이메일, 당신을 속이는 4가지 기법

프루프포인트 코리아
Sr. Account Manager 최윤환

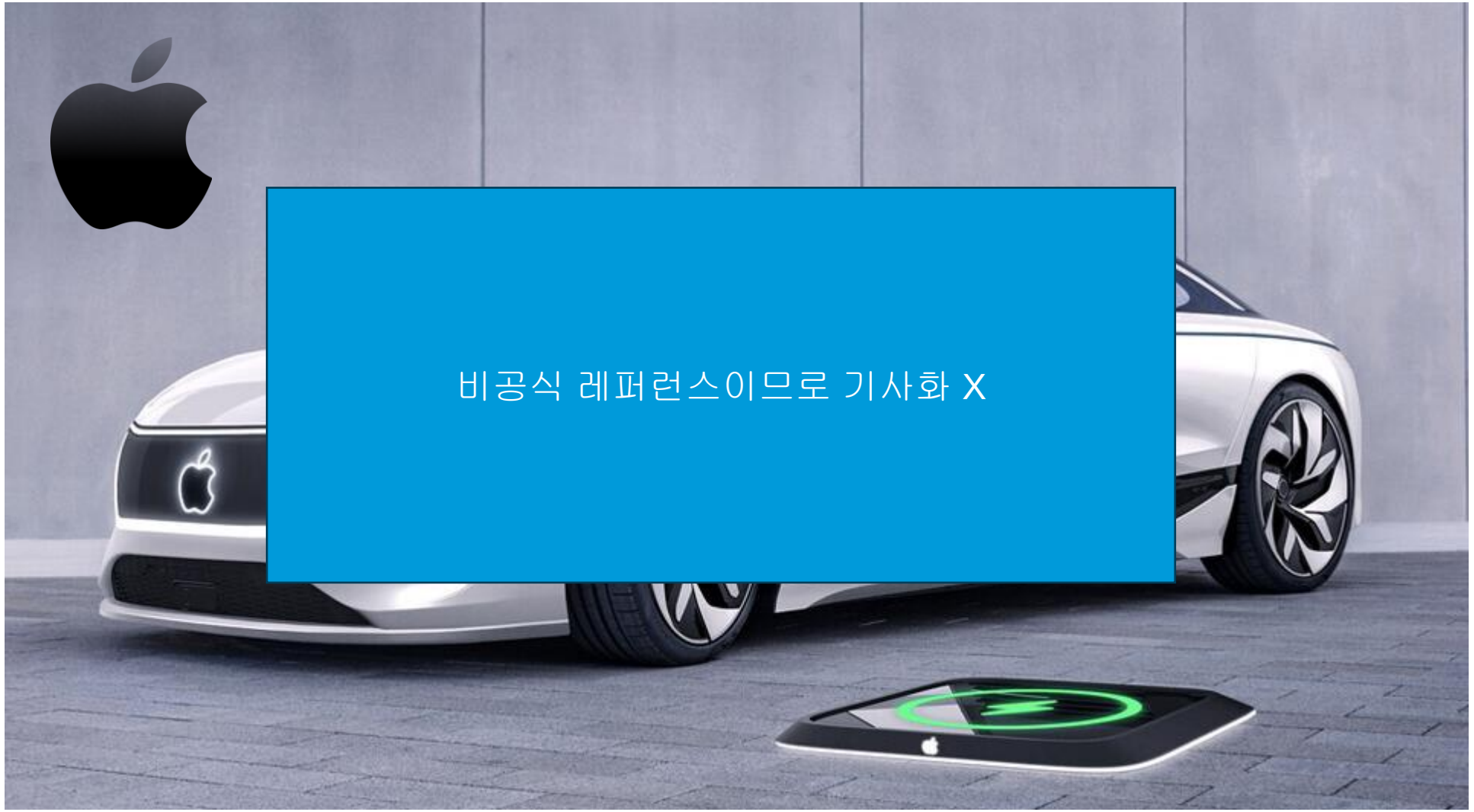
목차

01

Proofpoint 소개

이메일, 당신을 속이는 4가지 기법

1. Proofpoint 소개



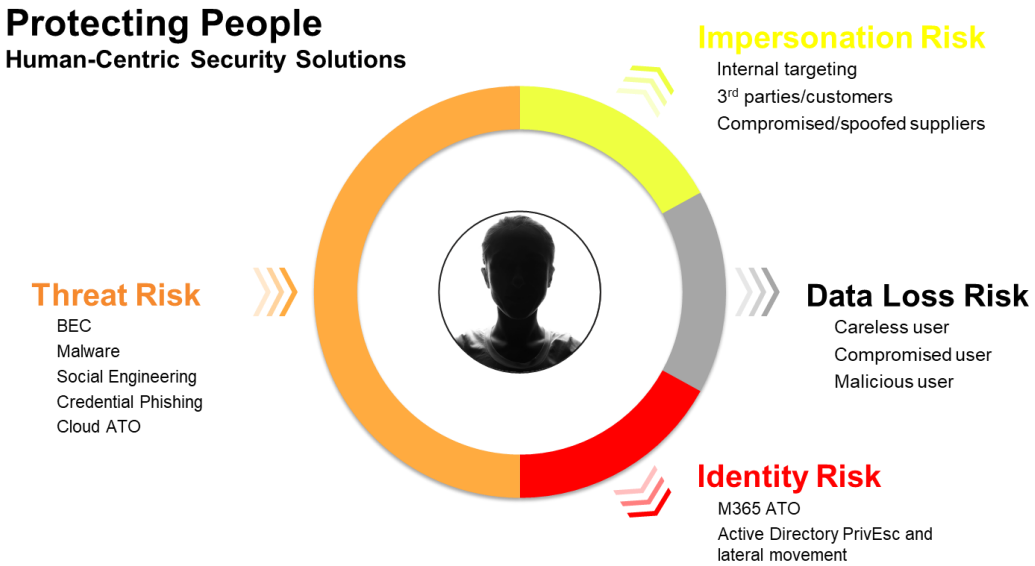
1. Proofpoint 소개

1. Proofpoint 소개

구분	내용
회사명	프루프포인트 코리아 유한회사
설립일	2002년 6월
CEO	Sumit Dhawan
본사	미국 캘리포니아 서니베일
임직원 수	약 4,000 명 (2024년 1월 기준)
매출액	2023년(E): 18억 달러 (한화 약 2조 4천억 원)
주요제품	E-mail Security (이메일사기, 첨부파일/URL, TI, Retro Active, Isolation) Security Awareness Training (모의훈련, 임직원 보안교육) Insider Threat Management (내부자 모니터링/위협관리) Identity Threat Detection (계정 위협 탐지/대응)
한국지사 주소	서울특별시 강남구 테헤란로 507 WeWork 13F

- ✓ **23년차 미국 보안회사**
- ✓ **세계 1위 이메일보안**
- ✓ **Human Centric 보안**

1. Proofpoint 소개



사이버공격의 74%는 '인간'의 취약점을 이용함

*Source: Verizon 2023 Data Breach investigations report

Human-targeted email
#1 vector for initial compromise

Human identities
#1 vector for privilege escalation, lateral movement

Human actions
#1 vector for data loss

proofpoint.

