디지털 신뢰 새 패러다임,
제로트러스트 적용 전략 콘퍼런스

"Go Ahead! Zero-Trust"

SKZT (SK쉴더스 제로트러스트)
도입방법론 및 수행사례 소개

SK 쉴더스

~ 2024

준비기

Ready for Zero-Trust

2025 ~

도입기

Go Ahead! Zero-Trust

SK shieldus

SKZT(SK쉴더스 제로트러스트)
도입 방법론 및 수행사례 소개

Ⅰ

제로트러스트 모델
전환 필요성

SK 쉴더스

01 비즈니스 환경 변화

비대면·디지털 전환 확산

코로나 19로 인한 '사회적 거리두기'
→ 디지털 전환 가속화

'언제 어디서든, 누구에게나'
사이버 위협이 가능한 상황에 직면

안전지대(경계) 밖 자산(원격, 모바일, 클라우드) 위협 가중
→ 보안관리 대상 양적 증가

新환경, 新보안위협

전통산업 영역에서 디지털 영향력 확대
→ 보안 필요성 증대

과거에는 예상하지 못했던
다양하고 복잡한 사이버위협 등장

지능화 기술 확산으로
사이버공격 은밀화 · 고도화

AI 활용 확대

ChatGPT 같은 대규모 언어모델 기관도입 확대
→ 프롬프트 주입, 추출을 통한 데이터 유출,
대규모 언어 모델 오염 등 새로운 위협

빅데이터와 AI를 활용한
새로운 형태의 사이버 위협 발생

주요국은 AI 위협에 따른
국가차원 전략 마련 중

정보보안 영역에서도 패러다임 Paradigm shift 의 대전환 필요성 발생!

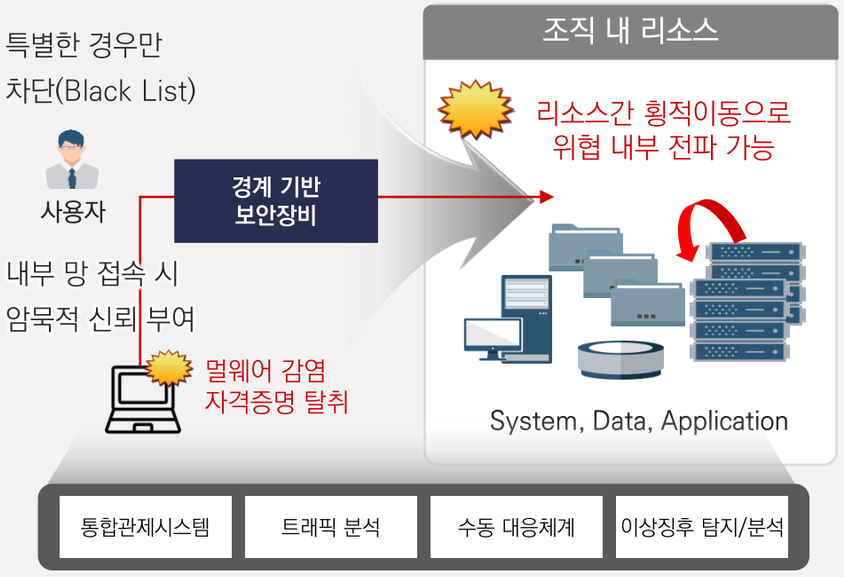
SK 쉴더스

02 제로트러스트 모델로의 전환 필요성

기존 경계 보안 모델 이슈 지속 발생

제로트러스트 전환 전

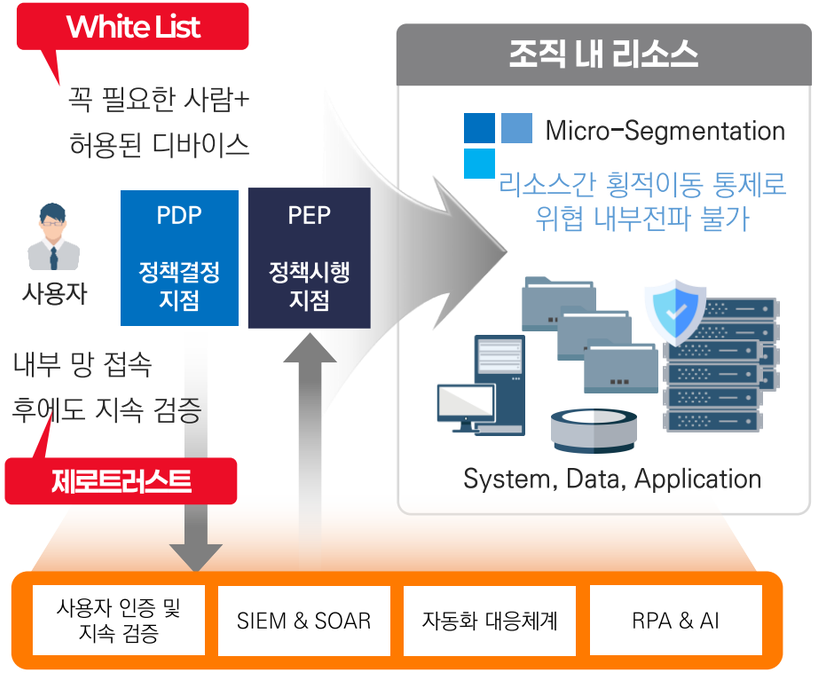
기업 망 단위 보안 경계



신규 제로트러스트 모델 전환 NEED 증대

제로트러스트 전환 후

리소스 단위 소프트웨어 정의 보안 경계 설정



1 변화하는 IT환경 대응 가능

- BYOD(개인 소유 디바이스) 활용
- 클라우드, 재택 등에서도 일관된 보안정책 적용 가능

2 사용자 및 디바이스 인증

- 네트워크와 무관하게 모든 액세스 요청에 대해 사용자 인증 및 디바이스 인증 강제화
- 이미 인증된 사용자 및 디바이스 상황 변화 또는 이상징후 등 포착 시 지속적인 재 검증

3 지속적인 검증

- 감사 로그 수집 및 분석 자동화
- 이상징후 탐지 및 차단 정책 활성화
- 동적 정책을 통한 자동화 대응체계

SK 쉴더스

03 국외 제로트러스트 도입 현황('24년)

국외 현황

제로트러스트 글로벌 동향 (~'25)

STAMFORD. Conn., April 22, 2024

Gartner Survey Reveals 63% of Organizations Worldwide Have plemented a Zero-Trust Strategy

Gartner 2024.04

"전 세계 조직의 63%가 제로트러스트 전략 도입"

NEWS PROVIDED BY StrongDM → Jan 29, 2025, 08:47 ET

Zero Trust Adoption Soars to 81%, but Fragmented Tools and Multi-Cloud Hurdles Remain, New Survey by StrongDM Finds

strongdm 2025.01

"전 세계 조직의 81%가 클라우드 환경에서 제로트러스트 보안 모델을 채택"

도입 사례

글로벌 기업의 제로트러스트 도입사례 (~'24)

Google

솔루션: BeyondCorp Enterprise

BeyondCorp Enterprise

도입사

Google wayfair 외 다수

도입 효과

- 사용자 인·검증을 통한 권한 부여로 내부위협 최소화
- 신뢰기기 기반 네트워크 접속을 통한 접근 원천차단
- 중앙관리 보안정책을 통한 접근 요제어 및 모니터링
- 이용자의 장소, 시간 구분없는 업무수행으로 사용자 경험 개선

MicroSoft

솔루션: Microsoft Security

MS Security
(Entra, Intune, SecOps 등)

도입사

외 다수

도입 효과

- 여러 계열 법인의 단일 테넌트 애플리케이션 사용 가능
- 다중 클라우드, 하이브리드 환경, 워크로드의 일관된 보안정책
- 제로트러스트 도입을 통한 시간장소의 구애 없는 액세스
- 게스트 사용자관리 및 공용 리소스 테넌트 이동 개선

Paloalto

솔루션: PRISMA ACCESS

NGFW, Prisma(SASE) 등

도입사

IMF THE WORLD BANK 외 다수

도입 효과

- 네트워크 트래픽을 어플리케이션 영역까지 제어해 보안을 강화
- 사용자와 디바이스를 지속적으로 검증하며, 최소권한 기반 접근
- 분산된 접속경로를 일원화하고 일관된 제로트러스트 정책 부여
- AI를 통해 실시간 위협 탐지 및 자동화 대응 기능 제공

