XDR GESTIONADO INSIGNIA — AGNÓSTICO DE FABRICANTE

ThreatRespond™

«Tus herramientas. Nuestro SOC.»

Envolvemos el SOC 24/7 de Vijilan alrededor del EDR que tus clientes ya utilizan. Sin sustituciones. Sin migraciones. Nuestros analistas no solo avisan: actúan.

84%
de los MSP están desbordados por las alertas de seguridad

1,2 M$
coste anual de montar un SOC 24/7 propio

60%
de las pymes cierran en los 6 meses siguientes a una brecha

CÓMO FUNCIONA — OTROS AVISAN, NOSOTROS ACTUAMOS

01 · Detectar
Monitorización 24/7 de los 6 dominios de seguridad por el SOC de Vijilan.

02 · Investigar
Un analista humano revisa cada alerta: nada de flujos puramente automáticos.

03 · ThreatContain™
El SOC actúa directamente: deshabilita cuentas comprometidas, aísla equipos, bloquea IPs maliciosas, elimina reglas de reenvío de correo.

04 · Informe de resolución
Entregado a ti, con tu marca. Tiempo medio de contención: menos de 15 minutos.

POR QUÉ THREATRESPOND™

Agnóstico de fabricante
Funciona con cualquier EDR existente: CrowdStrike, SentinelOne, Microsoft Defender, Carbon Black, Cortex XDR, Cylance, Sophos Intercept X, Malwarebytes.

ThreatLog™ SIEM incluido en todos los tiers
Powered by CrowdStrike LogScale. Sin límites de datos, sin tarifas por GB, nunca. 90 días en almacenamiento activo / 7 años de archivo.

White-label desde el primer día
Portal, informes, alertas y tickets de PSA con tu marca. Tus clientes nunca ven el nombre Vijilan.

ITDR completo
Detección de BEC, viaje imposible, MFA-fatigue, abuso de tokens OAuth, movimiento lateral y monitorización de credenciales en la dark web.

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

Essential	El SOC asesora: detecta y documenta, tu equipo actúa. Overlay sobre cualquier EDR · Monitorización de AD + Entra ID + M365 · ThreatLog™ SIEM · Ingesta de logs de red/firewall · Marcos de cumplimiento · 90 días activo / 7 años de archivo
Advanced	El SOC actúa. Todo lo de Essential · ThreatContain™ · ITDR completo + monitorización dark web · Cobertura de Okta + Google Workspace · Detección de MFA-fatigue y movimiento lateral · 20 análisis ThreatAssess™/mes
Premium	El SOC actúa + caza proactiva. Todo lo de Advanced · Threat hunting proactivo del SOC de Vijilan · Gestión de superficie de ataque externa (EASM) · Detección personalizada + ingeniería de parsers · Evidencias de auditoría CMMC L2 + SOC 2 · Analista concierge asignado
Elite	El SOC actúa + equipo concierge. Todo lo de Premium · Informe mensual de inteligencia de amenazas · SLA y ruta de escalado personalizados · Informes a medida · Retención de logs ampliada · Línea de soporte directa prioritaria

EL ECOSISTEMA

ThreatLog™ — SIEM sin límites de datos (CrowdStrike LogScale).
ThreatContain™ — contención activa del SOC (desde Advanced).
ThreatSensor™ — logs on-prem (Cribl Stream), compatible con air-gap.

ThreatAssess™ — evaluación de plataforma completa (desde Advanced).
Vijilan Guard™ — NFR gratuito: 25 lic. Essential / 100 lic. Advanced, 90 días, 0 €.

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

Ve el SOC en acción sobre tu propio equipo — solicita Vijilan Guard™ en vijilan.com/partners

Cobertura de cumplimiento: HIPAA, PCI DSS, NIST CSF, CMMC 2.0 (entrada en vigor nov. 2026), SOC 2. · partners@vijilan.com · +1 (954) 334-9988 · vijilan.com