ANOMALI®

“위협 인텔리전스 플랫폼”

(주)한국밸런스

우리가 필요한 것은: 위협 컨텍스트!

현재 공격을 받고 있는가?

공격으로 피해를 입었는가?

공격을 탐지하고 대응할 수 있는가?

85% 강력한 보안 포스처에 위협 인텔리전스가 필수다!

45% 효율적인 위협 인텔리전스 프로그램 확보

데이터

수백만의 지표들
조단위의 이벤트
복잡한 연동

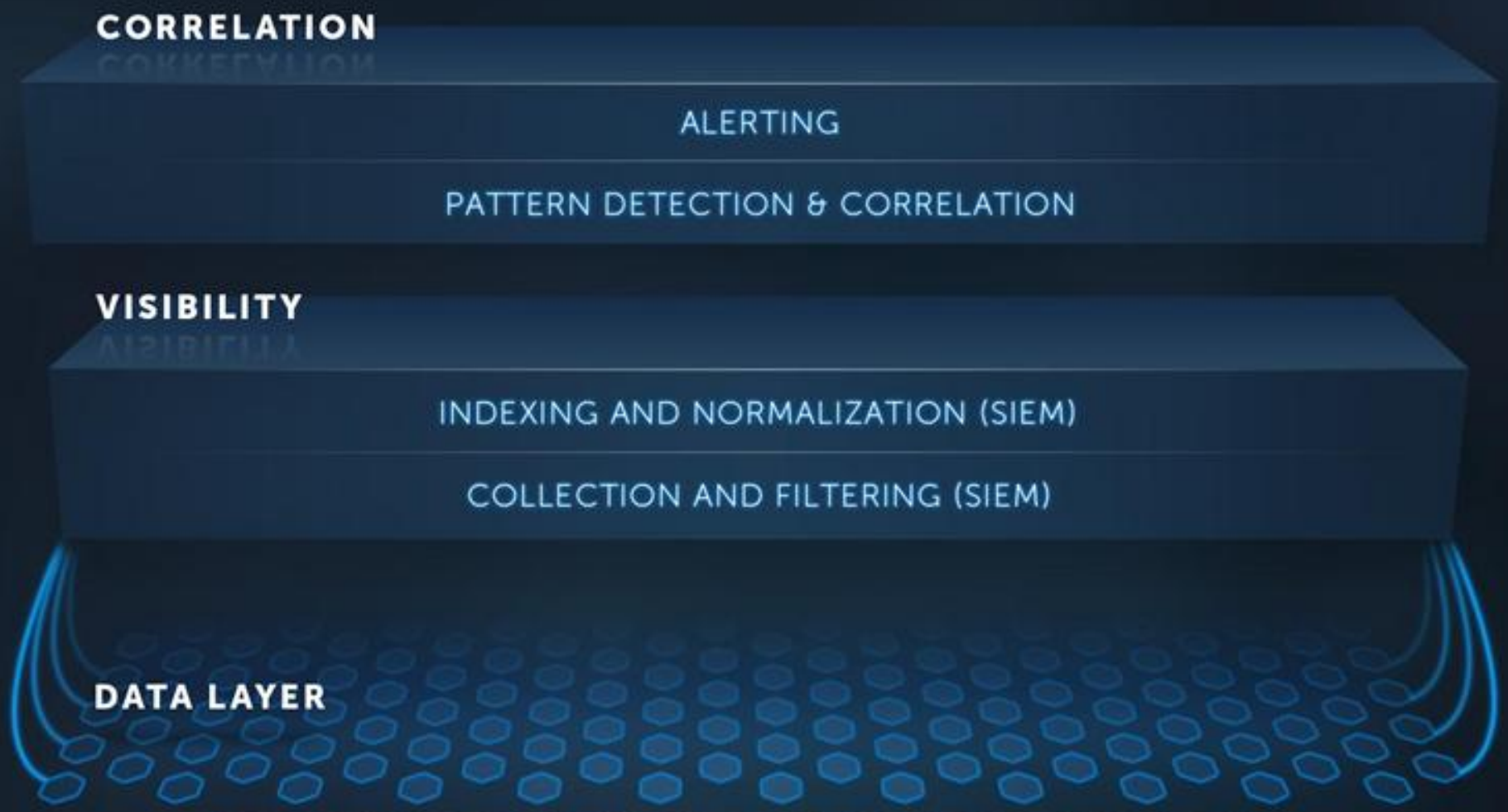
분석

위협 사냥
소급 포렌식
위협 조사

사람

제한된 인력
스킬 공백
지속성 문제

기존의 보안 관제: SOC (SIEM) 1.0



SOC 2.0: SECURITY TRANSFORMATION

INVESTIGATIONS AND RESPONSE
(침해 조사 및 대응)

