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**: (Jaecheol Lee) | qws941@kakao.com | 010-5757-9592

2 Nextrade Securities Exchange - Disaster Recovery Plan

2.1 Executive Summary

Comprehensive disaster recovery plan ensuring business continuity for critical trading infrastructure. Achieved **2.5-hour DR test** (37% better than 4-hour target) with **zero data loss** through automated failover procedures.

Scope: Trading platform, clearing system, market data, surveillance **RTO Target**: 4 hours (achieved 2.5 hours) **RPO Target**: 15 minutes (zero data loss) **Test Frequency**: Quarterly (4 tests/year) **Compliance**: FSC requirements, ISO 22301 aligned

---

2.2 RTO/RPO Objectives

System	Classification	RTO Target	RPO Target	2025 Achievement
Trading Platform	Critical	4 hours	15 min	**2.5 hours**
Clearing System	Critical	6 hours	30 min	4.2 hours
Market Data Feed	Critical	2 hours	5 min	1.8 hours
Surveillance	Important	8 hours	1 hour	6 hours
Back Office	Important	12 hours	4 hours	10 hours
Website/Portal	General	24 hours	8 hours	18 hours

Overall Performance: All systems recovered within target RTO/RPO

2.3 Disaster Scenarios

2.3.1 Scenario 1: Primary Data Center Failure

Cause: Power outage, fire, flood, physical breach **Impact**: Complete loss of primary site **Recovery**: Failover to DR site (2.5 hours)

2.3.2 Scenario 2: Ransomware Attack

Cause: Malware encryption of production systems **Impact**: Systems unavailable, data encrypted **Recovery**: Restore from immutable backups (4 hours)

2.3.3 Scenario 3: Network Connectivity Loss

Cause: ISP outage, DDoS, fiber cut **Impact**: External access unavailable **Recovery**: Failover to secondary ISP + BGP rerouting (15 minutes)

2.3.4 Scenario 4: Database Corruption

Cause: Software bug, hardware failure, human error **Impact**: Transaction data inconsistency **Recovery**: Point-in-time restore from backups (2 hours)

2.3.5 Scenario 5: Cyber Attack with Data Breach

Cause: APT, insider threat, credential theft **Impact**: System compromise, potential data exfiltration **Recovery**: Isolate + forensics + clean rebuild (8-12 hours)

2.4 DR Infrastructure

2.4.1 Primary Site (Production)

Location: Seoul Data Center (Gasan Digital Complex) - **Servers**: 150+ (physical + virtual) - **Storage**: Dell EMC Unity 600F (100TB all-flash) - **Network**: Dual 10Gbps links (active-active) - **Power**: N+1 redundancy, UPS + generator

2.4.2 DR Site (Standby)

Location: Busan Data Center (150km from primary) - **Servers**: 100+ (mirrored configuration) - **Storage**: Dell EMC Unity 400F (50TB all-flash) - **Network**: Dual 10Gbps links (active-active) - **Power**: N+1 redundancy, UPS + generator - **Replication**: Synchronous for critical systems

2.4.3 Backup Strategy

Primary Backups: Veeam Backup & Replication - **Full**: Weekly (Sunday 2 AM) - **Incremental**: Daily (2 AM) - **Retention**: 30 days local + 90 days offsite + 7 years archive (tape)

Offsite Storage: Immutable object storage (AWS S3 Glacier) - **Replication**: Daily (encrypted AES-256) - **Air-Gap**: Separate account, MFA required - **Test Restore**: Monthly validation

---

2.5 Recovery Procedures

2.5.1 Failover to DR Site (Scenario 1)

Phase 1: Declaration (10 minutes) 1. Incident Commander declares disaster 2. Notify recovery team (SMS + voice call) 3. Activate war room (Zoom + Slack) 4. Notify FSC within 1 hour

Phase 2: Assessment (20 minutes) 1. Verify primary site status (unreachable/damaged) 2. Check DR site readiness (power, network, storage) 3. Verify latest backup/replication timestamp 4. Confirm data consistency

