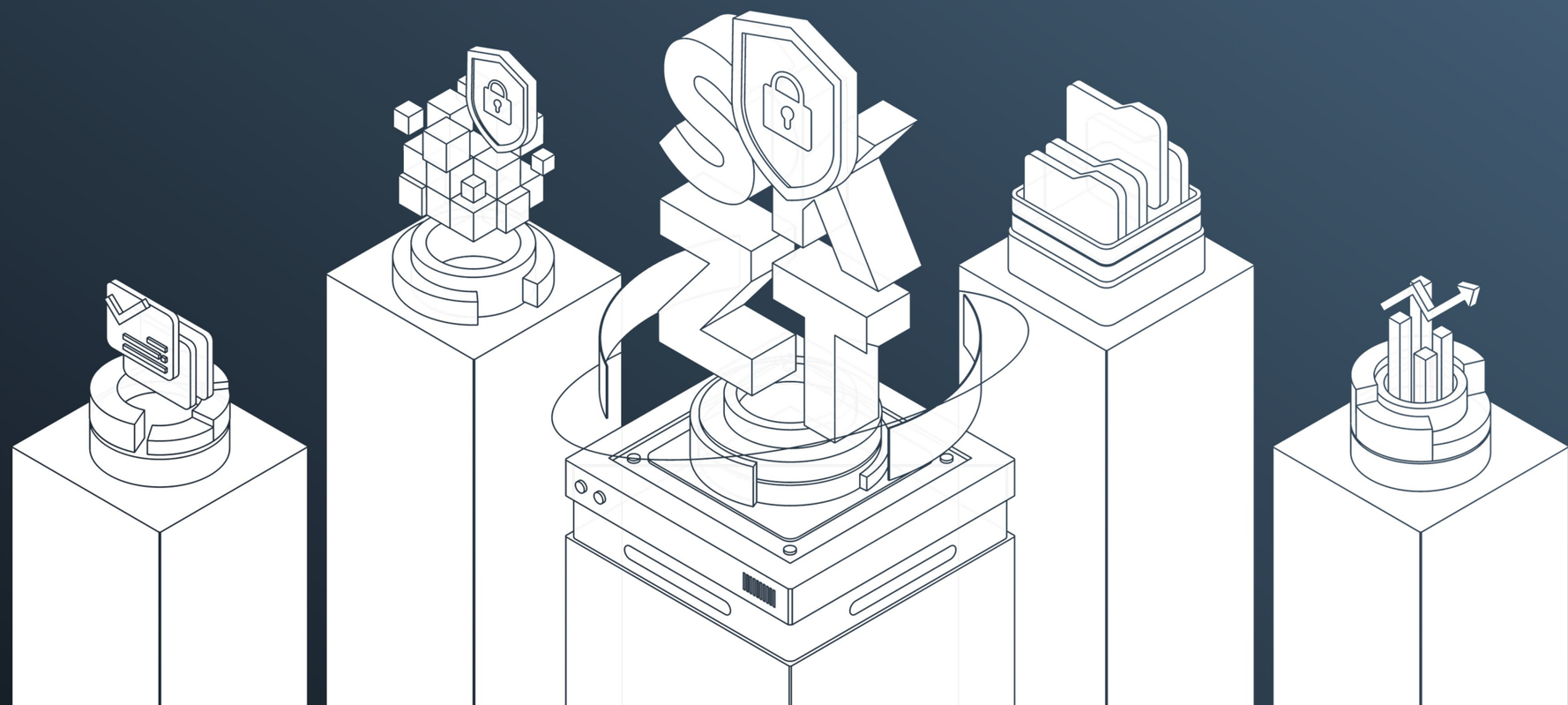
Go ahead

ZERO TRUST SKZT

SK 쉴더스

제로트러스트의 시작 +

SKZT로 완성하다



SK 쉴더스

경기도 성남시 분당구 판교로 227번길 23, 4F – 5F

T. 1800-6400
H. www.skshieldus.com

제로트러스트 도입을 고민하고 계시는 고객을 위한

SKZT를 소개합니다

STEP 1

SKZT 성숙도 평가

제로트러스트
도입 수준 진단

STEP 2

SKZT 환경 구축

진단 결과에 따른
제로트러스트 전환 수행

STEP 3

SKZT 운영 관리

제로트러스트
운영 체계 수립

STEP 4

SKZT 고도화 및 개선

제로트러스트
영역 점진적 확대

SKZT 국내 환경에 최적화된 제로트러스트 도입 방법론

국내·외 가이드라인이 반영된 방법론 보유

NIST	CISA	DOD	국가정보원	KISA
"SP 800-207" "SP 800-207A"	"Zero Trust Maturity Model V2.0"	"ZTStrategy V1.0" "ZT Capability Execution Roadmap"	"국가 망 보안체계 보안 가이드라인" (N²SF)	"제로트러스트 가이드라인 V2.0"