CORRELATION AND ANALYTICS
(상관 분석)

VISIBILITY
(가시화 / 대시보드)

DATA LAYER
(보안 데이터 수집)

ANOMALI

위협 인텔리전스 플랫폼

100+ 복합 인텔리전스 소스

ThreatStream

최적화 및 강화 | 위협 조사 | 안전한 공유

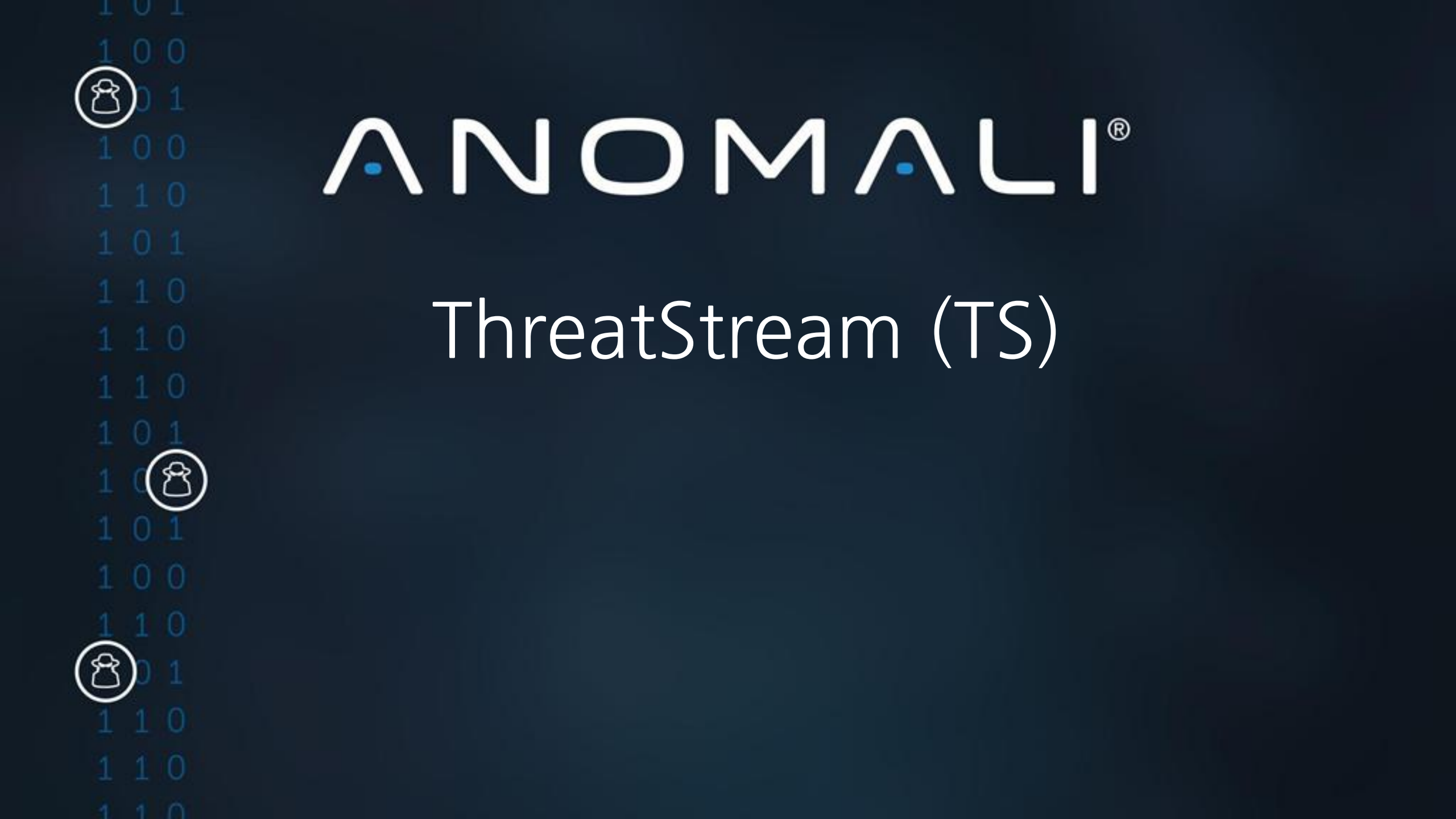
SIEM | 방화벽 | 침입탐지 | EDR | API/SDK

위협 탐지 엔진

SIEM | Network

Anomali Enterprise