Phase 3: Network Failover (30 minutes) 1. Update DNS records (TTL 60 seconds) 2. BGP route announcement (DR site IPs) 3. VPN gateway failover 4. Load balancer reconfiguration 5. Verify external connectivity

Phase 4: System Recovery (90 minutes) 1. Power on DR servers (priority order: DB → App → Web) 2. Start critical services (matching engine, order router, market data) 3. Verify database integrity (checksum validation) 4. Enable trading API endpoints 5. Run smoke tests (place test orders)

Phase 5: Verification (20 minutes) 1. Functional testing (end-to-end order flow) 2. Performance testing (latency $<$ 50ms) 3. Data integrity checks (order book reconciliation) 4. User acceptance testing (5 pilot users) 5. Go/no-go decision

Phase 6: Go-Live (10 minutes) 1. Enable production traffic 2. Notify users (email + website banner) 3. Monitor closely (first 2 hours) 4. Incident log updates

Total Time: **2.5 hours** (target 4 hours)

2.5.2 Ransomware Recovery (Scenario 2)

Phase 1: Isolation (15 minutes) 1. Disconnect infected systems from network 2. Disable network shares and backups 3. Block C2 domains on firewall 4. Capture forensic evidence

Phase 2: Assessment (30 minutes) 1. Identify encrypted systems/files 2. Determine ransomware variant (analysis) 3. Check backup availability (not encrypted) 4. Estimate recovery time

Phase 3: Eradication (60 minutes) 1. Wipe infected systems (secure erase) 2. Update all systems (OS patches, AV signatures) 3. Change all credentials (passwords, keys, tokens) 4. Block known IOCs (IPs, domains, hashes)

Phase 4: Restoration (120 minutes) 1. Restore systems from clean backups 2. Verify backup integrity (hash validation) 3. Apply security patches before production 4. Enable monitoring/alerting

Phase 5: Testing (30 minutes) 1. Malware scan on restored systems 2. Functional testing 3. Monitor for re-infection (48 hours)

Total Time: **4 hours**

2.5.3 Network Failover (Scenario 3)

Automated Failover ($<$15 minutes) 1. Monitor detects primary ISP down (2 consecutive failed pings) 2. BGP automatically withdraws primary routes 3. Traffic fails over to secondary ISP 4. Monitoring alert sent (no human intervention required)

Manual Steps (if automation fails) 1. Verify both ISPs down (rare: dual failure) 2. Activate backup 4G/5G links (100Mbps capacity) 3. Notify ISPs for troubleshooting 4. Enable traffic prioritization (critical services only)

2.6 DR Test Results

2.6.1 2025 Q2 Test (2025-04-15)

Scenario: Primary data center failure **Duration**: 2 hours 32 minutes (target: 4 hours) **Success Criteria**: All critical systems restored **Results**: - Trading platform: 2h 18m (RTO 4h) - Clearing system: 2h 25m (RTO 6h) - Market data: 1h 45m (RTO 2h) - All data verified (zero loss) - Minor issue: VPN certificate mismatch (resolved in 12 minutes)

Improvements Applied: - Pre-load VPN certificates on DR site - Add automated DNS update script - Parallel server startup (reduced by 30 minutes)

2.6.2 2025 Q3 Test (2025-07-20)

Scenario: Ransomware attack simulation **Duration**: 3 hours 58 minutes (target: 4 hours) **Results**: - All encrypted systems identified - Clean backup restored successfully - No re-infection detected (48-hour monitoring) - IOC blocking automated

Improvements Applied: - Immutable backup validation (monthly) - Faster malware scan (SSD-optimized)

2.7 Monitoring & Alerting

2.7.1 DR Site Health Checks

Automated Checks (every 5 minutes): - DR site power status - Network connectivity (ping + bandwidth test) - Storage replication lag (<15 minutes) - Backup job success (daily) - Server heartbeats

Alerts (Slack + PagerDuty): - Replication lag >10 minutes → P1 alert - Backup job failure → P1 alert - DR site connectivity loss → P0 alert (immediate escalation)