SK쉴더스 사업 수행 방법론

SK쉴더스의 다년간 검증된
방법론 개발 경험 바탕의
제로트러스트 도입 방법론 개발

프로젝트 수행 경험

기업, 금융권, 공공기관 등
다양한 규모와 산업 분야에서
성공적으로 프로젝트를 수행한 경험

STEP 01 제로트러스트 성숙도 평가

성공적 제로트러스트 도입을 위해 SK쉴더스만의
최적의 평가 방법으로 마스터플랜을 수립해 개선 방향을 제시합니다

철저한 분석기반 성숙도 평가를 통해 도입기관에 최적화된
맞춤형 제로트러스트 보안모델을 제시합니다

Analytics | 분석

단계 목표

- 성숙도 평가를 위한 현행 시스템 **환경 및 요구사항 분석**

수행 내용

- 성숙도 평가 기준 및 대상(리소스) 선정
- **제로트러스트 도입 요구사항 분석**

조직 | 업무 | 환경 | 자산

Evaluation | 평가

단계 목표

- 현행시스템 분석결과 기반 **ZT(6+3)요소별 성숙도 수준 진단**
- **SKZT 체크리스트 적용 성숙도 평가 및 결과 도출**
- **스코어링을 통한 성숙도 수준(R0~R3)평가**

수행 내용

- 성숙도 평가 대상 리소스 분류
- **Case별 성숙도 평가 SKZT체크리스트 적용**
- **결과 도출 및 수행을 통한 최종 성숙도 결과 도출**

사용자 | 디바이스 | 네트워크 | 시스템 | 애플리케이션 | 데이터 | 분석 | 자동화 | 거버넌스

Strategy | 전략 수립

단계 목표

- 성숙도 평가 결과 담당자 공유 및 배포
- **담당자 인터뷰를 통한 인적기반 정보 추가 수집 및 지속 반영**
- **최종 To-Be 모델 및 SKZT마스터플랜(전략) 도출**
- **단계별 개선과제 도입 및 구축 계획 수립 및 도출**

수행 내용

- 최종 성숙도 평가 결과 도출
- **To-Be 모델 도입전략 및 추진 계획과 방안 도출**
- **SKZT 마스터플랜 및 개선과제 도출**

성숙도 | 개선과제 | 추진방안 | 구축계획 | 모델도출

세부 분석 항목

조직
- 조직도 기반 사용자 업무 정의
- 외부 기관(협력사)와의 관계 정의 및 분석
- 외주 기관(계약관계)와의 관계 정의 및 분석
- 사용자별 IT자산 활용 정의 및 분석

업무
- IT관련 부서별 업무 정의 및 분석
- 업무별 타 부서, 타 기관 공유 업무 정의 및 분석
- 업무별 IT자산 접근 및 활용 정의 및 분석
- 제로트러스트 관련 교육 수행

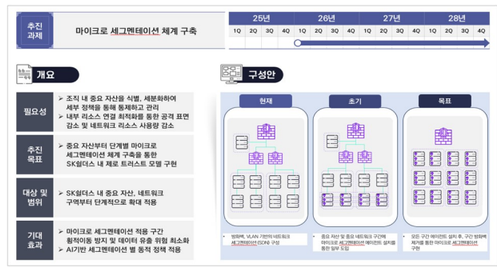
환경
- 리소스 접근 기반(네트워크) 환경 분석
- 외부접근환경(자택, 외근, 파견 등) 분석
- 다양한 업무 환경(클라우드, 온프라) 분석

자산
- IT자산의 종류 및 사용목적에 따른 정의
- IT자산의 내구연한 및 개선 가능성 분석
- IT자산의 접근 권한 및 주사용자, 관리자, 부서, 기관 정의 및 분석

