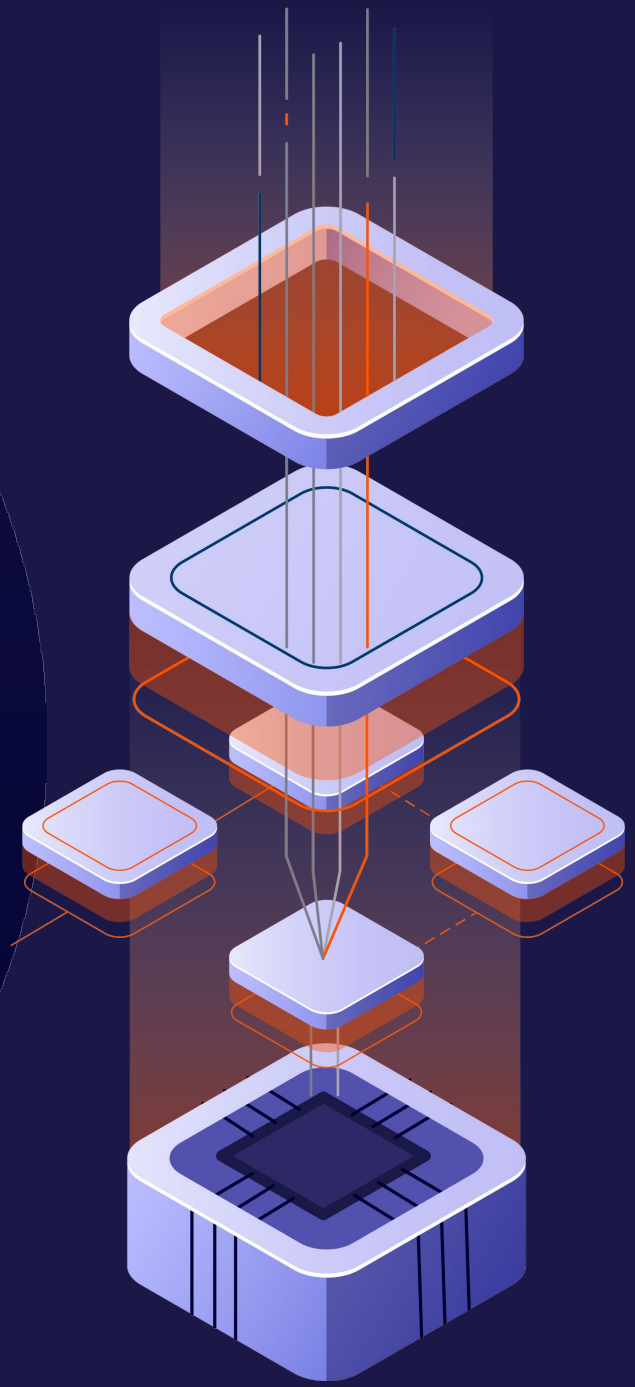
SSNC 에스에스앤씨

PERCEPTION POINT

AI 공격엔 AI로 더 똑똑하게 방어, 진화하는 이메일 공격 방어전략

Rafi Glickman

Perception Point APAC Channel Sales Manager



PERCEPTION POINT

Protecting the User's Modern Workspace

125
Employees

5
Offices

+5K
Customers

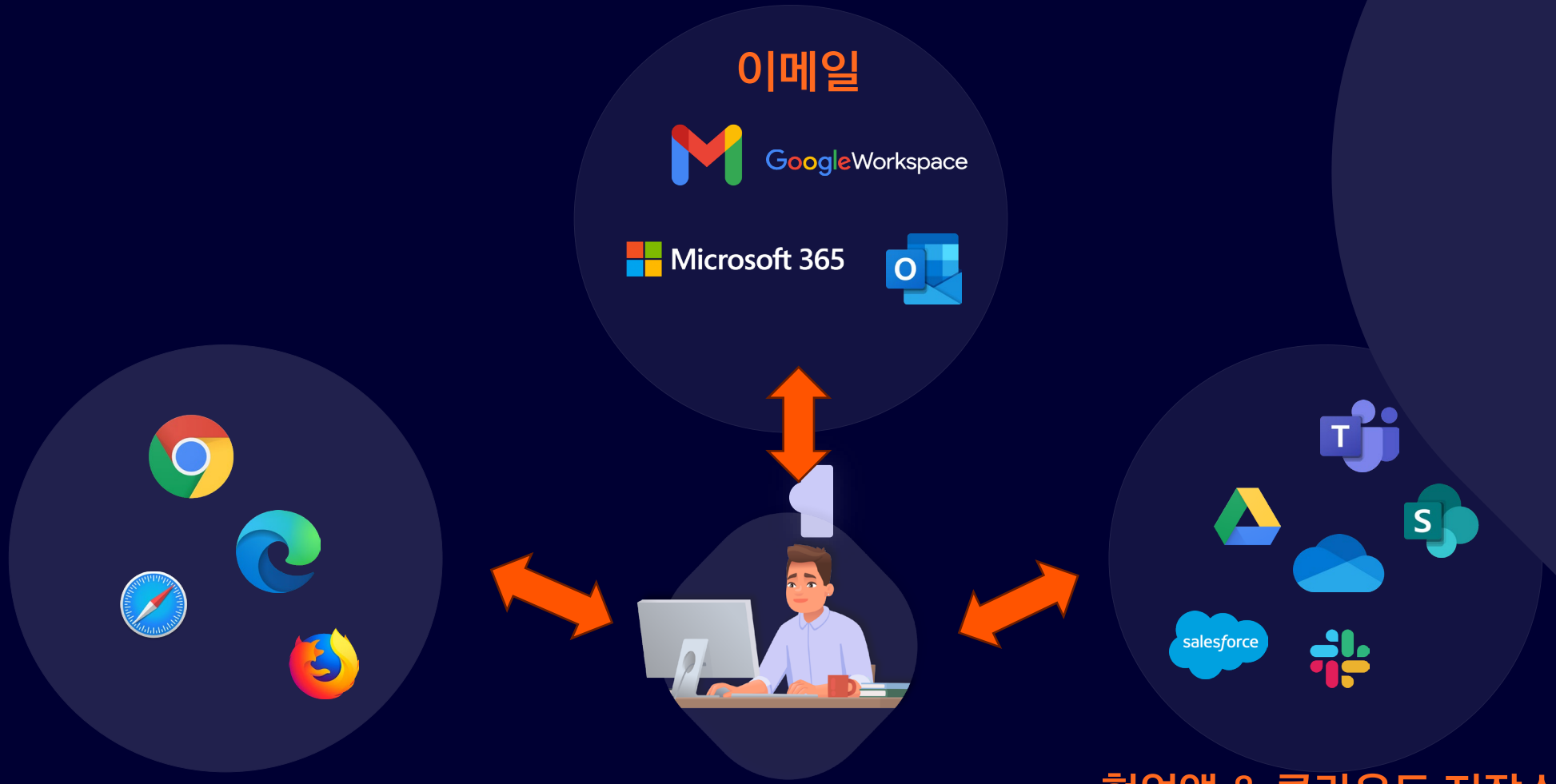
+100
Partners

SELECTED CUSTOMERS

TECHNOLOGY ALLIANCE PARTNERS

AWARDS

계속 변화하고 있는 요즘의 업무 환경



PERCEPTION POINT

점점 더 정교해진 공격 & 점점 더 증가하고 있는 우회 공격

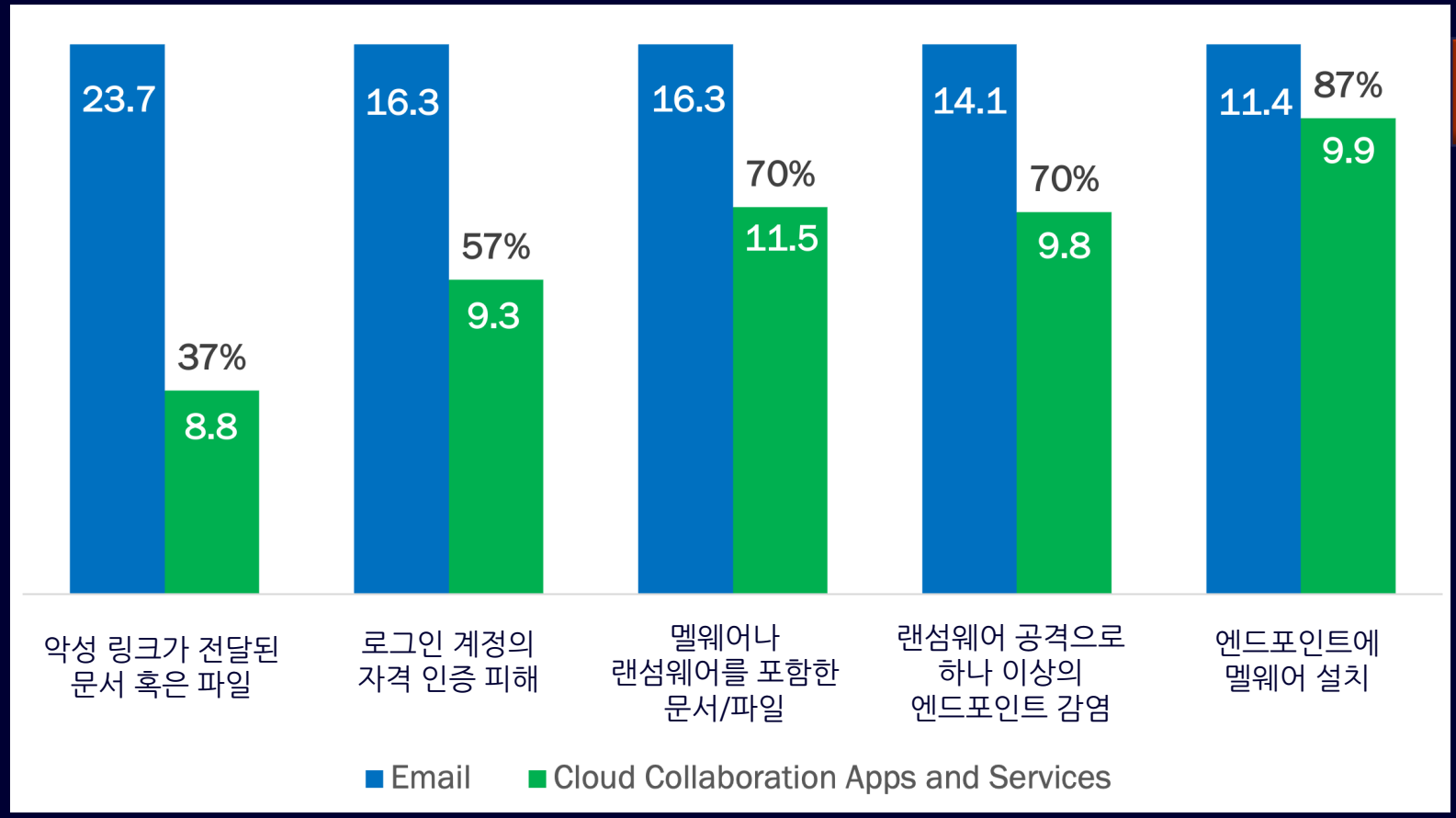
Browser-in-the-Browser	Two-Step Phishing	Thread Hijack	Delivery via Personal Email	Delivery via Legit SaaS Apps	Calendar Invites
GenAI-powered BEC	JavaScript Encryption	Local HTML files	Delivery via Social Media	IP Geofencing	Deep Malware Nesting
Mail Forwarding Rules	Account Takeover	Delivery via SaaS Apps	Vendor Email Compromise	Malicious Browser Extensions	Zero-Days
MFA Phishing	Malvertising	Password-Protected Files	Esoteric Archive Formats	Exfiltration via Browser	Captcha Evasion
Esoteric Document Types	Blob Evasion	User Interaction Evasion	HTML Smuggling	Mail Deletion Rules	Exploits
Leveraging N-Days	Crypto Stealers	Drive-by Downloads	UI Redressing	Clickjacking	Cross-Site Scripting (XSS)
Browser Tampering	Iframe Evasion	VM Detection	Delivery via File Sharing	Time Evasion	Droppers