02

BEC 란?

이메일, 당신을 속이는 4가지 기법

2. BEC 란?

BEC(Business Email Compromise):

공격자가 기업을 대상으로 하는 **사이버 범죄인 이메일 '사기'**입니다.

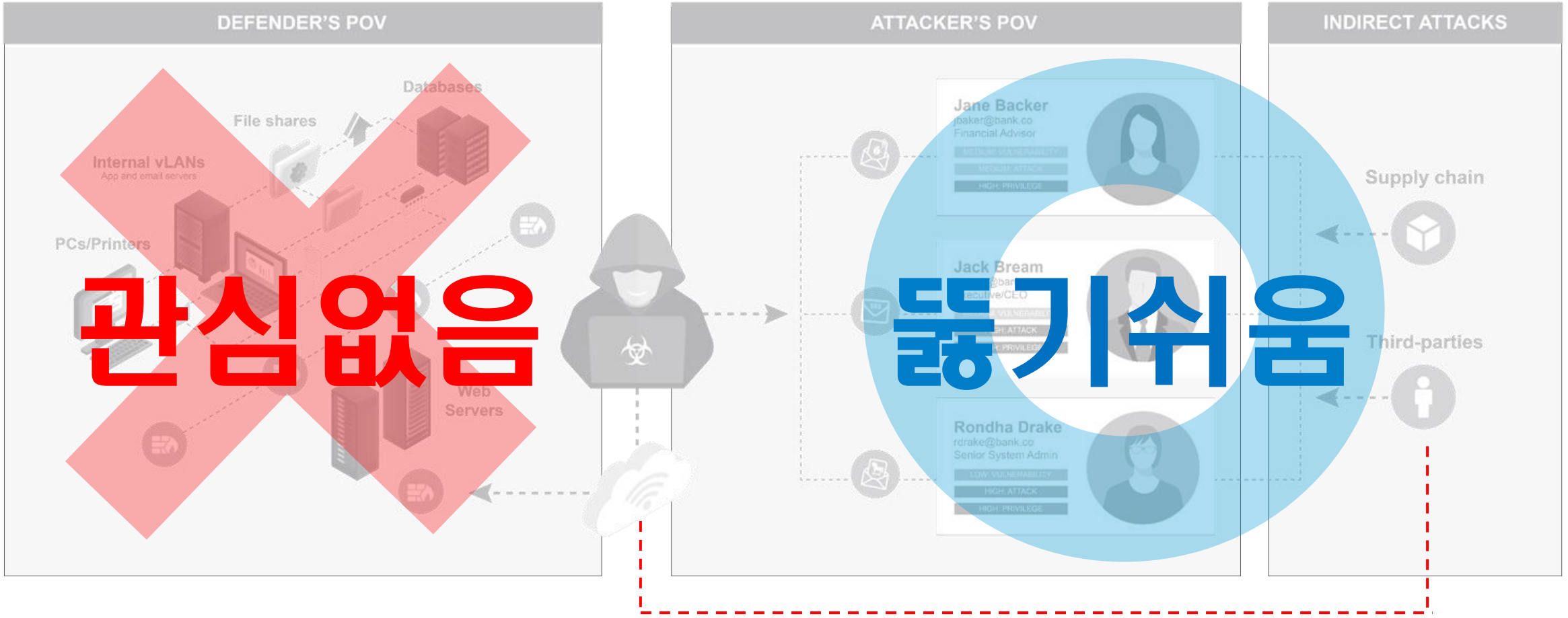
BEC는 전 세계적으로 피해 규모가 매우 크고 모든 규모의 조직을 대상으로 증가하고 있습니다.

BEC는 **악성 첨부파일, URL 없이 이메일 본문 내용만으로도 피해**를 입을 수도 있습니다.

따라서 기존의 이메일 보안솔루션이나 Endpoint 보안 솔루션으로 탐지하고 대응하기 어렵습니다.

"인류의 원초적인 사기 범죄 행위의 사이버화된 유형 "

2. BEC 란?



"해커들은 더 이상 복잡한 **인프라**를 직접 뚫으려 하지 않고, **사람**을 통해 공격"

proofpoint.

