HEGA GEOFFROY RENE ERNEST

Blockchain Security Engineer · AI Infrastructure Specialist · OpenClaw

- Website https://aiscan-security.online/
- LinkedIn https://www.linkedin.com/in/geoffroy-rene-hega-107952102/
- Instagram https://www.instagram.com/geoffroyrene/
- GitHub https://github.com/sakbayeme2015
- Platform ASVH v7.5 — AI Security Vulnerability Scanner

Level 1	Level 2	Level 3
Specialist	Specialist	Specialist
Hardware · Firmware · IPMI	Cloud · Kubernetes · IAM	AI Models · LLMs · APIs

HEGA GEOFFROY RENE ERNEST · OpenClaw · aiscan-security.online · 2026

CONFIDENTIAL — For authorized security research and investment analysis only

AI Infrastructure

3-Level Investment + Security Guide

Hardware · Cloud Infrastructure · AI Models — Stock Ecosystem + Pentest Surface Map

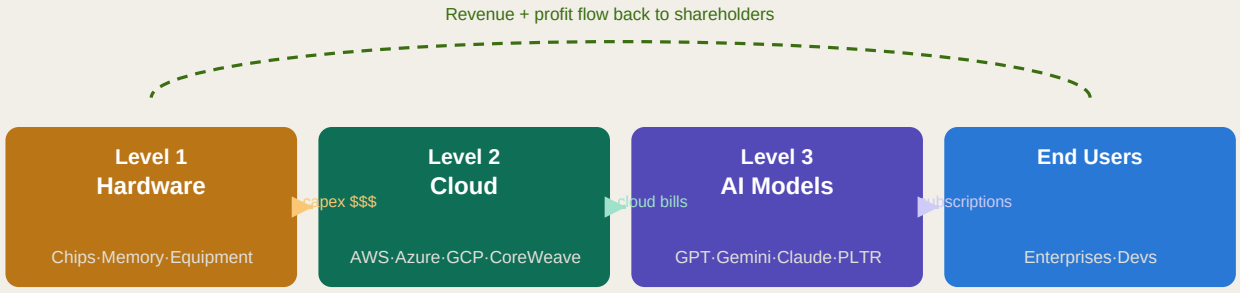
30+	3	25+	$650B
AI stocks	Security levels	Pentest tools	2026 AI capex

Part 1 — AI Stock Ecosystem: 3 Investment Levels

How capital flows from hardware through cloud to AI models — and back to shareholders

The AI investment universe splits into three distinct tiers, each with a different risk profile, revenue model, and role in the capital flow chain. The five largest US hyperscalers are on track to spend over $650 billion on AI infrastructure in 2026 alone, nearly double the $380 billion spent in 2025. That capital flows directly through all three levels.

Capital flow across all 3 AI investment levels



Level 1 — Hardware, Chips & Physical Infrastructure

Risk: Stable / cyclical. Highest barriers to entry. Every AI company at Level 2 and 3 must buy Level 1 products. No matter which AI model wins, they all need NVIDIA GPUs, TSMC wafers, and Micron HBM memory. Fabs cost $20B+ to build; ASML EUV machines take 3 years to deliver; CUDA has a decade of developer lock-in.

Ticker	Company	Sub-sector	Why it matters
NVDA	NVIDIA Corporation	GPU / AI accelerator	Dominant AI chip. CUDA moat. ~$5T market cap.
AMD	Advanced Micro Devices	GPU / AI accelerator	MI300 competitive vs H100. 2nd in AI compute.
AVGO	Broadcom Inc.	Custom silicon / ASIC	Custom AI chips for Google, Meta. AI networking.
ARM	Arm Holdings	Chip architecture	Licenses CPU arch. In every AI server + edge device.
QCOM	Qualcomm Inc.	Edge AI chips	On-device AI inference. Snapdragon X Elite AI PCs.
TSM	TSMC	Foundry / fabrication	Makes every advanced AI chip. 3nm/2nm process leader.
ASML	ASML Holding	Chip equipment (EUV)	Monopoly on EUV lithography. Required for sub-7nm.
AMAT	Applied Materials	Chip equipment	Deposition, etch, inspection for every global fab.
MU	Micron Technology	Memory / HBM	High Bandwidth Memory in every H100/H200 GPU.
MRVL	Marvell Technology	AI networking silicon	Custom DPUs and optical interconnects for AI DCs.

ETFs: SOXX (iShares Semiconductor), SMH (VanEck Semiconductor)

Level 2 — Cloud Infrastructure & Data Centres

Risk: Moderate / recurring revenue. Level 2 companies buy Level 1 hardware and rent the compute to Level 3. Google Cloud has a $364B infrastructure backlog. Azure AI Foundry is used by ~80% of Fortune 500 companies. CoreWeave went public in 2026.

