(주)에스케어

실 위협 노출 현황 관리를 통한 CTEM 관리 방안 제시

기업을 보호하기 위한 인간 중심의 프로세스 혁신을 추구합니다.
Cyber-security professional services & solutions

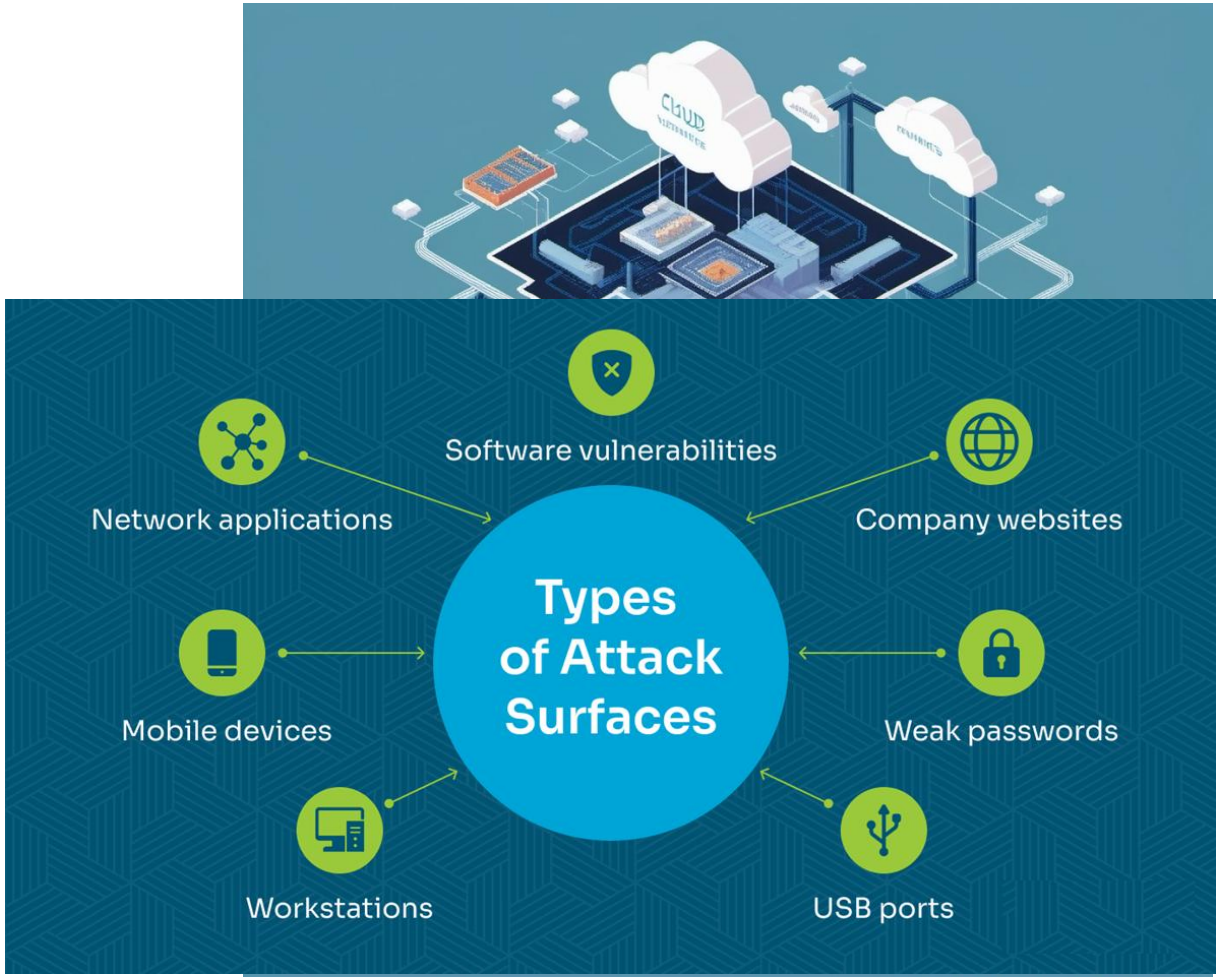
에스케어
윤우희 부대표 / WH.Yoon@escare.co.kr

01

공격 표면에 대한 정의

위협에 노출된 공격 표면 (Attack Surface)의 정의

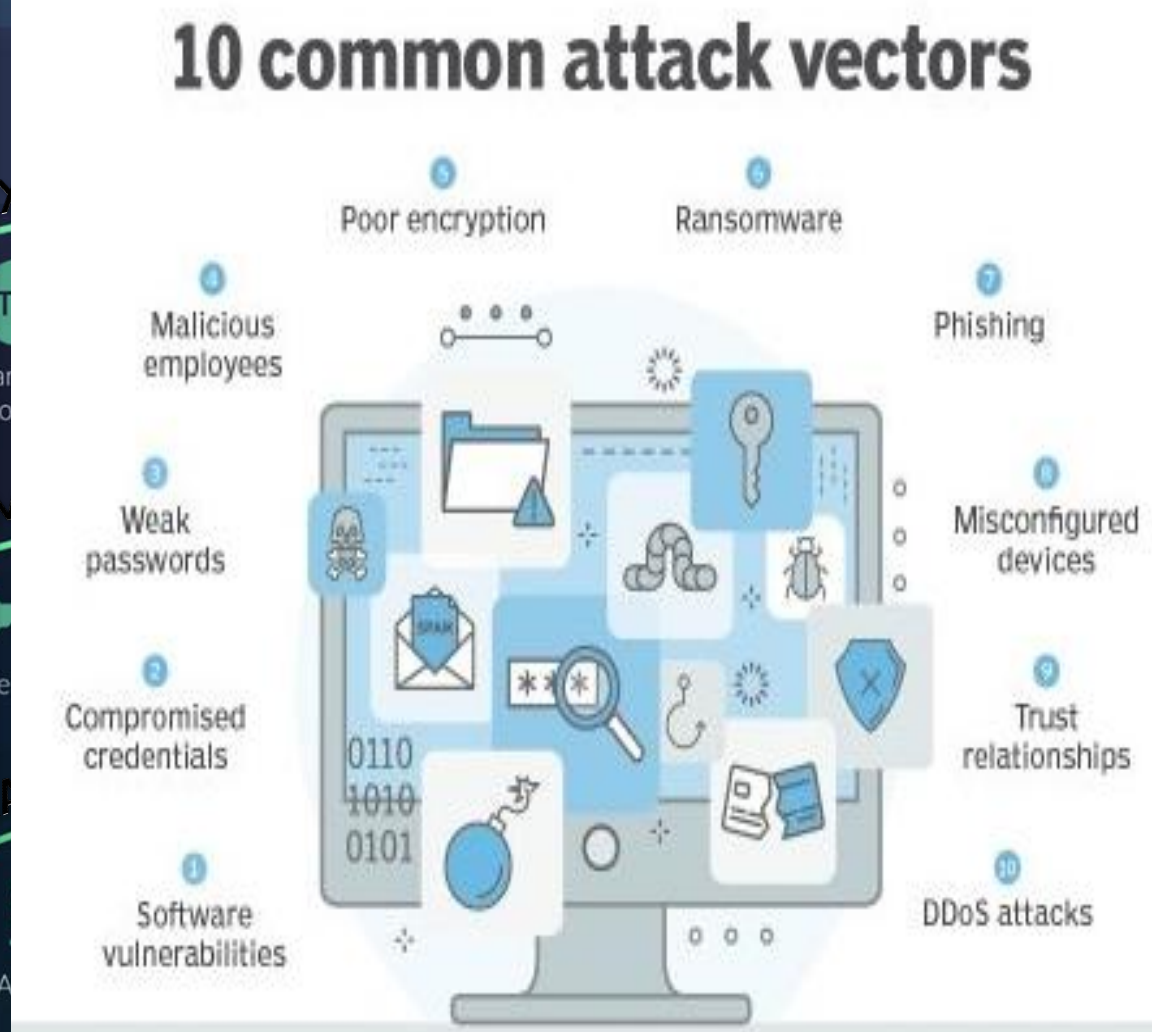
"공격 표면이란,
공격자가 내부 네트워크에 접근을
위해 잠재적으로 악용할 수 있는
모든 공격 경로의 집합입니다."



