Figure 1: Predictive Quantum Threat Detection System Architecture

Figure 1: Predictive Quantum Threat Detec
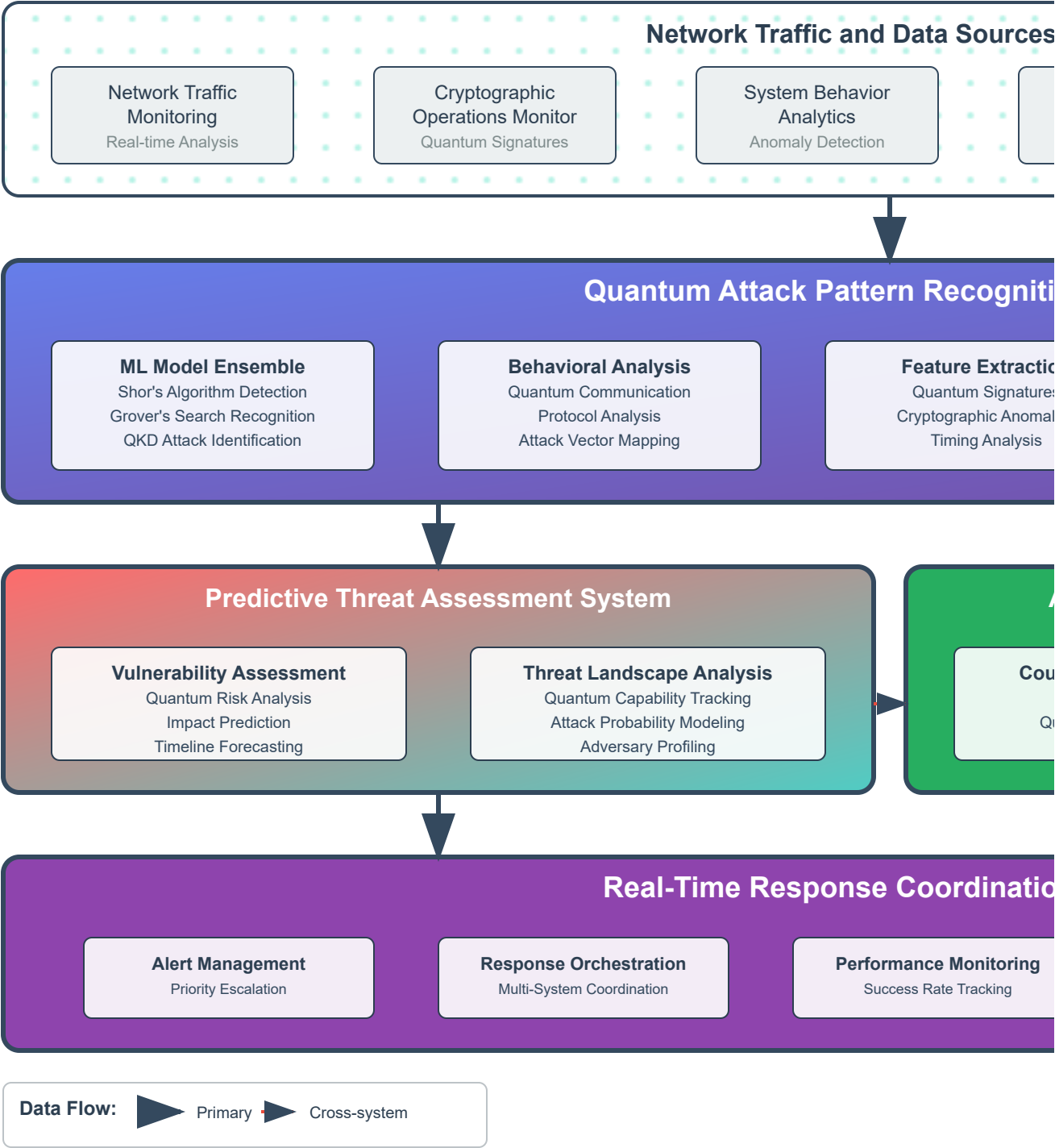

