SYSTEMS | ON-PREMISE ASSET DETECTION & RESPONSE

Contellix ADR

자산 기반 탐지·대응 플랫폼 — 맥락분석 엔진으로 “지금 위험한 자산”을 가려냅니다

자산 Discovery · 맥락엔진 기반 위험도 · 정책 탐지·대응 · 취약점 우선순위 · 즉시 조치 4종 · 완전 On-Premise(망분리환경)

Agentless · Passive

메타데이터만 수집

인터넷 연결 없이 Onprem 구축 및 운영

IT · OT · IoT · Cloud

제품소개서 요약본 (Pitch) · 2026. 11

“자산을 모르면 방어할 수 없습니다”

종합분석

대시보드

노출 위험

리포트

노출 경로 Map

ATT&CK 커버리지

차단 IP 리스트

즉시 조치 CVE

즉시 조치 Activity

PCAP 분석

자산

자산 목록

장비 목록

애플리케이션

운영체제

Purdue 모델

Cloud 자산

PCAP 분석 결과

사용자

보안 위협 대응

Risk Indicators

Activities

종합분석 / Network Map

노출.공격 경로 Map

Site · 바운더리 기준으로 자산과 외부 통신을 한 화면에서 확인합니다.

위협 중심 | 외부 노출 | 전체 구성 | ↻ | 내보내기 | 전체화면

Site · 바운더리 토폴로지 | 표시 자산 77/77 | 유선 66 | 무선 3 | 미지정 8 | 외부 호스트 19 | Alert 자산 2

지도에서 자산 찾기 | - 100% +



드래그하여 이동 · 휠로 확대/축소 · 자산을 선택하면 연결 경로를 강조합니다 | 단축키

외부로(OUT) | 비코닝 의심 | 높음 60+ | 보통 35+ | 차단됨 | 유선 | 무선 | 미지정 | 외부

바운더리 자산	외부 통신 피어	외부 연결 자산	악성 연결	고위험 자산	즉시조치 CVE
69	212	3	0	2	0
전체 자산 77개 중 표시	지도에 19개 표시	외부와 통신한 내부 자산	탐지된 악성 연결 없음	위험도 60 이상	즉시 조치할 취약점 없음

EXECUTIVE SUMMARY

Contellix ADR 한눈에 보기 — 다섯 가지 약속

보안 실무팀이 매일 부딪히는 “무엇이, 어디서, 얼마나 위험한가”에 자산 단위로 답하고, 경영진에게는 세 지표와 즉시 조치 4종으로 답합니다

1 모든 연결 자산을 본다

- Passive DPI · Topology Mapper · Adaptive Active Query 3중 탐지
- 자산 · 장비 · 외부 호스트를 네트워크 범위로 구분, 게이트웨이 자동 추정
- IT·OT·IoT·가상화·클라우드 워크로드

2 맥락으로 위험을 판단한다

- 위협·실효 취약·노출·영향 네 렌즈 융합
- “왜 이 점수인가” 점수 흐름·기여 가중치·산식까지 제시
- 자체 Early Warning 엔진 — KEV 등재 전 선행 경보

3 정책으로 탐지·대응한다

- 내장 정책 199개 + 커스텀 정책, 반복·스케줄·소급 평가
- Risk Indicator 필수 + Alert 선택 설계
- Alert·태그·경계·Enforcement·Email/Syslog/Webhook 발송

4 즉시 조치로 답한다

- 위험도 임계값 이상 자산을 4가지 결과로 확정 제시
- 즉시 조치 자산 · 즉시 차단 외부IP · 즉시 조치 CVE · 즉시 조치 Activity
- C-Level 대시보드 — 해킹·정보 유출·CVE 악용 가능성 세 지표

5 고객망 안에서 완결된다

- 분석 엔진까지 고객 내부 설치, 인터넷 불필요
- 서명된 Intelligence 패키지 오프라인 업데이트 · TLS 1.3/mTLS · 백업·복구
- 망분리·N2SF·데이터 주권 요건 충족 · KST 표시

이 요약본의 구성

01 Why Asset
02 솔루션 개요·구성도
03 자산 Discovery
04 핵심 차별점·맥락분석 엔진
05 정책 라이브러리
06 Early Warning·C-Level·즉시 조치 4종
07 국내 환경 최적화·도입 로드맵

한국을 강타한 사이버 전면전 — 공통점은 “보지 못한 내부 자산”

대형 침해사고는 모두 인지하지 못한 자산의 방치된 취약점과 내부 트래픽 이상행위에서 시작됐습니다

SKT

3,600만 건 개인정보 유출

리눅스 서버 CVE 취약점 + APT 장기침투(2021년~)로 HSS 접근

금융권 25곳

랜섬웨어 ‘킬린(Qilin)’ — 2TB 다크웹 공개

MSP 통한 연쇄 감염, 자산운용사 약 30여 개 피해

쿠팡

3,370만 계정 무단 열람

내부 인증·토큰 관리 취약으로 서버 비인가 접근

롯데카드

297만 명 신용정보 유출 · AD 서버 감염

2017년 공개된 CVE 패치 미적용 결제서버 공격

업비트

445억 원 상당 가상자산 탈취

서명 권한 탈취에 따른 정상 트랜잭션 기반 유출

넷마블

총 3,711만 건 정보 유출

임직원 계정 탈취(Credential 탈취)

공통 원인 — 인지하지 못한 내부 자산의 방치된 취약점(CVE)과 내부 네트워크 이상행위를 실시간 감시하는 체계의 부재

※ 언론 보도 기준으로 정리한 공개 사례입니다. 사고 원인은 각 사의 공식 발표·조사 결과에 따라 달라질 수 있습니다.

방어자의 현실 — 쏟아지는 취약점, 맥락 없는 경보

취약점은 사람이 읽을 수 있는 속도를 넘어섰고, 경보는 “어떤 자산의 무엇부터”를 말해주지 않습니다

120건

매일 신규 생성되는 CVE — 기존 CVE 변형까지 일 평균 220건

40,000+

CVSS 9.0 이상 초고위험 CVE 누적 — 7.0 이상 55,000여 건

매월 17건

실제 공격에 악용 확인(KEV) — 즉시 조치하지 않으면 침해로 직결

! 자산을 100% 알지 못한다

수작업 대장·부정확한 CMDB, 미인지(Shadow) 자산, OT·IoT 비관리 장비

! 경보에 맥락이 없다

단순 이벤트 경보 → 경보 피로. 정작 치명적인 약점은 스크리닝에서 빠진다

! 정보가 흩어져 있다

자산·취약점·트래픽이 서로 다른 도구에 분산 — “어떤 자산의 무엇부터” 판단 근거 부재

필요한 것은 CVE 목록이 아니라 — 자산 · CVE · 트래픽 · 인텔리전스를 융합한 “맥락적(Contextual)” 판단 능력입니다

Contellix ADR — See · Protect · Detect & Respond · Manage

Agent 없이 · 스캔 없이 · 업무 중단 없이 — IT 서버·PC부터 IoT·OT·가상화·클라우드 워크로드까지, 고객망 안에서 완결되는 자산 중심 탐지·대응 플랫폼

See – Asset & Traffic

완전한 자산 가시성

- 미러링 DPI로 통신하는 모든 자산을 수 분 내 발견
- Topology Mapper·Adaptive Active Query로 조용한 자산까지
- 자산·장비·외부 호스트 구분, 게이트웨이 자동 추정, Purdue 판정

Protect

위험 우선순위 · 선제 방어

- 맥락분석 Risk Score — 먼저 조치할 자산을 제시
- 도달 가능성 기반 CVE 우선순위 · 자체 Early Warning 엔진
- 공격 경로 분석 · 조치 작업 (Remediation) 묶음·배정·자동 검증

Detect & Respond

탐지 · 즉시 조치

- 내장 정책 199개 + 커스텀 정책, 반복·스케줄·소급 평가
- IOC·시그니처·Baseline 이상·킬체인 진행 탐지
- 즉시 조치 4종(자산·외부 IP·CVE·Activity) · Enforcement · 알림 발송

