Manuel Alejandro Roldán Mella

Application Security Expert

Argentina / Remoto Global | manuel.roldan80@gmail.com | in/manuel-alejandro-roldan-ktirex

PERFIL PROFESIONAL

Profesional en ciberseguridad con más de 17 años de trayectoria profesional, con una sólida base técnica en seguridad ofensiva y defensiva (Red/Blue Team) que ha evolucionado hacia roles de liderazgo en seguridad de aplicaciones (AppSec) y seguridad aplicada con IA. Experiencia dirigiendo y coordinando equipos de ciberseguridad y gobernando el ciclo de desarrollo seguro (SSDLC) en organizaciones de banca y fintech transaccionales líderes de la región (ueno bank, Pomelo, Naranja X, Veritran). Capacidad demostrada para alinear los controles técnicos de seguridad con la gestión de riesgos y estándares normativos (ISO 27001, PCI-DSS).

CERTIFICACIONES

CCSK v5
Certificate of Cloud Security Knowledge – CSA

AWS-SAA
AWS Certified Solutions Architect – Associate

CEH
Certified Ethical Hacker – EC-Council

CHFI
Computer Hacking Forensic Investigator

CSX
Cybersecurity Fundamentals – ISACA

CCENT
Cisco Certified Entry Networking Technician

Trayectoria Profesional

Security Champion Captain
Ene 2025 - Presente

Veritran

Buenos Aires, Argentina (Híbrido)

- **Estrategia de Seguridad en IA**: Liderazgo en la definición de la estrategia y gobernanza de Seguridad en IA, estableciendo directrices de control para la adopción de Large Language Models (LLMs) y agentes cognitivos.
- **Herramientas con IA**: Diseño y desarrollo de herramientas de seguridad potenciadas por IA y agentes autónomos para la clasificación, priorización y remediación automática de vulnerabilidades de código.
- **Modelado de LLMs**: Evaluación de riesgos y modelado de amenazas específicas para sistemas de IA (marcos OWASP Top 10 for LLMs), protegiendo la infraestructura de pagos globales.
- **Gobernanza SSDLC**: Liderazgo de un equipo multidisciplinario para la implementación de mejores prácticas de seguridad en los procesos de ciclo de vida de desarrollo de software seguro (SSDLC).
- **Automatización en Pipelines**: Integración y optimización de herramientas SAST, DAST y SCA automatizadas en la cadena de CI/CD.
- **Enlace & Capacitación**: Impartición de sesiones de entrenamiento técnico en desarrollo seguro e IA y enlace entre desarrollo y ciberseguridad.

Application Security Team Leader
Sep 2023 - Ene 2025

ueno bank

Asunción, Paraguay (Remoto)

- **Políticas y Estándares**: Diseño e implementación de políticas y estándares técnicos de codificación segura para todo el desarrollo bancario.
- **Controles en Pipeline**: Desarrollo y mantenimiento de integraciones SAST, DAST y SCA en las cadenas de integración continua para prevenir vulnerabilidades de forma temprana.
- **Modelado de Amenazas y Code Review**: Identificación proactiva de amenazas y revisiones detalladas de código (Java, PHP, NodeJS) para garantizar prácticas de diseño seguro.
- **Pentesting y Gestión de Vulnerabilidades**: Conducción de pruebas de penetración y análisis continuos de vulnerabilidades en aplicaciones y entornos cloud.
- **Programas de Concientización**: Diseño y despliegue del programa corporativo de concientización en seguridad para entrenar a los desarrolladores en prácticas seguras.
- **Gestión de Equipo y Metodología**: Coordinación y planificación de tareas del equipo mediante marcos de trabajo ágiles (Scrum), garantizando entregas eficientes en cada sprint.
- **Adquisición de Herramientas y Proveedores**: Dirección del proceso de evaluación y selección de herramientas de seguridad de aplicaciones y proveedores clave del área.

GOBERNANZA & TECH

LIDERAZGO & GESTIÓN

Liderazgo de Equipos

Gobernanza de Seguridad

Planificación Estratégica

ISO 27001 & PCI-DSS

Análisis de Riesgos

APPSEC & IA SECURITY

Seguridad con IA

SSDLC Governance

Arquitectura Segura

Threat Modeling

Auditoría de Código

Kubernetes Security

Docker

TÉCNICO & SECOPS

SecOps en la Nube

Integración CI/CD

Respuesta a Incidentes

Forense Digital

Pruebas de Intrusión

Terraform

Python / Scripting

EDUCACIÓN

TSU en Informática

UPTANCA

Los Teques, Venezuela

IDIOMAS

Español — Nativo

Inglés — Intermedio

Cybersecurity Engineer Team Leader

Abr 2022 - Sep 2023

Wazuh, Inc.