주요 글로벌 벤더

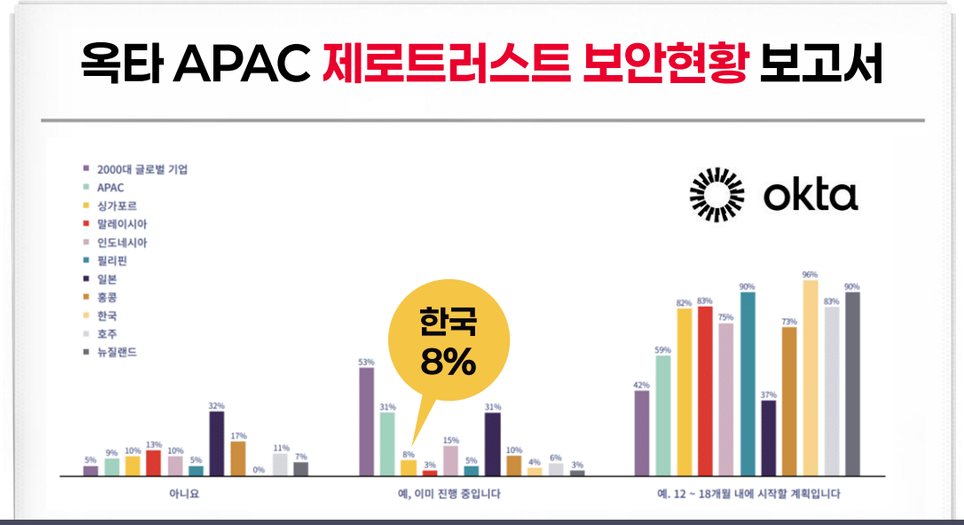
"제로트러스트 아키텍처 구현을 위해, 다양한 솔루션을 출시하고 벤더사 간 협업을 진행 중"

SK 쉴더스

04 국내 제로트러스트 도입 현황('24년)

국내 현황

옥타 APAC 보고서



"제로트러스트 보안을 진행중인 한국기업은 8%에 불과"
해외시장 대비 한국 시장도 발 빠른 대응이 필요

정부 주도 확산

- 정보체계 등에 대한 접속 요구 시 끊임없이 검증하여 접속을 제어하는 철통인증(K-제로트러스트)를 도입 확산 중
- 정부주도 민간기업 포함 공공, 금융기관 대상 보안모델을 개발, 실증함하여 최적화된 K-제로트러스트 도입가이드 및 레퍼런스를 제공

도입 사례

K-제로트러스트 보안모델 공공·금융서비스 도입 및 구현('24)

구분	연합체 (수요기관)	주요특징
공공분야 (1개)	SGA솔루션즈 컨소시엄 (국가정보자원관리원 외)	정부/공공기관 통합 전산센터 대상 철통인증(제로트러스트) 적용
민간분야 (3개)	지니언스 연합체 (야놀자, 에스트래픽)	해외지사 등 원격접속이 잦은 환경에서 철통 인증(제로트러스트)구현
	앰진 연합체 (이브이시스, SKB등 6개사)	일반 사무환경이 아닌 외부 고객/특수단말 접속이 많은 환경에 적용
	엠시큐어 연합체	금융분야 인터넷 기반 자원공유(클라우드)업무환경에 철통인증(제로트러스트)보안 구현

SGA 솔루션즈

국가정보자원관리원 · 공무원연금공단 외 다수

도입 효과

- KISA 주관 제로트러스트 보안모델 실증 사업
- 안전한 게임개발 인프라 환경 구축 및 내부데이터 보호
- 사용자별 리소스 접근통제 세분화를 통한 연동개선
- 제로트러스트 환경구축을 통해 보안성 41%개선

지니언스

yanolja · STraffic 외 다수

도입 효과

- 기존 VPN한계 극복일 위한 보안성 및 확장성 개선
- 제로트러스트 도입을 통한 빠른 디지털전환
- 네트워크 어플리케이션 워크로드에 대한 접근제어 개선
- 온프레미스, 클라우드등 다양한 인프라 환경의 일관된 보안정책

소프트캠프

SAMSUNG 삼성전기 · 하나손해보험 · KB증권 외 다수

도입 효과

- 브라우저 격리기술(RBI)를 통한 외부사용자들의 업무환경 개선
- 다양한 개인 기기를 업무환경에 사용할 수 있는 (BYOD)지원
- 사용자 권한 기반 접근통제로 제공서비스의 강력한 보안 제공
- 외부유입파일에 대한 무해화 (CDR) 제공으로 위협 감소

한국은 기존 시스템의 대체 및 고도화로 제로트러스트 도입 중
국내 벤더사도 꾸준한 기술개발 및 협업을 통해 대응 중

SK 쉴더스

05 제로트러스트 가이드라인 변화

주요 내용	가이드라인 V1.0 (2023.06)	가이드라인 V2.0 (2024.12)
제로트러스트 성숙도 모델	• 3단계 성숙도 수준 정의 • 기업망 핵심 요소별 20가지 기능 정의 (교차 기능 제외)	• '초기' 단계를 추가한 4단계 성숙도 수준 정의 • 기업망 핵심 요소별 27가지 정의 (교차 기능 제외) 및 단계별 특징 구체화 • 기업망 핵심 요소 및 2가지 교차 기능에 대한 52가지 보안 세부역량 및 각 세부역량의 성숙도 수준별 특징 정의 • 성숙도 모델에 기반한 구현 방안 제시
제로트러스트 도입 절차	• 제로트러스트 아키텍처 도입 고려사항 정리 (성숙도 모델 관점 및 기업 내외부 환경 관점) • 총 5단계의 제로트러스트 아키텍처 도입 단계 제시 (준비 → 계획 → 구현 → 운영 → 피드백 및 개선)	• 제로트러스트 아키텍처 도입 과정에서의 고려사항 구체화 (제로트러스트에 대한 명확한 이해 및 기업 내 인식 제고 등 추가) • 제로트러스트 도입 준비 단계 구체화 및 침투시험 추가 (업무 구체적 기술 및 예시 제시) • 제로트러스트 아키텍처 도입을 위한 조직 내 역할 및 목표 설정 방안 제시
기타	• 제로트러스트 구현에 대한 6가지 유스케이스 및 목표·요구사항, 구현 방안 등 제시 • 제로트러스트 도입 후 보안 수준 평가 방안 없음	• 제로트러스트 도입 후 기업망 보안 수준을 평가할 수 있는 2가지 방안 제시 (성숙도 기반 도입 수준 분석을 위한 체크리스트, 침투시험 기반 제로트러스트 효과성 분석 방안) • 부록에서 2023년도 제로트러스트 실증 사례 소개

SK 쉴더스

06 국내 제로트러스트 주요 이정표('24년)

MLS 참조모델 분과 TF 개설

제로트러스트와 연관된 다층 보안체계(MLS) 참조모델 관련 4개 분과 개설

제로트러스트 도입 시범사업

총 4개 컨소시엄이 업무망 환경에서 제로트러스트 모델을 실제 적용하고 운영, 과기정통부/KISA 주관 하에 총 예산 약 45억 원 규모로 지원

국가 망 보안체계(N²SF) 보안 가이드라인 발표

기존 다층보안체계(MLS)에서 발전된 형태로, 망 분리 정책을 대체하기 위한 보안가이드라인 발표

2023 12월 | 2024 1월 | 2월 | 3월 | 4월 | 5월 | 6월 | 7월 | 8월 | 9월 | 10월 | 11월 | 12월 | 2025 1월

제로트러스트실증사업 성과 공유회

23년도 실증사업 결과를 공유하고 중요 성과와 사례 발표를 통해서 제로트러스트 도입 가능성을 검토

한국은행 제로트러스트 기반 망 개선 실증 및 컨설팅 사업

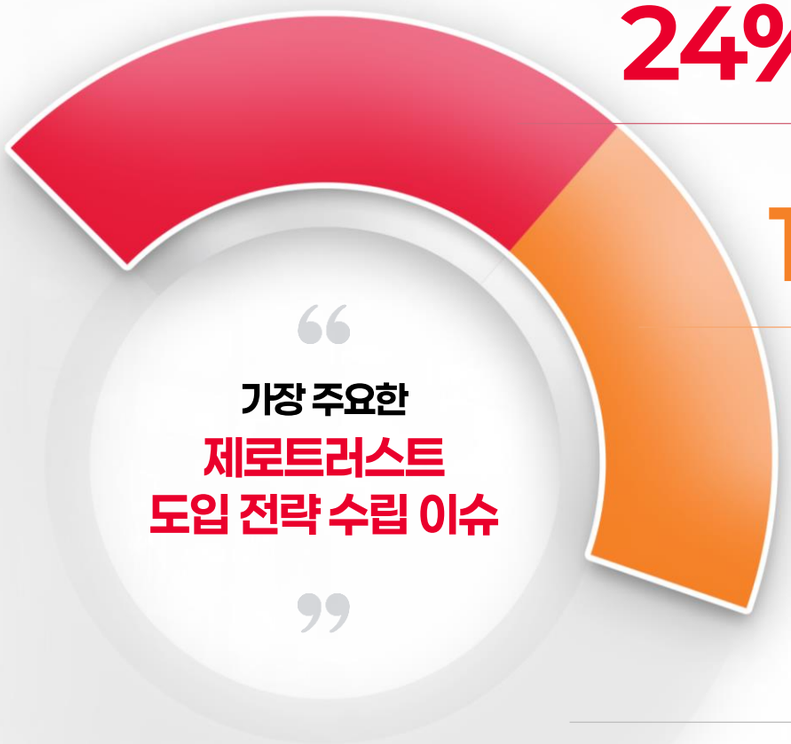
한국은행이 금융권 망 개선 작업의 첫 사례로, 약 26억 원 규모의 망 개선 프로젝트를 진행