Manage

지속 운영

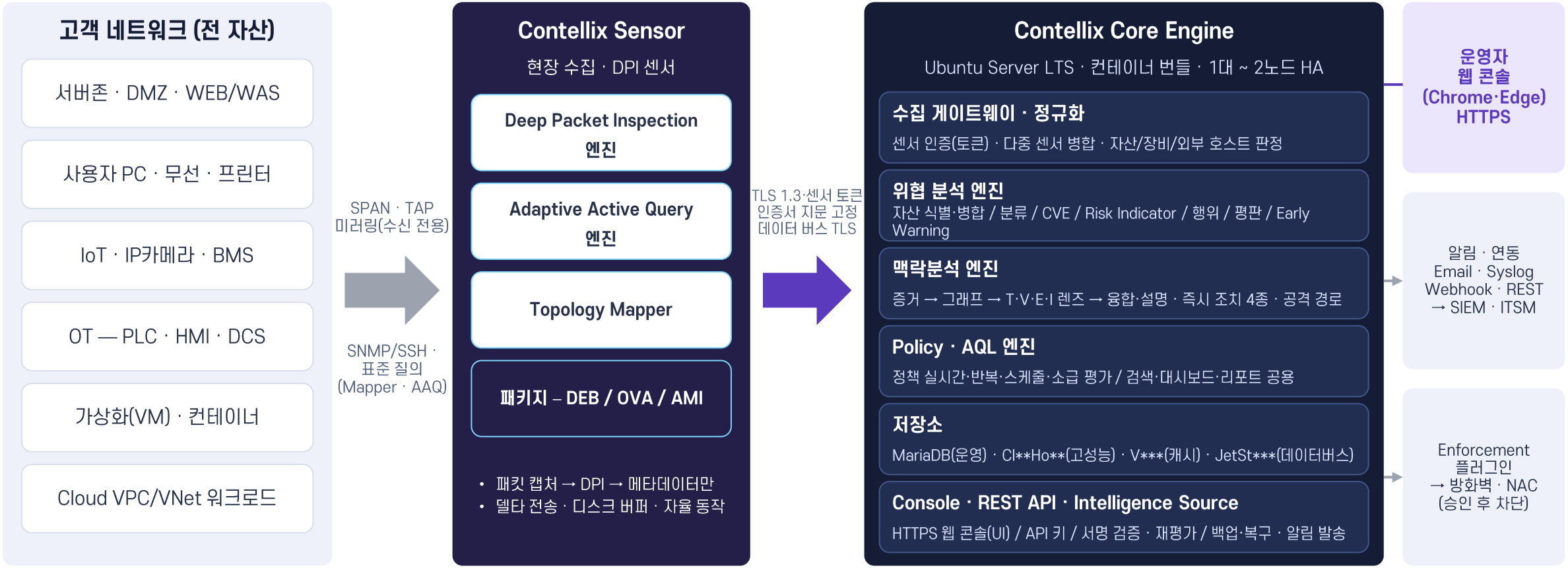
- C-Level 대시보드 · 위젯 대시보드 · 리포트 템플릿 14종
- Sites·Boundaries·네트워크 범위 ·Network Map·ATT&CK 커버리지
- 서명 패키지 오프라인 업데이트 · 백업·복구 · 감사 로그 · KST

자산 중심 보안 | Agentless · Passive 우선 | 메타데이터만 수집 | **Contextual 융합 판단** | Baseline 정상 행위 | See → Respond 사이클

Query-driven(AQL) | Policy 중심 운영 | 완전 자립 운영 | **맥락분석 엔진 (Contextual Analysis Engine)** | 국내 환경 최적화

시스템 구성도 — 미러링과 센서, 그리고 고객 내부의 분석 서버로 완결

On-Premise 구축 모델: 모든 수집·분석·탐지·대응이 고객망 안에서 이루어지고, 외부 지식은 서명된 패키지로만 반입됩니다



✓ Agent 설치 없음 ✓ 네트워크 구성 변경 없음 ✓ 운영 무중단(수신 전용 미러링) ✓ 인터넷 연결 불필요 ✓ 전 구간 TLS · 비밀정보 암호화

자산 Discovery — 세 가지 기술로 수 분 내 발견하고 교차 검증합니다

자산에 패킷을 보내지 않는 Passive가 기본, 조용한 자산은 스위치 조회와 안전 검증된 표준 질의로 보강합니다 — 능동 질의는 데이터 소스(ST-11)를 켠 대역에서만

01 트래픽 미러링 DPI (Passive)

- SPAN/TAP 미러링 트래픽 심층 분석으로 통신하는 모든 자산 발견
- 자산에 패킷을 보내지 않음 — OT·의료·레거시 장비에 안전
- OUI·DHCP 옵션·mDNS/SSDP·SMB/Kerberos·TLS JA3/JA4·User-Agent·LLDP/CDP·OT Identity 페이로드를 수동 추출
- ARP 송신자·NBNS·mDNS 응답·SSDP SERVER도 증거로 — 미러 소스 밖 장비도 IP/MAC/이름/제조사 수준으로

02 Adaptive Active Query (선택)

- Passive로 못 본 자산 탐지 + 기존 자산 정보 보강(OS 빌드·설치 SW·펌웨어)
- 2단계 — ① Safe Ping Sweep(ICMP·ARP·산업용 브로드캐스트, 64 IP 그룹·적응형 감속·대역별 시간 예산) ② 데이터수집(동적 프로토콜 순서화·최소 질의)
- IT: WMI/WinRM·SSH·SNMP / OT: S7 SZL·CIP Identity·Modbus FC43·BACnet Who-Is — 읽기 전용 함수 코드 화이트리스트, OT 기본 비활성
- 실행 창·블랙아웃을 요일·시간 UI로, 데이터 소스 없음/DISABLED = 스캔 없음

03 Topology Mapper

- 스위치·라우터를 SNMP v2c/v3 · SSH(읽기 전용)로 조회 — 자격증명은 센서 토큰으로 센서에만 전달
- 포트-MAC · ARP · LLDP/CDP · VLAN · 라우트 → 통신이 적은 자산과 물리 위치(스위치·포트) 확보
- BFS 토폴로지 확장 → Network Map 입력, 장비당 동시 질의 1개·속도 제한

발견한 자산을 "중복 없는 한 자산"으로 관리하는 인벤토리 엔진

자산 고유 ID

MAC을 가진 자산은 mac: 키, 옛 키는 별칭 — 하드웨어 시리얼·데이터 소스 ID·Hostname+OS·IP+시간창을 조합해 중복 없는 ID

저장 시 신원 대조

키 → MAC → IP 순으로 대조해 같은 자산에 합치고, 식별자 소유권은 최근에 본 자산에게 — 라우터 뒤의 상대는 게이트웨이 MAC을 공유하지 않음

수명주기 · 재분류

미관측 30일 Inactive → 90일 자동 삭제(ST-43), 대역·Intelligence 변경 시 소급 재분류 (ReclassifyLive) · 운영자 수정 속성은 잠금

Cloud 자산

AWS·Azure·GCP 미러링 트래픽을 Cloud Sensor가 DPI — ENI MAC+세션 매핑으로 식별, Category "Cloud" 분류

KEY DIFFERENTIATORS

무엇이 다른가 — 트래픽으로 증명하는 세 가지 고유 기술

점수를 더하는 대신 관계를 읽고, 목록 대신 닿는 것을 고르고, 공식 발표보다 먼저 경보합니다 — 세 기술 모두 인터넷 없이 고객망 안에서 계산됩니다

1 맥락분석 엔진

[특허 출원 #1]

같은 OS라도 위험은 다릅니다

위협 · 실효 취약 · 노출 · 영향 네 렌즈를 융합해 자산마다 위험도 0~100과 "왜 이 점수인가"를 함께 냅니다

가중 합산 자산의 83%가 Medium [예시]
맥락분석 Low 13 · High 65 · Critical 100

2 CVE 실효 악용 도달성

[특허 출원 #2]

