AI-Augmented Threat Detection Architecture for Financial Institutions

Author: Bilge Kayal■
Date: October 2025
Affiliation: Q Investment Bank (Conceptual Architecture – Not Based on Real Systems)

Abstract: This whitepaper presents a conceptual AI-augmented cybersecurity architecture for financial institutions, inspired by ISO 27001, NIST CSF, and MITRE ATT&CK; frameworks. The framework demonstrates how AI-driven behavioral analytics, combined with XDR telemetry and rule-based detection, can enhance early-stage anomaly identification while maintaining compliance and explainability.

1. Introduction

Financial institutions face evolving cyber threats that challenge traditional Security Information and Event Management (SIEM) systems. This conceptual model explores an AI-augmented detection layer that operates above conventional XDR systems to identify emerging attack vectors, using synthetic behavioral data and risk scoring models.

2. Conceptual Architecture

The architecture comprises five modular layers: (1) Telemetry Collection, (2) Data Lake & ETL, (3) AI Risk Scoring Engine, (4) Security Orchestration & Response, and (5) Compliance Audit Layer. AI models analyze synthetic event data (e.g., login anomalies, process behavior deviations) to dynamically assign risk scores, triggering pre-defined response playbooks when thresholds are exceeded.

3. Synthetic Dataset and AI Logic

A synthetic dataset simulates security alerts generated by an XDR platform. Each record includes timestamp, user ID, asset ID, event type, and anomaly score. A simple AI classifier (e.g., gradient boosting or LSTM) predicts whether an event indicates potential insider threats or lateral movement attempts. No real organizational data is used in this model.

4. Risk Scoring Model (Example Pseudocode)

if anomaly_score > 0.8 and user_activity_context == 'off_hours': risk_level = 'High' elif anomaly_score > 0.5: risk_level = 'Medium' else: risk_level = 'Low' trigger_response(risk_level)

5. Compliance and Explainability

All AI decisions are logged with SHAP value explanations to ensure transparency for audit teams. This design aligns with ISO 27001 Annex A controls and NIST CSF 'Detect' and 'Respond' functions, providing traceability and accountability in automated decision-making.

6. Future Development

Future iterations may incorporate federated learning models to enable multi-bank threat intelligence sharing without direct data exchange, improving both privacy and predictive capability across the financial sector.

Disclaimer:

This whitepaper is entirely conceptual and based on public cybersecurity frameworks. It does not reference, disclose, or represent any real systems or data belonging to any financial institution.