제로트러스트 가이드라인 V2.0 발표

글로벌 표준 및 국내 실증사업과 시범사업 결과를 반영하여 구체적인 실행 사례가 포함된 가이드라인 발표

SK 쉴더스

07 제로트러스트 도입 방법론 필요성



"가장 주요한 **제로트러스트 도입 전략 수립 이슈**"

24% 완벽한 제로트러스트 솔루션을 갖춘 적격한 벤더 부족!

19% 즉각적인 IT 보안 환경을 변경하기 위한 예산 부족!

Others

- ✓ 제로트러스트 전략 구현 방법 연구 중 (13%)
- ✓ 중앙 네트워크 보안 전략 없음 (11%)
- ✓ 제로트러스트 솔루션 선택에 대한 정보 부족 (10%)
- ✓ 여전히 기존 VPN에 의존 (10%)
- ✓ 인력, 자원 (7%)
- ✓ IT 부서 전체 조직 저항 (7%)

※ 출처 : Fortinet

83%의 조직들은 제로트러스트 구현에 어려움을 겪고 있음!

제로트러스트 전환을 위한 방법론 부재로 인해 도입 전략 수립이 어려운 상태!

Ⅱ

SKZT
도입 방법론 소개

SK 쉴더스

01 제로트러스트 도입 방법론 필요성

국내·외 가이드라인을 기반으로 하여 국내 1위 정보보안전문 기업 SK쉴더스는 국내 환경에 적합한 제로트러스트 도입 방법론을 개발 하였습니다.

국내 · 외 가이드라인

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

SK 쉴더스

SKZT

SK쉴더스 제로트러스트 도입 방법론

- 성숙도 평가
- 환경 구축
- 운영 관리

SK쉴더스의 노하우

Capability

SK쉴더스 사업 수행 방법론

- 보안컨설팅 방법론(SKPE-ISCM), 인프라 구축 방법론(SKPE-Infra), 운영관리 방법론(SKPE-OTM) 등 SK쉴더스의 다년간 검증된 방법론 개발 경험 바탕의 제로트러스트 도입 방법론 개발

Knowledge

SK그룹 보안 가이드

- SK그룹의 자체적인 보안 가이드를 참고하여 제로트러스트 핵심 요소별 인벤토리 관리, 취약점진단 및 관리, 패치배포 및 관리 등 세부적인 보안정책 및 관리방안을 포함한 방법론 개발

Experience

다양한 프로젝트 수행 경험

- 기업, 금융권, 공공기관 등 다양한 규모와 산업 분야에서 성공적으로 프로젝트를 수행한 경험(컨설팅, 구축, 운영)을 바탕으로 제로트러스트 도입 방법론 구성

SK 쉴더스

02 SK쉴더스 방법론(SKZT) 요약

SK쉴더스는 고객사의 체계적인 제로트러스트 환경 구성을 위해 자체적인 제로트러스트 도입 방법론(SKZT)을 다음과 같이 정의 하였습니다.

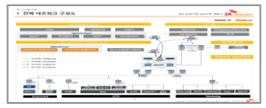
SKZT 성숙도 평가

제로트러스트
도입 수준 진단

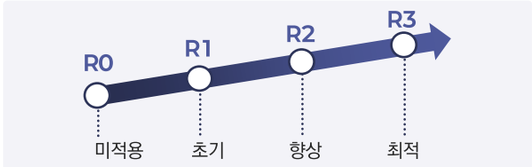
- 8가지 핵심요소 별 성숙도 수준 진단
- SK쉴더스 자체 설계 체크리스트 활용
- 스코어링을 통한 성숙도 수준(R0~R3) 평가

사용자 · 신원	디바이스 · 엔드포인트
네트워크	시스템
응용 · 워크로드	데이터
가시성 및 분석 능력	자동화 및 통합

체크리스트 평가



TO-BE 모델 도출



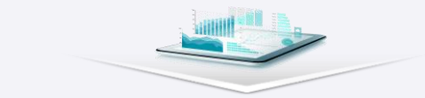
성숙도 수준 평가

SKZT 환경 구축

제로트러스트
환경 구축

- 도출된 To-Be 모델 기반 ZT 환경 구축 수행
- 제로트러스트 Alliance 를 통한 고객사에 특화된 솔루션 제공

기존 환경 내 TO-BE 모델 기반 ZT 환경 구현



User | Device | Network | System | App

관리적·기술적 개선내역 기반

제로트러스트 Architecture 기반 솔루션 적용

고객사 내 특화된 제로트러스트 솔루션 제공

SKZT 운영 관리

제로트러스트
운영 체계 수립

- 제로트러스트 운영에 필요한 모니터링 체계
- 비정상 행위 탐지 및 정밀 차단 수행
- 모든 위협 관찰 및 자동화 방어체계 적용

가시성 및 분석

모든 위협을 관찰하고, 자동화된 통합 보안 대응

비정상 행위 탐지 개선	동적 정책으로변경 (보안정책, 세션제어)
패킷 단위 이상 트래픽 분석	지능화된 방어기법 적용

자동화 및 통합

빅데이터 분석	대응 자동화
실시간 검색 및 상관분석	사고대응 표준화/간소화
이상행위 탐지/위협분석	정책 및 프로세스 자동화
데이터 수집/저장/분석	연관 장비 간 자동화

SKZT 고도화 및 개선

제로트러스트
영역 점진적 확대

- 운영 관리를 통한 지속적인 피드백 및 개선
- 점진적인 성숙도 레벨 고도화 준비
- 제로트러스트 범위 확대 진행

시범운영에 이은 정상운영 관리
운영 관리를 통한 지속적 피드백 및 개선 01

고객사 사이트 특성 고려
운영 환경에 따른 제로트러스트 환경 차별화 02

점진적인 제로트러스트 확대를 위한
Next 성숙도 레벨 진입 준비 03

SK 쉴더스

02 SKZT – 1단계 · 성숙도 평가

성숙도 평가를 통해 고객사 내 다양한 리소스를 6개의 핵심 요소와 3가지의 공통 요소로 구분하고, 각 항목 별 자체 설계한 체크리스트를 활용하여 고객사의 성숙도 수준을 진단합니다. 해당 성숙도 평가의 결과로써 제로트러스트를 구현할 수 있는 범위와 구현방안을 수립합니다.

6개의 핵심 요소 (Pillar)

사용자 · 신원

사람, 서비스 혹은 IoT 기기 등의 고유하게 설명할 수 있는 속성 혹은 속성의 집합

시스템

중요 응용 프로그램을 구동하거나 중요 데이터를 저장하고 관리하는 서버를 포함하며, 온프레미스 및 클라우드 구축 운용 중인 모든 서버 시스템

디바이스 · 엔드포인트

네트워크에 연결하여 데이터를 주고 받는 모든 하드웨어 장치

응용 · 워크로드

기업망 관리 시스템, 프로그램, 온프레미스 및 클라우드 환경에서 실행되는 모든 서비스와 인터페이스

네트워크

기업망의 유무선 네트워크, 클라우드 접속을 포함하며 인터넷 등 데이터를 전송하기 위해 사용되는 모든 형태의 통신 매체

데이터

기업 혹은 기관에서 가장 최우선적으로 보호해야 할 리소스

3개의 공통 요소 (Cross Pillar)

