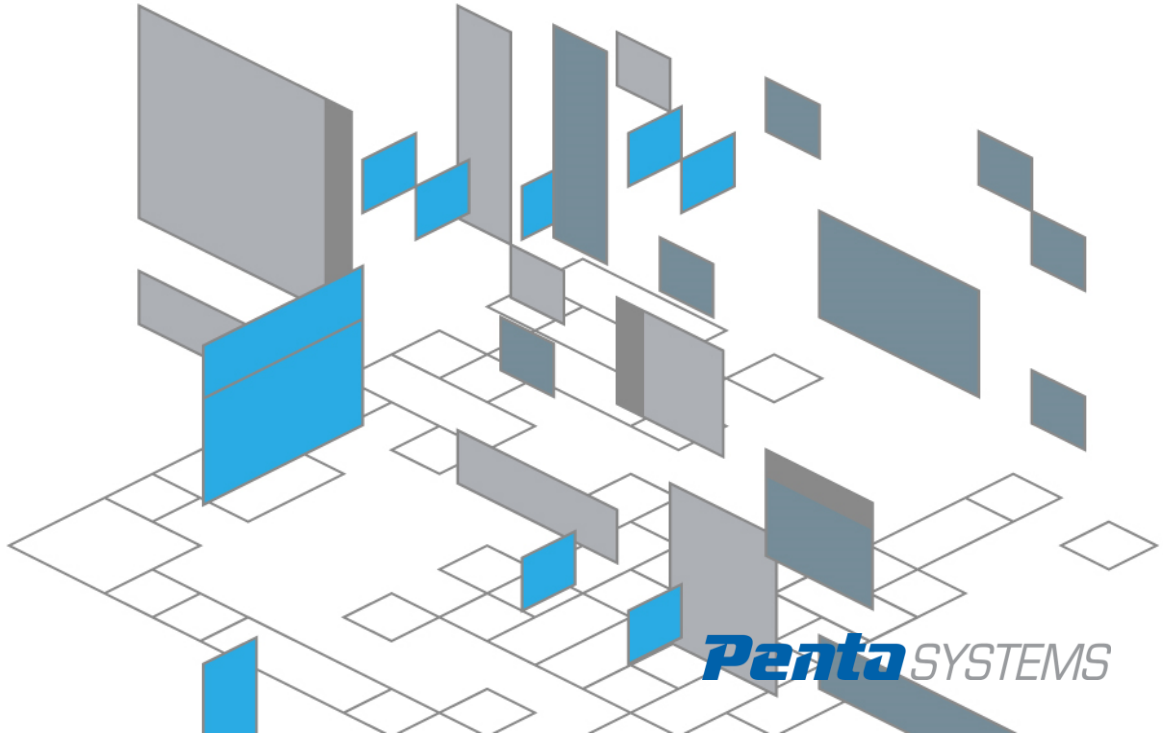
특권 사용자(Privileged User) 활동 기반의 시스템 접근 보안 위협 대응

2024.3.12(Tue)

펜타시스템테크놀러지
김동한(picollo@penta.co.kr)