2.7.2 Recovery Metrics

KPIs: - RTO Achievement: 100% (all systems within target) - RPO Achievement: 100% (zero data loss) - DR Test Pass Rate: 100% (4/4 tests passed) - Backup Success Rate: 99.8% (2 failures in 365 days) - Replication Lag: Avg 3.2 minutes (target <15 minutes)

2.8 Roles & Responsibilities

2.8.1 DR Team

Incident Commander: Security Lead (Jaecheol Lee) - Overall coordination and decision-making - FSC notification and communication - Go/no-go decision for go-live

Technical Lead: Infrastructure Manager - Execution of recovery procedures - System restoration and verification - Post-recovery monitoring

Database Lead: DBA - Database recovery and integrity checks - Transaction log analysis - Performance tuning post-recovery

Network Lead: Network Engineer - Network failover and routing - VPN/firewall reconfiguration - Connectivity verification

Communication Lead: Compliance Manager - User notification and status updates - FSC/regulator communication - Documentation and reporting

2.8.2 Escalation

```
Technical Issue → Technical Lead → Incident Commander → CTO → CEO (if >4h downtime)
```

2.9 Business Continuity

2.9.1 Critical Business Functions

Priority 1 (RTO <4 hours): - Order matching and execution - Market data distribution - Trade clearing and settlement

Priority 2 (RTO <8 hours): - Market surveillance - User account management - Customer support systems

Priority 3 (RTO <24 hours): - Reporting and analytics - Marketing website - Internal collaboration tools

2.9.2 Workarounds During Recovery

Manual Trading (if system unavailable): - Phone orders accepted (backup call center) - Manual order matching (emergency procedure) - Post-recovery electronic reconciliation

Communication Plan: - Website status page updates (every 30 minutes) - Email notifications to registered traders - Social media updates - FSC hourly updates (for >2 hour outages)

2.10 Compliance & Reporting

2.10.1 FSC Reporting Requirements

Incident Notification: - **Initial**: Within 1 hour of disaster declaration - **Progress**: Hourly updates until resolution - **Final**: Within 72 hours post-recovery

Report Contents: - Incident description and root cause - Systems affected and recovery status - Customer impact assessment - Corrective actions and timeline

2.10.2 Audit & Documentation

DR Test Reports (quarterly): - Test objectives and scenarios - Results and metrics (RTO/RPO achieved) - Issues identified and corrective actions - Evidence attachments (logs, screenshots)

Backup Logs (retained 7 years): - Backup job status (success/failure) - Restore test results (monthly validation) - Storage capacity and utilization

---

2.11 Continuous Improvement

2.11.1 Post-DR Test Actions

1. **Debrief Meeting** (within 48 hours)
   - What went well
   - What went wrong
   - Root cause analysis
2. **Action Items** (within 1 week)
   - Update DR procedures
   - Fix identified issues
   - Schedule automation improvements
3. **Procedure Updates** (within 2 weeks)
   - Incorporate lessons learned

- Update runbooks
- Retrain team on changes

4. **Next Test Planning** (within 1 month)
   - Define next scenario
   - Schedule test date
   - Coordinate with business

2.12 Key Achievements

- **RTO Performance**: 37% better than target (2.5h vs 4h)
- **Zero Data Loss**: 100% RPO achievement across all tests
- **Test Success Rate**: 100% (4/4 tests passed in 2025)
- **Automation**: 70% of recovery steps automated
- **Compliance**: 100% FSC requirement satisfaction

Document: Compact DR Plan for Resume/Portfolio **Classification**: Internal Use **Version**: 1.0 Compact **Date**: 2025-10-16 **Next Test**: 2025-10-30 **Contact**: (Jaecheol Lee) | qws941@kakao.com

3 Nextrade Securities Exchange - SOC Operations Runbook

3.1 Executive Summary

24/7 Security Operations Center handling **6,000+ security events/month** with **3.2-minute MTTD** and **27-minute MTTR**. Achieved **zero breaches** in 19 months through proactive monitoring and automated response.

