HexWatch

Centro de Operaciones de Seguridad · gestionado 24/7

DATASHEET
SOC · MDR · XDR

HexWatch es un Centro de Operaciones de Seguridad gestionado que unifica detección, investigación y respuesta en una sola plataforma, operada por analistas y asistida por IA. Se integra con su firewall, endpoints, correo y nube para **ver el ataque completo y contenerlo** —de día, de madrugada y en festivos—, sin que usted tenga que montar y sostener un SOC propio.

PLATAFORMA Capacidades

SIEM y correlación
Ingesta y normalización de logs de servidores, endpoints, firewall y nube, con reglas afinadas contra su realidad.

EDR y forense remota
Visibilidad profunda del endpoint: recolección de evidencia y caza de artefactos sin desplazarse al sitio.

Contención de endpoint
Aislamiento del equipo de la red y detención del proceso malicioso, con guardarraíles sobre la infraestructura crítica.

SOAR y automatización
Playbooks que ejecutan la respuesta, solos o con aprobación humana, según el nivel de autonomía que usted decida.

IA agéntica
Ante un incidente, la IA reúne evidencia, arma la línea de tiempo, evalúa si es real y propone la acción de contención.

Copiloto de IA
Resume el incidente, explica el hallazgo en lenguaje claro y propone el siguiente paso, con el botón para ejecutarlo.

Threat Intelligence
Enriquecimiento de cada IP, dominio y hash contra fuentes de reputación, con envejecimiento de indicadores.

Protección de marca (DRP)
Detección de dominios que suplantan su marca (typosquatting) y de certificados emitidos a su nombre.

UEBA y riesgo por entidad
Puntaje de riesgo por usuario y activo según comportamiento: qué es normal aquí y qué se salió del patrón.

MITRE ATT&CK
Cada detección mapeada a técnicas y tácticas reales para ubicar la fase del ataque y la cobertura faltante.

Vulnerabilidades
Escaneo continuo, priorización por exposición real y seguimiento del cierre. No 4.000 hallazgos: los que hay que parchar ya.

NDR — tráfico de red
Detección de movimiento lateral, exfiltración y canales de mando y control observando lo que viaja por la red.

Superficie expuesta (ASM)
Qué publica su organización hacia Internet —servicios, puertos y accesos de administración— para cerrar lo indebido.

Microsoft 365 e identidad
Accesos imposibles, reglas de reenvío maliciosas, consentimientos sospechosos y toma de cuentas en la nube corporativa.

Shadow AI
Visibilidad del uso de IA generativa: quién la usa y con qué riesgo, para gobernar la IA sin frenar al negocio.

Postura de firewall y correo
Auditoría del FortiGate contra hardening con IA, y verificación en vivo de SPF/DKIM/DMARC del dominio.

Inventario y criticidad
Inventario automático de activos con criticidad de negocio que pondera la priorización de alertas y vulnerabilidades.

Cumplimiento y reportes
Evidencia lista para auditoría e informes ejecutivos que la junta directiva entiende sin traducción técnica.

CÓMO OPERA De la señal a la contención, en cuatro movimientos

01
Detecta
Correlaciona señales de todas sus fuentes y separa la alerta que importa del ruido.

02
Investiga
La IA y el analista arman el contexto: alcance, línea de tiempo y veredicto real vs. falso positivo.

03
Contiene
Bloqueo en el firewall, aislamiento del equipo o freno del proceso, con o sin aprobación humana.

04
Reporta
Cierre del ciclo con evidencia, métricas y un informe que su dirección entiende.

SERVICIO

Qué incluye

- Monitoreo y vigilancia 24/7, con guardias y escalamiento on-call.
- Afinamiento continuo de reglas contra su realidad operativa.
- Parte de estado diario del estado de la flota.
- Respuesta ante incidentes: contención asistida o automática según su política.
- Informe ejecutivo periódico y métricas de servicio (MTTR, SLA, tasa de falsos positivos).
- Remediación y parcheo remoto en Windows y Linux, con simulación y bitácora.

INTEGRACIÓN

Compatibilidad

Firewalls
FortiGate (respuesta activa y postura); respuesta a la medida para SonicWall, pfSense, Palo Alto, Check Point y Sophos.

Endpoints
Windows, Linux y servidores: agentes de telemetría, EDR y forense remota.

Nube e identidad
Microsoft 365 y Entra ID; integración de nube IaaS (AWS/GCP/Azure) a demanda.

Correo
Verificación de postura (SPF/DKIM/DMARC/MX) y análisis del correo entrante.

MODALIDADES

Se adapta al tamaño de su operación

Esencial

Para quien necesita ver por primera vez.

- Monitoreo y SIEM sobre activos críticos
- Detección con reglas afinadas
- Gestión de vulnerabilidades
- Reporte ejecutivo mensual
- Atención en horario hábil

MÁS SOLICITADO

Gestionado

Para quien necesita que alguien responda.

- Todo lo de Esencial
- Vigilancia 24/7 con guardias y escalamiento
- EDR, forense remota y caza de amenazas
- Threat intelligence y riesgo por entidad
- Contención asistida con aprobación

SOC Total

Para quien no puede permitirse una pausa.

- Todo lo de Gestionado
- Respuesta automática con playbooks SOAR
- Cobertura de nube, identidad y red
- Cumplimiento y evidencia de auditoría
- Acompañamiento en respuesta a incidentes

Cada implementación se dimensiona sobre su inventario real de activos y su nivel de exigencia normativa. La puesta en marcha toma semanas, no trimestres: instalamos agentes, recibimos el syslog del firewall y conectamos su nube, y desde los primeros días empezamos a correlacionar eventos.

Veamos su superficie de exposición.
Agende una demostración y reciba un diagnóstico inicial de su postura.

WEB hexwatch.clicksolutions.com.co
CORREO comercial@clicksolutions.com.co
WHATSAPP +1 571 314 1995