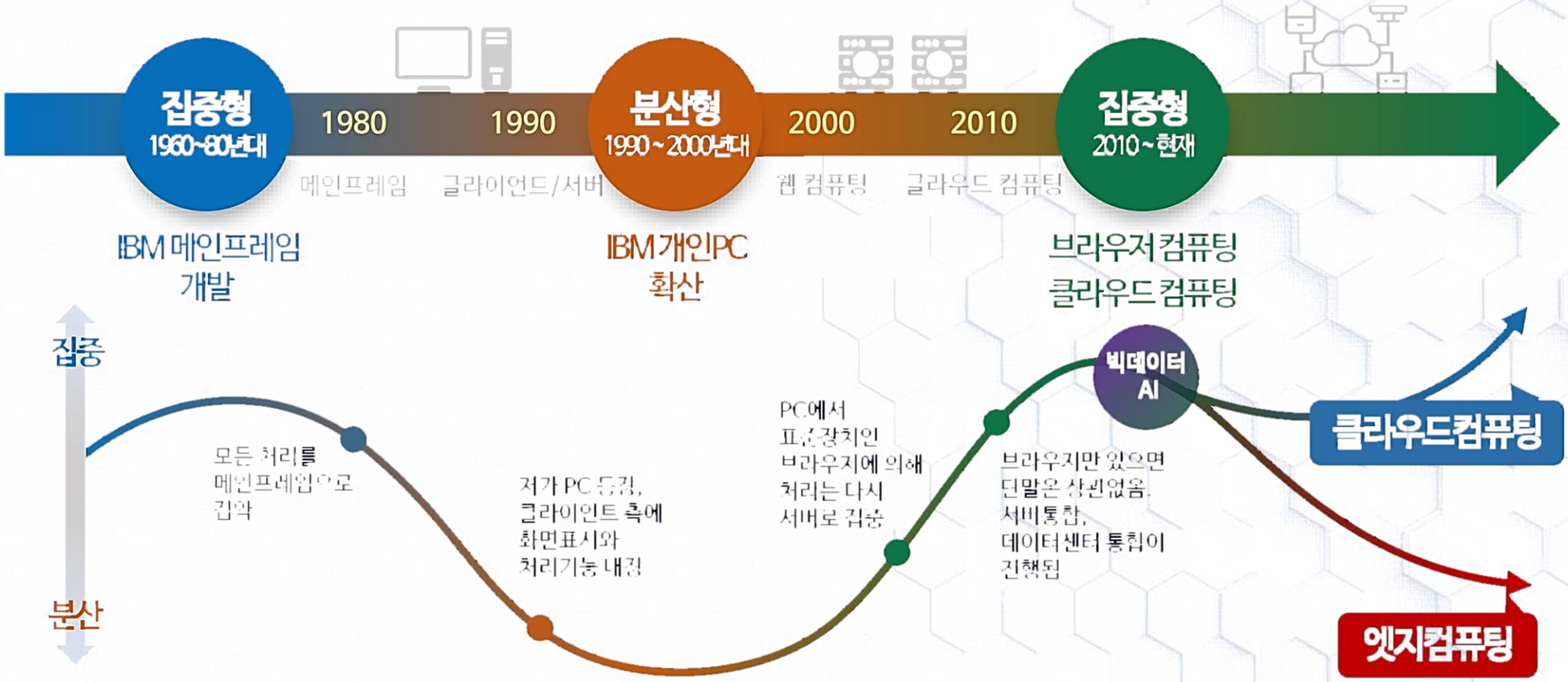
10th PentaLINK

PentaSYSTEMS

발표를 시작하며

컴퓨팅 패러다임과 시스템(서버) 환경의 변화

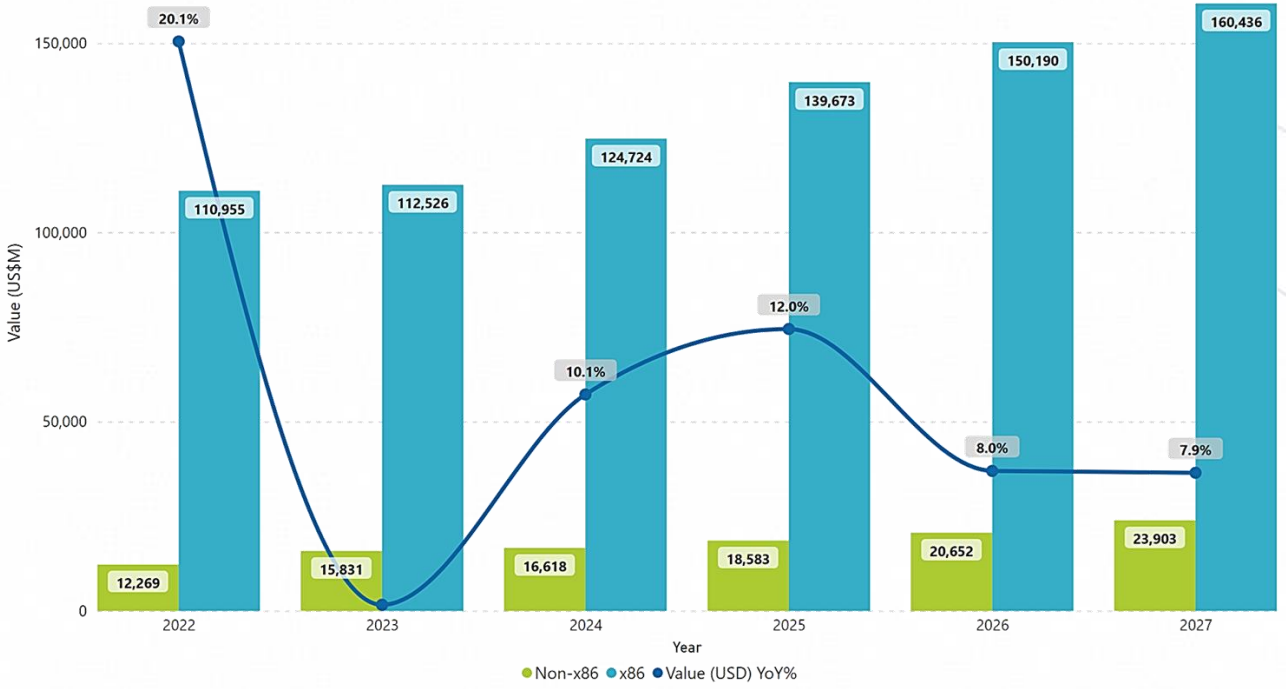
- Mainframe → Client-Server / Web → Cloud Computing → ?