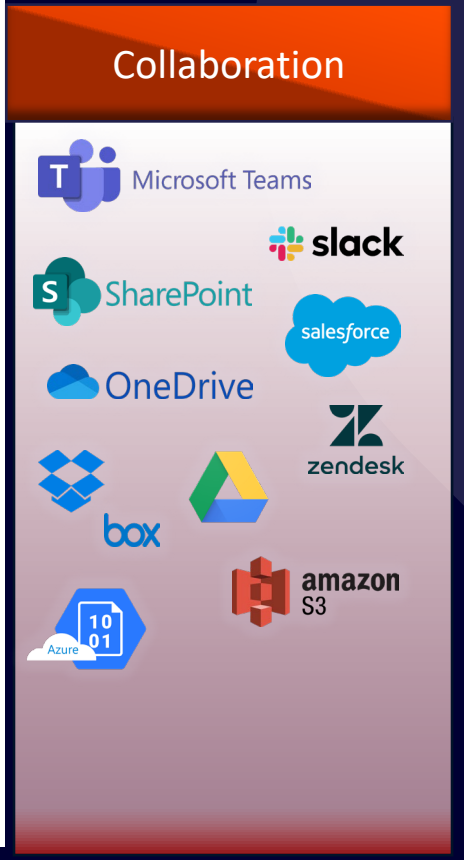
PERCEPTION POINT

새로운 위협 채널

클라우드 협업앱/서비스를 통해 성공한 보안위협 사고

직원 1,000명당 평균 사고 건수(N=144개 조직에서 공개한 자료)



