DOOSAN

2019 Annual Security Users' Festival
23rd 해킹방지워크샵

사이버보안 빅데이터 활용 사례

위협 인텔리전스/자동화를 통한 선제적 방어

2019.12.05(목)

㈜두산 디지털이노베이션BU 정보보안 Chapter

김민교 대리

목차

사고는 왜 계속되는가?

신/변종
악성코드 생성수
<최대 50만개 생성/일>

백신 업데이트 수
<약 200개 업데이트/일>

패턴 기반 보안장비의 한계

1. 시작하며

선제적인 방어

2. 위협 인텔리전스 개념

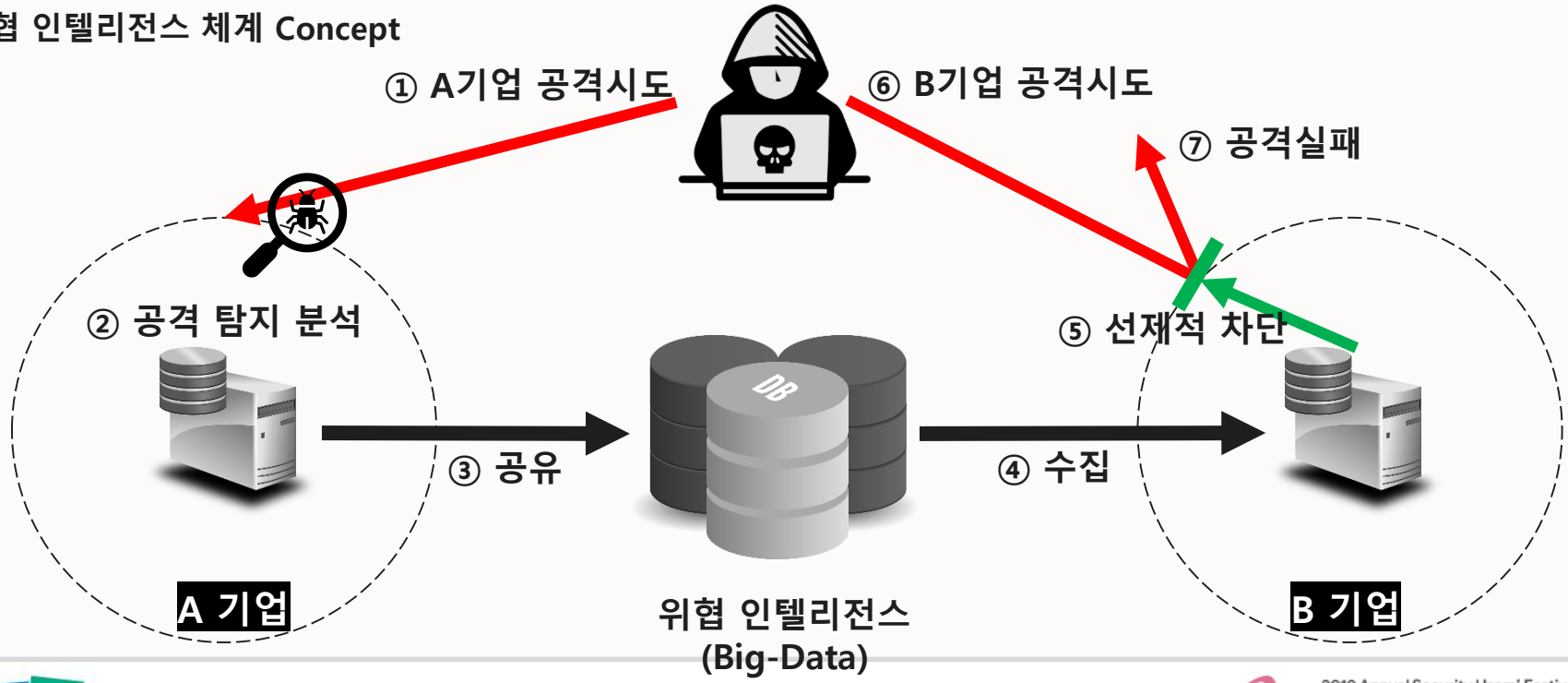
보안 시장이 Defensive security → Offensive Security로의 추세 전환에 따라 나온 개념

위협 인텔리전스(TI, Threat Intelligence)

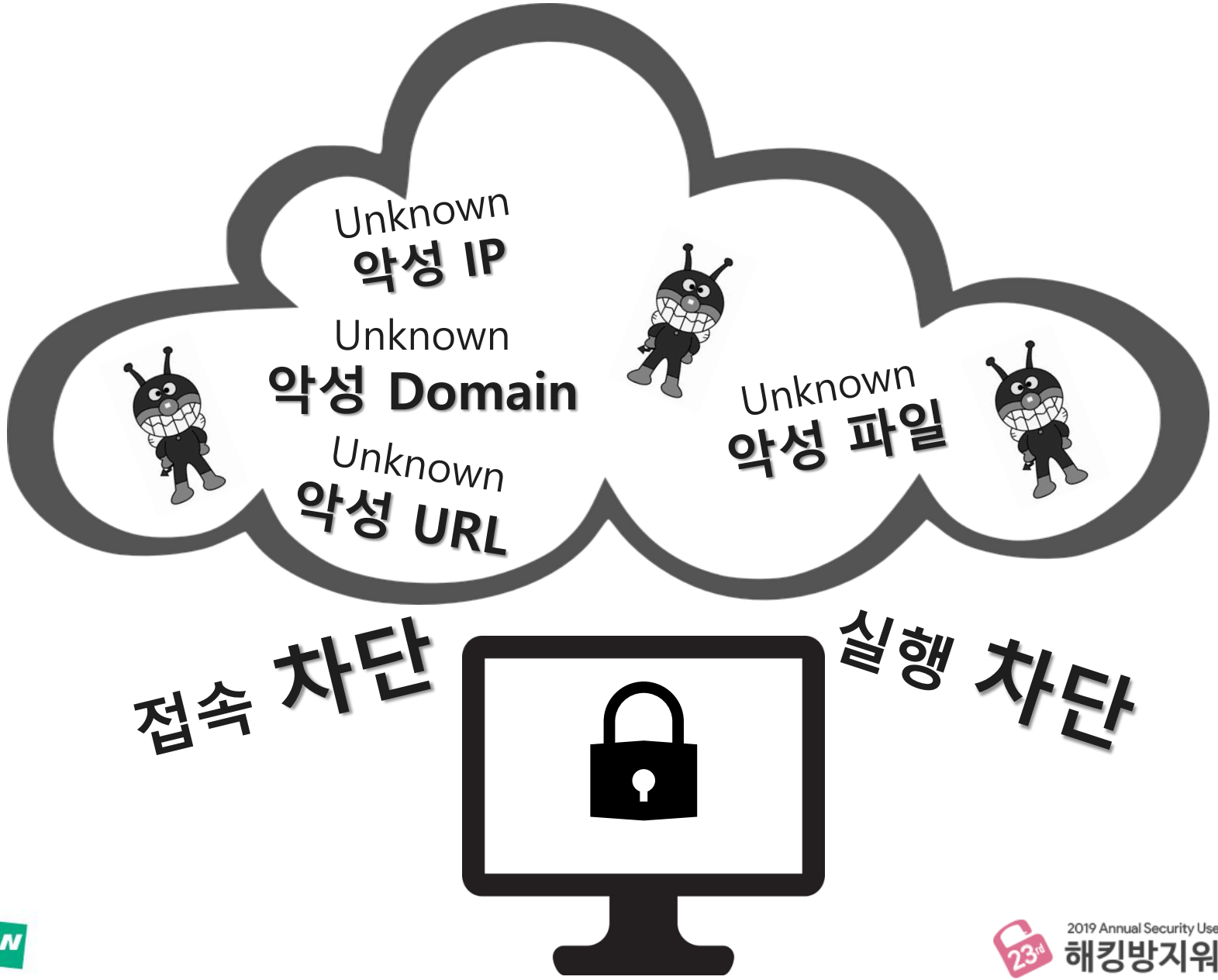
'증거를 기반하는 지식으로, 기업의 IT나 정보자산에 위협이 될 수 있는 부분에 실행가능한 조언을 컨텍스트나 메커니즘, 지표 등으로 제시하는 정보' – Gartner