Buenos Aires, Argentina (Remoto)

- **Recertificaciones de Cumplimiento**: Liderazgo técnico en proyectos de recertificación SOC 2 y PCI-DSS, garantizando conformidad y gestionando con éxito auditorías externas.
- **Controles en Ciclo de Desarrollo**: Diseño e implementación de controles SAST, DAST y SCA integrados en los pipelines de CI/CD del producto core.
- **Automatización en Detección**: Mejora de las capacidades de detección de amenazas en entornos de nube mediante la automatización de herramientas de seguridad.
- **Optimización XDR/SIEM**: Afinamiento avanzado (fine-tuning) de las alertas generadas por SIEM, IDS/IPS y soluciones XDR corporativas para robustecer la respuesta.
- **Desarrollo de Casos de Uso**: Propuesta y despliegue de nuevos casos de detección basados en amenazas emergentes y alineados con las prioridades de seguridad.
- **Playbooks de Respuesta Automatizada**: Creación de playbooks para respuestas automáticas ante eventos de seguridad, reduciendo tiempos de contención de riesgos críticos.

Cybersecurity Team Leader

Abr 2021 - May 2022

Pomelo

Argentina (Remoto)

- **Certificación PCI-DSS Express**: Dirección del proyecto de cumplimiento de PCI-DSS, logrando la certificación oficial en tan solo 5 meses mediante controles estrictos de seguridad.
- **Roadmap de Ciberseguridad Ofensiva**: Diseño de la planificación estratégica (H2-2021 y Q1-2022) enfocada en el desarrollo y consolidación del equipo de seguridad ofensiva.
- **Integración de HSM en la Nube**: Gestión integral del proyecto de integración de HSM en la nube, garantizando un despliegue seguro y alineado con los estándares del negocio.
- **Creación de Red Team & CloudSec**: Reclutamiento, estructuración y dirección de los equipos de Red Team y Seguridad Cloud en colaboración directa con la dirección ejecutiva (C-level).
- **Sprint Planning y Gestión Ágil**: Planificación y priorización de las actividades del equipo en cada ciclo de sprint, asegurando una ejecución en tiempo y forma.
- **Evaluación de Herramientas y Pentesting de APIs**: Conducción de pentests orientados a APIs, identificación de vulnerabilidades críticas y liderazgo en la compra de herramientas de seguridad.
- **Entrenamiento en Desarrollo Seguro & WAF**: Diseño de entrenamientos técnicos en codificación segura para el equipo de desarrollo y optimización de reglas de WAF para mitigar riesgos web.
- **Automatización en la Nube y CI/CD**: Despliegue de soluciones automatizadas en AWS (Lambdas, Security Hub, AWS Config) e integración automática de SAST/DAST en los pipelines.

Cyber Security Tech Lead

Feb 2020 - Abr 2021

Naranja X

Buenos Aires, Argentina

- **Pruebas de Penetración Avanzadas**: Ejecución de pentests dirigidos a plataformas cloud, aplicaciones móviles y APIs REST en entornos de microservicios backend.
- **Controles en Infraestructura AWS & Azure**: Evaluación y diseño de controles avanzados de seguridad para nubes públicas alineados con las mejores prácticas internacionales.
- **Gobernanza de Seguridad**: Conducción de auditorías de seguridad en contenedores (Docker/Kubernetes) y administración del ciclo de vida de vulnerabilidades.
- **Gobernanza de Código y Automatización de SecOps**: Desarrollo y despliegue de herramientas de automatización de operaciones de seguridad y revisiones de código de seguridad.
- **Integración CI/CD**: Automatización del despliegue de herramientas SAST/DAST integradas de forma nativa en pipelines de GitLab CI.