가시성 및 분석 능력

사용자 혹은 디바이스, 응용 및 워크로드의 상태 등을 확인하고 세부정보를 분석하여 가시성을 제공

자동화 및 오케스트레이션

기존 보안 프로세스를 개선하여 자동화된 정책 기반 보안 프로세스 및 통합 보안 대응을 제공

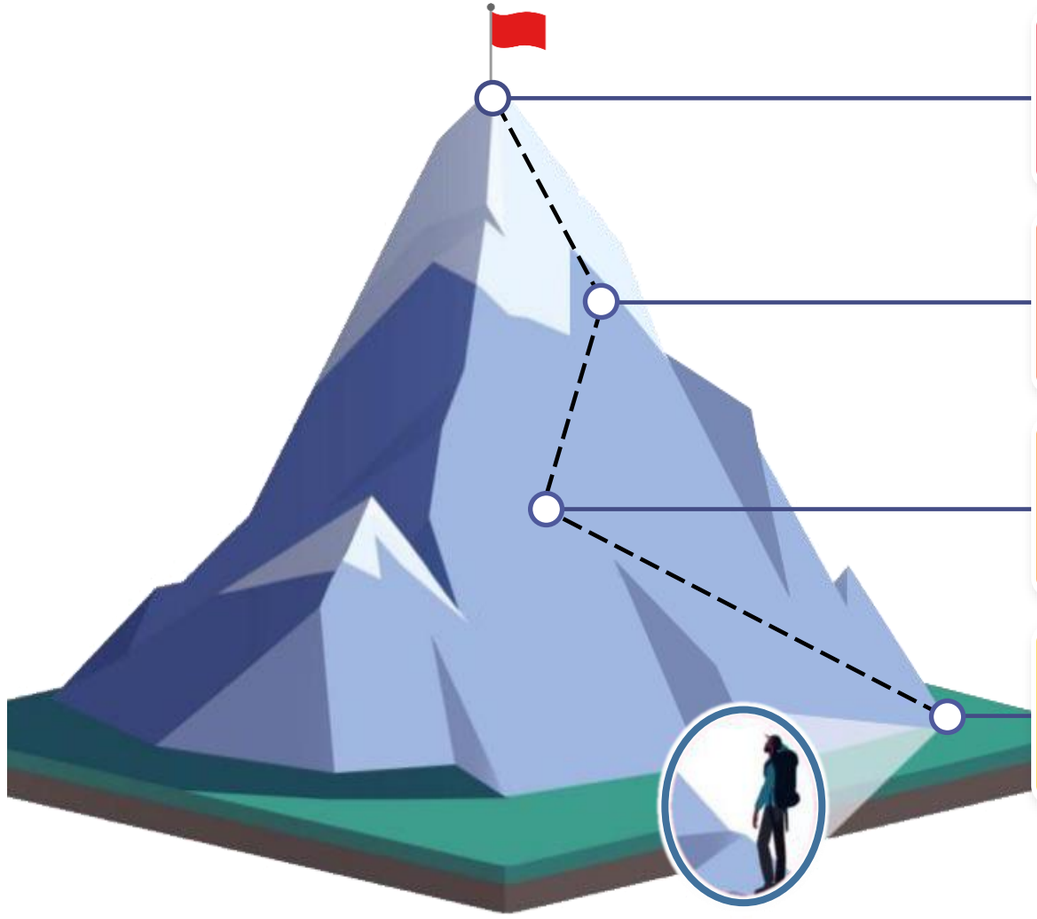
거버넌스 역량

거버넌스 관점에서 조직의 보안 정책 및 규정 준수를 보장하고 제로트러스트 환경 구현을 위한 방향성을 제공

SK 쉴더스

02 SKZT – 1단계 · 성숙도 평가

성숙도 평가는 조직의 제로트러스트 구현 수준을 객관적으로 측정하고 개선 방향을 제시하기 위한 평가 체계입니다.
구현 수준은 R0 단계부터 R3 단계까지 총 4단계로 구성되며, 각 단계별로 요구되는 보안 수준과 기능을 정의합니다.



R3 (최적)
- 제로트러스트 원칙이 전사적으로 적용되어 보안 운영체제가 자동화되고 행위 기반 탐지를 통해 세분화된 동적 정책 이 부여되고 있음
- 관련 기술: ICAM, AI, RPA, UEM, UEBA 등

R2 (향상)
- 제로트러스트 원칙이 도입되어 자동화된 보안 정책 시행 및 핵심 요소 간 통합을 통해 일부 구간 제로트러스트 환경이 구현되어 있음
- 관련 기술: SDP, Micro-Segmentation, IAM 등

R1 (초기)
- 제로트러스트 원칙을 부분적으로 도입하여, 사용자 및 디바이스 인증을 강화하고 접근제어 및 네트워크를 세분화하여 관리하고 있음
- 관련 기술: RBAC, MFA, EDR, SDN 등

R0 (미적용)
- 기존의 경계 기반 보안 모델을 유지하며 방화벽, IPS, 백신 등 기본적인 수준의 정보보안 체계가 구현되어 있음
- 관련 기술: 방화벽, IPS, VPN, NAC, 백신 등

※ R : Realization 의 약자

SK 쉴더스

02 SKZT – 1단계 · 성숙도 평가

성숙도 평가 체크리스트는 9개의 핵심 요소(Core Pillars)와 68개의 핵심 기능을 포함한 전체 192개 항목으로 구성되어 있습니다.
각 항목에 대해서 세부적으로 조직의 현재 성숙도 수준을 평가(R0~R3) 하고 다음 단계로 나아갈 수 있는 방향성을 제공합니다.

SK쉴더스 방법론
SKZT
1 SKZT 성숙도 평가
2 SKZT 환경 구축
3 SKZT 운영 관리

핵심 요소 (CORE PILLARS)

핵심 기능(CORE CAPABILITES)

1. 사용자 및 신원	2. 디바이스 및 엔드 포인트	3. 네트워크	4. 시스템	5. 애플리케이션 및 워크로드	6. 데이터	7. 가시성 및 분석	8. 자동화 및 통합	9. 거버넌스 역량
1.1 사용자 인벤토리	2.1 디바이스 인벤토리	3.1 네트워크 인벤토리	4.1 시스템 인벤토리	5.1 애플리케이션 인벤토리	6.1 데이터 인벤토리	7.1 통합로그관리	8.1 자동화 (Automation)	9.1 협의체 구성
1.2 사용자 계정 관리	2.2 디바이스 인증	3.2 네트워크 흐름 분석	4.2 시스템 계정 관리	5.2 애플리케이션 위험 관리	6.2 데이터 권한 관리	7.2 분석 및 대응	8.2 인공지능(AI)	9.2 데이터 보호 및 개인정보 보호
1.3 사용자 패스워드 관리	2.3 BYOD 관리	3.3 네트워크 트래픽 암호화	4.3 시스템 접근 통제	5.3 애플리케이션 접근 관리	6.3 데이터 접근 제어		8.3 오케스트레이션 (Orchestration)	9.3 보안 인식 및 교육
1.4 사용자 권한 관리	2.4 디바이스 취약점 관리	3.4 네트워크 액세스 관리	4.4 시스템 보안	5.4 애플리케이션 보안 테스트	6.4 데이터 암호화			9.4 의사 결정 프로세스
1.5 사용자 증명	2.5 디바이스 패치 관리	3.5 소프트웨어 정의 경계 (SDN/SDP)	4.5 시스템 분리	5.5 리소스 승인 및 통합	6.5 데이터 카탈로그 위험평가			9.5 규정 및 컴플라이언스
1.6 통합 ICAM 플랫폼	2.6 디바이스 위험 관리	3.6 네트워크분할 (Segmentation)	4.6 시스템 정책 관리	5.6 소프트웨어 개발&통합	6.6 데이터 모니터링 및 분석			9.6 기술 및 도구 평가/ 도입
1.7 사용자 위험평가	2.7 통합 엔드 포인트 관리 (UEM)	3.7 네트워크 유연성	4.7 시스템 패치 관리	5.7 CI/CD	6.7 정책 및 프로세스			9.7 지속적인 개선 및 성숙도 관리
	2.8 엔드 포인트 및 확장된 탐지 및 대응(EDR)	3.8 네트워크 모니터링 및 분석	4.8 시스템 로그 관리	5.8 클라우드 워크로드 보호				
	2.9 정책 및 프로세스	3.9 네트워크 리소스 관리	4.9 시스템 취약점 관리	5.9 SaaS 관리 플랫폼 (SMP)				
		3.10 정책 및 프로세스	4.10 시스템 가시성 및 분석	5.10 보안 액세스 서비스 엣지 (SASE)				
			4.11 정책 및 프로세스	5.11 클라우드 엑세스 보안 브로커 (CASB)				
				5.12 정책 및 프로세스				

표 구분	내용
핵심 요소(대분류)	9개
핵심 기능(중분류)	총 68개 (소분류 총 : 192개) • 사용자 및 신원 : 7(17) • 디바이스 및 엔드 포인트 : 9(25) • 네트워크 : 10(30) • 시스템 : 11(36) • 애플리케이션 및 워크로드 : 12 (40) • 데이터: 7(25) • 가시성 및 분석: 2(5) • 자동화 및 통합: 3(7) • 거버넌스 역량: 7(7)

SK 쉴더스

02 SKZT – 1단계 · 성숙도 평가

성숙도 평가는 체크리스트를 통한 점검 수행이 기본이며, 환경분석 및 현황파악 → 성숙도평가 수행 → To-Be 모델 수립 순으로 진행됩니다.
해당 평가작업의 결과로써 전체 항목에 대한 평가 결과서 및 상세 개선사항이 포함된 마스터플랜 내역이 제공됩니다.

