KARIM LEDESMA HARON

Experto en Ciberseguridad | SOC, CSIRT & Ethical Hacking

karimledesmaharon@gmail.com (+54 9) 3518588146

Córdoba, Argentina https://linkedin.com/in/kharon

karimledesmaharon.github.io

Perfil

Especialista en ciberseguridad con perfil técnico-estratégico y experiencia liderando SOC/CSIRT. Foco en respuesta a incidentes, reducción de riesgos y protección de activos críticos, con visión proactiva y colaborativa.

Experiencia profesional

Chief Information Security Officer (CISO) | Líder de Ciberseguridad | Nov2024 - Actual

Disal S.A

Responsable de la estrategia integral de ciberseguridad, combinando liderazgo operativo, gestión de riesgos, automatización y monitoreo avanzado. Trabajo transversalmente con equipos técnicos de seguridad/infraestructura, alineando tácticas ofensivas, defensivas y de análisis en un enfoque unificado.

Principales logros y responsabilidades:

Gestión estratégica y liderazgo

- Coordinación de equipos técnicos seguridad e infraestructura global, definición de SLAs, procedimientos operativos y programas de formación continua.
- Diseño e implementación de controles de seguridad alineados a estándares internacionales (NIST, ISO 27001).
- Análisis y presentación de reportes ejecutivos/técnicos para la toma de decisiones estratégicas.

Monitoreo, detección y respuesta

- Administración avanzada de SIEM (Wazuh): correlación de eventos, generación de alertas y gestión de incidentes.
- Detección de amenazas con Suricata, NetFlow, ElasticSearch y Graylog.
- Gestión de seguridad perimetral con Fortinet Manage, FortiGate, Mikrotik, Firewalls UTM y WAF Cloudflare.

Automatización y operaciones

- Automatización de procesos con scripting, mejorando tiempos de detección y respuesta.
- Administración de soluciones AV (NOD32) y sistemas de gestión de parches (WSUS).
- Auditorías técnicas (ADAudit Plus) y control de accesos privilegiados (Domain Admins, Root).

Infraestructura y continuidad operativa

- Gestión de entornos virtuales (vCenter, Xenserver), respaldos con Veeam y balanceo de carga con Cloudflare.
- Administración de políticas de seguridad en Office 365, antispam, antiphishing y cuarentenas.
- Soporte a soluciones de monitoreo y gestión: ManageEngine ADManager, Remote Desktop y otras.
- Gestión integral de servicios en Microsoft Azure, incluyendo Azure AD, políticas de seguridad, automatización con PowerShell, monitoreo con Log Analytics y despliegue de arquitecturas escalables y seguras.

Capacidad de respuesta y mejora continua

- Gestión de incidentes de seguridad desde la detección hasta su resolución.
- Implementación de soluciones anti-DDoS (Cloudflare, Incapsula, Arbor Peakflow) en capas 3, 4 y 7.
- Desarrollo de dashboards personalizados en Grafana y Zabbix para análisis proactivo de seguridad.

CISO y Líder Técnico – Analista Sénior de SOC & CSIR | Ene2018 - Dic2024

Universidad Empresarial Siglo 21

Lideré la estrategia de ciberseguridad institucional coordinando equipos de seguridad ofensiva, defensiva y de inteligencia dentro de entornos SOC/CSIRT. Impulsé mejoras operativas y desarrollé programas de formación técnica, elevando la madurez del equipo y reduciendo tiempos de respuesta ante incidentes.

Automatizé procesos críticos y definí KPIs para la gestión eficiente de grandes volúmenes de eventos, optimizando el monitoreo con plataformas SIEM como Splunk y QRadar. Gestioné incidentes complejos y desplegué protecciones multicapa contra DDoS con tecnologías como Akamai y Radware.

Administré infraestructuras de análisis de tráfico y logging (Zeek, Suricata, ELK Stack), junto con firewalls empresariales (Check Point, Cisco Firepower), soluciones endpoint (CrowdStrike, Microsoft Defender) y seguridad perimetral avanzada (F5 BIG-IP, AWS Shield).

Implementé políticas de seguridad en Google Workspace, gestioné antivirus centralizados (Trend Micro), escaneos de vulnerabilidades (Qualys), auditorías de AD (SolarWinds, BeyondTrust) y protección de aplicaciones web mediante WAFs como AWS WAF e Imperva.

CTO – Chief Technology Officer | Ene2018 - Dic2024

Gates Consulting

Lideré la estrategia tecnológica de la empresa, alineando los objetivos de TI con la visión de negocio para potenciar la eficiencia operativa, la innovación y el crecimiento sostenible.