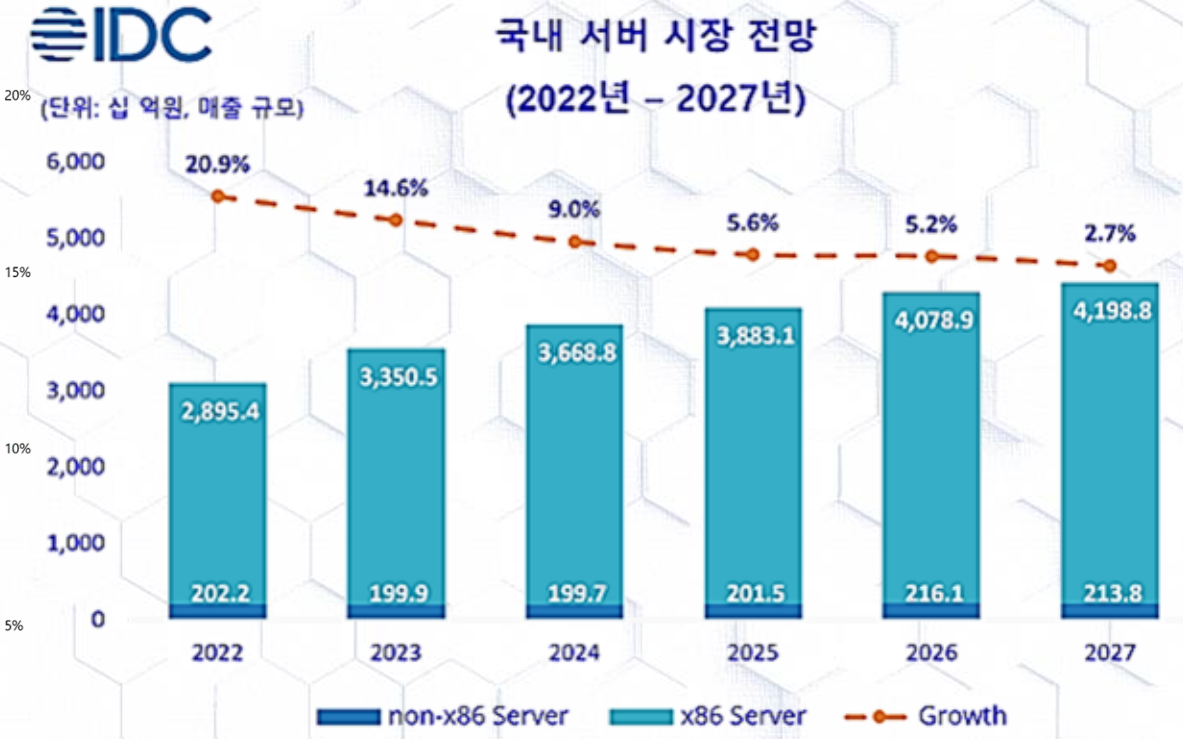


발표를 시작하며

컴퓨팅 패러다임과 시스템(서버) 환경의 변화

- Mainframe → UNIX → LINUX → ?
- x86, LINUX가 대세



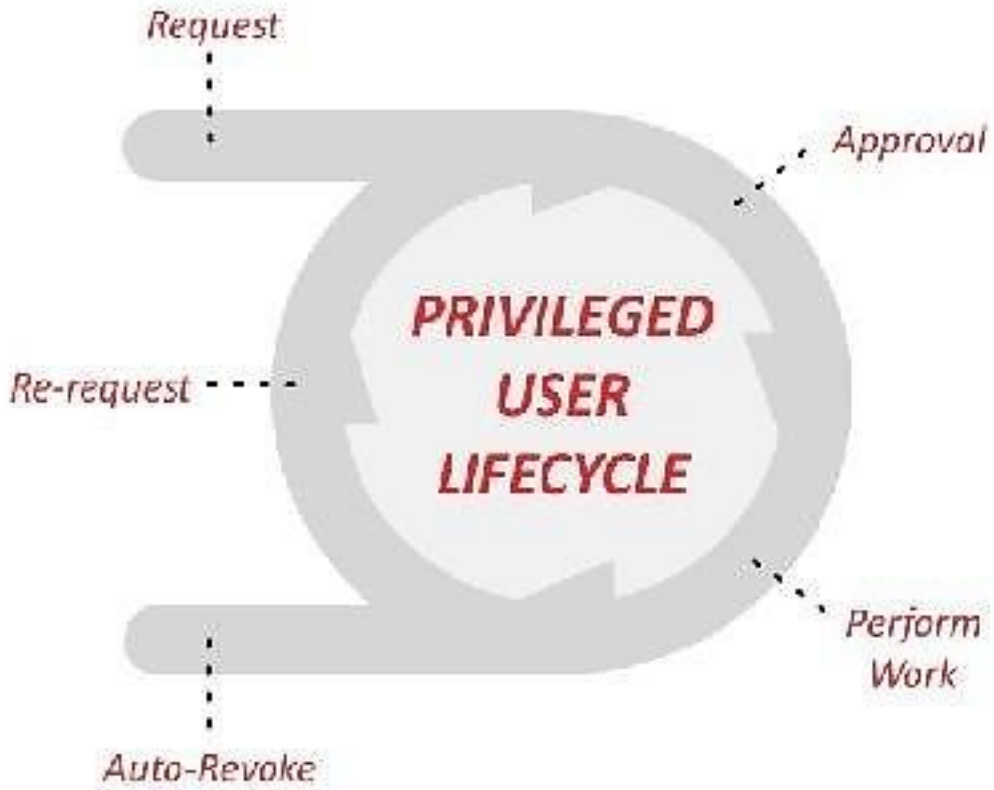


출처: (좌) IDC, 2022.12, (우) IDC, 2023.4

시스템/서버 보안 위협에 대한 접근

특권 사용자(Privileged User)?