SK쉴더스 방법론
SKZT

1 SKZT 성숙도 평가
2 SKZT 환경 구축
3 SKZT 운영 관리

환경분석 및 현황파악

환경 및 요구사항 분석

조직/업무/IT환경/자산 분석

수행계획서 작성

Task 일정 수립

성숙도 평가 기준 수립
성숙도 평가 대상 선정

SKZT 성숙도 평가 체크리스트 배포

성숙도 평가 수행

성숙도 평가 수행 활동

[성숙도 평가]

- 성숙도 평가 대상 리소스 식별 (사용자, 디바이스, 시스템 등)
- 성숙도 평가 체크리스트 적용 Case 선별
- Case 별 성숙도 평가 체크리스트 적용

[성숙도 평가 결과 도출]

- 체크리스트 기반 1차 성숙도 평가 결과 도출
- 담당자 공유 및 인터뷰 진행
- 2차 성숙도 평가 진행
- 최종 성숙도 평가 결과 도출

To-Be 모델 수립

To-B 모델 및 개선과제 도출

성숙도 평가 최종 결과 도출

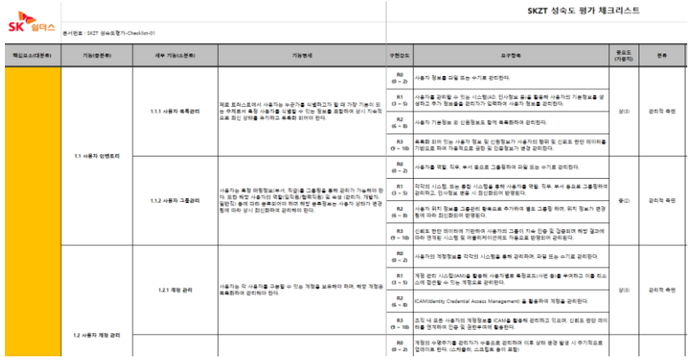
담당자 배포

성숙도 평가 결과서 작성 (TO-BE 모델 포함)

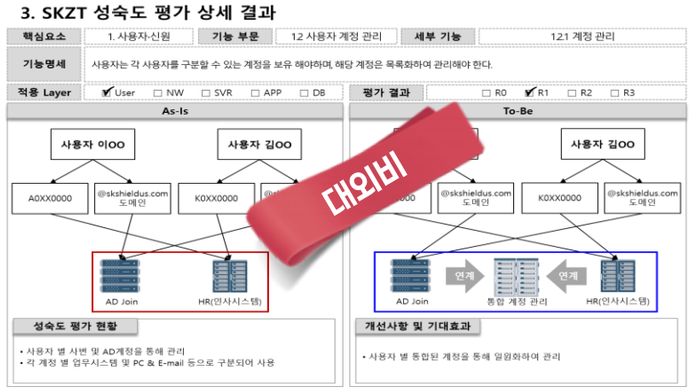
SKZT 마스터플랜 작성 (개선과제 포함)

담당자 검토 및 성숙도 평가 결과 확인

성숙도 평가 체크리스트 예시


SKZT 성숙도 평가 체크리스트

SKZT 성숙도 평가 결과서 예시



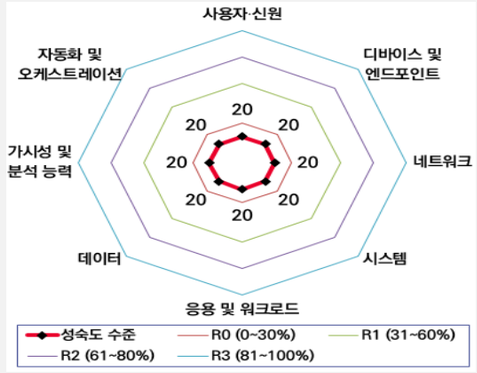
SK 쉴더스

02 SKZT – 1단계 · 성숙도 평가

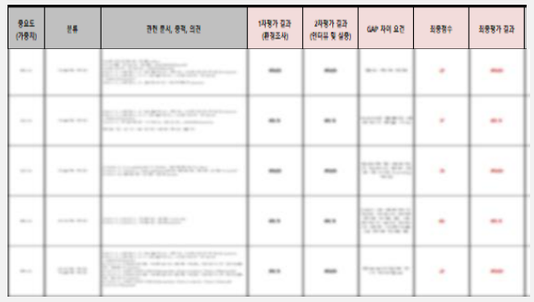
체크리스트를 기반으로 도출된 제로트러스트 성숙도 평가 결과를 분석하여 조직에 필요한 관리적 항목과 기술적 항목으로 구성된 개선과제를 도출합니다.
개선과제를 수행하기 위한 세부적인 계획과 방안이 포함된 마스터플랜을 제공하여 제로트러스트 환경을 구축하기 위한 토대를 마련합니다.

성숙도 평가 결과 분석

성숙도 평가 결과



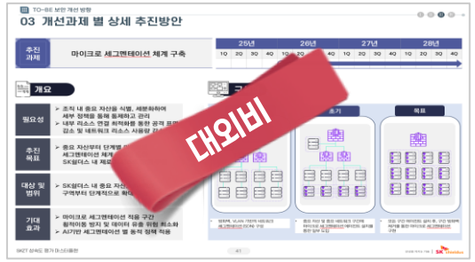
체크리스트 평가 결과



SKZT 마스터플랜 작성

성숙도 평가 결과에 따른 산출물 제공

개선과제 별 상세 추진방안



단계별 개선과제 도입 및 구축 계획

SKZT 성숙도평가 Toolkit

- 현황분석
- SKZT 체크리스트
- As-Is 환경 분석
- To-Be 모델
- 결과보고서
- 마스터플랜

"중·장기 마스터플랜 수립"

개선과제 도입 및 구축 계획

관리적 항목	기술적 항목
• 제로트러스트 전략 및 정책 등을 포함한 협의체 구성 • 기존 환경을 활용하여 관리 영역 확대 방안 • 사용중인 시스템을 활용하여 제로트러스트 관련 항목들 관리 방안	• 제로트러스트 환경 구성을 위한 기존 시스템 통합 구성 등 기술적 방안 제공 • 신규 기술, 시스템 도입을 통한 제로트러스트 환경 전환 • 신규 시스템 도입을 위한 주요 벤더사, 제조사 정보 제공 • 제로트러스트 환경 적용을 위한 기술적 방안 소요 예산 측정

SK 쉴더스

02 SKZT – 2단계 · 환경 구축

성숙도 평가가 완료되면, 도출된 마스터플랜에 기반하여 개선과제에 따라 제로트러스트 환경 구축을 진행합니다.
구축 방법은 가장 기초적인 제로트러스트 아키텍처 기반 사용자 인증 망 설계 구현 방법과 신규 시스템 구축 기반의 제로트러스트 구현 방법으로 구분됩니다.

SK쉴더스 방법론
SKZT

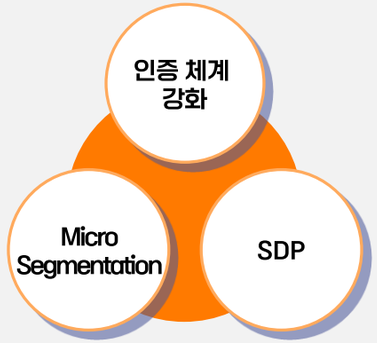
1 SKZT 성숙도 평가

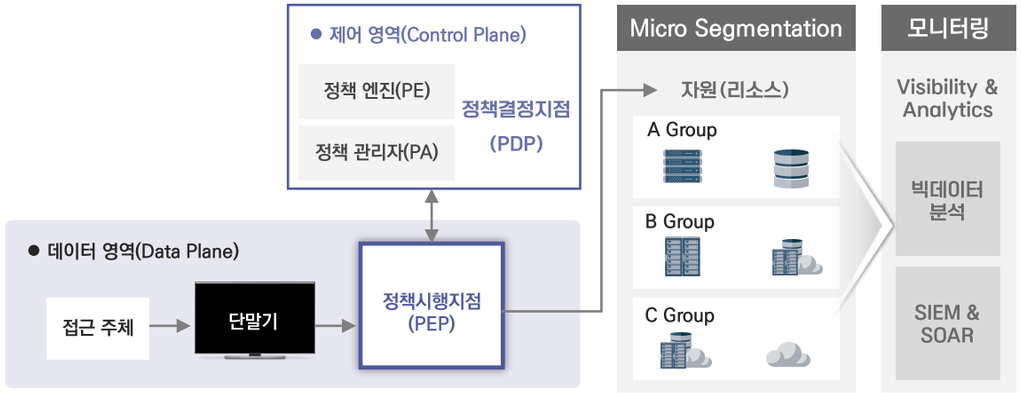
2 SKZT 환경 구축

3 SKZT 운영 관리

제로트러스트 아키텍처 기반 환경 구축

- 사용자, 기기에 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 상태에 대한 모니터링 및 로그수집 이를 통한 신뢰성 지속적 검증, 제어