'사이버 위협 정보(악성코드 정보, 명령제어 서버 정보, 취약점 및 침해사고 분석 정보 등)을 체계적으로 수집하고, 종합적으로 연관 분석하여 관계기관 간 자동화한 정보공유를 목적으로 하는 예방 대응 시스템' - KISA

위협 인텔리전스 체계 Concept

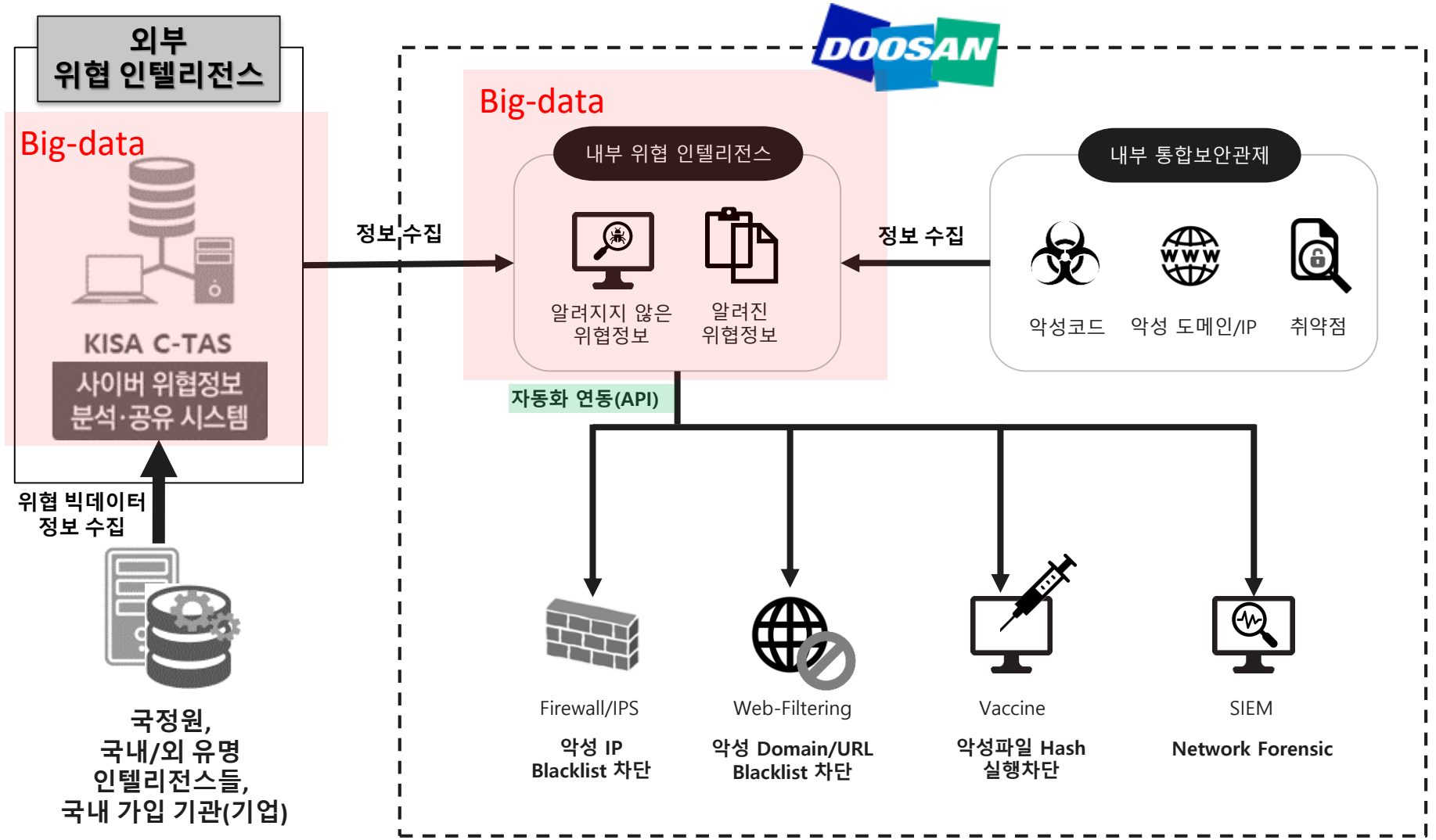


3. Idea of 선제 방어 전략



