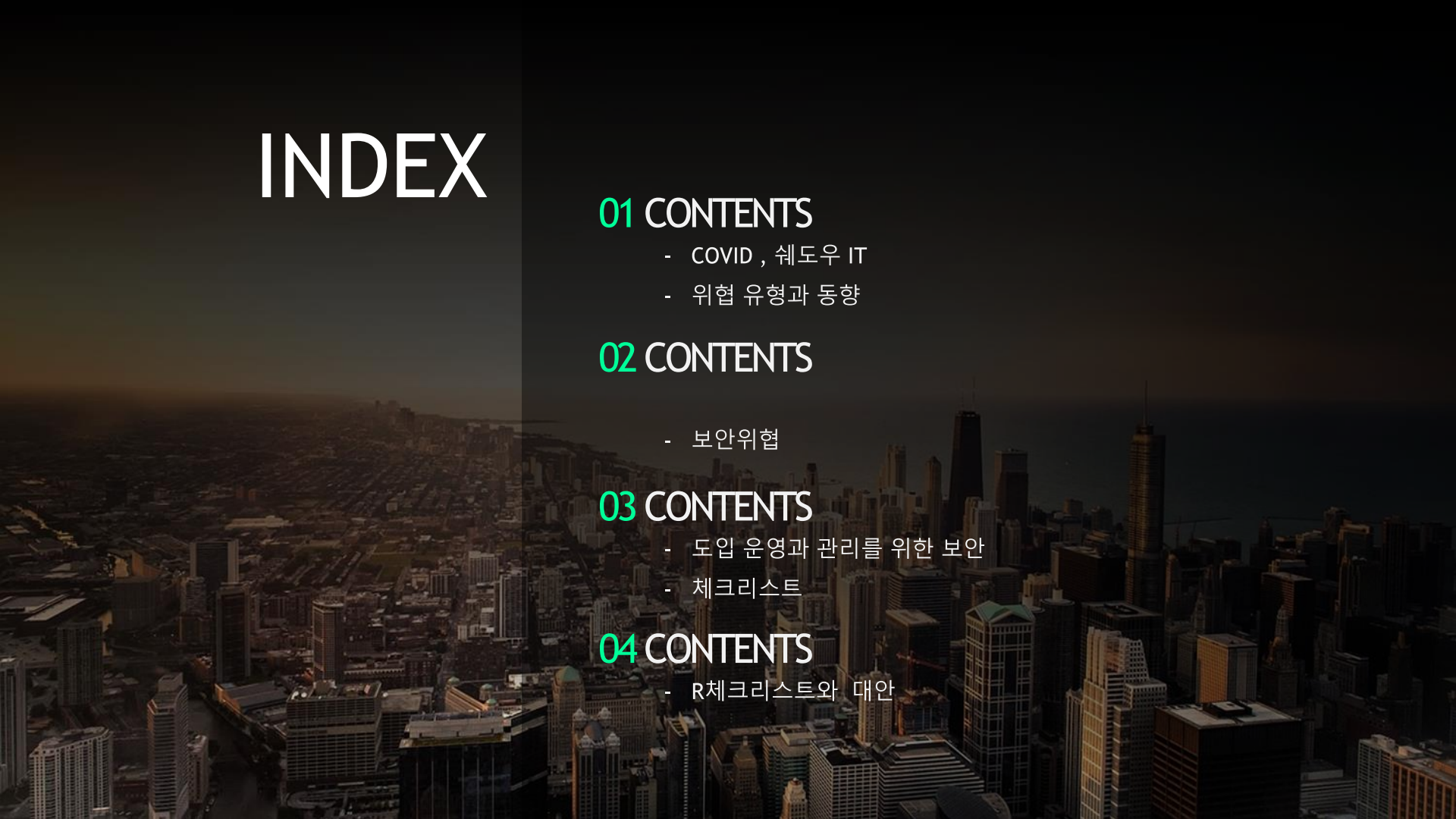
COVID19 보안 Issue 동향

2020.7

KSJ 박수곤



INDEX

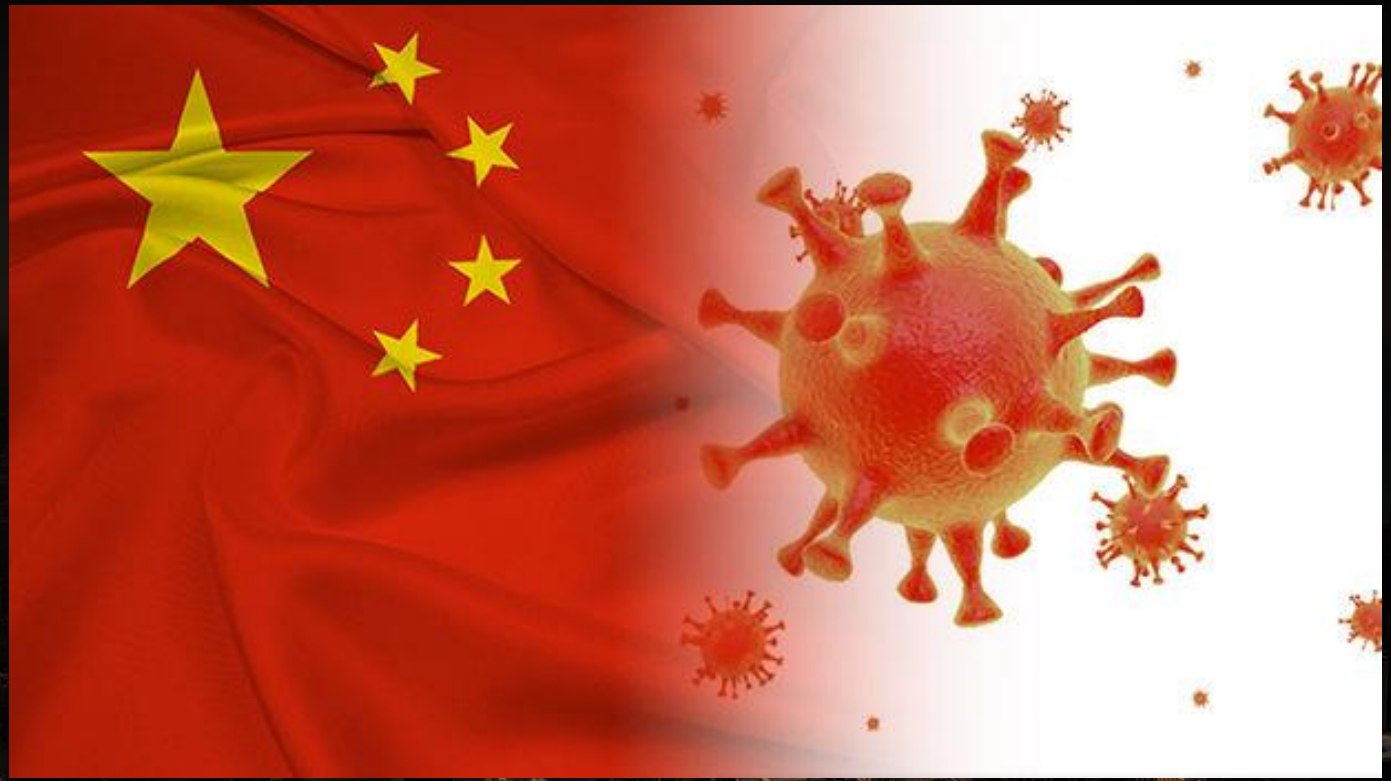
1. 개요

COVID-19

위협 유형과 동향

1. COVID

1. COVID

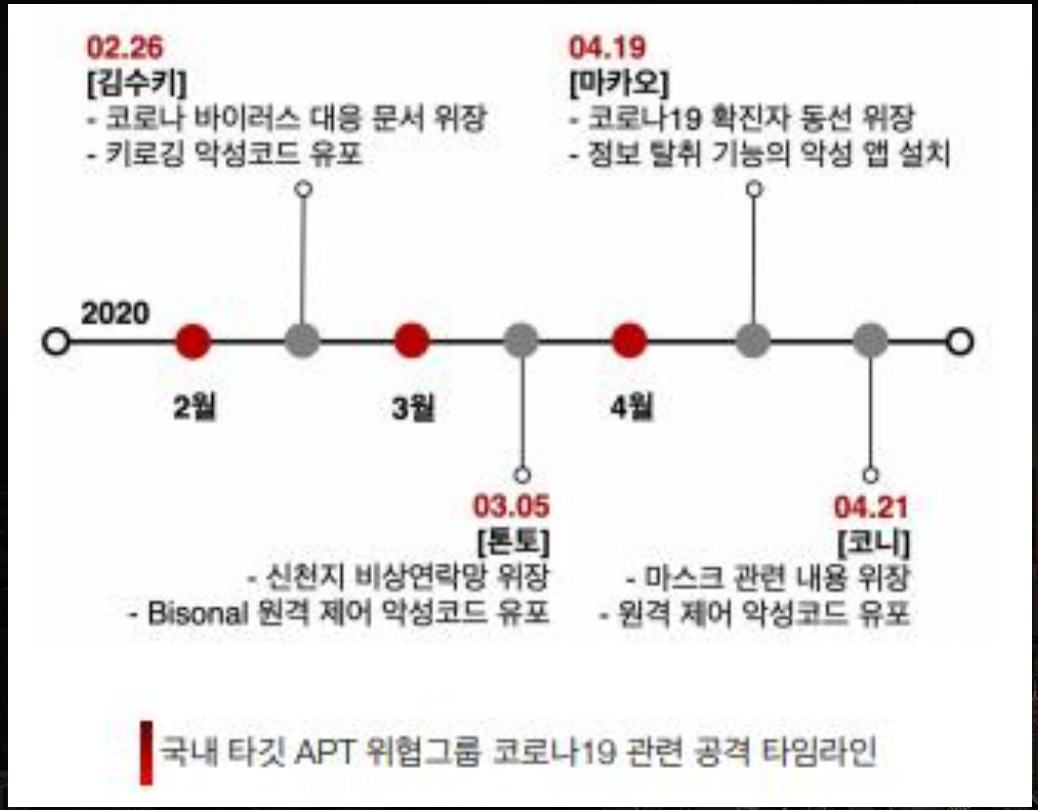


1. 공격 유형

코로나 바이러스가 전세계적으로 유행하면서