Ticker	Company	Sub-sector	Why it matters
MSFT	Microsoft	Hyperscaler (Azure)	Azure AI Foundry. OpenAI partnership. 80% F500 AI.

Ticker	Company	Sub-sector	Why it matters
AMZN	Amazon	Hyperscaler (AWS)	AWS Bedrock + SageMaker. Largest cloud share (~31%).
GOOGL	Alphabet / Google	Hyperscaler (GCP)	Custom TPU v5/v6. $364B cloud backlog. $180B capex.
ORCL	Oracle Corporation	Enterprise cloud	OCI GPU clusters. OracleDB + AI features growing fast.
CRWV	CoreWeave	Neo-cloud (GPU-only)	Pure GPU cloud. IPO 2026. Serves AI labs + startups.
EQIX	Equinix Inc.	Data centre REIT	200+ DCs globally. AI power demand beneficiary.
DLR	Digital Realty	Data centre REIT	300+ DCs. Hyperscaler AI expansion. REIT income.
VRT	Vertiv Holdings	DC power / cooling	Cooling + power for AI servers. Capex pass-through.
ANET	Arista Networks	AI networking	400G/800G switches for AI clusters. Ethernet vs IB.
IRM	Iron Mountain	Storage / DC	AI data storage + DC expansion. Dividend REIT.

ETFs: CLOU (cloud computing), WCLD (WisdomTree Cloud)

Level 3 — AI Models, Software & Applications

Risk: High growth / volatile. Level 3 companies use Level 2 cloud to build and serve AI models — selling intelligence as API calls, SaaS subscriptions, or enterprise licenses. Many are growing 30–100%+ annually. Alibaba plans $50B+ AI investment.

Ticker	Company	Sub-sector	Why it matters
PLTR	Palantir Technologies	Enterprise AI platform	AIP platform. Government + enterprise analytics.
CRM	Salesforce Inc.	Enterprise AI / CRM	Einstein AI across Sales, Service, Marketing clouds.
NOW	ServiceNow Inc.	Workflow AI	AI agents automating IT/HR. Fast AI revenue growth.
ADBE	Adobe Inc.	Creative AI / tools	Firefly image AI. AI in Photoshop, Premiere, Acrobat.
SNOW	Snowflake Inc.	AI data platform	AI data cloud. Cortex AI features for AI apps.
PATH	UiPath Inc.	AI automation / RPA	Agentic automation. AI bots replacing repetitive tasks.
BABA	Alibaba Group	Cloud + AI (China)	Qwen LLM family. Alibaba Cloud. $50B AI investment.
TEM	Tempus AI Inc.	Healthcare AI	Clinical AI + genomics. Partners with pharma + hospitals.
SOUN	SoundHound AI	Voice AI / NLP	Conversational AI for automotive, restaurants, IoT.
AI	C3.ai Inc.	Enterprise AI apps	Pre-built AI apps for industrial, financial, government.

ETFs: AIQ (Global X AI), BOTZ (Global X Robotics & AI $1.7B), THNQ

Investment Platforms by Capital Scale

Scale	Platform	Best for
$1K–$100K	Robinhood · Webull · eToro	Zero commission, fractional shares, mobile
$100K–$1M	Fidelity · Schwab · IBKR	ETF access, options, international (TSM, ASML)
$1M–$100M	Interactive Brokers (IBKR)	Lowest institutional fees, 150+ markets, margin
$100M+	Goldman Sachs / Morgan Stanley / JPMorgan	Prime brokerage, dark pools, block trading, pre-IPO
Any	Bloomberg Terminal + Prime desk	Required at institutional scale for real-time pricing

Disclaimer: For informational/educational purposes only. Not financial advice. Consult a licensed financial advisor before investing.

Part 2 — AI Infrastructure Pentest Surface Map

Attack vectors · Tools · Defensive strategies — Level by level · aiscan-security.online

AI infrastructure introduces attack surfaces across three fundamentally different domains: physical firmware (Level 1), cloud misconfiguration (Level 2), and AI-specific model attacks (Level 3). A compromised GPU firmware gives out-of-band server control. A misconfigured IAM role exposes training data. A successful prompt injection bypasses safety controls.

Engagement requirement: Written scope agreement required before any testing. Unauthorized access is illegal in all jurisdictions.

