OPTI
Security Operations

OPTI
tecnologías que dan valor

SEC
SERVICIOS DE CIBERSEGURIDAD

AI-DRIVEN | MICROSOFT NATIVE | 24x7

OPTI Intelligent SOC 24x7

AI-Driven Security Operations powered by

Microsoft Sentinel & Defender XDR

> De monitoreo reactivo a resiliencia cibernética continua impulsada por IA.

Propuesta Comercial
Ejecutiva

Febrero 2026

El Nuevo Panorama

El entorno de amenazas ha cambiado

OPTI
tecnologías que dan valor

Ataques automatizados impulsados por IA

Los adversarios utilizan inteligencia artificial para ejecutar ataques adaptativos y evasivos a velocidad masiva.

Superficie de ataque híbrida y multi-cloud

Infraestructuras distribuidas crean vectores de ataque complejos y difíciles de monitorear.

Escasez global de talento SOC

Déficit crítico de analistas calificados para operar centros de seguridad 24/7.

Exceso de alertas sin priorización

Volumen insostenible de alertas genera fatiga y respuestas tardías a incidentes críticos.

Presión regulatoria creciente

Normativas como GDPR, NIS2 y regulaciones sectoriales exigen reportes rápidos y medidas de seguridad demostrables.

La Solución

Las organizaciones necesitan **detección inteligente**

- + Respuesta automatizada
- + Visibilidad estratégica

Evolución

Del SOC Tradicional al SOC Inteligente

OPTI
tecnologías que dan valor

SOC Tradicional

- **SIEM aislado**
  Sin integración nativa con herramientas de respuesta
- **Investigación manual**
  Procesos lentos y propensos a errores humanos
- **Alta dependencia humana**
  Requiere equipos grandes y especializados
- **MTTR elevado**
  Horas o días para contener incidentes
- **Visibilidad parcial**
  Silos de información limitan la correlación

OPTI Intelligent SOC

- **Plataforma Microsoft unificada**
  Sentinel + Defender XDR + Entra ID integrados
- **SOAR automatizado**
  Playbooks inteligentes ejecutan respuestas
- **IA integrada**
  Detección proactiva y análisis contextual
- **MTTR optimizado**
  Contención en minutos, no en horas
- **Cobertura 360°**
  Visibilidad completa de la postura de seguridad

Mensaje clave: No operamos un SIEM. Operamos una **plataforma de resiliencia**.

Arquitectura

Arquitectura Microsoft Nativa

OPTI
tecnologías que dan valor

OPTI Intelligent SOC 24x7

Microsoft Sentinel
SIEM & SOAR

Defender XDR
Endpoint & Identity

Entra ID
Identity Protection

Microsoft 365
Email & Collaboration

Azure

Conectores

Logic Apps

Beneficios Clave

- **Plataforma escalable**
  Crece con su organización
- **Optimizada para Azure**
  Máximo rendimiento cloud
- **Alineada a Zero Trust**
  Nunca confiar, siempre verificar
- **Sin vendor lock-in**
  Conectores third-party

Integración Continua

Threat Intelligence y Logic Apps para automatización completa

Arquitectura nativa: Plataforma escalable, optimizada para Azure y alineada a Zero Trust .

Servicio

Qué incluye OPTI Intelligent SOC

OPTI
tecnologías que dan valor

Deploy & Optimization
Implementación y ajuste fino

- Configuración Sentinel
- Integración de conectores
- Hardening de seguridad
- Tuning de reglas analíticas

24x7 MDR
Detección y respuesta gestionada

- Monitoreo continuo
- Triage avanzado
- Contención inmediata
- Escalamiento estratégico

Automation & SOAR
Orquestación y automatización

- Playbooks automatizados
- Integración con ITSM
- Respuesta orquestada
- Reducción de MTTR

Threat Hunting & Advisory
Caza de amenazas y asesoría

- Hunting proactivo
- Análisis forense
- Reportes ejecutivos
- Mejora continua

24/7	<15min	360°	AI+
Operación continua	Tiempo de respuesta	Visibilidad total	Inteligencia artificial

Proceso

Ciclo Inteligente de Gestión de Incidentes

OPTI
tecnologías que dan valor

Detection
AI-driven analytics

Investigation
Correlación contextual

Containment
Playbooks automatizados

Eradication
Eliminación total

Recovery
Restauración de servicios

Improvement
Mejora continua

MTTD Optimizado
Mean Time To Detect
<5 min ↓

MTTR Reducido
Mean Time To Respond
<15 min ↓

Eficacia
Tasa de contención
99.5%

Resultado medible: Reducción significativa de MTTD y MTTR mediante automatización inteligente.

