TrustBridge Security Monitoring & Logging – MVP Implementation

Role: Cybersecurity Team
Project: TrustBridge MVP

1. Objective

This document defines the currently implemented security monitoring and logging mechanisms within the TrustBridge MVP.
The goal is to ensure that critical operations, authentication events, transaction confirmations, and file uploads are validated, controlled, and traceable where possible.

2. Security Logging Overview

- Logging occurs primarily at the **Backend API layer**.
- Backend enforces security controls and validates all sensitive operations.
- Critical events are handled through **JWT validation, ownership checks, and Supabase session verification**.

Currently monitored events include:

- Login attempts via Supabase Auth
- JWT token validation for transaction confirmation
- Ownership checks on transactions
- File upload validation (size and MIME type)

Note: Full centralized audit logging with severity categorization is not implemented in this MVP.

3. Authentication Event Monitoring

- Supabase Auth manages authentication sessions.
- JWT session tokens and expiration checks are enforced.
- Failed login attempts are handled by Supabase and prevent access.
- The system ensures **only authenticated users** can access protected endpoints.

What is enforced:

- Login required for all sensitive operations
- Expired or invalid JWT tokens are rejected

- Ownership validation ensures users cannot act on other users' transactions

4. Transaction Confirmation Security

- Confirmation links are JWT-based with a 72-hour expiration.
- Each transaction confirmation requires:
    - Valid JWT token
    - Ownership verification (`transaction.sme_id === req.user.id`)
    - One-time token usage (token invalidated after confirmation)
- Invalid or expired tokens are rejected immediately.

5. File Upload Security

- File uploads are handled via Multer middleware with:
    - **Maximum file size limit** (5MB)
    - **Allowed MIME types**: PDF, JPEG, PNG
    - **Authenticated upload only** (user must be logged in)
- Rejected uploads are prevented but not yet logged to a centralized audit trail.

6. Database & Backend Security Controls

- **Row-Level Security (RLS)** ensures users can only access their own data.
- Sensitive queries are filtered by the authenticated user ID.
- Supabase service role keys are **never exposed to the frontend**.
- HTTPS is enforced for all client-server communication.
- Parameterized queries prevent SQL injection.

7. Security Enforcement Summary

The TrustBridge MVP currently implements:

- Authentication enforcement via Supabase Auth
- JWT-based transaction confirmation with expiration and one-time use
- Ownership validation for all transaction-sensitive actions
- File upload validation (size and MIME type)
- Encrypted communications and database protection via RLS

Limitations:

- No full centralized audit log or severity-based event monitoring
- Suspicious activity detection (e.g., repeated failed attempts over time) is not yet implemented

8. Conclusion

The implemented security controls in TrustBridge MVP provide strong **preventive protection** for authentication, transaction confirmation, and file uploads.
While full audit logging and real-time anomaly detection are planned for future versions, the current implementation ensures **integrity, access control, and transactional security** consistent with MVP-level fintech deployment.