Pentest attack surface map — all 3 AI infrastructure levels

Level 1 Hardware	Level 2 Cloud	Level 3 AI Models
Attack vectors	**Attack vectors**	**Attack vectors**
GPU firmware exploit	IAM priv escalation	Prompt injection
BMC/IPMI takeover	S3 bucket exposure	Jailbreak bypass
PCIe DMA attack	Kubernetes escape	Model inversion
Supply chain implant	SSRF → metadata API	Training data poison
JTAG debug port	Insecure API keys	API key exfiltration
Side-channel (EM/power)	Container breakout	Adversarial inputs
Pentest tools	**Pentest tools**	**Pentest tools**
`Binwalk · Flashrom`	`Pacu · ScoutSuite`	`Garak · PyRIT`
`ipmitool · ipmiPwner`	`Prowler · CloudSploit`	`PromptBench · ART`
`PCILeech`	`kube-hunter`	`LLMFuzzer`
`ChipWhisperer`	`Nuclei · Nessus`	`Burp Suite+AI ext`
`Firmwalker`	`Trufflehog`	`OWASP LLM Top10`
Defensive steps	**Defensive steps**	**Defensive steps**
Secure Boot+UEFI sign	Zero-trust IAM+MFA	Input validation
BMC isolated VLAN	Private k8s API	Rate limit APIs
TPM 2.0 attestation	No public S3	Model access ctrl

Level 1 — Hardware & Firmware Pentesting

Step 1 — Recon IPMI/BMC exposure

nmap -sV -p 623,443,80,161 to identify exposed management interfaces. IPMI on public internet = immediate critical finding.

Step 2 — Test IPMI cipher-0 bypass

ipmitool -I lanplus -H -U '' -P '' chassis status — many older BMCs allow unauthenticated access via cipher-0 vulnerability.

Step 3 — Extract and analyse firmware

binwalk -e firmware.bin — look for hardcoded credentials, weak crypto, debug interfaces. firmwalker scans for sensitive strings inside extracted filesystems.

Step 4 — Physical firmware testing (lab only)

Flashrom for firmware dump. OpenOCD / JTAG debugger for live debugging. ChipWhisperer for power/EM side-channel analysis on crypto operations.

Step 5 — PCIe DMA attack

PCILeech with a DMA-capable device reads/writes system memory via PCIe — bypasses all OS security controls, can extract encryption keys from RAM.

Defenses:

- Disable IPMI remote; BMC on isolated VLAN, no internet
- Secure Boot + UEFI signature verification on all servers
- TPM 2.0 attestation to verify firmware integrity at boot
- SBOM from every hardware vendor; physical access biometric + card

Level 2 — Cloud Infrastructure Pentesting

Step 1 — Cloud security posture scan

Prowler or ScoutSuite: finds public S3, overpermissioned IAM, unencrypted storage, missing MFA, open security groups — covers AWS, Azure, GCP simultaneously.

Step 2 — IAM privilege escalation

Pacu (AWS exploit framework): enumerate permissions, escalate from low-privilege to admin. Common paths: iam:PassRole + lambda:InvokeFunction, iam:CreateAccessKey.

Step 3 — Secret and credential scanning

TruffleHog against git repos, CI/CD pipelines, S3 buckets. AI companies frequently commit OpenAI keys, AWS credentials, DB passwords to source control.

Step 4 — Kubernetes cluster testing

kube-hunter: anonymous API server access, etcd exposure, privilege escalation. kube-bench against CIS k8s benchmarks. Test privileged pod breakout + hostPath mounts.

Step 5 — SSRF to metadata endpoint

Test URL parameters for SSRF to 169.254.169.254 (AWS metadata). Successful SSRF gives IAM credentials and can lead to full account takeover.

Defenses:

- Least-privilege IAM; no wildcard * permissions; regular access reviews
- Block all public S3 at org level via Service Control Policies
- Kubernetes API server behind VPN; disable anonymous auth; audit logging
- CSPM tool (Wiz, Orca, Prisma Cloud) for continuous misconfiguration detection

Level 3 — AI Model & API Pentesting (OWASP LLM Top 10)

Step 1 — Automated LLM scan with Garak

garak --model_type rest --model_name — tests prompt injection, jailbreaks, data leakage, toxicity bypass, hallucination exploitation automatically.

Step 2 — Red-team with PyRIT

Microsoft PyRIT automates multi-turn adversarial conversations. Tests orchestration systems, plugins, tool-calling pipelines — not just single prompts.

Step 3 — API security testing with Burp Suite

Intercept and modify LLM API calls. Test: rate limiting (DoS), verbose errors leaking system prompts, IDOR across user sessions, unauthenticated endpoints.

Step 4 — Training data extraction

Prompt the model to repeat/complete content from training. PromptBench for adversarial suffixes causing consistent misbehaviour. ART (IBM) for adversarial robustness.

