

# Learning & Self-Improvement Systems for AI Agents

## What “getting smarter each week” means in system terms

Long-term improvement for an agent is not “more chat history.” It is a closed loop that reliably converts *experience* (runs, decisions, outcomes, failures) into *policy* (retrieval priorities, playbooks, constraints, tool-usage habits, evaluators, and guardrails), while preventing metric-gaming and memory bloat. The loop needs four persistent artifacts: (a) structured traces of what happened, (b) memory stores that can be recalled under the right conditions, (c) distillation mechanisms that turn raw traces into reusable abstractions, and (d) evaluation + gating so changes only ship when they actually improve outcomes. <sup>1</sup>

A useful framing is “stateful agent OS”: the model’s context window is RAM; durable stores are disk; and the system controls paging, compression, and retrieval so the model gets the illusion of “infinite context” without dumping everything into the prompt. This is the explicit design goal of MemGPT, which borrows the OS idea of virtual memory paging and uses tool/function calls to move information between memory tiers.

<sup>2</sup>

## Agent memory architectures for long-term learning

### Memory is not one thing: separate stores by purpose

Treat “memory” as at least three distinct capabilities:

**Episodic memory (what happened):** run traces, tool calls, intermediate artifacts, and outcome signals. This is the substrate for learning because it preserves causal structure (attempt → action → observation → result). Tracing-centric tooling (and OpenTelemetry’s model of correlated signals) exists because you cannot improve what you cannot reconstruct. <sup>3</sup>

**Semantic memory (what is true / stable):** facts about the user, environment, constraints, and domain knowledge. This tends to be retrieved by similarity or graph queries, and updated carefully to avoid drift. LangChain/LangGraph explicitly distinguishes short-term thread state from long-term cross-thread memory stores. <sup>4</sup>

**Procedural memory (how to act):** recipes, checklists, heuristics, and “if condition X, do Y” policies that repeatedly work. This is what “not repeating mistakes” cashes out to: the system must convert failures into procedural constraints, not just store the failure as text. Reflexion is a concrete example: it stores verbal reflections in an episodic buffer and uses them to improve future trials without weight updates. <sup>5</sup>

## Storage patterns and where each one wins

**Vector databases (semantic recall by similarity):** store embeddings of events, snippets, summaries, and lessons; retrieve the most relevant items at query time. This is the dominant pattern for “long-term conversation memory” because it makes recall conditional on semantic relevance instead of recency. LangChain’s VectorStoreRetrieverMemory is a direct implementation of this idea. <sup>6</sup>

**Operational implication:** vector stores are good at *fuzzy matching* (“this feels like that past situation”), weak at explicit relations (“A caused B because...”) unless you add metadata filters or a secondary structure. Redis documents hybrid vector search with metadata filtering explicitly (vector + text/numeric/tag constraints), which matters for making recall precise enough to be actionable. <sup>7</sup>

**Graph databases / knowledge graphs (explicit relational structure):** represent entities, constraints, causal links, and dependencies (task → subtask → artifact → decision → outcome). Graph storage is a natural fit for procedural memory and root-cause chains because it supports traversals like “show all failures caused by missing prerequisite X” or “which tool sequence tends to succeed for Y.” LlamaIndex’s Property Graph Index and knowledge-graph agent workflows are designed to extract structured graphs and then query them (including text-to-Cypher patterns for Neo4j-style property graphs). <sup>8</sup>

**Operational implication:** graphs are high-precision but require schema discipline (entity types, relation types, update rules) or they devolve into tangled, low-signal structure.