CVSS 10.0보다 8.1이 먼저 입니다

취약 서비스의 응답을 트래픽에서 실제로 봤는가로, 수천 건 중 지금 공격 가능한 CVE를 가려냅니다

EternalBlue CVSS 8.1 → 실효 악용 **85%**
IIS FTP CVSS 10.0 → 실효 악용 **38%**

3 Early Warning

자체 엔진 · 5인자 가중 모델

KEV 등재 전에 먼저 경보합니다

Intelligence 선행 신호와 우리 자산의 위험도를 융합해, 악용 직전의 CVE와 영향 자산을 지목합니다

같은 서버 · 같은 CVE [예시]
익스플로잇만 56% → **등재 63%** → KEV 70%

분석이 끝나면 **즉시 조치 4종** 자산 · 차단 외부IP · CVE · Activity + **C-Level 세 지표** 해킹 · 정보 유출 · CVE 악용 가능성

왜 “맥락”인가 — 가중 합산 점수는 우선순위를 주지 못합니다

실환경 681대 분석: 요소를 더하기만 하는 위험 점수는 대부분의 자산을 Medium으로 뭉개 버립니다. Contellix ADR은 요소 간 “관계”를 읽습니다

일반적인 분석 기법 – 가중 합산의 경우 [예시]

83%
Medium으로 판정 (예시 - 564대)
어디부터 손댈지 알 수 없음

94%
EoS/EoL OS 단일 요인 (예시 - 642대)
노출·행위·취약점 맥락 없이 “OS가 오래됨” 하나로 평가

680대
Business Impact 미지정
20% 가중 요소가 비어 있음 — 역할 추론 필요

413대
자산 유형 미식별(N/A)
역할·영향 추정이 전혀 없음

맥락분석 (맥락분석엔진)이 가르는 세 자산

Low 13

격리된 내부망의 Windows 7 PC
EoS OS이지만 노출 서비스 없음 · 인터넷·게스트망 도달 불가 · 행위 없음 → 등급 Low. 조치 우선순위에서 내려감

High 65

게스트망에서 접근되는 Windows 7 PC
SMBv1 사용 + EternalBlue(KEV) + SMB 445 서비스 관측 + EoS OS — 세 출처가 같은 가설을 확증 → High

Critical 100

인터넷 노출 + KEV + C2 통신 서버
외부 인바운드 수락 · KEV 취약점 도달 가능 · IOC 일치·비코닝(킬체인 7단계) · 역할 서버 → Critical

맥락분석 엔진 — 증거를 모으고, 관계를 읽고, 네 렌즈로 판단합니다

하나의 관측을 그 자체로 판단하지 않고, 자산의 역할·위치·실효 취약·외부 지식·행위 흐름을 함께 읽어 최종 위험도를 정합니다.

입력

- 행위(Activity · IP 연결)
- 자산 프로파일 · 통신 이력
- 취약점(CVE·KEV·EPSS·EW)
- 외부 인텔리전스 (IOC·EoL·Exploit)
- 정책 Risk Indicator(모든 정책)

① 증거 모델

- 모든 입력을 하나의 Evidence로 정규화
- Class · 가설 · 확률 p0 · 신뢰도 · 반감기
- p = p0 × conf × 2^(−Δt/반감기)
- 입력이 늘어도 증거 하나만 추가

② 맥락 그래프

- 노드: 자산 · 외부 호스트 · 서비스 · CVE
- 간선: TALKS · AUTH · ADMIN · IN_BOUNDARY · HAS_VULN · HOSTS
- 서비스 관측 · 노출 · 인증 중심성 · 피어 위험 파생

③ 네 렌즈

- **T** 위협 — 지금 공격받고 있는가
- **V** 실효 취약 — 뚫리면 무엇이 열리는가
- **E** 노출 — 공격자는 어디에 닿는가
- **I** 영향 — 뚫리면 얼마나 아픈가

④ 융합 · 출력

- noisy-OR · 교차 확증 · 킬체인 · 전염
- Risk 0~100 · 등급 · 히스테리시스
- “왜 이 점수인가” 점수 흐름 · 기여 가중치 · 서술 · 권장 조치
- 즉시 조치 4종 · C-Level 세 지표 · Alert 우선순위 · AQL context.*

