최근 사이버위협 동향 및 보안 고려사항

KISA 한국인터넷진흥원

Contents



Ⅰ 기업 ICT 환경 변화

Ⅱ 최근 사이버위협 동향

Ⅲ 보안 고려사항

I 기업 ICT 환경 변화



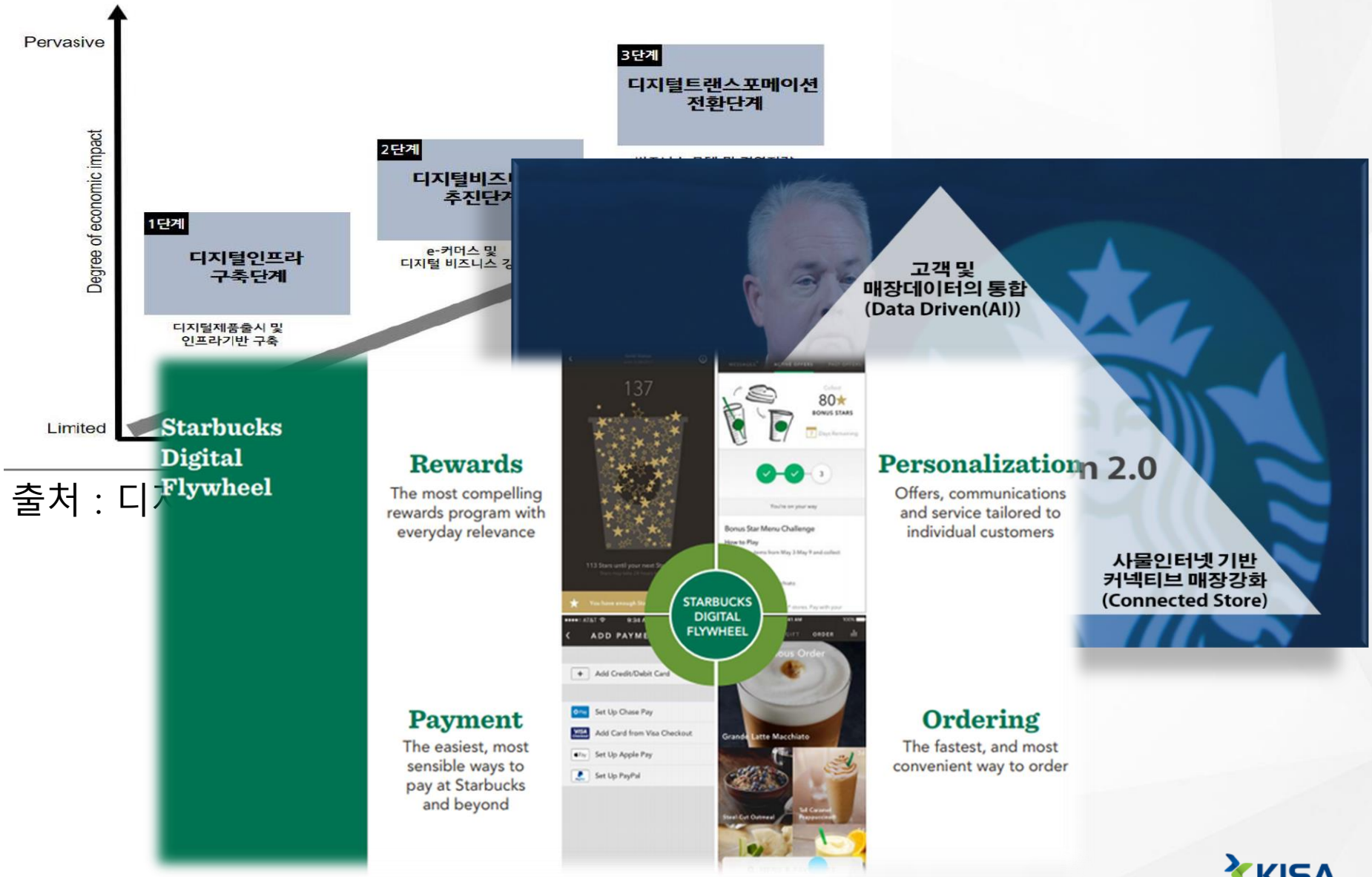
21세기 인류 삶의 변화 원동력 : 디지털



The evolution of the desk by the Harvard Innovation Lab

