SMB Security Platform

Slide 1: Project Overview

AI-Augmented Cyber Risk & Threat Intelligence for SMBs

- **Problem:** SMBs face enterprise-level threats without enterprise resources.
- **Solution:** An AI-augmented security platform that implements the NIST Cybersecurity Framework (CSF) 2.0.
- **Scope:** The platform covers all 6 core functions of the NIST CSF: Identify, Protect, Detect, Respond, Recover, and Govern.

Slide 2: Platform Architecture

- **Technology Stack:** A full-stack TypeScript application.
- **AI Capabilities:** Powered by 6 specialized AI agents using GPT-5.
- **Intelligence Feeds:** Real-time integration with over 7 Open-Source Intelligence (OSINT) feeds.
- **Deployment:** Production-ready with comprehensive security hardening.
- **Demo:** https://youtu.be/notH5ACUzBI

Slide 3: Open Source Intelligence Integration

- **Unified Adapters:** Integrates 7 OSINT sources (Shodan, AbuseIPDB, VirusTotal, etc.) through a unified adapter pattern.
- **Resilience:** Features automatic rate limiting and retry with exponential backoff to handle API quotas and transient failures.
- **Data Normalization:** All incoming data is normalized to a consistent internal schema for unified processing.
- **Ingestion Modes:** Supports both real-time and scheduled data ingestion.

Slide 4: Threat Detection & Correlation

- **Automated Matching:** Automatically matches threat indicators (IPs, domains, hostnames) to assets in the inventory.
- **AI-Powered Analysis:** Uses AI for contextual severity analysis and scoring.
- **Deduplication:** Prevents alert fatigue by deduplicating similar threat events within configurable time windows.
- **Risk Persistence:** Automatically updates and persists risk scores to asset records.

Slide 5: Six Specialized AI Agents

- **Function-Mapped:** One agent is dedicated to each NIST CSF function: Identify, Protect, Detect, Respond, Recover, and Govern.
- **Shared Framework:** Agents share a common prompting framework but have function-specific expertise and schemas.
- **Asynchronous Execution:** Agents run asynchronously with background scheduling for long-running tasks.
- **Structured Output:** Agent responses are parsed into structured data for seamless database integration.

Slide 6: Express.js Backend Architecture

- **RESTful API:** A clean, resource-based RESTful API with Zod for input validation.
- **Type-Safe Database:** Uses Drizzle ORM for type-safe, compile-time checked database queries.
- **Testable Storage Layer:** A storage abstraction layer allows for easy testing and swapping of database backends.
- **Security Hardening:** A robust security middleware stack including Helmet, rate limiting, and secure session management.

Slide 7: Security Controls & SOP Generation

- **Full NIST 800-53 Catalog:** Implements the complete NIST 800-53 revision 5 control catalog.
- **Implementation Workflow:** Controls follow a clear status workflow: `Proposed` → `In-Progress` → `Implemented`.
- **AI-Generated SOPs:** The "Protect Agent" generates actionable, step-by-step Standard Operating Procedures for each control.
- **CSF Mapping:** All controls are automatically mapped to NIST CSF categories and subcategories for high-level reporting.

Slide 8: Risk Management & Gap Analysis

- **Formal Risk Register:** A centralized risk register to formally document, score, and track security risks.
- **Automated Risk Creation:** High-severity detections can automatically generate new items in the risk register.
- **POA&M Tracking:** A Plan of Action & Milestones (POA&M) module to track and manage the remediation of identified gaps.
- **Evidence Freshness:** Tracks compliance assertion evidence and flags stale attestations to ensure continuous compliance.

Slide 9: Infrastructure Architecture

- **Serverless PostgreSQL:** Runs on Neon PostgreSQL, which provides serverless WebSocket connections suitable for serverless environments.
- **ORM and Migrations:** Uses Drizzle ORM with automated migration management based on schema changes.
- **Background Scheduler:** A robust scheduler for automated tasks like OSINT ingestion, SLA monitoring, and RPO/RTO checks.
- **Multi-Channel Alerting:** Supports alerting via both email and webhooks for critical events.

Slide 10: Production Security & Deployment

- **Secure Headers:** Uses Helmet.js to set crucial security headers like CSP, HSTS, and X-Frame-Options.
- **Rate Limiting:** Implements configurable rate limiting on API endpoints to prevent abuse and brute-force attacks.
- **Secure Sessions:** Manages sessions with secure, HTTP-only cookies and server-side invalidation.
- **Environment-Based Configuration:** All sensitive values (API keys, secrets) are managed via environment variables, not hardcoded.

Slide 11: Material Design Implementation

- **Component-Based:** Built with Material Design principles using shadcn/ui and Radix UI primitives for accessibility.
- **Consistent Typography:** Uses the Roboto font family with a consistent, hierarchical typography scale.
- **Semantic Colors:** A semantic color system provides instant meaning for severity badges and status indicators.
- **Light & Dark Mode:** Full support for both light and dark modes, with all components adapting to the selected theme.

Slide 12: React Application Architecture

- **Modern Stack:** Built with React, TypeScript, and Vite for a fast and modern development experience.
- **Server State Management:** Uses TanStack Query (React Query) for efficient caching, background refetching, and optimistic updates.
- **Lightweight Routing:** Employs Wouter for simple and lightweight client-side routing.
- **Data Visualization:** Uses Recharts to create interactive charts and graphs for dashboards and trends.