설계 핵심 네 가지

① 증거 융합 모델 — 네 입력을 하나의 증거로, 자산 중심 그래프에

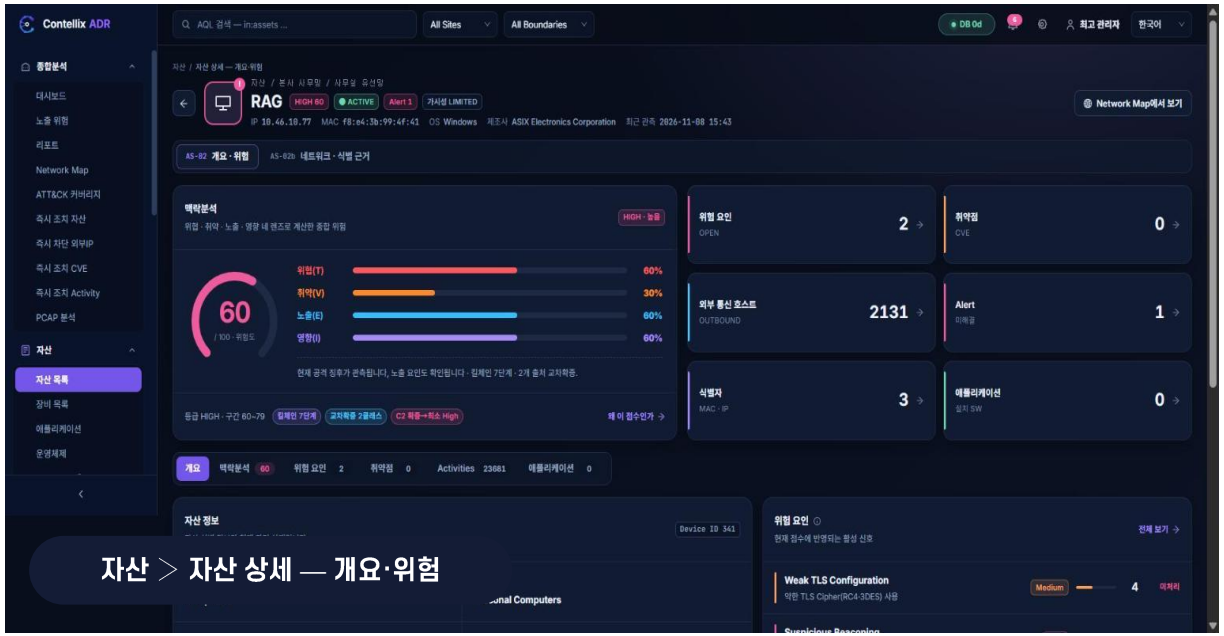
② 도달 가능성 기반 실효 취약 — CVE가 없어도 취약 통신으로 평가

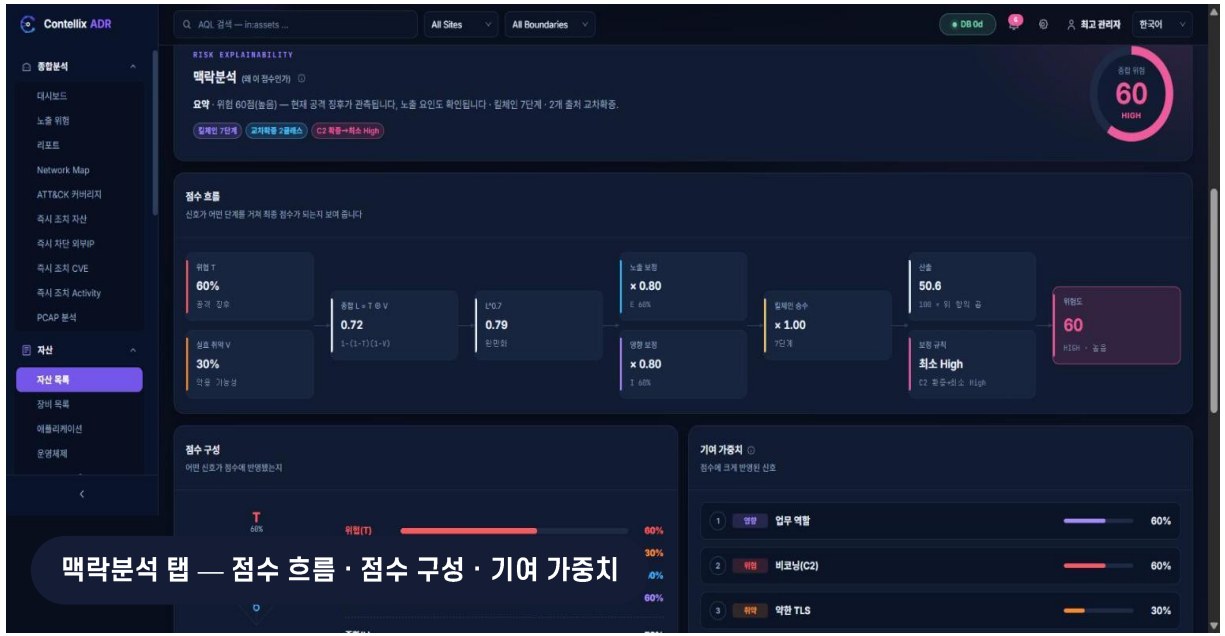
③ 교차 확증 + 킬체인 진행 — 단일 신호 과장 방지, 연쇄를 자산 단위로

④ 설명 가능성 — 모든 점수에 근거 3개 · 점수 흐름 · 한국어 서술

자산 상세 — 맥락분석 카드와 “점수 흐름”으로 Risk 점수에 이유를

머리(유형·위험 고리·배지) → 맥락분석 카드(게이지·네 렌즈) + 요약 카드 6개 → 탭(개요 · 맥락분석 · 위험 요인 · 취약점 · Activities · 애플리케이션)





맥락분석 카드

종합 위험 게이지(60/100 · HIGH) · 네 렌즈 막대(위협 60% · 취약 30% · 노출 60% · 영향 60%) · 요약 한 줄 · 배지(킬체인 7단계 · 교차 확증 2클래스 · C2 확증→최소 High)

요약 카드 6개

위험 요인(OPEN) · 취약점(CVE) · 외부 통신 호스트(OUTBOUND 2,131) · Alert(미해결) · 식별자(MAC·IP) · 애플리케이션 — 카드가 곧 링크

점수 흐름 · 산식

위협 T → 종합 L → L^0.7 → 노출 보정 → 영향 보정 → 킬체인 승수 → 산출 → 보정 규칙 → 위험도. “근거 및 해석”에 산식 항(stage_mult · l_term · e_term · i_term)까지

기여 가중치 · 권장 조치

점수에 크게 반영된 신호 Top 3(업무 역할 · 비코닝(C2) · 약한 TLS)를 막대로, 한국어 서술과 Remediation 템플릿 기반 권장 조치 — LLM 미사용

취약점 실효 악용 도달성 — CVSS 10.0보다 CVSS 8.1이 위에 오는 이유

VulnProb 산식이 엔진에 들어가 있습니다. 취약점 목록은 CVSS가 아니라 "실효 악용(도달성)" 확률로 정렬되고, 즉시 조치 CVE·C-Level CVE 지표가 같은 값을 읽습니다 **[특허 출원 #2]**

VulnProb = base × exploit × reach × av × conf

- **base** 0.5×CVSS/10 + 0.5×EPSS
- **exploit** KEV 1.0 · 공통 Early Warning 0.9 · 공개 Exploit 0.8 · 그 외 0.5
- **reach** 취약 서비스포트의 서버 응답이 DPI로 관측되면 1.0, 제품 매칭만이면 0.60, 추정 0.35
- **av** CVE 공격벡터(av) × 노출 — AV:N이고 외부 노출(E ≥ 0.8)이면 1.0, 내부 0.7, Adjacent 0.5, Local/Physical 0.2
- **conf** CPE 매칭 신뢰도 등급(Confirmed · High · Medium · Low)

검증 — 같은 자산, 두 CVE의 순서가 뒤집힙니다

CVE	CVSS	KEV	도달	실효 악용
CVE-2017-0144 (EternalBlue)	8.1	●	SMB 445 서버 응답 관측 1.0	**85%**
CVE-2010-3972 (IIS FTP)	10.0	—	제품 일치만 0.6	**38%**
CVE-2017-0144 (서비스 미관측)	8.1	●	제품 일치만 0.6	**34%**

등급 — 즉시 악용(실효 ≥ 0.6) · 도달 가능(서비스 관측) · 잠복. "심각도가 아니라 도달성 × 악용성"으로 정렬하므로 CVE 수천 건 중 지금 공격 가능한 것이 위로 올라옵니다.

맥락 스냅샷 영속화

자산별 맥락 현재값(T·V·E·I·L·단계·확증·서술·권장 조치)을 ctx_snapshot에 저장, 추이는 일별·시각별 이력 — 대시보드·리포트·즉시 조치 화면이 같은 값을 읽습니다

AQL context.* 9필드

risk · level · threat · vulnEff · exposure · impact · killChainStage · progression · corroboration — 검색·정책 조건에서 맥락을 직접 사용(비교 질의 context.exposure>=0.85)

설명 · 권장 조치 · 산식

서술(narrative)은 한국어 템플릿으로 생성(LLM 미사용), 권장 조치는 Remediation 템플릿에서 — v1.3.0부터 산식 항(RiskExplanation)까지 저장해 "근거 및 해석"에 표시

Policy Library — 내장 정책 199개를 켜고 · 고치고 · 만든다

실환경 검증된 정책 199개를 탐지 주제별로 재구성하고 국내 요구(N2SF·망분리)와 Cloud를 더했습니다. 정책은 코드가 아닌 데이터로 배포·버전 관리되고, 커스텀 정책(CUS-n)을 복제·생성합니다

카테고리(라이브러리 11종)	수	대표 정책
Threat Detection · Known Attacks	47	Tor · Cobalt Strike · 싱크홀 DNS, Log4j·Shellshock·ProxyLogon 공격 시도, 비코닝
External to Internal Communication	17	외부 IP와 RDP·VNC·SSH·SMB·FTP·Telnet·Modbus 세션
Authentication · Insecure Traffic	41	기본/약한 자격증명, 익명 FTP·SMB, Redis·MongoDB 무인증, 평문 자격증명, 약한 TLS
Configuration Hygiene · Deprecated SW/HW	37	SNMP public 커뮤니티, SMB 서명 해제, EoL/EoS OS·펌웨어
OT/ICS Risk	14	PLC 구성 변경·업로드·펌웨어·모드 변경·정지, 비감독 장비의 PLC 접근
Vulnerabilities	17	Zerologon·ModiPwn 취약 자산, KEV 보유, Early Warning CVE 보유 (VUL-013)
Device Behavior · Cloud Exposure	26	포트 스캔, 생성형 AI·소셜미디어 통신, 인터넷→관리 포트, 운영↔개발 VPC
국내 규제 · 지침 / 맥락(CTX)	포함	N2SF 자산식별·지속 검증, 망분리 위반 정황 / 맥락 Risk Indicator

정책 = 무엇으로 이루어지나

- Base Entity 7종 — Activity · Device · IP Connection · Vulnerability
- 조건 트리 — AND/OR 중첩, 잎은 AQL 절(부정 · 연관 하위 조건)
- 적용 범위 · 반복 조건("n초 안에 m회", 자산/쌍 단위) · 스케줄(요일·시간대) · 소급 평가(지난 N일)
- 출력(Action) · MITRE 라벨 · 속성 · 8개 탭 편집기 · 드라이런

