency of such features.
- Participated in the technical evaluation and integration of a risk-based vulnerability management platform (Brinqa) into the security infrastructure, including the definition of a remediation strategy utilizing Brinqa's asset management, risk scoring, and prioritization features.
- Provided technical recommendations and architectural design options to integrate Commerce environments with Cloud Identity Services, SAP’s standard product for Identity and Access Management.
- Contributed and acted as a subject-matter expert for escalations of Cybersecurity incidents.

Cloud Security Operations Lead | SAP CX | January 2017 – January 2018

- Responsible for developing and leading the security operations practice.
- Provided concrete technical solutions and strategic input associated with incident response, vulnerability management, and overall risk and compliance management for critical production environments.

Key tasks and initiatives:

- Owned and advanced the existing security operations practice, implementing tools and processes aligned with organizational goals and legal requirements while following internal and external standards, best practices and frameworks.
- Actively participated in the platform migration to Microsoft Azure following the adoption of a cloud-native approach while offering continuous support for live customers.

- Established, monitored, and reported key metrics to provide accurate and meaningful information on the effectiveness of the operational security initiatives.
- Holistically and continuously identified, recommended, and implemented appropriate risk reduction/response options to reduce impact to acceptable levels based on organizational risk appetite.
- Conducted post-incident reviews to determine the root cause of information security incidents, developed corrective actions, reassessed risk, evaluated response effectiveness and took appropriate remedial actions.

Cloud Security Engineer (Consultant) | SAP Hybris | June 2015 – January 2017

- Worked closely with project management, support, and development teams, as well as other relevant stakeholders, to implement and maintain technical security measures required to support compliant, secure, and stable operations of customer systems.

Responsibilities/initiatives included:

- Vulnerability Management Platform selection, implementation, and operationalization (Rapid7's Nexpose) in a globally distributed infrastructure.
- Handled and coordinated related security activities across all customers (vulnerability and incident management), including forensic reporting.
- Automation of the patching process for a large Linux (Debian and RedHat) environment (10K+ virtual machines).
- Evidence collection for external and internal audits.
- Documentation of security policies, processes, and procedures in alignment with the management team and related subject-matter experts.

Security Integrator | Morgan Stanley | October 2014 – June 2015

- Part of a global team providing a centralized, firm-wide control function for Privileged Access Administration, Exceptions, and Entitlement Management.

Duties and responsibilities included:

- Onboarded new services identified as Privileged Access and created control or entitlement processes using the ServiceNow platform.
- Identified flawed security practices and processes, and advocated for change.
- Assessed solutions to Risk, Audit, Entitlement, and Technology issues, suggesting recommendations for resolution while ensuring adherence to the Firm's security policies and standards.
- Maintained and regularly updated department-wide documentation and procedures for all services.
- Participated in weekly and quarterly entitlement reviews with Audit.
- Continuously improved services administered by the team.

Security Analyst | La Presse | December 2012 – October 2014

Duties: (Reporting to the Chief Security Officer – CSO

- Provided security architecture reviews for IT projects.
- Monitored and resolved alerts and IPS reports.
- Performed vulnerability assessments against corporate assets using tools like Nessus, OpenVAS, and Qualys.
- Assessed risk for outstanding vulnerabilities and coordinated patching activities on corporate assets, including reporting metrics to evaluate the effectiveness of the vulnerability management program.
- Acted as an SME in information security topics to provide oversight and best-practices advice for ongoing operations.
- Researched and evaluated information security technologies/tools.

Projects:

- Design, implementation, and administration of denial-of-service protection using Radware.
- Standardization of web authentication services based on SAML using OpenAM.
- Implementation of automated vulnerability scanning to improve efficiency and coverage.
- Integration of vulnerability management process with the Security Information and Event Management platform (AlienVault USM) for better threat detection.

Web Infrastructure Supervisor | La Presse | January 2011 – December 2012

Duties: (Reporting to the Director, Support & Infrastructure)

- Defined the technical architecture.
- Ensured that all components of the technical architecture were properly integrated and implemented.
- Coached the technical team in the development of the technical architecture.
- Resolved identified technical issues.
- Helped define the development toolkit and environment.

- Provided technical support and technical quality control throughout all stages of the projects related to web development/testing infrastructure.
- Coordinated vendor services related to technology selection and implementation.

Web Infrastructure Advisor (Consultant) | La Presse | November 2009 – January 2011

Duties: (Reporting to Director of Web Development)

- Reviewed solutions' technical architecture.
- Troubleshooted technical issues.
- Integration and implementation of web components in a production environment.
- Development environment design and management..

Sales Engineer | Canonical Ltd | September 2008 – November 2009

Duties: (Reporting to the Director, Global Support Services)

- Technical Solution Design: Devised solutions for customer needs and determined the suitability of solutions based on Ubuntu, including active participation in the general technology strategy (choice of tools, modules and system components, development tools, and methods). Provided technical representation at customer and prospect meetings.
- Requirements Gathering: Developed the scope of projects at inception, involving liaison with clients, interfacing with the Sales team to provide solutions to clients, and obtaining sign-off on the project scope from project stakeholders.
- Technical Account Management: Liaised with the client's technical and management team to enable them to successfully design and implement solutions based on Ubuntu and get the most out of them.
- Project Delivery: Managed bespoke changes to corporate sale services, and coordinated implementation by the client with the Technical team. Provided estimates on project scope, duration and cost. Assumed responsibility for delivery on time and budget.
- Post-Implementation Support: Helped customers with ongoing issues after successful implementation of a solution based on Ubuntu.

Projects

- Junta de Andalusia (province-wide Ubuntu deployment).
- Minimal desktop infrastructure roll-out (US-based large financial institution).

Education

Comprehensive Project Management Course – McGill University
Bachelor’s Computer Science – Universidad Industrial de Santander – Colombia

Certifications

Certified Information Systems Security Professional (CISSP) – (ISC)² – 4532447
Information Systems Security Architecture Professional (CISSP-ISSAP) – (ISC)² – 4532447
Certified Cloud Security Professional (CCSP) – (ISC)² – 4532447
GIAC Defensible Security Architecture (GDSA) – 10214690
Professional Scrum Master level I (PSM I) – Scrum.org – 480995
Azure Security Engineering Associate – 27F4K3-BC1043
Microsoft Certified: Cybersecurity Architect Expert – D6DF0I-D7A5A4

Languages

English – Bilingual
Spanish – Native
French – Fluent

Clearances

Secret Level
Government of Canada