XDR GESTIONADO (MXDR) — POWERED BY CROWDSTRIKE FALCON

POWERED BY CROWDSTRIKE

ThreatDefend™

«Nuestra tecnología. Nuestro SOC.»

CrowdStrike Falcon — desplegado, configurado y gestionado íntegramente por el SOC 24/7 de Vijilan. Contención activa desde el primer día, en todos los tiers.

El diferenciador que cierra ventas: el ITDR completo se incluye desde Essential — dark web, viaje imposible, MFA-fatigue, BEC, abuso de OAuth y movimiento lateral, desde el primer día. Ningún competidor lo hace.

La regla de oro: un cliente usa ThreatRespond™ o ThreatDefend™, nunca ambos. ¿Conserva su EDR? ▒ ThreatRespond™. ¿Quiere CrowdStrike o no tiene EDR? ▒ ThreatDefend™.

POR QUÉ THREATDEFEND™

CrowdStrike Falcon EDR + NGAV, totalmente gestionado
Sin necesidad de experiencia en CrowdStrike por tu parte ni del cliente. Falcon es la plataforma en la que confía más del 60% del Fortune 500.

El SOC actúa en todos los tiers
Aislamiento de equipos, deshabilitación de cuentas y bloqueo de IPs disponibles desde Essential (un nivel de protección de partida superior al de ThreatRespond™ Essential).

ThreatLog™ SIEM incluido
Sin límites de datos, powered by CrowdStrike LogScale.

Dos equipos de caza independientes en Premium
Threat hunting proactivo del SOC de Vijilan y CrowdStrike OverWatch, con metodologías y fuentes de inteligencia distintas sobre el mismo entorno.

TIERS — PROGRESIÓN DE FUNCIONES · PRECIOS EN EL PORTAL DE PARTNERS

Essential	CrowdStrike Falcon EDR + NGAV · ITDR completo desde el primer día · Monitorización de AD + Entra ID + M365 · Monitorización de credenciales en dark web · ThreatLog™ SIEM · 90 días activo / 7 años de archivo
▒ Advanced	Todo lo de Essential · Falcon Discover (descubrimiento de activos) · Falcon Spotlight (vulnerabilidades sin escaneo) · Superficie de ataque externa (Falcon Exposure) · SLA de respuesta del SOC de 15 minutos · ThreatAssess™ — prueba gratuita de 60 días
Premium	Todo lo de Advanced · Threat hunting proactivo del SOC de Vijilan · Caza de élite de CrowdStrike OverWatch (doble equipo) · Evidencias de auditoría CMMC L2 + SOC 2 · Analista concierge asignado
Elite (por invitación)	Todo lo de Premium · Precios personalizados por endpoint/usuario · Informe mensual de inteligencia de amenazas · SLA y ruta de escalado a medida · Informes personalizados · Retención de logs ampliada

THREATASSESS™ — VERLO TODO ANTES DE COMPROMETERTE

Evaluación en vivo de 60 días con todos los módulos de CrowdStrike Falcon excepto Complete (gratis en Advanced+). Seis dominios: Endpoint · Identidad e ITDR · Vulnerabilidades · Exposición · Seguridad cloud · Inteligencia global de amenazas. Informe escrito completo al día 60 — tuyo pase lo que pase.

EL ECOSISTEMA

ThreatLog™ — SIEM sin límites de datos (CrowdStrike LogScale).
ThreatAssess™ — evaluación completa de 60 días (Advanced+).
ThreatContain™ — contención activa del SOC, en todos los tiers.

ThreatSensor™ — logs on-prem (Cribl Stream), compatible con air-gap.
Vijilan Guard™ — NFR gratuito para probar antes el SOC sobre tu propio equipo.

SOC 2 Type 2 · ISO 27001 · CrowdStrike CPSP · Exclusivo de canal — nunca venta directa

Lanza una evaluación ThreatAssess™ de 60 días — partners@vijilan.com · vijilan.com/partners