Risk Indicator 필수 + Alert 선택

- 정책은 조건을 한 번만 평가 — 일치하면 Risk Indicator를 항상 남기고, Alert는 켜 둔 정책만 생성
- 같은 탐지를 Alert용·RI용 둘로 복제할 필요 없음 → 정책 수 절반, 탐지 일관성 확보
- 튜닝 기간에는 Alert만 꺼 두고 Risk Indicator로 추이를 관찰 — 라이브: 199 활성 · Alert 보유 5
- 기존 정책 가져오기(CSV) 시 A/R 쌍 자동 병합

Early Warning — KEV 등재 전에, 악용 직전의 CVE를 지목합니다

공식 악용 확인 목록(KEV)은 "이미 악용된 뒤"의 기록입니다. Contellix ADR은 외부 선행 신호와 우리 자산의 위험도를 자체 엔진으로 융합해, KEV 등재 전에 영향 자산과 함께 경보합니다 — 인터넷 없이 고객망 안에서 계산



5인자 가중 모델 — EW 점수 = Σ 가중치 × 인자 값(0~1) · 등재 기준 0.6

외부 선행 신호 75% — 공통 EW | 현장 신호 25%

EPSS 추세	공개 익스플로잇	벤더·KISA 권고	IOC 연관	고위험 자산 연관
30%	15%	15%	15%	25%

- EPSS 추세 = 최근 30일 상승폭 ÷ 0.10 · 공개 익스플로잇 · 긴급 권고 · 활성 IOC = 있으면 1 · 고위험 자산 = 위험도 ≥ 80(설정) 자산이 미해결로 보유
- 가중치 · 사용 여부 · 등재 기준은 운영자가 변경 · 데이터 없는 인자는 빼고 재분배 · 새 인자는 등록만으로 추가

공통 EW (Early Warning) — 외부 신호만

자산 위험도 계산에 들어갑니다 — 실효 악용 산식의 악용 계수 0.9(KEV 1.0 다음), 정책 VUL-013 "Early Warning CVE 보유"

현장 EW (Early Warning) — 우리 자산까지

Early Warning 화면의 표시 · 정렬 · 등재 — "이 CVE를 가진 고위험 자산이 있는가"를 더해 영향 자산을 지목합니다

계산 대상

LIVE 자산에 미해결(OPEN)로 남은 CVE만 — 조치할 대상이 있는 경보만 올립니다

다시 계산

기동 · 10분 주기 · Intelligence 적재 직후 · 설정 저장 · 화면의 "다시 계산"

등재 보호 규칙

외부 신호가 두 종류 이상일 때만 판정 · 고위험 자산에 있다는 사실만으로는 등재하지 않음

KEV 전환 추적 · 근거

KEV에 오르면 "선행 n일"을 기록 · 인자별 값 · 가중치 · 기여도를 신호 근거로 저장

Early Warning × 실효 악용 도달성 × 맥락분석 엔진 — 경보에서 조치까지

공통 EW는 실효 악용 산식의 악용 계수로 들어가고 [특허 출원 #2], 그 확률이 취약 렌즈 V를 거쳐 자산 위험도가 되며 [특허 출원 #1], 그 위험도가 현장 EW와 즉시 조치 CVE의 순서를 정합니다 — 경보가 목록으로 끝나지 않습니다

① 공통 Early Warning

Intelligence 신호 → KEV 등재 전 경보

- EPSS 추세 · 공개 익스플로잇 · 벤더 ·KISA 권고 · IOC 연관
- 가중 합 ≥ 0.60이면 등재 — 외부 신호만으로 계산
- Intelligence 적재 직후와 10분마다 다시 계산

② 실효 악용 도달성

[특허 출원 #2]

VulnProb = base × exploit × reach × av × conf

- **exploit** KEV 1.0 > **Early Warning 0.9** > 공개 Exploit 0.8 > 그 외 0.5
- **reach** DPI가 취약 서비스의 서버 응답을 관측 1.0 · 제품 일치만 0.6
- **AV** 공격 벡터 × 노출 — 외부 노출 1.0 · 내부 0.7

③ 맥락분석 엔진

[특허 출원 #1]

L = 1 − (1 − T) × (1 − V)

- 실효 악용 확률이 취약 렌즈 V의 증거로 — 상위 4개만 결합
- 위협 T · 노출 E · 영향 I 와 융합: 100 × L^0.7 × (0.5+0.5E) × (0.5+0.5I)
- 킬체인 진행 · 교차 확증으로 격상 → 자산 위험도 0~100

④ 결과 — 조치 목록

우리 자산의 순서 → 지금 할 일

- 현장 EW — 위험도 ≥ 80 자산이 보유하면 가중(25%)
- Early Warning 화면 · 취약점 목록 EW 태그 · 정책 VUL-013 Risk Indicator
- 즉시 조치 CVE · C-Level “CVE 악용 가능성” 지표

[예시] 같은 Early Warning CVE, 세 자산 — 조치 순서가 갈립니다

CVSS 9.8 · EPSS 0.42 · 공개 익스플로잇 · KEV 미등재 → base 0.70 × exploit 0.9(EW) × reach × av × conf 1.0

자산 (같은 CVE 보유)	도달 reach	벡터 × 노출 AV	실효 악용	판정
인터넷 노출 서버 — 취약 서비스 응답 관측	관측 1.0	외부 노출 1.0	63%	즉시 악용
내부 서버 — 취약 서비스 응답 관측	관측 1.0	내부 0.7	44%	도달 가능
내부 PC — 제품 일치만(서비스 미관측)	제품 일치 0.6	내부 0.7	26%	잠복

같은 서버 · 같은 CVE — 등재가 순서를 앞당깁니다

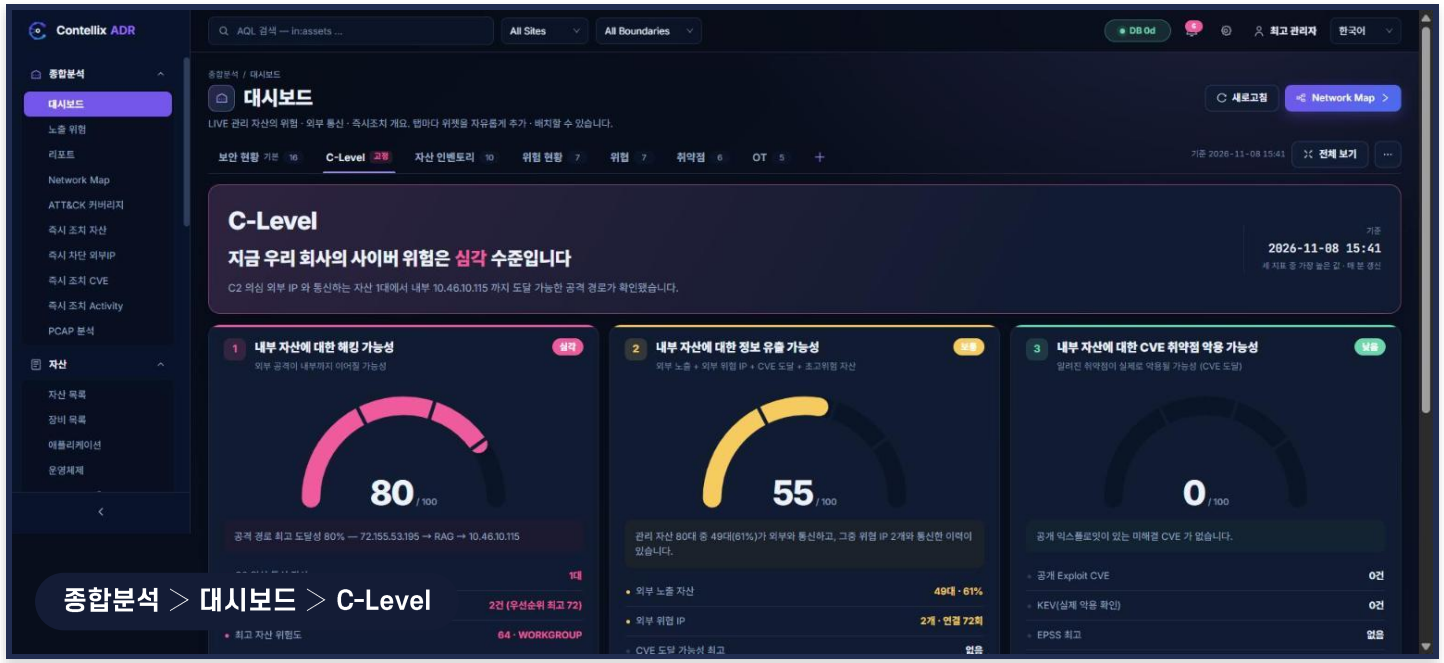


점선 = “즉시 악용” 기준 60% — KEV를 기다리지 않고 조기 경보(EW)