- 권한 있는 사용자
- 다양한 사용자(표준 비즈니스 사용자, 계약 직원, 고객, 특권 사용자 등)

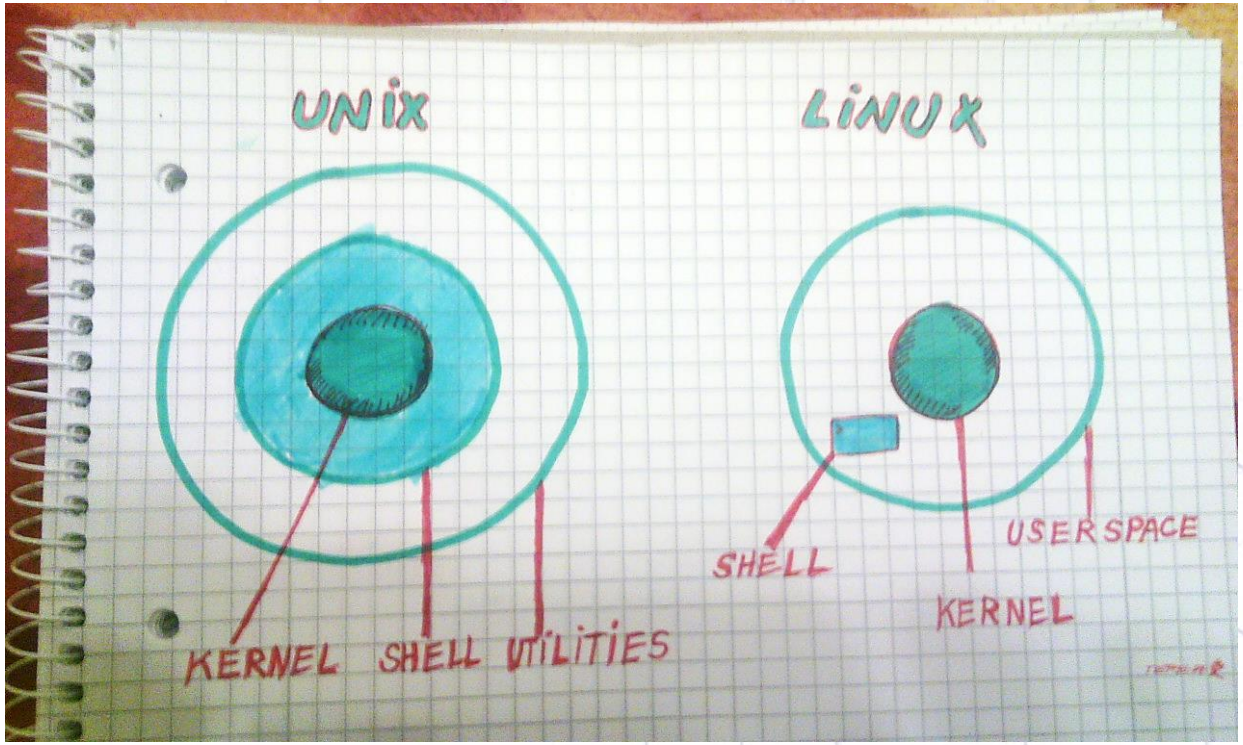


출처:(

시스템/서버 보안 위협에 대한 접근

SecureOS(aka eTrust Access Control, Trusted OS)

- SecureOS는 **운영 위험성이 높음(ex. Memco SeOS 사례)**
  - 커널 모듈을 로드하는 것이 시스템 안정성에 심대한 영향
- "장애를 많이 일으키는 보안 솔루션"으로 인식, OS 자체의 안정성, 보안 능력 고도화 및 내재화



출처: What are the very fundamental differences in architecture between Unix and Linux?, 2015

시스템/서버 보안 위협에 대한 접근

특권 사용자(Privileged User) ?

- 사용자에게 시스템에 대한 추가 권한이 부여되거나, 일반 사용자에 비해 더 높은 우선순위 수준의 접근 권한이 부여되는 경우, 사용자를 특권이 있다고 함

출처: Verizon, 2019

시스템/서버 보안 위협에 대한 접근

정보보호산업 분류 상 솔루션 구분

- 플랫폼보안/보안관리 〉서버접근통제 〉**보안운영체제(Secure OS)/시스템접근통제**

구분	
정보보안 제품 (솔루션)	네트워크보안 솔루션
	엔드포인트보안 솔루션
	플랫폼보안/보안관리 솔루션
	클라우드보안 솔루션
	컨텐츠/데이터 보안 솔루션
	공통인프라보안 솔루션
	소계
정보보안 관련 서비스	보안 컨설팅
	보안시스템 유지관리/보안성 지속 서비스
	보안관제 서비스
	보안교육 및 훈련 서비스
	보안인증 서비스
	소계

