Table of Contents

# 1 Nextrade Securities Exchange - Infrastructure Architecture

## 1.1 Executive Summary

Led design, implementation, and operation of **South Korea’s first new securities exchange in 20+ years**. Built zero-trust security architecture achieving:

* **Security**: 0 breaches (19 months), 0 FSC audit findings (3 consecutive)
* **Availability**: 99.98% platform uptime (target 99.95%)
* **Compliance**: ISMS-P 90%, ISO 27001 85%, FSC 100%
* **Efficiency**: $188K annual savings, 461 hours/year automated

**Duration**: 2024.03 ~ Present (19 months) **Phases**: Construction (11 months) → Operations (8 months) **Scale**: 300+ endpoints, 150+ servers, 80+ network devices, 10TB+/day

## 1.2 System Architecture

### 1.2.1 Infrastructure Topology

Internet → DDoS Scrubbing (20Gbps) → Edge Firewall (Fortigate 600F HA)  
 ├─ DMZ Zone (Web/API Gateway)  
 ├─ Internal Zone (App/Database)  
 ├─ Trading Zone (Air-Gap, Matching Engine)  
 └─ Management Zone (SIEM/Monitoring)

### 1.2.2 Network Segmentation

**Physical Separation**: 1. **Trading Network** (Air-Gap): Matching engine, order router - biometric access 2. **Office Network**: NAC-controlled, DLP-monitored, proxy-based internet 3. **Management Network**: Jump server only, PAM enforced, session recording

**Logical Segmentation**: - DMZ: 172.16.10.0/24 (External services) - Application: 10.0.20.0/24 (Business logic) - Database: 10.0.30.0/24 (Data persistence) - Management: 10.0.99.0/24 (Admin tools) - Trading Core: 10.100.30.0/24 (Air-gapped)

## 1.3 Security Solutions (15 Products)

### 1.3.1 Perimeter Security

* **DDoS Protection**: 20Gbps scrubbing, 47 attacks mitigated (2025), 0 downtime
* **NGFW**: Fortigate 600F HA (10Gbps FW, 3Gbps IPS), 150B+ sessions/month, 50K+ threats blocked
* **IPS**: 10K+ signatures, 2,300 SQL injections blocked, 3 zero-days detected
* **WAF**: OWASP Top 10 protection, 15K+ attacks blocked, <0.1% false positives

### 1.3.2 VPN & Remote Access

* **SSL VPN**: 500 concurrent users, MFA mandatory, 150-200 daily active users
* **IPsec VPN**: 5 site-to-site tunnels, AES-256-GCM, 99.95% availability

### 1.3.3 Endpoint Security (300+ Endpoints)

* **EPP/EDR**: CrowdStrike + Symantec, 180+ malware blocked, 5 threats contained (<10min)
* **NAC**: Genian 802.1X, 350+ devices, 15-20/month quarantined, 2hr avg remediation
* **DLP**: Symantec, 3,200+ incidents analyzed, 120 true positives, 0 confirmed breaches

**EPP/DLP Optimization Achievement**: - Problem: Concurrent scans caused 60% CPU usage - Solution: Priority tuning + exclusions + scheduling + kernel patch - Result: **30% improvement** (60% → 42%), 90% complaint reduction

### 1.3.4 Access Control

* **PAM**: CyberArk, 150+ servers, 1,200+ sessions/month, 15 dangerous commands blocked
* **Database Security**: Imperva, 50+ databases, 500M+ queries analyzed, 80+ blocked actions

### 1.3.5 Advanced Threat Detection

* **APT Protection**: FireEye + WildFire, 150K+ files analyzed, 2 APT campaigns identified
* **SIEM**: Splunk, 10GB/day ingestion, 80+ log sources, 120+ correlation rules

## 1.4 Automation & DevSecOps

### 1.4.1 Firewall Policy Automation

**Framework**: Python + FortiManager API + Git versioning

**Results**: - Deployment time: **8h → 4h** (50% reduction) - Error rate: **5% → 0%** (100% accuracy) - Policies deployed: 500+ (100% automated) - ROI: 200+ hours/year saved

### 1.4.2 NAC Exception Automation

**Framework**: Ansible + ServiceNow integration

**Results**: - Processing time: **30min → 3min** (90% reduction) - Error rate: **3% → 0%** - Approval compliance: 100%

### 1.4.3 SOAR Playbooks

**Automated responses**: - Malware detected → Isolate + Kill process + Block IOCs + Create ticket - Brute force → Block IP + Force password reset + Enable MFA - DLP violation → Block action + Notify manager + Preserve evidence

## 1.5 Compliance & Regulatory

### 1.5.1 FSC (Financial Services Commission)

**Pre-License Audit (2024.12)**: **Zero findings** → License approved **Quarterly Audits (2025)**: **Zero findings** (2 consecutive)

**Key Requirements**: - Network isolation (5-layer physical separation) - Access control (PAM + session recording) - Data protection (AES-256 encryption + DR) - Incident response (NIST SP 800-61 framework) - Vulnerability management (Critical 7d, High 14d SLA)