신규 시스템 구축 기반 제로트러스트 구현

권장 시스템

- 사용자 인증
- SDP
- Micro-Segmentation

환경 별 구축 고려요소

- A.I , DT
- 클라우드
- 데이터 추적
- 이상징후 분석
- RBI
- EDR

SK 쉴더스

02 SKZT – 2단계 · 환경 구축

차세대 보안체계인 제로트러스트는 사용자 인증, 디바이스, 네트워크 접근통제, 데이터 등급 통제와 위협대응으로 구성되어 있습니다.
각 항목은 국가정보보안기본지침 및 제로트러스트 가이드라인 2.0, 국가망보안체계보안가이드라인을 기반하여 구성되어 있습니다.

국가정보보안 기본지침

제로트러스트 가이드라인 2.0

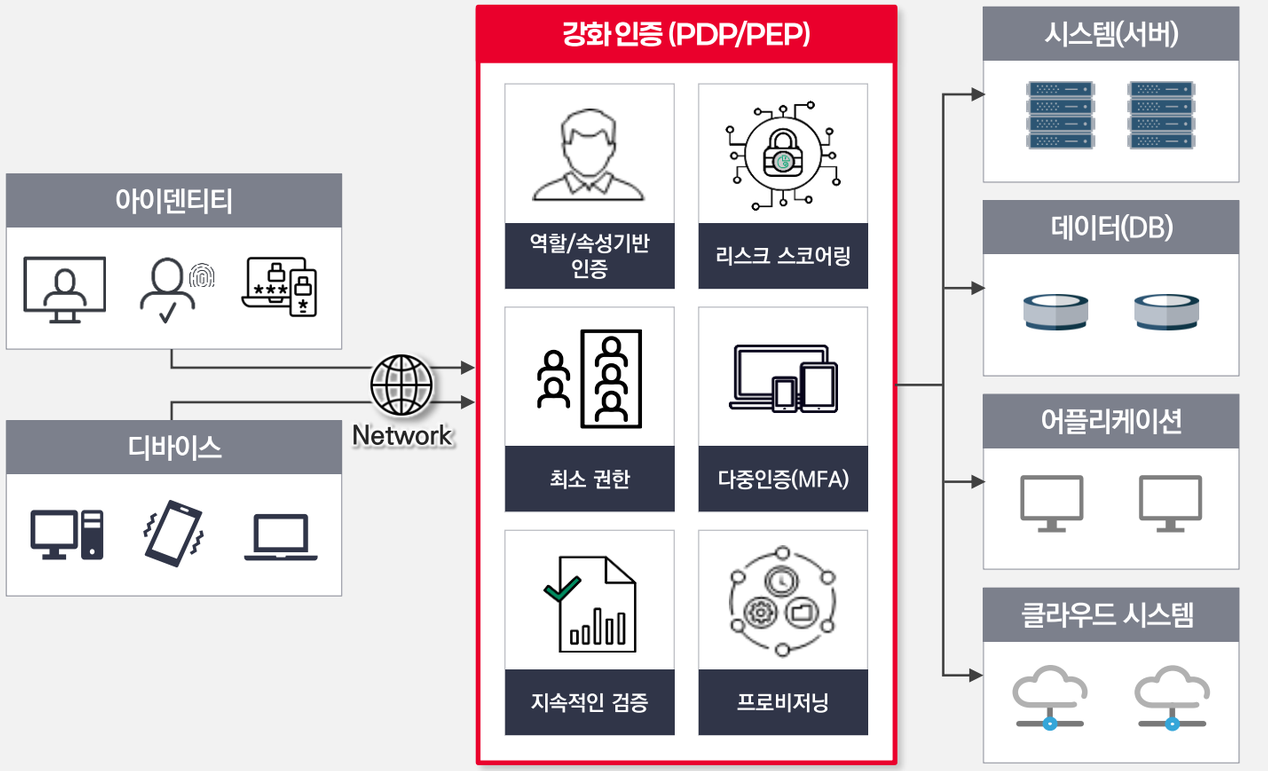
국가 망 보안체계 보안가이드라인

SK 쉴더스

02 SKZT – 2단계 · 환경 구축(사용자 인증)

조직 내 다양한 리소스에 접근하는 모든 아이덴티티와 디바이스를 식별하고 식별된 정보를 관리합니다.
식별된 정보를 활용하여 제로트러스트 기반의 강화된 인증을 적용함으로써 조직 내 리소스에 접근 하는 사용자에 대한 인증을 강화할 수 있습니다.

사용자 인증 구현방안



주요 기술

기대효과

아이덴티티와 디바이스 기반의 강화 인증을 통해 접속환경과 무관한 사용자 인증 강화

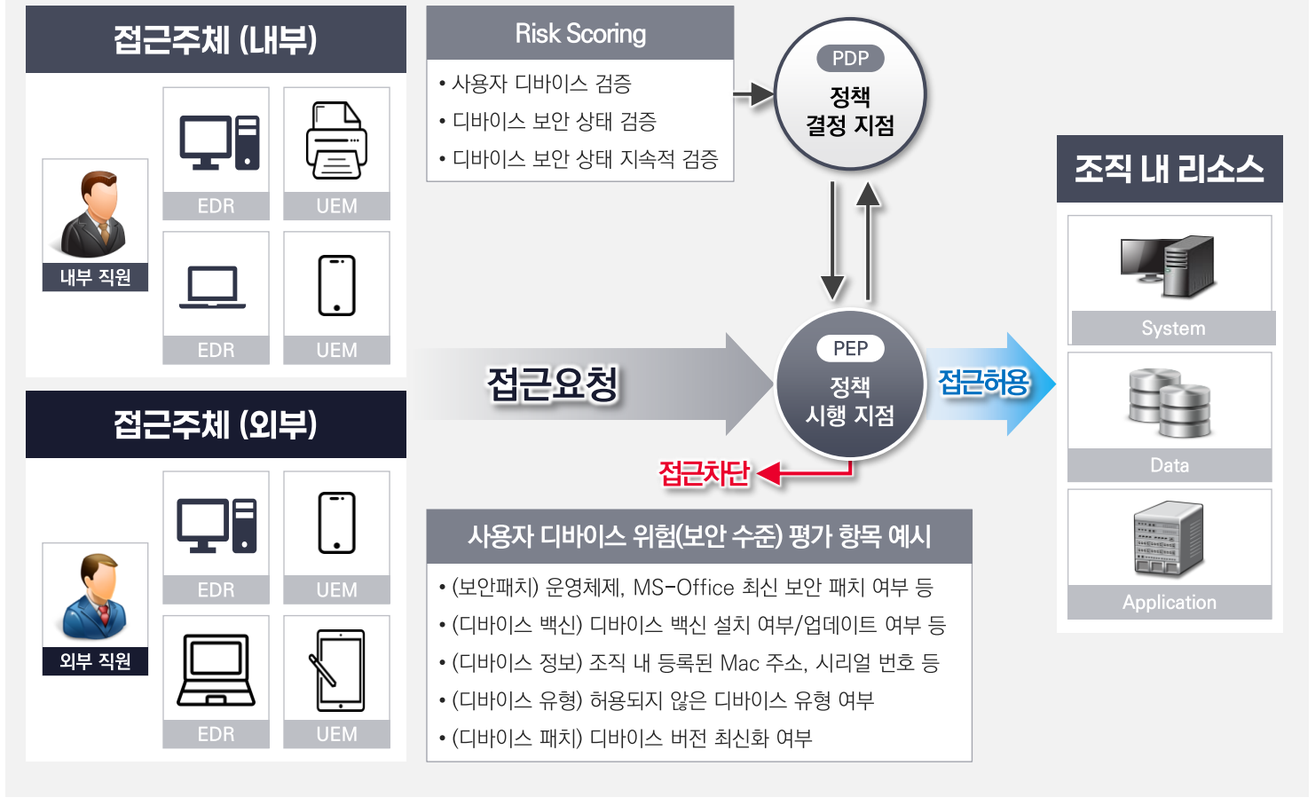
SK 쉴더스

02 SKZT – 2단계 · 환경 구축(접근통제/디바이스 보안)

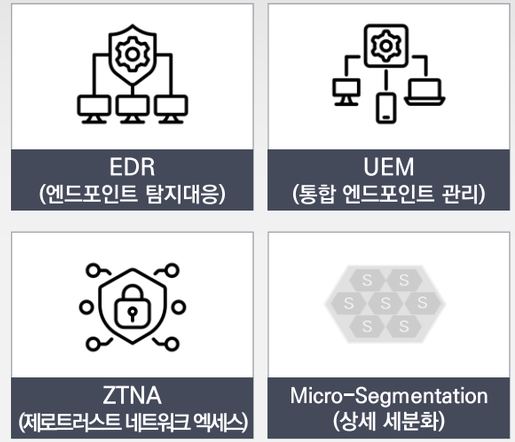
조직 내 리소스에 접근하는 접근주체에 대해 강력한 검증체계를 적용하여 허용된 리소스에 허용된 접근주체만이 접근할 수 있도록 통제합니다.
접근주체의 모든 행위는 모두 모니터링되며 실시간으로 변동사항에 대해 정책이 적용됩니다.

