Sentinel Gateway Cybersecurity Simulation

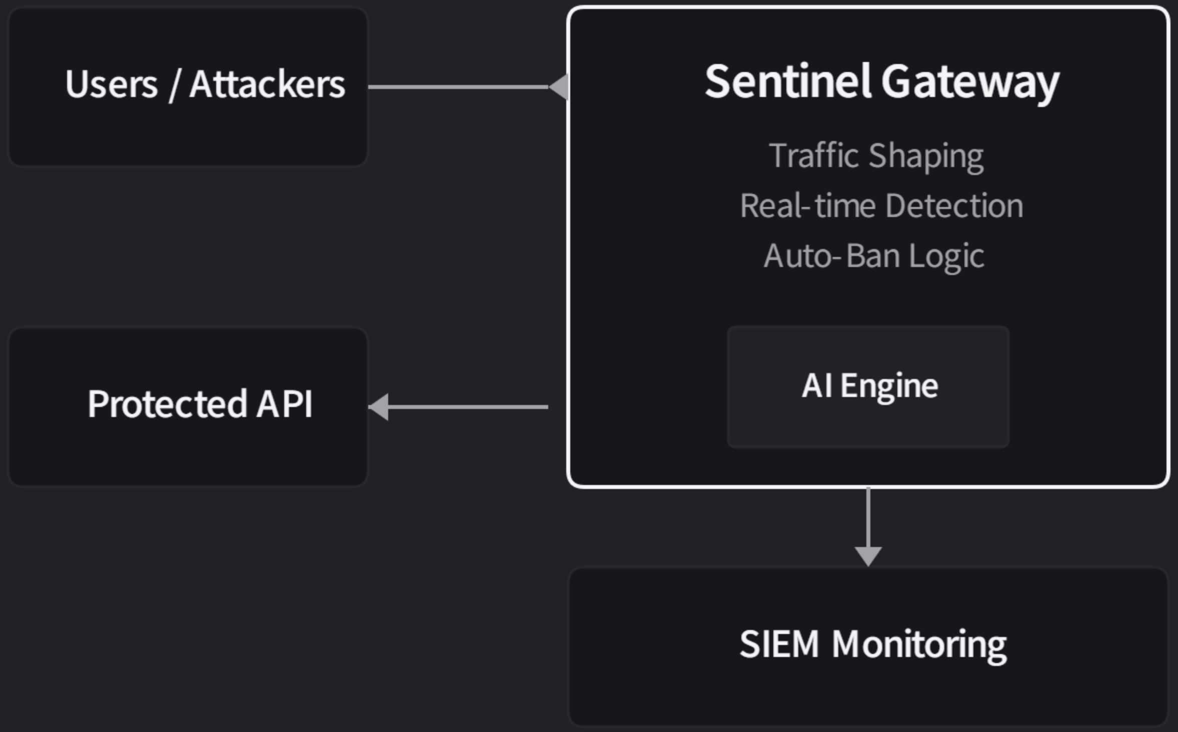
Next-Gen platform for advanced security simulations.

Sentinel API Gateway

Next-Gen Cybersecurity Learning Platform

Platform Architecture

AI-aware API Gateway Simulation



Users / Attackers

Sentinel Gateway

Traffic Shaping

Real-time Detection

Auto-Ban Logic

AI Engine

Protected API

SIEM Monitoring

Cybersecurity Learning & Practice

An interactive sandbox for red-team exercises and defensive architecture demos.

Engaging Cyberpunk UI

A modern, immersive interface that makes the complex concepts of API security engaging.

Flexible AI Integration

Run with rule-based logic or integrate a self-hosted inference engine for AI-powered detection.

Live Demo Available: **https://secure-api-gateway.vercel.app/**

Target Audience and Simulation Capabilities

Sentinel simulates professional API gateway responses to diverse traffic types.

Target Audience

- Cybersecurity Students
- Red/Blue Team Labs
- API Security Demos
- Classroom Simulations

Behavior / Traffic Type	Gateway Response	Outcome
Normal Traffic	200 OK	Request Succeeded
Rate Limit Exceeded	429 Throttled	Request Delayed
Malicious Payload	403 Blocked	Risk Score Calculated
Severe Repeated Threats	🔥 Auto-Ban	Source IP Blocked

Key Capabilities

Threat Detection and Traffic Control

Threat Detection

Identifies suspicious behavior and malicious patterns.

