Hyperflex

Enterprise Financial Services Platform

From Slow Log Analysis to Real-Time Fraud Detection

Challenge

The organization struggled with **delayed threat detection** and **fragmented security visibility** across multiple systems. Manual investigations **slowed response times** and increased risk of undetected fraud.

Objective

- Detect suspicious activity in real time
- Unify security logs across distributed systems
- Process 1.5TB+ security events daily
- Improve incident response time for fraud
- investigations

Solution

Hyperflex implemented an **Elastic Security architecture** using Elasticsearch, Logstash, and Kibana. We centralized security logs, optimized ingestion pipelines, and deployed real-time threat detection with automated alerting.

Results

Real-time threat detection	120+ systems monitored continuously	<3 min incident response time	1.5 tb+ of security logs processed daily

Strategic Impact

- Unified security monitoring into a **single Elastic platform**
- Enabled **proactive fraud detection** and investigation
- **Improved visibility** across distributed financial systems
- **Strengthened security posture** for critical operations