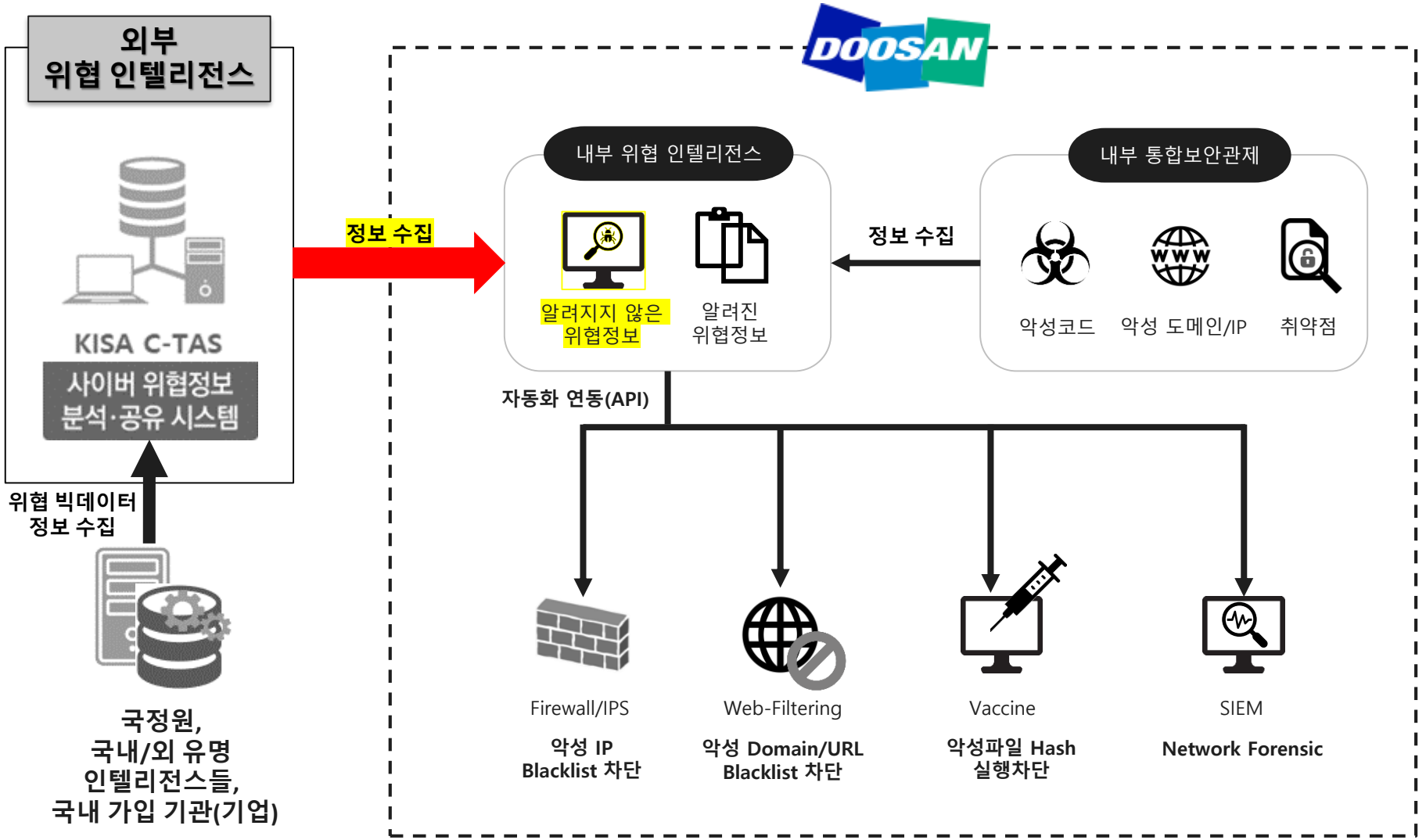
4. 빅데이터 기반 위협 인텔리전스 적용 사례

국내/외 타 기관 및 기업의 위협 정보 활용으로 침해에 대한 사전 방어 혹은 빠른 인지



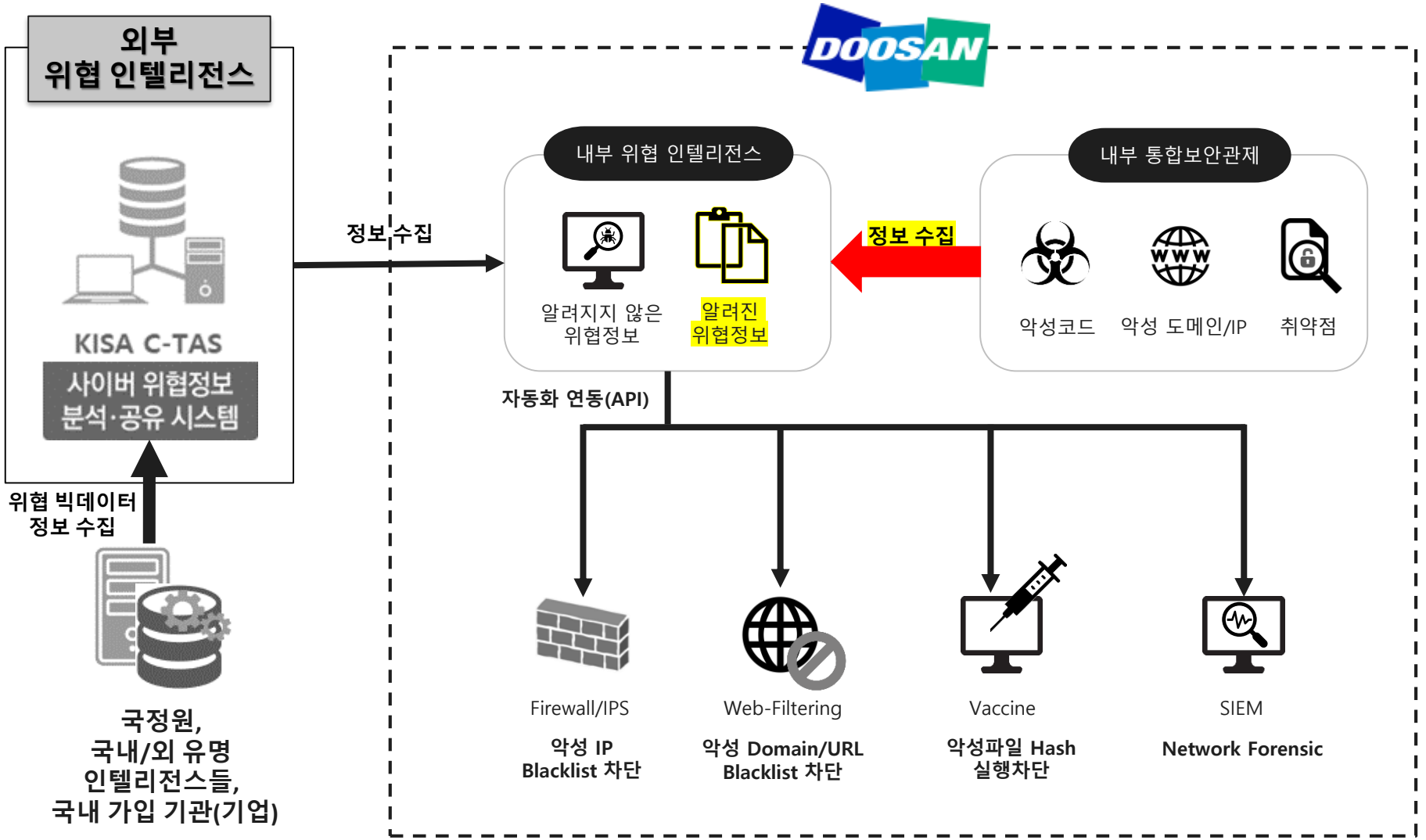
4. 빅데이터 기반 위협 인텔리전스 적용 사례

국내/외 타 기관 및 기업의 위협 정보 활용으로 침해에 대한 사전 방어 혹은 빠른 인지



