HONEYPOTSEC

Monitoriza Amenazas. Educa a tu Equipo.

PLATAFORMA SAAS · PROYECTO FINAL ASIR 2025-2026 · SERGIO FERMIÑÁN & GERARD MARTINEZ

El Problema:
¿Por qué no basta con protegerse?

LA AMENAZA

- **Bots de fuerza bruta 24/7**
  Ataques automatizados sin descanso contra servicios expuestos
- **Exploits automatizados**
  Herramientas que escanean y explotan vulnerabilidades en segundos
- **Escaneos masivos de red**
  Miles de IPs barridas cada hora buscando puertos abiertos
- **Malware y ransomware**
  Código malicioso que cifra, roba o destruye datos críticos

LA VULNERABILIDAD

- **Phishing e ingeniería social**
  El eslabón más débil sigue siendo el factor humano
- **Contraseñas débiles o reutilizadas**
  Credenciales predecibles que los atacantes explotan en minutos
- **Falta de concienciación**
  Empleados que no reconocen amenazas reales del día a día
- **Sin formación práctica**
  La teoría no prepara para reaccionar ante ataques reales

HoneypotSEC: Plataforma SaaS B2B de Honeypots

Infraestructura de Honeypots

Captura de ataques y monitorización. Red de señuelos aislada y multiprotocolo (HTTP, FTP, SSH) que captura tácticas reales de los atacantes y vectores de amenaza.

Dashboard en Tiempo Real

Información y análisis instantáneo de amenazas. Visualización centralizada de ataques con mapa 3D en tiempo real y alertas.

Módulos Académicos

Formación para trabajadores y usuarios. Uso de la inteligencia de amenazas capturada para generar rutas de aprendizaje interactivas y simulaciones de phishing.

Así funciona...

Seguridad y Proxy

Nginx, Let's Encrypt (Certbot), UFW (Drop All), SSH Auth (RSA/Ed25519)

Frontend

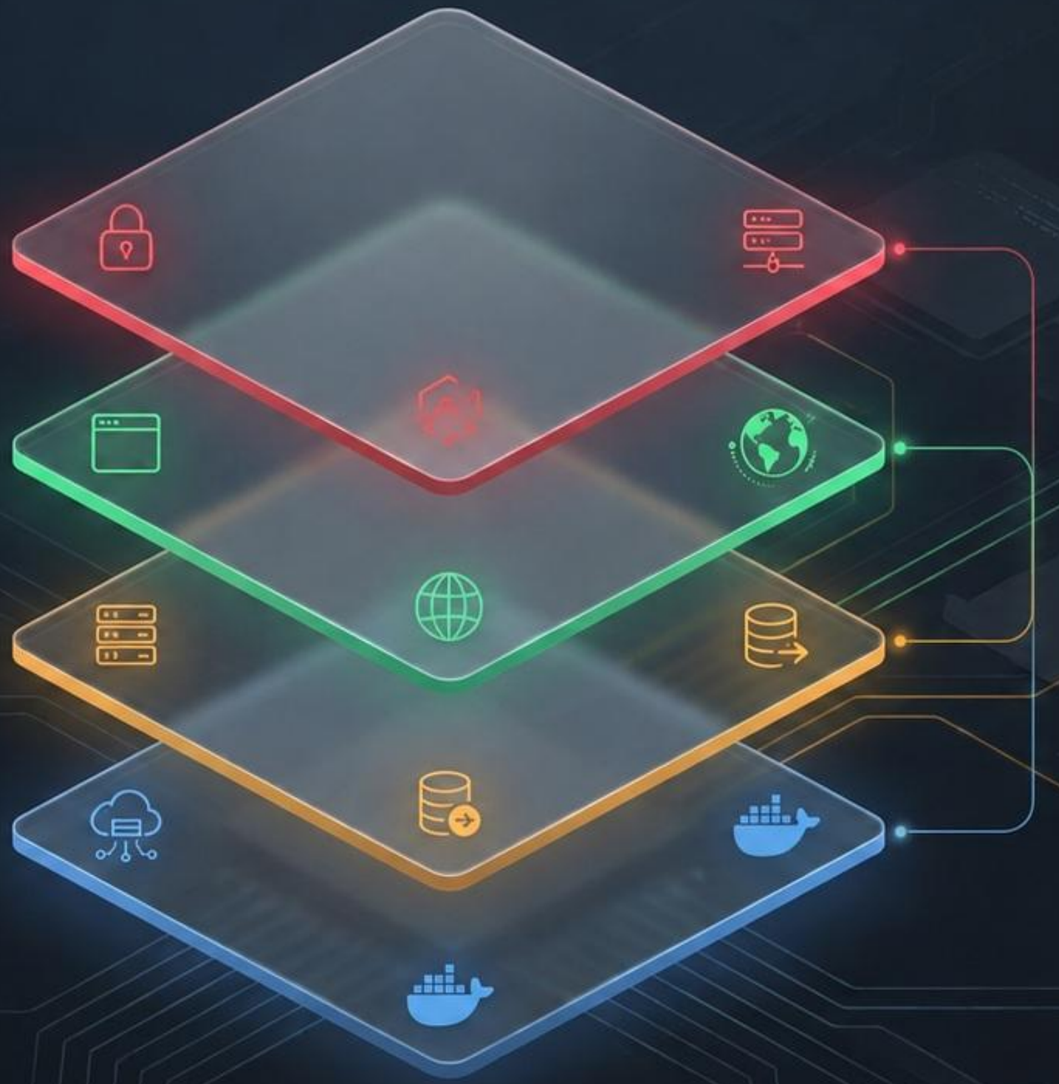
React, Vite, TailwindCSS, COBE (WebGL 3D Globe)