Coverage: 24/7/365 (3 shifts, 2 analysts per shift) **Daily Events**: 15M raw events → 200 alerts → 5-7 investigations **Response Times**: P0 <15min, P1 <30min, P2 <2hr **False Positives**: 33% (improved from 60%)

3.2 SOC Organization

3.2.1 Shift Structure

Shift A (08:00-16:00): 2 analysts + Security Lead **Shift B** (16:00-00:00): 2 analysts **Shift C** (00:00-08:00): 2 analysts

Escalation Path:

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

3.2.2 Tools Access

- **SIEM**: Splunk Enterprise Security (primary dashboard)
- **EDR**: CrowdStrike Falcon console
- **Firewall**: FortiManager (read + limited write)
- **NAC**: Genian NAC console
- **Ticketing**: ServiceNow (incident management)
- **Communication**: Slack (#soc-alerts channel) + PagerDuty

3.3 Daily Operations

3.3.1 Shift Handover Checklist

Previous Shift: 1. Brief on active incidents (status, next steps) 2. Review pending investigations (priority queue) 3. Report system health issues 4. Document shift summary (ServiceNow)

Incoming Shift: 1. Review handover notes 2. Check dashboard health (all panels green) 3. Review overnight alerts (if morning shift) 4. Acknowledge on-call assignment (PagerDuty)

3.3.2 Daily Tasks

08:00 - Morning briefing (15 minutes) - Review previous 24-hour incidents - Check compliance dashboards - Review security news/threat intel

09:00 - Vulnerability scan review - Check critical/high vulnerabilities - Create remediation tickets (if any)

14:00 - Access review - Review privileged access logs (CyberArk) - Check for after-hours access - Investigate anomalies

17:00 - Evening shift handover - Update incident status - Brief evening team

---

3.4 Alert Triage Process

3.4.1 Priority Classification

Priority	Criteria	Response Time	Examples
P0	Active breach, trading platform down	<15 minutes	Ransomware, DDoS, critical system compromise
P1	High-severity threat, confirmed malware	<30 minutes	APT detection, data exfiltration, brute force success
P2	Medium threat, suspicious activity	<2 hours	Single malware, phishing victim, policy violation
P3	Low threat, informational	<4 hours	Failed login, recon attempt, minor violation

3.4.2 Triage Steps (3-5 minutes)

1. **Read Alert**: Title, description, severity
2. **Check Context**:
   - User: Employee or external?
   - Asset: Critical system or workstation?
   - Time: Business hours or after-hours?
   - Location: Office or remote?
3. **Validate**: True positive or false positive?
4. **Classify**: Assign priority (P0-P3)
5. **Assign**: Self-assign or escalate
6. **Ticket**: Create ServiceNow incident

3.5 Investigation Playbooks

3.5.1 Playbook 1: Brute Force Login Attempt

Alert Trigger: 5+ failed logins within 5 minutes

Investigation Steps: 1. Check user account status (active/locked?) 2. Review source IP (internal/external/VPN?) 3. Check authentication logs (last 24 hours) 4. Verify legitimate user activity (contact user if needed)

Splunk Query:

```
index=windows_events EventCode=4625 user=[USERNAME] earliest=-24h
| stats count by src_ip, logon_type
| sort -count
```

Common Outcomes: - **False Positive**: User forgot password (3 attempts, then locked) - **True Positive**: Attacker brute forcing (>100 attempts, multiple IPs)

Response Actions: - If internal user: Contact user, force password reset - If external attacker: Block source IP (30-min temp block), notify CISO if >1000 attempts

---

3.5.2 Playbook 2: Malware Detection

Alert Trigger: EDR detects malicious file or behavior

Investigation Steps: 1. Check file details (name, path, hash, signature) 2. Review process tree (parent/child processes) 3. Check network connections (C2 communication?) 4. Verify user activity (what was user doing?) 5. Check for lateral movement (other systems infected?)