다. 플랫폼보안/보안관리 솔루션

플랫폼보안은 여러 위협을 분석하고 대응할 수 있도록 다양한 보안 솔루션들이 하나의 플랫폼으로 작동하여 보안성을 유지할 수 있도록 함. 이는 보안 운영 및 관리에 있어 여러 채널의 보안 이슈를 동시에 확인·처리하고 효과적으로 대응하기 위한 솔루션들이 포함되어 있으며, 보안관리 솔루션은 비인가된 접근으로부터 통신네트워크 및 시스템, 응용서비스 등을 보호하기 위한 관리 기능을 갖춘 제품으로 보안 서비스와 메커니즘의 생성, 제어, 삭제 기능, 보안 관련 정보의 분배 기능, 보안 관련 이벤트의 보고 기능, 암호키의 분배제어 기능, 인가된 사용자의 접근 권한 관리 기능 등 다양한 서브기능들이 포함됨.

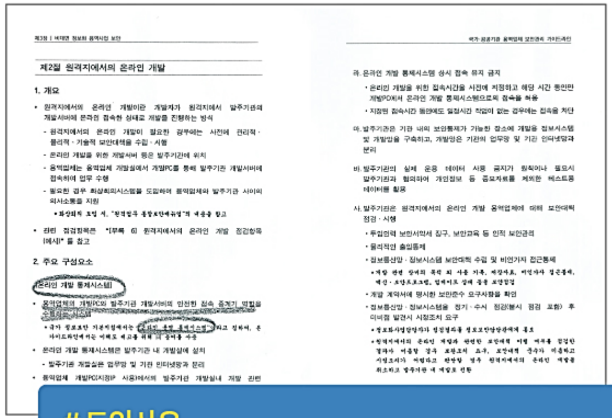
1) **서버 접근 통제** : 시스템 접근 통제와 SecureOS를 말함. 시스템접근통제는 네트워크, 서버, IT 인프라 운영 시스템으로의 모든 접속과 작업을 통제·관리, 작업 모니터링, 로그 기록 저장 등을 수행하는 보안 솔루션임. 보안운영체제(Secure Operating System)는 컴퓨터 운영 체제의 보안상 결함으로 인하여 발생 가능한 각종 해킹으로부터 시스템을 보호하기 위해 기존의 운영 체제(OS) 내에 보안 기능이 추가된 운영 체제임. 서버의 보호, 시스템 접근 제한, 시스템 관리자에 의한 권한 남용 제한, 사용자의 권한 내 정보 접근 허용, 응용 프로그램 버그를 악용한 공격으로부터 보호 등이 요구되는 운영 체제임.

출처: 과기부/KISIA, 2023년 국내 정보보호산업 실태조사 보고서, 2023.9

시스템/서버 보안 관련 Compliance

각종 컴플라이언스 이슈 100% 충족 및 최신 '국가용 보안요구사항 V3.0' 적용 필요

- 내부회계관리제도
- ISMS, ISMS-P
- 개인정보보호법 시행령
- 전자금융감독규정
- 국가 · 공공기관 용역업체 보안관리 가이드라인
- 과학기술정보통신부: '기간통신사업자' 연결망(네트워크) 안정성 확보방안 마련