SK쉴더스 방법론
SKZT
1 SKZT 성숙도 평가
2 SKZT 환경 구축
3 SKZT 운영 관리

접근통제 및 디바이스 보안 구성안



주요 기술



기대효과

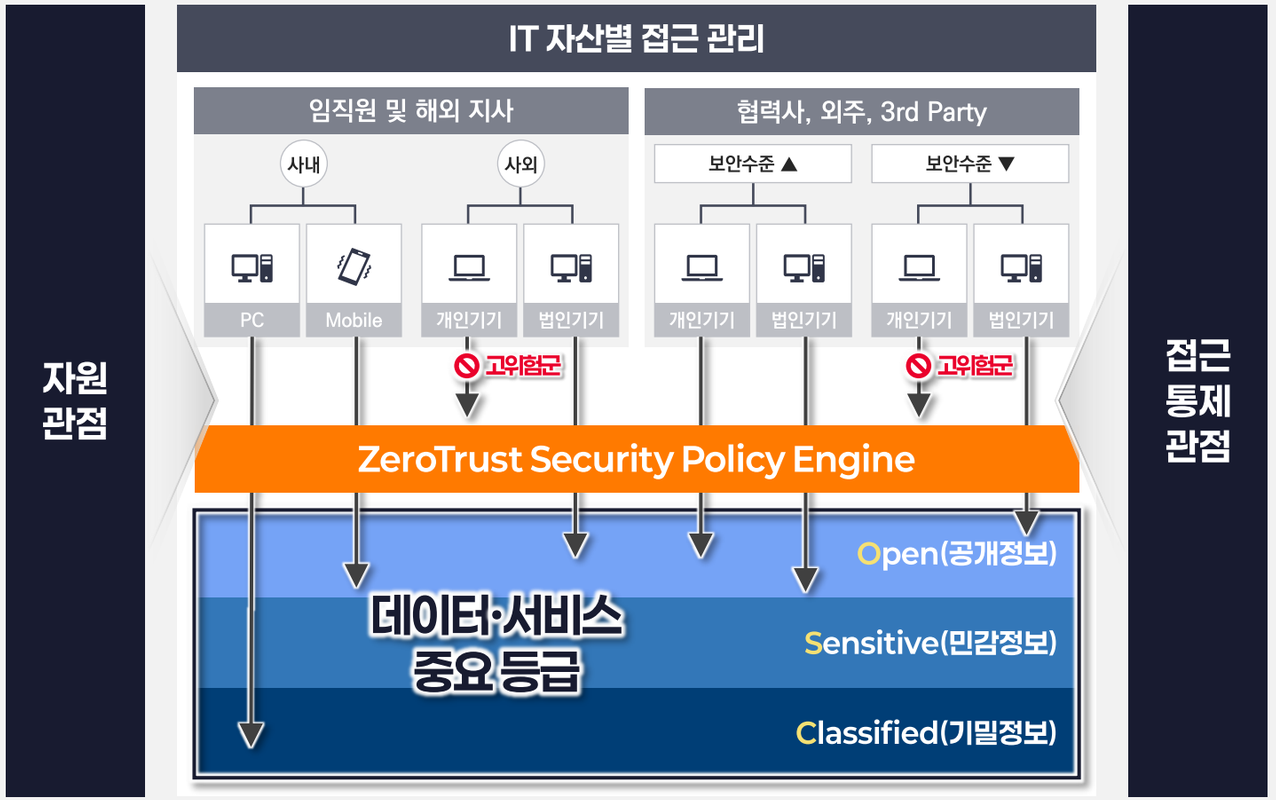
접근주체의 보안 상태를 지속적으로 확인하여 조직 내 리소스에 대한 접근통제를 강화

SK 쉴더스

02 SKZT – 2단계 · 환경 구축(데이터 보안)

업무 정보의 중요도(민감도)에 따라 세부 등급 분류(C. S. O)를 통해 발생가능한 구조적 위협의 사전 식별을 제공합니다.
제로 트러스트 보안원칙에 N2SF의 추가 적용을 통해 보다 강화된 데이터 보안을 제공 할 수 있습니다.

데이터 보안 구성안



주요 기술

- DSPM (데이터 보안태세 관리)
- Data Classification (데이터 식별관리)
- DLP (데이터 유출방지)
- RBI (원격브라우저격리)

기대효과

데이터 식별 및 등급화를 통한 데이터 보안 강화

SK 쉴더스

02 SKZT – 2단계 · 환경 구축(Z·T 위협대응)

제로트러스트 환경을 구현하기 위해서는 기존 사이버 위협 대응체계를 넘어, 다양한 영역에서 방대한 로그를 수집하고 분석해야 합니다.
제로트러스트 핵심 요소들을 기준으로 주요 로그들을 수집하고 분석하여, 자동화된 사이버 위협 대응 체계를 구현합니다.

Z·T 위협대응 및 가시성 확보방안

가시성 확보

사용자 | 디바이스 | 네트워크 | 시스템 | 어플리케이션 | 데이터

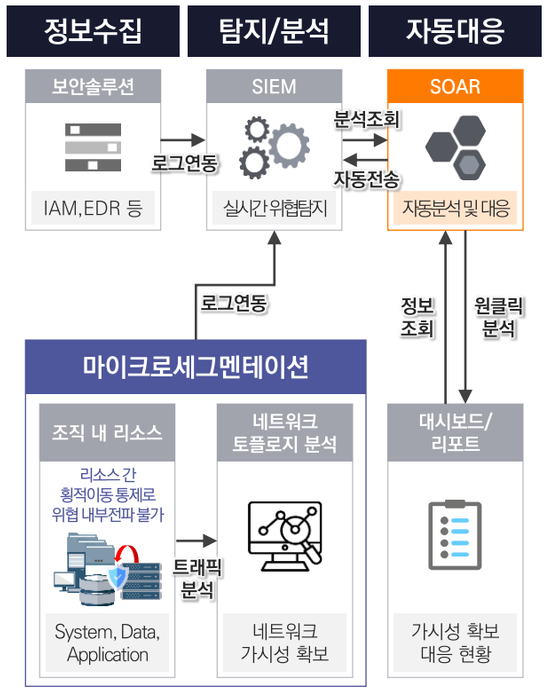
모든 종류의 위협을 관찰하고, 지능화된 방어기법 적용

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

자동화 대응 체계 수립

빅데이터(SIEM) 분석	대응 자동화(SOAR)
데이터 수집/저장/분석	사고대응 표준화/간소화
실시간 검색 및 상관분석	정책 및 프로세스 자동화
이상행위 기반 위협분석	보안 운영 효율화

주요 프로세스



주요 기술

- SIEM (보안정보 및 이벤트 관리)
- SOAR (보안 오케스트레이션, 자동화 및 대응)
- BigData (빅데이터)
- AI / ML (인공지능/머신러닝)

기대효과

제로트러스트 기반의 다양한 로그를 수집하여 사이버 위협에 대한 자동화 대응 체계 구현

SK 쉴더스

02 SKZT – 3단계 · 운영 관리

제로트러스트 환경의 운영 관리는 정책의 자동화 및 통합, 전사적인 제로트러스트 환경의 가시성 및 분석 환경의 구성을 목표로 하고 있으며,
이를 위해 기존의 빅데이터 수집 분석 체계의 고도화 또는 신규 구축이 필요합니다.