CrowdStrike Query:

```
DeviceID = [DEVICE_ID] AND DetectionType = "Malware"
| Show ProcessTree, NetworkConnections
```

Response Actions: 1. **Contain**: Isolate endpoint (NAC quarantine + network block) 2. **Kill**: Terminate malicious process 3. **Collect**: Memory dump + forensics 4. **Eradicate**: Full scan + remove artifacts 5. **Recover**: Restore if needed, re-enable endpoint 6. **Post-Mortem**: Update IOCs, document lessons learned

---

3.5.3 Playbook 3: DLP Violation (Data Exfiltration)

Alert Trigger: DLP blocks sensitive data transfer

Investigation Steps: 1. Review file details (name, size, sensitivity) 2. Check destination (email, USB, cloud upload?) 3. Verify user intent (legitimate business need?) 4. Check user history (previous violations?) 5. Review manager approval (if required)

Splunk Query:

```
index=dlp user=[USERNAME] action=block earliest=-7d
| table _time, file, destination, reason
```

Response Actions: - **Low-Risk**: Notify user, educate on policy - **Medium-Risk**: Notify user + manager, create HR ticket - **High-Risk**: Disable account, preserve evidence, escalate to legal

---

3.5.4 Playbook 4: Suspicious Outbound Traffic

Alert Trigger: Firewall detects unusual outbound connection

Investigation Steps: 1. Check destination IP/domain (reputation, geolocation) 2. Review source system (server or workstation?) 3. Analyze traffic pattern (volume, frequency, protocol) 4. Correlate with other events (EDR alerts, auth logs) 5. Check threat intelligence (known C2?)

Splunk Query:

```
index=firewall action=allowed dst_ip=[SUSPICIOUS_IP]
| stats sum(bytes) as total_bytes by src_ip, dst_port
| where total_bytes > 10485760
```

Response Actions: - **Benign**: Whitelist if legitimate (e.g., new SaaS tool) - **Suspicious**: Contain endpoint, deep investigation - **Confirmed C2**: Full incident response (isolate, eradicate, recover)

3.6 SIEM Dashboards

3.6.1 Main SOC Dashboard

Panels: 1. **Real-Time Alerts**: Last 24 hours by severity 2. **Top Threats**: Most common alert types 3. **Failed Logins**: Brute force attempts by source 4. **Malware Detections**: Endpoint threats by user 5. **DLP Violations**: Data exfiltration attempts 6. **Network Anomalies**: Unusual traffic patterns 7. **Vulnerability Counts**: Critical/High by system

3.6.2 Compliance Dashboard

Panels: 1. **Privileged Access**: CyberArk session count 2. **Access Reviews**: Quarterly recertification status 3. **Patch Compliance**: Systems missing critical patches 4. **Backup Success Rate**: Daily backup job status 5. **Firewall Policy Changes**: Recent modifications

---

3.7 Automated Response

3.7.1 SOAR Integrations

Malware Detected: → Isolate endpoint (NAC API) → Kill process (CrowdStrike API) → Block IOCs (FortiManager API) → Create ticket (ServiceNow API) → Notify SOC (Slack webhook)

Brute Force >100 Attempts: → Block source IP (Firewall API, 30-min block) → Force password reset (AD API) → Enable MFA (if not already) → Notify user (Email API)

DLP High-Severity: → Block action (automatic) → Notify user + manager (Email) → Create HR ticket (ServiceNow) → Preserve evidence (copy to secure storage)

3.8 Escalation Procedures

3.8.1 When to Escalate

To Security Lead (L2): - P0 incidents (always) - P1 incidents (if unclear response) - Multiple related incidents (potential campaign) - Need for privileged actions (firewall changes, account disable)

To CISO (L3): - Active breach or suspected APT - Potential regulatory notification (FSC) - Major incident (>4 hour impact) - Executive account compromise

To CTO: - Business-critical system down (trading platform) - Potential financial impact >$100K - Reputation risk (media attention)