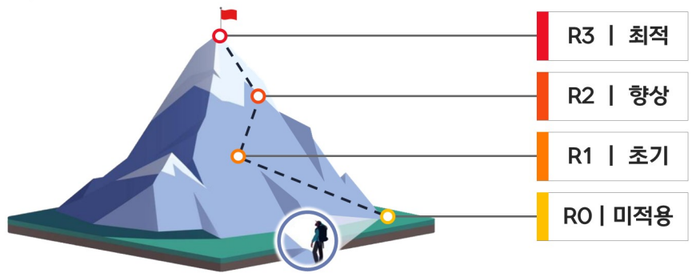
핵심요소별 세부 평가항목

개선과제 도출 및 구축 계획

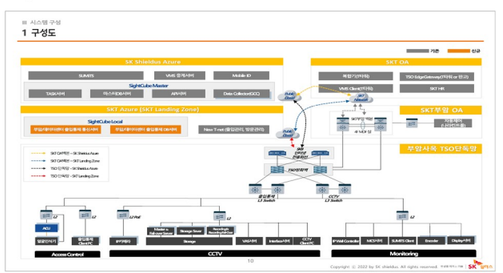
개선과제별 상세 추진방안



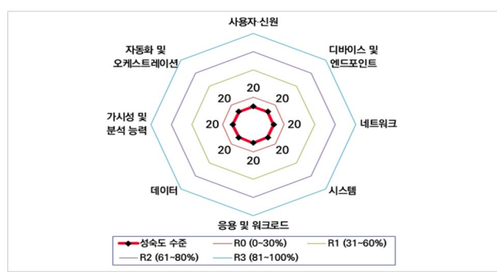
스코어링 기반 ZT 성숙도 수준 등급 정의



TO-BE 모델 도출



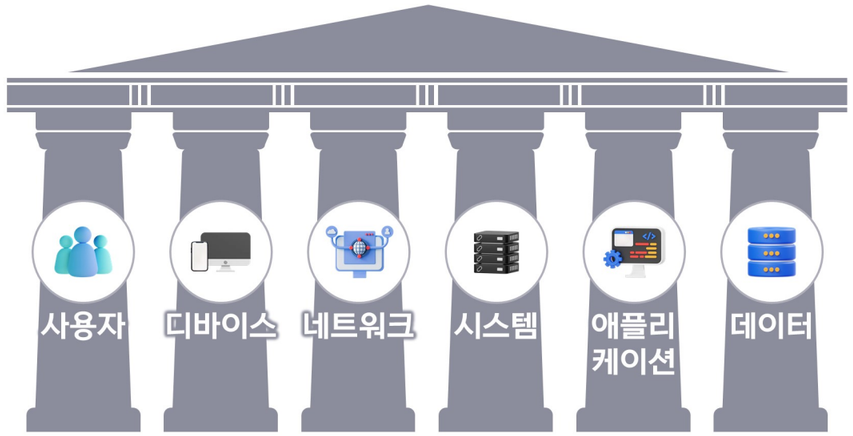
성숙도 평가 결과 다이어그램



STEP 02 제로트러스트 보안 모델 환경 구축

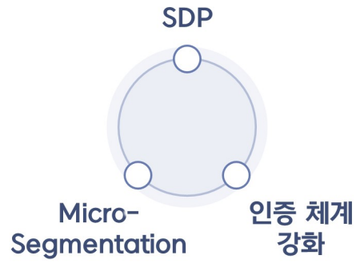
제로트러스트 보안 아키텍처 기반 SK쉴더스만의 최적화된 모델로
제로트러스트 환경을 구축합니다

아키텍처 구성 핵심요소 6가지와 가시성과 분석, 자동화와 통합, 거버넌스를 더한 통합 환경구축을 통해
보다 철통같은 제로트러스트 환경을 구현합니다



제로트러스트 아키텍처 구현

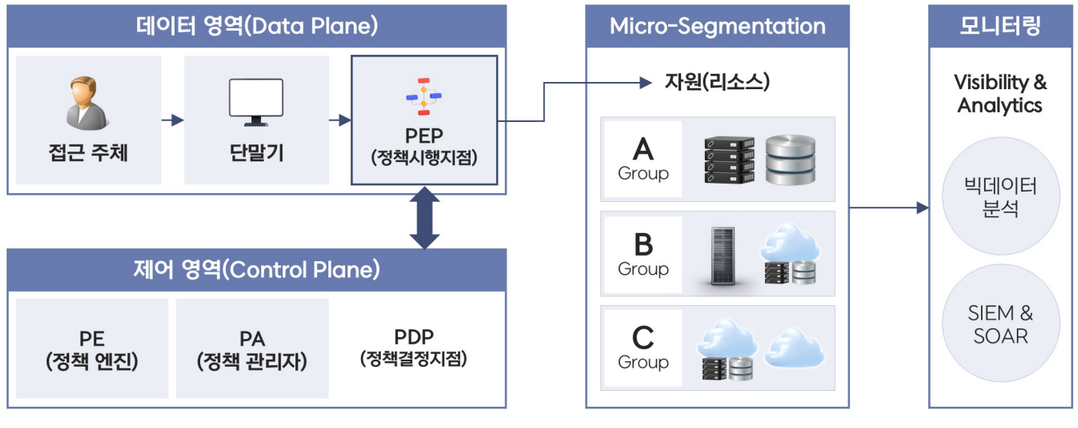
- 사용자, 디바이스에 대한 관리 및 강력한 인증
- 리소스 분류 및 관리를 통한 세밀한 접근제어(최소 권한 부여)
- 논리 경계 생성 및 세션 단위 접근 허용, 통신 보호 기술 적용
- 모든 상태의 모니터링 및 로그 수집을 통한 신뢰성 지속적 검증, 제어



제로트러스트 기능 구현

권장 시스템	환경별 구축 고려요소	
사용자 인증	AI, DT	RBI
SDP	이상징후 분석	데이터 추적
Micro-Segmentation	클라우드	EDR