공격 표면 (Attack Surface)의 정의

"Attack Surface 란,
인프라 발전에 따라 공격표면은 계속 확장됩니다.
디지털 자산 측면에 관리 항목은 늘어나고
비즈니스 위협이 될 수 있는 모든 것이
공격표면입니다."

"Attack Vector 란,
공격 표면을 대상으로 진입을 위해
사용되는 기술들을 의미합니다."

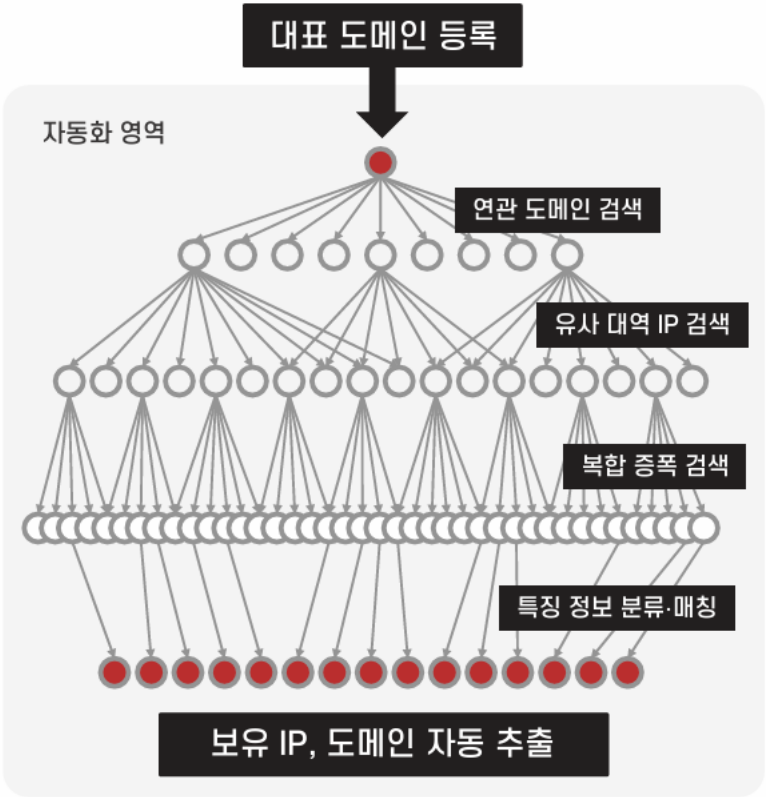


ASM은 어떻게 자산을 식별하는가?

도메인 및 호스트 자산 식별 범위는 취약점 스캔 범위를 관장합니다.

- 대표 도메인 기반 연관 도메인 검색 (DNS Record)
- TLS 인증서 기반 도메인 검색 (TLS Certification)
- WHOIS, CRT.SH (Administrative Contact 담당 이메일) 기반 연관 도메인 검색
- 타 전문기관 Intelligence 연동 (Shodan, Google Security, Recorded Future)
- CTI 인텔리전스에 등록된 연관 도메인 검색
- 유사 대역 IP 검색을 통한 추가 자산 대역 검색
- 내부 인텔리전스 등록 정보 추가 하여 자산 추가 검색

※ 폐쇄망 내부 도메인이 EASM으로 조회가 됩니다. 어떻게 공개된거죠?