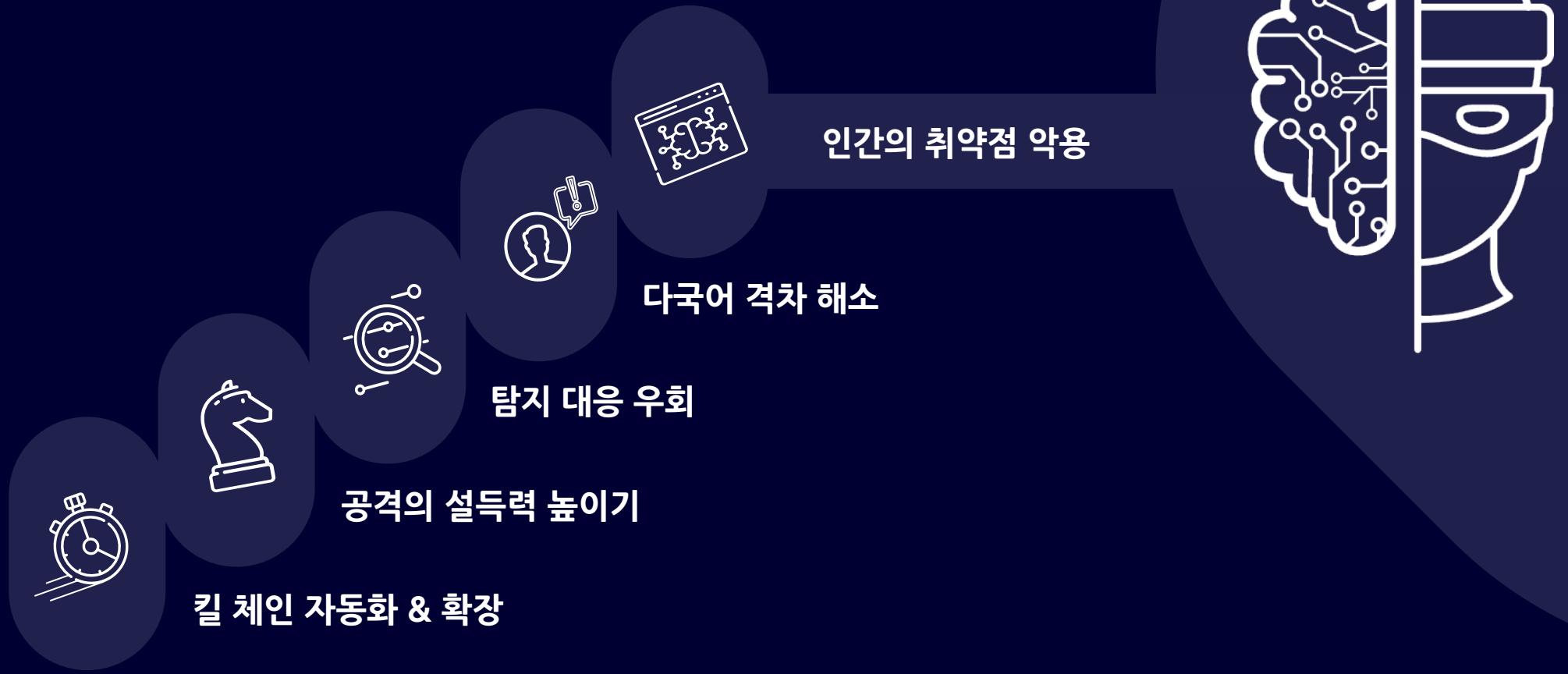


Source: Osterman Research

PERCEPTION POINT

사이버 범죄에 혁명을 일으킨 AI 도구

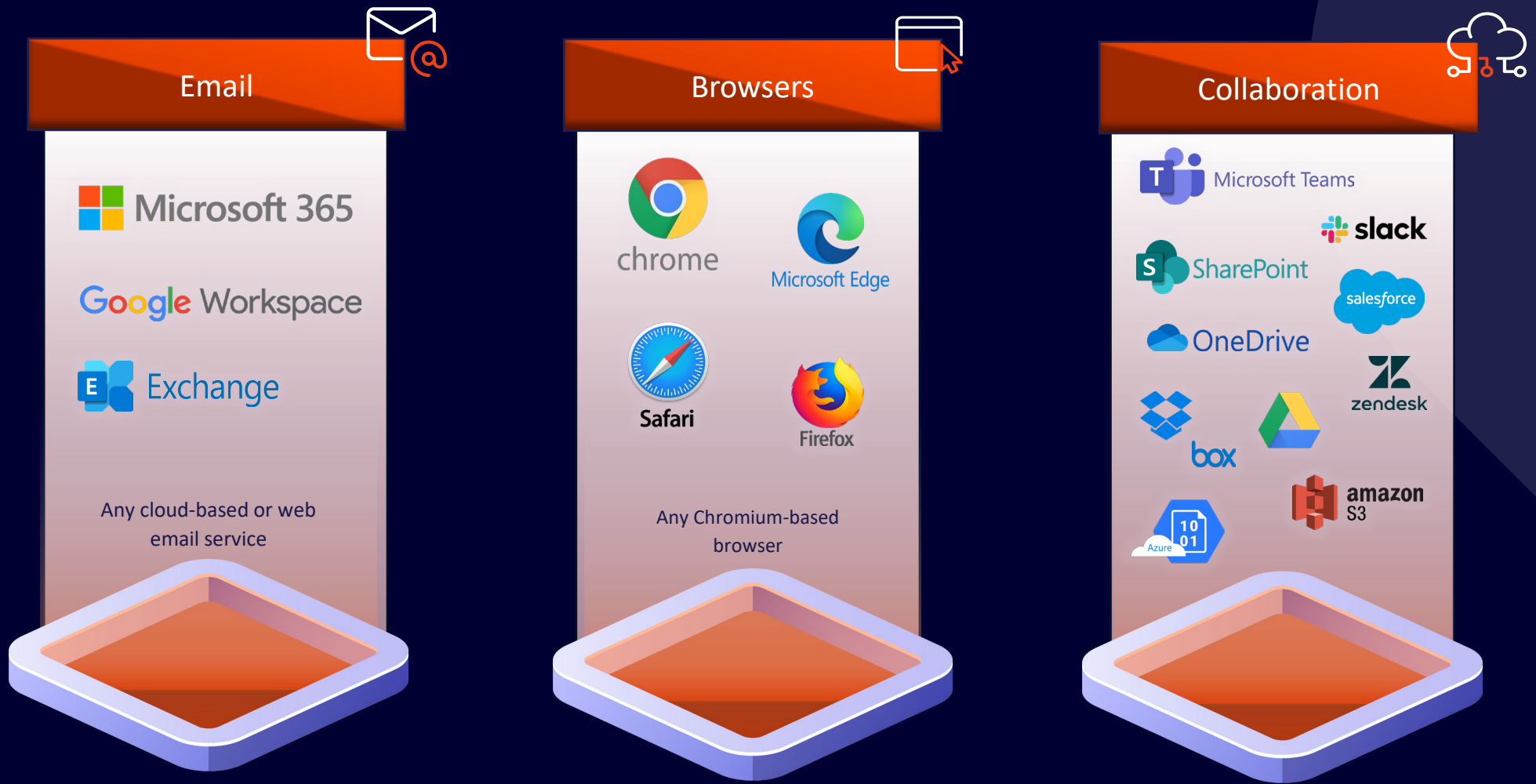
ChatGPT와 GenAI가 BEC 및 피싱 캠페인을 강화하는 방법



PERCEPTION POINT

주요 공격 채널 보호

보안을 통합하고 오버헤드를 낮추면서 탐지·분석·치료 강화



PERCEPTION POINT

요즘의 업무환경을 위한 사이버보안

더 많이 보호하고, 덜 관리하세요. Protect More. Manage Less.