제로트러스트 접근제어 절차 구현



STEP 03 제로트러스트 운영 관리

제로트러스트 환경 구축을 통해 환경이 구현되면 기존의 운영체계와는 다른
새로운 제로트러스트 운영 환경에서의 관리 방법이 필요합니다

제로트러스트의 모든 영역을 관찰 및 탐색하기 위한 가시성 확보는 물론
더욱 고도화되고 자동화된 방어체계를 통해 위협에 대응해야 합니다

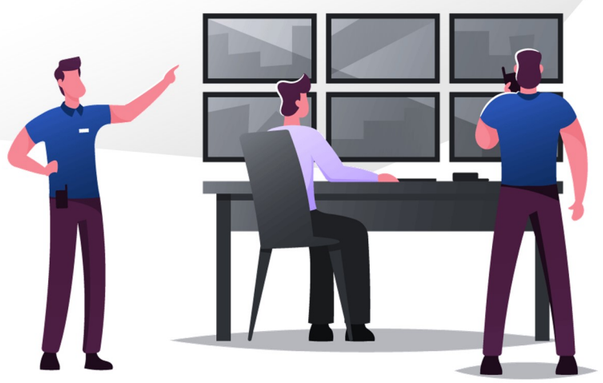
제로트러스트 운영 관리를 통한 가시성 확보 및 위협 대응

가시성 확보

- 사용자
- 디바이스
- 네트워크
- 시스템
- 애플리케이션
- 데이터

모든 종류의 위협을 관찰하고, 지능화된 방어기법 적용

- 행위 기반 모니터링
- 동적 로그수집
- 패킷 단위 이상 트래픽 탐지
- 위협 인텔리전스



자동화 대응 체계 수립

빅데이터(SIEM) 분석

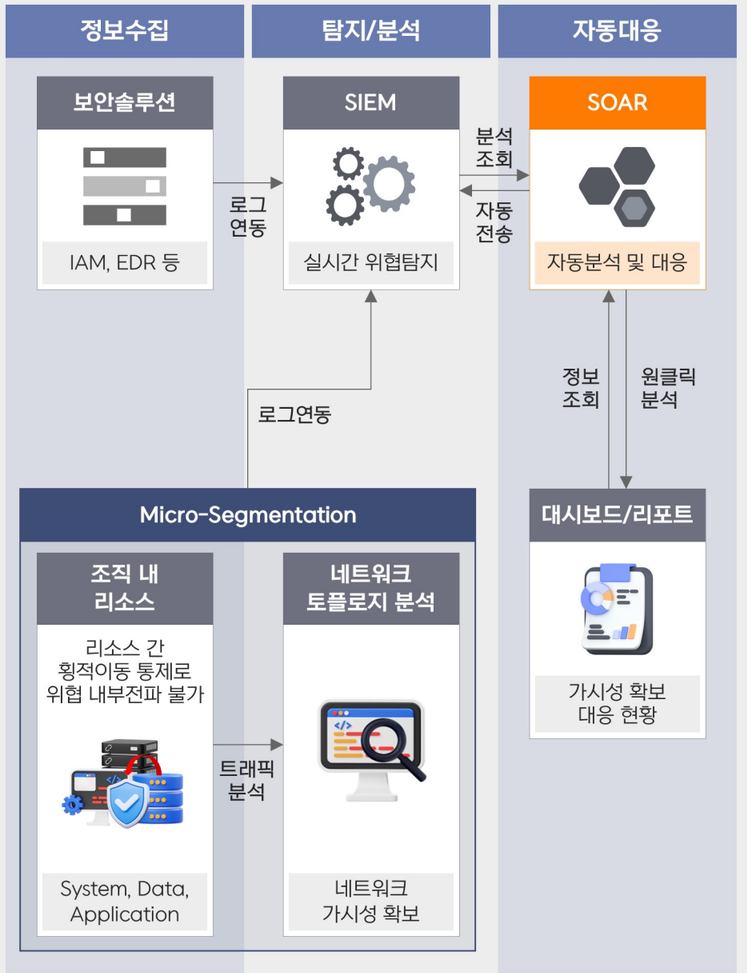
데이터 수집/저장/분석	실시간 검색 및 상관분석	이상행위 기반 위협분석

+

대응 자동화(SOAR)

사고대응 표준화/간소화	정책 및 프로세스 자동화	보안 운영 효율화

주요 프로세스



STEP 04 제로트러스트 고도화 및 개선

제로트러스트 보안 모델은 일회성 도입 및 전환으로 구현 불가하며,
또 다른 위기를 초래할 수 있습니다

도입 후 안정적인 운영을 위해 계획된 점진적 전환이 필요하고,
지속적인 고도화로 보안 모델의 성숙도를 개선해야 합니다

제로트러스트 보안 모델 도입 후 점진적인 전환 및 성숙도 고도화를 위한 지속적 환경 운영관리 필수

구축

ZT 구성요소: 사용자 | 디바이스 | 네트워크 | 시스템 | 애플리케이션 | 데이터

DATA

기존 레거시 솔루션			ZTA 기반 신규 솔루션			로그정보, 위협정보		
Server	Service	Data	Server	Service	Data	보안 로그	네트워크 로그	위협 정보

운영

가시성 및 분석

빅데이터(SIEM)분석 + 대응 자동화(SOAR)

- 사고대응 **표준화/간소화**
- 정책 및 프로세스 **자동화**
- 연관 장비 간 **자동화**

자동화 및 통합

지능화 방어기법

- 지능화된 방어기법
- 이상 트래픽 분석
- 동적정책 변경
- 비정상 행위 탐지

고도화

- 정책정보지점(PIP)
- AI Threat Intelligence
- Machine Learning
- Cyber Hygiene
- Robotic Process Automation

Next 레벨 성숙도 도입 시

- 접근 주체, 자산, 비즈니스 프로세스/워크플로우에 대해 재식별·평가하는 과정으로 전환
- 인프라 관련 부서와의 긴밀한 협업 체계 구성 필수
- 사내 관리자(임원 등)에게 지속적 객관적 근거 기반 성숙도 향상 필요성 보고

프로세스 구현 시 고려사항

- 비즈니스 프로세스
- 워크플로우
- 접근 주체의 변화
- 관련 타 부서 협업
- 내부 정책 변화
- 법률 및 지침 변경

점진적 전환

장애 최소화를 위한 점진적 전환

- 과도한 권한 부여
- 정상 사용자 리소스 접근 거부
- 필요 권한 취득 거부
- 비인가 장비 접근 허용
- 보안 어플라이언스 추가 및 강화로 인한 사용자 불만 증가
- 기타 돌발적이고, 다양한 문제 발생 여지

