



Karim Ledesma Haron

EXPERTO EN SEGURIDAD: LÍDER EN SOC & CSIRT & ETHICAL HACKING

T: 3518588146 | E: kharon.info@gmail.com | [Mi linkedin](#)

Para más detalles, consulta mi CVOnline: karimledesmaharon.github.io

Con más de 19 años en Seguridad Informática, he destacado en roles diversos, desde el diseño de arquitecturas robustas hasta liderar equipos de respuesta a incidentes. Mi experiencia está respaldada por certificaciones de élite. Como arquitecto de confianza digital, mi enfoque estratégico anticipa amenazas y ofrece soluciones innovadoras. Con dos décadas de experiencia, estoy listo para liderar en la batalla cibernética con maestría y habilidades inigualables.

CTO y Líder Técnico: Analista Sénior de SOC & CSIRT

UNIVERSIDAD SIGLO21/ 2019 - Presente

Trabajo como CTO (Chief Technology Officer) del grupo de analistas perteneciente al grupo de seguridad de la Universidad Siglo 21.

Entre las tareas que desempeño, destacaré las siguientes:

- Formo parte activa operativa en los equipos de Red Team, Blue Team y Cyber Intelligence.
- Diseño, desarrollo y ejecución de controles de seguridad de la información para SOC y CSIRT.
- Gestión y supervisión de las tareas del grupo. Presentación de mejoras e implementación de planes de formación para el grupo.
- Ejecución de procedimientos y parametrización de métricas para medir los SLAs y controlar la volumetría.
- Automatización de tareas y procedimientos propios del sector.
- Administración e implementación de SIEM (Alienvault, FortiSIEM).
- Gestión de Incidentes internos y externos.
- Análisis y gestión de alertas, monitoreo y reportes.
- Despliegue, gestión y administración de soluciones prevención DDOS Layer3-4 Layer7.
- Cloudflare -Incapsula - Peakflow (Arbor Networks).
- Gestión centralizada de Logs de Seguridad, generación de eventos y Alarmas automatizadas.
- NetFlow - Suricata NIDS.
- Unified Threat Management (UTM) (Fortinet 600-500-300 IPS-FW).
- Soporte Firewalls (Palo Alto, Fortigate, Forticlient EMS).
- Monitoreo Seguridad Perimetral (Fortinet Analyzer).
- Business Continuity Plan (Cloudflare CDN y Load Balancing)
- Administración y gestión de herramientas de tráfico de correo limpio gestión de la cuarentena y configuración de políticas. Office365.
- Administración de AV Kaspersky Security Center 12,13 y 14 & Defender.
- Patch Management - Vulnerability Managemet - Threat Risk Mgt.
- Ad Audit Plus ManageEngine.
- Auditoria de Active Directory.
- Manager PRO ManageEngine, ADManager, Remote Desktop.
- Session Management - Gestión de sesiones Root- Domain Admins.
- WAF (Web Application Firewall) Cloudflare.
- Gestión Logs vía ElasticSearch (Graylog-Kibana).
- Nessus, Rapid7.

CTO

GATES CONSULTING/ 2018-2023

Como estrategia de TI, alinee cuidadosamente las metas tecnológicas con los objetivos comerciales y empresariales. Mi liderazgo se refleja en la gestión y desarrollo del equipo de profesionales de TI, dirigiendo la evolución estratégica. Diseño planes y protocolos para la gestión eficaz de incidencias, priorizando un enfoque proactivo y la implementación estratégica de soluciones tecnológicas avanzadas. Mi responsabilidad incluye atraer y gestionar talento tecnológico, contribuyendo activamente a la dirección estratégica global de la empresa mediante un diálogo continuo con la Dirección General.

COORDINADOR IT

AUTOENTRADA S.A / 2019-2020

Como líder técnico en seguridad informática, mi enfoque primordial fue garantizar la estabilidad y eficiencia de los entornos informáticos, destacando en la gestión proactiva de incidentes y liderando equipos. Encabecé la gestión integral de tecnologías de trabajo, desde el ciclo de vida de dispositivos hasta la optimización de la experiencia de usuario. Además, desempeñé un papel crucial en la eficiente gestión del servicio y el establecimiento de relaciones con proveedores especializados. Coordiné equipos para la administración de ambientes y servicios, asegurando la sincronización de esfuerzos y el cumplimiento de objetivos en un entorno tecnológico avanzado y resistente.

ESPECIALISTA EN SEGINFO Y SYSADMIN DE INFRAESTRUCTURA

MINISTERIO PUBLICO FISCAL / 2012-2019

Como especialista en seguridad informática, lideré proyectos clave para fortalecer entornos informáticos, centrándome en la configuración de redes y la protección de su integridad. Gestioné operaciones de seguridad en telefonía fija y móvil con políticas protectoras. Construí infraestructuras robustas, destacando en Routing & Switching con tecnologías de Cisco, HP y MikroTik. Implementé soluciones críticas, como Firewalls y Cisco ASA, impulsando la adopción de virtualización y liderando la migración estratégica del centro de datos. Mi rol especializado involucró la guía de acciones, ejecución de estrategias y la impartición de capacitaciones, consolidando una cultura centrada en la resiliencia técnica y la protección contra amenazas cibernéticas..