공격표면관리는

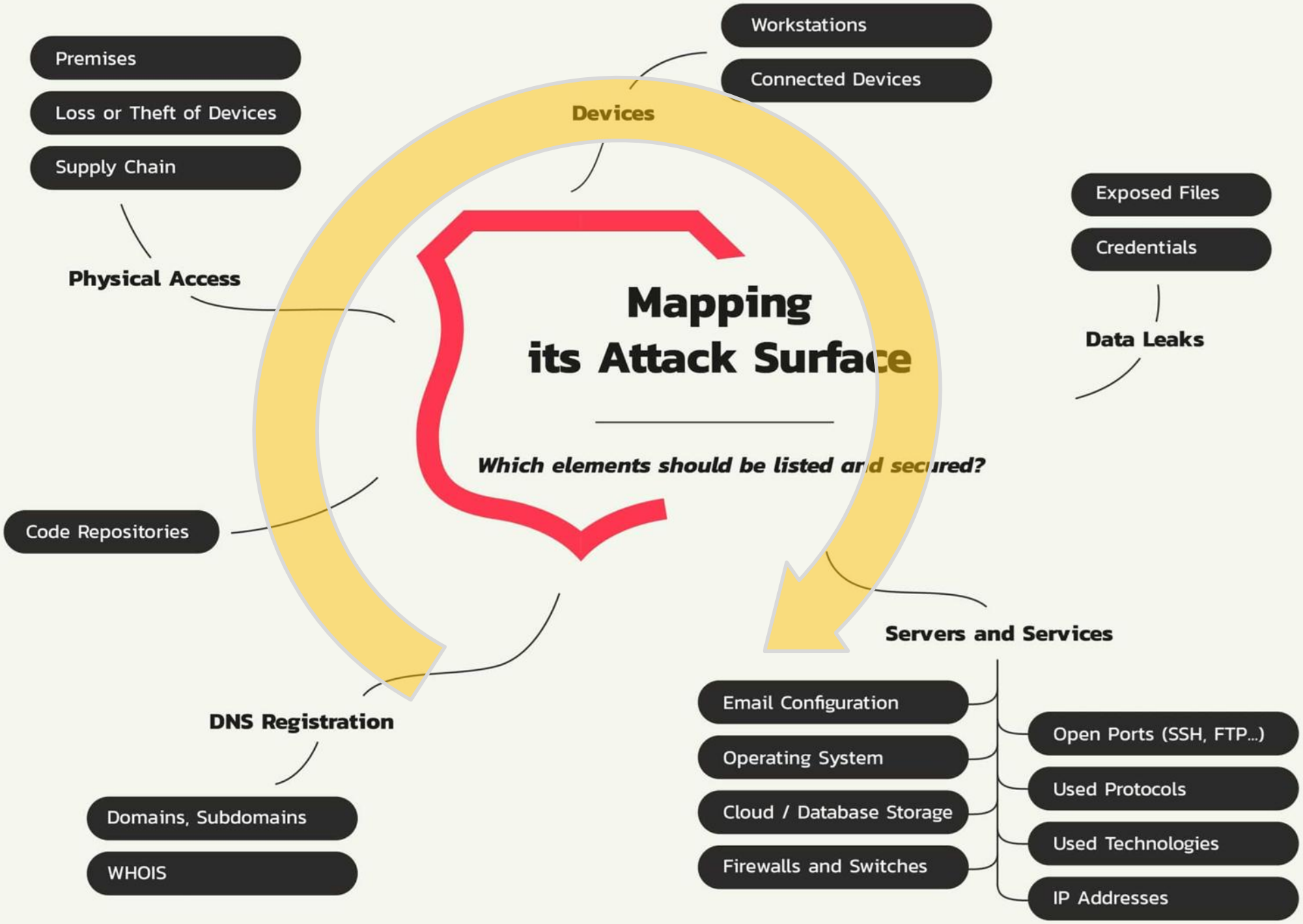
해커의 관점에서

내부로 접속하거나

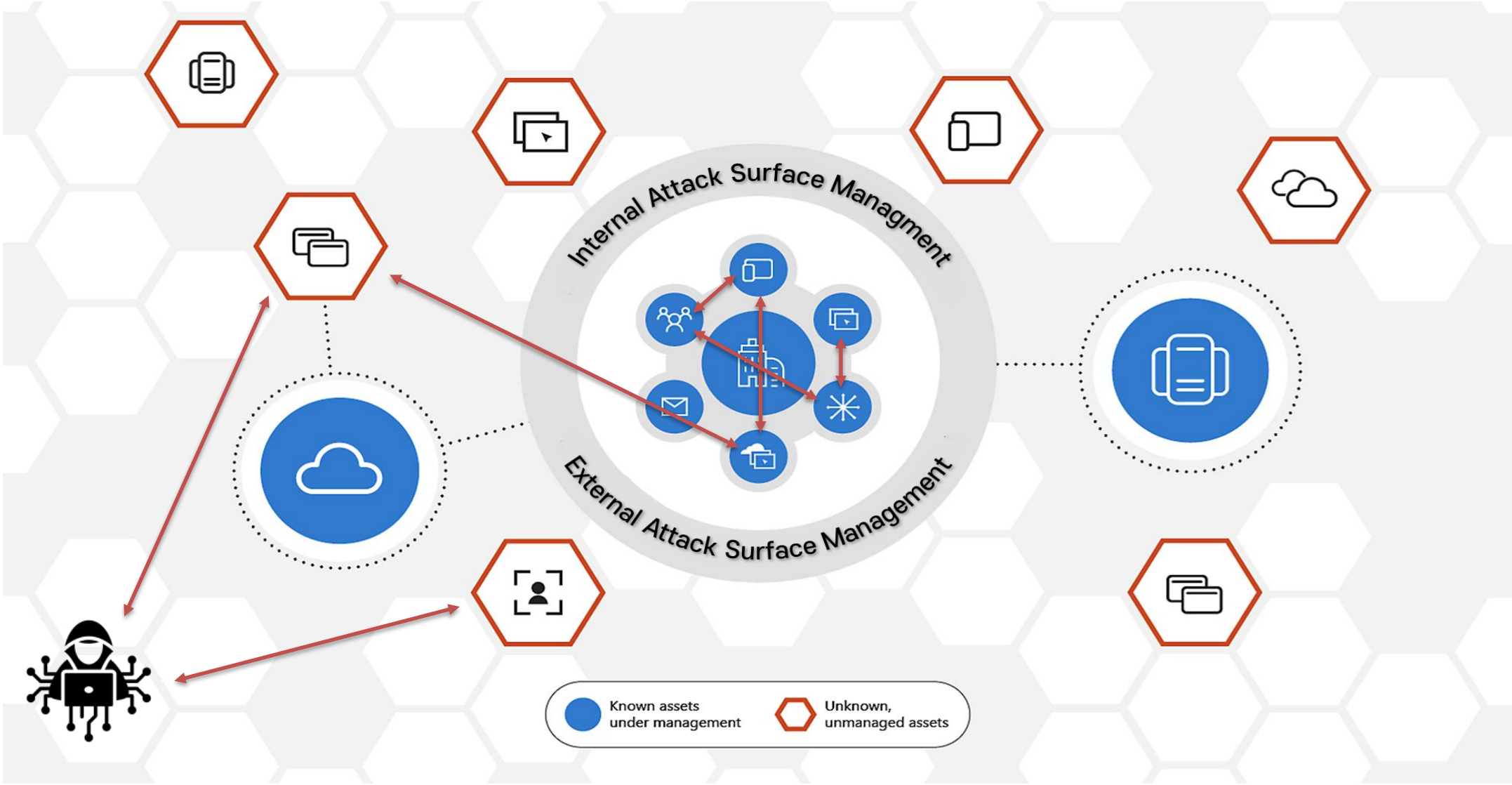
활용 할 수 있는

모든 부분을

점검해야 한다.