시범 운영

지속적 수정 및 모니터링, 리포팅 수행

민감문제 발생 시 리포팅만 수행

장애분석 및 분류(정책, 위협 등)를 위한 Raw데이터 수집

비 정상적인 접근제어 모니터링

비정상적인 접근제어 발생 여부의 지속적 모니터링 과 로그 생성

- 접근제어 정책의 지속적으로 개선 및 현행화
- 실 운영시 발생할 수 있는 돌발적 장애에 대한 훈련과 대비 및 보안책 수립

정상 운영

운영 환경 적용 지속적인 모니터링

- 시범운영 완료 후 운영 관리자 판단을 통한 정상운영으로의 전환
- 성숙도 수준 별 사용자와 자산, 네트워크 접근제어의 지속적 모니터링
- 트래픽 및 어플라이언스 정보에 대한 연속적인 로그 기록
- 필요에 의한 접근제어 정책 튜닝 시 망 전체 영향 전파 가능성에 유의

제로트러스트 필러별 핵심 시스템

사용자

사람, 서비스 혹은 IoT 기기 등을
고유하게 설명할 수 있는 속성이나 속성 집합

구현 내용

조직 내 사용자를 식별해, 최소 권한 원칙 기반으로
인증절차를 강화하고 계정 및 권한을 통제

핵심 시스템

IAM
- 사용자의 아이덴티티를 중앙에서 관리
- 계정및 권한을통합적으로관리하며, RBAC과 ABAC 정책을 적용

SSO
- 다양한 시스템을 한번의 인증으로 접근하도록 지원
- 인증 진행 간 사용자의 위험도를 평가해 동적으로 액세스 관리

MFA
- 다중 인증 요소를 활용하여 사용자 인증 강화를 지원
- 생체정보, OTP 등을 활용한 추가 인증 수단 제공 및 Passwordless 인증

AD(인증)
- 사용자의 디렉토리 서비스 관리 및 인증 지원
- 그룹 정책 설정 및 권한 부여

HR시스템
- 사용자의 역할, 부서, 직급 등 다양한 속성정보를 제공
- ICAM과 연동하여 최신화된 인사정보를 제공

디바이스

IoT 기기, 휴대폰, 노트북, PC, 서버 등
데이터를 주고받는 모든 하드웨어 기기

구현 내용

디바이스를 고유하게 식별해 등록하여 관리하고,
엔드포인트 보안을 강화해 디바이스 신뢰도 확보

핵심 시스템

자산관리 시스템
- 조직 내 모든 OA장비를 식별 및 관리
- 다른 보안솔루션과 실시간 연동을 통해 디바이스 상태를 실시간 모니터링

AD(PMS)
- 디바이스의 보안 설정을 중앙에서 관리하며, 일괄적인 패치 관리
- 도메인 내 모든 디바이스를 체계적으로 관리

EDR
- 디바이스의 위협을 실시간으로 탐지하고 대응
- 비인가 접근을 방지하고, 디바이스에 대한 신뢰성를 지속적으로 평가

UEM
- 모바일 기기뿐만 아니라 다양한 IoT 기기까지 통합적으로 관리
- 개인 기기와 업무용 데이터를 분리하여 BYOD 환경을 관리 가능

EPP
- 디바이스에 대한 통합 보안 플랫폼
- 백신, 패치관리, 개인정보보호 등 다양한 보안기능을 제공

네트워크

기업망의 유무선 네트워크와 클라우드 접속을
포함하는 인터넷 등 모든 데이터 전송 매체

구현 내용

네트워크 내·외부 트래픽 흐름을 실시간으로
모니터링하고 관리하여, 세분화 단위로 통제

핵심 시스템

ZTNA
- SDP(소프트웨어 정의 경계)의 확장
- 최소 권한 원칙 기반으로 사용자와 디바이스를 평가하고, 안전한 연결만 허용

NGFW
- 전통적인 방화벽 기능에 IPS, SSL 복호화 등 고급 보안 기능 제공
- 애플리케이션 콘텐츠 기반 정책 설정 및 세분화된 보안 관리 기능

SDN
- 소프트웨어 기반으로 네트워크 리소스를 세분화하고 관리
- 동적 트래픽 라우팅 및 정책 적용으로 네트워크 자원을 최적화

Micro-Segmentation
- 네트워크를 논리적으로 세분화하여 각 세그먼트 간의 트래픽을 관리
- 민감한 자산에 대한 접근을 최소화하며, 내부 위협 확산을 방지

NDR
- 풀 패킷 모니터링으로 네트워크 트래픽 실시간 분석과 이상징후 탐지
- AI/ML 기반 분석으로 이상 트래픽을 식별하고, 자동화된 조치 수행

시스템

중요 애플리케이션을 실행하거나 데이터를
저장·관리하는 서버

구현 내용

시스템(서버)의 보안을 강화하여 위협을 사전에
탐지하고 확산을 방지

핵심 시스템

Micro-Segmentation
- 각 시스템(서버) 단위로 세분화하여 각 워크로드를 독립적으로 보호
- 침입자의 시스템(서버) 간 횡적 이동 방지