SIEM | SOAR


ANOMALI®
ThreatStream (TS)

Anomali의 임무

아래 임무 수행을 위한 플랫폼 제공

1. 인텔리전스의 수집과 집계
2. 커뮤니티를 통한 인텔리전스의 공유
3. 연동을 통한 인텔리전스 활용

위협 인텔리전스 카테고리

컨텍스트 (위협 모델)

- 사람이 읽을 수 있는
- 액터 프로파일, 보고서, TTP
- 전략적
- CTI 팀 (무엇을 감시할 것인가?)

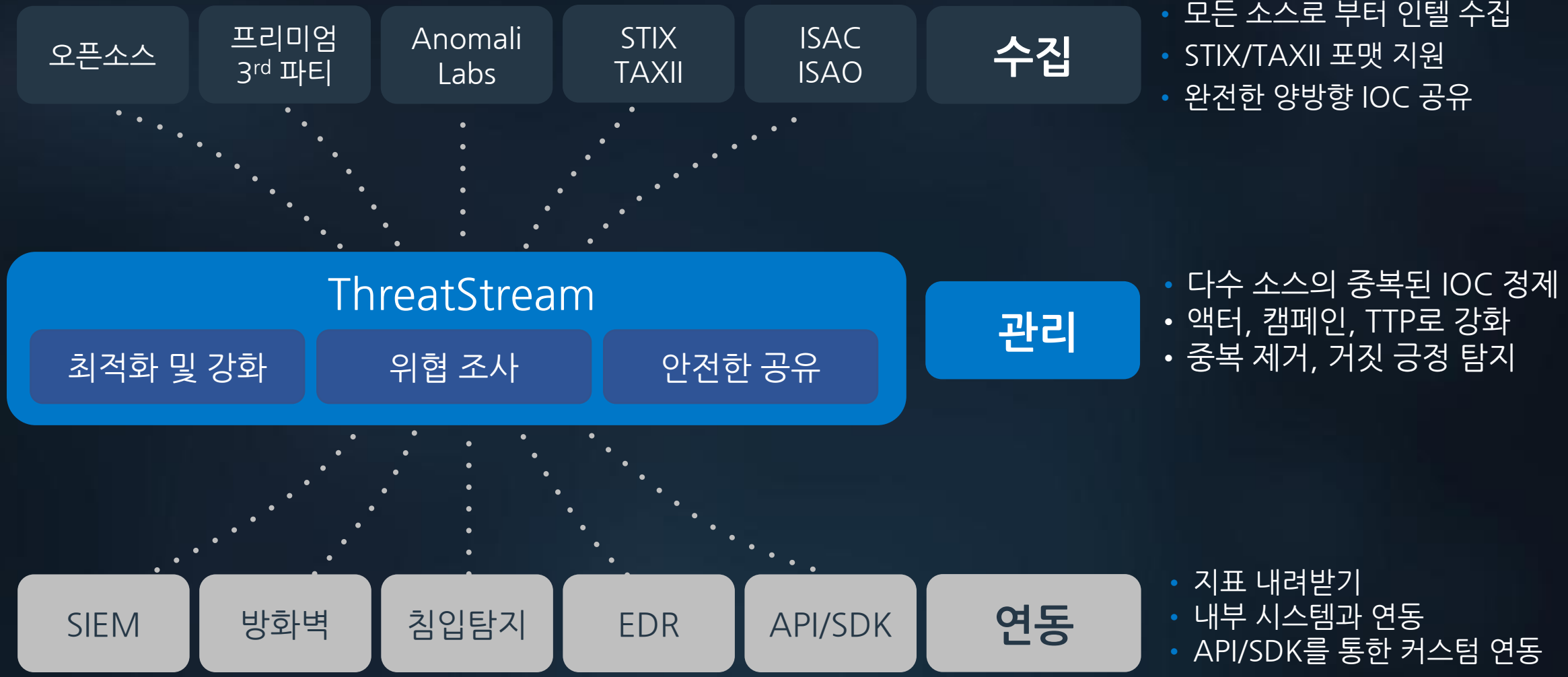
IOCs (식별 대상)