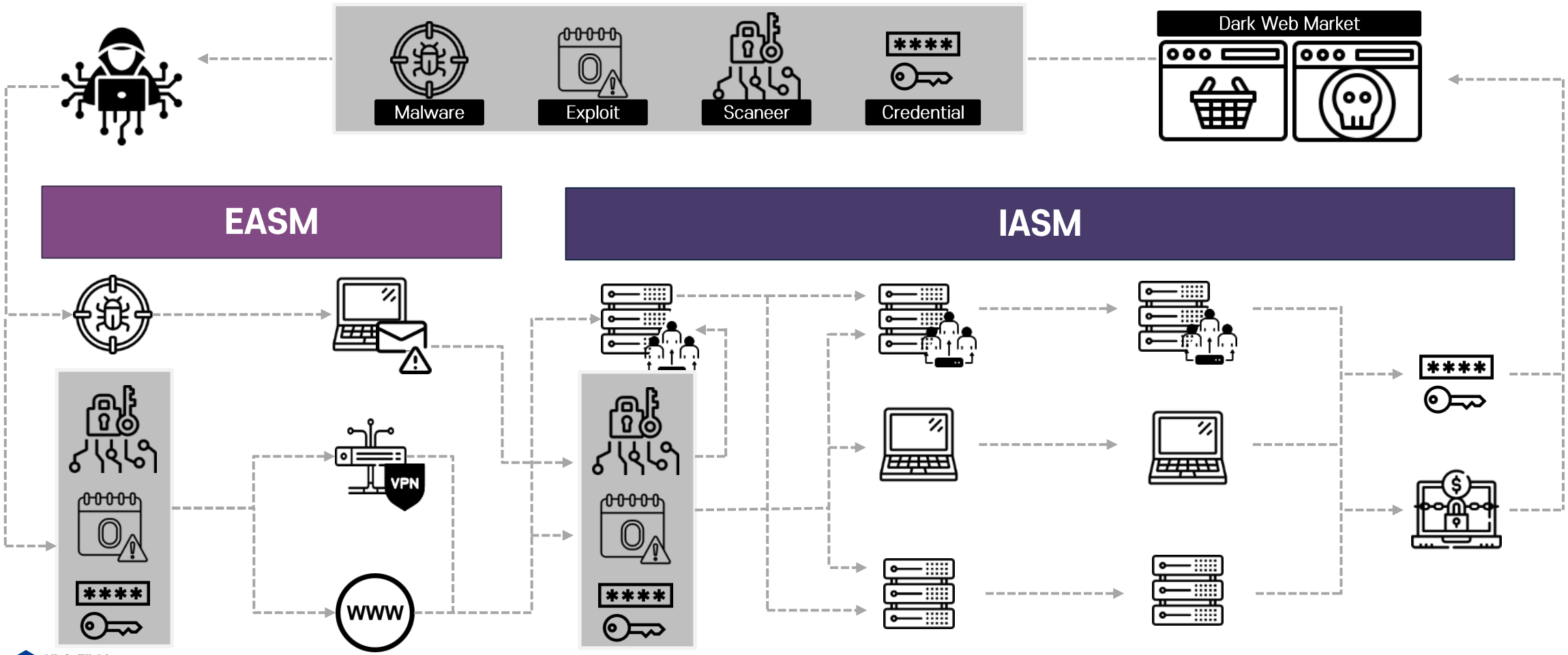


Attack Surface Type (공격 표면 유형)



내부 정찰 및 공격 흐름도

ASM은 해커의 공격 기술을 반영하여 진화 됩니다.



EASM, IASM (공격 표면 관리)

ASM은 EASM과 IASM으로 구분되어지며, 기업은 양방향 관리 모두 필요합니다.

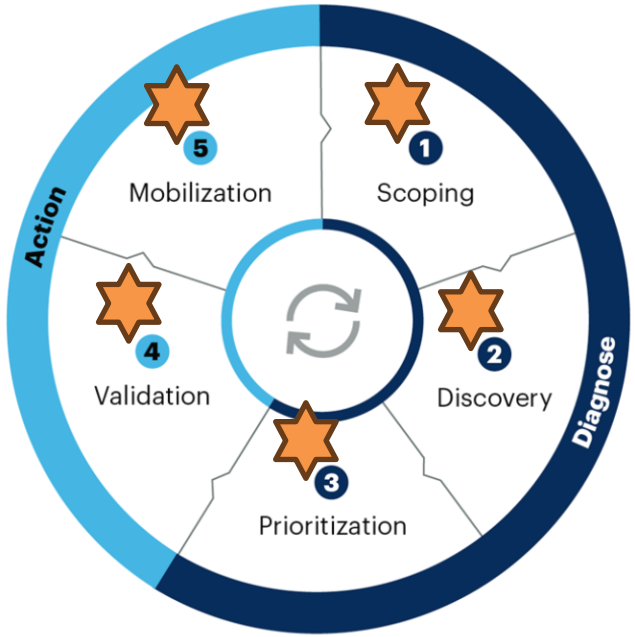
구분	EASM (외부향 공격표면)	IASM (내부향 공격표면)
점검대상	외부에서 보이는 공격 표면	내부 네트워크와 자산의 보안 관리
관리목적	외부 노출 자산(웹 서비스, API, 클라우드, 사용자 계정 등)	내부 자산(서버, 네트워크, 내부 IT 자산 및 사용자 계정 등)
위협 유형	외부 공격자에 의한 정찰, 피싱, 공개된 취약점 활용	내부자 위협, 권한 오남용, 권한 취득, 정찰, 피싱, 공개된 취약점 활용, 내부 네트워크 확산형 공격
위험 관리 범위	외부 위협, 노출된 비 관리 자산, 제3자 관련 리스크 식별	내부 인증 통신 탈취, 인증서버 공격, 내부 시스템 및 권한 관리의 취약점 식별
도입효과	외부로 노출된 자산 최소화, 외부 공격 차단	내부 자산 보안 강화, 내부 네트워크에서의 문제점 사전 대응 방안 제공