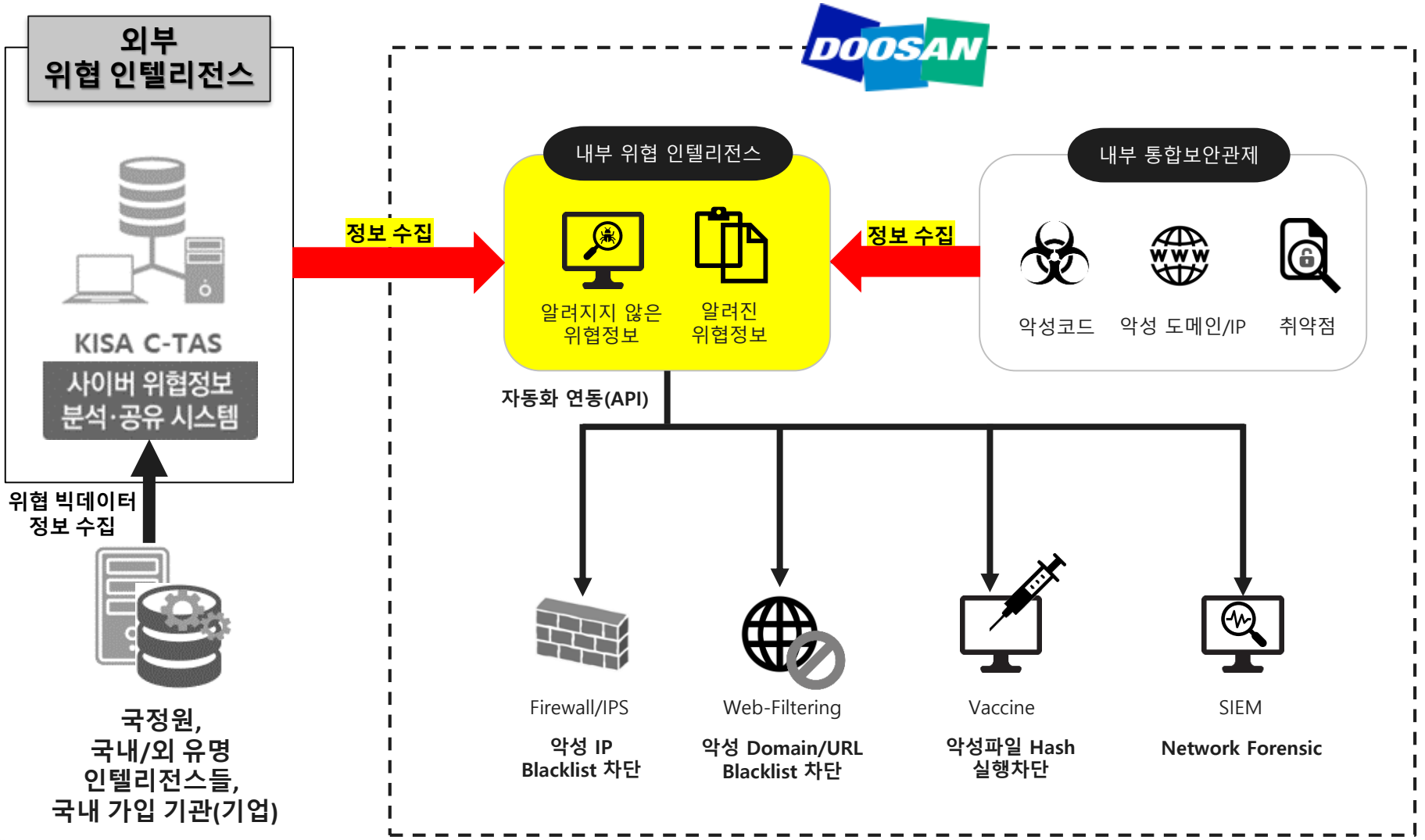
4. 빅데이터 기반 위협 인텔리전스 적용 사례

국내/외 타 기관 및 기업의 위협 정보 활용으로 침해에 대한 사전 방어 혹은 빠른 인지



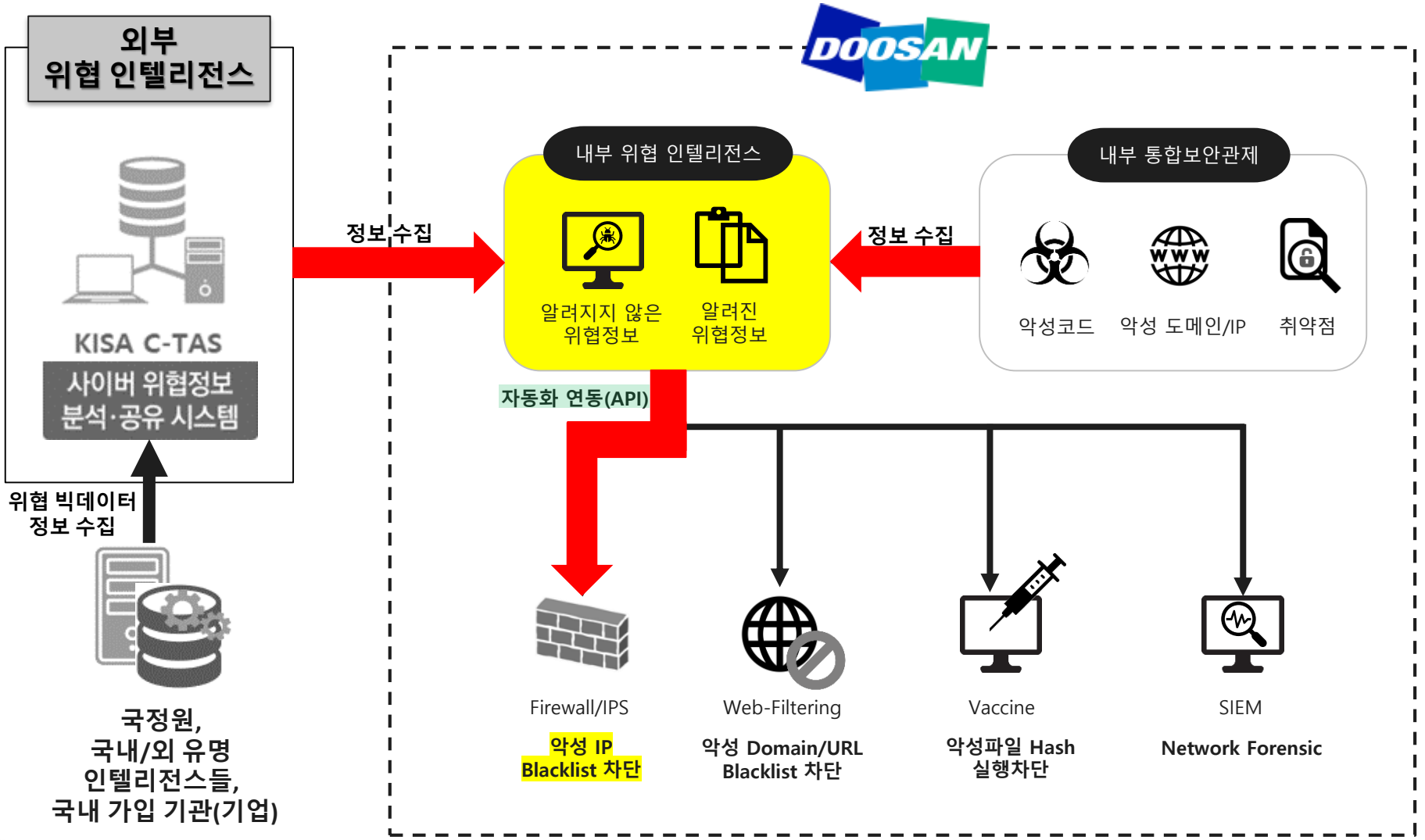
4. 빅데이터 기반 위협 인텔리전스 적용 사례