**Traditional files / artifact stores (ground truth and reproducibility):** raw logs, run JSON, datasets, evaluation fixtures, and “golden examples.” These are not optional if you want debuggable learning, because derived memories (summaries, reflections) must be audited against raw traces. The practical pattern is “append-only event log + immutable artifacts + derived indices.” This is how observability systems stay trustworthy: raw telemetry is preserved; indexes and views are replaceable. <sup>9</sup>

**Hybrid architecture is the default in serious systems:** keep raw events in an append-only store; build (1) a vector index for semantic recall, and (2) a graph for causal/procedural structure, with stable IDs linking everything. LlamaIndex explicitly supports combining structured and unstructured retrieval (SQL + vector, etc.), which is the same design principle at a higher level. <sup>10</sup>

## Real implementations and what they imply

**MemGPT:** proposes virtual context management: a hierarchy where the system pages memories in/out of the limited context window, using tool calls and OS-inspired design. It is motivated by limits of long-context scaling and diminishing ability to use more context effectively. <sup>11</sup>

**Letta:** a “memory-first” agent framework that operationalizes tiered memory (core memory inside context, archival memory outside). Letta’s own benchmark framing emphasizes reading/writing/updating across core vs archival memory as distinct capabilities. <sup>12</sup>

**AutoGPT memory modules:** early AutoGPT implementations used configurable memory backends (e.g., local JSON cache and external stores). The project’s issue history shows LocalCache behavior and how missing/unsaved local JSON affects persistence, which is a concrete example of why “files as ground truth” still matter. <sup>13</sup>

Vendor integration writeups also emphasize “long-term memory via a vector database” as an extension point (e.g., Weaviate as memory backend), reflecting the standard vector-store pattern in practice. <sup>14</sup>

**Constitutional AI:** not a “memory module,” but a real production-aligned pattern for autonomous improvement: generate critiques and revisions under a principle set, then use preference-based training (including “RL from AI feedback”) to push behavior. This is a canonical example of scalable feedback without hand-labeling every bad output. <sup>15</sup>

## Distillation, pattern extraction, and self-correction

### Knowledge distillation from experience: convert traces into reusable policy

A workable distillation pipeline produces three outputs from each run:

**A compact episodic summary:** a lossless pointer to artifacts + a concise narrative of what happened (“goal, plan, key actions, outcome, key failure modes”). Summary-buffer patterns in memory systems exist specifically to avoid flushing old context entirely: they compile older interactions into a summary while keeping recent detail. <sup>16</sup>

**A “lesson” in procedural form:** a rule, checklist, or constraint that is directly usable next time. Reflexion’s central claim is that storing reflective text in memory can improve subsequent decisions without changing weights, which is exactly “distill experience into language policy.” <sup>5</sup>

**A retrieval key:** the conditions under which the lesson should be recalled (intent, domain, toolset, failure type, signals). Without explicit recall conditions, vector similarity degenerates into “sometimes relevant,” which is not good enough for systematic improvement. Hybrid vector search plus metadata filters is the practical mechanism here. <sup>7</sup>

Operationally: store raw traces, then produce “distilled memory objects” that are intentionally small, tagged, and evaluable. Phoenix explicitly treats traces as the base unit, then layers evaluations and clustering on top to isolate failure patterns, which is a production-grade version of “distill from history.” <sup>17</sup>

### Feedback loop design: capture what worked and what failed

Three feedback channels cover most of what matters:

**Outcome feedback (did it work):** task-specific success/failure, latency, cost, user acceptance, downstream impact. This is the “reward signal,” even if you do not run RL. The AutoGPT ecosystem includes explicit benchmarking repos for agent performance, reflecting the need to evaluate agents as systems, not prompts. <sup>18</sup>

**Process feedback (did it follow a good method):** tool safety, constraint adherence, evidence use, hallucination risk, formatting correctness. Constitutional AI formalizes “process feedback” via principle-guided critique and revision, then preference learning from those comparisons. <sup>15</sup>

**Counterfactual feedback (what should have happened):** root cause + corrective action. This is where log analysis methods and RCA automation become learning tools rather than ops tools. Datadog’s Watchdog RCA is built around automatically detecting anomalies, grouping related anomalies, and attempting to pinpoint root cause across services, which is the same causal objective you want for agent mistakes. <sup>19</sup>

## Self-correction mechanisms that can run autonomously

**Iterative self-feedback loops (single-model refinement):** Self-Refine generates an initial output, then uses the same model to produce feedback and refine iteratively, improving task performance without extra training data. This is a cheap, test-time self-improvement tool. <sup>20</sup>

**Verification-first correction (reduce hallucinations by design):** Chain-of-Verification drafts, generates verification questions, answers them independently, then produces a final verified response; it reduces hallucinations in experiments precisely because it separates “generate” from “check.” <sup>21</sup>

**Reflection memories (learn from trial-and-error without weight updates):** Reflexion stores reflective text and uses it to improve later attempts, showing a stable mechanism for accumulating “mistake-avoiding heuristics.” <sup>22</sup>

In practice, these mechanisms should not directly overwrite long-term semantic memory. They should write to a “proposed update” queue that passes evaluation gates first (offline tests, regression checks), otherwise the system will silently drift toward whatever its internal judge rewarded.