### 1.5.2 ISMS-P & ISO 27001

* **ISMS-P**: 90% compliant (104 controls, certification pending 2025 Q4)
* **ISO 27001**: 85% compliant (gap analysis complete, certification target 2026 Q2)

### 1.5.3 Automated Compliance

* Daily evidence collection (firewall changes, PAM sessions, SIEM alerts, vuln scans)
* Continuous monitoring (policy drift detection, access reviews, config scanning)
* Immutable storage (audit trails preserved for 7 years)

## 1.6 Operational Metrics

### 1.6.1 SOC Performance (24/7/365)

**Event Processing**:

15M raw events/month → 6K correlated alerts → 200 triaged → 150 investigated → 5 confirmed threats

**SLA Compliance (2025)**: | Priority | Detection | Response | Compliance | |———-|———–|———-|————| | P0 (Critical) | <1 min | <30 min | 100% (2/2) | | P1 (High) | <5 min | <2 hours | 95% (38/40) | | P2 (Medium) | <15 min | <1 day | 92% (110/120) |

**False Positive Rate**: - Initial (2024 Q1): 60% (120/200 alerts) - Current (2025 Q4): 33% (100/300 alerts) - **Improvement**: 45% reduction through ML tuning

### 1.6.2 Vulnerability Management

**Remediation SLA**: | Severity | SLA | 2025 Compliance | Avg Time | |———-|—–|—————–|———-| | Critical | 7 days | 100% (23/23) | 4.2 days | | High | 14 days | 98% (153/156) | 9.1 days | | Medium | 30 days | 95% (378/398) | 18.5 days |

**Statistics (2025 YTD)**: - Total discovered: 847 - Total remediated: 797 (94%) - Accepted risks: 12 (documented) - Overdue: 0

### 1.6.3 System Availability

| Service | Target | 2025 Actual | Downtime Used |
| --- | --- | --- | --- |
| Trading Platform | 99.95% | **99.98%** | 1.0h / 4.4h allowed |
| Website/Portal | 99.9% | 99.94% | 3.2h / 8.8h allowed |
| Security Services | 99.9% | 99.95% | 2.5h / 8.8h allowed |

**Mean Time Metrics**: - **MTTD**: 3.2 minutes (improved from 5 min) - **MTTR**: 27 minutes (improved from 45 min) - **MTBF**: 720 hours (30 days)

## 1.7 Cost Optimization

### 1.7.1 TCO Analysis

**Year 1 Investment**: $1.85M (Hardware $800K + Software $400K + Personnel $600K) **Industry Benchmark**: $2.3M **Savings**: **$450K** (20% below benchmark)

### 1.7.2 Annual Savings (2025)

| Source | Hours/Value |
| --- | --- |
| Firewall automation | 200 hours |
| NAC automation | 90 hours |
| Vuln reporting | 87.5 hours |
| Compliance automation | 84 hours |
| **Total labor reduction** | **461.5 hours = $46K** |
| MTTR improvement | $60K |
| False positive reduction | $32K |
| Incident cost reduction | $50K |
| **Total annual savings** | **$188K** |

### 1.7.3 Cost Avoidance

* Data breaches prevented: 0 (industry avg: 1-2/year, $500K+ each)
* Ransomware prevented: 0 ($500K avg per incident)
* Regulatory fines: $0
* **Estimated avoidance**: $600K-$1.5M/year

**ROI**: 43%-91% in Year 1, Payback: 13-28 months

## 1.8 Security Incident Response

### 1.8.1 IR Framework (NIST SP 800-61 Rev 2)

**Severity Classification**: - **P0 (Critical)**: Business-critical compromise, active breach, trading down → <15min response - **P1 (High)**: Non-critical compromise, confirmed malware → <30min response - **P2 (Medium)**: Single endpoint compromise, suspected access → <2hr response - **P3 (Low)**: Policy violation, false positive investigation → <4hr response

### 1.8.2 IR Team & Escalation

Security Analyst (L1) → Security Lead (L2) → CISO (L3) → CTO → CEO (Critical Only)

**Core Team (24/7 on-call)**: - Incident Commander: Security Lead - Technical Lead: Senior Security Engineer - Communication Lead: Compliance Manager

### 1.8.3 Key Playbooks

#### 1.8.3.1 1. Malware/Ransomware

**Containment** (<5min): NAC quarantine + Firewall block + Disable account + EDR contain **Analysis** (<30min): Memory dump + Disk snapshot + Malware sandbox + Threat intel **Eradication** (<2hr): EDR remediation + Patch vulnerability + Block IOCs network-wide **Recovery** (<4hr): Restore from backup or re-image + Re-enable access

#### 1.8.3.2 2. Data Breach

**Containment** (<10min): Block exfiltration path + Disable account + Isolate system **Assessment** (<30min): Identify data accessed + Exfiltration channels + Impact scope **Evidence** (<1hr): Preserve logs (immutable) + Memory/disk forensics + Chain of custody **Notification**: FSC report if >1000 records or >100 PII (within 72 hours)