PAM
- 최소 권한 원칙을 적용하여 접근 필요한 서버(Linux, Window, DB 등)에 대한 계정·권한을 통합하여 관리

취약점 관리 시스템
- 시스템(서버)의 취약점을 주기적으로 스캔하고 관리하여 보안성을 강화
- 보안 상태를 실시간으로 모니터링

백업 관리시스템
- 시스템의 주요 정보를 주기적으로 백업하고 복구 가능한 환경을 제공

제로트러스트 필러별 핵심 시스템

애플리케이션

기업망에서 실행되는 모든 애플리케이션과
관련된 API, 프로그램, 서비스 등

구현 내용

애플리케이션을 식별하고 워크로드 및 API를
모니터링하여 보안 상태를 강화

핵심 시스템

SASE
- 클라우드 기반으로 분산된 환경에서도 네트워크와 보안 정책을 일관되게 적용하여 워크로드를 보호

CASB
- 클라우드에 엑세스하는 환경에서 민감 데이터 보호, 사용자 활동 모니터링 등 다양한 보안기능을 제공

OSS 취약점 관리시스템
- 오픈소스 라이브러리와 구성 요소의 취약점을 식별하고 관리
- 사용 중인 오픈소스의 라이선스 준수 여부 확인 및 보안 패치 적용 지원

SAST
- 소스코드 단계에서 정적 분석을 통해 애플리케이션 취약점을 탐지하고 관리

DAST
- 실행 중인 애플리케이션 대상으로 동적 분석을 수행하여 취약점을 탐지하고 관리

데이터

민감정보, 비즈니스 정보, 고객 정보, 지적 재산 등
조직 내에서 보호해야 할 가장 중요한 리소스

구현 내용

데이터를 식별하고 분류하여 소유자, 중요도, 권한 등의
프로세스를 적용해 보안성을 향상

핵심 시스템

DSPM
- 조직 내 데이터를 식별하고 민감도에 따라 분류하여 관리
- 데이터의 가시성을 확보하여 일관된 보안정책을 적용

RBI
- 웹 브라우저를 격리하여 악성 웹 사이트로부터 데이터를 보호하고 격리된 환경에서 데이터를 전송

DLP
- 민감한 데이터를 식별하고 비인가 전송을 차단하여 데이터의 유출을 방지

DRM
- 디지털 콘텐츠와 파일에 대한 권한 관리 및 보호를 제공하여 무단 복제 및 유출을 방지

가시성 및 분석

제로트러스트 아키텍처 내 주요 필러들의 활동을
모니터링하고, 이를 기반으로 실시간 정보를 제공

구현 내용

주요 필러에서 발생하는 다양한 위협 정보를
수집하고 분석하여 실시간 가시성을 제공

핵심 시스템

SIEM
- 사용자, 네트워크, 애플리케이션 등에서 발생하는 방대한 로그 데이터를 수집하여 보안 위협 탐지 대응

BigData
- 대규모 데이터를 처리하고 분석하여 조직의 보안 태세 강화
- 머신 러닝, AI(인공지능)와 같은 기술을 활용하여 정상 활동, 비정상 활동을 구분하여 위협을 사전 탐지

통합로그
- 조직 내 다양한 리소스에서 생성 된 로그 데이터를 중앙에서 관리 및 분석

자동화 및 통합

제로트러스트 아키텍처에서 보안 운영의 효율성을
높이고 일괄된 정책 적용을 제공

구현 내용

기존 수동적으로 적용하던 보안 프로세스를 개선하여
자동화된 정책 기반 보안 프로세스를 적용

핵심 시스템

SOAR
- 다양한 보안 도구와 데이터를 연계하여 위협 탐지 및 자동화 대응
- 보안 운영을 효율화하고 일괄된 대응 절차를 구현

RPA
- 단순하고 반복적인 작업을 자동화 처리하여 효율성을 높이고, 인적 오류를 줄이며, 조직의 생산성을 강화

ML
- 대규모 데이터 패턴을 식별하고, 비정상적인 활동 탐지
- 시스템에서 수집된 데이터를 전달하고, 통합적으로 분석하여 위협 탐지 및 대응

AI
- 데이터를 학습하고 분석하여 운영 절차 자동화 및 최적화 관리
- 로그 분석, 위협 탐지 대응

○○ 기업 제로트러스트 모델 예시

제로트러스트 TO-BE 과제 모델

T01 제로트러스트 거버넌스 체계 구성	제로트러스트 협의체 구성	데이터 보호 및 개인정보 보호 방안 관리	제로트러스트 체계 인식 및 교육	제로트러스트 거버넌스 원칙 정의	의사 결정 프로세스
	규정 및 컴플라이언스	제로트러스트 기술 평가	제로트러스트 기술 도입 프로세스	지속적인 개선 프로세스	제로트러스트 성숙도 관리

제로트러스트 통합 모니터링 체계

T11 제로트러스트 환경 모니터링 체계 구축	전 영역 통합 모니터링	모든 트래픽 기록	**T08** 네트워크 흐름 풀패킷 분석 체계 구축	네트워크 가시성	네트워크 패킷 모니터링
	SIEM & SOAR	통합 위협 인텔리전스		TCP 트래픽 관리	DNS 트래픽 관리
	UEBA 기반 분석	빅데이터 분석		기타 트래픽 관리	네트워크 트래픽 분석
	자동화 동적 정책	가시성 확보		네트워크 패킷 분석	네트워크 가용성

+

사용자 & 디바이스

사용자 인증/위험정보

사용자 정보 수집	보안 컨텍스트 수집
MFA 인증	사용자 행동 분석
사용자디바이스검증	Risk Scoring

T06 UEM 도입을 통한 디바이스 관리

엔드포인트 통합관리	BYOD 관리
디바이스 상태 확인	디바이스 상태 평가
디바이스 데이터 관리	지속적인 확인 및 평가

내부 시스템

PDP (정책결정지점)

