LUCAS MORRONE

ESPECIALISTA EN CIBERSEGURIDAD OPERATIVA, SOC/DFIR, INFRAESTRUCTURA SEGURA Y CONTINUIDAD

Buenos Aires, Argentina, CP 2804
+54 9 1530 556594
lucasgenaromorrone@gmail.com
linkedin.com/in/lucas-genaro-morrone

PERFIL PROFESIONAL

Especialista en ciberseguridad operativa para infraestructura empresarial, SOC/DFIR, redes seguras y continuidad en entornos industriales, logísticos y corporativos. Cuenta con experiencia en administración de firewalls, hardening Linux/Windows, monitoreo de redes, análisis de tráfico, respuesta a incidentes, análisis forense digital y protección de activos críticos. Posee trayectoria en liderazgo técnico de equipos SOC, reducción de ruido operacional, mejora de procesos de seguridad, implementación de backups 3-2-1 y soporte a clientes simultáneos con necesidades de continuidad, cumplimiento y disponibilidad.

EXPERIENCIA LABORAL

TEAM LEAD - ANALISTA DE INFRAESTRUCTURA Y SEGURIDAD DE REDES **2025 Actualidad**

SUMMA HS | Modalidad híbrida

- Liderazgo de un equipo técnico de tres analistas junior para gestionar infraestructura y seguridad de más de cinco clientes simultáneos, incluyendo filiales internacionales.
- Diseño, administración y mantenimiento de entornos de red con tecnologías MikroTik, Palo Alto, Cisco, Fortinet, Active Directory, VPN, DNS y DHCP.
- Ejecución de auditorías técnicas y tareas de hardening en sistemas Linux y Windows, incluyendo modificación de credenciales de fábrica, autenticación por llaves RSA y doble factor de autenticación.
- Despliegue de laboratorios SOC con Security Onion, Suricata y Elastic Stack para monitoreo de tráfico de red troncal, análisis de archivos PCAP y revisión técnica mediante Wireshark.
- Gestión de controles orientados a Active Directory Security, segmentación de red, hardening de servidores y reducción de superficie de ataque.
- Coordinación de migración por fin de vida de Windows 10 para 16 equipos físicos y 5 usuarios remotos, utilizando imágenes de Veeam Backup para preservar continuidad operativa sin tiempo de inactividad.
- Reemplazo de esquemas de copias en USB por servidores TrueNAS con políticas 3-2-1 y copias espejo, fortaleciendo la protección ante pérdida de datos, fallas críticas y escenarios de ransomware readiness.
- Reducción del volumen de eventos de seguridad a un promedio de 100 a 150 mensuales mediante listas blancas, filtros y ajuste de reglas, logrando que solo un 10% requiera revisión manual.
- Mejora del monitoreo y triage de eventos, disminuyendo ruido operacional y permitiendo mayor foco técnico en alertas relevantes para la continuidad del negocio.

FUNDADOR Y CONSULTOR PRINCIPAL DE SEGURIDAD **2022 Actualidad**

Secompilers Consulting | Remoto

- Prestación de servicios integrales de consultoría en ciberseguridad, cumplimiento y operaciones SOC para pequeñas y medianas empresas.
- Implementación de programas de seguridad desde cero, incluyendo gestión de privilegios, segmentación de red, hardening, monitoreo, backups y controles de continuidad.
- Ejecución de pruebas de penetración, evaluación de vulnerabilidades y actividades de Threat Hunting utilizando MITRE ATT&CK para identificar riesgos y fortalecer capacidades de detección.
- Integración y operación de plataformas de seguridad como Vicarius vRx y Security Onion, con foco en monitoreo, priorización de riesgos y respuesta ante incidentes.
- Aplicación de marcos ISO/IEC, NIST, ITIL y eTOM de acuerdo con el nivel de madurez tecnológica de cada organización.
- Realización de análisis forense digital mediante copias bit a bit de evidencia con FTK Imager y Cellebrite UFED, manteniendo cadena de custodia para respaldo legal y técnico.
- Desarrollo de automatizaciones para procesos operativos y de monitoreo, agilizando la detección de incidentes y reduciendo tareas manuales repetitivas.
- Elaboración de reportes técnicos y ejecutivos orientados a explicar riesgos, evidencias, prioridades de remediación e impacto sobre la operación.

ANALISTA DE INFRAESTRUCTURA WEB Y DESARROLLO **2021-2023**

Fobutec | México

- Administración y optimización de infraestructura web para sitios corporativos y plataformas de comercio electrónico.
- Desarrollo de herramientas internas mediante Node.js y Elixir para soporte operativo y mejora de procesos.
- Gestión de entornos de hosting, mantenimiento de servicios web y ejecución de auditorías enfocadas en rendimiento, seguridad básica y posicionamiento SEO.
- Capacitación a personal de desarrollo junior en lineamientos fundamentales de ciberseguridad, buenas prácticas técnicas y prevención de riesgos en ambientes web.
- Vinculación entre desarrollo, infraestructura y seguridad para reducir vulnerabilidades operativas y mejorar la estabilidad de servicios digitales.