국내/외 타 기관 및 기업의 위협 정보 활용으로 침해에 대한 사전 방어 혹은 빠른 인지



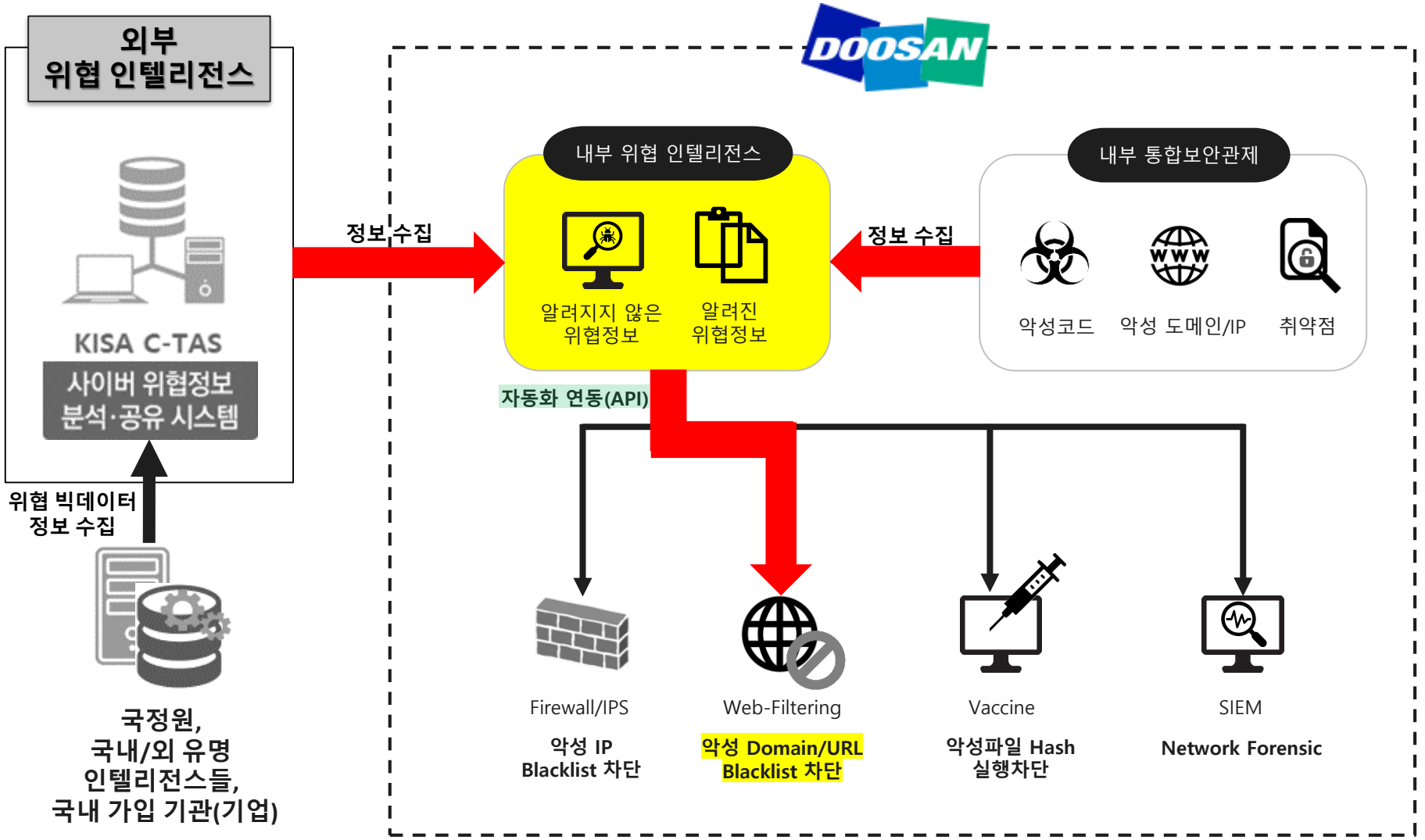
4. 빅데이터 기반 위협 인텔리전스 적용 사례

국내/외 타 기관 및 기업의 위협 정보 활용으로 침해에 대한 사전 방어 혹은 빠른 인지



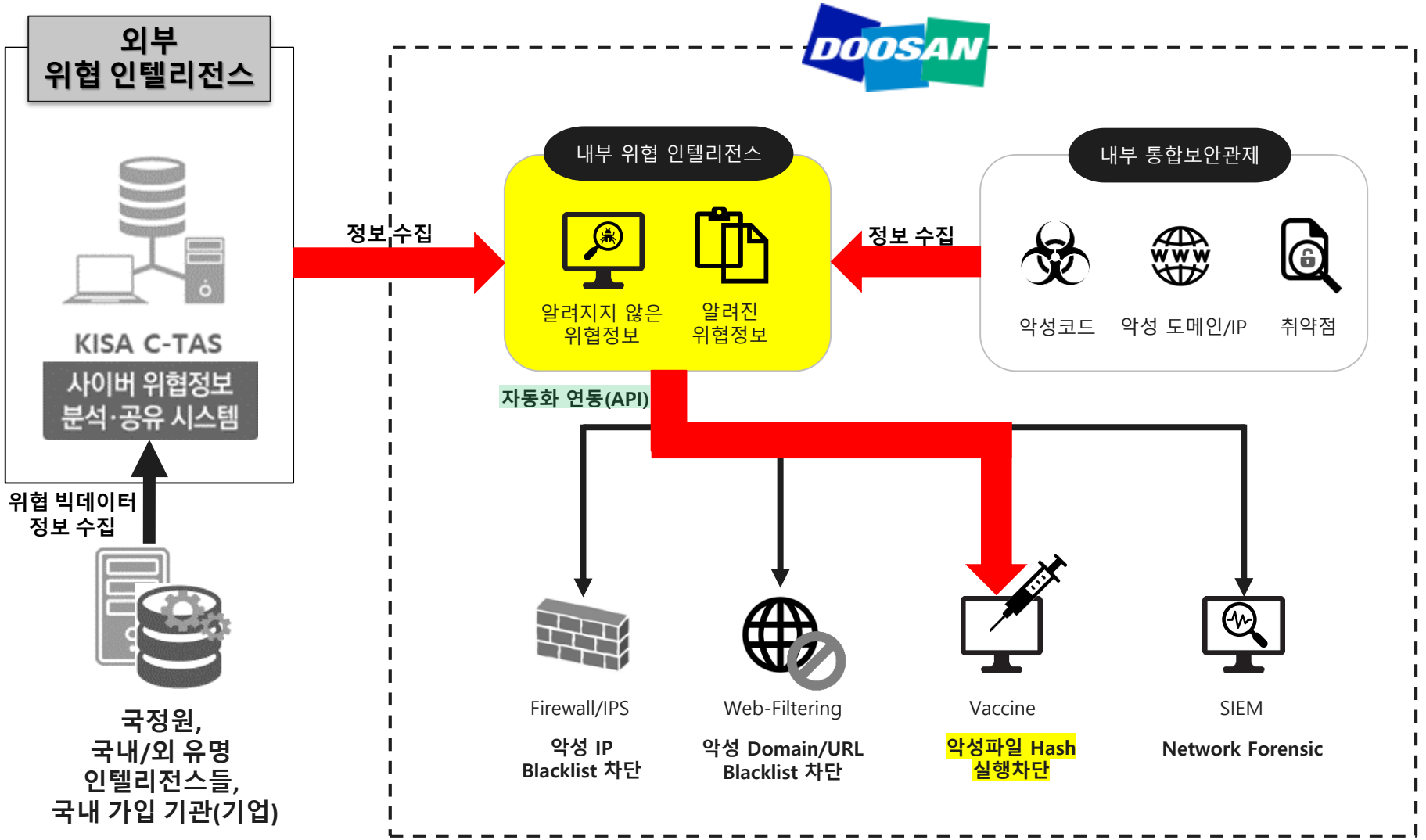