Dirigí la evolución del área tecnológica, conformando y gestionando un equipo de alto rendimiento.

Diseñé planes de mejora continua, protocolos de respuesta ante incidentes y procesos orientados a la prevención, integrando soluciones avanzadas en seguridad, infraestructura y servicios digitales.

Participé activamente en decisiones clave junto a la Dirección General, aportando visión tecnológica al planeamiento estratégico de la empresa. Asimismo, lideré la atracción, desarrollo y retención de talento IT, consolidando una cultura de mejora continua y excelencia técnica.

Coordinador IT | Ene2019 - Oct2020

Autoentrada S.A

Coordiné la infraestructura tecnológica de la compañía, liderando equipos técnicos con foco en la continuidad operativa, seguridad y experiencia de usuario.

Implementé procesos de gestión proactiva de incidentes, asegurando la estabilidad de entornos productivos y optimizando el ciclo de vida de dispositivos.

Establecí relaciones con proveedores especializados y gestioné servicios críticos, garantizando el cumplimiento de SLA y la eficiencia operativa del área IT.

Especialista en seguridad informática & sysadmin | Nov2011 - Ene2019

Ministerio Público Fiscal

Lideré proyectos de fortalecimiento de la infraestructura tecnológica del MPF, con foco en seguridad informática, redes y virtualización.

Implementé políticas de protección para entornos de telefonía fija/móvil, configuré firewalls (Cisco ASA), y lideré la migración estratégica del centro de datos.

Construí redes de alta disponibilidad con tecnologías Cisco, HP y MikroTik. Promoví una cultura de resiliencia técnica mediante capacitaciones internas y gestión operativa alineada a estándares de ciberseguridad.

Profesional de seguridad IT y soporte técnico | Mar2004 - Dic2013

Telecom Argentina

Desarrollé tareas de seguridad y soporte IT en entornos críticos, implementando medidas de protección en redes y sistemas de usuarios finales. Ejecuté instalaciones, mantenimiento y aseguramiento de enlaces dedicados y redes de datos, garantizando calidad en los servicios de Última Milla. Mi enfoque operativo y preventivo contribuyó al fortalecimiento de la infraestructura técnica, con foco en continuidad de servicio y seguridad.

Educación

03/2017 – En curso **Ingeniería en Sistemas de Información**
Santa Fe, Argentina *UTN, FACULTAD REGIONAL SANTA FE*

Habilidades

Liderazgo efectivo y motivación de equipos | Comunicación clara y asertiva | Resolución ágil de problemas | Pensamiento estratégico y proactivo | Adaptabilidad y manejo del cambio | Ética profesional y compromiso | Enfoque orientado a resultados | Trabajo colaborativo interdisciplinario | Capacidad para tomar decisiones bajo presión | Orientación al aprendizaje continuo

Logros

Disal S.A.
Reducción del 93,4 % en intentos de ataque mediante el diseño e implementación de una arquitectura de defensa en profundidad. Se optimizaron políticas de firewall, se integraron soluciones UTM y WAF, y se fortaleció el monitoreo con un SIEM centralizado, logrando bloquear ataques en capas 3, 4 y 7.

Eliminación total de incidentes de malware o ransomware durante 60 meses consecutivos. Este resultado se alcanzó mediante un plan integral que combinó segmentación de red, backups automatizados, capacitación continua en seguridad para el personal y la implementación de controles avanzados de EDR.

Mejora sostenida en la gestión de incidentes y automatización de procesos críticos, logrando una mayor eficiencia operativa y el cumplimiento sistemático de los SLA del área.

Certificaciones

OSCP - OSWP - CEH - CPHE - CISSP - CompTIA Security+ - CCNA - Diplomatura en Seguridad de la Información - Ethical Hacking

Referencia actual

Ing. Jose Antunez, *Gerente de sistemas,* Disal S.A
jantunez@grupodisal.com.ar, (+54 9) 351 326-7491

Experiencia Internacional en Ciberseguridad

• Más de 600 horas dedicadas a la resolución de CTFs y desafíos de hacking en plataformas líderes como Hack The Box, TryHackMe, CTFtime, y VulnHub.
• Top 5 de participantes en eventos de CTF en Hack The Box y TryHackMe, con un enfoque en pruebas de penetración, explotación de vulnerabilidades y análisis forense.
• Participante regular en competiciones de CTF organizadas por conferencias internacionales de ciberseguridad, obteniendo menciones destacadas por su desempeño.
• DEFCON (Las Vegas, 2023): Participante y competidora en el "Capture The Flag Contest", contribuyendo en la resolución de desafíos de red y seguridad web.