- 기계가 읽을 수 있는 것
- 위험 IP, 도메인, 파일 해시 등
- 전술적
- SOC 운영팀(왜 위협적인가?)

Linux Kernel 4.17.10
__del_reloc_root() Null Pointer Dereference Vulnerability

14.174.61.166
https://ftp.maggietalkspolicy.com/
d42efdc3152ad6ded7ac8a22c9760c2
1657fab43

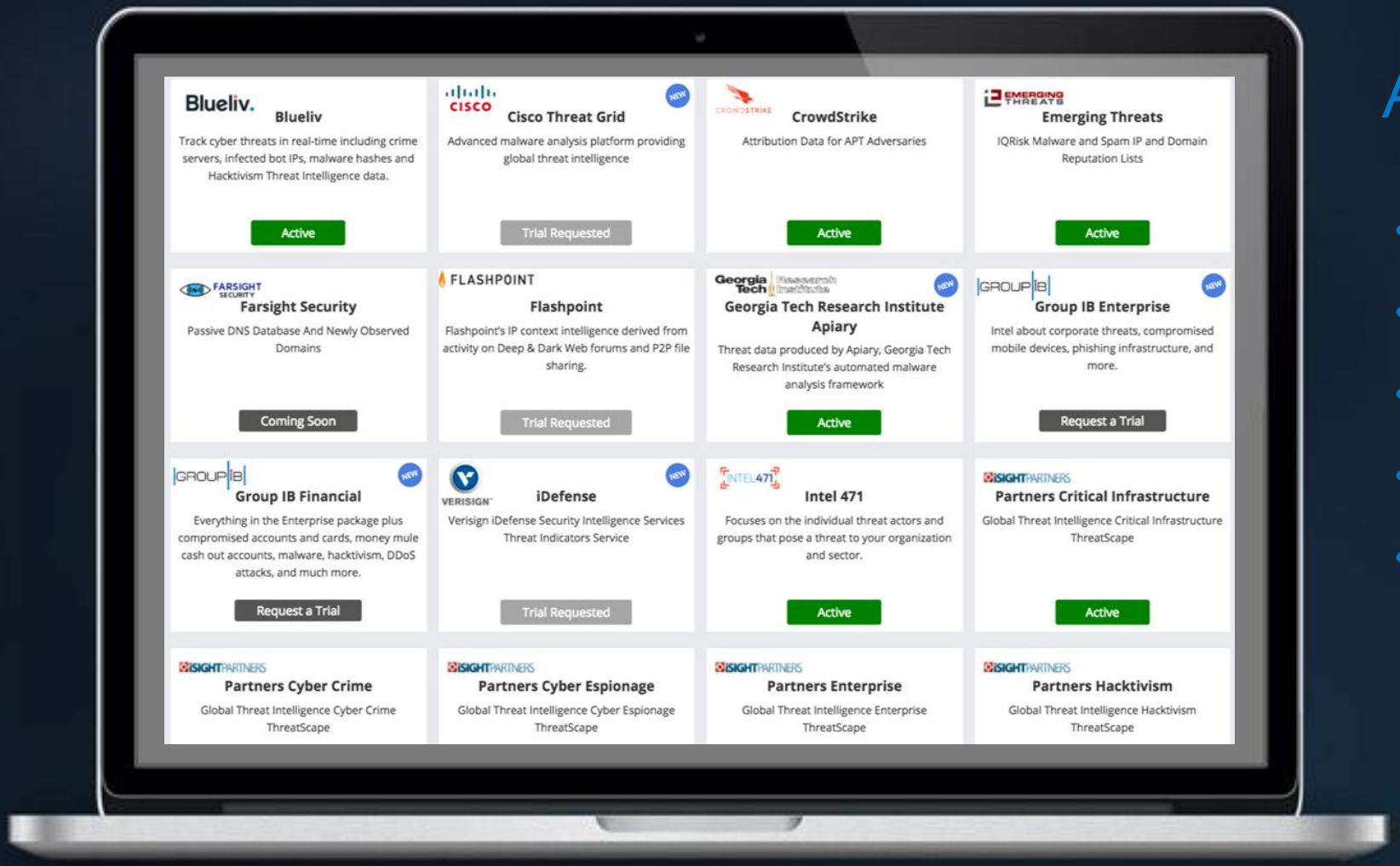
위협 인텔리전스와 플랫폼



- 모든 소스로 부터 인텔 수집
- STIX/TAXII 포맷 지원
- 완전한 양방향 IOC 공유