4. 빅데이터 기반 위협 인텔리전스 적용 사례

국내/외 타 기관 및 기업의 위협 정보 활용으로 침해에 대한 사전 방어 혹은 빠른 인지



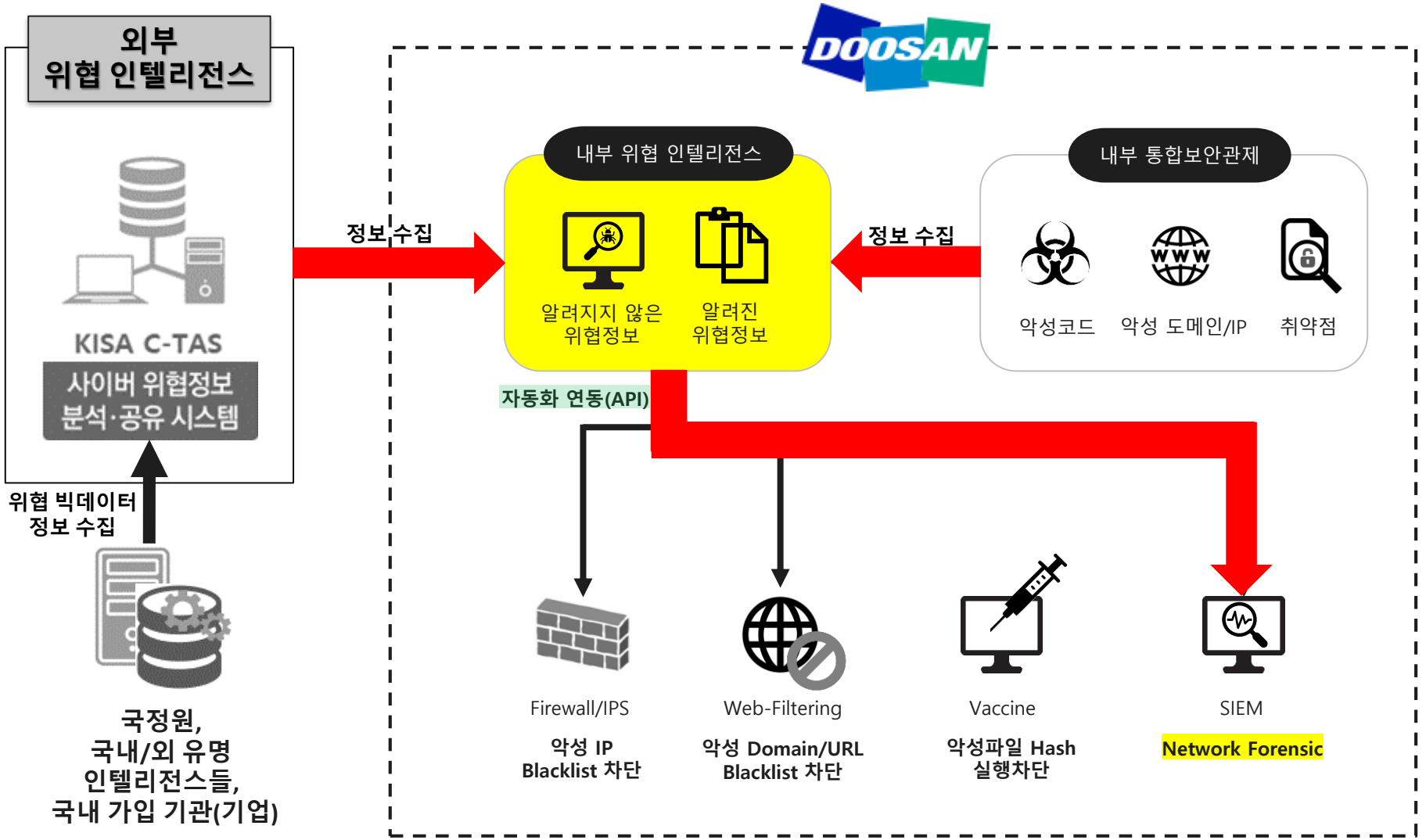
4. 빅데이터 기반 위협 인텔리전스 적용 사례

국내/외 타 기관 및 기업의 위협 정보 활용으로 침해에 대한 사전 방어 혹은 빠른 인지



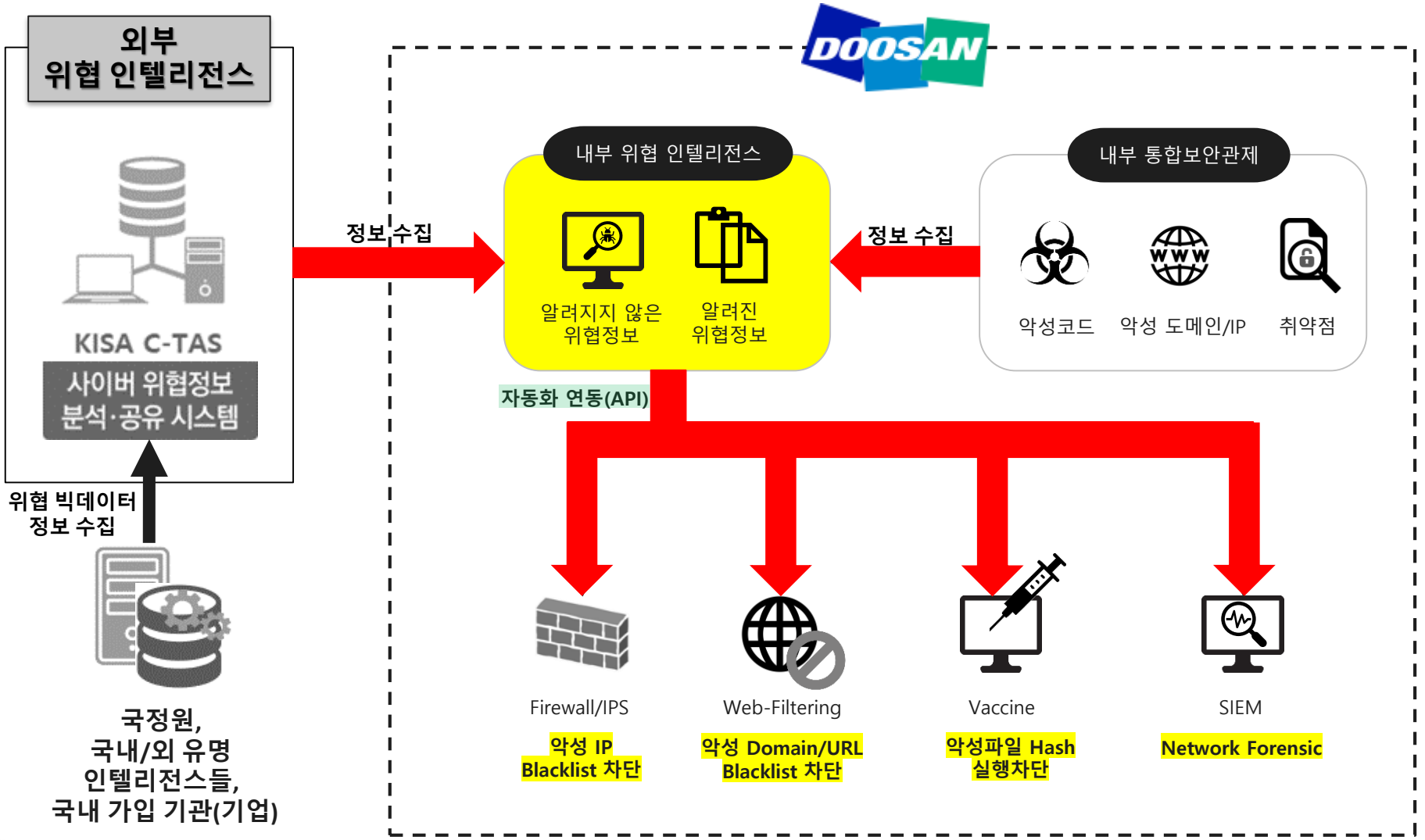