2. BEC 란?

3조원

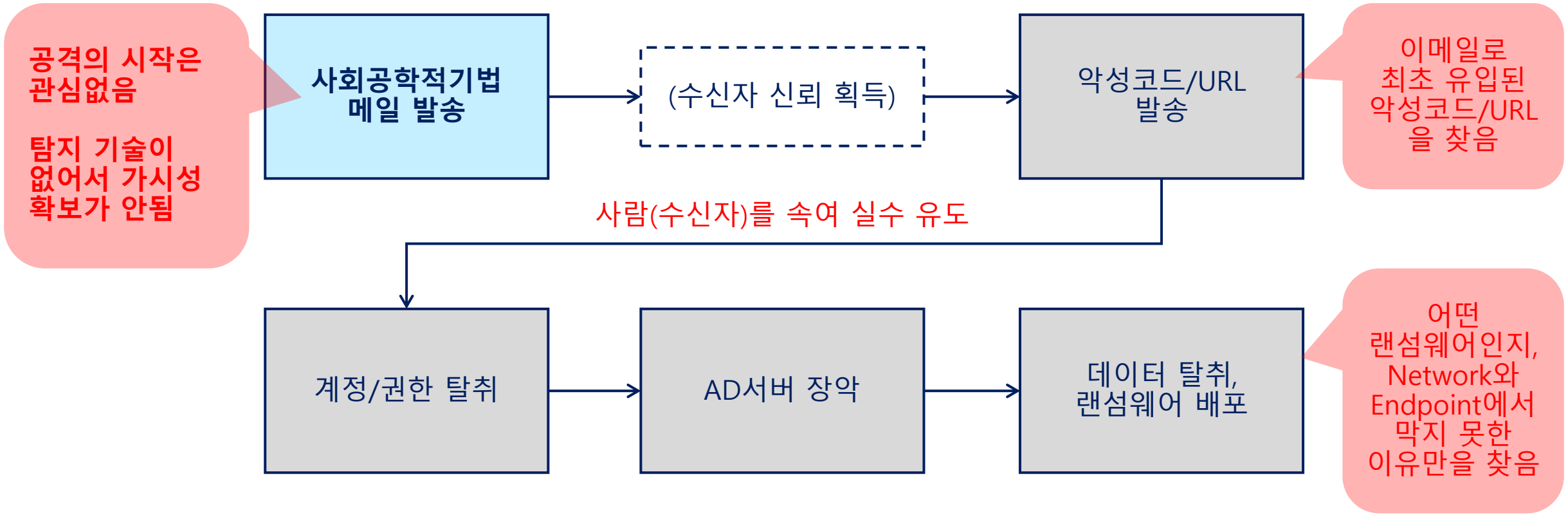
2021년 이메일 사기로 인한 피해금액

Internet Crime Report- The FBI

*Source: Internet Crime Report, FBI, 2022

2. BEC 란?

우리나라에서 BEC공격을 탐지하기 어려운 이유



"일반적으로 기업의 보안은 ***악성코드, URL 관점에서만 대비하기 때문"***

proofpoint.

2. BEC 란?

해킹 그룹 Scattered Spider

*Source: techwireasia

피싱 공격으로 계정탈취 후 임직원으로 위장하여

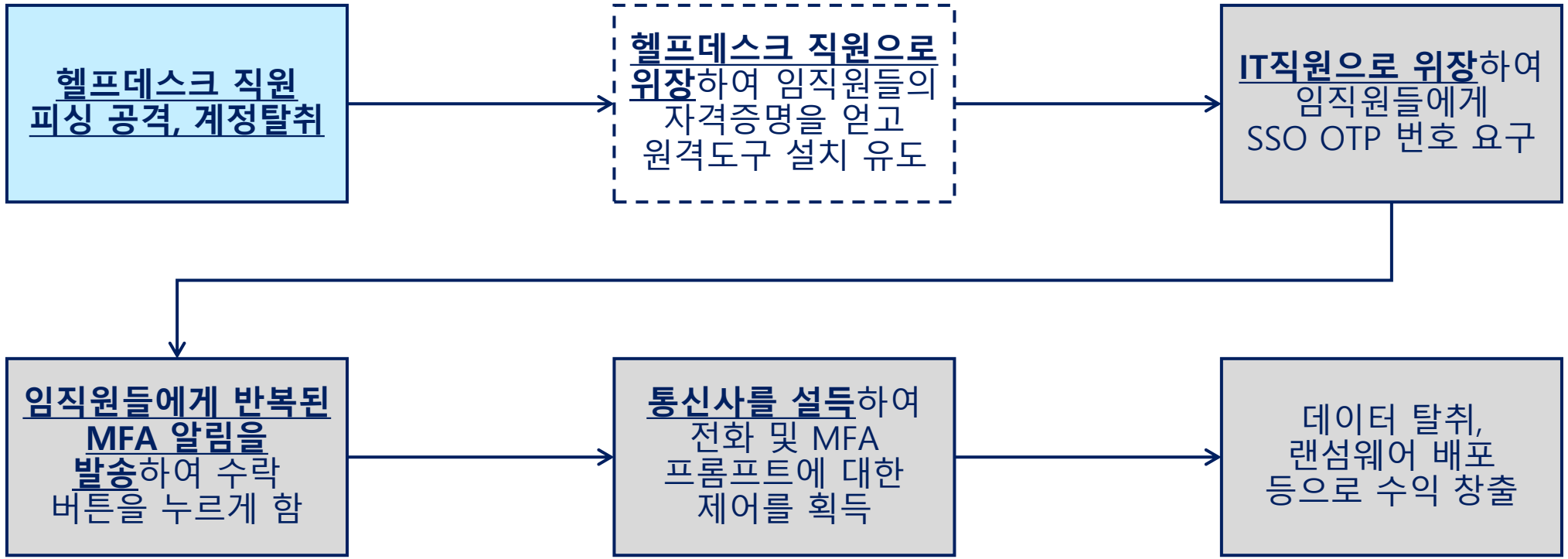
클라우드/온프렘 인프라에 침투하는 새로운 공격기법을 사용하는 범죄그룹

proofpoint.

2. BEC 란?

Scattered Spider -> MGM 공격 Case (1,300억원 피해 예상)

*Source: Reuters, Oct 2023



*Source: CISA.gov, Nov 2023

"피싱으로 인한 계정탈취 이후에 공격을 막기가 쉽지 않음"

proofpoint.

