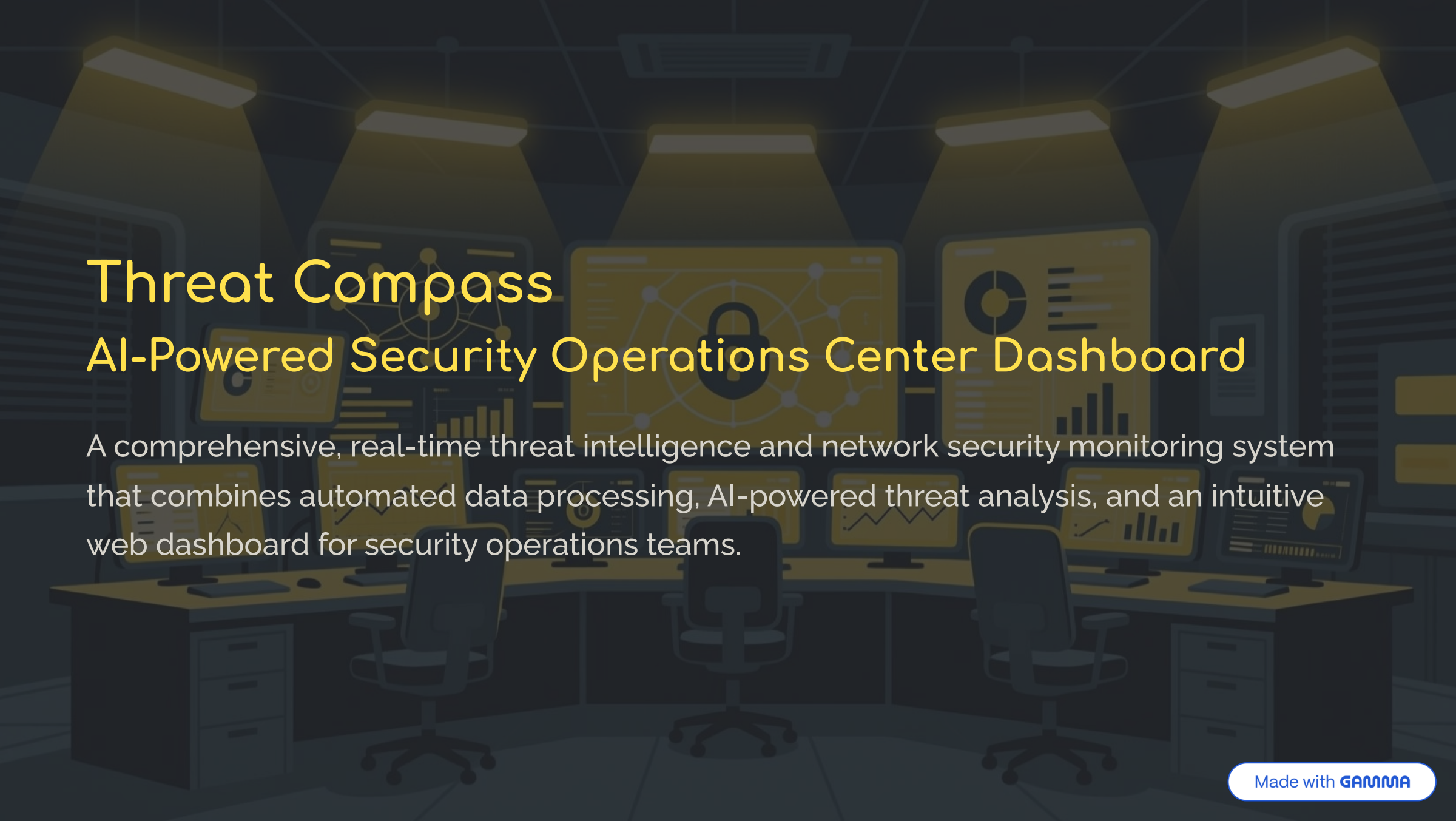

Threat Compass

AI-Powered Security Operations Center Dashboard

A comprehensive, real-time threat intelligence and network security monitoring system that combines automated data processing, AI-powered threat analysis, and an intuitive web dashboard for security operations teams.

