

디지털 트랜스포메이션 시대의 보안위협 대응방안

'19.4.24(수)

KISA 이동근 단장



Contents

- I** ▶ 디지털 환경 변화
- II** ▶ 최근 보안위협 동향
- III** ▶ 향후 대응방안

I

디지털 환경 변화



인류 삶의 변화

'70년 이전



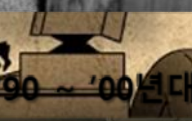
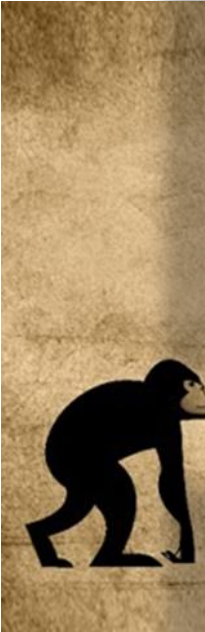
'70 ~ '80년대



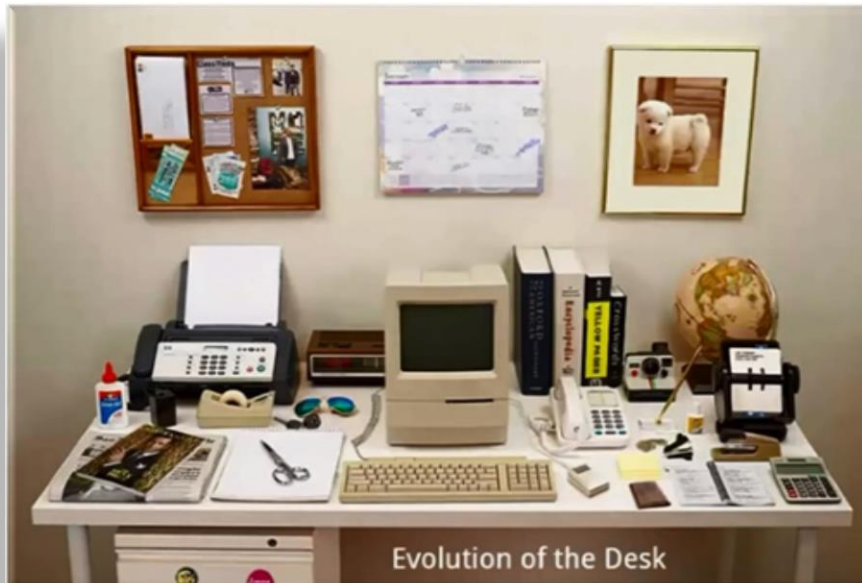
'90년 이후



'90 ~ '00년대



21세기 인류 삶의 변화 원동력 : 디지털



The evolution of the desk by the Harvard Innovation Lab
<http://imgur.com/tWvyfya>

디지털 트랜스포메이션 시대

Pervasive
Degree of economic impact

1단계

디지털인
구축단

디지털제품출시
인프라기반 구

Starbucks
Digital
Flywheel

Rewards

The most compelling
rewards program with
everyday relevance

3단계

디지털트랜스포메이션



Personalization

Offers, communications
and service tailored to
individual customers

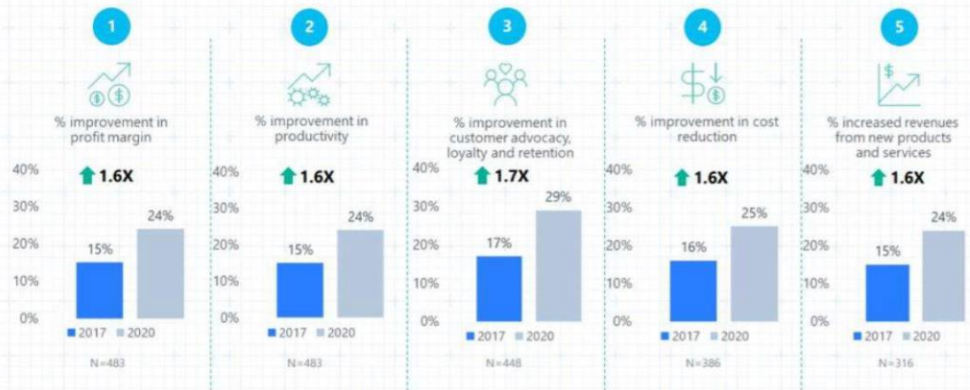
Ordering

The fastest, and most
convenient way to order

사물인터넷 기반
커넥티브 매장강화
(Connected Store)