3.9 Metrics & Reporting

3.9.1 Daily Metrics (Shift Summary)

- Total Alerts: [Count]
- Investigated: [Count]
- True Positives: [Count]
- False Positives: [Count]
- Incidents Created: [Count]
- Average Response Time: [Minutes]

3.9.2 Weekly Report (Monday Morning)

- Total Events: 15M
- Alerts Generated: 1,500
- Incidents Investigated: 150
- Confirmed Threats: 5-7
- Top Alert Types: [List]
- Top Threat Actors: [List]
- Remediation Status: [Open/Closed counts]

3.9.3 Monthly Report (First Friday)

- Security Posture: Trend analysis
- SLA Compliance: P0/P1/P2/P3 percentages
- MTTR Trend: Improving or degrading?
- False Positive Rate: Current vs. target
- Top Vulnerabilities: Critical/High counts
- Compliance Status: ISMS-P/ISO checkpoints

3.10 Knowledge Base

3.10.1 Common False Positives

Antivirus False Alarm: - Legitimate software flagged (e.g., PuTTY, Wireshark) - Action: Add to whitelist, notify endpoint team

DLP Over-Blocking: - Encrypted file detected as PII (zip password) - Action: Manual review, adjust DLP policy

Firewall Noise: - Network scanner traffic (Nessus scans) - Action: Create exception for scanner IPs

3.10.2 Quick Reference

Block IP on Firewall:

```
ssh admin@firewall.local
config firewall address
  edit "BLOCK_[IP]"
  set subnet [IP]/32
end
config firewall policy
```

```
  edit [POLICY_ID]
  set srcaddr "BLOCK_[IP]"
  set action deny
end
```

Quarantine Endpoint (NAC):

```
curl -X POST https://nac.local/api/quarantine \
  -H "Authorization: Bearer [TOKEN]" \
  -d '{"mac":"XX:XX:XX:XX:XX:XX","duration":"24h"}'
```

Disable AD Account:

```
Disable-ADAccount -Identity "USERNAME"
Set-ADUser -Identity "USERNAME" -Description "Disabled by SOC: [INCIDENT_ID]"
```

3.11 Team Training

3.11.1 Onboarding (2 weeks)

Week 1: Tool training - Splunk SIEM basics - CrowdStrike console - ServiceNow ticketing - Read-only monitoring (shadow experienced analyst)

Week 2: Incident response - Playbook walkthroughs - Practice investigations (historical incidents) - Escalation procedures - First on-call shift (with mentor)

3.11.2 Ongoing Training

Monthly: Tabletop exercises (simulate incidents) **Quarterly**: Tool updates and new feature training **Annually**: Security certifications (GCIA, GCIH, CySA+)

3.12 Shift Notes Template

```
# SOC Shift Summary: [Date] [Shift A/B/C]

## Analyst: [Name]

## Active Incidents
1. [INC-12345] - Brute force on admin account - P1 - In Progress
2. [INC-12346] - DLP violation - P2 - Awaiting user response

## Alerts Reviewed: [Count]
- True Positives: [Count]
- False Positives: [Count]
- Dismissed: [Count]

## Notable Events
- [Time] - [Brief description]
- [Time] - [Brief description]

## System Issues
- None / [List any tool/dashboard issues]

## Handover Notes
```

```
- [Any pending items for next shift]
- [Any follow-up required]

## Next Shift Action Items
1. [Action 1]
2. [Action 2]
```

3.13 Key Performance Indicators

2025 Achievements: - Events Processed: 15M/month - Alert Accuracy: 67% (33% false positives, down from 60%) - MTTD: 3.2 minutes (target <5 min) - MTTR: 27 minutes (target <30 min) - SLA Compliance: P0 100%, P1 95%, P2 92% - Incidents Prevented: 150+ confirmed threats neutralized - Zero Breaches: 19 months continuous

---

Document: Compact SOC Runbook for Resume/Portfolio **Classification**: Internal Use **Version**: 1.0 Compact **Date**: 2025-10-16 **On-Call**: See PagerDuty schedule **Contact**: SOC Lead (Jaecheol Lee) | qws941@kakao.com | 010-5757-9592