Transforming Security Operations

The Challenge:

- Security teams are overwhelmed with massive volumes of network logs
- Manual threat analysis is time-consuming and error-prone
- API costs for threat intelligence services are prohibitively high
- Delayed threat detection leads to increased security risks

Our Solution:

Threat Compass automates the entire threat intelligence pipeline—from data ingestion to actionable insights—using intelligent caching, dual AI validation, and real-time visualization to empower security teams with instant, accurate threat assessments.

Real-Time Threat Monitoring & Analytics

🔍 Live Threat Monitoring

- Automatic data refresh every 3-10 seconds
- Lightweight metadata-based update detection
- Real-time threat intelligence metrics across all dashboards

📊 Comprehensive Analysis

- Advanced multi-criteria filtering (threat level, attack type, country, protocol, risk score)
- Detailed threat profiles with source/destination IPs, geolocation, and AI verdicts
- Search and sort capabilities for rapid threat assessment

🗺️ Geographic Visualization

- Interactive 3D globe showing threat origins worldwide
- Color-coded threat levels for instant pattern recognition
- Clickable markers with complete threat details

Dual AI Model Validation System

🤖 Advanced AI Architecture

GPT-4 Initial Assessment

- Primary threat evaluation with confidence scoring
- Detailed risk factor analysis
- Anomaly detection and pattern recognition

Google Gemini Review & Validation

- Independent secondary analysis
- Consensus detection between models
- Validation of threat level assessments

Final Decision Engine

- Actionable recommendations: BLOCK, MONITOR, or ALLOW
- Confidence-based decision making
- AI-generated reasoning for each verdict
- Manual review flagging when models disagree

Cost-Effective Threat Intelligence

1

💾 Intelligent Caching System

45% API Cost Reduction

- Smart 7-day TTL (Time-To-Live) cache
- Automatic cache hit routing
- Reduces redundant API calls for known threats

2

Smart Cache Management

- Automatic trimming to 10,000 entries for optimal performance
- Cache statistics and performance logging
- Seamless fallback to fresh API data when needed

3

Multi-Source Enrichment

- AbuseIPDB for IP reputation scoring
- VirusTotal for malware detection
- OTX (AlienVault) for threat intelligence
- Geolocation services for IP mapping

Robust, Scalable Architecture

🏗️ Technology Stack

Frontend Excellence

- React 18 + TypeScript for type-safe development
- Modern UI with shadcn-ui components and Tailwind CSS
- Recharts & Three.js for advanced data visualization
- TanStack Query for optimized data fetching

Backend & Automation

- N8N workflow automation for the complete data pipeline
- Docker containerization for easy deployment
- Node.js for automation scripts and data synchronization

Automated Data Pipeline

1. CSV security logs → N8N workflow
2. Cache check → API enrichment (if needed)
3. Dual AI analysis (GPT-4 + Gemini)
4. Automatic sync to dashboard
5. Real-time frontend updates

Empowering Security Teams

📈 Measurable Impact

- 45% reduction in threat intelligence API costs
- Real-time updates every 3 seconds for instant threat awareness
- Dual AI validation ensures high-confidence threat assessments
- 7-day intelligent caching balances cost and data freshness

🎯 User Experience

- Responsive design works on desktop, tablet, and mobile
- Dark mode support for extended monitoring sessions
- Advanced filtering and search for rapid threat investigation
- Export capabilities for reporting and compliance

🚀 Future Vision

- WebSocket integration for instant push updates
- Custom alert rules and notifications
- SIEM system integration
- Advanced ML-based threat prediction
- Historical trend analysis and custom report generation