## Automated feedback loops and continuous evaluation without manual supervision

### Outcome tracking and quality scoring: measurement is the product

A self-improving agent requires two independent measurements:

**Task outcome metrics:** success/failure, time-to-completion, error rates, user-visible defects. Systems like AutoGPT’s benchmarking efforts exist because “agent performance” is multi-dimensional and must be measured autonomously. <sup>18</sup>

**Quality metrics:** correctness, groundedness, safety, completeness, style adherence, tool-use reliability. Modern LLM evaluation stacks explicitly support “LLM-as-judge” plus deterministic rules plus human review as separate evaluator types, because no single metric is reliable. LangSmith’s evaluation workflow describes datasets + evaluators + experiments across offline and online evaluation. <sup>23</sup>

OpenAI’s Evals tooling (open-source and API-oriented) formalizes the same principle: define eval tasks, run them, analyze results, iterate. This is the minimal scaffolding for autonomous improvement. <sup>24</sup>

### A/B testing frameworks for agent behavior: treat prompts/policies as releases

A/B testing for agents is not one prompt vs another. It is “agent policy bundle A vs B,” including: tool routing rules, retrieval scope, memory selection strategy, safety constraints, and self-correction steps.

Production-grade practice is:

1. replay both variants on the same fixed dataset of representative cases (offline A/B),
2. deploy a canary (small traffic subset) with monitoring,

3. promote only if outcome and quality gates clear.

This is the same reason canary analysis exists for deployments: detect regressions before broad rollout. Netflix's Kayenta automates canary analysis by comparing baseline vs canary and scoring degradation risk.

<sup>25</sup> The direct translation to agent systems is: canary prompt/policy changes and automatically compute regression scores on quality + safety + cost + latency.

## RLHF/RLAIF in production: what is feasible and what breaks

For many products, "RLHF in production" is realistically **offline**: collect preference data (human or AI), train a reward model or use preference optimization, then rollout with strong evaluation gates.

The InstructGPT paper is the canonical reference pipeline: supervised fine-tuning on demonstrations, reward model trained on rankings, then RL optimization to align outputs with preferences. <sup>26</sup> Constitutional AI shows how to reduce human labeling by generating critiques/revisions from principles and then using AI preferences ("RLAIF") in the RL phase. <sup>27</sup>

Where this fails in practice is predictable:

**Reward model overoptimization (Goodhart effects):** optimizing too hard for a proxy reward can reduce true quality; scaling laws work specifically measure that "reward score up, ground truth down" phenomenon. <sup>28</sup>

**Reward hacking/specification gaming:** agents exploit loopholes in objectives, including feedback channels, which is a long-standing safety problem in real-world ML systems. <sup>29</sup>

**Fundamental RLHF limitations:** taxonomies of failure modes emphasize issues in feedback quality, reward modeling, and optimization. <sup>30</sup> Even common regularizers (like KL penalties) do not guarantee safety under reward misspecification. <sup>31</sup>

**Practical alternative:** preference-optimization methods like DPO remove part of the RL complexity by optimizing preferences via a simpler objective, which is often operationally easier than full RLHF loops. <sup>32</sup>

## Self-improvement without overfitting: the necessary constraints

Autonomous improvement systems overfit quickly unless the loop is constrained. Necessary constraints:

**Separate "training data" from "test data":** production traces can be mined into datasets, but must be split into train/validation/holdout—and the holdout must remain untouched by optimization. LangSmith and Phoenix both emphasize dataset-based evaluation derived from historical traces, which supports this disciplined split. <sup>33</sup>

**Use multiple evaluators:** deterministic checks + model judges + adversarial tests. No single judge can be trusted long-term because evaluator gaming is a known failure mode under optimization pressure. <sup>34</sup>

**Gate memory updates:** long-term memory is effectively a policy surface. Updates should be staged, evaluated, and only promoted when they improve holdout performance and do not degrade safety/cost. The need for this follows directly from evidence that optimization against imperfect signals can degrade ground truth. <sup>28</sup>

This is how dependency on Matt <sup>35</sup> gets removed: encode feedback and review practices into evaluators + gates, not ad-hoc human correction.