Backend y Base de Datos

Python (Motor Collector), FastAPI (API RESTful asíncrona), PostgreSQL 15 (Persistencia)

Cloud e Infraestructura

Hostinger KVM2, Linux Ubuntu 24.04, Docker, Docker Compose



6 HONEYPOTS

Tactical Sensor Matrix

SENSOR	NIVEL DE INTERACCIÓN	CAPA / SERVICIO EMULADO	PROPÓSITO TÁCTICO
Cowrie	Media-Alta	Consola (SSH 2222 / Telnet)	Capturar fuerza bruta y comandos interactivos.
Dionaea	Media	Multi-protocolo (FTP, SMB, MySQL)	Recolección automatizada de malware.
Glastopf	Baja-Media	Aplicación Web (HTTP)	Simular vulnerabilidades SQLi y XSS.
Conpot	Baja	Industrial (SCADA / Modbus)	Detectar escaneos contra infraestructuras críticas.
Honeytrap	Baja	Listener dinámico	Descubrir nuevos vectores en puertos no configurados.
Honeyd	Baja	Simulación de Red	Crear topologías falsas para confundir al atacante.

Flujo de Inteligencia de Amenazas

Protocol: TCP/UDP, HTTP(S), SSH, FTP · Docker: Containerized · Database: PostgreSQL 15, Relational · Analytics: Real-time Python Processing · UI: WebGL 3D Globe (React/COBE)

Decisiones de Hosting

Análisis comparativo · Proveedores evaluados

	Oracle Cloud	AWS EC2	Google GCP	Hostinger KVM2
ELECCION	✗ Descartado	✗ Descartado	✗ Descartado	✓ ELEGIDO
PRECIO	Free tier limitado	~20–60 €/mes	~25–70 €/mes	8,99 €/mes
RECURSOS	1 vCPU / 1 GB	Variable / complejo	Variable / complejo	2 vCPU · 8 GB 100 GB NVMe
IP PÚBLICA	✗ Rotativa / restringida	✗ Coste adicional	✗ Coste adicional	✓ Estática incluida
HONEYPOTS	✗ Políticas restrictivas	✗ Puertos bloqueados	✗ Puertos bloqueados	✓ Puertos libres
COMPLEJIDAD	Alta	Muy alta	Muy alta	Baja

Validación de Deception: Perspectiva del Atacante

Falso NAS Synology DiskStation para atraer ransomware.

Evidencia de aislamiento: El atacante ve la red interna de Docker, no la IP real.