- 다수 소스의 중복된 IOC 정제
- 액터, 캠페인, TTP로 강화
- 중복 제거, 거짓 긍정 탐지

- 지표 내려받기
- 내부 시스템과 연동
- API/SDK를 통한 커스텀 연동



APP Store

- 인텔리전스를 위한 마켓플레이스
- 상용 인텔리전스 탐색, 구입
- ThreatStream과 통합
- 25개 이상 프리미엄 피드
- 100개 이상 무료 피드

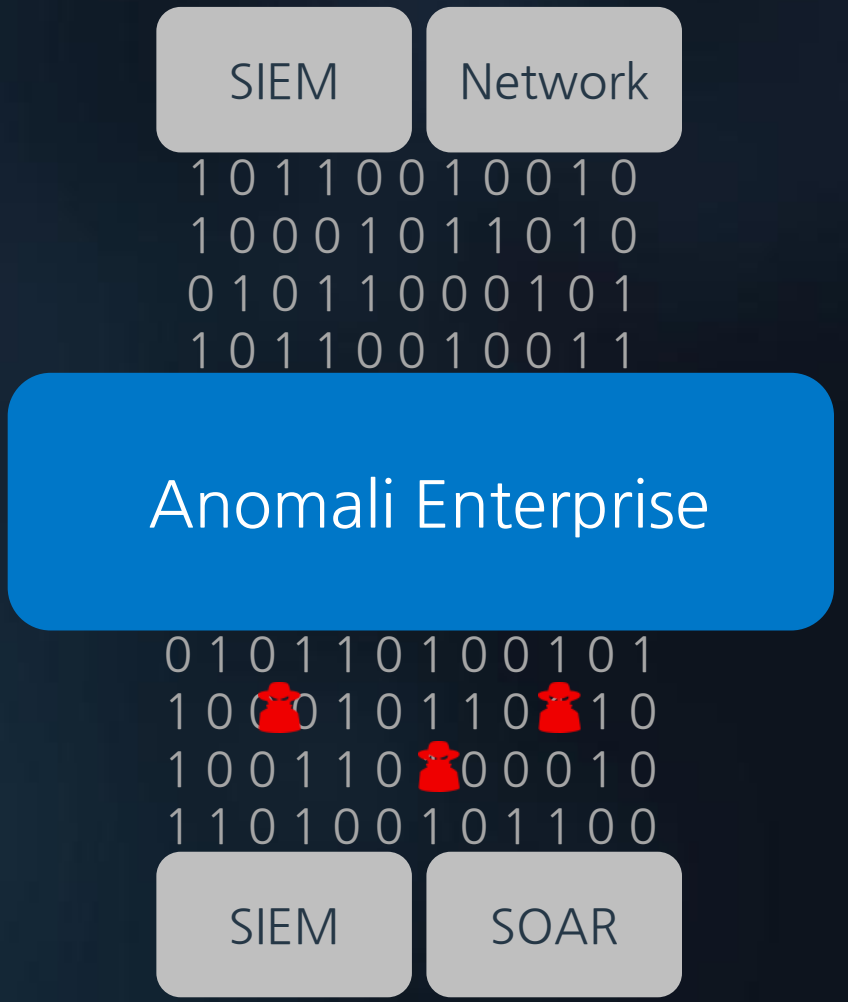
통합

- 즉시 사용할 수 있는 검증된 연동
- 내부 시스템과 통합
- 차단 및 모니터링 룰 생성
- SIEM, 방화벽, 엔드포인트 등 지원
- API/SDK를 이용한 커스텀 통합