KEV 등재 전에 알고 · 닿는 것만 고르고 · 위험한 자산부터 — 세 단계 모두 고객망 안에서 계산됩니다

C-Level 대시보드 — “지금 우리 회사의 사이버 위험 수준”을 세 지표로

경영진용 고정 탭 : 종합 판단 한 줄 · 세 지표(해킹 · 정보 유출 · CVE 취약점 악용 가능성) · 근거 값 · 지금 조치가 필요한 초고위험 항목 → 즉시 조치 화면으로 연결



C-Level 표출 위험도 판정

- **해킹 가능성** 0.35×공격 경로 최고 도달성 + 0.25×(C2 의심 IP 통신 자산 있으면 100) + 0.20×미해결 Alert 최고 우선순위 + 0.20×최고 자산 위험도
- **정보 유출 가능성** 0.30×외부 노출 비율 + 0.30×위협 IP 점수(60 + 15×개수, 최대 100) + 0.25×EPSS 최고 + 0.15×최고 자산 위험도
- **CVE 악용 가능성** 0.40×EPSS 최고 + 0.30×(공개 익스플로잇 CVE 있으면 100) + 0.30×최고 실효 악용 확률 + (KEV 있으면 +10)
- **등급 · 종합** 자산 위험도와 같은 구간 · 종합 판단 = 세 지표 중 최고 등급 · 입력은 모두 LIVE 관측·분석 결과

예시 - PoV 라이브 결과

종합 “심각” — 해킹 80(심각) · 정보 유출 55(보통) · CVE 악용 0(낮음). 근거: C2 의심 IP 2개와 통신한 자산 1대, 공격 경로 최고 도달성 80%, 외부 노출 49대/61%

조치 항목(근거 있을 때만)

C2 의심 외부 IP 차단 → 즉시 차단 외부IP · 공격 경로 끊기 → 노출 위험 · Exploit 공개 CVE 패치 → 즉시 조치 CVE · 처리 안 된 Alert → Alerts

고정 구성 · 전체 보기

위젯 갤러리·편집 대상이 아닌 고정 탭, 첫 탭 뒤에 늘 위치 · 회의·보고용 전체 보기 · 문장은 콘솔이 한국어/영어로 생성

위젯 대시보드

기본 탭 6개(보안 현황·자산 인벤토리·위협 현황·위험·취약점·OT) + 사용자 탭 · 24열 격자 끌어 옮기기 · 위젯 32종 + AQL 위젯 · 탭 잠금

즉시 조치 4종 — 맥락분석이 끝나면 네 가지 결과를 확정해 제시합니다

위험도 임계값, 즉시 조치 임계값(기본 85)을 넘은 관리 자산을 기준으로 “어느 자산을 · 어떤 외부 IP를 끊고 · 어떤 CVE를 패치하고 · 무슨 일이 있었는지”를 한 세트로 — 종합분석 메뉴 4개 화면

증거 입력

Activity · IP 연결 · 자산 프로파일 · CVE/KEV/EPSS/EW · IOC · 정책 Risk Indicator

맥락분석 엔진

증거 모델 → 맥락 그래프 → T·V·E·I 렌즈 → noisy-OR · 교차 확증 · 킬체인 · 전염

자산 위험도 0~100

RISK = 100 × L^0.7 × (0.5+0.5E) × (0.5+0.5I) × mult · 보정 규칙(C2 확증 → 최소 High) · 증적(risk_summary) 저장

즉시 조치 임계값

risk_score ≥ immediate_action_risk_threshold (ST-42 운영 설정, 기본 85 · API ?threshold= 우선) · managed=1 · LIVE(세션 0)

AN-13 즉시 조치 자산

임계값 이상 관리 자산 전부(위험도 내림차순)

- 자산 · IP · MAC · 분류·유형 · 제조사 · OS · Site · 바운더리 · 업무 중요도 · 최근 관측
- 자산마다 미해결 Alert · 미해결 CVE · 활성 Risk Indicator 수 (MariaDB) + Security Activity 수 · 악성 통신 외부 IP 수 (ClickHouse 집계)
- 증적 = 맥락분석 서술 + 킬체인 단계 · 교차 확증 수 · 근거 코드 (role+beaconing+weak_tls)

AN-10 즉시 차단 외부IP

그 자산들의 악성·의심 통신 상대 IP

- Security Activity 중 Known Malicious Host · Suspicious Host의 peer IP — 최신순, 중복 제거, ::/빈 값 제외
- 행마다 사유(activity_type) · 활동 제목 · 관련 자산 · 자산 위험도·등급 · 증적
- action = FORTIGATE_BLOCK — 방화벽 즉시 차단 후보 목록(플러그인 자동 차단은 Phase 4)

AN-11 즉시 조치 CVE

그 자산들의 미해결(OPEN) 취약점

- asset_vulnerability JOIN asset — CVE · 유형(OS/APPLICATION) · Confidence · 도달(OBSERVED / PRODUCT_MATCH) · 상태
- 자산 위험도 내림차순 → CVE 순. 실효 악용(VulnProb) 정렬의 취약점 목록과 같은 데이터
- 증적은 자산의 맥락분석 서술 — “어떤 자산의 CVE라서 지금인가”

AN-12 즉시 조치 Activity

그 자산들의 보안 Activity 이력(최신 500)

- type_group=Security 전부 — 시각 · 유형 · 심각도 · 제목 · 상대 IP · 자산 · 자산 위험도
- 비코닝 · IOC 일치 · 포트 스캔 · Brute Force · OT Control Command 등이 시간순으로
- “무슨 일이 있었나”를 자산 위험도와 함께 — 사고 대응 타임라인

국내 환경 최적화 — 망분리 · 데이터 주권 · 한글 · OT 안전 · KST

금융·공공·제조의 폐쇄망에서 인터넷 없이 전 기능이 동작하도록 설계했고, 수집하는 데이터와 수집하지 않는 데이터를 분명히 했습니다

완전 독립 운영

- 분석 엔진까지 고객 내부 설치, 인터넷 연결 없이 수집·분석·탐지·대응·Early Warning 전 과정
- 외부 정보는 서명된 오프라인 패키지로만 반입, 반입 확인서(SHA-256) 동봉, 적재 후 소급 재분류
- IOC 유효기간(aging)으로 반입 간격 중 오탐 억제

데이터 주권 · 메타데이터만

- 자산·트래픽 데이터가 고객망 밖으로 나가지 않음 — 콘솔·버스·센서 전 구간 TLS, 비밀정보 AES-256-GCM
- 페이로드·파일·메일 본문·OT 공정값 미수집, 자격증명 값 마스킹
- 로그인 게이트 · API 키 · 감사 로그(해시 체인) · 역할 기반 권한 · Site 범위

한글 · 국내 지식 · KST

- 한글 UI(영문 전환) · 한글 리포트 템플릿 14종(N2SF 준수 · PoV 종합진단 양식 포함) · 한국어 위험 서술·권장 조치(LLM 미사용)
- KISA/KrCERT 긴급 공지 · C-TAS 위협정보 반영 · 국내 장비 배너 규칙 보강
- 표시 시각은 한국 표준시(KST) 기본 — 저장은 UTC, API·CSV·알림 모두 일관(ADR-0023)

