OASM ASSISTANT

SUPPORT IN MANAGING, MONITORING, AND PREVENTING ATTACK SURFACES

BUILT BY: TEAM OASM-PLATFORM

BACKGROUND AND MOTIVATION

Current Challenges

- High costs for pentesting and attack surface scanning services
- Lack of quality open source tools for attack surface management
- Difficulties in managing and monitoring digital assets

Project Origin

- Developed from experience at National Cybersecurity Monitoring Center
- Goal: To create a reputable open source product for the international community
- Reduce dependency on expensive commercial solutions

OASM ECOSYSTEM OVERVIEW

OASM-PLATFORM

Open-ASM (Core platform)

External Attack Surface Management

Microservices architecture

Discovery tools: Subfinder, Dnsx, Naabu, Httpx

Vulnerability scanning: Nuclei, Nessus

OASM-ASSISTANT (AI layer)

AI layer on top of core platform

Multi-agent system with LangGraph

Automation and optimization of security workflows

OASM-PLATFORM

SYSTEM ARCHITECTURE

OASM CORE (Central block)

- Asset Management
- Job Scheduling and Management
- Forward to OASM Assistant
- API Gateway
- MCP Integration
- Data Storage & Caching

MCP

gRPC APIs

OASM ASSISTANT (AI Layer)

- Domain Classifier
- Threat intelligence agent
- Analysis agent
- Incident responder agent
- Orchestration agent

RESTful APIs

SSE

OASM WORKERS (Tools Execution Layer)

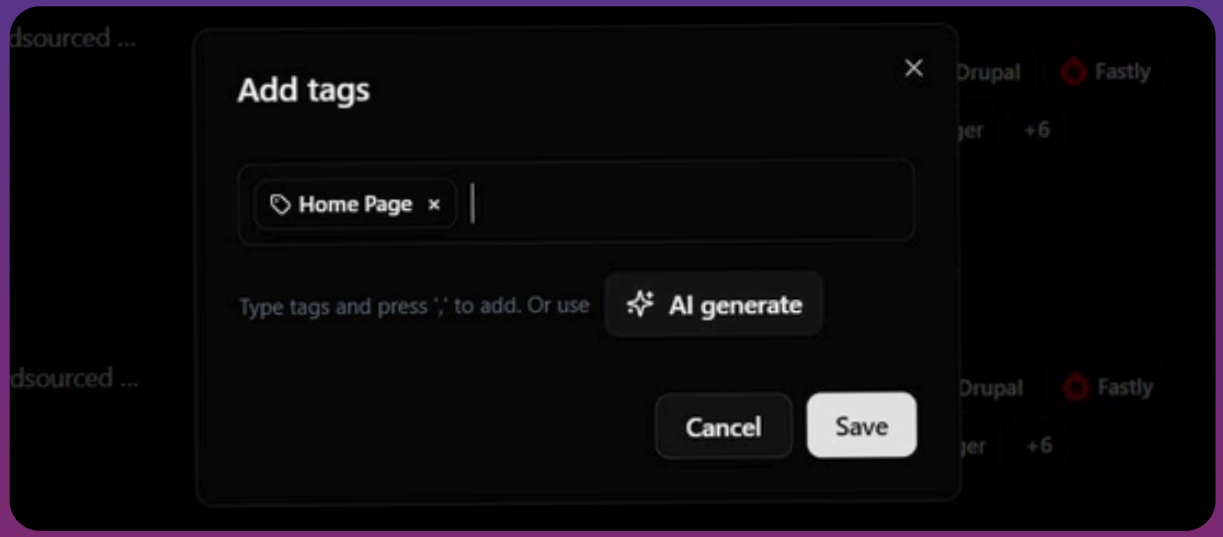
Execute tools and return result to OASM Core

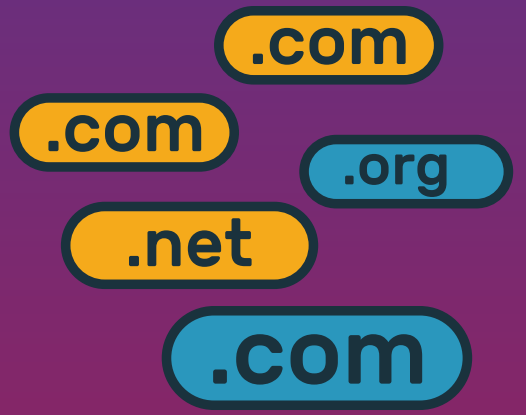
- Discovery: Subfinder, dnsx, naabu, httpx
- Scan vuln: Nuclei, nessus