사이버 공간에서도 관련 위협이 지속되고 있다.

Apt 위협 그룹들을 포함한 다양한 공격자들이
이슈를 적극적으로 활용하고 있다.

1. 공격 유형


02.26
[김수키]
- 코로나 바이러스 대응 문서 위장
- 키로깅 악성코드 유포
04.19
[마카오]
- 코로나19 확진자 동선 위장
- 정보 탈취 기능의 악성 앱 설치
2020
2월
3월
4월
03.05
[톤토]
- 신천지 비상연락망 위장
- Bisonal 원격 제어 악성코드 유포
04.21
[코니]
- 마스크 관련 내용 위장
- 원격 제어 악성코드 유포
국내 타깃 APT 위협그룹 코로나19 관련 공격 타임라인

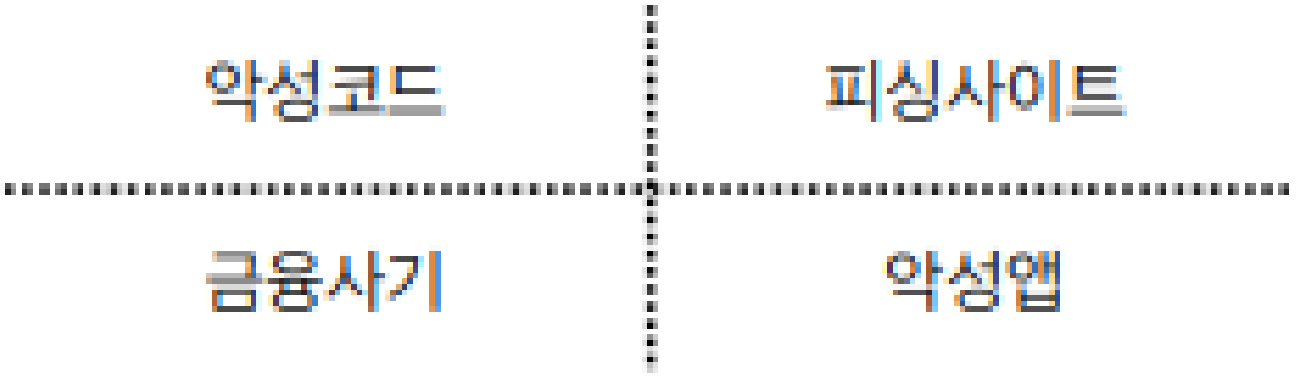
1. 공격 유형

공격자들이 주로 사용한 공격은 사회공학적 기법인 피싱 공격이며

공격 대상에 따라 악성코드, 피싱사이트 , 금융사기, 악성 앱 유포와

같은 기존 침해사고와 비슷한 형식으로 식별 분류할 수 있다.