02

CTEM의 정의 및 구성요소

위협 노출 관리의 성숙도 모델 (CTEM)

5 Steps in the Cycle of Continuous Threat Exposure Management



gartner.com

Gartner

High-Level Maturity Model for a CTEM Program

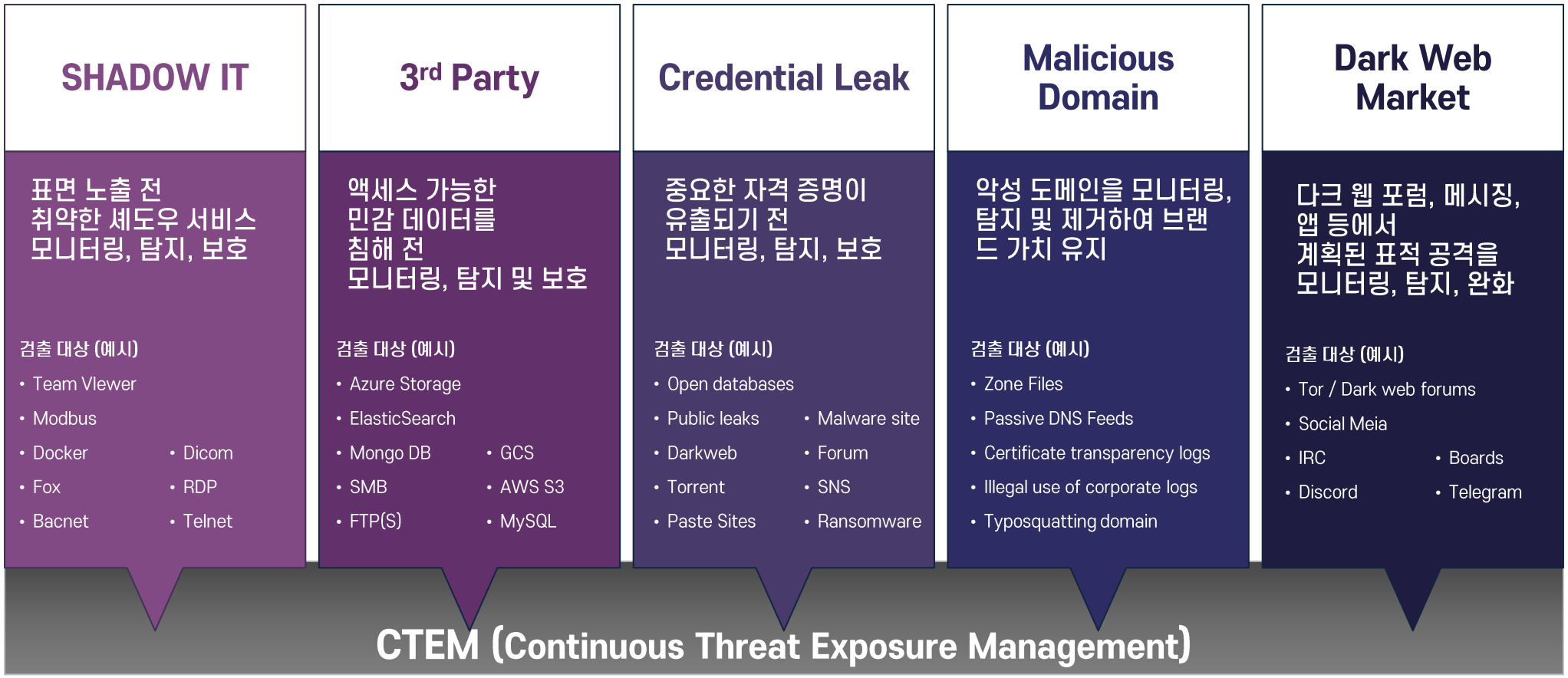
	Establishing	Advanced	Optimized
Scope	All business assets	High-Risk Business Functions	Business-Risk Driven
Discover	Fixed Asset List	Vulnerability Assessment	Composed Risk Discovery
Prioritize	Tool Scoring	Framework Aligned	Outcome-Driven
Validate	Passive Diagnostics	Red Teaming	Purple Team
Mobilize	(Virtual) Patch Prioritization	Remediation Framework	Secure-By-Design

Source: Gartner
763954_C

Gartner

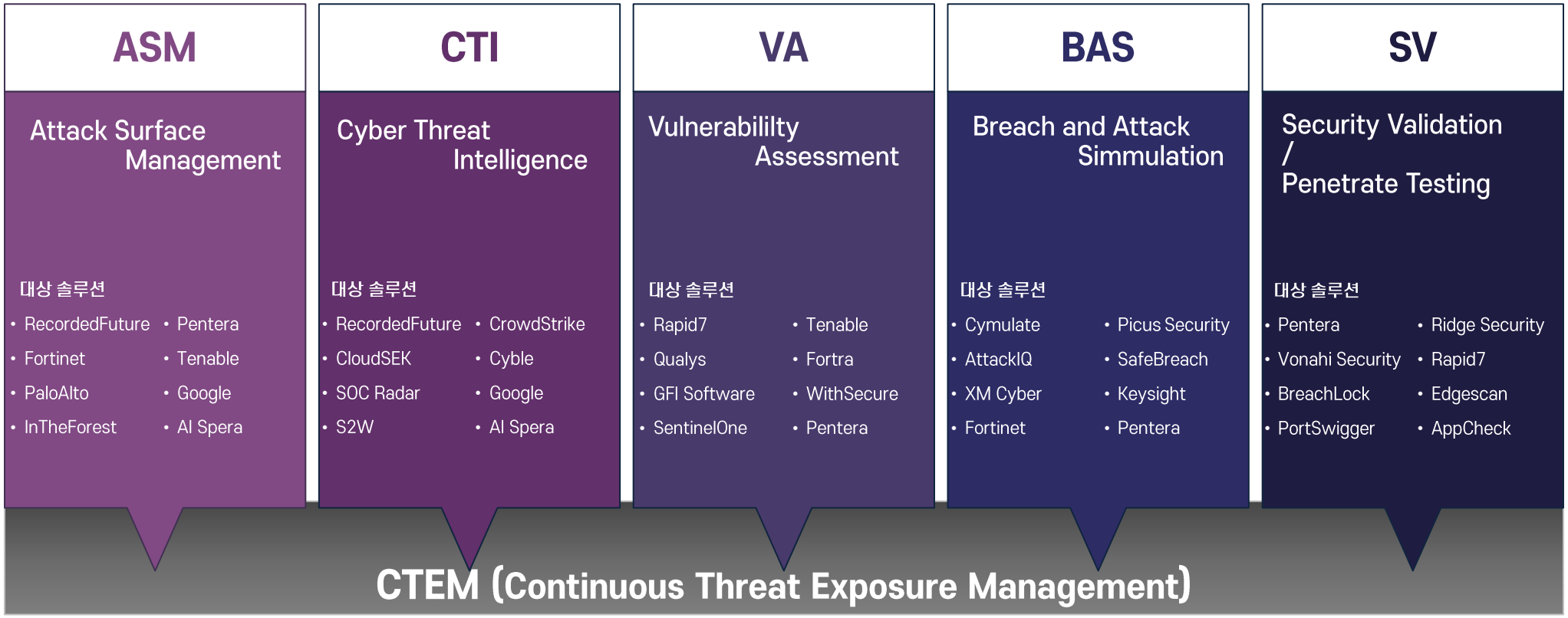
CTEM (지속 위협 노출 관리 체계)