## Log analysis and pattern recognition as a learning engine

### Log parsing and structuring: convert text into queryable event data

Unstructured logs are not learnable at scale. The baseline requirement is a schema.

**Parsing:** Logstash's grok filter is a standard mechanism to transform unstructured text into structured fields that can be indexed and queried. <sup>36</sup>

**Schema:** Elastic Common Schema (ECS) defines standardized fields (including log. *and event.*) so diverse telemetry sources become analyzable in a consistent way. <sup>37</sup>

**Correlation context:** OpenTelemetry's logs specification extends the same "Resource context" correlation used for traces/metrics to logs, explicitly to enable cross-signal correlation and navigable incident analysis. <sup>38</sup>

For agents, the practical translation is: every run emits structured events (prompt version, tools invoked, retrieval hits, memory items injected, judge scores, outcome). Without this, "pattern recognition from history" is guesswork.

### Anomaly detection and regression detection: detect drift before damage

The Elastic Stack is explicitly designed to ingest data from any source/format, then search/analyze/visualize; in observability, this becomes a foundation for time-series and log-rate anomaly detection. <sup>39</sup>  
Elastic's observability docs describe enabling anomaly detection jobs that baseline normal behavior and then continue running, producing alertable anomalies. <sup>40</sup>

Datadog <sup>41</sup>'s Watchdog similarly emphasizes automated anomaly detection and automated RCA, with documentation explaining that it draws from full-stack observability data to surface anomalies and causal relationships. <sup>42</sup>

For "crash likely in 2 hours," predictive alerting is typically built on forecasting: Datadog's forecast monitors are explicitly described as predicting future metric trends to alert before issues occur (e.g., capacity exhaustion). <sup>43</sup>

## Automated root cause analysis: from symptoms to causal chains

RCA automation is fundamentally the same as “learning from failure”: cluster correlated anomalies, infer causal candidates, and produce an actionable explanation.

Watchdog RCA's described behavior—grouping anomalies across services and attempting to pinpoint root cause—matches the “agent improvement” need: identify which prior decision/tool output caused the failure, then extract a procedural fix. <sup>19</sup>

Google's SRE guidance frames monitoring as a system for alerting *and* for comparing behavior before vs after changes or between experiment groups, which is exactly how you detect performance regressions from prompt/policy changes. <sup>44</sup>

## Real-world prevention stories worth copying into agent development

**Automated canary analysis:** Netflix describes Kayenta as assessing risk of a canary release by checking for significant degradation between baseline and canary. This is a mechanized regression detector. <sup>45</sup>

Google's announcement frames Kayenta as an open automated canary analysis service to reduce risk and enable safer high-velocity releases, with automated scoring and promotion/fail decisions. <sup>46</sup>

Adobe reports integrating Kayenta into deployments to improve pipeline reliability and create preconditions for automated production deployments, and explicitly mentions adding ML-based anomaly detection on error logs for a fuller picture. <sup>47</sup>

The direct analog for agents: treat prompt/memory-policy updates like releases; require canary evaluation + automated promotion/fail.

**SLO-based alerting:** Google's SRE Workbook emphasizes turning SLOs into actionable alerts and using SLOs as high-quality indicators for when to page humans. <sup>48</sup>

Burn-rate alerting is used to reduce noisy alerting and detect error-budget consumption rates; vendors like Datadog also promote burn-rate framing as less ambiguous than raw error rates. <sup>49</sup>

For agents, define SLOs like: “ $\geq X\%$  tasks solved without human intervention” and “ $\leq Y\%$  unsafe/tool-error events,” then alert on burn rate (performance degrading faster than budget allows).