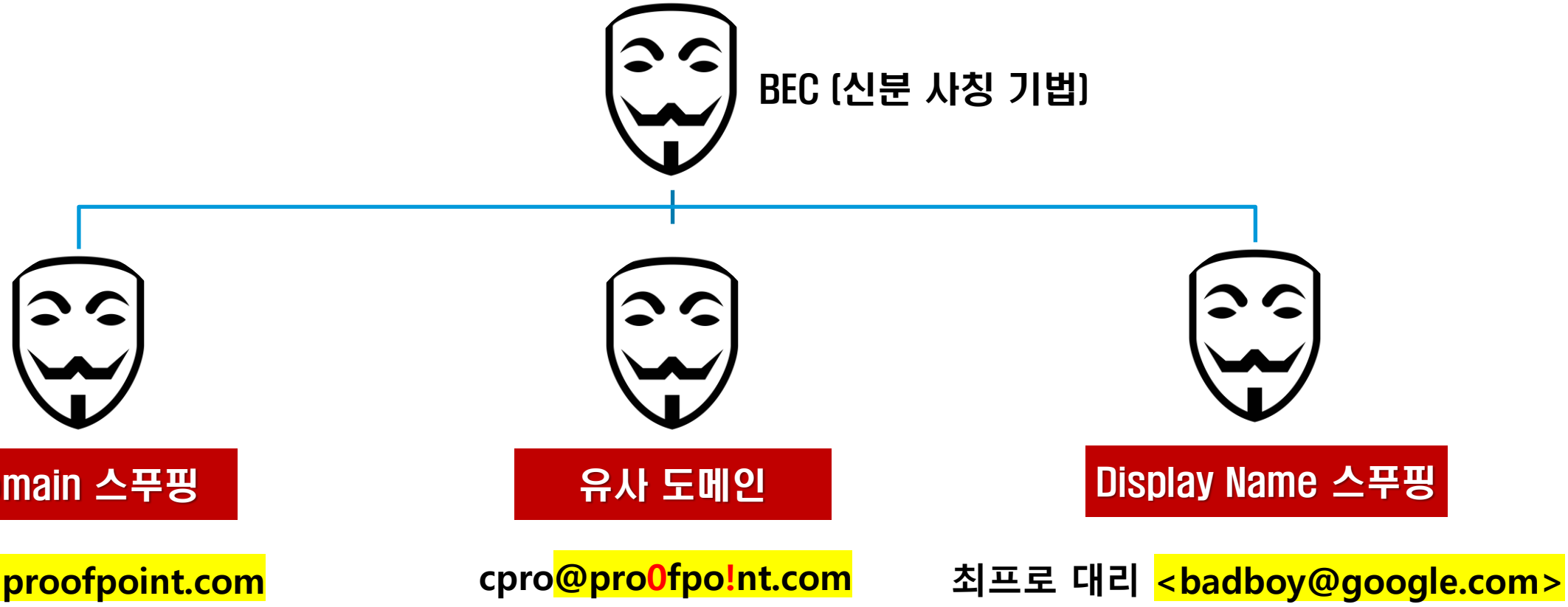
03

BEC 공격 4가지 기법

이메일, 당신을 속이는 4가지 기법

3. BEC 공격 4가지 기법

신분 사칭 기법



3. BEC 공격 4가지 기법

메일 텍스트로 속이기

*Source: Istock

![긴급요청] 결제 계좌 변경 및 대금 지급 요청

보낸 사람 : 김프로 대리<kpro@profpoint.com>

받는 사람 : 최프로<cpro@xxx.co.kr>

첨부 파일 : 없음

안녕하세요 최프로님,
프루프포인트 김프로입니다.

잘 지내고 계신지요?
다름이 아니라 저희 회계부서로부터 긴급하게 요청 받아서 메일 드립니다 .

저희 쪽 세금 신고 문제로 인해서
금번 대금 지급을 아래 계좌로 변경하여 진행 부탁드립니다.
그리고 저희가 긴급히 세금 신고 마감 처리를 해야 되서
가급적 대금 지급을 오늘 중으로 처리 해주시기 바랍니다.

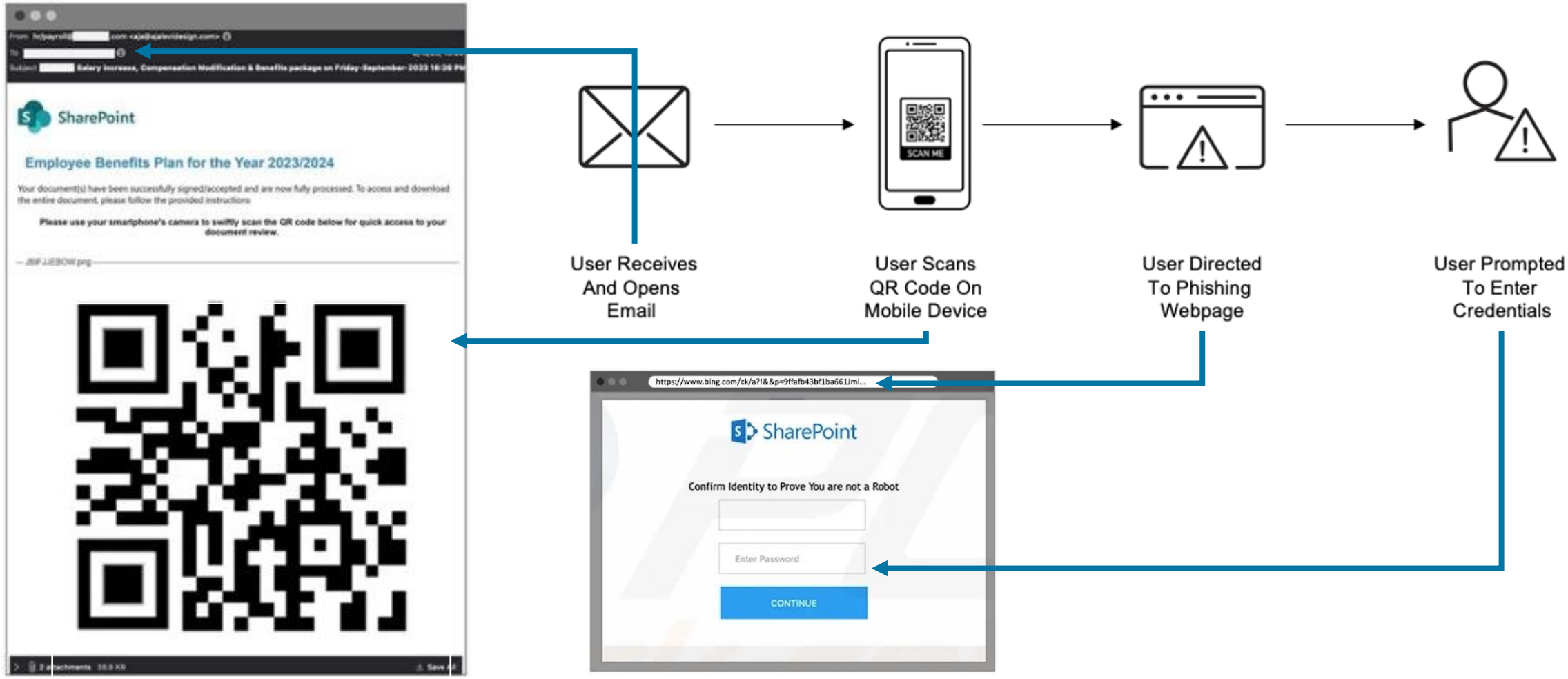
ABC Bank : 123-456-789999

감사합니다.