SQL Injection

XSS Payloads

Command Injection Patterns

Sensitive Data Leaks (PII)

Detects repeated malicious traffic signatures

Traffic Control Engine

Manages request flow and enforces security policies.

Customizable Request Rate Limits (RPM)

Distinguishes between throttled and blocked requests.

Auto-Ban Functionality

Includes cooldown timers for persistent threats.

Rule-Based Mode

AI-Assisted Mode

Developer & Attacker Simulation Features

Comprehensive testing of API gateway responses under various conditions.

Developer Simulation

Load Generator

Stress test gateway performance.

Authentication Toggle

Simulate varied access scenarios.

Attacker Simulation

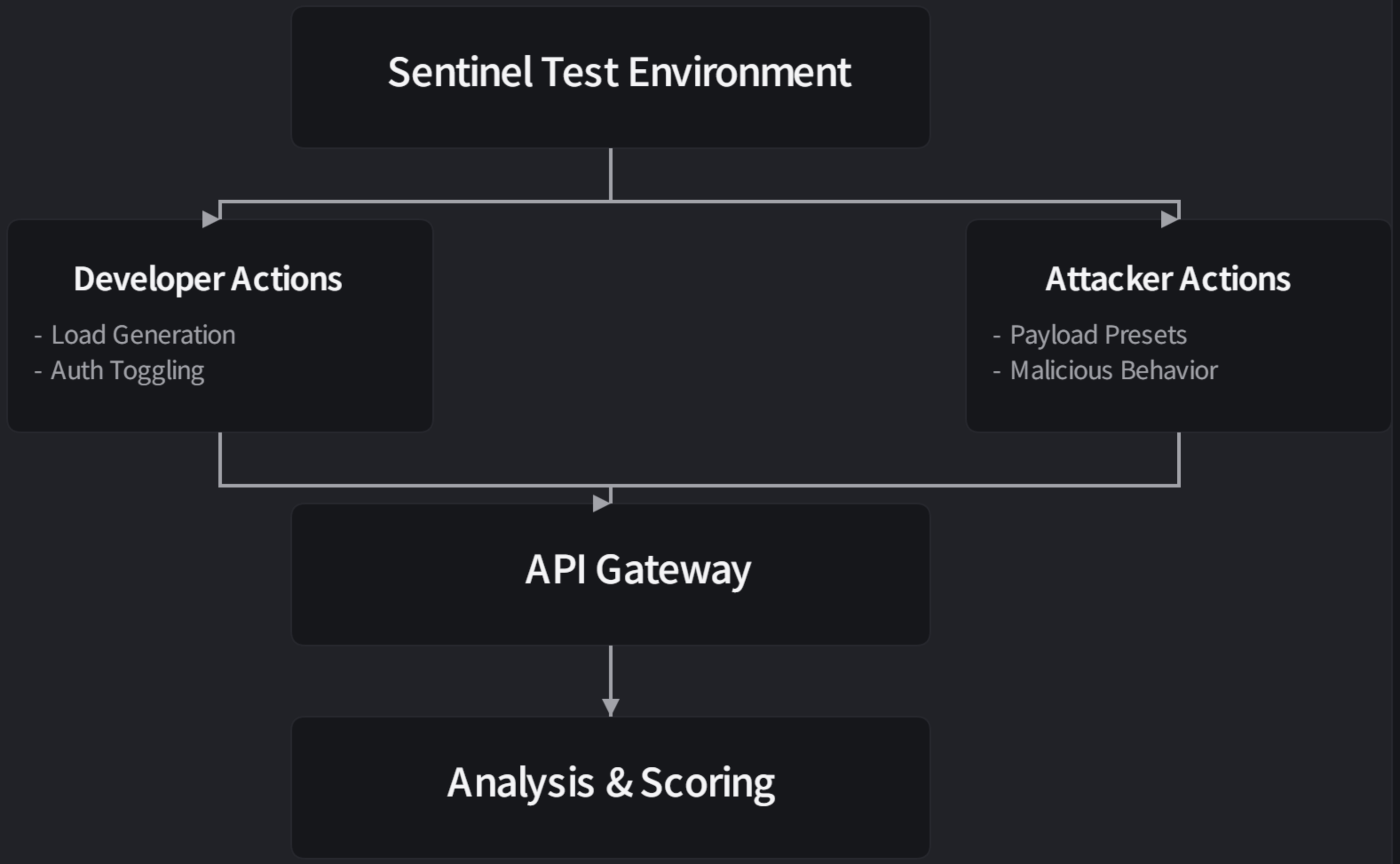
Attack Payload Presets

Simplify simulation of various attack types.

Risk Scoring per Session

Gain insights into suspicious user behavior.