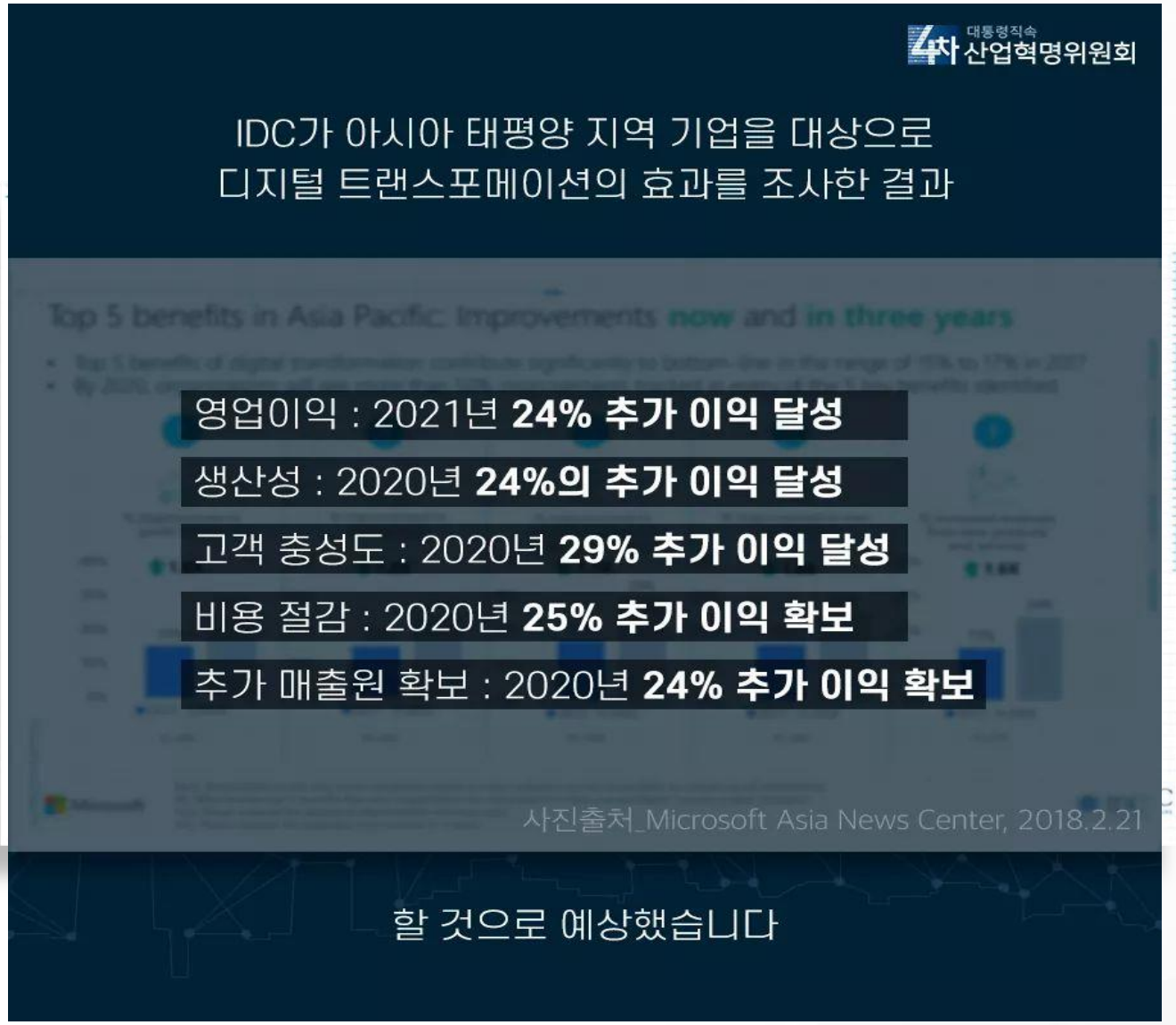
http://imgur.com/tWvyfya

디지털 트랜스포메이션 시대



출처 : 디

디지털 트랜스포메이션 - 효과



디지털 트랜스포메이션 - 국내상황



Ⅱ 최근 사이버위협 동향



해커의 공격대상



무엇이 문제가 되고 있는가?