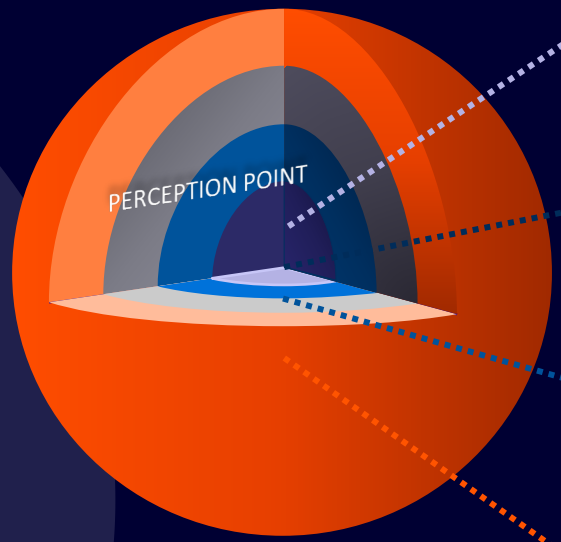
99.95% 탐지 정확도

100% 동적(Dynamic) 스캐닝

75% SOC 리소스 절약

<10 배포 시간

1 플랫폼



거의 모든 유형의 위협 예방

이메일, 브라우저 & SaaS앱 보호

인시던트 대응 관리

AI로 강화되고, 인간이 주도

PERCEPTION POINT

PERCEPTION POINT

Perception Point AI Technologies

AI로 움직이고, 사람이 주도하는 기술

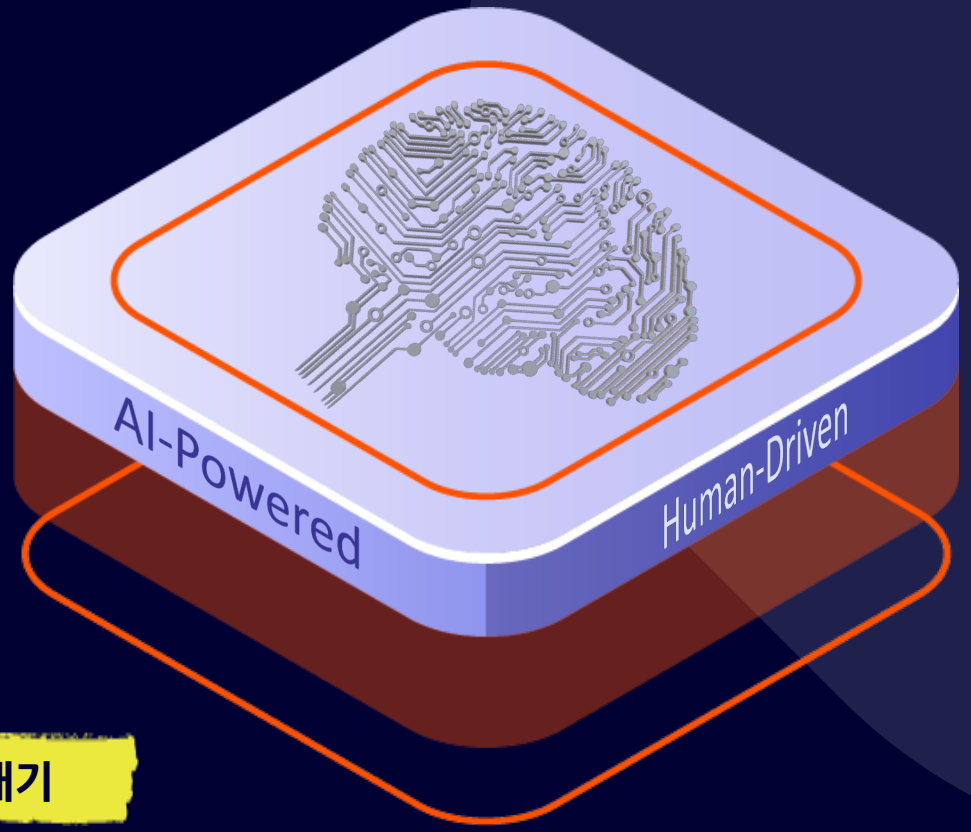
고급 피싱 및 사회 공학적 공격에 대한 스마트한 예방 방법

NLP 과 GenAI 모델
조직의 관계와 커뮤니케이션 패턴 **이해하기**

이미지 인식 엔진
고급 피싱 및 브랜드 스푸핑 공격 **파악하기**

행위 & 컨텐츠 분석
이상 징후, 악의적인 의도와 우회 기술 **인식하기**

24/7 사람의 인사이트
탐지 최적화, ML(Machine Learning) 정책 관리 및 잘못된 경고 **찾아내기**

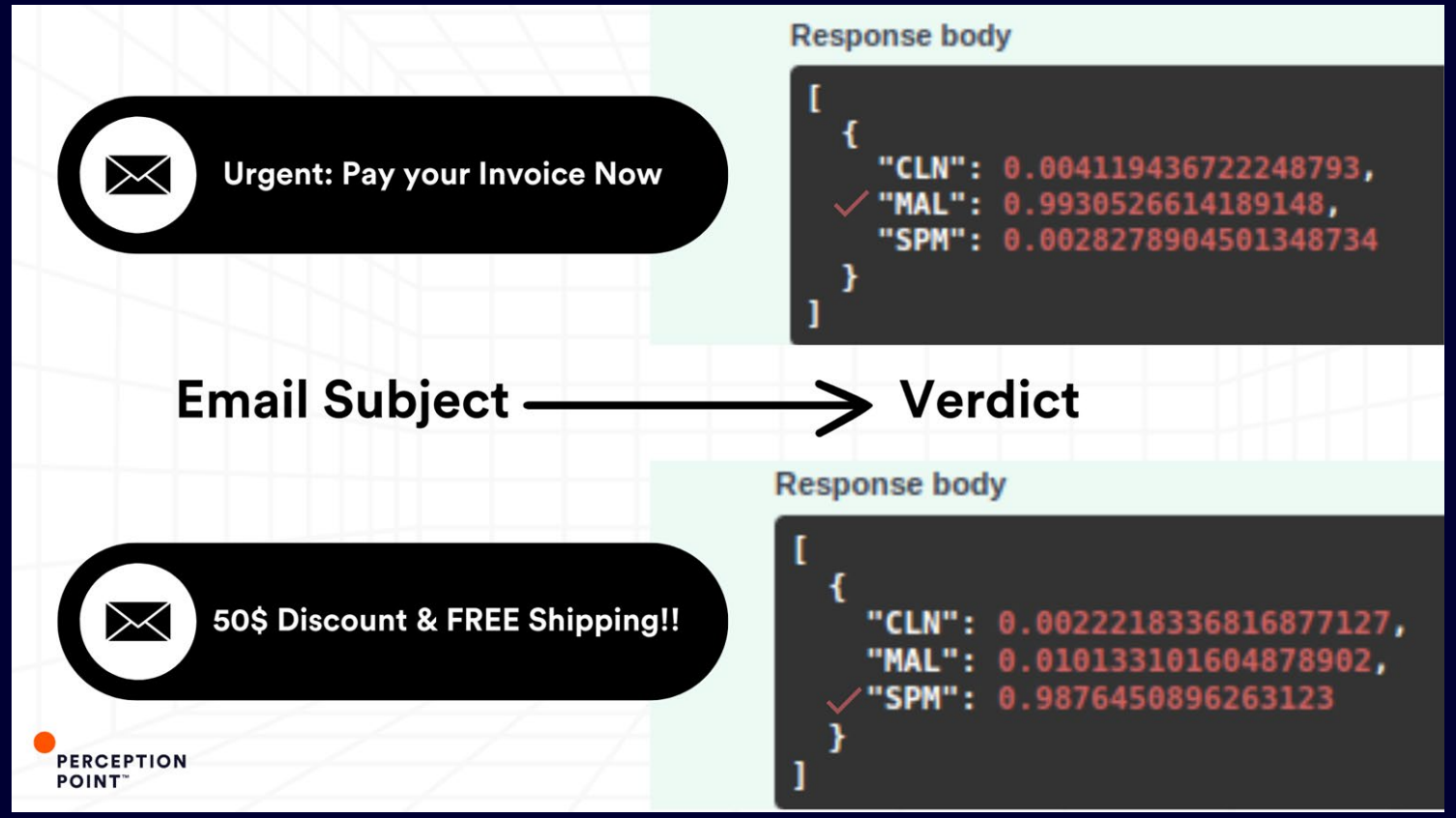


PERCEPTION POINT

제목 분석기 – New

이메일 제목의 CLM, SPM 및 MAL 수준을 분석하고 점수를 매깁니다.