CO-FUNDADOR **2017-2022**

CryptoFarm | Argentina

- Diseño y despliegue de granjas de infraestructura de minería de criptomonedas basadas en hardware GPU.
- Optimización del consumo eléctrico y mejora de la eficiencia de sistemas de refrigeración para sostener disponibilidad y rendimiento.
- Desarrollo de soluciones de automatización mediante scripting para monitoreo de disponibilidad, integración con wallets vía API y control de operación.
- Administración de hardware crítico, mantenimiento preventivo y resolución de fallas orientadas a minimizar interrupciones operativas.
- Gestión de infraestructura distribuida con foco en continuidad, eficiencia energética, automatización y monitoreo técnico.

FORMACIÓN ACADÉMICA

Licenciatura en Ciberdefensa | UNDEF | Finalización estimada: 2028

Tecnicatura en Redes y Seguridad de Servidores | TECLAB | 2025

Diplomatura en Penetration Testing | DDLR Security + UAI | 2024

COMPETENCIAS

Liderazgo e influencia: Capacidad para guiar equipos técnicos junior, promover la toma de acción proactiva, debatir directivas de forma constructiva y registrar aprendizajes para la mejora continua del equipo.

Resolución de eventualidades: Implementación de sistemas de alerta temprana, mantenimiento de hardware crítico y restablecimiento de servicios ante incidentes, fallas o necesidades operativas urgentes.

Toma de decisiones críticas: Análisis de costos, urgencias del negocio, criticidad técnica y requerimientos de seguridad para implementar soluciones alineadas al presupuesto y a la continuidad operativa.

Mejora de procesos: Identificación de tareas manuales y repetitivas para automatizarlas progresivamente, reducir tiempos de ejecución y sostener calidad técnica en operaciones de seguridad.

Adaptabilidad: Ajuste de estrategias de seguridad, redistribución de funciones y reestructuración técnica frente a cambios de infraestructura, migraciones a la nube o necesidades imprevistas del negocio.

HERRAMIENTAS, SISTEMAS Y CONOCIMIENTOS TÉCNICOS

Firewalls, redes y VPN: Fortinet, FortiGate, Palo Alto, PAN-OS, Cisco, MikroTik, RouterOS, VPN, DNS, DHCP, segmentación de red, redes seguras, monitoreo de tráfico, administración de perímetro.

SIEM, NSM y SOC: Security Onion, Elastic Stack, Suricata, Wireshark, análisis PCAP, SIEM, NSM, MITRE ATT&CK, Threat Hunting, Incident Response, detección, triage y reducción de falsos positivos.

Microsoft, servidores y hardening: Active Directory, Active Directory Security, Windows Server, Linux Hardening, Windows Hardening, Microsoft Azure Fundamentals, autenticación MFA, llaves RSA, gestión de privilegios.

DFIR y evidencia digital: FTK Imager, Cellebrite UFED, Magnet AXIOM, Physical Analyzer, Volatility, análisis de memoria, copias bit a bit, cadena de custodia, chain of custody, preservación de evidencia y reporte técnico.

Backup, continuidad y resiliencia: Veeam Backup, TrueNAS, políticas 3-2-1, copias espejo, BCP/DRP, continuidad operativa, ransomware readiness, recuperación ante fallas críticas y protección de información.

Virtualización y contenedores: Proxmox VE, VMware, VirtualBox, QEMU, Docker, Podman.

Cloud y scripting: Microsoft Azure, Python, Bash, TypeScript, Scala, Elixir, Node.js, automatización de procesos, integración vía API.

Marcos, cumplimiento y buenas prácticas: ISO/IEC, ISO 27001, NIST CSF, ITIL, ETOM, gestión de riesgos, evaluación de vulnerabilidades, controles de seguridad y mejora continua.

Base IT/seguridad de redes con proyección IT/OT: Conocimientos de seguridad de redes, segmentación, monitoreo y continuidad aplicables a entornos empresariales e industriales, con ruta de especialización orientada a IEC 62443, OT/ICS y seguridad de infraestructura crítica.

CURSOS Y CAPACITACIONES

- DFIR Forensic Analyst | LetsDefend | 2026
- Incident Responder | LetsDefend | 2026
- Threat Hunting | LetsDefend | 2026
- CRTA / CRTO | CyberWarFare Labs | 2025
- SOC Analyst | LetsDefend | 2025
- Cisco Networking Associate | Cisco | 2023
- Microsoft Azure Fundamentals | Microsoft Learn | 2023
- SysAdmin, Networking y Elixir | Platzi | 2023
- Backend con JS/TS | CoderHouse | 2022
- Bootcamp en Data Science | Henry | 2022

INFORMACIÓN ADICIONAL E IDIOMAS

Idiomas: Español: nativo | Inglés: avanzado, C1 - EF SET

Disponibilidad: Modalidad remota, híbrida o presencial.

Viajes: Disponibilidad para realizar viajes laborales.