Table of Contents

# 1 KMU Next-Generation System - Technical Overview

## 1.1 프로젝트 개요

**기간**: 2021.11 ~ 2022.04 (6개월) **소속**: ㈜조인트리 **역할**: 인프라·시스템 엔지니어 **프로젝트**: 국민대학교 차세대 정보시스템 구축 **규모**: 대학 전체 IT 인프라 차세대 시스템 전환

## 1.2 시스템 아키텍처

### 1.2.1 네트워크 세분화 (Micro-Segmentation)

**기술 스택**: VMware NSX-T, UTM (Unified Threat Management)

**구성**: - **Zone-based Segmentation**: 업무 특성에 따른 네트워크 zone 분리 - **Micro-segmentation**: 애플리케이션 레벨 트래픽 제어 - **Zero Trust 아키텍처**: 모든 트래픽 검증 및 제어

**효과**: - 측면 이동(Lateral Movement) 공격 차단 - 네트워크 장애 영향 범위 최소화 - 보안 정책 세밀화

### 1.2.2 보안 솔루션 통합 운영

#### 1.2.2.1 1. NAC (Network Access Control)

**목적**: 단말 접속 제어 및 보안 정책 준수

**기능**: - 단말 인증 및 등록 관리 - 보안 정책 준수 검사 (백신, 패치 상태) - 비인가 단말 접속 차단 - MAC 주소 기반 접근 제어

**성과**: - 비인가 단말 접속 차단율 95% - 단말 보안 정책 준수율 90% 이상

#### 1.2.2.2 2. DLP (Data Loss Prevention)

**목적**: 민감정보 유출 방지

**기능**: - 개인정보(주민등록번호, 계좌번호 등) 탐지 - 이메일/USB/네트워크 경로 차단 - 민감 문서 암호화 강제 - 실시간 콘텐츠 검사

**성과**: - 민감정보 탐지율 20% 향상 (탐지 누락 50건 → 10건/월) - DLP 룰 재설계로 오탐 30% 감소

#### 1.2.2.3 3. APT (Advanced Persistent Threat) 방어

**목적**: 지능형 지속 위협 탐지 및 대응

**기능**: - 샌드박스 기반 악성코드 분석 - 제로데이 공격 탐지 - C&C (Command & Control) 통신 차단 - 행위 기반 위협 분석

**성과**: - 월 평균 200건 위협 차단 - 침해사고 예방률 80% 달성

## 1.3 오픈소스 기반 보안 모니터링

### 1.3.1 OSS (Open Source Software) 모니터링 시스템 구축

**기술 스택**: - **ELK Stack**: Elasticsearch, Logstash, Kibana - **Grafana**: 실시간 대시보드 - **Prometheus**: 메트릭 수집 및 알림 - **Zabbix**: 인프라 모니터링

**구성**: 1. **로그 수집**: Logstash를 통한 보안 장비 로그 수집 2. **로그 분석**: Elasticsearch 기반 로그 분석 및 검색 3. **시각화**: Kibana 대시보드를 통한 실시간 모니터링 4. **알림**: Prometheus AlertManager를 통한 이벤트 알림

**효과**: - 보안 이벤트 탐지 시간 70% 단축 - 통합 대시보드를 통한 가시성 확보 - 상용 솔루션 대비 비용 절감

## 1.4 주요 성과

### 1.4.1 1. 안정성 향상

**목표**: 시스템 안정성 및 가용성 향상

**구현**: - 네트워크 세분화를 통한 장애 격리 - 이중화 아키텍처 구축 - 실시간 모니터링 체계 구축

**성과**: - 네트워크 장애율 25% 감소 (월 12건 → 9건) - 서비스 가용률 99.9% 유지 (연간 다운타임 8.7시간 이하) - 장애 복구 시간(MTTR) 40% 단축

### 1.4.2 2. 보안 강화

**목표**: 다층 보안 체계 구축 및 위협 대응 능력 향상

**구현**: - NAC, DLP, APT 통합 운영 - Zero Trust 네트워크 아키텍처 - 실시간 위협 모니터링

**성과**: - 침해사고 예방률 80% 달성 (월 200건 위협 차단) - 민감정보 유출 시도 100% 차단 - 보안 이벤트 대응 시간 50% 단축

### 1.4.3 3. 정책 최적화

**목표**: 보안 정책 정교화 및 운영 효율성 향상

**구현**: - DLP 룰 재설계 (패턴 최적화) - NAC 정책 정비 (단말 그룹별 차별화) - 네트워크 세분화 정책 수립

**성과**: - DLP 오탐률 30% 감소 - NAC 정책 적용 시간 50% 단축 - 보안 정책 준수율 90% 이상

### 1.4.4 4. 고가용성 구현

**목표**: 무중단 서비스 제공

**구현**: - Active-Active 이중화 - Load Balancer 구성 - Failover 자동화

**성과**: - 연간 다운타임 8.7시간 이하 (99.9% 가용성) - Failover 시간 30초 이내 - 장애 영향 범위 최소화

## 1.5 기술 스택

### 1.5.1 Network Security

* **Micro-Segmentation**: VMware NSX-T
* **UTM**: Unified Threat Management
* **Firewall**: Next-Generation Firewall

### 1.5.2 Endpoint Security

* **NAC**: Network Access Control
* **DLP**: Data Loss Prevention
* **APT**: Advanced Persistent Threat Defense

### 1.5.3 Monitoring & Logging

* **ELK Stack**: Elasticsearch, Logstash, Kibana
* **Grafana**: Metrics Visualization
* **Prometheus**: Metrics Collection & Alerting
* **Zabbix**: Infrastructure Monitoring

### 1.5.4 Infrastructure

* **Virtualization**: VMware vSphere
* **Load Balancer**: F5 BIG-IP
* **Storage**: Enterprise SAN

## 1.6 핵심 역량

1. **네트워크 세분화**: VMware NSX-T 기반 Micro-segmentation 설계 및 구축
2. **통합 보안 운영**: NAC, DLP, APT 등 다층 보안 솔루션 통합 관제
3. **OSS 모니터링**: ELK Stack, Grafana 기반 실시간 보안 모니터링 시스템 구축
4. **고가용성 아키텍처**: 이중화 및 Failover 자동화를 통한 99.9% 가용성 달성
5. **정책 최적화**: 보안 정책 정교화를 통한 오탐 감소 및 운영 효율성 향상

## 1.7 교훈 및 인사이트

### 1.7.1 1. 네트워크 세분화의 중요성

VMware NSX-T를 활용한 Micro-segmentation은 측면 이동 공격을 효과적으로 차단하고, 장애 영향 범위를 최소화합니다. Zero Trust 아키텍처의 핵심 요소입니다.

### 1.7.2 2. 통합 보안 운영의 효율성

NAC, DLP, APT를 통합 운영하여 월 200건의 위협을 차단했습니다. 각 솔루션의 로그를 ELK Stack으로 통합하여 가시성을 확보한 것이 핵심입니다.

### 1.7.3 3. OSS 기반 모니터링의 장점

상용 SIEM 솔루션 대신 ELK Stack과 Grafana를 활용하여 비용을 절감하고, 커스터마이징을 통해 유연한 모니터링 체계를 구축했습니다.

### 1.7.4 4. 정책 최적화의 실질적 효과

DLP 룰 재설계로 민감정보 탐지율을 20% 향상시키고 오탐을 30% 감소시켰습니다. 보안 정책은 지속적인 최적화가 필요합니다.

**문서 작성일**: 2025-10-20 **작성자**: 이재철 (인프라·보안 엔지니어)