내부확산 문제



망접점 문제



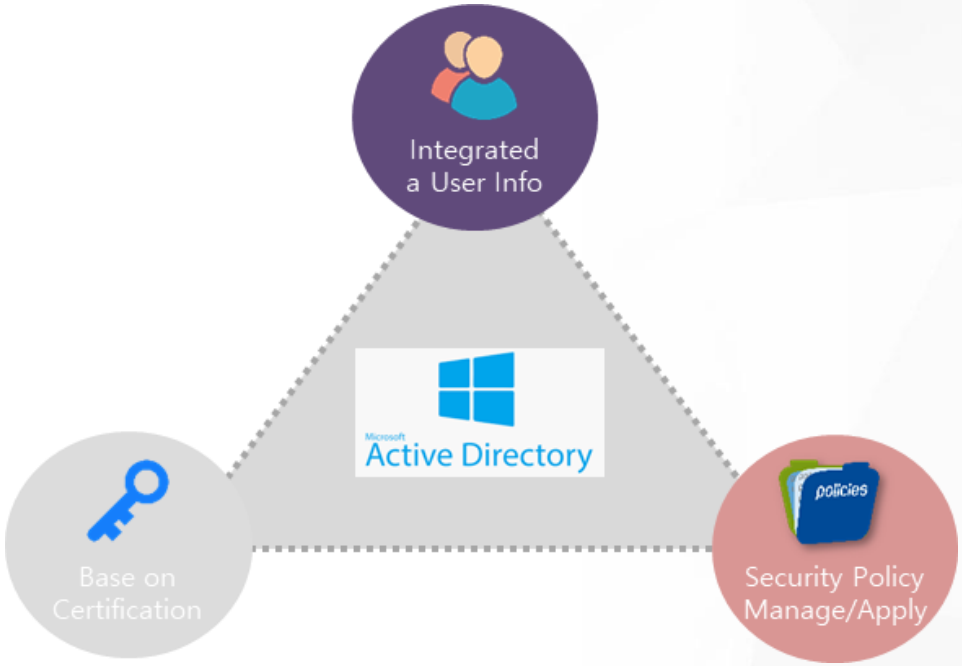
개발환경 문제



내부확산 문제 - AD를 알고 계십니까?

AD(Active Directory)

- MS 윈도우에서 제공하는 리소스(컴퓨터, 사용자 등) 중앙관리 및 디렉터리 서비스
  - 분산된 전사 자원을 계층적 구조로 저장하여 통합관리 가능



내부확산 문제 - AD 보안이슈를 알고 계십니까?

KISA

당신의 AD는 안녕하십니까?

AD(Active Directory) 관리자 계정 탈취를 통한 기업 내부망 장악 사례와 대응방안

2019.02.27

※ 본 사고노트의 전부나 일부를 인용 시 반드시 [자료: 한국인터넷진흥원]을 명시하여 주시기 바랍니다.