AI-Enhanced SOC

AI-Enhanced SOC (Add-On Estratégico)

OPTI
tecnologías que dan valor

Powered by Microsoft Copilot for Security

Inteligencia artificial integrada en cada fase del SOC

Aceleración

Investigaciones en segundos, no en horas

Automatización

Análisis complejos automatizados

Inteligencia

Reportes ejecutivos en minutos

Capacidades Principales

- **Resúmenes automatizados**
  De incidentes complejos en lenguaje natural
- **Línea de tiempo automática**
  Secuencia completa del ataque
- **Evaluación de riesgo**
  Priorización inteligente de amenazas

Filosofía

La IA **potencia** al analista.

No lo **reemplaza**.

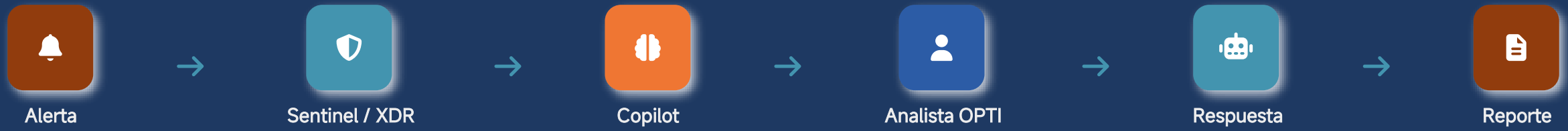
> El analista humano toma decisiones estratégicas con el respaldo de IA.

Arquitectura AI

SOC Cognitivo Integrado

OPTI
tecnologías que dan valor

Flujo de Procesamiento Inteligente



Investigación Contextual

En segundos
Análisis completo del incidente

Correlación automática
Entre múltiples fuentes de datos

Enriquecimiento TI
Threat Intelligence integrada

Análisis Asistido

Correlación avanzada
Patrones de ataque complejos

Identificación
De indicadores de compromiso

Recomendaciones
De contención contextualizadas

Reportes Ejecutivos

Generación automática
En lenguaje ejecutivo

Insights estratégicos
Tendencias y patrones

KPIs para comité
Métricas de negocio

Capacidades

Capacidades Clave del AI-Enhanced SOC

OPTI
tecnologías que dan valor

Resúmenes Automatizados

Línea de tiempo
Secuencia completa del incidente

Activos impactados
Inventario de sistemas afectados

Evaluación de riesgo
Impacto potencial del ataque

Acciones ejecutadas
Registro de respuestas aplicadas

Investigación Asistida

Correlación avanzada
Conexiones entre eventos dispersos

Identificación de patrones
TTPs de actores de amenazas

Recomendaciones
De contención y erradicación

Análisis retrospectivo
Búsqueda de IoC históricos

Reportes Ejecutivos

Insights estratégicos
Análisis de amenazas relevantes

Tendencias de amenazas
Evolución del panorama

KPIs para comité
Métricas de negocio claras

Lenguaje ejecutivo
Sin tecnicismos complejos

Transformación: De datos técnicos a **decisiones estratégicas** en minutos.

Beneficios

Impacto en el Negocio

OPTI
tecnologías que dan valor

60%
Reducción

Tiempos de Investigación
De horas a minutos con IA asistida

100%
Mejora

Calidad de Reportes
Ejecutivos claros y accionables

Real
Tiempo

Visibilidad Ejecutiva
Dashboards y métricas instantáneas

2x
Eficiencia

Optimización de Talento
Analistas enfocados en lo estratégico

Preparación para Amenazas con IA
Capacidad de defenderse contra ataques automatizados y adaptativos impulsados por inteligencia artificial

Evolución: El SOC evoluciona de reactivo a **predictivo**.

Comercial

Modelos de Servicio

OPTI
tecnologías que dan valor

SOC Advanced
24x7

- ✓ **Monitoreo continuo**
  24x7 de infraestructura
- ✓ **Respuesta automatizada**
  Playbooks SOAR
- ✓ **Triage avanzado**
  Priorización inteligente
- ✓ **Reportes operativos**
  Métricas y KPIs

$5,000 USD/mes
Desde

SOC Premium
24x7

- ✓ **Todo de Advanced**
- \+ **Threat Hunting**
  Proactivo semanal
- \+ **Investigación Forense**
  Análisis profundo
- \+ **Advisory Estratégico**
  Reuniones mensuales
- \+ **Reportes ejecutivos**
  Para comité directivo

$8,500 USD/mes
Desde

AI-Enhanced
Add-On

- **Copilot for Security**
  Integración completa
- **Investigación asistida**
  IA en cada incidente
- **Reportes automáticos**
  Ejecutivos en minutos
- **60% más rápido**
  Reducción de MTTR

$2,500 USD/mes
Adicionales

Nota: Precios basados en volumen de datos (GB/día) y número de conectores. Descuentos por compromiso anual.

Alineación Estratégica con Microsoft

Microsoft Azure
Inteligencia de uso

Microsoft Sentinel
Adopción

Defender XDR
Implementación integral

Copilot
Integración completa

Modelo
Escalable y recurrente

> OPTI acelera la adopción de **Microsoft Security** generando **valor recurrente** y **resiliencia empresarial**.

OPTI
Intelligent SOC 24x7

Microsoft

AI-Driven Security for the Modern Enterprise