제로트러스트 운영 = 정책설정 및 시행 (자동화 및 통합) + 모니터링 (가시성 및 분석)

운영

가시성 및 분석

모든 종류의 위협을 관찰하고, 지능화된 방어기법 적용

- 비정상 행위 탐지 개선
- 동적 정책으로 변경 (보안정책, 접근제어)
- 패킷 단위 이상 트래픽 분석
- 지능화된 방어 기법 적용

자동화 및 통합

일관된 보안정책 시행으로 자동화된 통합 보안 대응

빅데이터(SIEM) 분석

- 데이터 수집/저장/분석
- 실시간 검색 및 상관분석
- 이상행위 탐지 및 위협분석

대응 자동화(SOAR)

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

구현

성숙도 모델 수준

- Identity
- Device/Endpoint
- Network
- System
- Application & Wokrload
- DATA

ZT 성숙도 단계별 수준 정책 적용

Data

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

SK 쉴더스

02 SKZT – 3단계 · 운영 관리

제로트러스트 운영 관리의 목적은 전환이 완료된 제로트러스트 영역을 관리함으로써 발생하고 있는 문제점의 도출 및 최소화를 위한 지속적인 노력입니다.
이러한 운영 관리는 이후 Next 레벨의 성숙도 도입을 위한 사전 작업이며, 가장 중요한 작업이기도 합니다.

SK쉴더스 방법론
SKZT

1 SKZT 성숙도 평가

2 SKZT 환경 구축

3 SKZT 운영 관리

한번에 완벽한 제로트러스트 전환은 불가능 하며, 지속적인 성숙도 관리가 필요

점진적 전환

문제 발생 최소화를 위한 점진적 전환

한번에 완벽한 시행 불가능

- 과도한 권한 허락 문제
- 정상 사용자 리소스 접근 거부
- 필요 권한 취득 거부
- 비인가 장비 접근 허용
- 기타 다양한 문제 발생
- ⋮

시범운영

리포팅 수행 지속적 수정

시범운영 모드

- 민감한 문제 발생 시 리포팅만 수행
- 비정상적인 접근제어 확인
  로그를 모니터링하면서 비정상적인 접근제어가 이루어지는지 확인
- 접근제어 정책을 지속적으로 수정하여 운영 개선

정상운영

운영 환경 적용 지속적인 모니터링

정상적 운영

- 시범운영 후 관리자의 판단 하에 정상적 운영 시행
- 성숙도 수준 별 사용자와 자산, 네트워크를 속적으로 모니터링
- 트래픽과 관련 정보를 로그 기록
- 필요 시 접근제어 정책 튜닝 가능하나 기업망 전체 영향을 주지 않도록 특히 유의

Next 레벨 성숙도 도입 시

접근 주체, 자산, 비즈니스 프로세스/워크플로우에 대해 재식별·평가하는 과정으로 전환

인프라 관련부서와의 긴밀한 협업 체계 구성 필수

프로세스 개선 시 고려사항

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

Ⅲ

ZETIA 소개

ZEro Trust Initiative Alliance

SK 쉴더스

01 ZETIA 필요성 및 목적

ZETIA는 글로벌 및 국내 최고의 제로트러스트 기술을 보유한 기업의 연합을 총칭하며 제로트러스트 시장의 주도적인 개척 및 활성화를 통한 국내 정보보안 수준을 한 단계 더 높여, 기업의 사회적 책무를 강화하고자 합니다.

국내 제로트러스트 사업 활성화의 지연

국내 제로트러스트 사업 진행방식은 개별 Vendor 사 제품 위주의 구현 방식 지향

→ 제로트러스트의 개념을 인지하고 있는 고객사 대상으로는 만족도 ↓

→ 고객사의 환경을 고려하지 못한 일방적인 제품 도입 설득으로 신뢰도 ↓

ID인증강화, Micro-Segmentation, SDP의 분류 기준으로 ZTNA 제품 구현

→ 해당 제품 구현으로 제로트러스트 구현이 완료된 것으로 오해하여 추가 사업기회 닫힘

→ 관리적/기술적 기반으로 고객사 별 차별화된 적용방안 제시 필요

ZETIA 필요성 및 목적

고객사의 정확한 제로트러스트 구현 NEED 반영

- 모든 환경, 모든 NEED에 부합할 수 있는 제로트러스트 구현 방안 공조
- 컨설팅, ID(인증), Micro-Segmentation, SDP 각 영역별 전문 기업, 완전한 제로트러스트 구현을 위한 로그 관리, 이상행위 탐지를 위한 AI 전문 기업 등 공통된 목적을 위한 Alliance 결성 및 사업 협력 진행

제로트러스트 시장의 주도적 개척 및 활성화

- 각 제로트러스트 영역 별 전문 기업과의 연합을 통해 다양한 시장 활성화 방안 논의
- 주기적 성과보고 및 진행내역 등 공유

SK 쉴더스

02 ZETIA 참여사 주요활동 및 역할

ZETIA는 현재 10개의 참여사와 함께 활동을 수행하고 있으며, 각 참여사는 제로트러스트 영역의 전문 파트를 전담하여 활동하고 있습니다.
이후 더 많은 참여사가 합류할 예정입니다.

참여사 공통 역할

제로트러스트 정보 공유

- 관련 기술동향 공유
- 사고 이슈 정보 공유
- 신규 제품 및 기능 공유

제로트러스트 활성화 관련 협력

주요 사업 내역 공유
- 신규 사업 정보
- 주요 사업 진행 현황
- 성공사례 및 이슈 내역

공동 사업 추진
- 사업 컨설팅
- 구축
- 운영관리

아카마이&엔큐리티 (Akamai)

컨텐츠, 엔터프라이즈 고객에게 다양한 CDN, 보안, Cloud 서비스 제공

파트: Micro-Segmentation

시스코 (cisco)

Global Cybersecurity Solution Company

파트: 제로트러스트 기반 MFA

클럼엘 (ClumL)

인공지능 머신러닝 기반 보안 솔루션

파트: AI/머신러닝 비지도학습& 준지도학습 모델링, 신변종 위협 & 이상 징후 탐지

다이퀘스트 (diquest)

인공지능 및 자연어처리 전문기업

파트: 대용량 Log 수집, 고성능 로그검색엔진

지니언스 (Genians)

ZTNA, NAC, EDR 등 통합 보안 플랫폼 기업

파트: 사용자 및 단말인증, 단말 보안성 평가, SDP & ZTNA, 통합 권한 권리

인텔리코드 (intellicode)

이상징후 탐지 솔루션 구축 (보안, IoT) 및 빅데이터 분석 플랫폼

파트: 인공지능 기반 이상징후/행위 분석 모델 개발

팔로알토 (paloalto NETWORKS)

안전한 디지털 혁신을 지원하는 사이버 보안 글로벌 기업

파트: SDP, 로그수집, AI분석 Micro-Segmentation

시큐레이어 (SecuLayer)

빅데이터 분석/인공지능 플랫폼 기반 로그 관리/통합 보안관제 솔루션

파트: 제로트러스트 기반 이상징후/행위 분석 시스템

에스지에이솔루션즈 (sga 에스지에이솔루션즈(주) SGA Solutions Co., Ltd.)

차세대 통합 보안 솔루션 공급 기업

파트: ID/인증/통합보안 Micro-Segmentation

에스케이쉴더스 (SK 쉴더스)

Total Security Company 물리·사이버 보안 전문 서비스 제공업체

파트: SKZT 성숙도 평가 컨설팅, SKZT 운영 및 관제 수행, 이상징후 분석모델 구성

소프트캠프 (SOFTCAMP)

제로트러스트 보안 중심의 정보보안업체

파트: ID / 인증, SDP-RBI, SDP-IAP, DATA 암호

SK 쉴더스

03 ZETIA 주요 활동

ZETIA는 대외적으로 제로트러스트 도입을 위한 컨설팅, 구축, 운영, 관리 전반에 대한 지원 체계 서비스를 주요 활동 범위로 지정하며 대내적으로는 지속적인 제로트러스트 환경 확대 및 변화 대비를 위한 협력방안 제시 등의 활동을 진행합니다.

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

- 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

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

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

- Next 성숙도 레벨 고도화 사전 준비
- 점진적 제로트러스트 범위 확대 요청 대응 (고객사)

행사장에서 공개

Ⅳ

SKZT 성숙도 평가
수행사례

디지털 신뢰 새 패러다임,
제로트러스트 적용 전략 콘퍼런스

"Go Ahead Zero-Trust"

SK쉴더스와 함께 SKZT를 통해 제로트러스트 도입을 시작하세요

공공영업팀 이정수 팀장 (jslee0106@sk.com, 010-5449-9384)
기업영업팀 최얼 팀장 (ulnonoz@sk.com, 010-9500-3652)
금융영업팀 김신철 팀장 (sc_kim@sk.com, 010-2545-6896)

SK 쉴더스