Network Traffic and Data Sources

| Network Traffic Monitoring | Cryptographic Operations Monitor | System Behavior Analytics |
| Real-time Analysis | Quantum Signatures | Anomaly Detection |

Quantum Attack Pattern Recogniti

ML Model Ensemble
Shor's Algorithm Detection
Grover's Search Recognition
QKD Attack Identification

Behavioral Analysis
Quantum Communication
Protocol Analysis
Attack Vector Mapping

Feature Extractio
Quantum Signatures
Cryptographic Anomal
Timing Analysis

Predictive Threat Assessment System

Vulnerability Assessment
Quantum Risk Analysis
Impact Prediction
Timeline Forecasting

Threat Landscape Analysis
Quantum Capability Tracking
Attack Probability Modeling
Adversary Profiling

Cou
Q

Real-Time Response Coordinatio

Alert Management
Priority Escalation

Response Orchestration
Multi-System Coordination

Performance Monitoring
Success Rate Tracking

Data Flow: ▶ Primary ▶ Cross-system

Figure 2: Machine Learning-Based Quantum Attack Detection Engine

Figure 2: Machine Learning-Based Quantum

Multi-Modal Input Data Sourc

Network	Crypto	System	Timing	Prot
Traffic	Operations	Behavior	Analysis	Anom
Packet Analysis	Key Exchange	CPU/Memory	Side-Channel	QKD A

Quantum Feature Extraction and Preproc

Shor's Algorithm	Grover's Search	Quantum Fourier	Variation
Pattern Extraction	Signature Detection	Transform Analysis	Algorithm Dete

Machine Learning Model Ensemble for Quan

Deep Neural Network
Convolutional Layers

Transformer Model
Attention Mechanism
Sequence Analysis

Attention Weights

Random Forest
Ensemble Learning
Decision Trees

Ensemble Voting and Confidence Weig

Weighted Voting Algorithm	Confidence Calibration	Threat Clas
Model Performance History	Uncertainty Quantification	Multi-class

Quantum Threat Detection Out

HIGH THREAT	MEDIUM THREAT	LOW THREAT	SHOR'S DETE

Performance Metrics:
- Sub-millisecond detection time
- 99.7% accuracy on quantum attacks

