SHOPSMART SOLUTIONS

REAL-TIME THREAT INTELLIGENCE

Team 6: Zach Green, Maisha Islam, Hallee Pham, Luis Sanchez, Morgan Sansone

University of Missouri-Kansas City

CS 361 Final Presentation

Introduction & Project Objectives

Business Context
Our client is a small online retailer of consumer electronics. Being fully digital, they're highly exposed to cyber threats like fraud, data breaches, and DDoS attacks.

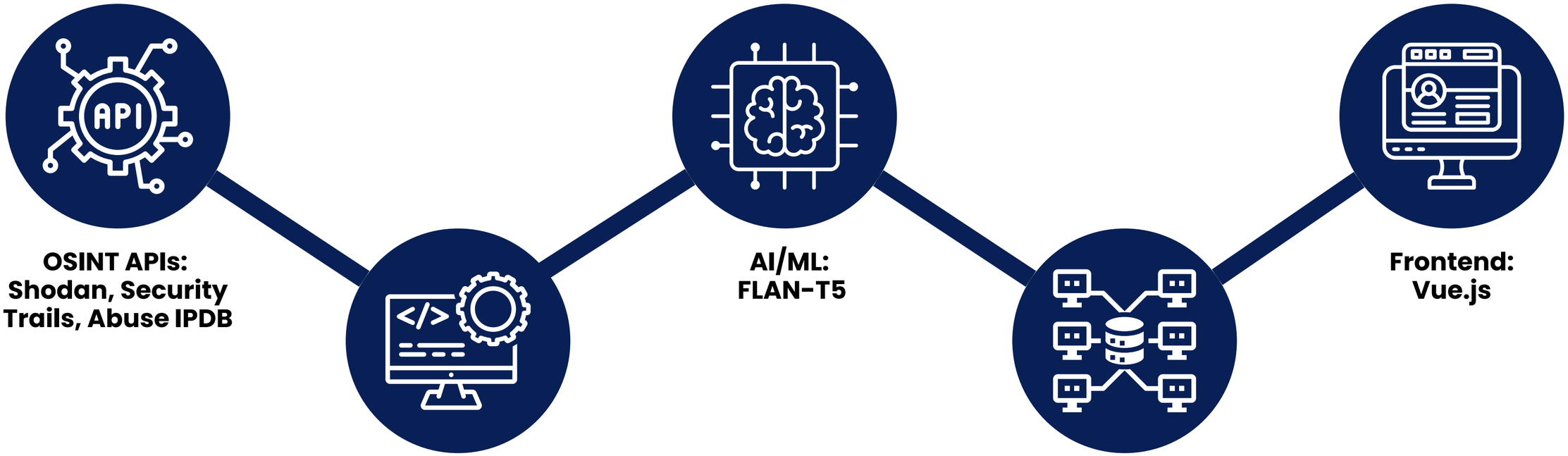
Our Role
We were hired to:

- Find system weaknesses
- Set up a threat intelligence system
- Add automated defenses without disrupting daily operations

Objectives

- Integrate OSINT APIs
- Automate risk scoring
- Enable dynamic threat response

System Architecture & Technologies



Live System Demo

Security Features & Risk Management

Security Features

- API Key Protection
  - Keys stored securely using environment variables.
- Real-Time Alerts
  - Immediate notifications for high-risk threats.
- Firewall
  - Protects against brute-force attacks and blocks unused ports.
- Event Logging
  - All threats and system actions are logged for auditing.

Risk Managment

- LLM-Based Risk Scoring
  - Automated scoring using context-aware analysis, reducing bias and improving insight.
- Risk Prioritization Model
  - Sorts risks by impact and urgency.
- Threat Mitigation Recommendations
  - AI recommends steps to respond to detected threats.
- Weekly Database Query Optimization
  - Faster risk detection through weekly SQL tuning.
- Security Validation Reports
  - Regular checks and validations included in project deliverables.

Testing & Evaluation Metrics

API UNIT TESTING

- All core backend endpoints (alerts, risk scoring, threat reports) passed with 100% success rate.
- Automated tests implemented using Jest and Postman collections.

PERFORMANCE TESTING

- Average API response time: < 500ms, even under simulated load.
- Threat detection flow benchmarked for consistency and speed.

MANUAL QA & WALKTHROUGH

- Full system tested manually across:
  - Frontend dashboard views, Real-time alert pipeline, AI threat prediction, Deployment stability
- QA checklist aligned with final system walkthrough guide.

DATABASE QUERY OPTIMIZATION

- Heavy joins (e.g., risk scores + threat logs) optimized using:
  - Indexes on critical columns
  - Batched queries and views
- Improved query execution time by over 40% during Week 9 testing.

Challenges

Throughout development, we encountered a number of real-world issues related to scalability, data reliability, deployment security, and explainability. Addressing these issues was critical to ensuring that our system remained strong, secure, and accurate in a high-risk cybersecurity environment.

- **API Integration Without API Keys**
  - **Challenge**: Wanted to use AI for threat analysis but didn't want to pay for commercial API keys.
  - **Solution**: Created a local AI service using Hugging Face models (ai_threat_service.py) that runs locally and provides threat predictions without external API costs.

- **Real-time Data Processing**
  - **Challenge**: Processing threat data in real-time while maintaining system performance.
  - **Solution**: Created an efficient polling mechanism and implemented database optimizations (shown in query_optimizations.sql) to handle large volumes of threat data.

- **Database Performance**
  - **Challenge:** As the threat database grew, query performance degraded.
  - **Solution**: Implemented materialized views and optimized queries in query_optimizations.sql that significantly improved dashboard responsiveness.

- **Risk Scoring Complexity**
  - **Challenge**: Developing an accurate time-weighted risk scoring algorithm that accounts for threat decay over time.
  - **Solution**: Implemented a sophisticated algorithm in risk_scoring.js that factors in likelihood, impact, and time since last detection to provide dynamic risk assessments.

Future Improvements

As we move forward, we will prioritize automation, expanding intelligence sources, and improving usability. These enhancements will make the system faster, smarter, and more adaptable to changing threats. By incorporating anomaly detection, streamlining workflows, and broadening data coverage, we hope to provide a more robust and scalable threat intelligence solution that supports real-time decision-making and long-term security growth.

Add email/SMS alerts for critical threats

Expand threat source integrations

Enable compliance reporting

Automate triage & threat tagging

Reduce API calls & manual effort

Add anomaly detection (ML)

SHOPSMART SOLUTIONS

THANK YOU

Questions?