SECURITY · 바이브 코딩 거버넌스

바이브 코딩 환경의 공격 표면 관리 방안

윤재웅 · www.kpredict.co.kr · 2026.10

1. 배경

- 샌드박스(Power Platform 개발 환경)와 가상 PC 기반 바이브 코딩 환경이 갖춰지면, 비개발 직원이 직접 만드는 앱과 사이트가 빠르게 늘어납니다.
- AI 도구로 만든 결과물은 빠르게 늘지만, 어디에 배포되고 무엇이 외부에 노출되는지 파악하기 어렵다는 보안 우려가 있습니다.
- 이 자료는 바이브 코딩을 **막기보다 안전하게 넓히기 위한** 공격 표면 관리 방안을 정리한 것입니다.

2. 공격 표면 관리(ASM)와 지속적 위협 노출 관리(CTEM)

개념	내용
공격 표면 관리 (ASM)	인터넷에 노출된 회사 자산(도메인, 서브도메인, IP, 웹앱, 인증서, 열린 포트 등)을 지속적으로 찾아내고 위험도를 관리하는 방식
지속적 위협 노출 관리 (CTEM)	자산 발견, 취약점 분석, 공격 경로 파악, 조치 우선순위를 하나의 체계로 묶어 반복 관리하는 방식

> **기대 효과** 특정 취약점(예: PHP 이슈)이 발생했을 때 "전체 자산 중 어디까지 조치됐고 어디가 남았는지"를 한눈에 보고할 수 있습니다.

3. 바이브 코딩에서 생기는 노출 유형

유형	예시	기존 ASM으로 탐지
회사 도메인·IP에 배포	회사 서브도메인에 연결된 앱	가능
외부 호스팅·개인 계정에 배포 (섀도 IT)	개인 계정의 클라우드 호스팅 주소	어려움 (회사 자산과 연결 고리 없음)
코드 내부 문제	API 키 하드코딩, 취약한 라이브러리 사용	불가 (코드 보안 도구 필요)

4. 관리 방안

① 발견: 네트워크 기록과 CASB로 외부 서비스 사용 파악

- 프록시, 방화벽, DNS 기록 및 CASB(예: Microsoft Defender for Cloud Apps)로 직원들이 사용하는 외부 호스팅·개발 서비스를 식별
- 회사 IP 대역 스캔만으로는 외부 호스팅 앱을 찾을 수 없으므로, "누가 어디에 접속·배포했는지"를 기준으로 발견

② 등록: 발견한 자산을 공격 표면 관리 목록에 시드로 등록

- EASM 도구는 도메인, 서브도메인, IP를 직접 등록(시드)할 수 있어, 외부 호스팅 앱도 등록 후 지속 점검 가능
- 샌드박스·바이브 코딩 환경에서 만든 앱은 **배포 시 자산 등록을 기본 규칙**으로 설정

③ 코드 보안: 개발 단계 점검 도구 적용

- 시크릿 스캔(비밀 정보 노출 감지), 의존성 점검(SCA), 정적 코드 분석(SAST)
- API 키 등은 코드가 아닌 환경 변수로 관리하도록 가이드

④ 환경 통제: 정해진 환경에서 만들고 배포

- 샌드박스·가상 PC 환경 안에서 개발·배포하도록 하면 노출 범위가 명확해져 관리가 쉬워짐
- 통제된 환경 제공 자체가 바이브 코딩 확대와 보안을 동시에 달성하는 방법

5. 도구 예시

- **Microsoft Security Exposure Management**: 기기, 계정, 애플리케이션, 하이브리드 환경 데이터를 모아 공격 표면을 통합 관리. 공격 표면 관리, 공격 경로 분석, 통합 노출 인사이트로 구성. 보유한 Microsoft 365 보안 라이선스로 사용할 수 있는지 먼저 확인
- Microsoft는 2026년 4월, AI 기반 자동화 공격에 대비해 패치, 오픈소스, 소스 코드, 인터넷 노출 자산, 기본 보안 위생 점검을 권고하는 가이드를 Exposure Management를 통해 제공
- 그 외: Tenable, Qualys, Rapid7, Palo Alto Networks(Cortex Xpanse), CrowdStrike 등

6. 단계별 추진안

단계	내용
1단계 (시범)	샌드박스·바이브 코딩 환경에서 만든 앱을 대상으로 자산 등록 규칙 적용
2단계	CASB 등으로 외부 서비스 사용 현황 파악 및 주요 자산 등록
3단계	취약점 발생 시 조치 현황을 공격 표면 기준으로 보고하는 체계 정착

7. 기대 효과

- 보안 이슈 발생 시 전체 노출 자산 기준의 조치 현황 가시화
- 바이브 코딩·시민개발 확대와 보안 관리의 양립
- 현업은 쉽게 만들고, 정보보호는 안심하고 관리하는 구조 마련

참고 자료

- Microsoft Highlights Security Exposure Management at Ignite (ITPro Today)
- Microsoft Launches New Security Exposure Management Tool (Petri)
- MC1288236 - Microsoft Security Exposure Management Secure Now