ANOMALI®
Anomali Enterprise (AE)

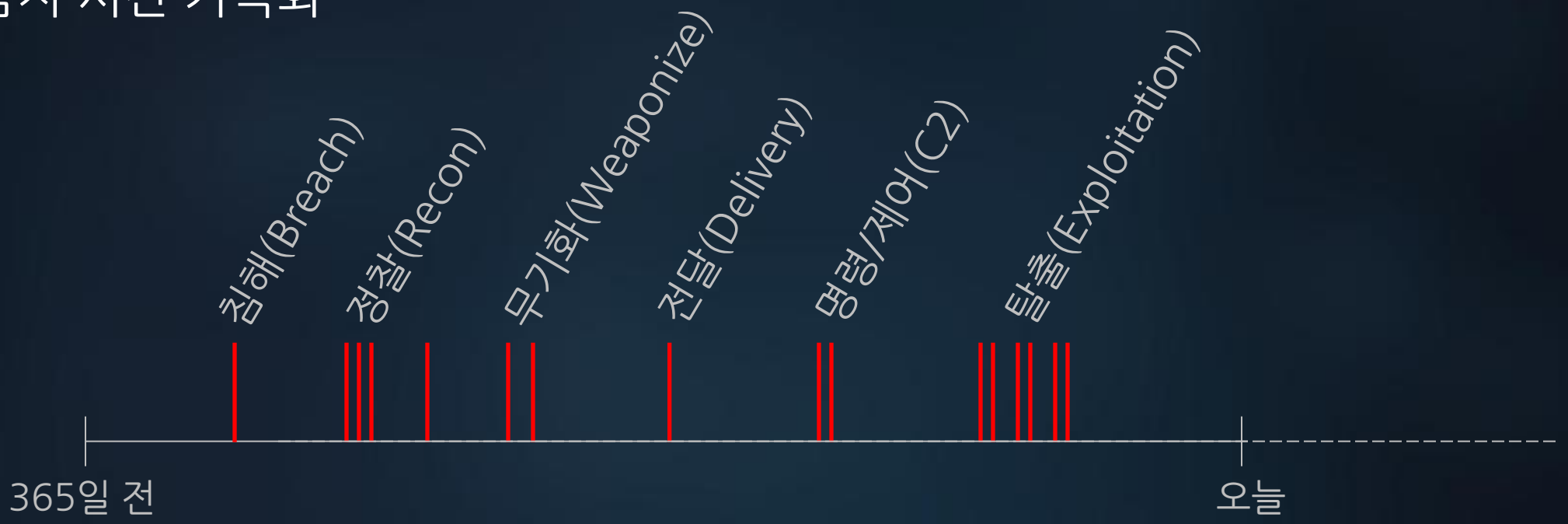
Anomali Enterprise

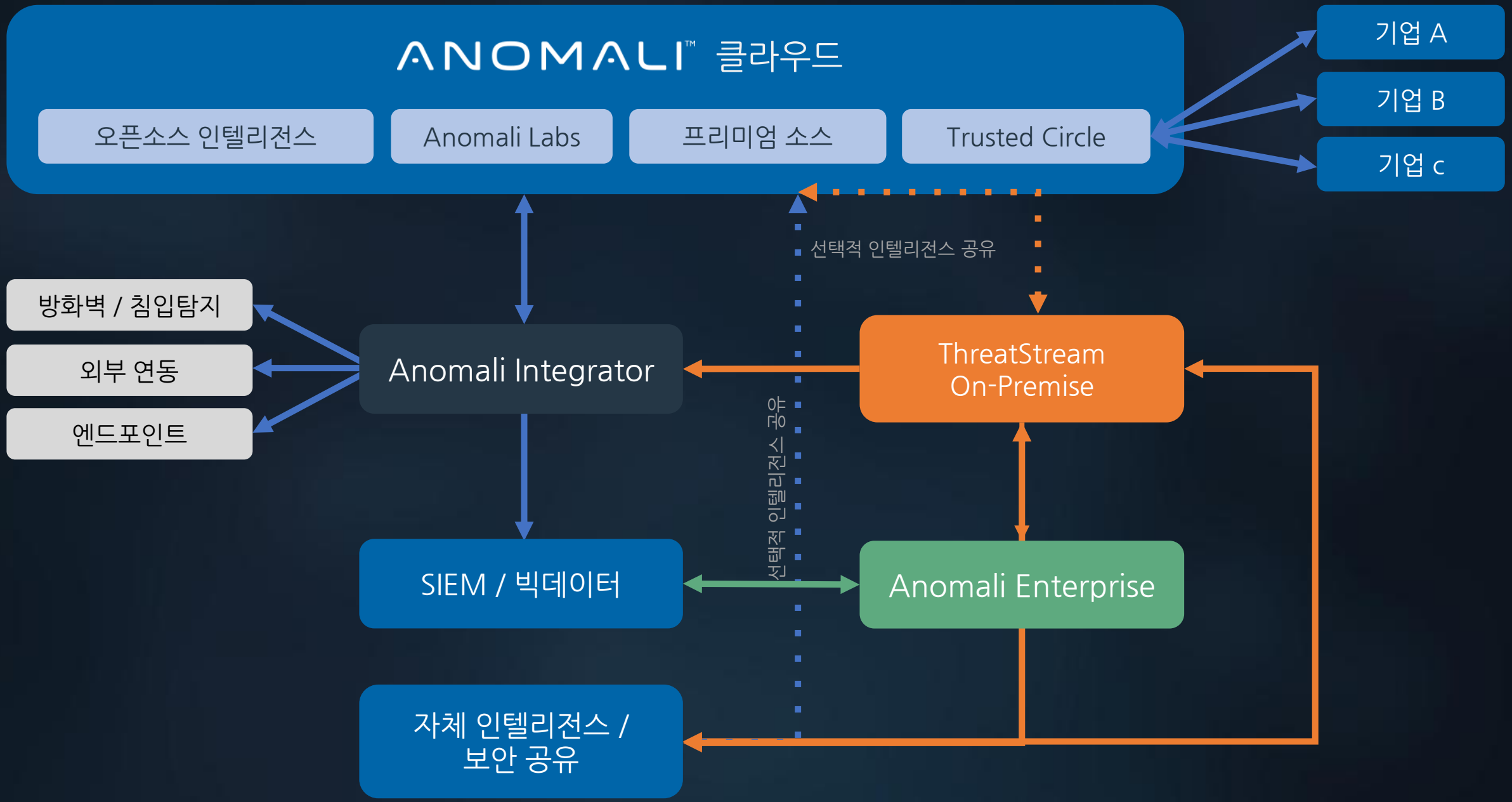
- 네트워크의 활성 위협 탐지
- 365일 이력 데이터 검색
- 별도의 로그 데이터 저장소 불필요
- DGA 도메인 탐지
- 중요 IOC에 대해 필터링/우선 순위 분류/추정 불필요
- 탐지 결과를 SIEM 또는 대시보드에 전송
- 내장된 위협 조사 도구 및 워크플로우



소급 분석(Retrospective Analysis)

- 이전 12개월의 이벤트 데이터를 대상으로 수백만의 IOC 대입 검색
- 모든 매치를 타임라인으로 시각화 및 검토
- 탐지된 공격과 관련한 모든 IOC를 상관하여 심도 있게 해부
- 탐지 시간 가속화





ANOMALI®

- **Comprehensive:** 위협 인텔리전스 + 위협 탐지 + 위협 조사
- Proven: 포춘 100대 기업 35%가 도입, 상위 은행 5곳 중 4곳 도입
- **Trusted:** 대부분의 ISAC과 위협 인텔 공동체와 협력
- **Research:** Anomali Labs, 위협 보고서, 주간 위협 브리핑 제공
- Global: 6개 대륙 운영, 글로벌 서포트

감사합니다.

Contact :
㈜한국밸런스
김 형덕 영업대표
Mobile : 010-7138-8889
Email : hdkim@valence.co.kr