KISA
Korea Internet & Security Agency

당신의 AD는 안녕하십니까? Season 2

AD(Active Directory) 관리자가 피해야 할 6가지 AD 운영 사례

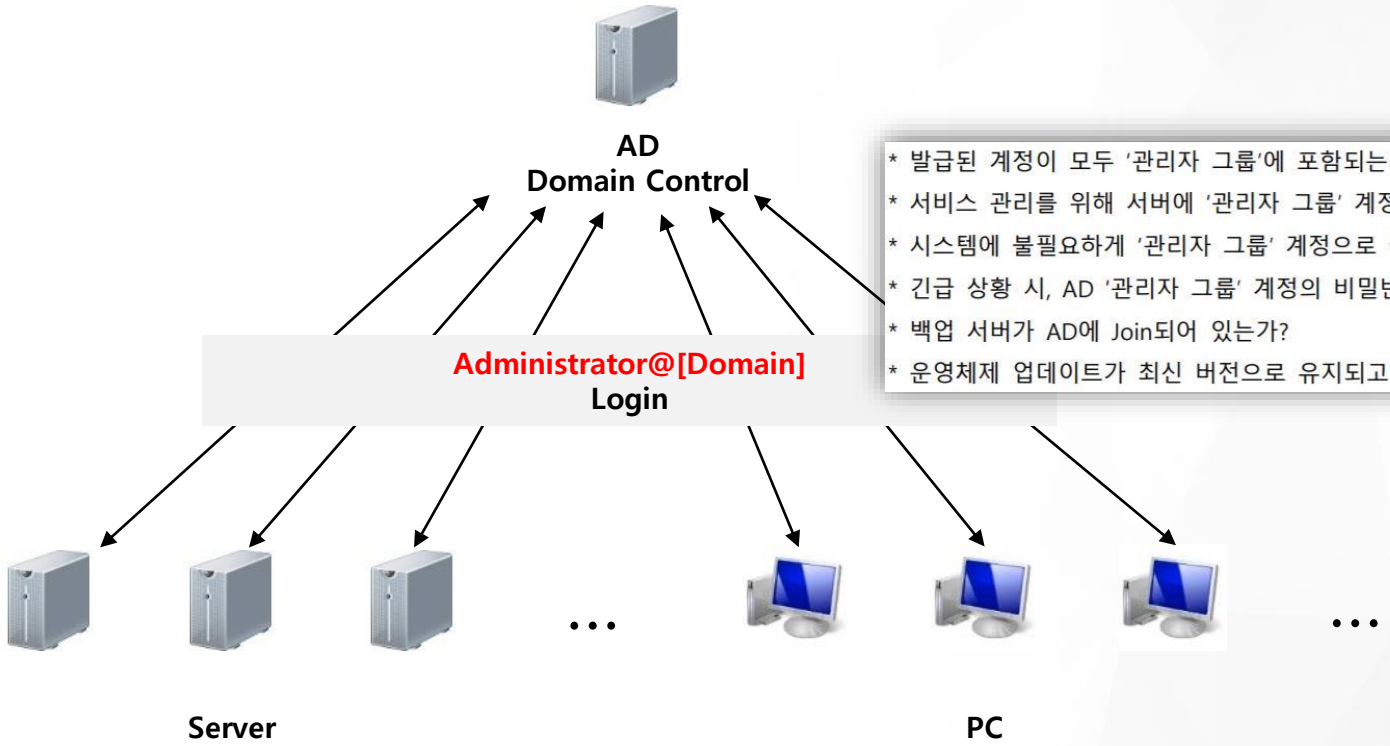
2019.04.01

※ 본 사고노트의 전부나 일부를 인용 시 반드시 [자료: 한국인터넷진흥원]을 명시하여 주시기 바랍니다.

내부확산 문제 - AD 보안이슈

취약한 AD 환경 관리

- 모든 서버/PC가 AD 관리자 그룹 계정으로 AD에 연동된 경우
- AD 관리자 계정으로 각 서버/PC에 로그인해 관리하는 경우
  - AD 관리자 그룹 계정 탈취 시 AD에 연동된 전사 서버/PC 장악 가능



* 발급된 계정이 모두 '관리자 그룹'에 포함되는가?
* 서비스 관리를 위해 서버에 '관리자 그룹' 계정으로 로그온 하는가?
* 시스템에 불필요하게 '관리자 그룹' 계정으로 실행되고 있는 서비스가 있는가?
* 긴급 상황 시, AD '관리자 그룹' 계정의 비밀번호를 신속히 바꿀 수 있는가?
* 백업 서버가 AD에 Join되어 있는가?
* 운영체제 업데이트가 최신 버전으로 유지되고 있는가?