Top 5 benefits in Asia Pacific: Improvements now and in three years

- Top 5 benefits of digital transformation contribute significantly to bottom-line in the range of 15% to 17% in 2017
- By 2020, organizations will see more than 50% improvements tracked in every of the 5 key benefits identified



Base: Respondent counts vary across all options as this is a top 3 question so not all benefits are chosen by all respondents.
A5: What are the top 3 benefits that your organization has observed from their current Digital Transformation initiatives?
A5B: Please indicate the degree of improvement from last year.
A5C: Please indicate the expected improvement in 3 years.



디지털 트랜스포메이션 - 국내상황

IDC ANALYZE THE FUTURE

IDC DIGITAL TRANSFORMATION AWARDS

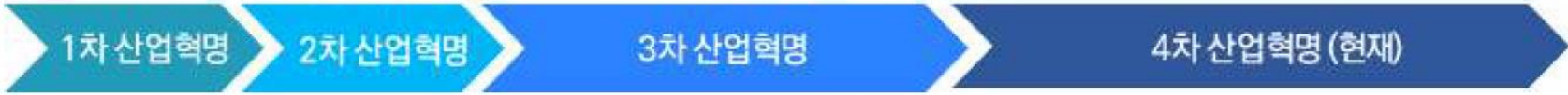
**South Korea
IDC Digital Transformation Awards 2018**

- DX Leader**
국자정보자원관리원
(National Information Resources Service)
- Operating Model Master**
현대차그룹 (Hyundai Motor Group)
LS산전 (LSIS)
- Information Visionary**
기아자동차 (KIA Motors)
- Omni Experience Innovator**
신한금융투자
(Shinhan Investment Corp.)
- Digital Disruptor**
뷰노(VUNO)

#IDCDXa
For more information, visit www.idcdxawards.com



IoT



디지털 트랜스포메이션 시대의 보안 고려사항



3rd Party(Supply Chain)



Digital Infa

II

최근 보안위협 동향



끝나지 않는 랜섬웨어 위협

피고 소환장:

09-CV-2018-323877.50

소송일시: 2018/09/5 10:11 KST

- 귀하는 고소를 당했습니다. -

귀하가 본 통지서를 받은 후 법원에 답변을 제출하고 다른 법적 조치를 취할 수 있는 28일이 남았습니다. -

허용된 시간 내에 회신을 해 귀하에 대한 심판이 진행될 수 있습니다. -

2019.3.18 세계최대 알루미늄 생산기업 랜섬웨어 감염, 생산차질 발생(출처 : BBC)

소환장을 여기에서 다운로드

*** 피고에게

KISA 인터넷침해사고 경보

2019.03.21. 13:26

- 위의 링크

- 피고가 출석
따르십시오.

자료실

보안공지

보고서

취약점 정보

가이드 및 매뉴얼

자료실

보안공지

보고서

취약점 정보

가이드 및 매뉴얼

보안공지

기업 대상 윈도우 서버를 공격하는 클롭(CLOP) 랜섬웨어 감염 주의 권고(2차)

2019.03.04

□ 개요

○ 마이크로소프트 윈도우 서버를 이용하는 제조물류 등의 기업 내부 시스템을 침투하여 특정 랜섬웨어(클롭, clop)를 감염시키는 공격이 지속적으로 발생함에 따라 오프라인 백업 등 기업 보안관리 강화 필요