Model Training:
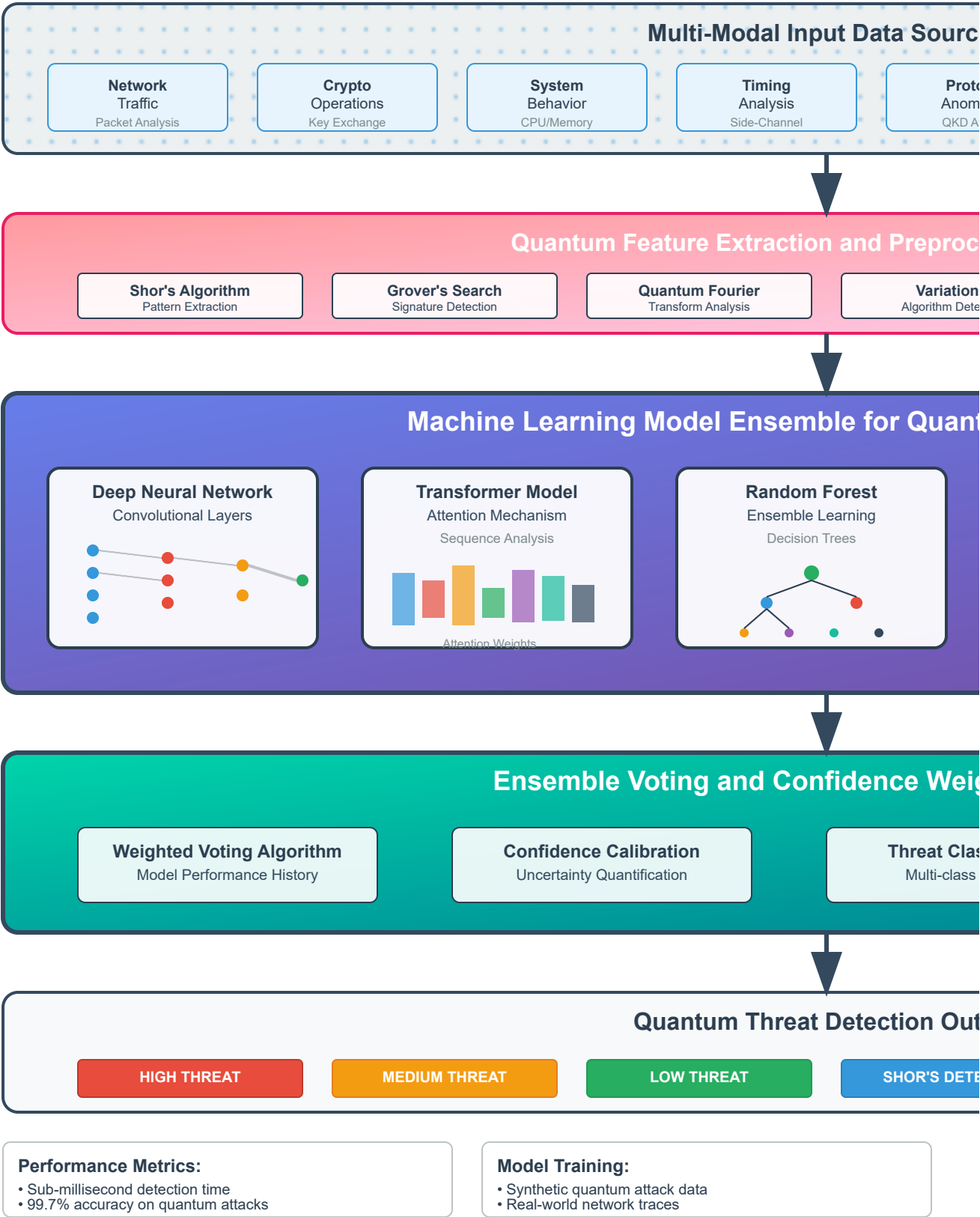- Synthetic quantum attack data
- Real-world network traces

Figure 3: Automated Quantum Countermeasure Deployment System

Figure 3: Automated Quantum Countermea

⚠ **QUANTUM THREAT DETECTED - AUTOMATED R**

Threat Type: Shor's Algorithm | Confidence: 97.3% | ETA: 2.1 s

Emergency Response Decision Engine (Su

Threat Severity Analysis
CRITICAL - Immediate Response

Asset Priority Mapping
High-Value Crypto Assets

Response Strategy Selection
Emergency Protocol Alpha

Parallel Countermeasure Deployment (E

Post-Quantum Crypto Deployment Track
- CRYSTALS-Kyber | CRYSTALS-Dilithium
- SPHINCS+ | Key Migration

Network Security Isolation Track
- Traffic Filtering | Quantum VPN
- Port Blocking | Honeypot Deploy

System Harden Protection Tra
- Access Control | Privile
- Log Enhancement | Back

Real-Time Deployment Monitoring

Track 1: DEPLOYING
Post-Quantum Crypto
Progress: 73% (1.2s elapsed)
ETA: 0.4s remaining

Track 2: ACTIVE
Network Isolation
Progress: 95% (0.8s elapsed)
🔒 Quantum channels secured

Track 3: COMPLETE
System Hardening
Progress: 100% (0.6s elapsed
✓ All systems protected

Deployment Validation and Continuous F

Crypto Validation
Key Exchange Tests

Network Tests
Connection Integrity

System Health
Performance Impact

Threat Sta
Attack Mitiga

Emergency Response Timeline:
T+0.0s: Threat Detected → T+0.1s: Decision → T+0.2s: Deployment → T+1.8s: Protection Active