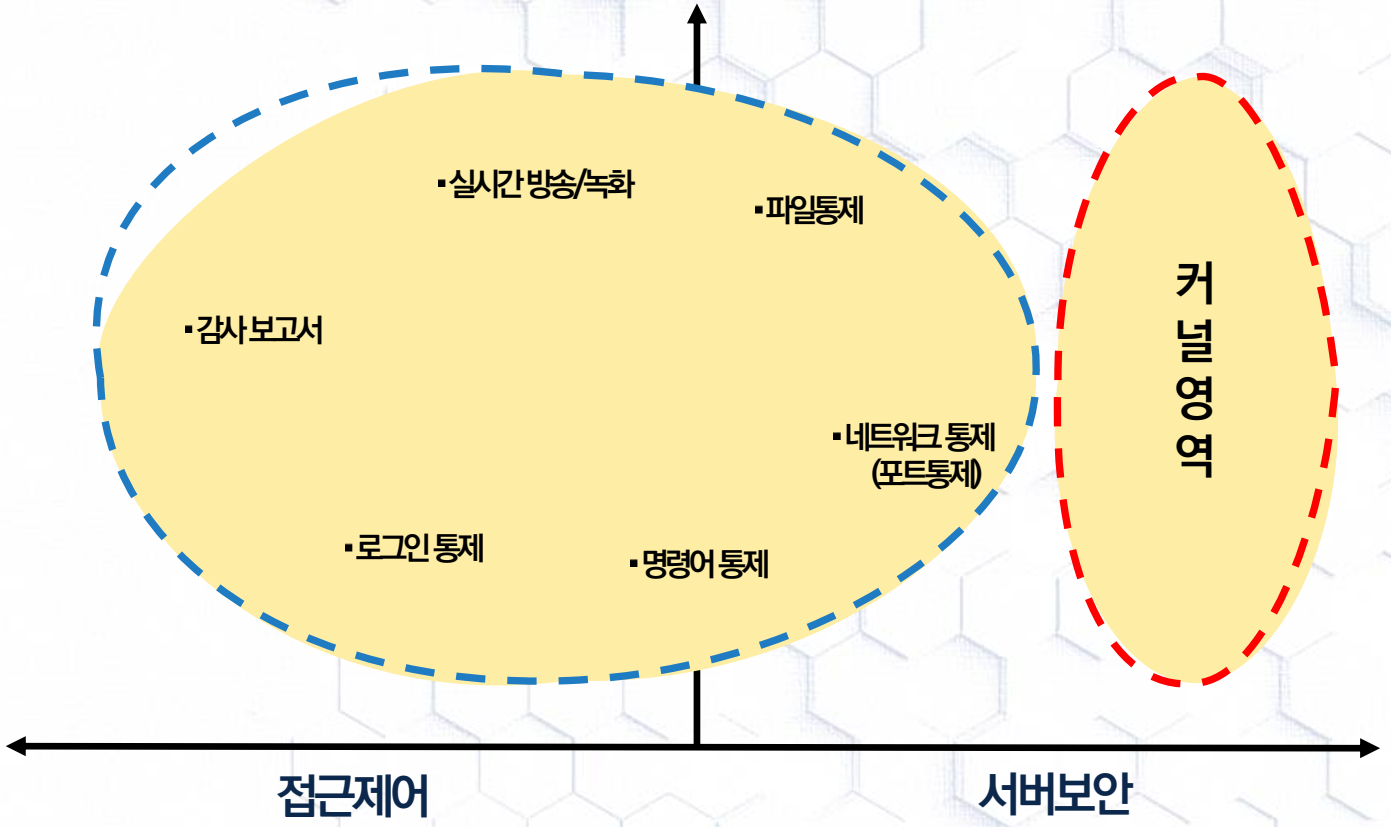
 # 도입사유

- 외부 유지보수 업체(사용자)의 내부 시스템 접근에 대한 사용자별 인증 및 보안 적용
- 사고 시, 빠른 장애 원인 분석 및 조치
- 원격지에서 용역 서비스/개발 업무가 있는 경우

펜타시스템의 접근 방법

OS에 대한 보안은 OS에 맡기고 …

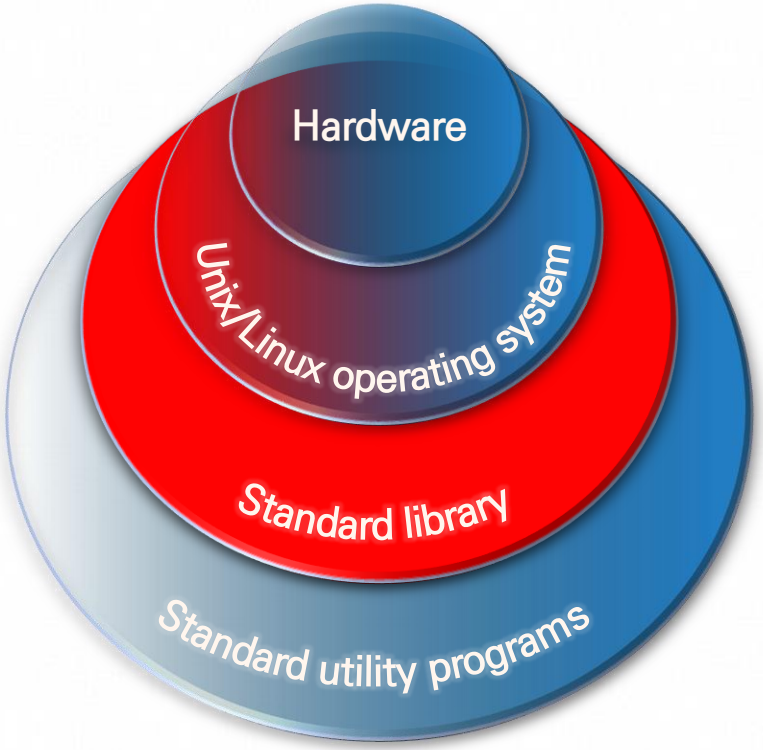
- 운영 위험성이 높은 커널 방식 외의 다른 방식 은 없는가?
- 서버보안 시장에 형성된 고가의 제품을 쓸 수 밖에 없는가?
- 변경 작업 시, Reboot 등 복잡한 작업 절차를 간편화 방안 은 없는가?
- 계정관리, 접근제어 같은 추가적인 기능을 제공할 수 없는가?
- Proxy/Gateway 방식의 한계를 극복할 수는 없을까?