Simulation Flow



Sentinel Test Environment

Developer Actions
- Load Generation
- Auth Toggling

Attacker Actions
- Payload Presets
- Malicious Behavior

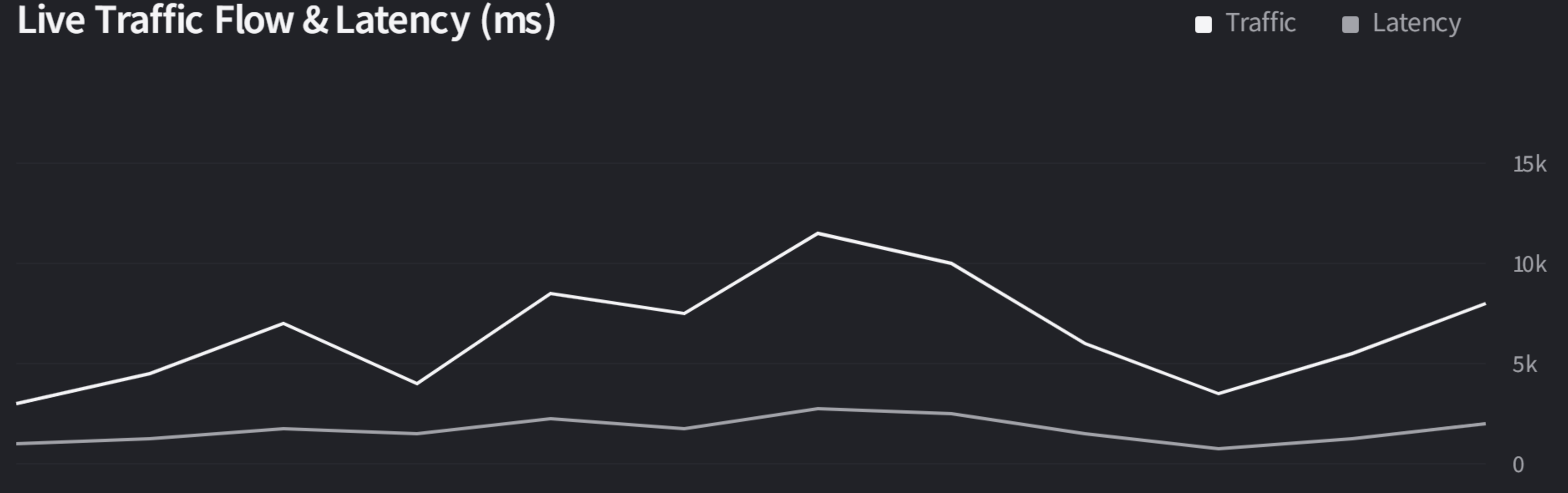
API Gateway

Analysis & Scoring

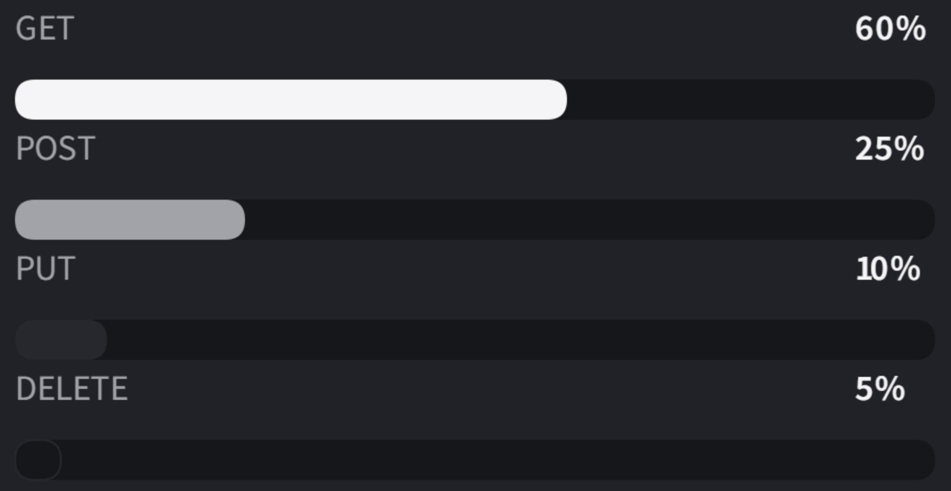
Real-Time Monitoring Dashboard

Live traffic flow, performance metrics, and client intelligence.

Live Traffic Flow & Latency (ms)



Method Distribution



Live Event Logs

```
[2024-07-28 14:30:15]GET /api/v1/users200 OK 15ms
[2024-07-28 14:30:16]POST /api/v1/data201 Created 45ms
[2024-07-28 14:30:18]GET /api/v1/status200 OK 8ms
[2024-07-28 14:30:19]GET /assets/img.png304 Not Modified 5ms
[2024-07-28 14:30:21]PUT /api/v1/users/123200 OK 32ms
[2024-07-28 14:30:22]GET /favicon.ico200 OK 2ms
[2024-07-28 14:30:25]DELETE /api/v1/data/xyz204 No Content 50ms
```

Client Intelligence

Client ID: 8A4F-C1E9-B2D3-77A1

RISK SCORE

78

HIGH

BAN STATUS

CLEAN

VIOLATIONS (24H)

12

Rate Limiting

Technological Foundation and Installation

Sentinel API Gateway Tech Stack Overview

Core Stack

Frontend

React 19, TypeScript, Vite

UI & Visuals

TailwindCSS (Cyberpunk Theme)
Lucide Icons, Recharts

State Persistence

LocalStorage, React Hooks

ML & Deployment

Optional ML Layer

Connects to any self-hosted or external inference service.

Vendor Lock-in

None. Full flexibility.

Installation Steps

1. Requirements

Node.js 18+, Optional ML backend

2. Clone Repository

Get the latest source code from the repo.

3. Install Dependencies

Run the package manager install command.

4. Configure & Run

Set up environment variables and execute.

Demo Credentials & Usage Scenarios

Practical examples for testing Sentinel's defensive capabilities

Demo User Credentials

Role	Username	Password
Admin	admin	sentinel
Standard User (Blue Team)	blue	sentinel
Red-Team Simulation	red	sentinel
Malicious Actor	hacker	sentinel
Tester	tester	sentinel

1 Simulate Attack Traffic

Log in as a standard user (e.g., 'blue') and use the 'Load Attack Payload' feature. Enable token if necessary, then click 'Send Request' to trigger a simulated attack.

Expected Outcome:
Observe 'blocked' status in the UI and review detailed log output for the event.