PROFESIONAL DE SEGURIDAD IT Y SOPORTE IT

TELECOM ARGENTINA / 2004-2013

En mi trayectoria en Telecom, asumí un rol integral como especialista en seguridad informática y soporte IT. Implementé medidas específicas para proteger la integridad de los sistemas y brindé asistencia para mantener la operatividad continua. En servicios de Última Milla, realicé acciones operativas, instalación y mantenimiento, contribuyendo a la calidad del servicio. Dirigí la configuración de enlaces dedicados y equipos, optimizando el rendimiento de las redes. Mi experiencia incluyó la instalación y aseguramiento de redes de datos e Internet, fortaleciendo la robustez de los servicios en Telecom con un compromiso constante con la excelencia operativa y la seguridad informática.

UES21: Ing. José Antúnez - Cargo: Gerente de tecnología - Contacto: joseantunez@ues21.edu.ar

GATESCONSULTING: Lic. Carmen Ahumada - Cargo: Director de recursos humanos y relaciones laborales - Contacto: 3518670628

MINPUBFIS: Pablo Gerez - Cargo: Coordinador de área informática - Contacto: pgerez@mpfsde.gob.ar

TECO: Ing. Daniel Iriarte - Cargo: Gerente - Contacto: diriarte@teco.com.ar

UTN, FACULTAD REGIONAL SANTA FE: Técnico universitario en software libre finalizado / Ing. En Sistema (en curso)

CERTIFICACIONES / CURSO RELAVENATES: OSCP (Offensive Security Certified Professional) / OSWP (Offensive Security Wireless Professional) / CEH (Certified Ethical Hacker) / CPHE (Certified Professional Hacker Expert) / CISSP (Certified Information Systems Security Professional) / CompTIA Security+ / CCNA / Diplomatura UTNBA en Seguridad de la Información, UTNBA Ethical Hacking.

Me especializo en el ámbito de seguridad informática y cuento con experiencia en:

Políticas ISO/IEC 27001:2013	Hacking Ético	Metodologías OWASP	OWASP MOBILE	OSSTMM
Criptografía	OpenSAMM	Análisis de Vulnerabilidades	IoT security OWASP	Web Application Forensics
Hacking Developer	Certificaciones Especializadas	Endpoint Security	Seguridad en la Nube	Seguridad de Redes
Gestión de Incidentes	Blockchain Security	Gestión de Identidad y Acceso	Auditoría de Seguridad	Investigación de Amenazas
Análisis de Tráfico	Desarrollo Seguro de APIs	Resiliencia Cibernética	Auditoría de Cumplimiento	Evaluación de Riesgos de Seguridad
Seguridad en Sistemas Críticos	Seguridad en Entornos Virtuales	Monitoreo de Eventos de Seguridad	Protección de Datos Personales	Seguridad en Entornos de Teletrabajo
Seguridad en Dispositivos Móviles	Seguridad en Sistemas Embebidos	Protección contra Ataques de DDoS	Protección de la Privacidad en Línea	Pruebas de Penetración
Protección contra Amenazas Internas	Seguridad en Sistemas de Pagos	Cumplimiento de Normativas	Seguridad en Sistemas Operativos	Seguridad en Transacciones Electrónicas
Seguridad en Redes Inalámbricas	Seguridad de Datos Biométricos	Seguridad en Servidores	Seguridad en Redes (WAN)	NOC/SOC

Hacking	Forense	SecurityPolicy	Cloud	Auditoría
DefensaOfensa	Penetración	ThreatHunting	Firewalls	EndpointSecurity
Cryptography	QA Security	S.O & DBA	Compliance	ThreatAnalysis
Risk Mgmt.	Incident Resp.	DataProtection	AccessControl	Patch Mgmt.
ThreatMitigation	Programación	Redes	MalwareAnalysis	MobileSecurity
IAM	DevSecOps	Virtualization	CrisisManagement	WebSecurity
SecurityEducation	SecurityMetrics	SecurityGovernance	SecurityCompliance	SecurityOperations
Comunicación Efectiva	Trabajo en Equipo	Resolución de Problemas	Adaptabilidad	Pensamiento Crítico
Ética Profesional	Gestión del Tiempo	Atención al Detalle	Toma de Decisiones	Liderazgo
Colaboración	Empatía	Creatividad	Resiliencia	Capacidad de Aprendizaje
Responsabilidad	Innovación	Autodisciplina	Gestión del Estrés	Proactividad
Pensamiento Estratégico	Negociación	Conciencia Cultural	Facilitación	Analítico