내부확산 문제 - 기업 내부망 랜섬웨어 대량 감염

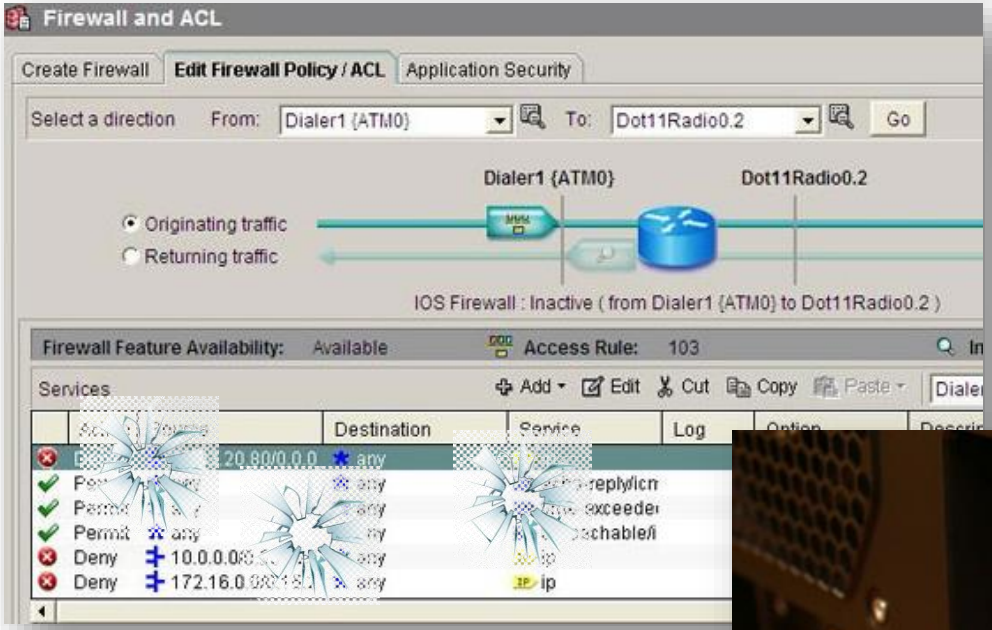


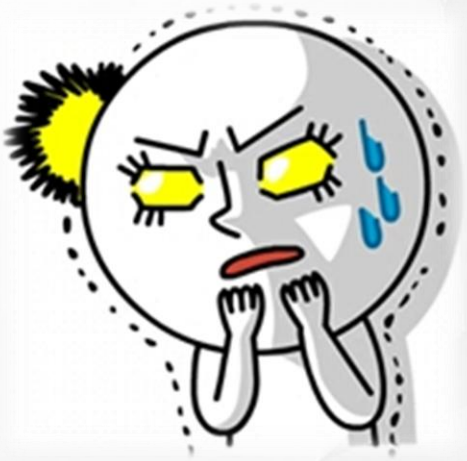
ing...