Terminal - Nmap Output

```
nmap -T4 -A -v 187.127.230.202
Not shown: 991 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
21/tcp  open  ftp      Synology DiskStation NAS ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV IP 172.18.8.5 is not the same as 187.127.230.202
22/tcp  open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.16 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 f9:c7:32:87:4f:3f:ec:1b:6f:1e:87:e5:52:f6:a3:8b (ECDSA)
|   256 7f:fe:ed:57:b4:cd:82:b1:06:a4:8a:ec:f0:50:d9:9a (ED25519)
80/tcp  open  http     nginx 1.27.5
| http-title: Did not follow redirect to https://srv1652887.hstgr.cloud/
| http-server-header: nginx/1.27.5
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS
443/tcp open  ssl/http nginx 1.27.5
| ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=localhost/organizationName=HoneypotPlatform/stateOrProvinceName=Madrid/countryName=ES
| Subject Alternative Name: DNS:localhost, DNS:localhost, IP Address:127.0.0.1
| Issuer: commonName=localhost/organizationName=HoneypotPlatform/stateOrProvinceName=Madrid/countryName=ES
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2026-05-07T16:57:45
| Not valid after: 2027-05-07T16:57:45
| MD5: 13ea:1895:a41a:bef0:56f6:3887:8638:56c9
| SHA-1: bb6f:57d4:0b96:09bd:0663:8c85:6859:cb1f:6988:ec5a
| http-server-header: nginx/1.27.5
| tls-alpn:
|   http/1.1
|   http/1.0
|   http/0.9
| http-title: HoneyWatch \xE2\x80\x94 Plataforma de Honeypots
| http-favicon: Unknown favicon MD5: 0931E25A27B135C4303FB8DA772C67D7
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS
445/tcp  open  microsoft-ds  Windows XP microsoft-ds
1433/tcp open  ms-sql-s      Microsoft SQL Server 2000 8.00.528.00; SP1+
| ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
| ms-sql-info: ERROR: Script execution failed (use -d to debug)
1722/tcp open  pptp (Firmware: 1)
3306/tcp open  mysql      MySQL 5.7.16
| mysql-info:
```

Emulación de Windows XP obsoleto para recibir exploits tipo EternalBlue.

Base de datos MySQL obsoleta con clave salt predecible.

Gracias al VPS con IP pública estática de Hostinger, fue posible validar el acceso a la plataforma desde cualquier dispositivo y ubicación.

Pruebas realizadas desde clientes móviles y portátiles sobre redes externas, simulando condiciones reales de producción.

HONEYPST

Sensor Installer v1.0

```
curl -sL https://honeypotsec.duckdns.org/install | sudo bash -s -- --token TOKEN
```

Paso 1: Generación de Identidad

Administrador B2B emite un token JWT único (Tenant ID).

Paso 2: Ejecución Unificada

El cliente ejecuta un único comando en su servidor.

Paso 3: Orquestación Total

Autodetección de SO, instalación de Docker, descarga de docker-compose.yml y conexión Heartbeat al SOC.

12 Microservicios Concurrentes operando de forma estable.

CPU

Uso medio en reposo
(Backend: 0.15%, Conpot: 0.44%)

RAM

Optimización extrema. El sensor más pesado (Conpot SCADA) requiere solo 116.4 MiB sobre 8GB.

Viabilidad técnica demostrada: El plan VPS KVM 2 de Hostinger soporta la infraestructura sin cuellos de botella bajo carga de producción.

Plan Básico

5€/mes

- Hasta 50 empleados.
- 2 sensores (Cowrie, Dionaea).
- 30 días de retención.