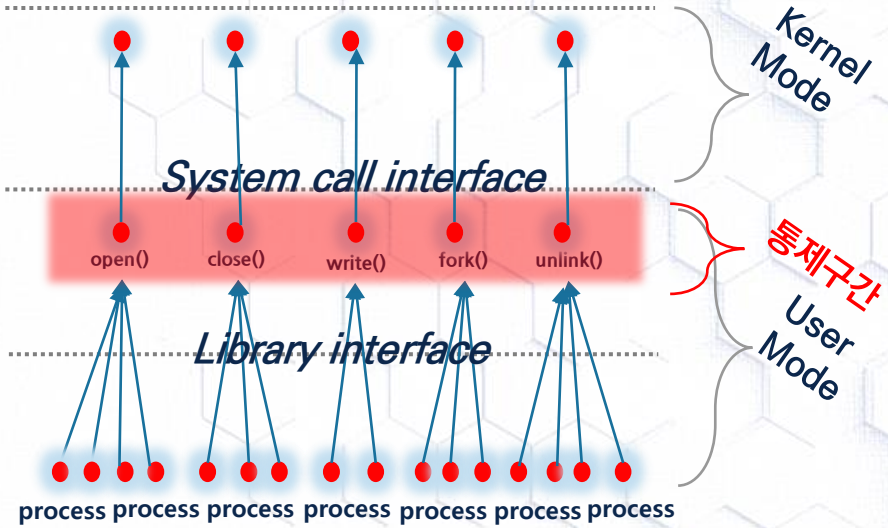


펜타시스템의 접근 방법

시스템 접근제어 SW 개발

- 특화된 보안 터미널 장치 개발 → 커널 방식에 비해 위험성 DOWN! 안정성 UP!
- 사용자모드에서 시스템 라이브러리 통제
- 클라우드 환경의 대표적인 장점인 빠른 확장성, 유연성을 위한 Auto Scaling In/Out 지원





펜타시스템의 접근 방법

ACRA Point

- 국내 특허 받은 터미널모니터링과 시스템라이브러리 통제기술을 바탕으로 서버에서 사용자의 모든 작업활동을 통제/감시하는 **'시스템 접근제어 솔루션'**

- 강제 세션차단
- 금지명령어 제한
- 접근IP 및 프로토콜 제한
- 2-factor 인증
- 결재시스템
- 서버/사용자 사용시간 제한

- 계정 생성
- 계정 변경
- 계정 삭제
- 계정 잠금 및 해제
- 패스워드 변경

- 실시간 세션 녹화
- 녹화세션 재생기능
- 녹화구간 내 동작검색
- 동작검색 시 녹화시점 이동

- 로그인 접속 이력 조회
- 활성 세션 조회
- 사용자 정책 조회
- 정책 변경 이력 조회
- 성공/차단 명령어 이력 조회
- 서버 계정 조회

펜타시스템의 접근 방법

경쟁 솔루션 비교

		ACRA Point		국내 접근제어 솔루션	
구분	항목	가능	설명	가능	설명
구현	하이브리드 방식 (유연한 구성)	●	가능	○	프록시 방식 지원
로그인	원격 및 로컬 접속 통제 제한 (사용자/IP 주소/접속시간)	●	가능	●	원격만 가능
	다양한 로그인 프로토콜을 지원 (telnet, ssh, ftp, sftp, rdp)	●	가능	●	가능
	로그인 시 2차 인증 제공	●	가능	●	가능
통제	사용자 별 금지 명령어에 대한 사용 제한	●	가능 (Agent방식일경우)	◐	우회가능
	사용자 별 네트워크 통제	●	가능	●	가능
	사용자 별 su 가능한 계정목록 통제	●	가능	●	가능
감사	사용자의 작업내용을 녹화 및 재생	●	가능	●	가능
	텍스트 형식의 이벤트 조회 및 시점 이동	●	가능 (Agent방식일경우)	◐	RDP 불가능
사용	사용 가능한 터미널 프로그램 종류 제약	◔	제한없음	◐	지원되는 터미널 종류 일부 제한
	사용자 PC에 전용프로그램이나 혹은 Web browser plug-in 을 설치 없이 동작	●	제한없음	○	설치 필수
	관리자용 웹 콘솔을 통해 기능 제공	●	가능	●	가능

