# Informe Detallado: Darktrace

## 1. Resumen ejecutivo

Darktrace Holdings Ltd., fundada en 2013 en Cambridge (Reino Unido), ofrece una plataforma de ciberseguridad basada en inteligencia artificial. Su ActiveAI Security Platform permite detección de amenazas, respuesta autónoma y visibilidad integral en correo, red, nube, OT y endpoints. Tiene más de 10,000 clientes en 110 países y fue adquirida en 2024 por Thoma Bravo.

## 2. Características técnicas principales

- Self-Learning AI: aprende el comportamiento normal y detecta anomalías. - ActiveAI Security Platform: detección, respuesta, simulación y prevención. - Darktrace/Email: protección contra phishing y pérdida de datos. - PREVENT: análisis de firewall y rutas de ataque. - Cobertura OT/IoT: monitoreo y protección en entornos industriales. - Autonomous Response (Antigena): aislamiento automático de amenazas.

## 3. Fortalezas

- Detecta amenazas zero-day y desconocidas. - Cobertura integral en correo, red, nube, identidad y OT. - Respuesta autónoma rápida frente a incidentes. - Innovación en IA con múltiples patentes y alianzas con Microsoft y AWS.

## 4. Debilidades

- Posibles falsos positivos y ruido en alertas. - Costo elevado para organizaciones públicas. - Curva de aprendizaje inicial y necesidad de personal especializado. - Riesgo de acciones automáticas que afecten operaciones críticas.

## 5. Consideraciones para la CDMB

- Evaluar infraestructura y compatibilidad. - Capacitar al equipo de TI y seguridad en operación de la plataforma. - Revisar presupuesto y modelo de licenciamiento. - Establecer políticas claras de respuesta automática. - Validar cumplimiento con normativas locales de protección de datos.

## 6. Comparación con otras soluciones

Alternativas como CrowdStrike Falcon, Microsoft Defender y Palo Alto Cortex XDR también ofrecen protección avanzada. Darktrace se diferencia por su IA adaptativa y cobertura integral, aunque el costo puede ser mayor.

## 7. Costos y licenciamiento

Modelo de suscripción con posibles costos adicionales por endpoints, tráfico, usuarios, integración y soporte. Puede requerir appliances de hardware para monitoreo de red.

## 8. Recomendaciones para CDMB

1. Realizar prueba piloto (PoC) para validar efectividad. 2. Definir umbrales para respuesta automática con cuidado. 3. Integrar Darktrace con el SOC o equipo de seguridad. 4. Ajustar políticas de privacidad y gobernanza de datos. 5. Capacitar personal y monitorear métricas clave.

## 9. Conclusión

Darktrace es una plataforma avanzada de ciberseguridad basada en IA que puede mejorar la postura de seguridad de la CDMB. Su adopción requiere inversión, gobernanza y capacitación, pero aportaría gran valor en detección y respuesta a amenazas complejas.