4. 빅데이터 기반 위협 인텔리전스 적용 사례

국내/외 타 기관 및 기업의 위협 정보 활용으로 침해에 대한 사전 방어 혹은 빠른 인지



4. 빅데이터 기반 위협 인텔리전스 적용 사례

국내/외 타 기관 및 기업의 위협 정보 활용으로 침해에 대한 사전 방어 혹은 빠른 인지

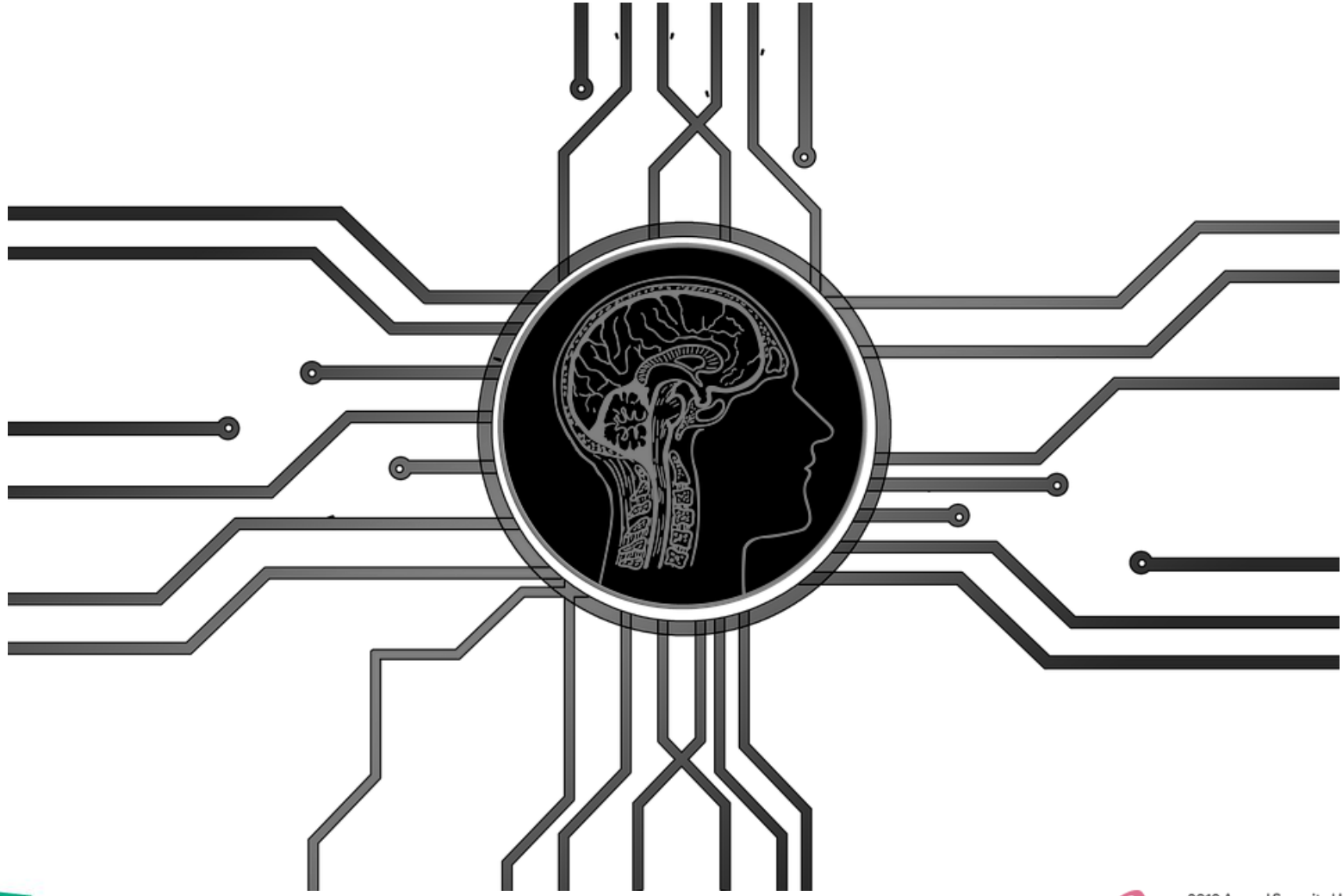


