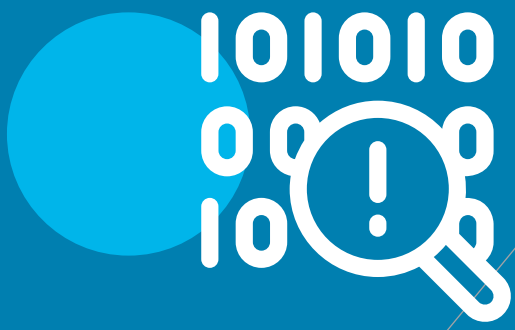
Inycom
innovation technologies

+34 902 995 820
info@inycom.es

# SOLUCIONES
# DETECCIÓN CIBERAMENAZAS

Ciberseguridad Avanzada



Esta Solución de Detección de ciberamenzas ayuda a proteger Dominios Empresariales de ataques avanzados en marcha (APT's y Zero day).

Proporciona una manera simple y rápida de entender lo que está sucediendo en su red mediante la identificación de usuarios sospechosos, la actividad de dispositivos comprometidos y proporciona información de amenaza clara y relevante mostrando un cronograma del ataque.

Aprovecha tecnología Machine learning y la inspección profunda de paquetes, así como información de fuentes de datos adicionales (SIEM y AD) para construir un gráfico de seguridad organizacional y detectar ataques avanzados en tiempo casi real.

Permite detectar automáticamente actividades sospechosas, ataques y robos de identidad en el Active Directory "on premise" de una organización.

## CARACTERÍSTICAS Y BENEFICIOS

- **Detecta amenazas con rapidez mediante análisis del comportamiento.** Utiliza Algoritmos y tecnología Machine Learning para ayudarle a detectar actividad sospechosa en sus sistemas.
- **Adaptación rápida a nuevos patrones de ataque Hacker.** Aprendizaje continuo del comportamiento de usuarios, dispositivos y recursos, Conforme los atacantes elaboran tácticas más sofisticadas,
- **Detección de ataques maliciosos:**
  - Pass-the-Ticket (PtT)
  - Pass-the-Hash (PtH)
  - Overpass-the-Hash
  - Forged PAC (MS14-068)
  - Golden Ticket
  - Malicious replications
  - Reconnaissance
  - Brute Force
  - Remote execution
  - Malicious DPAPI
- **Detección por comportamiento anómalo**
  - Anomalous logins
  - Unknown threats
  - Password sharing
  - Lateral movement

## MERCADO OBJETIVO

- Organizaciones con infraestructura de red basada en Microsoft Active Directory.
- Compañías del Sector financiero, Telecomunicaciones o Industria con departamentos de Seguridad.
- Compañías con información sensible que requieren un alto nivel de protección.

## SERVICIOS OFRECIDOS

- Consultoría sobre principales amenazas de Ciberseguridad en el entorno del cliente.
- Diseño , arquitectura e implantación de los Sistemas de detección, gateway de red y consola de Gestión de Ciberamenazas.
- Integración con SIEM y AD para recopilar logs y alertas de seguridad
- Identificación de ataques en curos y transferencia de tecnología con el cliente
- **Ayuda en la actualización de su estrategia de ciberseguridad para cumplir la nueva legislación,** centrándonos especialmente en la respuesta ante incidentes y en las preocupaciones por la privacidad.
- **Consultoría y revisión del ciclo de vida de la seguridad,** analizando la red para indicando qué aplicaciones se están utilizando, así como los posibles riesgos de exposición.