Plan Profesional

30€/mes

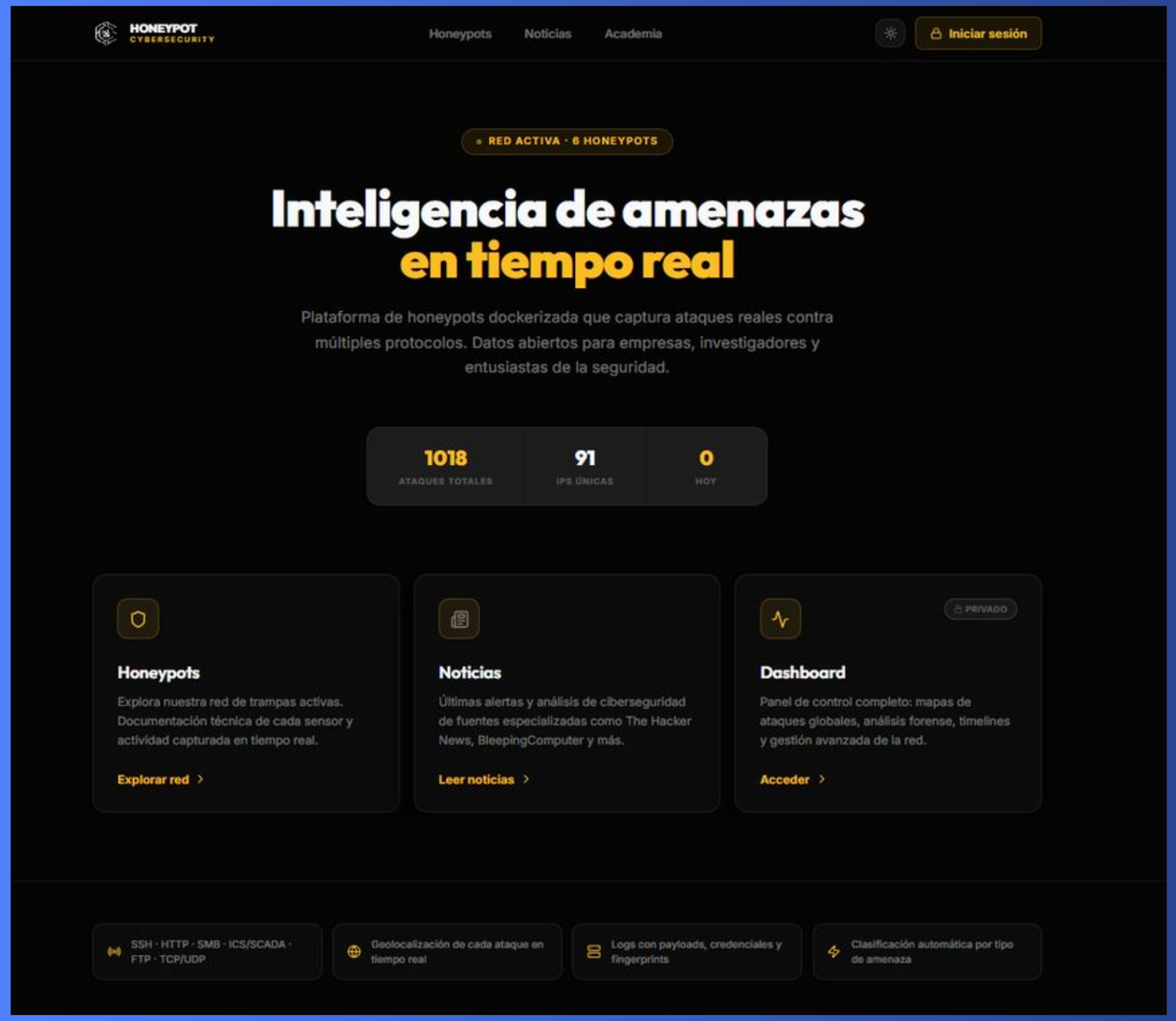
- Hasta 200 empleados.
- 4 sensores (incluye SCADA/Web).
- 90 días retención.

Plan Empresarial

50€/mes

- Ilimitado.
- Ecosistema completo (6 sensores).
- Soporte 24/7.

Coste Operativo Base: 8.99€/mes (VPS Hostinger + 0€ Licencias Open Source).
Rentabilidad altamente escalable.



LIMITACIONES Y **FUTURAS PROPUESTAS**

PRÓXIMAS FASES

Por limitaciones de tiempo, quedaron fuera del alcance final varias funcionalidades previstas: alertas automáticas vía Telegram y correo, algún sistema de ciberseguridad para asegurar la integridad de los datos, integración con Active Directory para autenticación SSO, y un módulo de detección de anomalías basado en IA.

Todas ellas están identificadas y documentadas como líneas de desarrollo futuro.

MONITORIZA Y APRENDE

WWW.HONEYPOTSEC.DUCKSDNS.ORG