ASM 솔루션의 필수 기술 요소, Intelligence를 활용한 IOC 분석



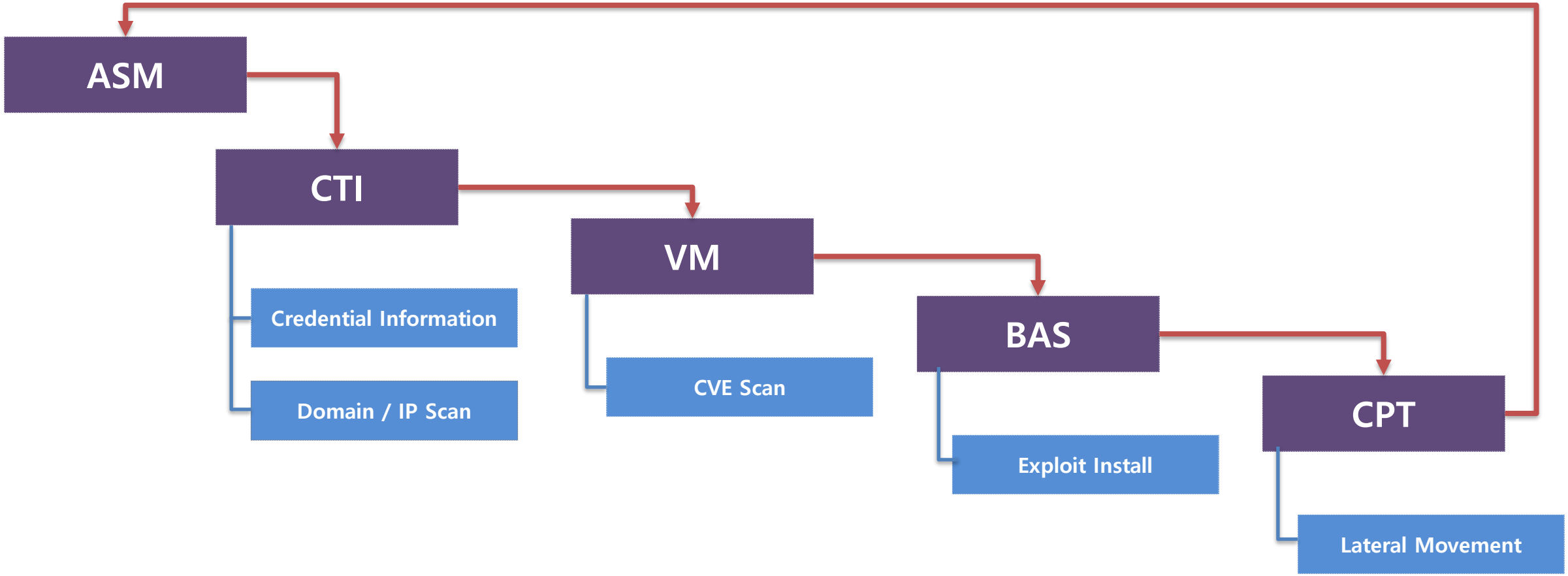
CTEM (지속 위협 노출 관리 체계)

CTEM은 ASM을 포함한, 다양한 점검 기술을 포함해야 합니다.



CTEM은 어떻게 위협을 평가하는가?

CTEM은 ASM 기술을 포함한 다양한 관리 기술을 필요합니다.

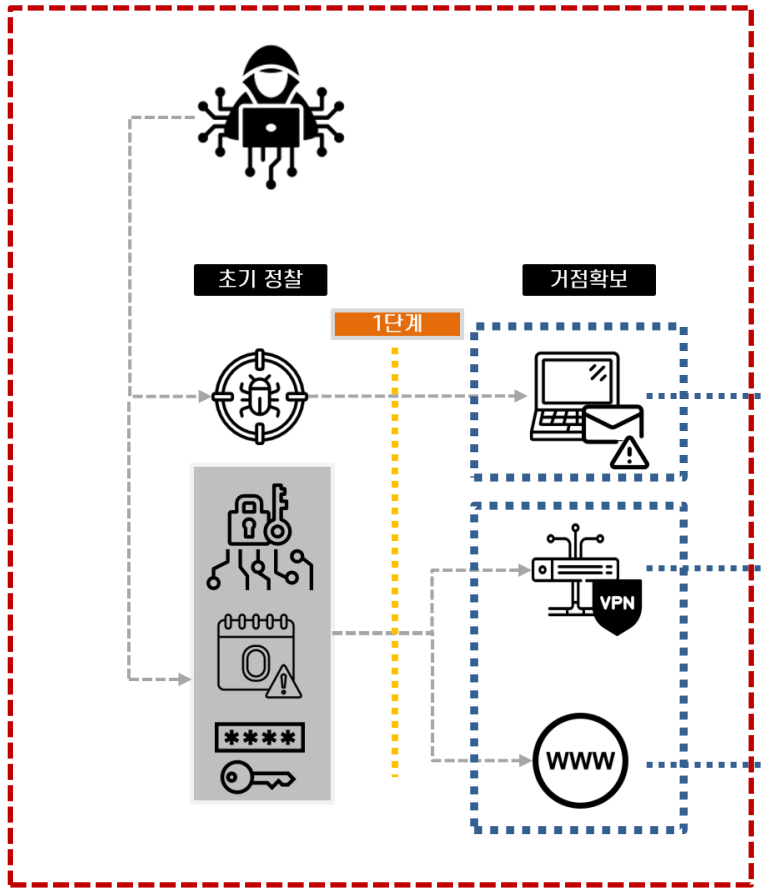


03

CTEM 범위에 따른 보안 대책 수립방안

해킹과 비교해 본 CTEM 기술 범위

1차 관문의 보안체계는 네트워크 침입 차단 솔루션으로 방어되고,
EASM 점검은 해당 솔루션으로 탐지 / 차단 되어야 합니다.