OASM-PLATFORM

DOMAIN CLASSIFIER

Domain Classifier automatically classifies digital assets. It assigns labels based on the title and content of the HTML extracted by domain. It helps manage and identify whether the assets are the target of hacker attacks so that you can prioritize asset management and monitoring.





OASM-PLATFORM

THREAT INTELLIGENCE AGENT

- Threat monitoring
- Intelligence analysis (IOC correlation)
- Exploring enemy weapons research
- Attack prediction
- Threat alerts

OASM-PLATFORM

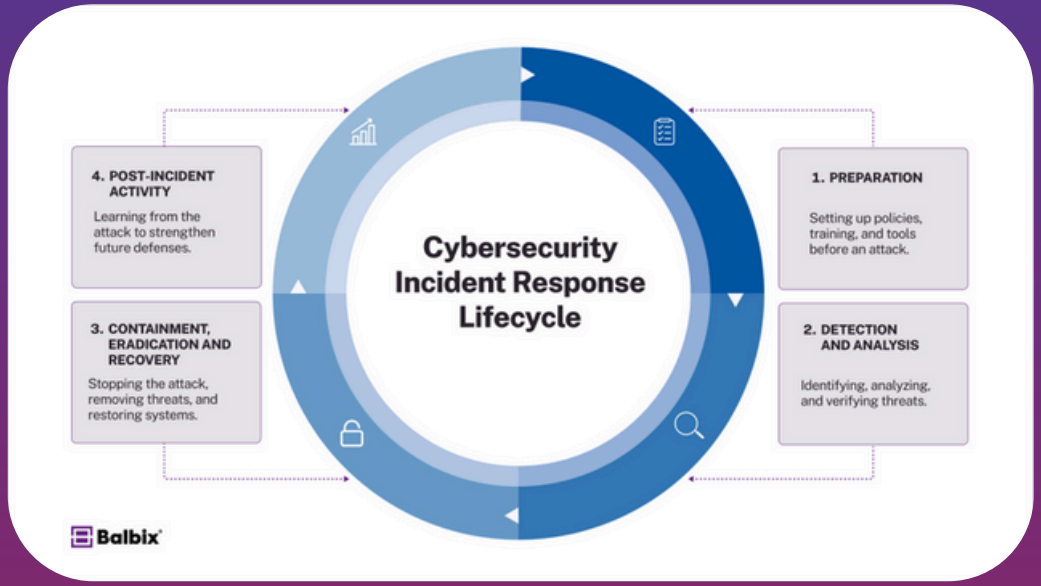
ANALYSIS AGENT

- Collect results from Core
- Compare security status with international standards (OWASP, CWE, PCI-DSS, ISO 27001)
- Prioritize vulnerabilities by context
- Prepare a report with a detailed remediation plan

OASM-PLATFORM

INCIDENT RESPONDER AGENT

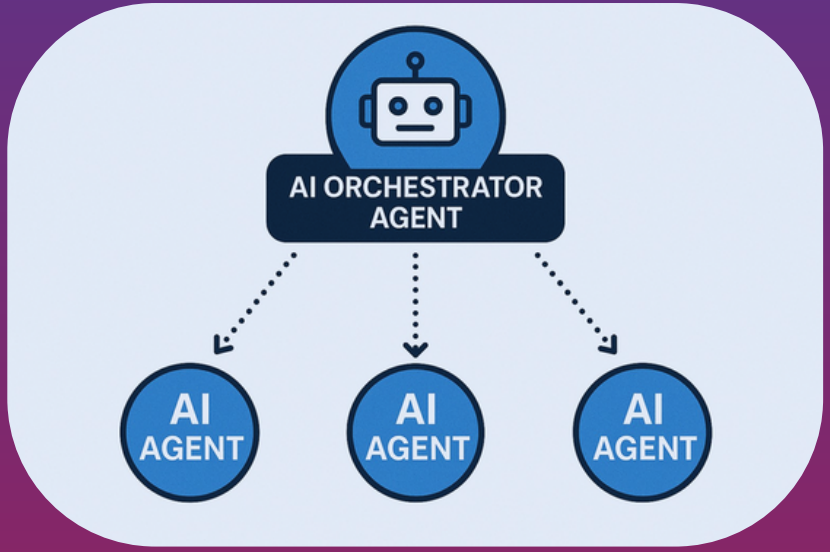
- Detect attack in progress
- Attack method analysis
- Generate incident response plan
- Automatically prevent vulnerabilities
- Investigate the entire incident