랜섬웨어에 걸린 잭슨 카운티, 범인들에게 돈을 주기로 하다

떨어진 곳이다. 2018년
둘 다 표적 공격의 형태



이더센터 KrCERT/CC

홈 > 자료실 > 보안공지

제어망 위협 증가

MK 뉴스

"세계 최악의 '살인 해킹프로그램' 트리톤 사

입력 : 2019.03.07 16:36:35

2017년 사우디 석유화학공장 비상안전장치 공격 미수로 정
"고의로 직접 인명 피해를 노리는 점에서 전례 없는 악성프

지난 2017년 여름 해킹이 의심되는 사우디 아라비아의 한 석
보안 전문가 줄리언 것머니스는 피가 얼어붙는 느낌을 받

MIT
Technology
Review

Log in / Create an account Search Q



Topics+ The Download Magazine Events More+



MIT Technology Review
Global Panel

JOIN NOW

Connectivity

Triton is the world's most murderous malware, and it's spreading

The rogue code can disable safety systems designed to prevent catastrophic industrial accidents. It was discovered in the Middle East, but the hackers behind it are now targeting companies in North America and other parts of



2019

ARIEL DAVIS



5

ICS tailored malware families

- Stuxnet
- Havex
- Blackenergy 2
- Industroyer/Crashoverride
- Triton/Trisis

4

Malware intent to disrupt industrial processes

- Stuxnet
- Blackenergy 2
- Industroyer/Crashoverride
- Triton/Trisis

3

Successfully attacked

- Stuxnet
- Industroyer/Crashoverride
- Triton/Trisis

Scripts



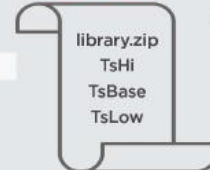
Triconex
Controller

TRITON

TriStation Communication

inject.bin
imain.bin

Masqueraded
Trilog Application
trilog.exe



SIS Engineering
Workstation




출처 : Dragos Inc

FireEye

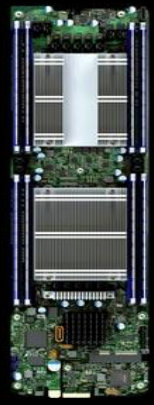
KISA

ICT 제품 신뢰성 위협

① A Chinese military unit designed and manufactured microchips as small as a sharpened pencil tip. Some of the chips were built to look like signal conditioning couplers, and they incorporated memory, networking capability, and sufficient processing power for an attack.



② The microchips were inserted at Chinese factories that supplied Supermicro, one of the world's biggest sellers of server motherboards.



스파이 칩???



5G 백도어???