Step 5 — Plugin and tool-call injection

Indirect prompt injection: content the AI reads (webpages, docs) can contain instructions hijacking subsequent tool calls — especially dangerous with code execution plugins.

Defenses:

- Input validation + output sanitisation at API gateway layer
- Rate limit all model endpoints; per-user, per-IP, per-API-key
- Canary tokens in training data to detect and confirm exfiltration
- Never expose system prompts in error messages or API responses

Complete Pentest Toolchain — All 3 Levels

Organized by phase: Recon · Scan · Cloud · k8s · Firmware · Hardware · AI/ML · Web · Report

Phase	Tool	Level	Purpose
Recon	Nmap / Masscan	L1-L2	Port scan + service fingerprint
Recon	Shodan / Censys	L2	Internet-exposed AI assets
Recon	theHarvester	L2-L3	Email, subdomains, API endpoints
Scan	Nessus / OpenVAS	L1-L2	CVE detection across hosts
Scan	Nuclei	L2-L3	Template-based vuln scanner
Cloud	Pacu	L2	AWS exploitation framework
Cloud	ScoutSuite	L2	Multi-cloud security audit
Cloud	Prowler	L2	AWS/GCP/Azure misconfig
Cloud	Trufflehog	L2-L3	Leaked secrets in repos/CI
Cloud	Trivy	L2	Container image scanning
k8s	kube-hunter	L2	Kubernetes attack surface
k8s	kube-bench	L2	CIS Kubernetes benchmark
Firmware	Binwalk	L1	Firmware extraction + analysis
Firmware	Flashrom	L1	Read/write firmware chips
Firmware	ipmitool	L1	BMC/IPMI enumeration
Hardware	ChipWhisperer	L1	Side-channel / power analysis
Hardware	PCILeech	L1	PCIe DMA memory access
AI/ML	Garak	L3	LLM vulnerability scanner
AI/ML	PyRIT (Microsoft)	L3	AI red-team automation
AI/ML	PromptBench	L3	Adversarial prompt testing
AI/ML	ART (IBM)	L3	Adversarial robustness test
AI/ML	LLMFuzzer	L3	LLM API fuzzing
Web	Burp Suite	L2-L3	HTTP interception + AI plugins
Report	DefectDojo	All	Finding management + metrics

Your ASVH v7.5 Platform — Integration with 3-Level Framework

scanner.c (C multi-threaded TCP) [L1+L2] — Port scanner finds exposed IPMI (623), BMC management interfaces, cloud service endpoints. Add IPMI-specific probes and BMC banner grabbing for Level 1 coverage.

scanner.asm (x86-64 Assembly) [L1] — CPUID hardware fingerprinting: CPU vendor, features (AES-NI, AVX), virtualisation flags. Identifies hardware capabilities for firmware compatibility testing.

scanner.py (Python web scanner) [L2+L3] — HTTP/HTTPS vuln scanner already probes /.env, /.git/config, /actuator/env. Add AI paths: /v1/models, /api/chat, /api/generate, /admin/, /metrics for L3 coverage.

Web Vulnerability Scanner tab [L2+L3] — Add OWASP LLM Top 10 probe templates. Test prompt injection via HTTP parameters. Check API authentication, rate limiting, CORS configuration.

1,500-agent pool [All levels] — Distribute scanning load across subnets. Coordinate cloud posture checks and parallel model endpoint fuzzing across the full agent fleet.

Kali Linux — Install All Pentest Tools

```
# AI/ML specific tools
pip install garak pyrit promptbench adversarial-robustness-toolbox --break-system-packages
# Cloud security tools
pip install prowler scoutsuite pacu trufflehog checkov --break-system-packages
# Hardware/firmware
sudo apt install -y binwalk flashrom nmap masscan ipmitool nasm gcc
# Build ASVH scanner backends
bash build_scanners.sh
```

HEGA GEOFFROY RENE ERNEST

Blockchain · AI Security · Full-Stack · OpenClaw

Website	https://aiscan-security.online/
LinkedIn	https://www.linkedin.com/in/geoffroy-rene-hega-107952102/
Instagram	https://www.instagram.com/geoffroyrene/
GitHub	https://github.com/sakbayeme2015
Platform	ASVH v7.5 · aiscan-security.online · Douala, Cameroon

Hardware L1 | **Cloud L2** | **AI Models L3**

Pentesting | **Blockchain** | **Full-Stack**

OpenClaw · ASVH v7.5 AI Security Vulnerability Scanner · 2026

This document was authored by HEGA GEOFFROY RENE ERNEST for authorized security research