- ✓ **CLP: Content Length Modifier**
  컨텐츠 길이 수정자, 이메일 컨텐츠 길이 수정하는데 사용
- ✓ **SPM: Spam Probability Modifier**
  스팸 확률 수정자, 스팸으로 분류될 가능성 수정하는데 사용
- ✓ **MAL: Maliciousness**
  이메일의 악의성 여부 나타내는데 사용



PERCEPTION POINT

예시:
생성AI로 만든
상품권 사기공격

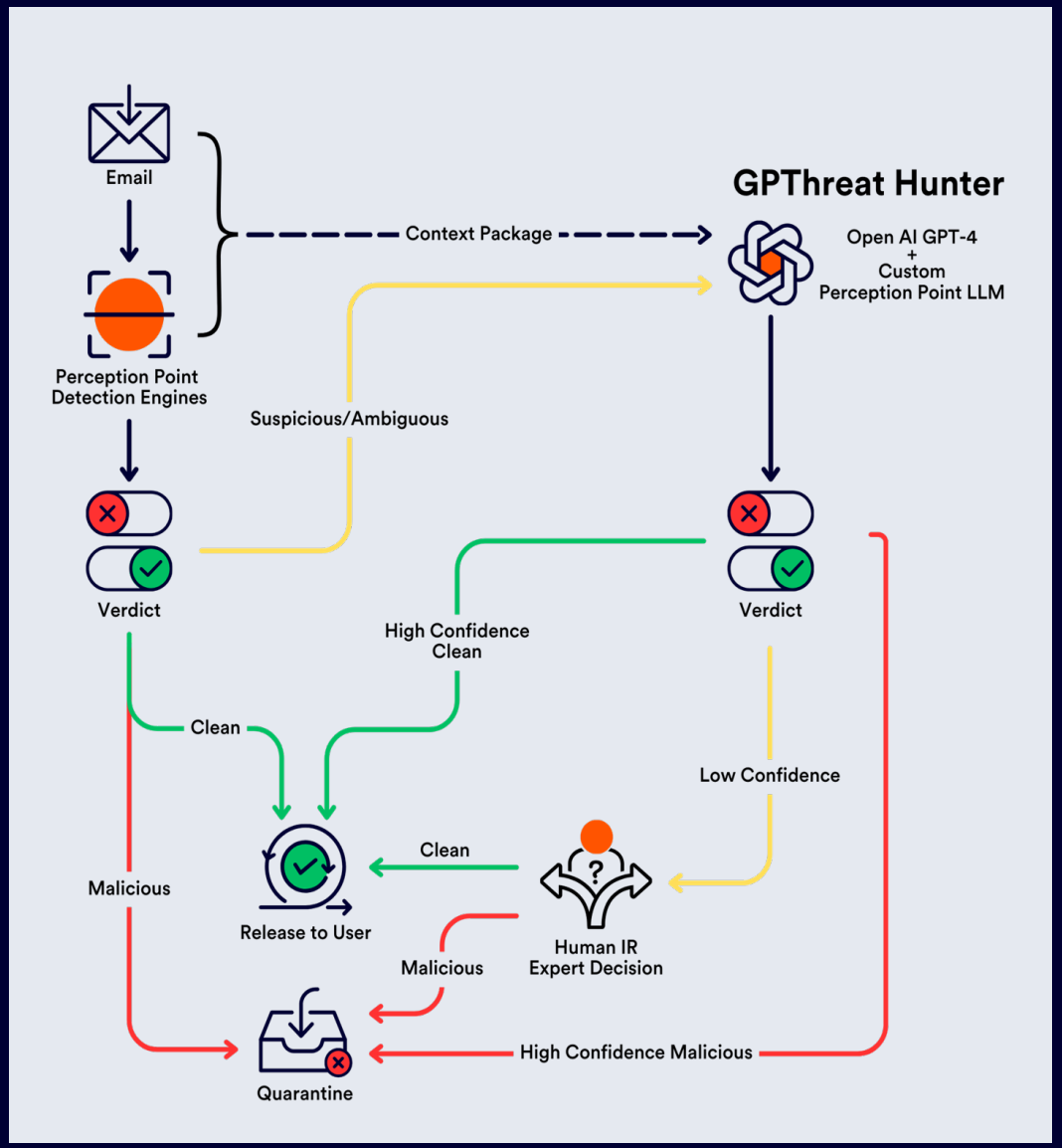
- Zero-Hour 사회공학 캠페인의 일환으로 두가지 다른 상품권 사기 이메일 제작
- 각 이메일은 완전히 다른 새로운 텍스트/구문으로 작성되었지만 동일한 의미/구조로 되어 있음
- 전통적인 패턴 기반 탐지로는 잡힐 수 없음
- Perception Point의 LLM기반 유사성 엔진에 의해 탐지됨

	Malicious Email #1	Malicious Email #2
	From: staffgiftmail077@gmail.com **Subject**: RE: Response Surprise Gift	**From**: surprisegiftniail040@gmail.com **Subject**: Re: Get Rack To Me Promptly!
인사말	Hi	Good day
감사 메세지	It has been an incredible journey over the past few months, and **everyone has worked extremely hard** and shown a level of commitment that inspires me and the rest of senior management.	Trust all is well and that you're looking after yourself. I wanted to personally thank you for **your commitment and hard work** that is creating a future that is so promising and bright.
비밀 서프라이즈 이유	I must reward the commitment to work and the dedication of the staff during this period. Therefore, I am **Surprising some executive staff** today, and I would appreciate your confidentiality so as **not to spoil the impact of the surprise.**	I'm planning a New year **surprise for some favorite employees**, and your confidentiality would be appreciated so as **not to ruin the impact of this surprise**, something small, but Just a way to spur them on to even greater heights of excellence and deep appreciation for what they've done for this company.
액션 요청	I will need you to make an online purchase on my behalf or at any stores near you for gift cards to say thank you, and well done. Any such cards like **Amex /Visa or Amazon gift cards** for variety depending on their tastes. **Your input on this idea** would be appreciated before purchasing, so I know what you as a staff feel about this;	The first thing that popped into my mind was a **Visa. Target, or Amex gift card**, which gives the flexibility of using it anywhere. What's the closest store you can think of to make a purchase quickly on my behalf? It Is a wonderful gesture that everyone would appreciate and would be a very nice surprise. **Let me know what you suggest about this plan** before going ahead with the purchase.
긴급함 표현	My schedule is quite tight during this period, but please reply to the email as soon as you get this so we can find the best possible way to do it.	My schedule is quite tight during this period, but please reply to the email as soon as you get this so we can find the best possible way to do it.
인사	Happy Thanksgiving! Kind regards	I wish you and your family a good new year and always happy and healthy. My Regards

