Zero-Day Cyber Sentinel

Demonstration Pipeline

Documentation

January 20, 2026

Total Duration: ∼ 2-3 Minutes
Goal: Demonstrate the real-time nature of the pipeline and the AI analysis value.

Prerequisites

Before starting the demo, ensure a clean state:

```
# 1. Clear old data for a clean demo
rm stream.jsonl alerts.jsonl knowledge_base.jsonl 2>/dev/null

# 2. Start the system (Docker method)
docker build -t sentinel .
docker run -p 8501:8501 --env-file .env -v "${PWD}:/app" sentinel

# 3. Wait ~30 seconds for initial NIST data to populate
```

Demo Flow

Step 1: Show the Architecture (30 seconds)

Open the 3 terminals/logs running in Docker or your local environment:

1. **Stream Generator**: Fetching NIST CVE data every 5 seconds.
2. **Pathway Engine**: Processing and matching threats.
3. **Streamlit Dashboard**: Real-time visualization.

Step 2: Show the Dashboard (30 seconds)

Navigate to `http://localhost:8501`:

- Point out the **Live NIST Threat Intelligence** table (raw stream).
- Point out the **Matched Alerts** section (currently empty = system is secure).
- Show the **Threat Detection Timeline** chart.

Step 3: Inject a Custom Threat (1 minute)

This is the "magic moment":

1. Click the **"Inject Demo Threat"** button on the dashboard sidebar.

2. Watch the threat appear in the Stream table within seconds.
3. Observe the toast notification pop up.
4. Show the new **CRITICAL** alert card with Gemini's AI analysis.

Step 4: Explain the AI Analysis (30 seconds)

Zoom in on the **Gemini Insight** box:

- Show how the AI explains the threat in plain English.
- Highlight the actionable recommendation (e.g., "Update Nginx to v1.19+").

Step 5: Ask the Chatbot (Optional)

In the sidebar, ask SENTINEL:

> "What should I do about this nginx vulnerability?"

Show the AI-powered response utilizing the knowledge base.

Key Talking Points

1. **Speed**: "From NIST publication to alert in under 5 seconds."
2. **Filtering**: "Only alerts on YOUR inventory, not every CVE."
3. **AI Context**: "Gemini explains WHY it matters, not just the score."
4. **Real-Time**: "No refresh button needed - it's truly streaming."

Fallback: Manual Injection

If the dashboard button doesn't work, inject via terminal:

```
echo "CRITICAL: Zero-day exploit in production server" > manual_input.txt
```