김프로 드림
Proofpoint

3. BEC 공격 4가지 기법

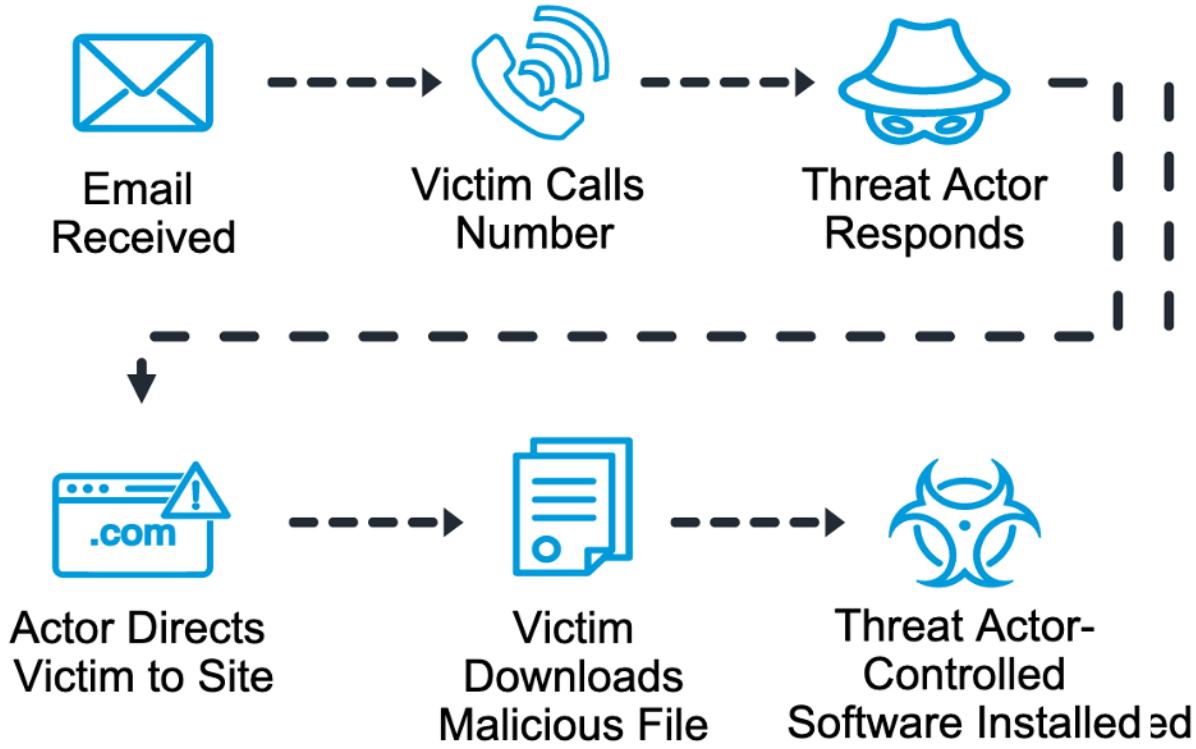
Quishing: Phishing using QR (Quick Response) codes



3. BEC 공격 4가지 기법

TOAD (Telephone-Oriented Attack Delivery)

음성통화와 이메일 피싱기술을 결합한 새로운 피싱 공격.
해커는 신뢰할 수 있는 기관을 사칭하여 수신자를 속이고
전화를 통해 로그인 자격증명, 금융데이터 등 민감정보를 오픈하도록 유도함. 이후 피싱링크 및 첨부파일을 통해 악성코드 공격 수행.



04

BEC 공격 대응

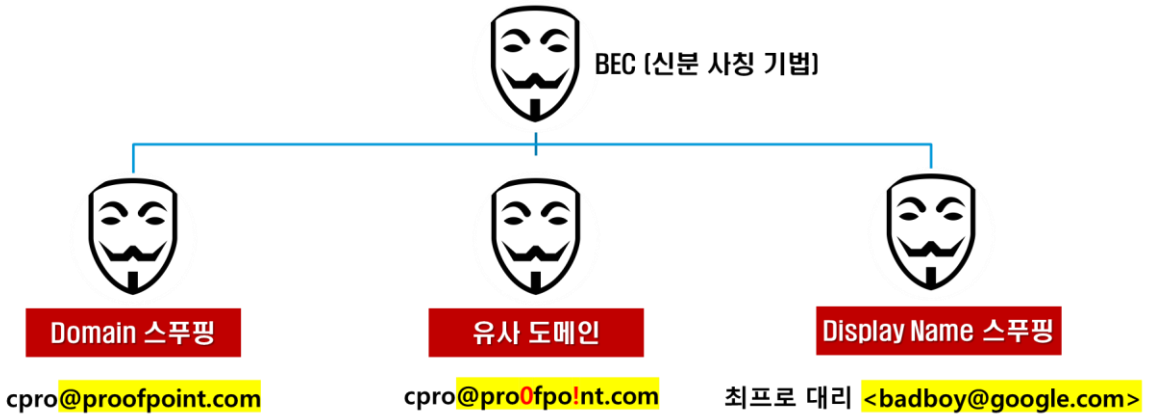
이메일, 당신을 속이는 4가지 기법

4. BEC 공격 대응

신분 사칭 기법

- DMARC 확인 절차를 통해 도메인 스푸핑 방지
- 도메인 평판 관련 인텔리전스 보유

"코스피 200 기업 중 99%가 DMARC 검역 설정을 하지 않음 "



4. BEC 공격 대응

메일 텍스트로 속이기

- 제목, 본문에 대한 구문 분석 기술 보유
- 계좌번호 식별 기술 보유

"첨부파일, URL 이 아닌 메일 제목과 본문 텍스트를 분석하는 기술 미흡 "

*Source: Istock

![긴급요청] 결제 계좌 변경 및 대금 지급 요청

보낸 사람 : 김프로 대리<kpro@profpoint.com>

받는 사람 : 최프로<cpro@xxx.co.kr>

첨부 파일 : 없음

안녕하세요 최프로님,
프루프포인트 김프로입니다.

잘 지내고 계신지요?
다름이 아니라 저희 회계부서로부터 긴급하게 요청 받아서 메일 드립니다 .

저희 쪽 세금 신고 문제로 인해서
금번 대금 지급을 아래 계좌로 변경하여 진행 부탁드립니다.
그리고 저희가 긴급히 세금 신고 마감 처리를 해야 되서
가급적 대금 지급을 오늘 중으로 처리 해주시기 바랍니다.

ABC Bank : 123-456-789999

감사합니다.