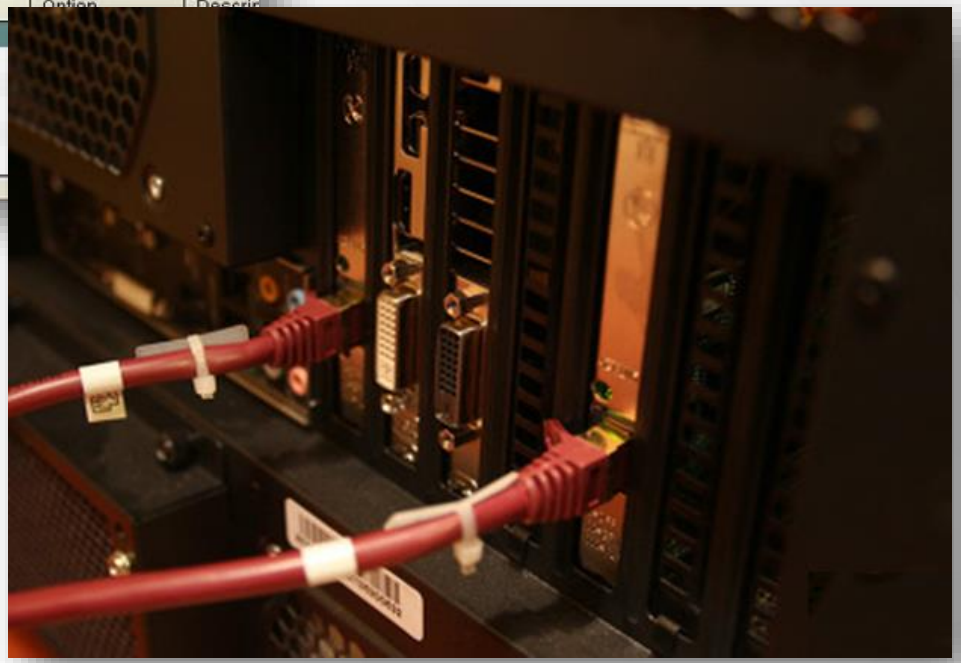


KISA

망접점 문제 - 기술적, 물리적 관리 부실



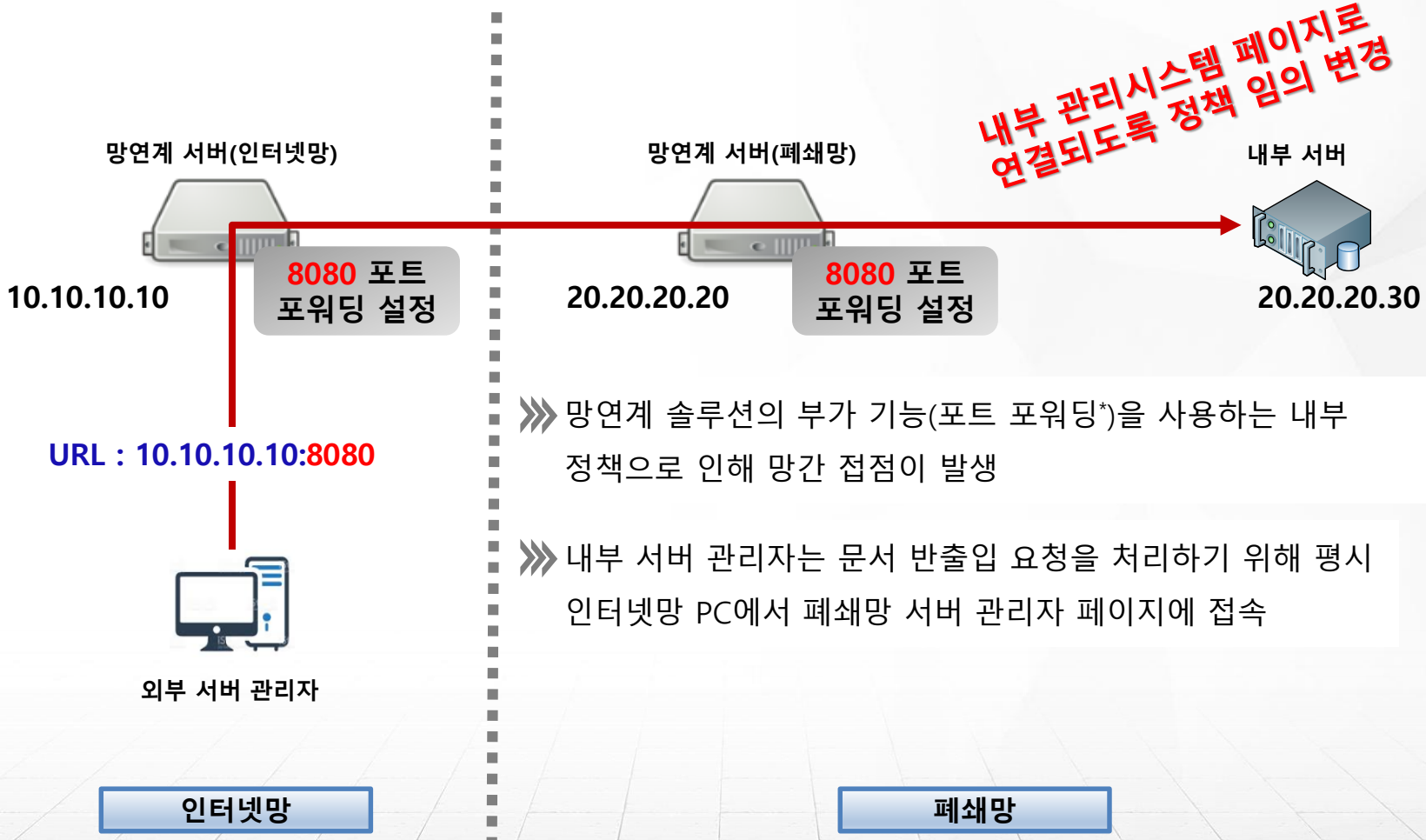




KISA

망접점 문제 - 망연계 보안이슈(정책 취약점)

임의 보안정책 변경에 의한 내-외부 망간 접점 생성



- 망연계 솔루션의 부가 기능(포트 포워딩*)을 사용하는 내부 정책으로 인해 망간 접점이 발생
- 내부 서버 관리자는 문서 반출입 요청을 처리하기 위해 평시 인터넷망 PC에서 폐쇄망 서버 관리자 페이지에 접속