PERCEPTION POINT

GPThreat Hunter™

- LLM 기반: 자체 + GPT 4.0
- 자동 판단
- 일반적으로 IR(Incident Response) 대기열로 전송되었던 신뢰도 낮은 스캔에 대해 자신만의 추론 설명
- PP 최고 탐지엔진 결과 기반 (“AI-powered”)



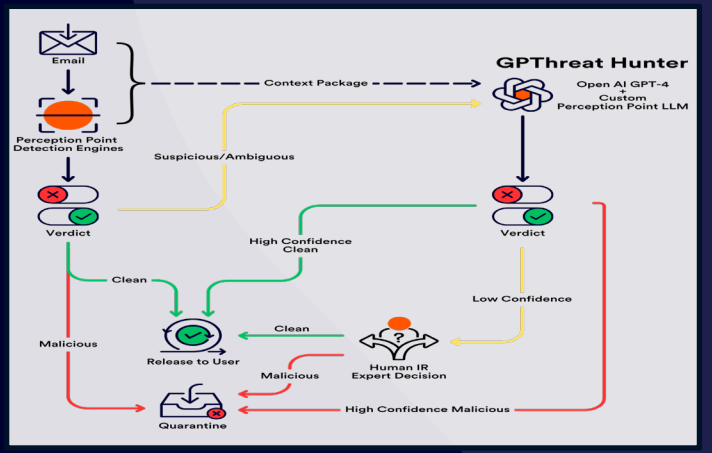
PERCEPTION POINT

Powered by AI. Empowered by People. Revolutionized by

GPThreat Hunter™

Truly Explainable

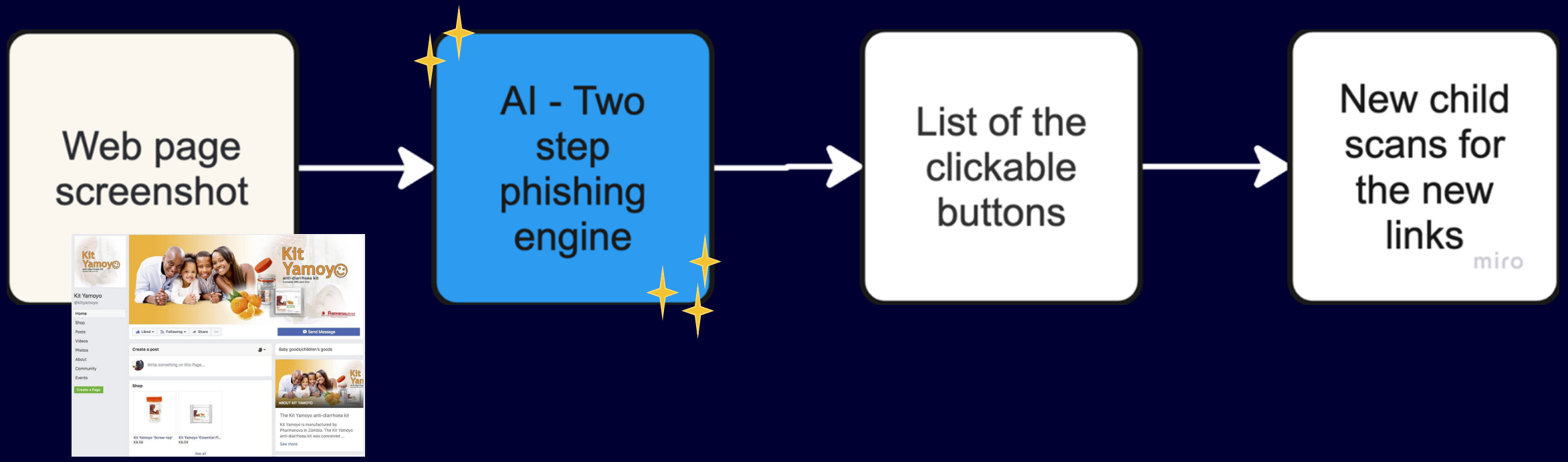
보안 담당자, 관리자, 엔드유저에게 상세한 설명과 충분한 판단 이유 제공
미래의 악성 위협에 대한 내성 증진



