DERIV AI TALENT SPRINT 2026

ThreatSynth AI

Autonomous AI-Powered Penetration Testing & Threat Intelligence Platform

Pentest Automation | Threat Intelligence | AI Briefings

The Problem

3,500+
NEW CVES PER MONTH (2025)

$4.88M
AVG COST OF DATA BREACH

277 days
AVG TIME TO DETECT BREACH

Security teams juggle **disconnected tools** — vulnerability scanners, threat feeds, pentest frameworks, and report generators — with **no unified intelligence layer**

Our Solution

One platform that ingests threats, scans infrastructure, validates exploits, and generates briefings — autonomously.

THREAT INTELLIGENCE ENGINE

6 real-time sources (NVD, CISA KEV, ExploitDB, GitHub, Shodan CVE DB, EPSS) auto-correlated with your asset inventory

MULTI-AGENT PENTEST PIPELINE

4-phase autonomous assessment: Recon → Vulnerability Scan → Exploit Validation → AI Report Generation

HUMAN-IN-THE-LOOP

Mandatory approval gate before active exploitation — AI suggests, humans decide

AI-POWERED BRIEFINGS

LLM generates executive summaries, remediation steps, and business impact analysis per threat-asset pair

Architecture

PHASE 1

Recon Agent

nmap • whatweb
wafw00f • gobuster

→

PHASE 2

Vuln Scanner

nikto • sqlmap
security headers

→

PHASE 3

Exploit Validator

SQLi • XSS • CMDi
⚠ Human Approval Gate

→

PHASE 4

AI Reporter

LLM analysis
executive reports

React 19 + Tailwind | FastAPI + SQLAlchemy | Ollama (Local LLM)

WebSocket Streaming | Docker Compose

Live Threat Intelligence

6 real APIs • No fake data • All free, no API keys required

NVD

20

National Vulnerability Database

CISA KEV

30

Known Exploited Vulns

ExploitDB

19

Public Exploits (GitLab CSV)

GitHub

20

Security Advisories

Shodan CVE DB

9

KEV + EPSS + Ransomware

FIRST EPSS

20

Exploit Prediction Scoring

118 real threats ingested • **56** critical • **59** actively exploited

AI Correlation & Briefings

Threats auto-matched to your asset inventory → AI generates actionable briefings

CRITICAL

CVE-2024-23897 → ci-runner-01 (Jenkins 2.426)

10.0

CRITICAL

CVE-2021-22205 → git-server (GitLab 16.5)

10.0

CRITICAL

CVE-2020-1938 → web-server-01 (Apache 2.4.54)

10.0

HIGH

CVE-2019-17558 → web-server-01 (Apache httpd)

9.0

CVE-2024-23897 → Jenkins ci-runner-01 **10/10**

Jenkins 2.441 and earlier allows unauthorized file read via CLI. Affects ci-runner-01 on port 8080.

Remediation: Update to Jenkins 2.442+, restrict CLI access, rotate credentials.

Impact: Source code theft, credential exfiltration, supply chain compromise.

Why ThreatSynth?

TRADITIONAL TOOLS

Separate vulnerability scanners, threat feeds, pentest frameworks, and reporting tools. Manual correlation. Delayed response.

THREATSYNTH AI

Unified platform: ingest → correlate → scan → exploit → report. AI-powered. Real-time. One command.

SELF-HOSTED & PRIVATE

Local LLM via Ollama. No data leaves your network. Perfect for regulated industries (defense, healthcare, finance).

RESPONSIBLE AI

Human-in-the-loop approval before exploitation. AI advises, humans authorize. Full audit trail via WebSocket logs.

Tech Stack

```
# Frontend React 19 + React Router 7 + Tailwind CSS 4 + Recharts + Lucide Icons # Backend FastAPI (async) + SQLAlchemy (async ORM) + SQLite + WebSockets # AI / LLM Ollama → gemma3:4b (local, private, no API key) # Security Tools nmap · whatweb · wafw00f · gobuster · nikto · sqlmap # Threat Intel APIs (all free, no keys) NVD · CISA KEV · ExploitDB · GitHub Advisories · Shodan CVE DB · FIRST EPSS # Infrastructure Docker Compose + DVWA (safe vulnerable test target)
```

Business Value

90%

REDUCTION IN MANUAL TRIAGE TIME

6

INTEL SOURCES AUTO-CORRELATED

$0

API COST (ALL FREE SOURCES)

- **For SOC Teams:** Automated threat-to-asset correlation eliminates hours of manual CVE triage
- **For Pentesters:** 4-phase autonomous pipeline with human oversight — faster assessments, better coverage
- **For Executives:** AI-generated briefings with priority scores, remediation steps, and business impact

- **For Compliance:** Full audit trail, approval gates, self-hosted — meets regulatory requirements

DERIV AI TALENT SPRINT 2026

ThreatSynth AI

Autonomous Security Intelligence.
Real Threats. Real APIs. Real Protection.

github.com/edwardtay/threatsynth

MIT Licensed • Built with FastAPI + React + Ollama

Speaker notes