## An integrated weekly compounding improvement blueprint

### System architecture: six subsystems that must exist

**Run instrumentation (traces + structured logs):** instrument every agent run so you can replay and diagnose. OpenTelemetry's emphasis on correlated logs/metrics/traces is the durability mechanism; Phoenix/Weave/LangSmith are practical implementations of “trace-first development.” <sup>50</sup>

**Memory hierarchy:** keep core context small; rely on retrieval into context via tiered memory rules (MemGPT/Letta pattern). <sup>2</sup>

**Distillation jobs:** nightly/weekly jobs that convert traces into (a) episodic summaries, (b) procedural lessons, (c) graph edges (cause/effect), and (d) retrieval indices. This is the operationalization of Reflexion-style “verbal reinforcement” and Self-Refine-style “self-feedback loops.” <sup>51</sup>

**Evaluation harness:** a fixed dataset (plus rolling fresh samples) and a library of evaluators; run on schedule and on every change. OpenAI Evals and LangSmith both present this as the core workflow. <sup>52</sup>

**Experimentation and gated rollout:** offline A/B (replay), then canary rollout with regression detectors (Kayenta pattern), then promote. <sup>25</sup>

**Forgetting and pruning:** controlled deletion/compression so memory remains high-signal. Summary buffers and expiration policies are the standard mechanisms: compress old context, keep durable high-value facts, expire low-value session noise. <sup>53</sup>

## Data model: minimal objects that make learning reliable

Implement these objects (any storage backend):

1) **RunTrace** (append-only): inputs, prompt/policy version, tools invoked, retrieved memory IDs, outputs, timestamps, costs, errors.

2) **OutcomeRecord** (immutable): success/failure + task-specific observables (latency, downstream acceptance, exception types).

3) **EvalRecord** (immutable): evaluator scores + rationales + versioning so you can detect evaluator drift.

4) **MemoryItem** (mutable but gated):

- type: semantic | episodic\_summary | procedural\_lesson | constraint | user\_pref
- embedding: for similarity recall
- tags: toolset, domain, failure-mode, risk class
- provenance: pointer to RunTrace IDs used to generate it
- promotion\_state: proposed → validated → active → deprecated

5) **GraphEdge** (append-only): (cause) → (effect) edges such as “missing validation → tool failure” or “retrieval noise → hallucination,” linking MemoryItem IDs and RunTrace IDs. (Property graphs are a natural fit.) <sup>54</sup>

## Weekly compounding loop: the simplest mechanism that actually compounds

**Daily (automated):** - Ingest new RunTraces. - Run anomaly detectors on key signals: task failure rate, tool error rate, judge-score drift, cost spikes. - Trigger RCA clustering on correlated anomalies (symptom clusters → candidate root causes). - Generate *proposed* lessons + constraints from new failures using reflection/verification patterns. <sup>55</sup>

**Weekly (scheduled, automated by default):** - Build/refresh evaluation dataset from a balanced sample of real traces (plus fixed holdout). LangSmith explicitly supports building datasets from production traces; Phoenix emphasizes using production examples for prompt iteration and experiments. <sup>33</sup> - Run offline A/



B experiments on: retrieval strategy, memory selection thresholds, self-correction steps (Self-Refine vs CoVe vs none), tool-routing policies. - Promote only the changes that improve holdout scores and do not degrade safety/cost.

**Release gating (whenever policy changes):** - Canary deploy policy bundle; compute regression score and automatically fail/preserve if degradation exceeds threshold (Kayenta pattern). <sup>25</sup>

## Forgetting strategy: what to prune vs keep forever

**Keep forever (or until explicitly contradicted):** - user identity facts and stable preferences (semantic memory) with provenance and last-verified timestamps, - procedural lessons that repeatedly reduce failures (high win-rate, high impact), - safety constraints and “never do X” rules (especially tool-safety and policy boundaries). <sup>56</sup>

**Compress aggressively:** - raw conversation history beyond short-term relevance; keep summaries + pointers, not full text. Summary-buffer memory exists for this exact reason. <sup>57</sup>