T09 신원기반 접근권한관리(ICAM) 도입

통합 인증	실시간 인증	실시간 인가
지속적 검증	인증 강화	신뢰도 정보

T12 통합계정권한 관리체계 일원화

계정관리 통합	접근권한 통합	접근권한 신청
Life-Cycle 관리	Work-flow 관리	계정 프로비저닝

T02 영역(필러)별 인벤토리 식별

인벤토리 식별	인벤토리 목록	인벤토리 그룹
식별항목 선정	관리 자동화	주기적인 최신화

PEP (정책시행지점)

T05 SDP 구축을 통한 사용자 인증 강화

논리적 경계 설정	엑세스 관리	보안 터널링
사용자 인증	SPA 패킷인증	최소 권한

T07 Micro-Segmentation 체계 구축

엑세스 제어	통신 제어	최소 권한

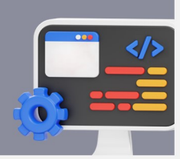
PDP (정책결정지점)

시스템 (서버)

T07 Micro-Segmentation 체계 구축

자산 식별	자산 관리		
라벨 기반 정책	동적 정책 부여		
측면이동 방지	호스트 기반 탐지		
디셉션 로직	가시성 강화		
시스템 인벤토리	**시스템 패치 관리**	**시스템 취약점 관리**	**시스템 로그 관리**

애플리케이션 & 워크로드



T04 개발영역 내 보안관리 절차 도입 및 확대

개발 프로세스 수립	App 소유자 관리		
DevSecOps	CI/CD		
오픈소스 관리	시큐어 코딩		
취약점 관리 및 조치	지속적인 위험분석		
애플리케이션 인벤토리	**SAST/DAST**	**SASE**	**CASB**

데이터

T03 데이터 관리방안 수립

데이터 통합 관리체계	데이터 시스템 통합		
데이터 유형 분류	데이터 관리 및 운영		
데이터 모니터링	컴플라이언스		
데이터 관리 기술	데이터 품질관리		
데이터 인벤토리	**데이터 권한 관리**	**데이터 접근 제어**	**데이터 암호화**

□□ 금융 제로트러스트 모델 예시

디바이스 및 엔드포인트 (Device/End-point)

사용자 인증 / 위험정보

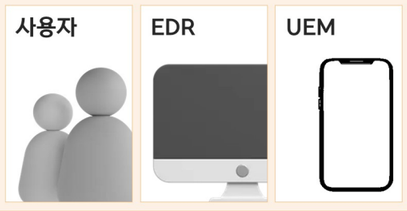
- 사용자 정보 수집(인사정보 등)
- 사용자 보안컨텍스트 수집
  (사용자 IP, 접근 시간, 접근 위치 등)

기기 인증 / 위험정보

- 디바이스 정보 수집 (식별자, MAC 등)
- 디바이스 보안 컨텍스트 수집
  (디바이스 취약점, 위험도, S/W 등)

접근주체(내부)

접근주체(외부)



엔드포인트 탐지 대응(EDR)

- 업무 디바이스(PC,VDI 등) 대상
- 실시간 위협탐지 및 대응체계 구현

통합 엔드포인트 관리(UEM)

- 기타 디바이스(태블릿,플린터 등) 대상
- 다양한 디바이스 통합관리 지원

사용자·신원 (User/Identity) / 네트워크 (Network)

정책결정지점(PDP)

사용자/디바이스 지속적인 식별 및 검증 위험 정보 판단

사용자 아이덴티티

Risk Scoring

디바이스 아이덴티티

지속적인 정책 감사

통합계정권한관리(IAM)

- 다양한 사용자 계정권한 통합관리
- RBAC/ABAC 기반 최소 권한
- 지속적인 사용자계정권한 검증

SDP Controller

- 내·외부 사용자 식별 및 관리
- 사용자 및 디바이스 정보 연동
- 보안 컨텍스트를 통한 동적정책 부여

지속적인 정책 검증 및 반영 ↔ 신뢰된 수준에 따라 접근 권한 적용

정책시행지점(PEP)

동적 접근제어 제공 및 이상 발생 시 추가 인증

실시간 세션 모니터링

다양한 인증 수단 연동

통합인증(SSO)

- 리스크 기반 접근통제
- 인증 세션에 대한 지속적인 검증
- 역할/신청 기반 통합인증(SSO)포탈

SDP Gateway

- 소프트웨어정의 경계 생성
- 허가 받은 자원에 대해서만 연결
- 세션별 보안 터널링 생성

시스템 (System) / 애플리케이션 (Application) / 데이터 (Data)

조직 리소스

시스템 (서버)

Micro-Segmentation

- 상세 세분화를 통한 횡적이동 차단
- 네트워크/시스템 상호작용 가시성 확보
- 시스템 별 개별 방화벽 체계를 통한 워크로드 수준의 트래픽을 관리

애플리케이션 & 워크로드

- 업무시스템별 계정권한 세분화
- 업무시스템 동적 권한 부여 체계
- CWPP, CSPM을 통한 클라우드 워크로드 보호

데이터

데이터 암호화
(정형 데이터, 비정형 데이터)

- 데이터 식별 및 중요 데이터 분류체계 구현

시각화 및 자동화 (Visibility/Automation)

