POWERED BY MOZILLA

ODIN THREAT FEED DATASHEET

Real World Vulnerability Feed For LLM's

Fortify your GenAI deployments with real-time intelligence drawn directly from 0DIN's research and pioneering GenAI Bug-Bounty program.

BOLSTER YOUR GENAI DEFENSES KNOWING YOUR WEAK SPOTS.

As global enterprises scale GenAI to drive innovation and efficiency, adversaries just as quickly probe for novel attack in models that ingest live data, call external plugins, and adapt on-the-fly to compromise infrastructures. 0DIN's Threat Feed is engineered to close that gap.

- Real-World Adversary Data, Not Simulations
  Our weaponized techniques are delivering the exact tactics now being used against production models.
- Comprehensive Visibility - Ongoing research, uncovering misconfigurations, insecure integrations, and logic flaws allow organization to understand their data exposure.
- Actionable Hardening Guidance - Each finding arrives with step-by-step understanding of why the compromise is successful and guardrail rules so security and ML teams can detect and manage risks.

Backed by industry-leading research regularly featured in tier-one media platforms, 0DIN keeps enterprises ahead of the threat curve enabling confident, secure adoption of transformative GenAI at enterprise scale.

Why Choose 0din.ai's GenAI–Driven Threat Feed?

Accelerated Threat Recognition

0din.ai's advanced Threat Feeds rapidly allows for the detecting of anomalies with 0DIN Signatures - hybrid prompt pattern matching (keywords + semantic + LLM) detection with heightened speed and precision.

Strategic Threat Anticipation

Leveraging predictive models, 0din.ai moves beyond reactive defense. Our feed provides foresight into emerging threat vectors and attacker behaviors.

With this intelligence, organizations can proactively reinforce vulnerable systems, simulate breach scenarios to bolster preparedness. This forward-looking approach helps reduce exposure to high-impact cyber events and strengthens overall resilience.

Intelligent Resource Allocation

By automating the collection, enrichment, and analysis of threat intelligence, 0din.ai frees security teams from the burden of understanding why an event was detected instead of manually triaging.

KEY BENEFITS

Enhance Detection Accuracy:
Improve anomaly & vulnerability detection using real-world adversarial insights directly derived from simulated and actual threat environments.

Stay Ahead of Threat Actors:
Leverage timely intelligence on emerging LLM exploitation techniques before they become widespread in the wild.

Integrate Seamlessly Across Environments:
Designed for plug-and-play integration into existing SOC and threat intelligence workflows for minimal overhead via API.

Empower Strategic Security Planning:
Inform red-teaming, tabletop exercises, and security architecture decisions with high-fidelity threat data.

Mitigate Real-Time Risks:
Utilize findings from successful and failed adversarial attempts to preemptively secure your GenAI systems.

Support Proactive Governance & Compliance:
Bolster documentation and regulatory readiness with data-backed insights from a recognized GenAI threat research initiative.

As AI systems advance, conventional defenses can't keep pace with the sophistication of emerging threats. Without preemptive security measures, critical data and infrastructure remain exposed.

0DIN's Threat Feeds empower you with real-time, adversary-aware intelligence arming your GenAI deployments with the foresight needed to neutralize attacks before they materialize.

Product Specifications

1. Platform Overview
   - Product Name: 0Din Threat Feed
   - Release Model: Subscription-based GenAI threat intelligence service
   - Core Offering: Verified vulnerability data and analytics across GenAI models
   - User Interface: Web dashboard with interactive visualizations and REST API
2. Core Features

A. Dashboard Analytics
- Visual summaries of total threat reports, model vulnerabilities, and trend timelines
- One-shot vulnerability identification
- Heatmaps and radar graphs for taxonomy & model vulnerabilities
- Geographic mapping of researcher submissions
- Categorized jailbreak strategy analysis (e.g., Language, Stratagems)

B. Detailed Vulnerability Reports
- Vulnerability title, UUID, and severity level (Low to Severe)
- Technical breakdown: affected models, taxonomy, and attack techniques
- Sample prompts and responses demonstrating exploits
- Test results including reproducibility scores and temperature sensitivity
- Social impact scoring (Level 1–10)
- Nudity Risk Rating: Abstract/Symbolic Representation (highly stylized, minimal anatomical detail)

C. API Access
- RESTful API access to the same vulnerability data presented in the dashboard
- Supports rich filtering and search across multiple fields (e.g., severity, model, taxonomy)
- JSON-based responses optimized for integration with security tools and dashboards
- Secure token-based access
- Rate limiting

3. User Access Model
   - Multi-User Access: Organizations can onboard teams via grouped permissions
   - Multi-Factor Authentication (MFA): Required for all platform access
   - Access Bound to Group Membership: All permissions are inherited from assigned group roles

0DIN: Securing Tomorrows AI.

Learn More: https://www.0din.ai
Email: 0din@mozilla.com