PERCEPTION POINT

Two-Step Phishing

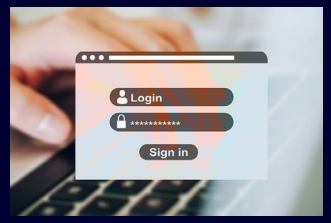
- 웹페이지 스크린샷 안에 있는 클릭 버튼 탐지

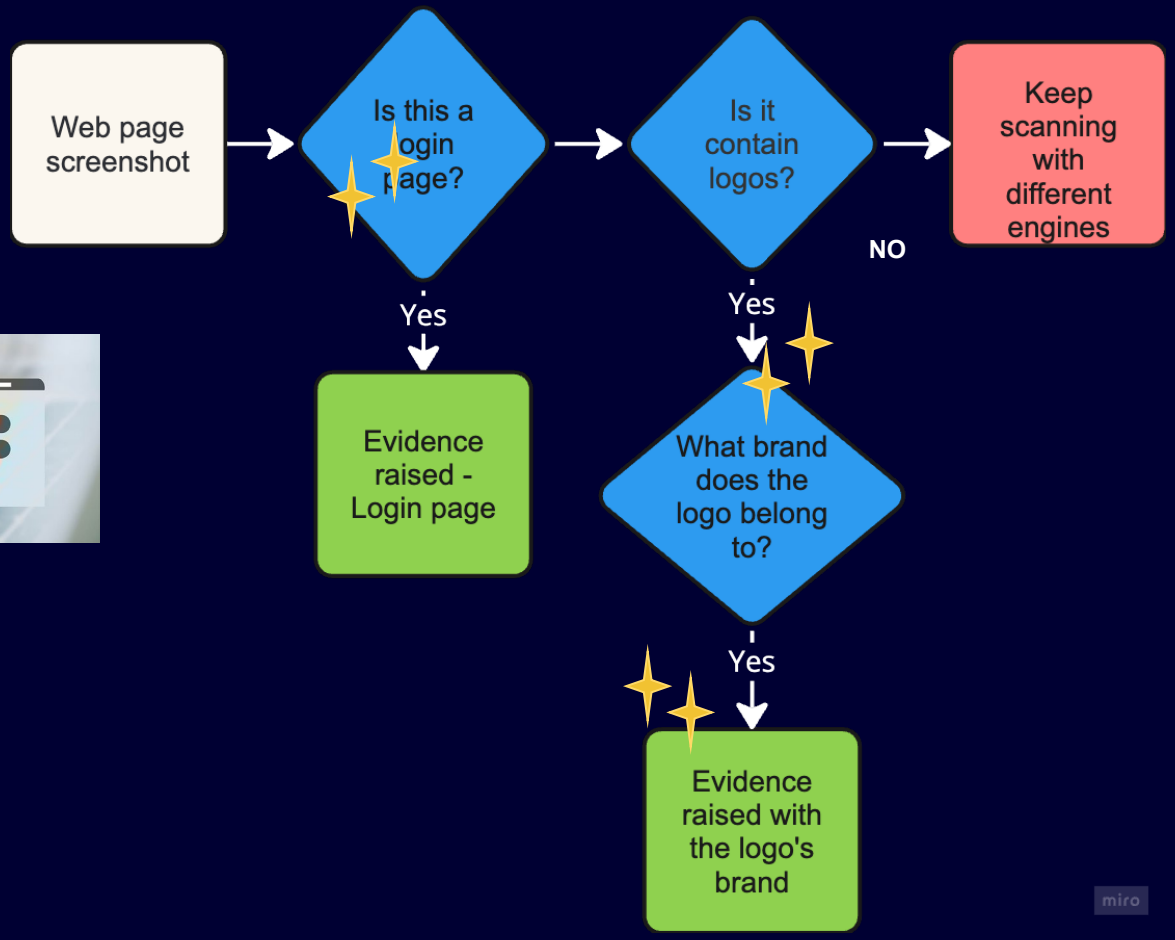


PERCEPTION POINT

로그인 Form & 로고 인식

- 웹페이지 스크린샷에 있는 로그인 Form 탐지
- 로고 탐지
- 브랜드 인식
- BEC & phishing 공격에 유용



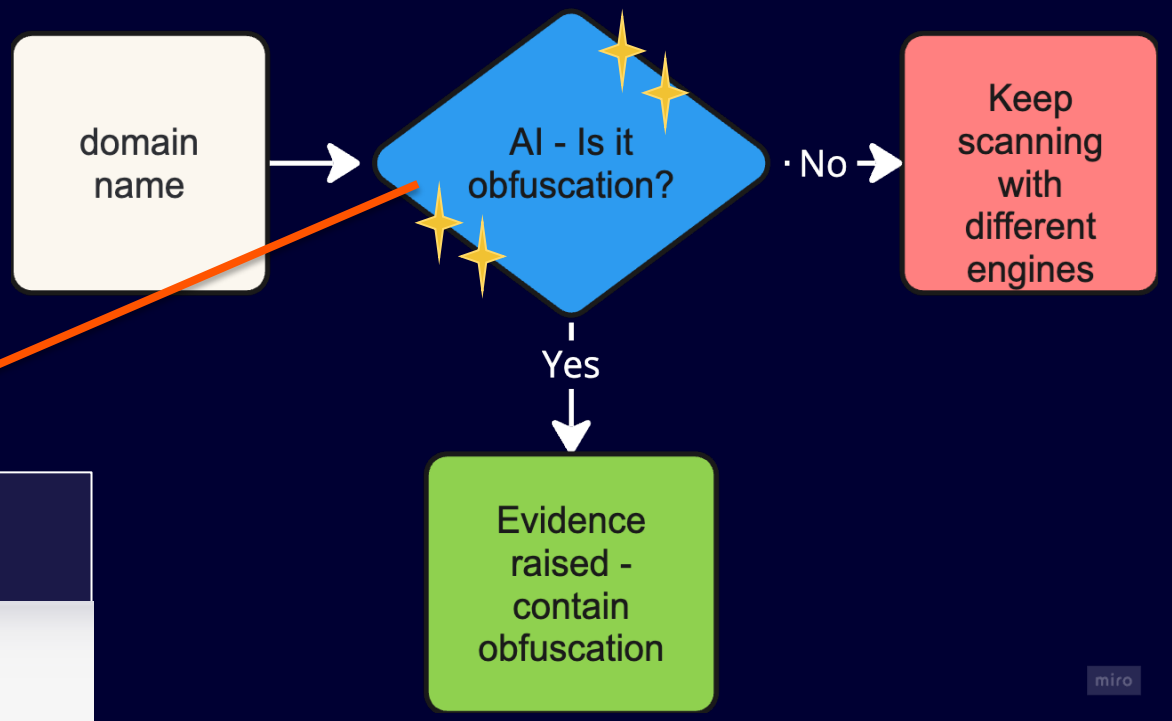


PERCEPTION POINT

텍스트 맞춤법(Misspelling) 검사기

- 난독화** 탐지
- 스푸핑과 피싱 캠페인에 유용

**난독화: 이해하기 어렵게 만드는 방식



PERCEPTION POINT

Thank You

상세문의: sales@ssnc.co.kr
www.ssnc.co.kr

PERCEPTION POINT

SSNC
에스에스앤씨