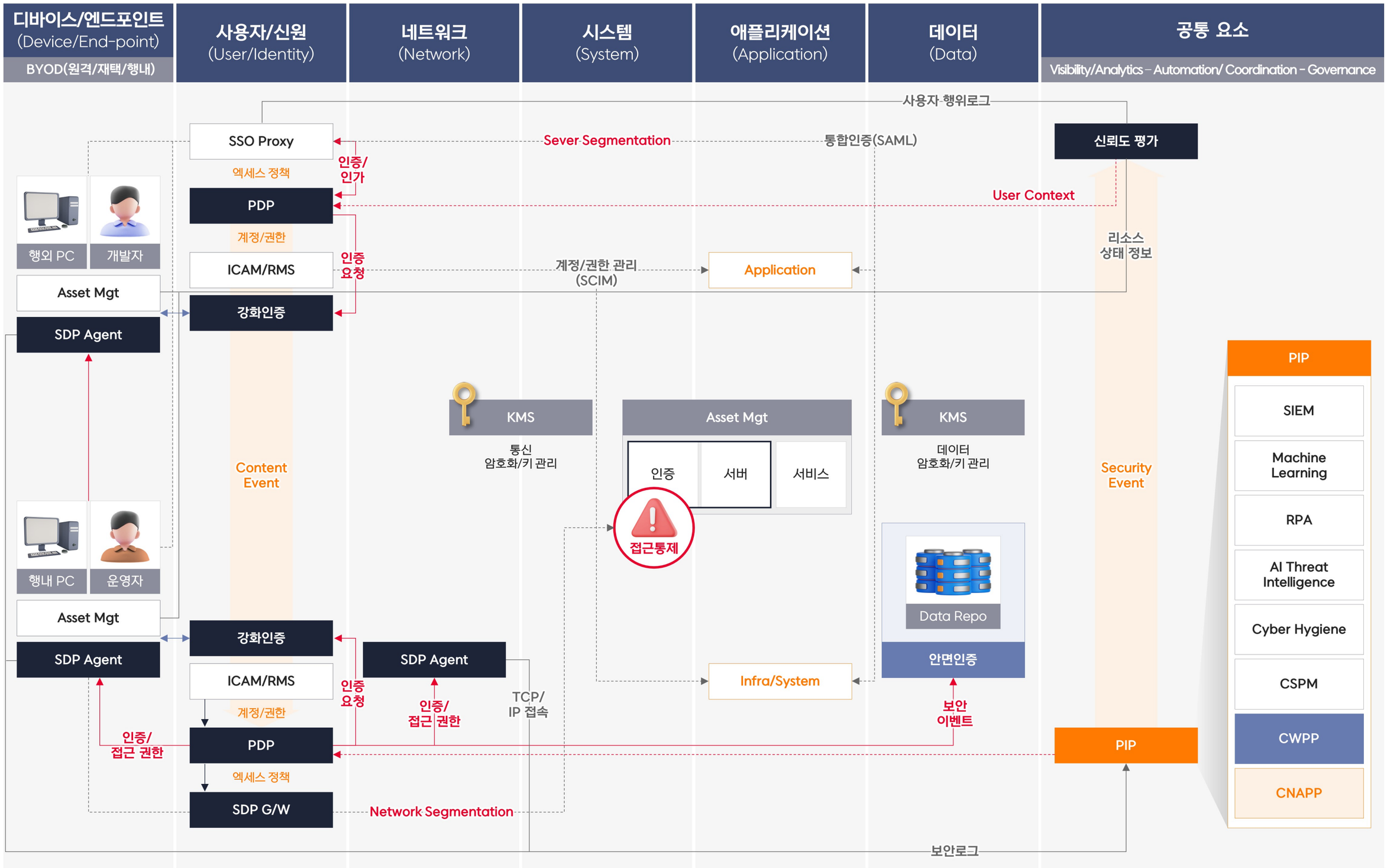
정책정보지점(PIP)

- SIEM
- SOAR
- 이상징후탐지
- EDR
- SDP
- Micro -Segmentation
- NDR
- 위협 인텔리전스

범 례

- 제로트러스트 주요 구성요소
- MP 구성요소

△△ 금융 제로트러스트 모델 예시



ZETIA

Zero Trust Initiative Alliance

제로트러스트 협의체

제티아(ZETIA)는 SK쉴더스가 제로트러스트 구현 활성화를 위해 국내·외 주요 보안 기업과 함께 2024년에 발족한 협의체 입니다
현재 대표 기업 10개사가 참여하고 있으며, 이후 참여기업은 더욱 확대 될 예정입니다

ZT 도입 컨설팅

- 제로트러스트 도입 성숙도 평가
  - 체크리스트 기반 성숙도 평가 수행
  - To-Be 모델 구성

ZT 고도화

- Next 성숙도 레벨 고도화 사전 준비
- 점진적 제로트러스트 범위 확대 요청 대응 (고객사)
- ZETIA 내 다양한 제품 간 연동을 통해 고도화 지원

ZT 구축

- Architecture 설계 및 제품 구축
- To-Be 모델 기반 관리적, 기술적 요건 적용
- ZETIA 내 고객사 특화 제품 선정
- 침투시험을 통한 ZT구축 검증 및 효과성 분석

ZEro Trust Initiative Alliance

ZETIA

ZT 관리

- ZT 운영을 통한 지속적 피드백 및 개선(고객사)
- 운영 환경에 따른 차별화 특성 수집(고객사)

ZT 운영

- 제로트러스트 운영 체계 수립
- 운영 및 관제 사업 수행
- 이상징후 분석에 대한 Security Model 제시 (SK쉴더스+참여벤더)