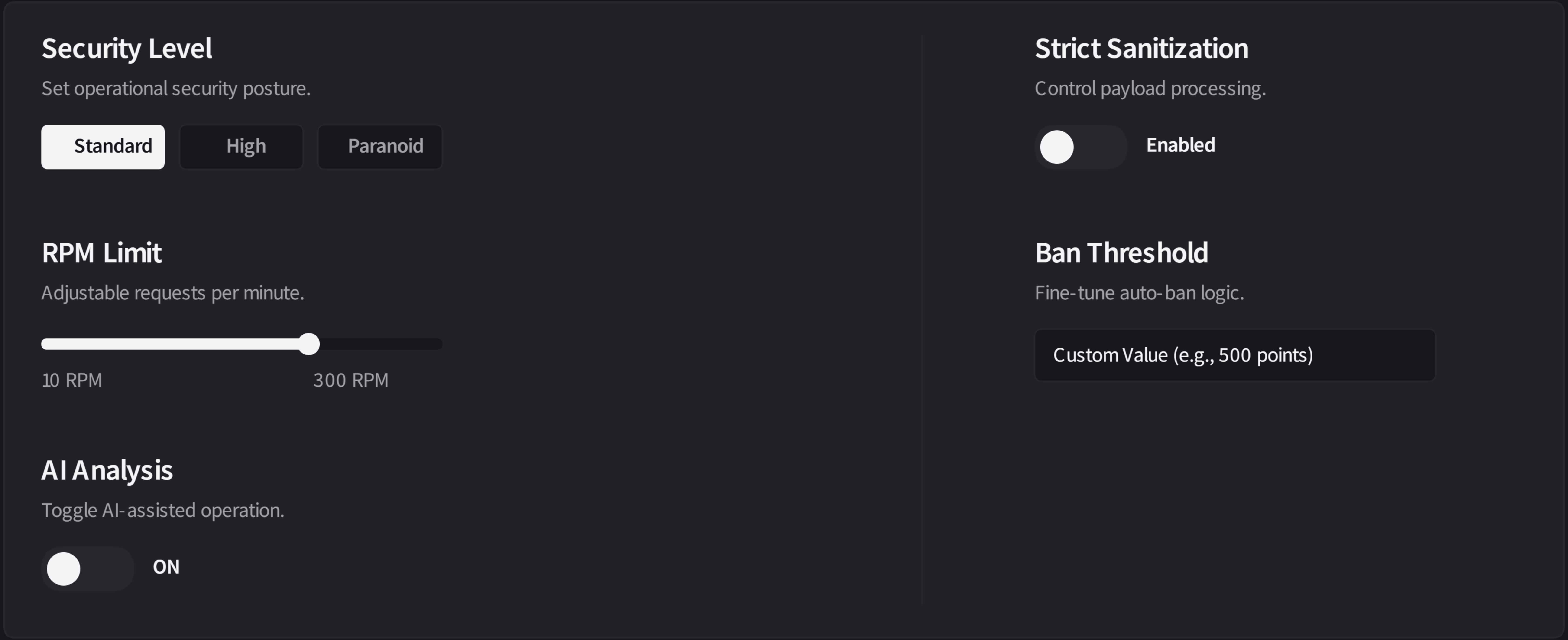
2 Stress Test Rate Limits

Open the Traffic Generator tool. Set a specific 'Requests Per Second' (RPS) value to define the load.

Expected Outcome:
Click 'Start Auto-Fire' and watch the dashboard dynamically respond to the high traffic volume, demonstrating rate limiting in action.

Dynamic System Policy Controls

Administrators can adjust critical system policies live, without requiring a restart.



Security Level

Set operational security posture.

[✓ Standard] High Paranoid

RPM Limit

Adjustable requests per minute.

10 RPM 300 RPM

AI Analysis

Toggle AI-assisted operation.

ON

Strict Sanitization

Control payload processing.

Enabled

Ban Threshold

Fine-tune auto-ban logic.

Custom Value (e.g., 500 points)

Sentinel: Next Generation

Future Roadmap & Ethical Use Guidelines

Future Roadmap

JWT Role-Based Access Simulation

Enhance authentication realism for sophisticated security testing.

Persistent Backend Logging

Implement SQLite/Postgres for comprehensive historical data analysis.

Distributed Node Simulation

Mimic complex network environments for large-scale scenario testing.

Custom Attack Builder Playground

Design and test custom attack vectors in a secure sandbox.

Ethical Use Notice

Authorized Use Only

Sentinel is designed exclusively for educational and professional development within authorized contexts. Its intended applications are strictly limited to:

- Training & Skill Development
- Academic & Corporate Research
- Controlled Security Simulations
- Ethical Penetration Testing

Strict Prohibition

Users are strictly prohibited from deploying payloads or simulated attacks outside of authorized, sandboxed environments. Unauthorized use is a violation of terms and may be unlawful.