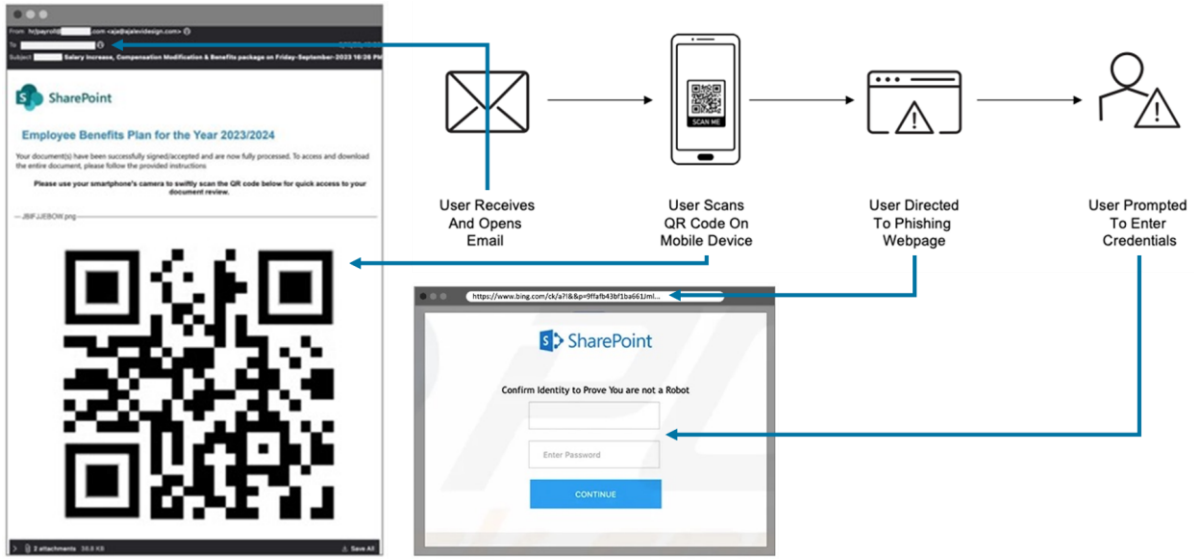
김프로 드림
Proofpoint

4. BEC 공격 대응

Quishing: Phishing using QR (Quick Response) codes

- QR코드 스캔 및 탐지기술 보유

"QR코드는 레거시 보안인프라를 우회할 수 있음 "



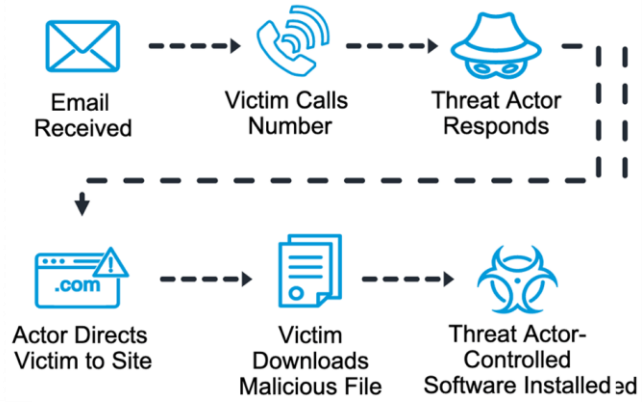
4. BEC 공격 대응

TOAD (Telephone-Oriented Attack Delivery)

- 다양한 BEC 공격 대응 기술 보유
- 임직원 대상 정보보안 교육

"보안 인프라 외적인 환경으로 공격하는 방법은 솔루션으로 방어가 어려움 "

음성통화와 이메일 피싱기술을 결합한 새로운 피싱 공격. 해커는 신뢰할 수 있는 기관을 사칭하여 수신자를 속이고 **전화를 통해 로그인 자격증명, 금융데이터 등 민감정보를 오픈하도록 유도함**. 이후 피싱링크 및 첨부파일을 통해 악성코드 공격 수행.



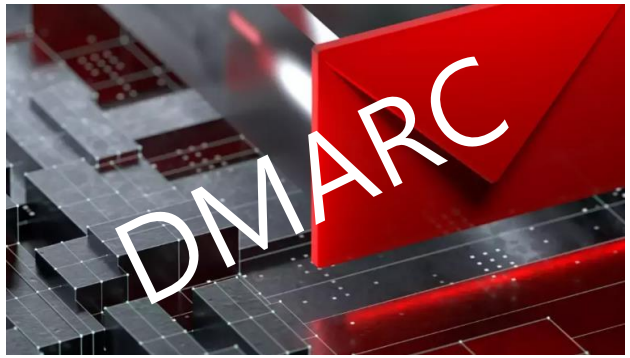
4. BEC 공격 대응

새로운 관점에서 준비 필요

[BEC 공격에 대한 가시성 확보]

- BEC 공격대응 기술/솔루션 보유

[DMARC 정책 설정]



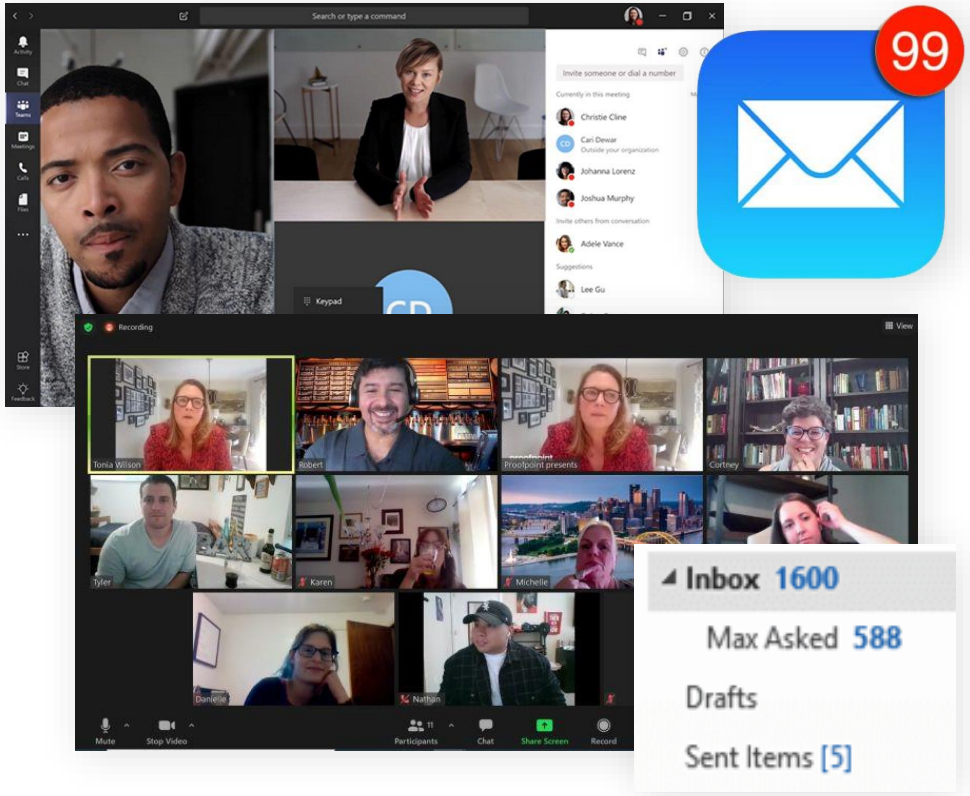
- 발신자를 속이는 스푸핑에 대한 가시성 확보
- 구글 Gmail, 2024년 2월부터 DMARC 정책 적용

[임직원 보안 훈련/교육]

- 사이버 공격에 취약한 임직원에 대한 가시성 확보
- 취약한 부분에 대한 집중 훈련 및 교육

proofpoint.