1. 공격 식별 분류



코로나19 관련 사이버위협 유형 4가지

1. 쉐도우 IT

쉐도우 IT

그러나 이 중 대다수는 기업 IT 부서가 직접 개발하거나 관리하는 공식 서비스가 아니다.

직원들이 IT 부서에서 승인하지 않은 클라우드 애플리케이션이나 서비스를 구입하고,

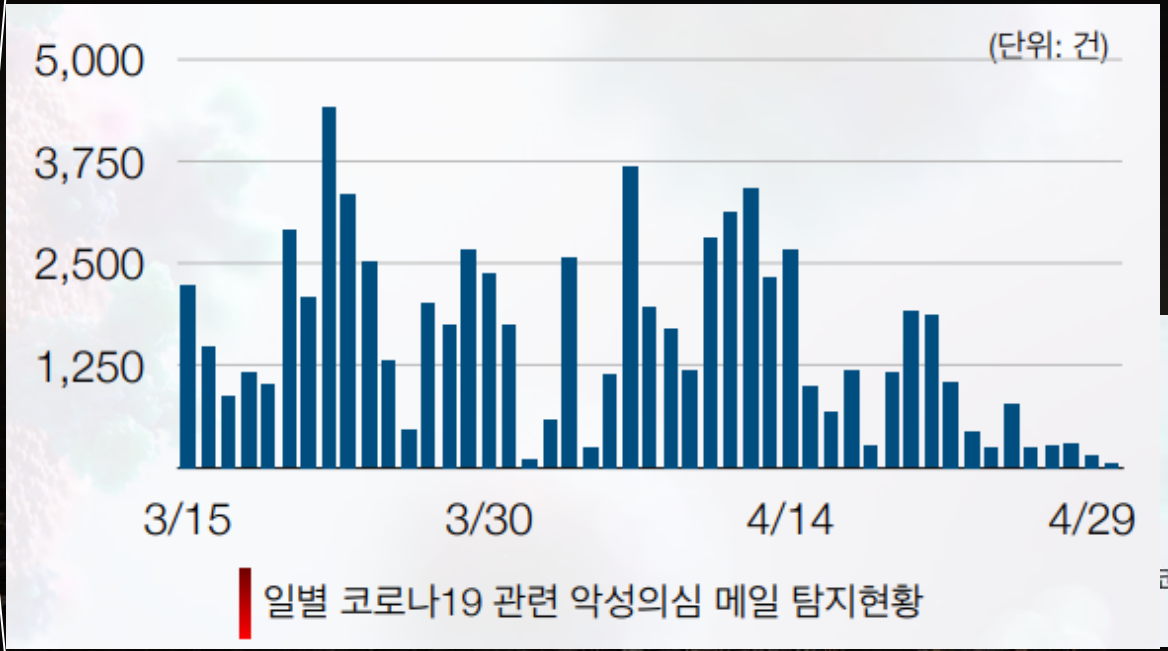
이를IT 관리 부서나 책임자가 파악하지 못하는 현상을 가리켜 섀도우 IT(Shadow IT)라 통칭

1. 위협 동향

코로나 19의 확산과 더불어 관련 침해위협이 대폭 증가하였으나
공격기법이나 유형들은 큰 변화를 보이지 않고 있다.

또한 코로나 19로 인한 화상회의와 원격근무등이 변화됨에 따라 주의가 필요하다.