국가 배후 의심 해커조직 위협 확대

BREAKOUT TIME BY ADVERSARY FOR 2018

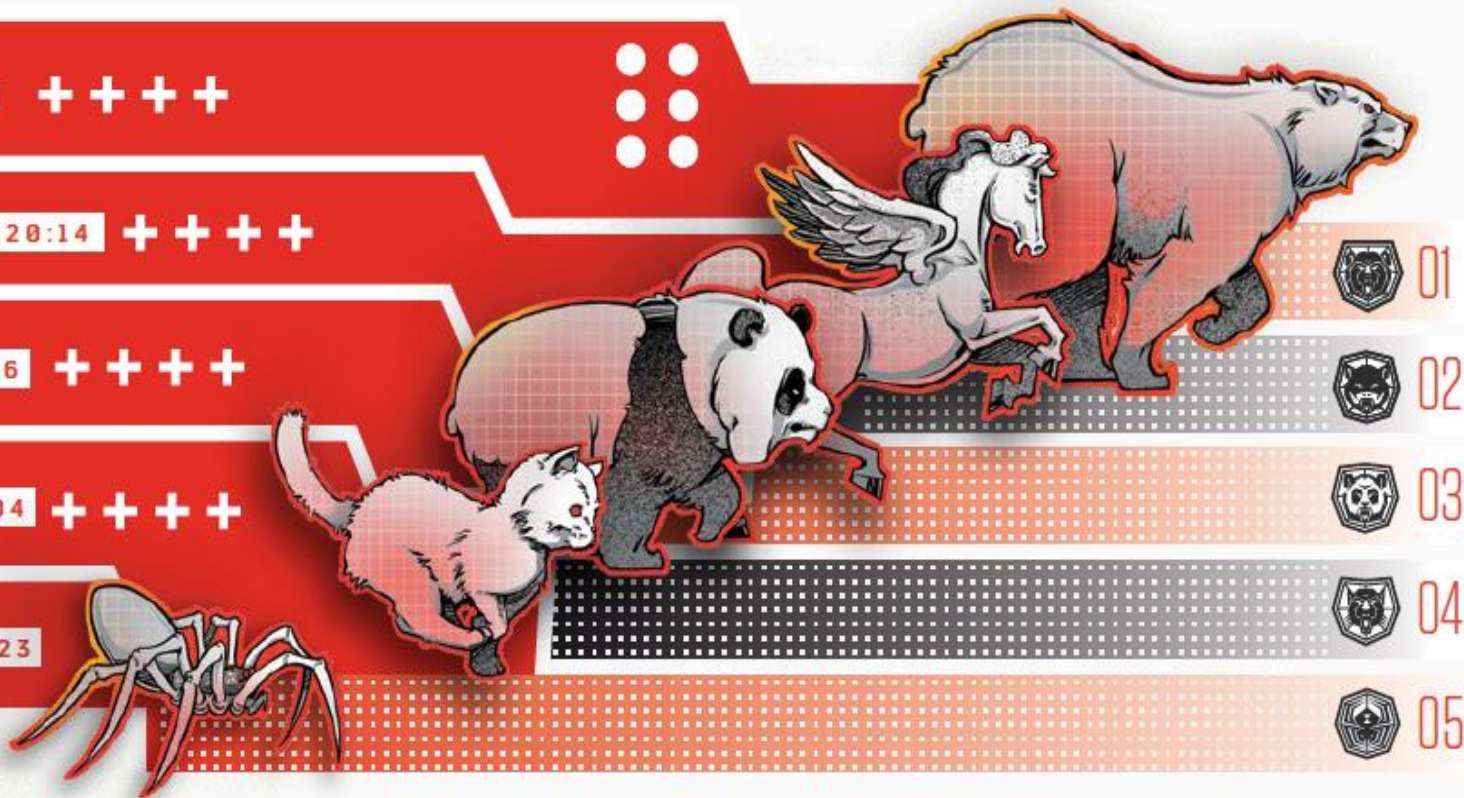
BEAR 00:18:49 + + + +

CHOLLIMA 02:20:14 + + + +

PANDA 04:00:26 + + + +

KITTEN 05:09:04 + + + +

SPIDER 09:42:23



[Source : CrowdStrike, 2019 Global Threat Report]

국가간 사이버 분쟁 심화



美 닐슨장관 "北·中·러 해커, 美 선거개입 등 중대 위협"

류강훈 기자 | hooney0405@newsis.com

등록 2019-03-19 04:53:34



【워싱턴=AP/뉴스시스】 키어스틴 닐슨 미 국토안보부 장관이 18일(현지시간) 미국은 북한, 러시아, 중국 등 다른 나라의 지원을 받는 해커들을 다룰 준비가 돼있지 않은 만큼 사이버공격에 맞서 싸울 전 사회적인 태세를 갖춰야 한다고 촉구했다. 2019.03.18



III

향후 대응방안



무엇이 문제가 될 수 있는가?

공급망 문제

Supply Chain Management

자재공급망관리(SCM)을 통해 기업 간 전자거래망 구축이 가능하며, 바코드 물류관리를 통해 표준화 납품명세서를 기준으로 전사적 구매/자재 업무를 지원하는 서비스입니다.