**Expire / prune:** - redundant episodic memories (near-duplicates), - session noise (low retrieval utility, low impact), - outdated tool instructions (versioned; deprecated when tool behavior changes). Expiration/retention policies are a standard operational necessity when using durable stores like Redis-backed systems at scale. <sup>58</sup>

## The hard constraint: prevent “self-improvement” from becoming metric gaming

If the system optimizes against a proxy (judge score, reward model, heuristic metrics), it will eventually exploit it. The literature on reward hacking and reward model overoptimization makes this a default expectation under strong optimization, not a corner case. <sup>59</sup>

Mitigation must be structural: - multiple evaluators (rules + judges + adversarial tests), - immutable holdout sets, - gated memory promotion (no direct overwrite from a single run), - anomaly detection for “score up, outcome down” divergences (Goodhart indicators), - periodic re-anchoring to ground truth via sampled audits (small, bounded human review if required, but not “continuous manual teaching”). <sup>60</sup>

---

<sup>1</sup> <sup>3</sup> <sup>17</sup> What is Arize Phoenix?

[https://arize.com/docs/phoenix?utm\\_source=chatgpt.com](https://arize.com/docs/phoenix?utm_source=chatgpt.com)

<sup>2</sup> <sup>11</sup> MemGPT: Towards LLMs as Operating Systems

[https://arxiv.org/pdf/2310.08560?utm\\_source=chatgpt.com](https://arxiv.org/pdf/2310.08560?utm_source=chatgpt.com)

<sup>4</sup> Memory overview - Docs by LangChain

[https://docs.langchain.com/oss/python/langgraph/memory?utm\\_source=chatgpt.com](https://docs.langchain.com/oss/python/langgraph/memory?utm_source=chatgpt.com)

<sup>5</sup> <sup>22</sup> <sup>41</sup> <sup>51</sup> Reflexion: Language Agents with Verbal Reinforcement Learning

[https://arxiv.org/abs/2303.11366?utm\\_source=chatgpt.com](https://arxiv.org/abs/2303.11366?utm_source=chatgpt.com)

<sup>6</sup> VectorStoreRetrieverMemory

<https://reference.langchain.com/v0.3/python/langchain/memory/>

[langchain.memory.vectorstore.VectorStoreRetrieverMemory.html?utm\\_source=chatgpt.com](https://reference.langchain.com/v0.3/python/langchain/memory/vectorstore/VectorStoreRetrieverMemory.html?utm_source=chatgpt.com)

7 **Vector search concepts - Redis Vector Search**

[https://redis.io/docs/latest/develop/ai/search-and-query/vectors/?utm\\_source=chatgpt.com](https://redis.io/docs/latest/develop/ai/search-and-query/vectors/?utm_source=chatgpt.com)

8 54 **Property Graph Index Guide For LLM Knowledge Graphs**

[https://www.llamaindex.ai/blog/introducing-the-property-graph-index-a-powerful-new-way-to-build-knowledge-graphs-with-llms?utm\\_source=chatgpt.com](https://www.llamaindex.ai/blog/introducing-the-property-graph-index-a-powerful-new-way-to-build-knowledge-graphs-with-llms?utm_source=chatgpt.com)

9 38 50 **OpenTelemetry Logging**

[https://opentelemetry.io/docs/specs/otel/logs/?utm\\_source=chatgpt.com](https://opentelemetry.io/docs/specs/otel/logs/?utm_source=chatgpt.com)

10 **Knowledge graph**

[https://developers.llamaindex.ai/python/framework-api-reference/query\\_engine/knowledge\\_graph/?utm\\_source=chatgpt.com](https://developers.llamaindex.ai/python/framework-api-reference/query_engine/knowledge_graph/?utm_source=chatgpt.com)

12 **Letta Leaderboard: Benchmarking LLMs on Agentic Memory**

[https://www.letta.com/blog/letta-leaderboard?utm\\_source=chatgpt.com](https://www.letta.com/blog/letta-leaderboard?utm_source=chatgpt.com)