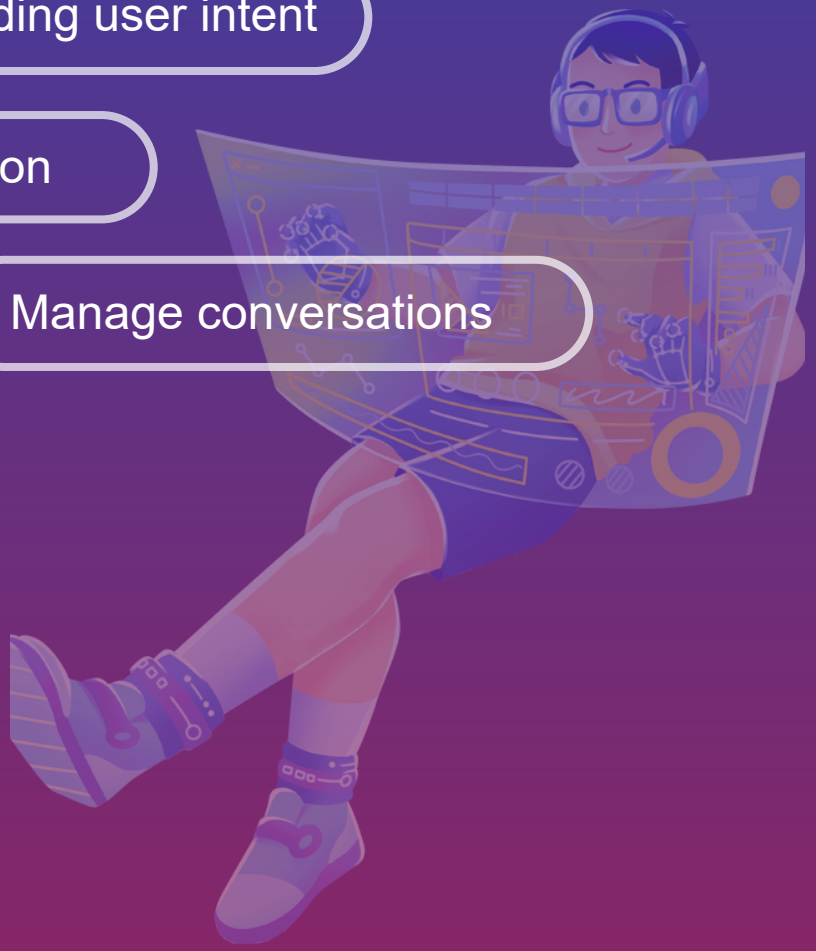


OASM-PLATFORM

ORCHESTRATOR AGENT

- Understanding user intent
- Agent coordination
- Summary of results
- Manage conversations





TECHNOLOGY STACK

OASM-PLATFORM

LangGraph: Building LLM-powered agents with tools

LLMs: GPT-4, Claude, Gemini, Llama, Mistral ... Transfer Learning, Reinforcement Learning

LangGraph: Building LLM-powered agents with tools

RAG: Using HNSW algorithm combined with full-text search and re-ranking to enhance data based on memory agent, knowledge base, nuclei template

gRPC: High-performance RPC between AI layer and Core platform

MCP: Provide real-time asset context to AI agents, SearXNG, ...

Data Storage & Processing: PostgreSQL as the primary database storage, use batch processing for embedding generation and extract content in file PDF, docx, yaml... and parallel vector search

OASM-PLATFORM

THANK YOU