5. 적용 성과

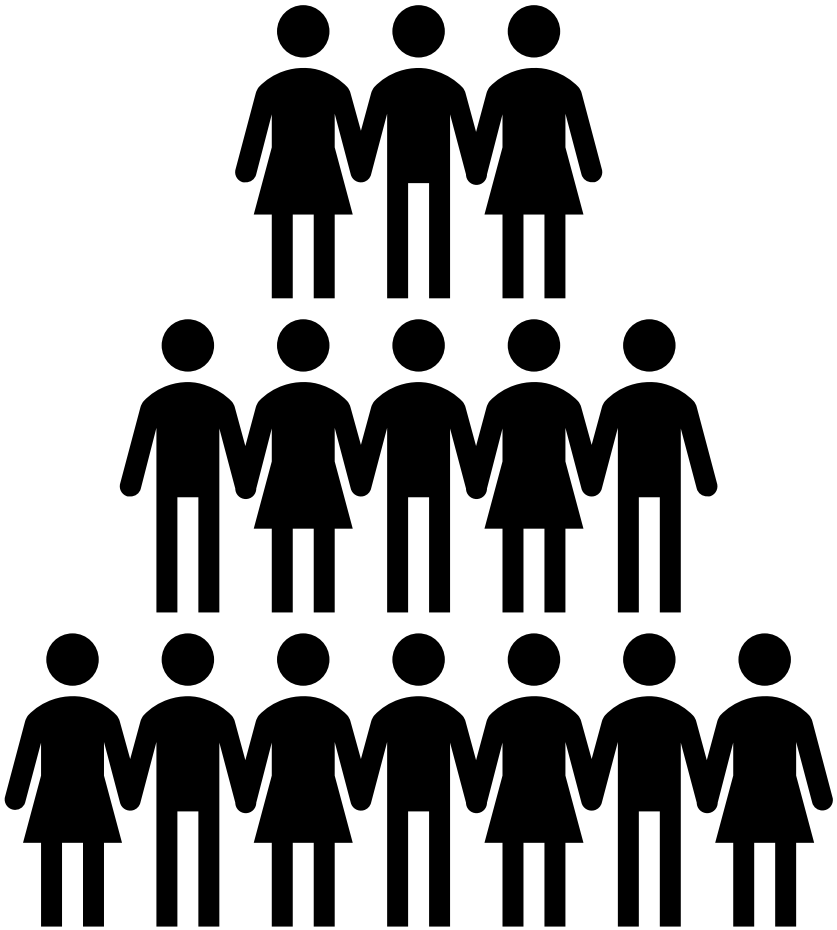
위협 인텔리전스 체계 적용/보안장비간 자동화 연동으로 인한 성과

Confidential

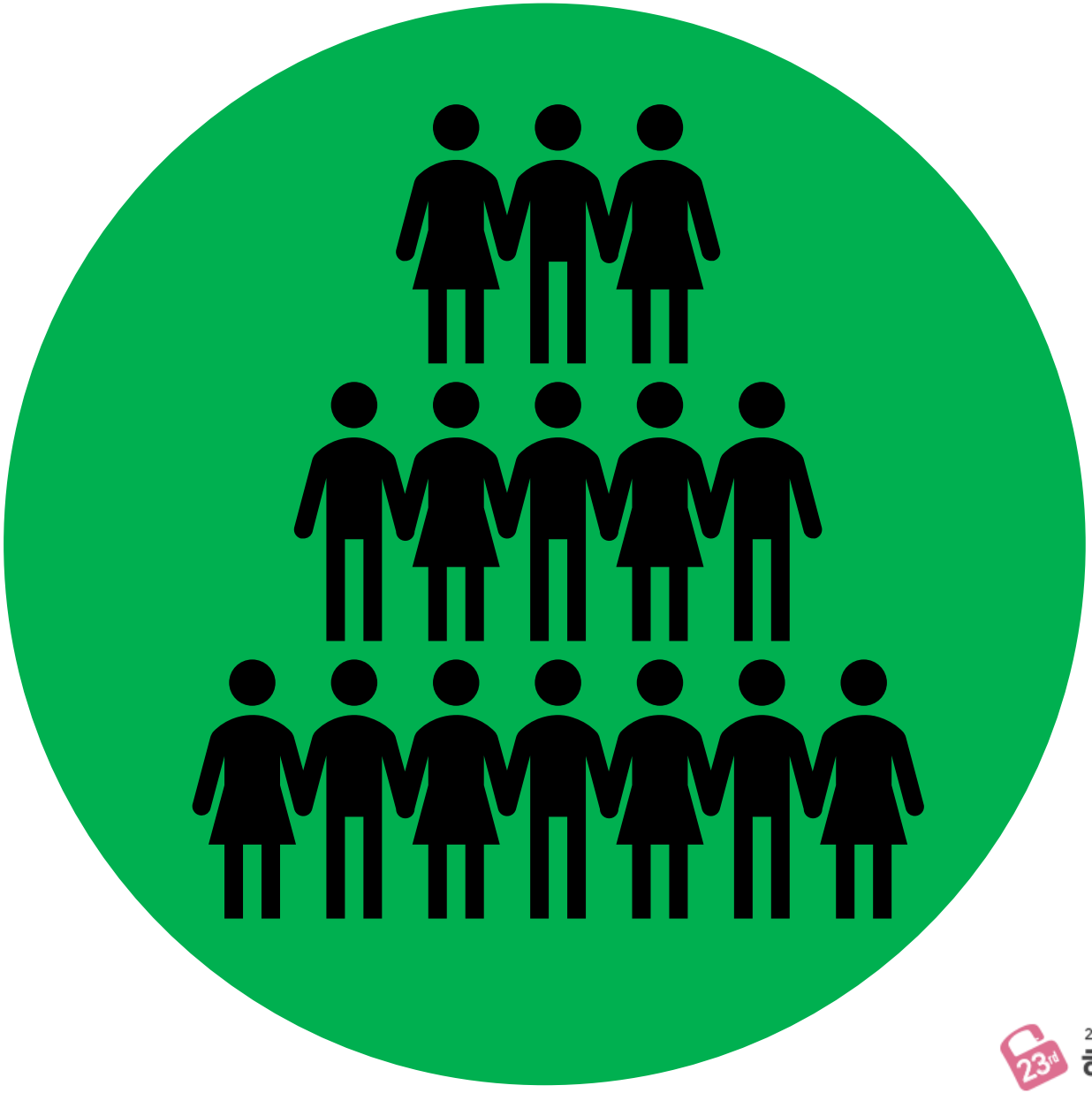
보안관제 머신러닝/AI 기술 적용



7. 맺음말



7. 맺음말



8. Q&A

End Of Presentation