4. BEC 공격 대응



"**임직원이** 강력한 방어를 수행하는 정보보안의 **보호막** 역할을 수행할 수 있음"

proofpoint.

05

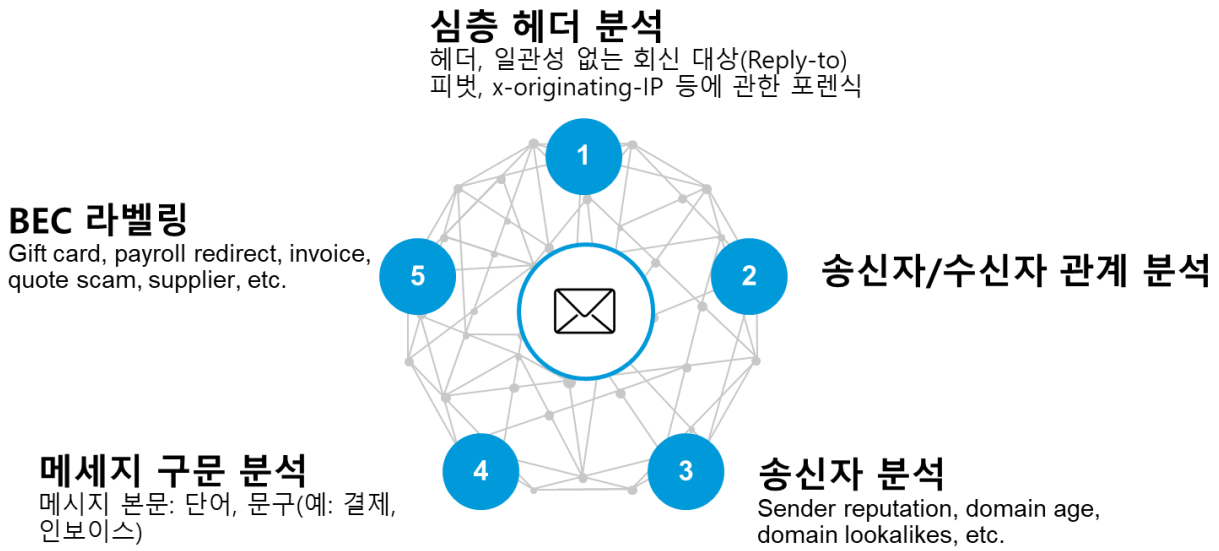
Proofpoint 솔루션

이메일, 당신을 속이는 4가지 기법

5. Proofpoint 솔루션

PPS

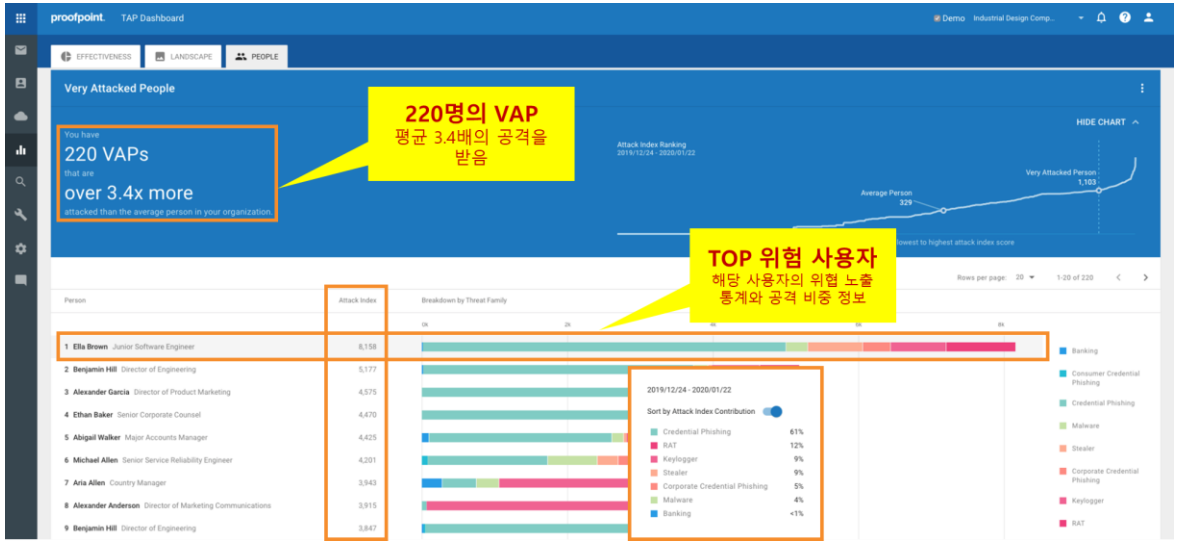
BEC 공격 차단
이메일인증
스팸/바이러스 차단

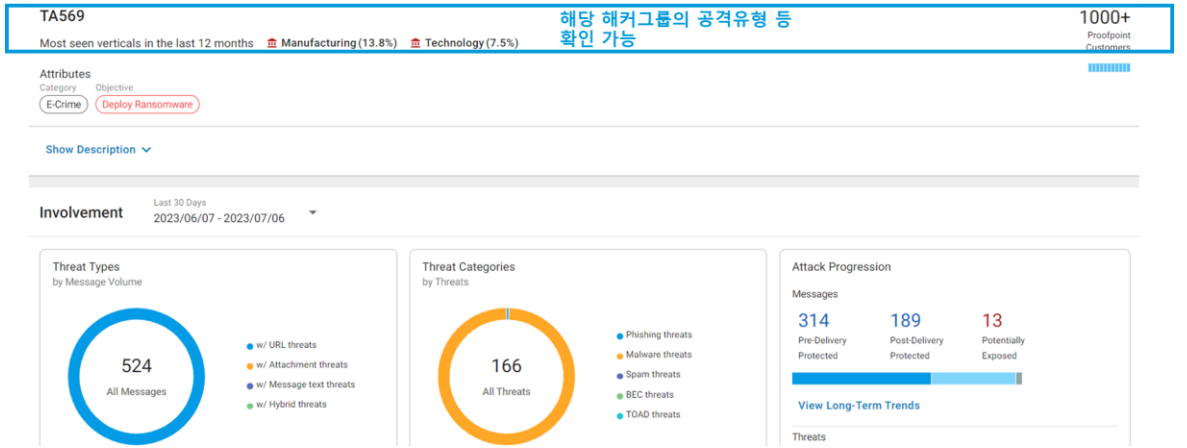


5. Proofpoint 솔루션

TAP

향상된 대시보드
공격자 정보(TI) 확인
위험한 임직원 가시성
첨부파일, URL 샌드박싱





proofpoint.