망분리 환경 · N2SF 정책

- N2SF 자산식별·지속 검증, 업무망↔인터넷망 직접 통신 정황 탐지 정책 기본 제공
- Corporate→Guest 교차, Boundary 간 비인가 통신 세분화 정책 · 경계 매트릭스
- 국내 환경 및 인증 요건을 고려한 제품 및 로드맵(국내 인증 준비는 Phase 4)

OT 안전

- OT 구간 Passive 전용 기본값, 능동 질의는 ST-11 데이터 소스를 켠 대역에서만 · 실행 창·블랙아웃
- 쓰기·제어 명령 절대 미사용, 읽기 전용 함수 코드 화이트리스트를 코드로 강제
- Siemens · Rockwell · Schneider · LS · Mitsubishi Zero-Impact 검증

라이선스 · TCO

- 고객사 TCO에 맞춘 에디션 구성 · 자산(Assets) 수 기준 라이선스, 장비(Devices)는 비과금
- 영구 라이선스 기반 + 유지보수(인텔리전스 업데이트 · 정기 점검 방문 포함) · 오프라인 서명 키 활성화
- 오픈소스 플랫폼(Ubuntu · MariaDB · ClickHouse) — 별도 상용 DB 라이선스 없음 · 구독형 도입 가능, 5년 일괄 시 영구

도입 로드맵 — 1주 PoV로 시작하십시오. 결과 보고서가 곧 기대효과입니다

무중단 · No Agent · 미러링만으로 귀사 네트워크의 실제 위험을 먼저 보여드립니다 — PoV에서 센서 1대·SPAN 1포트로 관리 자산 80 · 외부 호스트 1,204 · C2 의심 통신 2건을 라이브로 확인했습니다

1 환경 분석
1일

미러링 지점·센서 배치 설계, 배포 모델(올인원/표준) 선정, 네트워크 범위(내부망·도입 범위) 협의, 반입 절차 협의

2 PoV 수행
1주

무중단 Passive 수집(+선택 AAQ), Success Criteria 실측, PCAP 사전 분석 병행, 즉시 조치 임계값 튜닝

3 결과 보고
1일

자산·위험 종합분석 보고서(PoV 종합진단 양식), C-Level 세 지표, 즉시 조치 4종 결과, 공격 경로·차단 리스트·조치안

4 본 구축
규모별

전사 확대·정책 튜닝 ·Site/Boundary 설계, 알림 채널 ·SIEM/ITSM·Enforcement 연동, 백업 일정

5 운영 · 유지보수
지속

정기 점검 방문 + Intelligence 패키지 적용, 긴급 업데이트, 정책 업데이트, 업그레이드(DB·설정 유지)

PoV 산출물 — 산출 보안위협과 CVE 위협을 그대로 귀사 데이터로 제공

- 자산 실태 종합분석 보고서 — 전수 인벤토리(자산·장비·외부 호스트) · 미인지 자산 · Critical 자산 · “왜 이 점수인가” 근거 · 공격 경로
- 즉시 조치 4종 — 즉시 조치 자산 · 즉시 차단 외부IP 리스트(방화벽 적용용) · 즉시 조치 CVE(패치·완화 가이드) · 즉시 조치 Activity 타임라인
- C-Level 보고 — 해킹 · 정보 유출 · CVE 악용 가능성 세 지표와 근거, 본 구축 제안(아키텍처·센서 배치·투자 규모)

PoV 준비물 (고객)

- 코어 스위치 SPAN(또는 TAP) 포트 1~2개
- 센서용 서버 1대(올인원 12C/32GB급) 또는 CK 어플라이언스 대여
- 관리 IP 1개, 콘솔 접속용 브라우저, 내부망·도입 범위 대역 목록
- (선택) 스위치 SNMP 읽기 전용 계정

자산을 알면, 지킬 수 있습니다

경계보안을 넘어 자산 중심 보안으로 — Contellix ADR과 함께

취약점 목록이 아니라
공격 가능한 지점을 보여 줍니다

도달 가능성 기반 실효 취약 · 관측 연결 기반 공격 경로 — DPI On-Prem 제품만 가능한 증명

CVE가 없어도
위험은 보입니다

OS 계열별 취약성 통신과 설치 앱의 통신 이력을 트래픽에서 직접 읽어 평가

한 가지 신호로
호들갑 떨지 않습니다

독립 출처 교차 확증과 noisy-OR, 킬체인 진행으로 연쇄를 자산 단위로 포착

맥락분석이 끝나면
네 가지 결과로 확정합니다

즉시 조치 자산 · 즉시 차단 외부IP · 즉시 조치 CVE · 즉시 조치 Activity — 그리고 경영진에게는 C-Level 세 지표

씨케이시스템즈㈜

제품 문의 · PoV 신청 · 파트너(리셀러) 프로그램
tac@cksystems.co.kr · hschoi@cksystems.co.kr (컨설팅본부장)
T. 02-538-6001

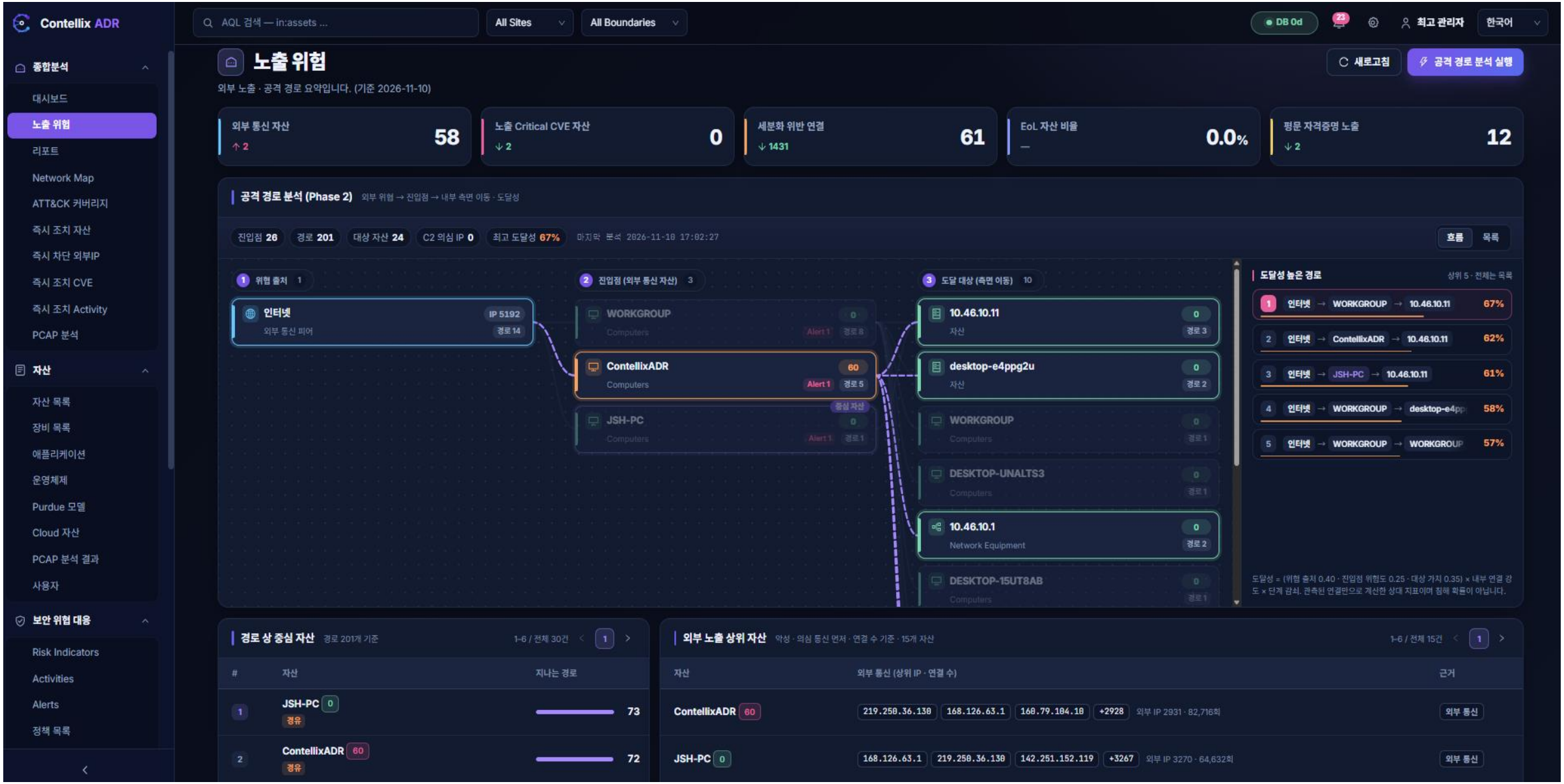
파트너사 안내

본 자료는 고객사 실무 검토용으로 그대로 사용하실 수 있습니다. PoV 체크리스트 · 보고서 양식(리포트 템플릿 "PoV 종합진단 결과 양식" 내장) · 데모 시나리오(같은 OS 다른 위험 / 지금 공격 가능한 CVE / 조용한 침해 연쇄 / 즉시 조치 4종 / 폐쇄망 동작)는 CK 파트너 포털에서 제공합니다.