Proxy

NG AV / EDR / XDR

Web Isolation

NGFW / UTM

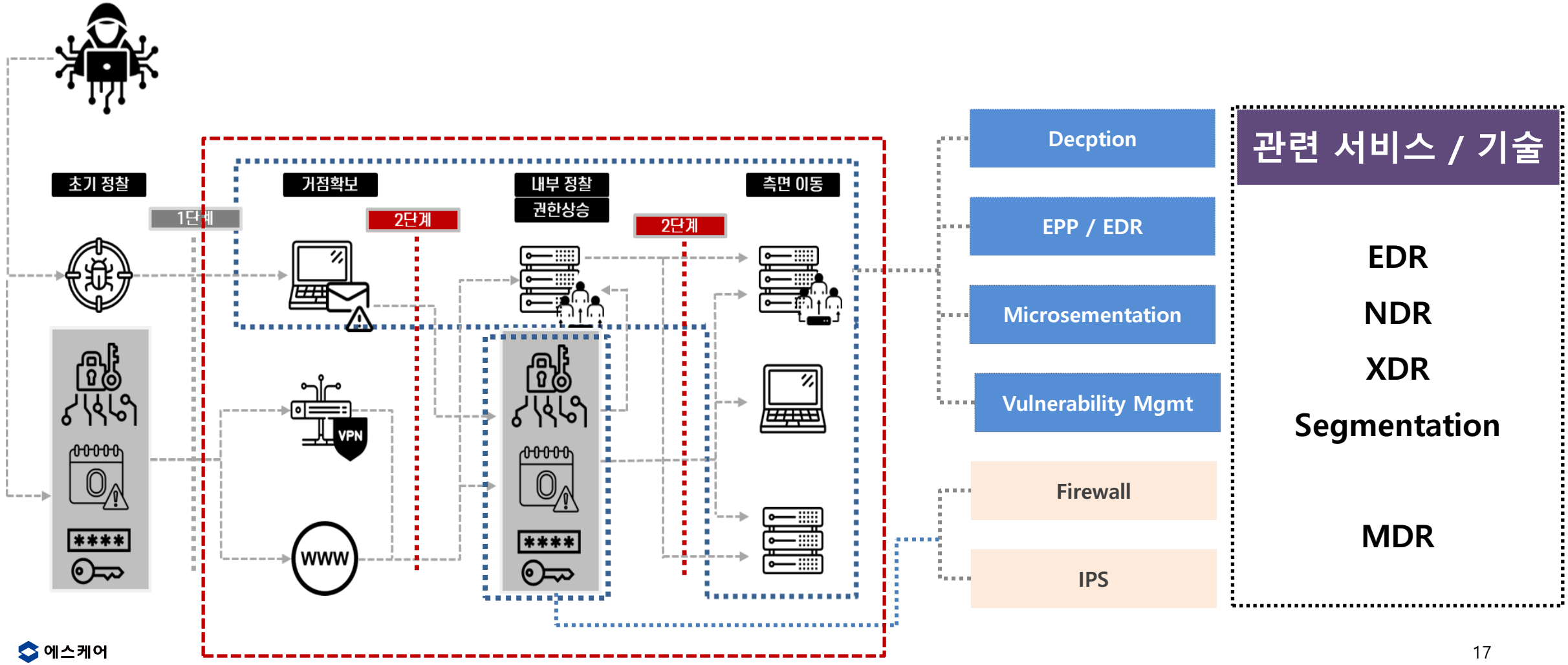
NG VPN (SSE)