1. 위협 동향



일별 코로나19 관련 악성의심 메일 탐지현황

코로나19 관련 키워드 포함 악성의심 메일 탐지현황

2. CONTENTS

보안과 위협

2. 보안과 위협


4차 산업혁명이란 무엇인가?
파괴적 기술과
역사적 산업혁명의 전개
4차 산업혁명
IoT
로봇
AI
3D 프린팅
AR/VR
AI 기술을 핵심동인으로
상품·서비스의 생산·유통·소비 전 과정에서
모든 것이 연결되고 지능화
3차 산업혁명
컴퓨터·인터넷
20세기 후반
2차 산업혁명
전기·내연기관
19-20세기
1차 산업혁명
증기기관
18세기

2. 보안과 위협

이슈 사항

코로나

쉐도우IT

재택근무

망분리

2. CASE1

악성코드 실행 시 위장용으로 실행되는 ppt 파일

2. CASE2

Face masks are only recommended for those who are taking care of a person with suspected COVID-19 infection.

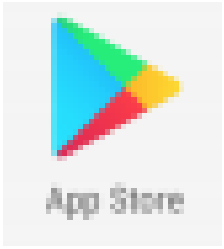
Best Type: N95 particulate respirator, without respiration valve

Specification

WHO standard

코로나19 마스크 관련 내용으로 위장한 문서

2. CASE3



긴급재난상품권 관련 스미싱 사례

1. CONTENTS

보안 ?

