KARIM LEDESMA HARON

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

(+54 9) 3518588146
karimledesmaharon@gmail.com
Córdoba, ARG
Mi Linkedin | CV Online

RESUMEN

Apasionado de la Ciberseguridad y el Hacking, Máster en Ciberseguridad, Offensive Security Team Lead, Docente de Ciberseguridad, más de 20 años trabajando en Tecnologías de la Información, Cybersecurity Speaker, CTF Player.

EXPERIENCIA PROFESIONAL

CISO Y LÍDER CYBERSEGURIDAD
Grupo DISAL S. A **NOV 2024 - Presente**
Trabajo como CISO (Chief Information Security Officer) y Líder de Ciberseguridad.

Algunas de mis tareas y responsabilidades:

- Participación en equipos operativos de Red Team, Blue Team y Cyber Intelligence, integrando estrategias ofensivas, defensivas y de análisis de amenazas.
- Diseño, implementación y optimización de controles de seguridad para entornos SOC y CSIRT, alineados a estándares internacionales.
- Coordinación y supervisión de equipos técnicos, promoviendo la mejora continua e implementación de programas de formación especializados.
- Ejecución de procedimientos operativos y definición de métricas de rendimiento (SLAs) para la medición de volumetría y eficiencia del equipo.
- Automatización de tareas clave mediante scripting y herramientas específicas del sector, mejorando tiempos de respuesta y detección.
- Administración avanzada de SIEM como AlienVault y FortiSIEM, incluyendo correlación de eventos, generación de alarmas y gestión de casos.
- Gestión integral de incidentes de seguridad, internos y externos, desde su detección hasta su contención y resolución.
- Análisis proactivo de alertas de seguridad, monitoreo de eventos y elaboración de reportes ejecutivos y técnicos.
- Despliegue y gestión de soluciones anti-DDoS en capas 3, 4 y 7, utilizando tecnologías como Cloudflare, Incapsula y Peakflow (Arbor Networks).
- Administración centralizada de logs, generación de eventos automatizados y definición de políticas de respuesta.
- Implementación y análisis de tráfico con NetFlow y NIDS como Suricata, para detección de amenazas en la red.
- Gestión de entornos UTM Fortinet con configuración avanzada de políticas IPS y firewall.
- Soporte y configuración de firewallsNXG (Palo Alto, FortiGate) y soluciones de endpoint como FortiClient EMS.
- Monitoreo de la seguridad perimetral utilizando herramientas como Fortinet Analyzer.
- Desarrollo y mantenimiento de planes de continuidad operativa mediante soluciones como Cloudflare CDN y Load Balancing.
- Administración de políticas de seguridad de correo electrónico en Office 365, gestión de cuarentenas y filtros antispam/antiphishing.
- Gestión de soluciones antivirus centralizadas: Kaspersky Security Center, Microsoft Defender, Sophos y NOD32.
- Implementación de programas de gestión de parches, vulnerabilidades y riesgos (Nessus, Rapid7).
- Auditorías técnicas con AdAudit Plus, revisión de accesos y monitoreo de cambios críticos en Active Directory.
- Administración de herramientas de gestión y monitoreo: ManageEngine (ADManager, Remote Desktop, Manager PRO).
- Control y monitoreo de sesiones privilegiadas (Root, Domain Admins), con enfoque en trazabilidad y cumplimiento.
- Administración de WAF Cloudflare, configurando políticas para protección de aplicaciones web.
- Gestión avanzada de logs y dashboards en ElasticSearch, Graylog y Kibana.
- Administración y monitoreo avanzado de infraestructuras virtuales en vCenter, junto con gestión de seguridad utilizando Veem Backup.

Referencia:
Ing. Jose Antunez
Gerente de sistemas
jose.antunez@ues21.edu.ar
(+54 9) 351 326-7491

KARIM LEDESMA HARON

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

(+54 9) 3518588146
karimledesmaharon@gmail.com
Córdoba, ARG
Mi Linkedin | CV Online

Entre las tares que desempeño, destacó los logros:

Reducción del 93.4% en intentos de ataque mediante una nueva arquitectura de defensa en profundidad, optimizando políticas de firewall, integrando soluciones UTM y WAF, y fortaleciendo el monitoreo con un SIEM centralizado. Este enfoque permitió bloquear ataques en las capas 3, 4 y 7, mejorando la seguridad general de la organización.	Eliminación total de incidentes de malware o ransomware en los últimos 60 meses mediante un plan integral que incluyó segmentación de red, copias de seguridad automatizadas, formación en seguridad para el personal y controles avanzados de EDR. Esto fortaleció la resiliencia de la organización, evitando pérdidas financieras y la interrupción de operaciones críticas.

Otros logros incluyen mejoras continuas en la gestión de incidentes, optimización de procesos de automatización, y capacitación del equipo para alcanzar altos niveles de eficiencia operativa y cumplimiento de SLA.

CISO Y LÍDER TÉCNICO: ANALISTA SÉNIOR DE SOC & CSIRT
UNIVERSIDAD EMPRESARIAL SIGLO21 | **2018-2024**
En este puesto integré y coordiné equipos de seguridad ofensiva, defensiva y ciberinteligencia dentro de entornos SOC y CSIRT, liderando mejoras operativas y programas de formación técnica. Automatizé procesos críticos, definí KPIs y optimicé el análisis de grandes volúmenes de eventos de seguridad mediante plataformas SIEM como Splunk y IBM QRadar. Gestioné incidentes complejos, implementé protecciones multicapas contra ataques DDoS con Akamai y Radware, y administré infraestructuras de monitoreo y logging con Zeek, Suricata y ELK Stack. Cuento con experiencia en administración de firewalls Check Point y Cisco Firepower, soluciones endpoint como CrowdStrike y Microsoft Defender, y en seguridad perimetral con F5 BIG-IP y AWS Shield. Además, gestioné políticas de correo en Google Workspace, antivirus centralizados como Trend Micro, herramientas de gestión de vulnerabilidades como Qualys, y auditorías de Active Directory utilizando SolarWinds y BeyondTrust, complementando la protección de aplicaciones críticas con WAFs de AWS y Imperva.

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

CTO
GATES CONSULTING | **2018-2023**
Como estratega de TI, alineo 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.

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.

KARIM LEDESMA HARON

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

(+54 9) 3518588146
karimledesmaharon@gmail.com
Córdoba, ARG
Mi Linkedin | CV Online

EDUCACION Y CERTIFICACIONES

Técnico universitario en software libre finalizado | Ing. En Sistema (en curso).
UTN, FACULTAD REGIONAL SANTA FE: **Ener 2013**

Certificaciones relevantes
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 (Cisco Certified Network Associate)
Diplomatura en Seguridad de la Información - UTN Buenos Aires (UTNBA)
UTNBA Ethical Hacking - UTN Buenos Aires (UTNBA)

Experiencia en CTF y Hacking:

- Más de 500 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.

Participación en conferencias internacionales:

- DEFCON (Las Vegas, 2023): Participante y competidora en el "Capture The Flag Contest", contribuyendo en la resolución de desafíos de red y seguridad web.