

NINE PILLARS OF

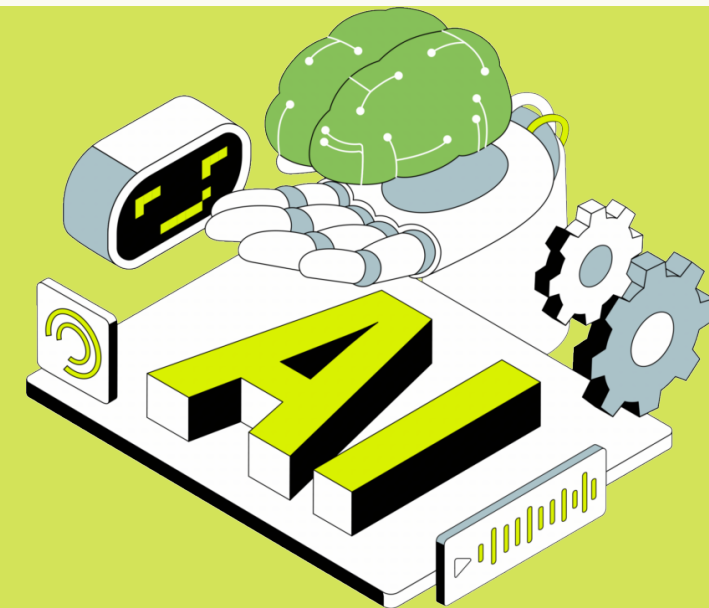
SECURITY & POSTURE OF YOUR GENERATIVE AI APPLICATIONS



1

AI VISIBILITY

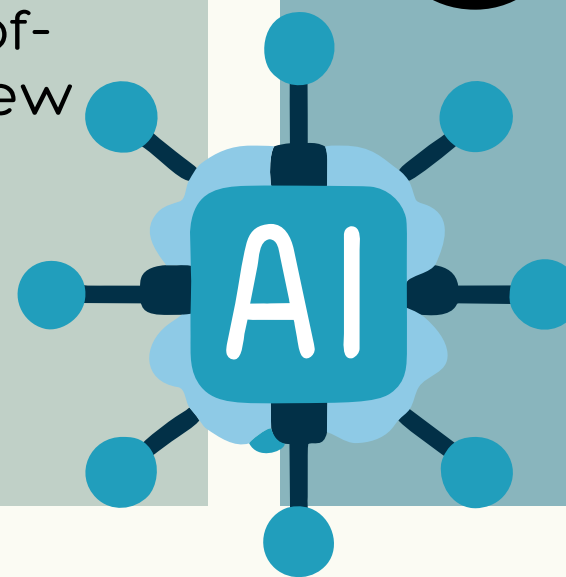
Discover, track, alert on insecure access, unusual usage of AI assets, AI Apps, AI agents, AI Workflows .



2

AI LINEAGE

Trace back to single point-of-origin with AI lineage. 360 view command, control, reconnaissance, lateral movements.



3

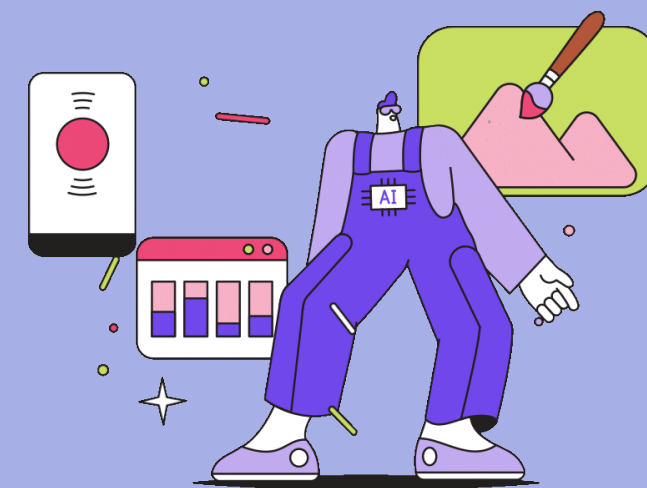
LLM & MODEL VULNERABILITIES

Automate LLM and model Vulnerability scan. Domain-specific integration, Model, LLM, Prompt, RAG, AI agent Vulnerability database.