마치면서 …

검증된 접근 방법: G기관 경쟁BMT 평가항목 및 시험 결과

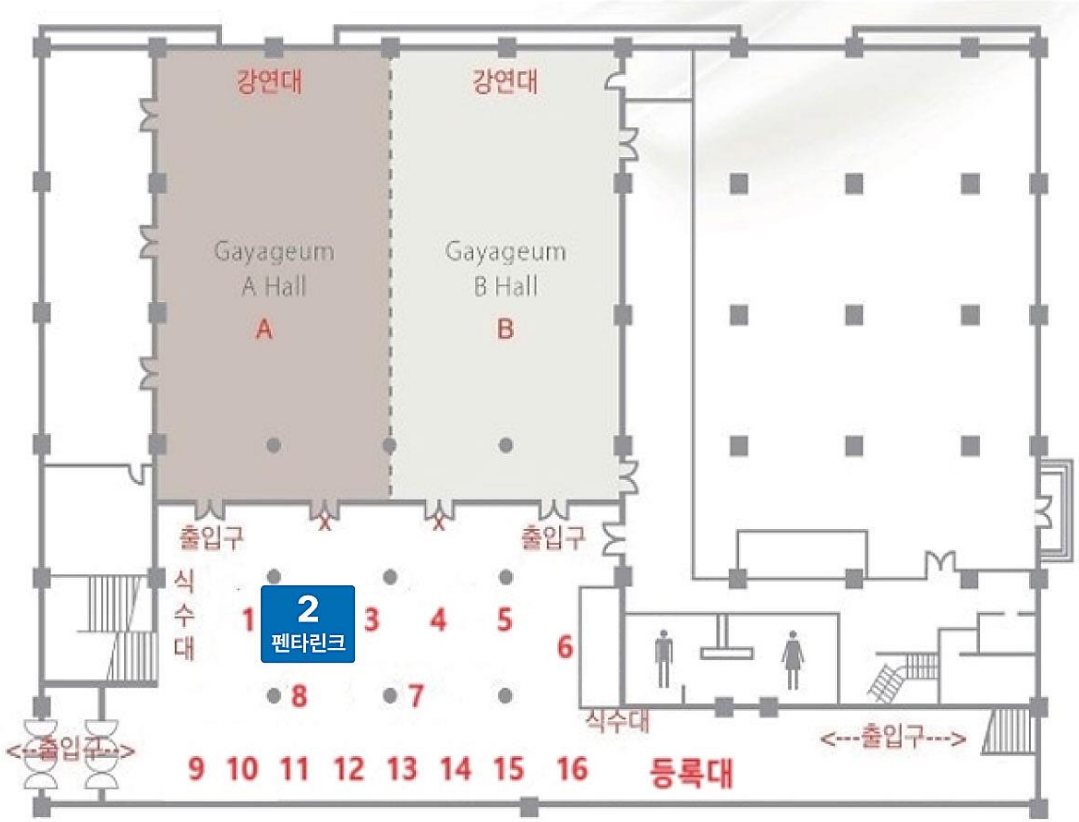
- 대규모 시스템 운영환경에서 처리속도 검증(55점 배점 55점 만점 획득, 2023)

구분	평가항목	결과
기능 확인	사용자별 권한 관리 기능	합격(P)
	사용 단말(IP, MAC 등) 별 권한 관리 기능	합격(P)
	시스템 접근관리조건 및 규칙 관리 기능	합격(P)
	사용자 계정 사용 관련 관리 기능	합격(P)
	평문통신 프로토콜 차단 기능	합격(P)
	금지명령어 설정 및 차단 기능	합격(P)
	특정 조건 차단 기능 -금지명령어 입력 횟수 초과 시 -접근관리시스템 경유 우회접속 시도 시	합격(P)
	실시간 모니터링 시 세션 차단 기능	합격(P)
	사용자별 정보 감사 기능	합격(P)
	세션별 사용자 정보 조회 기능 -접근시간, 시스템명, 사용자 IP, 사용자 ID 등	합격(P)
	금지명령어 사용 이력 조회 기능	합격(P)
	이벤트 발생 시 관리자 및 사용자 알림 기능 -금지 명령어 실행 -사용자 계정, 패스워드, 장비접속시간만료 등	합격(P)
	사용자 세션 실시간 모니터링	합격(P)
성능 확인	대량 명령어 발생 시 응답시간 확인	최우수

마치면서 …

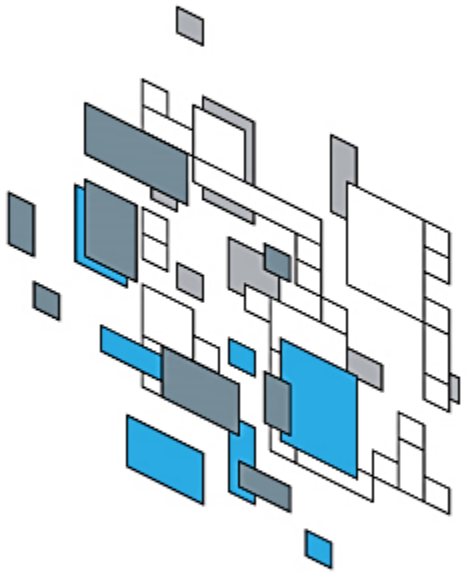
#2 Booth에 오셔서 체험하세요!

G-PRIVACY 2024 전시부스 배치도



1	좋을	2	펜타린크
3	소만사	4	안랩
5	시큐레터	6	파수
7	이지서티	8	지란지교데이터
9	한화보험사	10	KISIA
11	센티널테크놀로지	12	위즈코리아
13	컴엑스아이	14	엘세븐시큐리티
15	데이타스	16	KISA

Q&A



감사합니다

Thank you~!

Manage, Enhance & Secure Data

Penta Systems Technology Inc. Sewoo Bldg.,10~11Fl. 115, Yeouigongwon-ro, Yeongdeungpo-gu, Seoul, Republic of Korea **T.** 82-2-769-9700 **F.** 82-2-784-5550