Contents

1 Nextrade Securities Exchange - SOC Operations Runbook

1.1 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%)

1.2 SOC Organization

1.2.1 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
```

1.2.2 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

1.3 Daily Operations

1.3.1 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)

1.3.2 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

---

1.4 Alert Triage Process

1.4.1 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

Priority	Criteria	Response Time	Examples
P3	Low threat, informational	<4 hours	Failed login, recon attempt, minor violation

1.4.2 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

1.5 Investigation Playbooks

1.5.1 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

---

1.5.2 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

---

1.5.3 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

---

1.5.4 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)

1.6 SIEM Dashboards

1.6.1 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

1.6.2 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

---

1.7 Automated Response

1.7.1 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)

1.8 Escalation Procedures

1.8.1 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)

1.9 Metrics & Reporting

1.9.1 Daily Metrics (Shift Summary)

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

1.9.2 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]

1.9.3 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

1.10 Knowledge Base

1.10.1 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

1.10.2 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]"
```

1.11 Team Training

1.11.1 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)

1.11.2 Ongoing Training

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

1.12 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]
```

1.13 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