Maintenance



네트워크 신뢰 문제

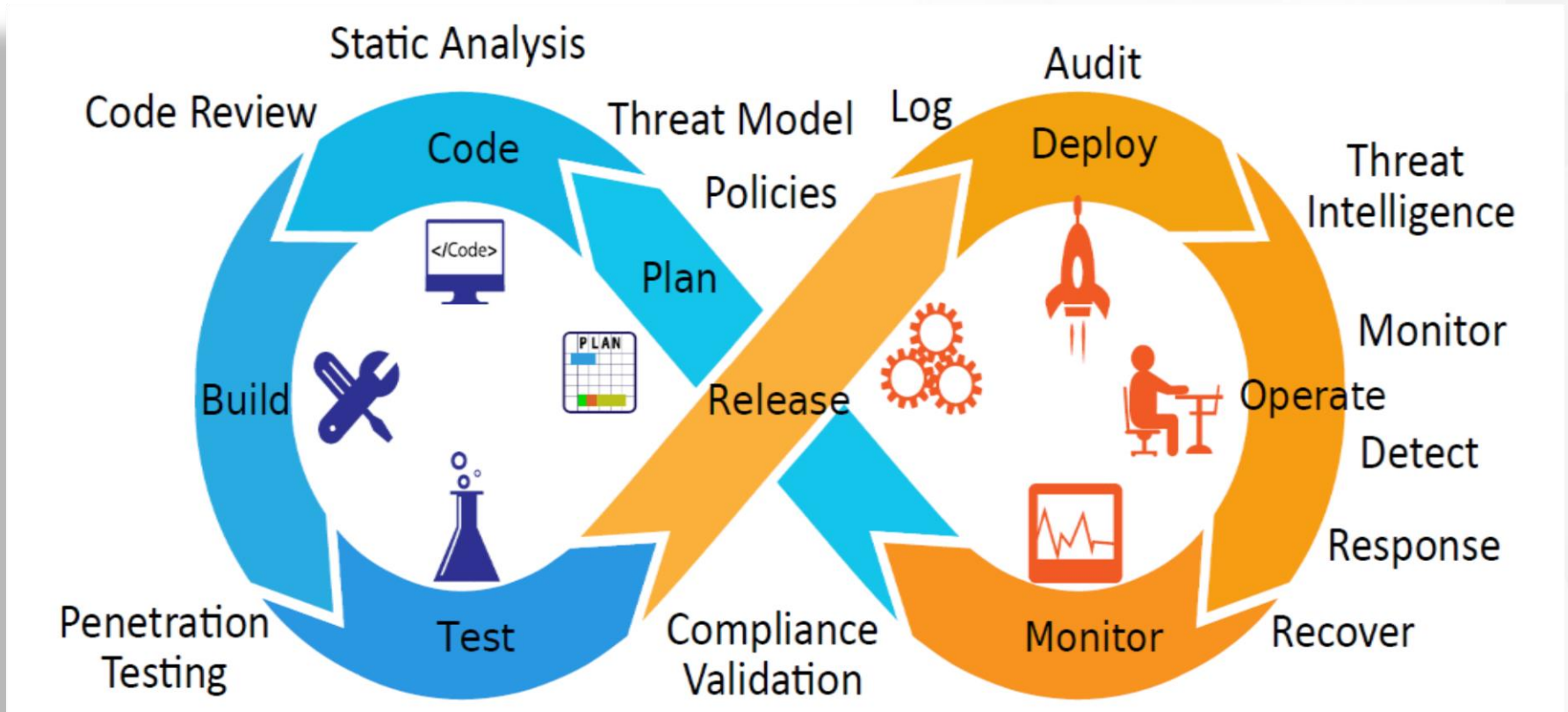


가시성 문제



대응방안 - 함께 하는 보안

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



대응방안 - 접근통제에 대한 재설계



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

대응방안 - 사각지대 제거



단순 보안로그
모니터링만으로는 대응 한계



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

* KISA 사이버 위협정보 분석· 공유(C-TAS) 활용
https://www.krcert.or.kr/data/noticeView.do?bulletin_writing_sequence=25824

감사합니다