IPS

관련 서비스 / 기술
SASE / ZTNA
NGFW/UTM
EDR / XDR
MFA
ASM
CTI

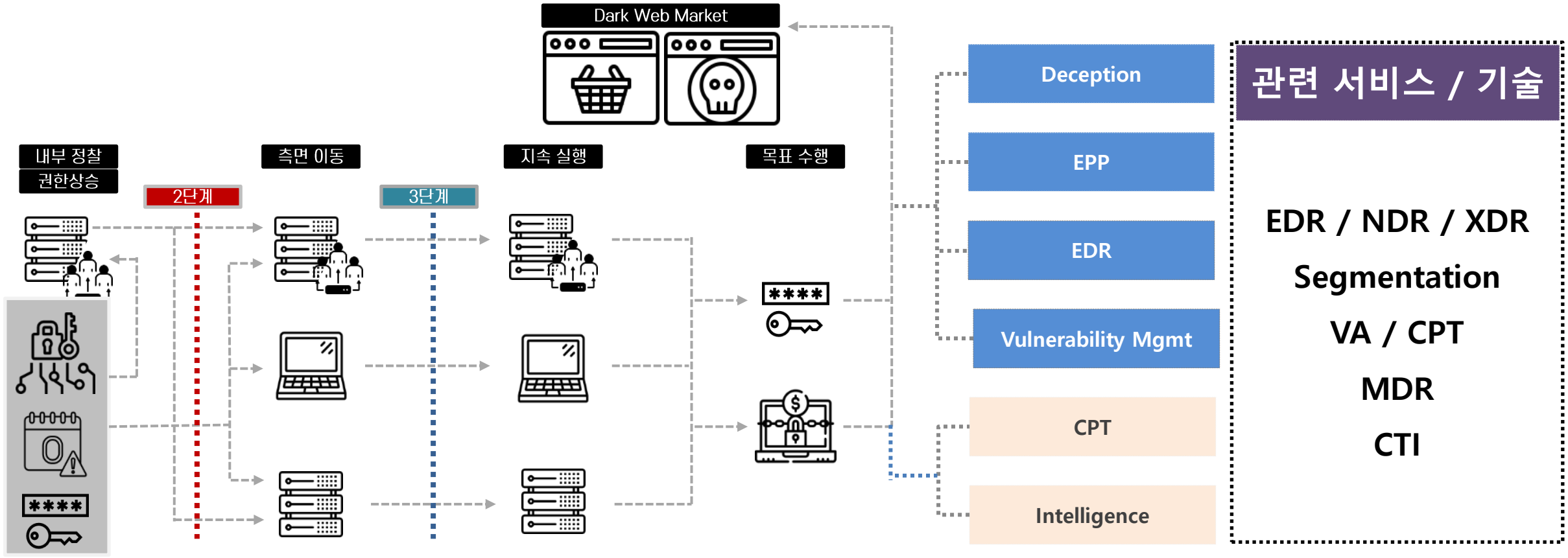
해킹과 비교해 본 CTEM 기술 범위

외부의 해커의 관점의 2차 관문, 내부 침해 확산 방지 솔루션으로 방어되어야 합니다.



해킹과 비교해 본 CTEM 기술 범위

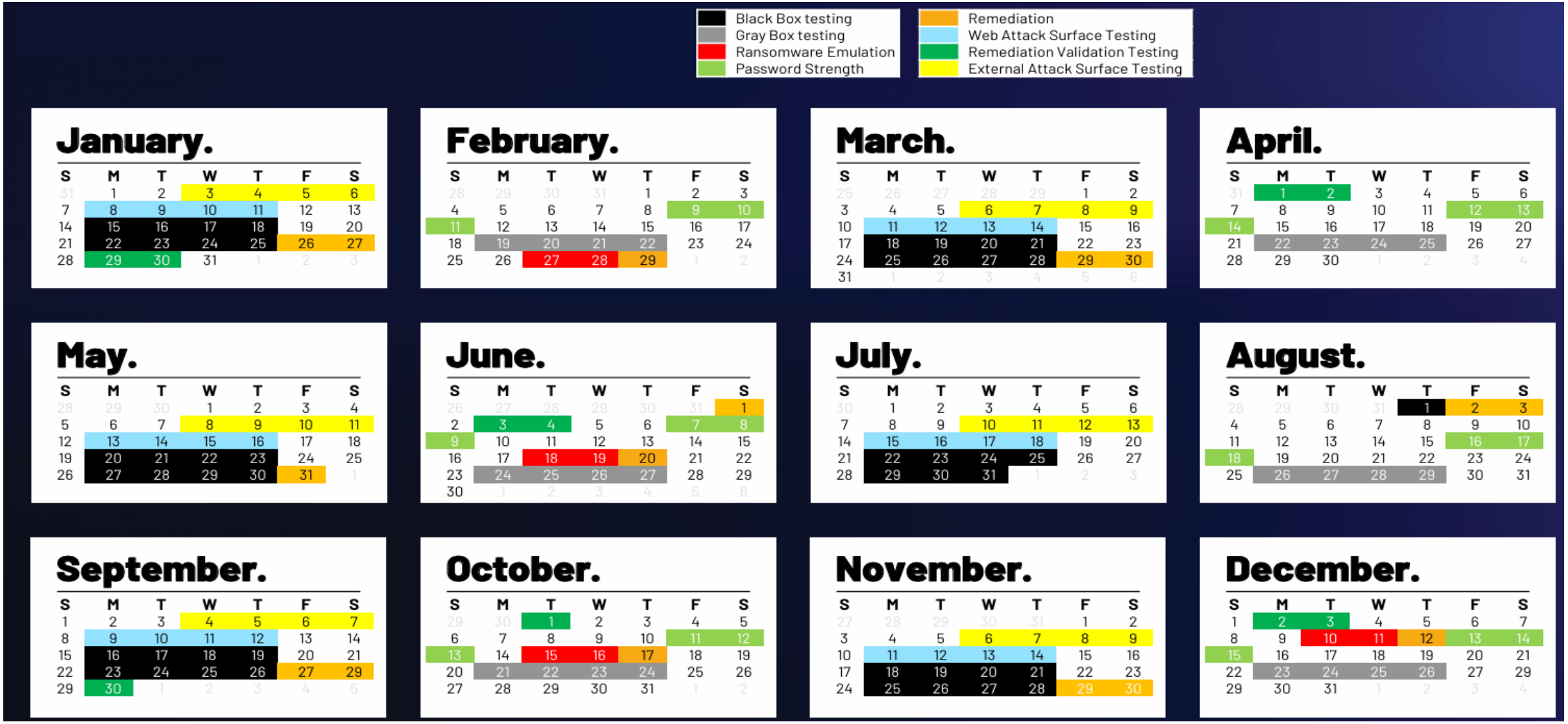
3단계 지속적 위협관리를 위해 필요한 요소는 지속적 취약점 관리 체계를 구축해야 합니다.



글로벌 기업의 CTEM 관리 TASK 상세

구분	내용	적용 대상
Blackbox Testing	소프트웨어의 내부 구조나 구현 세부사항을 알지 못한 채, 외부에서 기능과 동작을 테스트 (해커 관점)	EASM, IASM SV, CPT
Graybox Testing	소프트웨어의 내부 구조 및 동작 방식을 이해한 상태에서 일부 권한을 부여하여 테스트 (일부 권한, 계정 반영)	IASM, BAS, SV, CPT
Ransomware Emulation	랜섬웨어의 행동을 모방하여 보안 시스템, 방어 메커니즘, 조직의 대비 상태를 테스트하는 과정	IASM, BAS, SV, CPT
Password Strength Test	사용자가 생성한 비밀번호의 보안 수준을 평가하는 과정으로, 비밀번호가 얼마나 강력하고 안전한지를 측정	CTI, IASM, CPT
Remediation Validation Test	보안 취약점이나 문제를 수정(완화)한 이후, 해당 수정이 효과적으로 작동하는지 확인하고 검증하는 테스트	IASM SV, CPT, SOAR
Web Attack Surface Test	웹 애플리케이션의 보안 상태를 평가하기 위해 공격 표면을 식별하고 분석하는 과정	CTI, EASM, IASM, CPT,
External Attack Surface Test	조직의 외부 자산과 네트워크가 외부 공격자로부터 얼마나 노출되어 있는지 평가하는 과정	EASM, IASM

글로벌 기업의 CTEM 관리 스케쥴 (예시)



감사합니다 !

(주)에스케어