Senior SecOps Specialist

Nov 2019 - Feb 2020

gA

Buenos Aires, Argentina

- **Evaluación y Controles Cloud**: Diseño e implementación de controles de ciberseguridad sobre infraestructuras multinube en AWS y Azure.
- **Respuesta ante Incidentes y Forense**: Automatización de respuestas operativas ante alertas de seguridad y ejecución de análisis forenses e investigaciones de incidentes.
- **Análisis de Amenazas**: Provisión de análisis profundos de amenazas y vulnerabilidades, generando recomendaciones técnicas para mitigar riesgos.
- **Seguridad en SDLC y Pentesting**: Integración de controles técnicos de seguridad en el ciclo continuo de software y conducción de pruebas de intrusión tácticas.

SOC Engineer

Ene 2019 - Nov 2019

Despegar.com

Buenos Aires, Argentina

- **Diagnóstico de Dispositivos**: Diagnóstico, soporte y resolución de fallas en consolas y servidores de antivirus, sensores IDS/IPS y escáneres de vulnerabilidades.
- **Afinación Avanzada de Alertas SIEM**: Tuning y calibración fina de reglas de correlación en un SIEM basado en Big Data (AV, NIDS, HIDS, EDR) para reducir falsos positivos.
- **Automatización Operativa**: Diseño y desarrollo de scripts para automatizar tareas repetitivas de operaciones de ciberseguridad corporativa.
- **Análisis de Vulnerabilidades & Playbooks**: Provisión de recomendaciones técnicas de seguridad a líderes de área y redacción de playbooks y procedimientos estándar (SOP) para el SOC.

Senior Security Consultant

Ago 2017 - Nov 2018

BTR Consulting

Gran Buenos Aires, Argentina

- **Consultoría y Auditoría de Nube**: Diagnósticos de seguridad y análisis de GAP sobre infraestructuras cloud en AWS y Azure.
- **Hacking Ético y Pentesting**: Conducción de simulaciones de ataques en aplicaciones web y móviles, escaneo de vulnerabilidades y campañas controladas de Phishing.
- **Forense y Hardening**: Investigación forense digital de incidentes y ejecución de hardening y aseguramiento técnico de servidores.
- **Automatización de Procesos**: Automatización de tareas de auditoría empleando herramientas de IaC (CloudFormation, Ansible, Jenkins).

Server and Network Security Manager

Ago 2014 - Jul 2017

Banco Bicentenario del Pueblo

El Rosal, Caracas, Venezuela

- **Gobernanza y SGSI**: Definición, planeación y supervisión de las políticas de ciberseguridad, lineamientos y estándares corporativos del Sistema de Gestión de Seguridad de la Información (SGSI).
- **Liderazgo del Equipo de Incidentes (IRT)**: Dirección del equipo técnico encargado de la contención, análisis y mitigación de incidentes críticos de seguridad bancaria.
- **Dirección de Pentesting**: Coordinación y planificación del equipo de seguridad ofensiva para evaluar la postura interna del banco y mitigar brechas de seguridad.
- **Cultura de Seguridad**: Dirección de programas y talleres técnicos de concientización y Awareness en ciberseguridad para todo el personal de la institución financiera.

Information Security Specialist

Mar 2011 - Jul 2014

Banco del Tesoro

Caracas, Venezuela

- **Resiliencia de Servidores y Cajeros (ATMs)**: Ejecución de hardening técnico sobre servidores y sistemas transaccionales de cajeros automáticos contra vectores de ataque físicos y lógicos.
- **Monitoreo y Correlación (SIEM)**: Implementación, administración y soporte operativo de la herramienta de correlación de eventos OSSIM.
- **Gobernanza de Identidades**: Administración y gestión de políticas de acceso y control de identidades mediante Active Directory.
- **Seguridad Perimetral y Pentesting**: Administración técnica de firewalls perimetrales, IPS y soluciones WAF de Cisco y Fortinet. Conducción de pentests tácticos y de ethical hacking sobre los sistemas del banco.

Senior Technology Specialist

Abr 2007 - Dic 2010

Banco de Venezuela

Caracas, Venezuela

- **Soporte y Optimización**: Soporte técnico y optimización de servidores Windows críticos de negocio en ambientes productivos.
- **Despliegue de Servidores**: Instalación y configuración de software base para el aprovisionamiento seguro de servidores de desarrollo y pruebas.
- **Liderazgo Técnico de Proyectos**: Dirección técnica de iniciativas críticas de infraestructura de TI coordinando con equipos multidisciplinarios.
- **Active Directory & Antivirus**: Administración del directorio corporativo (Active Directory 2003) y consolas centralizadas de antivirus corporativo.