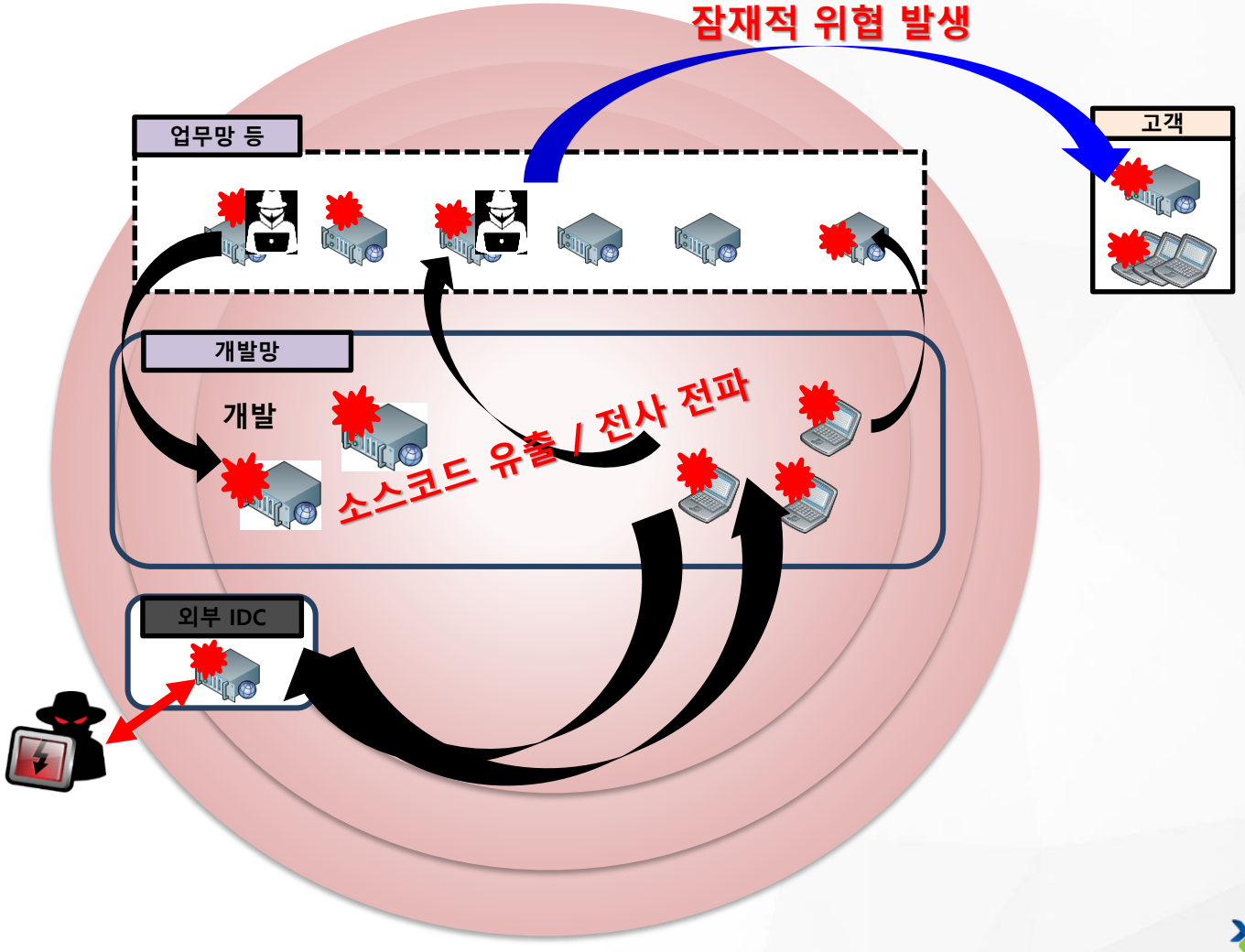
개발환경 문제 - 온라인 소스코드 저장소 관리 부실





개발환경 문제 - 개발환경 보안 관리 부실

개발환경을 중심으로 소스코드 유출 및 전사 전파 피해 발생

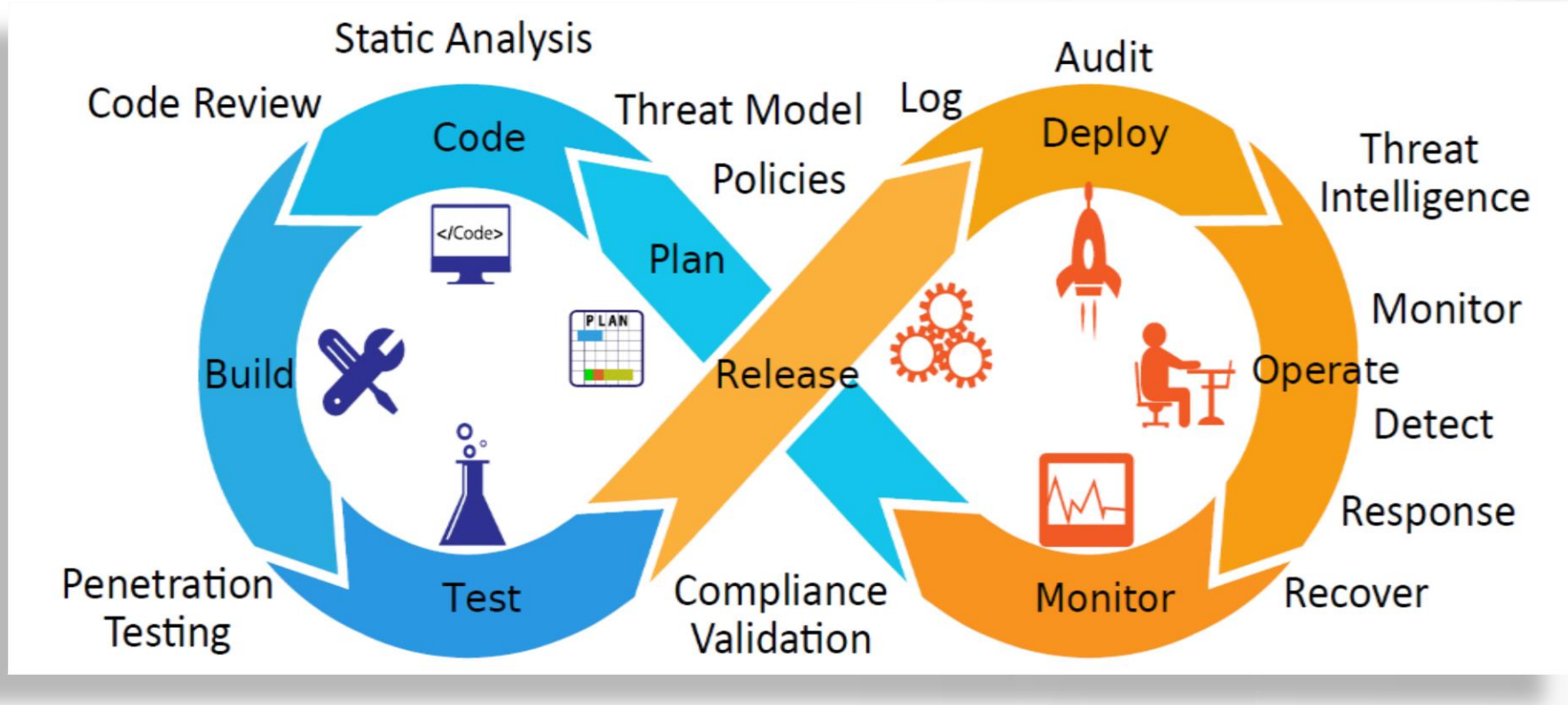


Ⅲ 보안 고려사항



고려사항 - 함께하는 보안

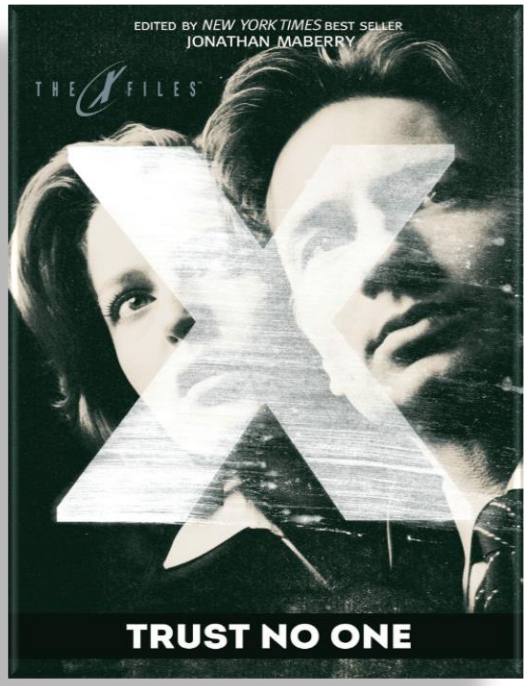
보안팀, 운영팀, 개발팀 협력



DevSecOps: Integrate Security Into DevOps(출처 : OWASP, 2018)

고려사항 - 접근통제에 대한 재설계

기업의 중요한 정보자산을 중심으로 고려





출처 : FORRESTER, "The **Zero Trust** eXtended Ecosystem Framework"

KISA

고려사항 - 사각지대 제거

로그를 모았으면 분석!!!



단순 보안로그
모니터링만으로는 대응 한계



[End to Net : Seamlees]
공격정보 수집/연관분석을
통한 종합적 대응 필요



감사합니다