예산 삭감 , 사이버 위협 노출 증가 , 보안운영 가중도 상승

(원격 근무, 영상회의) = AKA. 비대면 업무 환경

(규제) 해외와 국내의 차이 = 중요도

2. 보안위협

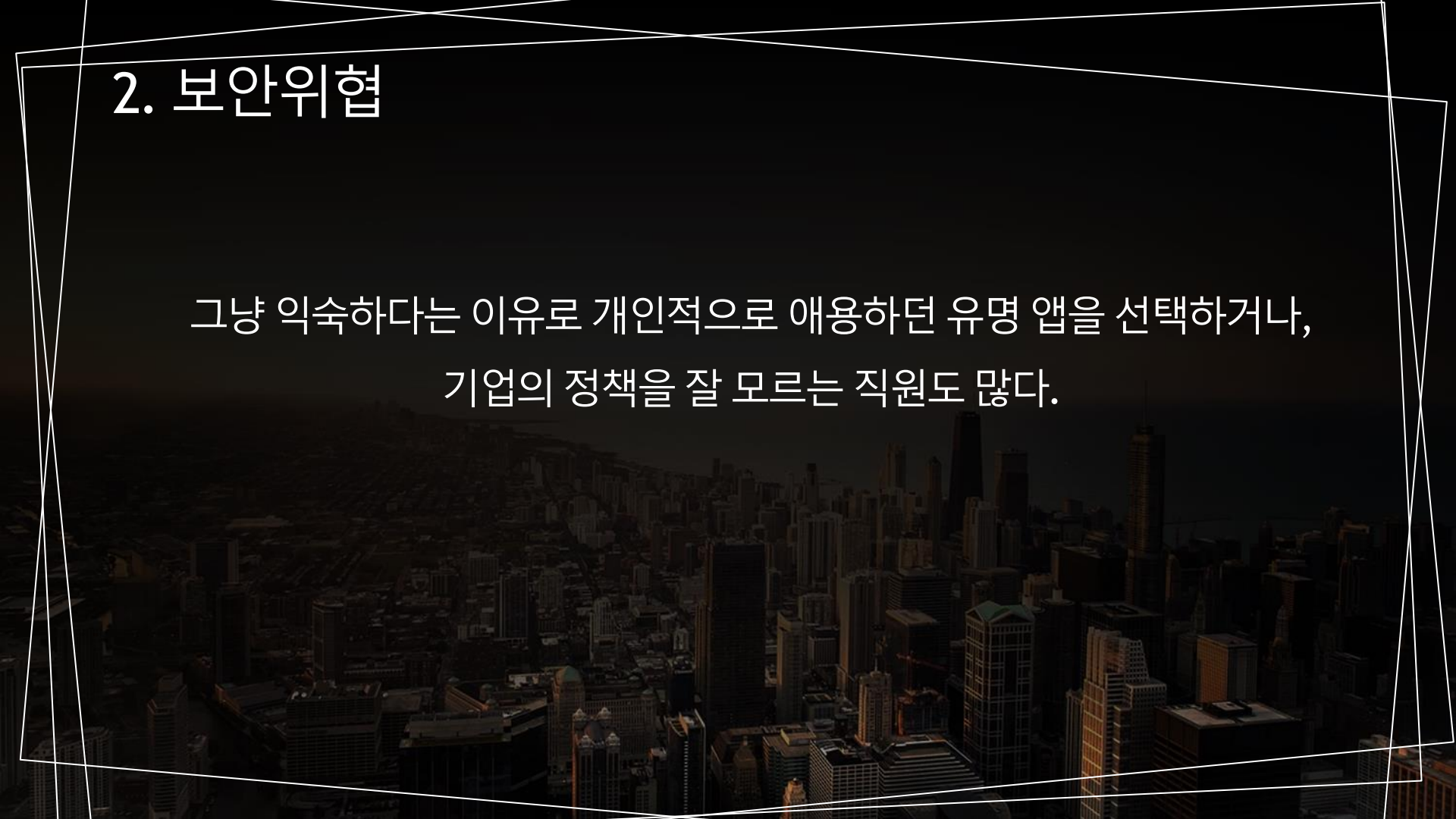
우선 각 부서 실무자들이 중앙 IT 부서를 통하지 않고도

직접 컴퓨팅 자원과 서비스를 간편하게 사용할 수 있게 된
환경 변화가 큰 요인이다.

또한, 기업의 공식 앱이나 프로세스가 느리고 비효율적이며
원하는 기능을 제공하지 않는다.

2. 보안위협

그냥 익숙하다는 이유로 개인적으로 애용하던 유명 앱을 선택하거나,
기업의 정책을 잘 모르는 직원도 많다.



2. 보안위협

또, 기업의 공식 앱이나 프로세스가 느리고 비효율적이며
원하는 기능을 제공하지 않기 때문이기도 하다.

그냥 익숙하다는 이유로 개인적으로 애용하던 유명 앱을 선택하거나,
기업의 정책을 잘 모르는 직원도 많다.

2. 보안위협

이러한 사항은 그 자체로 기업의 비용으로 작용한다.
우선 정식 관리자가 아닌 직원들이 데이터를 다루고
재확인할 때 낭비되는 시간이 크다.

2. 보안위협

관련 데이터가 제때 업데이트되지 않을 때도
데이터 일관성이 손상되고 오류가 일어날 수 있다.

IT 자원이 기존 공식 인프라와 중복된 상태로 존재하면
효율적인 기업 IT 전략과 프로세스 수립을 방해할 수도 있다.

2. 보안위협

디바이스와 애플리케이션 사용에 있어
효율과 편의성 등을 이유로 IT 보안 부서의
관리 범위를 벗어난 경우가 증가하고 있다.

이러한 현상은 사이버 보안 위협 노출과 새로운 취약점의 등장 등
보안 문제를 가져왔습니다.

2. 보안위협

이러한 현상은 사이버 보안 위협 노출과 새로운 취약점의 등장 등
보안 문제를 가져왔다.

3. CONTENTS

도입 운영을 위한 보안

체크리스트

3. 도입 운영을 위한 보안

패치 관리 솔루션

문서 중앙화 솔루션

EDR

3. 체크리스트

한눈에 파악할 수 있는 위협 가시성 확보

운영 리소스 최소화 및 근본적인 대응을 위한 보안장비 연동

보안 전문성을 보완하는 표준 체계 형태의 위협 인텔리전스 제공

3. R

출처 : http://it.chosun.com/site/data/html_dir/2016/03/14/2016031485042.html

출처: https://blog.alyac.co.kr/2813

출처 : 코로나 19 금융부문 사이버 위협 동향 _ 금융보안원

출처 :

https://www.kisa.or.kr/covid19/main.jsp?fbclid=IwAR3A2jxUT6z6UirpIKxV9_fqjjHn5DXumF8v51XhatYEuKcmhVNzz4WZn1k

https://www.boannews.com/media/view.asp?idx=87471&fbclid=IwAR0eYmYf3RbKw5XnfX-CSD88ynmnkeSDEKsp-HoDQ3eStouq9KZ1Z7u1WeE


Q&A


THANK YOU