4

DATA PRIVACY CONTROLS

Identify and Obfuscate Sensitive Information. Alert Sensitive information disclosures, Data privacy violations, Copyright Legal exposures .



5

DOMAIN-SPECIFIC GUARDRAILS

Use domain-specific security guardrails, in GenAI apps and workflows, track AI Agents, RAG tasks .Use Custom detections for application specific.filters, security controls.



NINE PILLARS OF

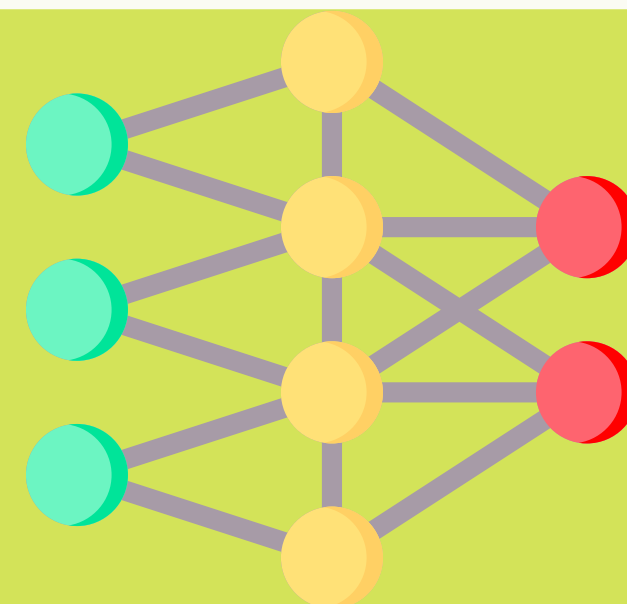
SECURITY & POSTURE OF YOUR GENERATIVE AI APPLICATIONS



6

AI INTEGRITY MONITORING

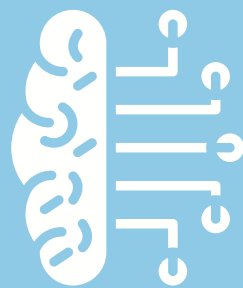
Secure, track Tokenizer Manipulations, and Detect Attacks on AI Integrity



7

ADVERSARIAL ML

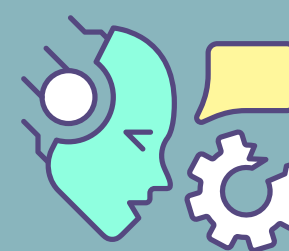
Poison, Evasion, Jailbreak, Exfiltration, Infiltration, Feature corruption attacks. Map Adversarial Threat Intelligence with Indicators of compromise (IOC) and indicators of attack (IOA).



8

PROMPT & MODEL BEHAVIOUR ANALYTICS

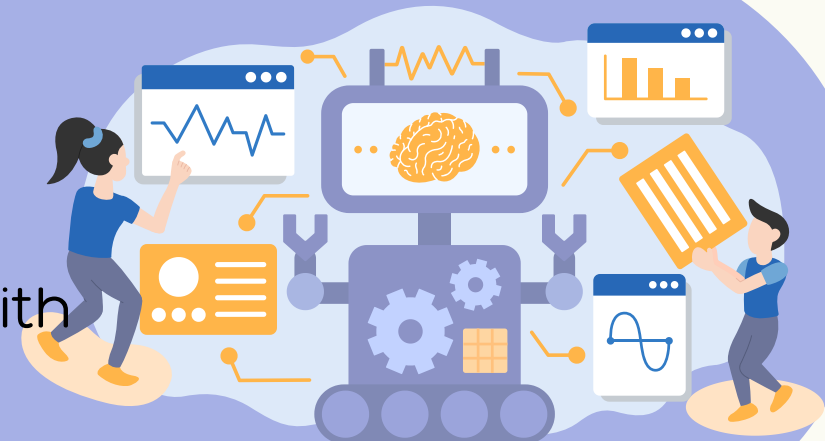
Discover Rogue Models, Risky Pipelines, Harmful Prompts



9

AI FORENSICS

Review, Reports, Audit, Compliance, Forensics. Enrich AIDR (AIDetection & Response) events with Alert data. Forward to AI SIEM, Audits, Governance, Compliance reports.





www.AlertAI.com
contact@alertai.com