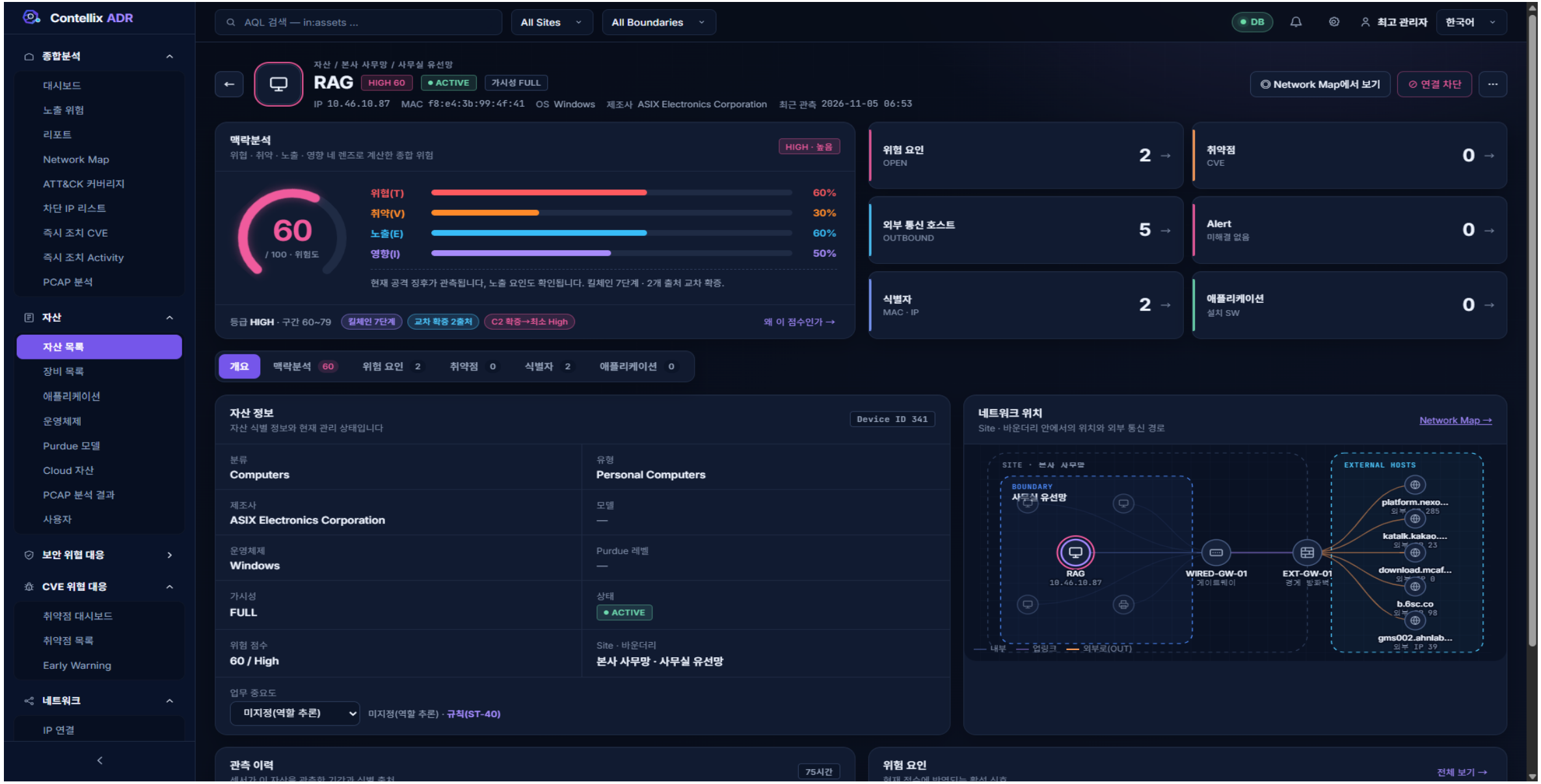
첨부 – 주요 분석 화면 : Contellix ADR – 대시보드



첨부 – 주요 분석 화면 : Contellix ADR - 노출위험



첨부 – 주요 분석 화면 : Contellix ADR – 자산위험도 맥락분석 결과



종합분석

대시보드

노출 위험

리포트

Network Map

ATT&CK 커버리지

즉시 조치 자산

즉시 차단 외부IP

즉시 조치 CVE

즉시 조치 Activity

PCAP 분석

자산

자산 목록

장비 목록

애플리케이션

운영체제

Purdue 모델

Cloud 자산

PCAP 분석 결과

사용자

보안 위협 대응

Risk Indicators

Activities

Alerts

대시보드

LIVE 관리 자산의 위험 · 외부 통신 · 즉시조치 개요. 자산 · Alert · 취약점 지표는 전체(상태형), 연결 지표는 최근 24시간입니다. 탭마다 위젯을 자유롭게 추가 · 배치할 수 있습니다.

새로고침 | Network Map

보안 현황 기본 16 | C-Level 고정 | 자산 인벤토리 10 | 위험 현황 7 | 위협 7 | 취약점 6 | OT 5 | +

기준 2026-11-11 17:11 | 전체 보기 | ...

C-Level

지금 우리 회사의 사이버 위험은 높음 수준입니다

공개 익스플로잇이 있는 CVE 4건이 자산에서 도달 가능합니다 — 최고 실효 악용 확률 18.4%.

기준
2026-11-11 17:12
세 지표 중 가장 높은 값 · 매 분 갱신

1 내부 자산에 대한 해킹 가능성

보통

외부 공격이 내부까지 이어질 가능성



공격 경로 최고 도달성 69% — 인터넷 → RAG → SN-SEOCHO-22

C2 의심 통신 자산	0대
처리 안 된 Alert	3건 (우선순위 최고 68)
최고 자산 위험도	50 · RAG

공격 경로 보기 →

2 내부 자산에 대한 정보 유출 가능성

낮음

외부 노출 + 외부 위협 IP + CVE 도달 + 초고위험 자산



관리 자산 101대 중 46대(46%)가 외부와 통신하고, 그중 위협 IP 0개와 통신한 이력이 있습니다.

외부 노출 자산	46대 · 46%
외부 위협 IP	없음
CVE 도달 가능성 최고	CVE-2026-123158 · EPSS 16.5%
초고위험 자산 (위험도 70+)	0대 · 50+ 1대

노출 위험 보기 →

3 내부 자산에 대한 CVE 취약점 악용 가능성

높음

알려진 취약점이 실제로 악용될 가능성 (CVE 도달)



공개 익스플로잇이 있는 CVE 4건이 자산에서 도달 가능 — 최고 실효 악용 확률 18.4%.

공개 Exploit CVE	4건
KEV(실제 악용 확인)	있음
EPSS 최고	CVE-2026-123158 · 16.5%
영향 자산	2대

취약점 대시보드 →