#### 1.8.3.3 3. DDoS Attack

**Mitigation** (<5min): Activate scrubbing + Rate limiting + GeoIP blocking **Analysis** (<15min): Identify attack type + Attack sources **Blocking** (<30min): Block top 100 IPs + Block attack patterns + Update WAF rules **Recovery**: Monitor normalization + Gradual unblocking + Performance verification

#### 1.8.3.4 4. Insider Threat

**Monitoring** (<1hr): Enable session recording + Keystroke logging + Screen capture (covert) **Evidence** (<4hr): Historical activity + Data exfiltration indicators + Privileged access audit **Response**: Coordinated account disable + Credential revocation + Device wipe (requires HR+Legal)

### 1.8.4 Communication Templates

**P0 Critical Notification**: - Incident summary + Business impact + Current status + Actions taken + Response team + Next update

**FSC Regulatory Report**: - Incident summary + Affected systems + Impact assessment + Root cause + Response actions + Customer notification + Preventive measures

## 1.9 Lessons Learned

### 1.9.1 What Worked Well

✅ **Automation-first**: 30% construction time on automation → 10x ROI in operations ✅ **Vendor diversity**: CrowdStrike outage → Symantec fallback saved operations ✅ **Aggressive tuning**: 2-month tuning period → 45% false positive reduction ✅ **Comprehensive documentation**: Runbooks → 40% MTTR reduction

### 1.9.2 Challenges Overcome

💪 **EPP/DLP Conflict**: Systematic debugging → 30% CPU improvement 💪 **False Positive Fatigue**: ML tuning + correlation rules → 50% reduction 💪 **Manual Deployment**: Full automation → 50% time saved, 0% errors 💪 **Audit Prep Panic**: Continuous compliance → 95% less prep time

### 1.9.3 Anti-Patterns to Avoid

❌ Single vendor reliance → ✅ Multi-vendor with integration ❌ Manual repetitive tasks → ✅ Automate >3x/month tasks ❌ Alert overload → ✅ Quality over quantity, aggressive tuning ❌ Deferred documentation → ✅ Document as you build

## 1.10 Technology Stack

### 1.10.1 Security Products (15 vendors, $400K/year)

| Category | Product | Purpose |
| --- | --- | --- |
| NGFW | Fortigate 600F | Perimeter + IPS + WAF + VPN |
| SIEM | Splunk ES | Centralized logging + correlation |
| EPP/EDR | CrowdStrike Falcon | Endpoint protection + response |
| NAC | Genian NAC | Network access control |
| DLP | Symantec DLP | Data loss prevention |
| PAM | CyberArk | Privileged access management |
| DB Security | Imperva | Database monitoring + audit |
| APT | FireEye + WildFire | Advanced threat detection |
| Backup | Veeam | Backup + disaster recovery |
| Vuln Scanner | Tenable Nessus | Vulnerability assessment |

### 1.10.2 Infrastructure

* **Compute**: VMware vSphere 7.0 (10 hosts, 500 VMs)
* **Storage**: Dell EMC Unity 600F (100TB all-flash)
* **Network**: Cisco Catalyst 9500/9300, F5 BIG-IP LB
* **OS**: RHEL 8 (70%), Windows Server 2022 (30%), Windows 11 Enterprise (90%)

## 1.11 Future Roadmap

### 1.11.1 2025 Q4

* UEBA (User & Entity Behavior Analytics) → Detect insider threats
* Automated threat hunting (SOAR playbooks)
* AI-powered DLP (33% → 20% false positives)
* ISMS-P certification

### 1.11.2 2026

* Zero Trust Architecture (ZTNA replacement for VPN)
* Cloud Security Posture Management (AWS migration)
* ISO 27001 certification
* SOC 2 Type II (for US clients)

### 1.11.3 2027+

* AI-driven autonomous security operations
* Quantum-safe cryptography (NIST post-quantum standards)
* Automated penetration testing (continuous red team)
* Blockchain-based immutable audit trails

## 1.12 Key Achievements Summary

**Security Posture**: - 19 months zero breaches, zero data leaks - 3 consecutive FSC audits with zero findings - 98% vulnerability SLA compliance - MTTD 3.2min, MTTR 27min (50% better than industry avg)

**Operational Excellence**: - 99.98% trading platform availability - 461 hours/year automated - 45% false positive reduction - DR test 37% faster than target

**Business Impact**: - $188K annual recurring savings - $600K-$1.5M cost avoidance (incidents prevented) - 20% below industry TCO benchmark - ROI 43%-91% in Year 1

**Document**: Compact Architecture Overview for Resume/Portfolio **Classification**: Internal Use **Version**: 1.0 Compact **Date**: 2025-10-16 **Contact**: 이재철 (Jaecheol Lee) | qws941@kakao.com | 010-5757-9592