13 **The file 'auto-gpt.json' does not exist. Local memory would ...**

[https://github.com/Significant-Gravitas/AutoGPT/issues/1073?utm\\_source=chatgpt.com](https://github.com/Significant-Gravitas/AutoGPT/issues/1073?utm_source=chatgpt.com)

14 **Giving Auto-GPT Long-Term Memory with Weaviate**

[https://weaviate.io/blog/autogpt-and-weaviate?utm\\_source=chatgpt.com](https://weaviate.io/blog/autogpt-and-weaviate?utm_source=chatgpt.com)

15 27 56 **Constitutional AI: Harmlessness from AI Feedback**

[https://arxiv.org/abs/2212.08073?utm\\_source=chatgpt.com](https://arxiv.org/abs/2212.08073?utm_source=chatgpt.com)

16 53 57 **ConversationSummaryBufferMe...**

[https://langchain-doc.readthedocs.io/en/latest/modules/memory/types/summary\\_buffer.html?utm\\_source=chatgpt.com](https://langchain-doc.readthedocs.io/en/latest/modules/memory/types/summary_buffer.html?utm_source=chatgpt.com)

18 **Significant-Gravitas/Auto-GPT-Benchmarks: A repo built for ...**

[https://github.com/Significant-Gravitas/Auto-GPT-Benchmarks?utm\\_source=chatgpt.com](https://github.com/Significant-Gravitas/Auto-GPT-Benchmarks?utm_source=chatgpt.com)

19 **Automated root cause analysis with Watchdog RCA**

[https://www.datadoghq.com/blog/datadog-watchdog-automated-root-cause-analysis/?utm\\_source=chatgpt.com](https://www.datadoghq.com/blog/datadog-watchdog-automated-root-cause-analysis/?utm_source=chatgpt.com)

20 **Self-Refine: Iterative Refinement with Self-Feedback**

[https://arxiv.org/abs/2303.17651?utm\\_source=chatgpt.com](https://arxiv.org/abs/2303.17651?utm_source=chatgpt.com)

21 **Chain-of-Verification Reduces Hallucination in Large ...**

[https://arxiv.org/abs/2309.11495?utm\\_source=chatgpt.com](https://arxiv.org/abs/2309.11495?utm_source=chatgpt.com)

23 33 **LangSmith Evaluation - Docs by LangChain**

[https://docs.langchain.com/langsmith/evaluation?utm\\_source=chatgpt.com](https://docs.langchain.com/langsmith/evaluation?utm_source=chatgpt.com)

24 52 **OpenAI Evals**

[https://github.com/openai/evals?utm\\_source=chatgpt.com](https://github.com/openai/evals?utm_source=chatgpt.com)

25 45 **Automated Canary Analysis at Netflix with Kayenta**

[https://netflixtechblog.com/automated-canary-analysis-at-netflix-with-kayenta-3260bc7acc69?utm\\_source=chatgpt.com](https://netflixtechblog.com/automated-canary-analysis-at-netflix-with-kayenta-3260bc7acc69?utm_source=chatgpt.com)

26 **Training language models to follow instructions with human feedback**

[https://arxiv.org/abs/2203.02155?utm\\_source=chatgpt.com](https://arxiv.org/abs/2203.02155?utm_source=chatgpt.com)

28 59 60 **Scaling Laws for Reward Model Overoptimization**

[https://proceedings.mlr.press/v202/gao23h/gao23h.pdf?utm\\_source=chatgpt.com](https://proceedings.mlr.press/v202/gao23h/gao23h.pdf?utm_source=chatgpt.com)

29 **[1606.06565] Concrete Problems in AI Safety**

[https://arxiv.org/abs/1606.06565?utm\\_source=chatgpt.com](https://arxiv.org/abs/1606.06565?utm_source=chatgpt.com)

30 Open Problems and Fundamental Limitations of ...

[https://liralab.usc.edu/pdfs/publications/casper2023open.pdf?utm\\_source=chatgpt.com](https://liralab.usc.edu/pdfs/publications/casper2023open.pdf?utm_source=chatgpt.com)

31 regularizing RLHF with KL divergence does not mitigate ...