5. Proofpoint 솔루션

Isolation

이메일 내 URL 클릭 시
격리된 안전한 브라우저에서
Display

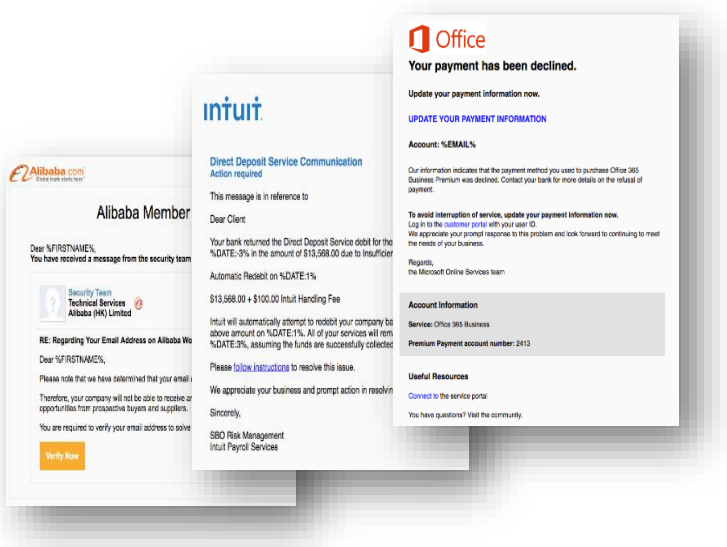
TRAP

사후 악성으로
변경/탐지되는 메일에 대해
자동으로 메일서버에서
검색하여 삭제
(Retro Active)

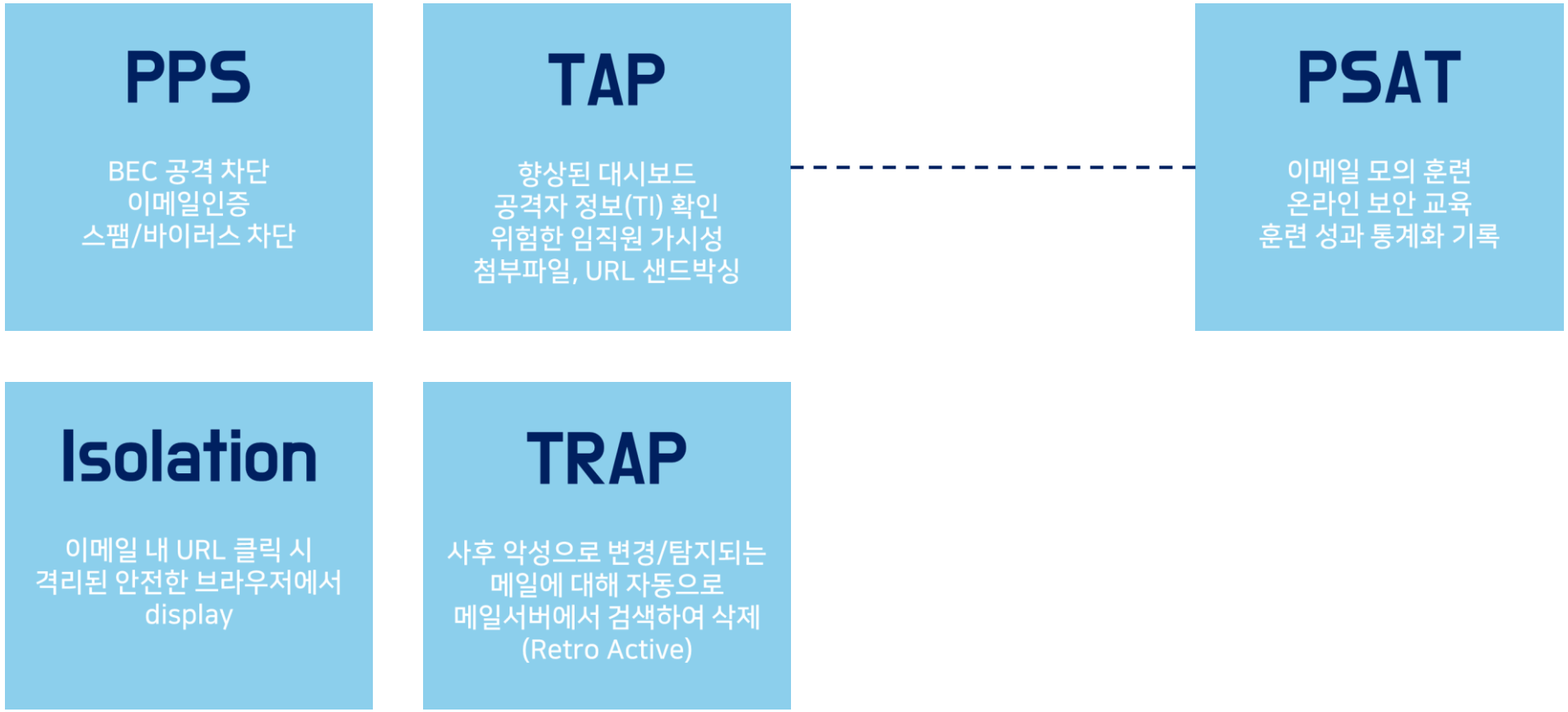
5. Proofpoint 솔루션

PSAT

이메일 모의 훈련
온라인 보안 교육
훈련 성과 통계화 기록



5. Proofpoint 솔루션



"실제 환경과 훈련 환경을 바탕으로 취약한 임직원을 분류하여 집중 교육 수행"


proofpoint®