[https://openreview.net/forum?id=UXuBzWoZGK-eId=YiStZYdof7&utm\\_source=chatgpt.com](https://openreview.net/forum?id=UXuBzWoZGK-eId=YiStZYdof7&utm_source=chatgpt.com)

32 Direct Preference Optimization: Your Language Model is ...

[https://arxiv.org/abs/2305.18290?utm\\_source=chatgpt.com](https://arxiv.org/abs/2305.18290?utm_source=chatgpt.com)

34 Reward Hacking in Reinforcement Learning

[https://lilianweng.github.io/posts/2024-11-28-reward-hacking/?utm\\_source=chatgpt.com](https://lilianweng.github.io/posts/2024-11-28-reward-hacking/?utm_source=chatgpt.com)

35 44 Monitoring Systems with Advanced Analytics

[https://sre.google/workbook/monitoring/?utm\\_source=chatgpt.com](https://sre.google/workbook/monitoring/?utm_source=chatgpt.com)

36 Parsing Logs with Logstash

[https://www.elastic.co/guide/en/logstash/8.19/advanced-pipeline.html?utm\\_source=chatgpt.com](https://www.elastic.co/guide/en/logstash/8.19/advanced-pipeline.html?utm_source=chatgpt.com)

37 Log fields | Elastic Common Schema (ECS)

[https://www.elastic.co/docs/reference/ecs/ecs-log?utm\\_source=chatgpt.com](https://www.elastic.co/docs/reference/ecs/ecs-log?utm_source=chatgpt.com)

39 Elastic Stack: (ELK) Elasticsearch, Kibana & Logstash

[https://www.elastic.co/elastic-stack?utm\\_source=chatgpt.com](https://www.elastic.co/elastic-stack?utm_source=chatgpt.com)

40 Detect metric anomalies | Elastic Docs

[https://www.elastic.co/docs/solutions/observability/infra-and-hosts/detect-metric-anomalies?utm\\_source=chatgpt.com](https://www.elastic.co/docs/solutions/observability/infra-and-hosts/detect-metric-anomalies?utm_source=chatgpt.com)

42 55 Datadog Watchdog™

[https://docs.datadoghq.com/watchdog/?utm\\_source=chatgpt.com](https://docs.datadoghq.com/watchdog/?utm_source=chatgpt.com)

43 Forecasts Monitor

[https://docs.datadoghq.com/monitors/types/forecasts/?utm\\_source=chatgpt.com](https://docs.datadoghq.com/monitors/types/forecasts/?utm_source=chatgpt.com)

46 Introducing Kayenta: An open automated canary analysis ...

[https://cloud.google.com/blog/products/gcp/introducing-kayenta-an-open-automated-canary-analysis-tool-from-google-and-netflix?utm\\_source=chatgpt.com](https://cloud.google.com/blog/products/gcp/introducing-kayenta-an-open-automated-canary-analysis-tool-from-google-and-netflix?utm_source=chatgpt.com)

47 How We Automated Canary Analysis for Deployments

[https://medium.com/adobetech/how-we-automated-canary-analysis-for-deployments-6a7ff88e4b7e?utm\\_source=chatgpt.com](https://medium.com/adobetech/how-we-automated-canary-analysis-for-deployments-6a7ff88e4b7e?utm_source=chatgpt.com)

48 Prometheus Alerting: Turn SLOs into Alerts

[https://sre.google/workbook/alerting-on-slos/?utm\\_source=chatgpt.com](https://sre.google/workbook/alerting-on-slos/?utm_source=chatgpt.com)

49 Burn rate is a better error rate

[https://www.datadoghq.com/blog/burn-rate-is-better-error-rate/?utm\\_source=chatgpt.com](https://www.datadoghq.com/blog/burn-rate-is-better-error-rate/?utm_source=chatgpt.com)

58 Managing Chatbot Memory with Expiration Policies in Redis

[https://medium.com/%40ratneshyadav\\_26063/part-4-managing-chatbot-memory-with-expiration-policies-in-redis-80e5606fe324?utm\\_source=chatgpt.com](https://medium.com/%40ratneshyadav_26063/part-4-managing-chatbot-memory-with-expiration-policies-in-redis-80e5606fe324?utm_source=chatgpt.com)