DOOSAN

K-CTI 2020

2020 대한민국 사이버위협·침해사고대응 인텔리전스 컨퍼런스

위협 인텔리전스 활용을 통한 위협 선제적 방어 방어 사례

2020. 2. 5(수)

㈜두산 디지털이노베이션BU 정보보안 Chapter

김민교 대리

(minkyo2.kim@doosan.com / kim@minkyo.net)

목차

김민교 (Minkyo Kim)

0x01. Career

+ ㈜두산 디지털이노베이션BU 정보보안 Chapter 근무
+ 제 2기, 3기 사이버보안전문단(KISA)
+ 고려대학교 정보보호대학원 석사 수료

0x02. Interest

+ Security : Digital Forensics, Big Data, Compliance
+ Etc : Car Sports

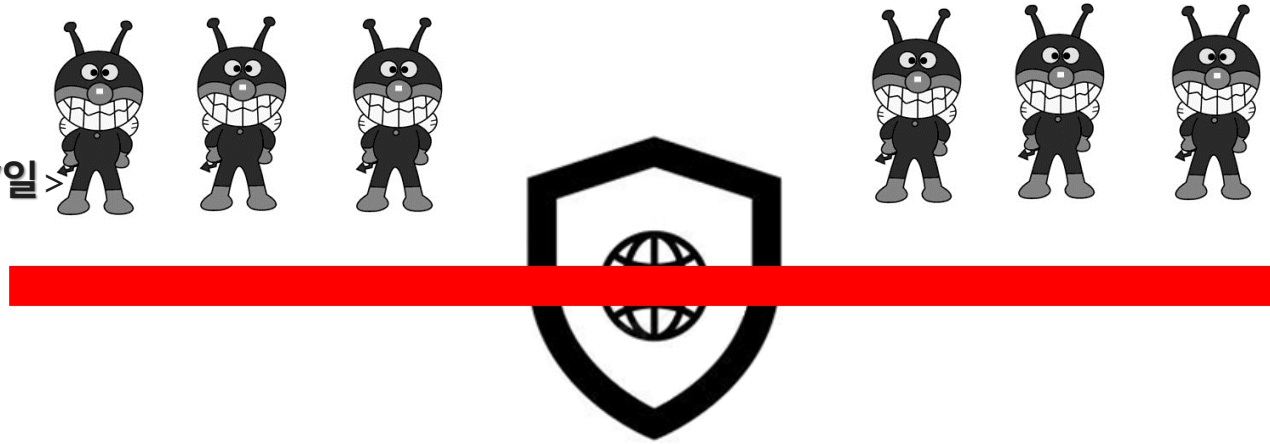
사고는 왜 계속되는가?

2. 고민의 시작

백신 패턴 업데이트 수

<약 200개 업데이트/일>

신/변종
악성코드 생성수
<최대 50만개 생성/일>



IPS/IDS, Vaccine, APT Solution, Etc…

"Very Expensive Security Solution"

패턴 기반 보안장비의 한계

선제적인 방어

위협 인텔리전스

(Threat Intellignece)

3. 위협 인텔리전스 개념

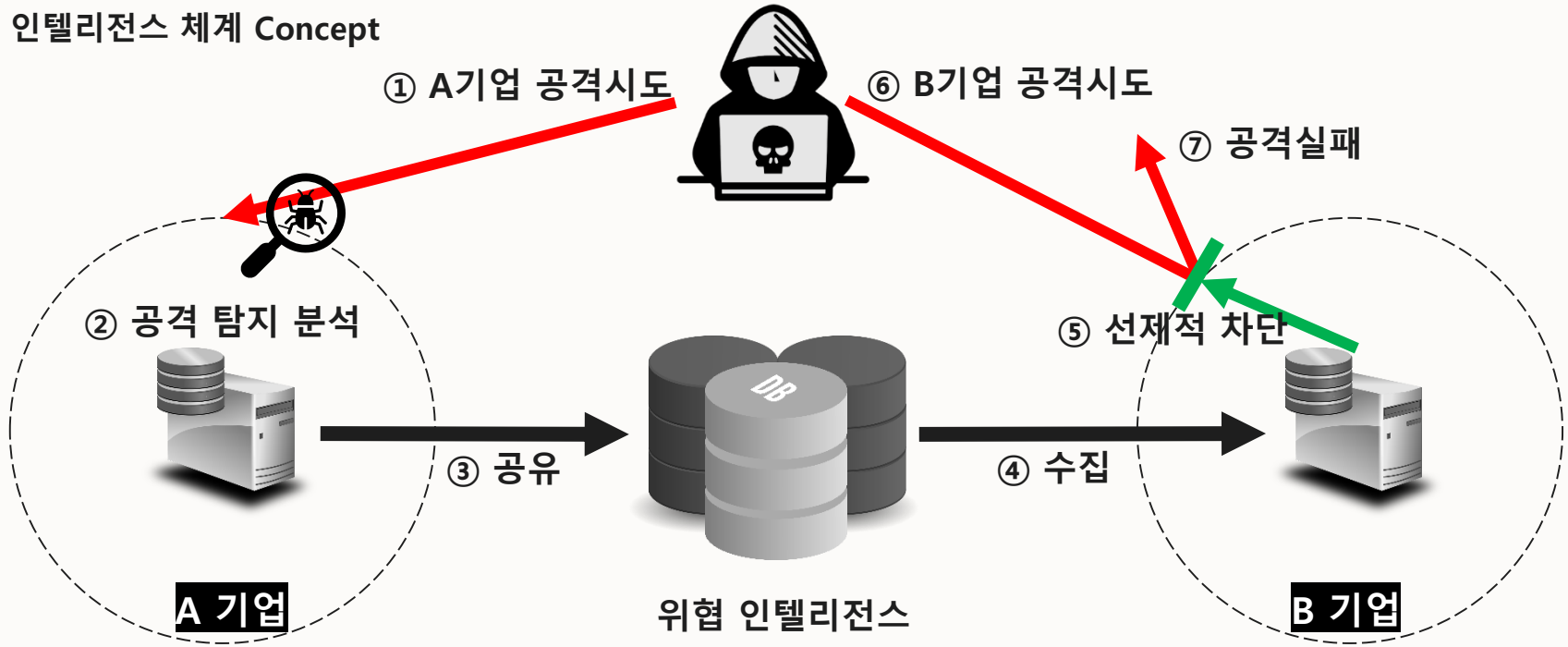
보안 시장이 Defensive security → Offensive Security로의 추세 전환에 따라 나온 개념

위협 인텔리전스(TI, Threat Intelligence)

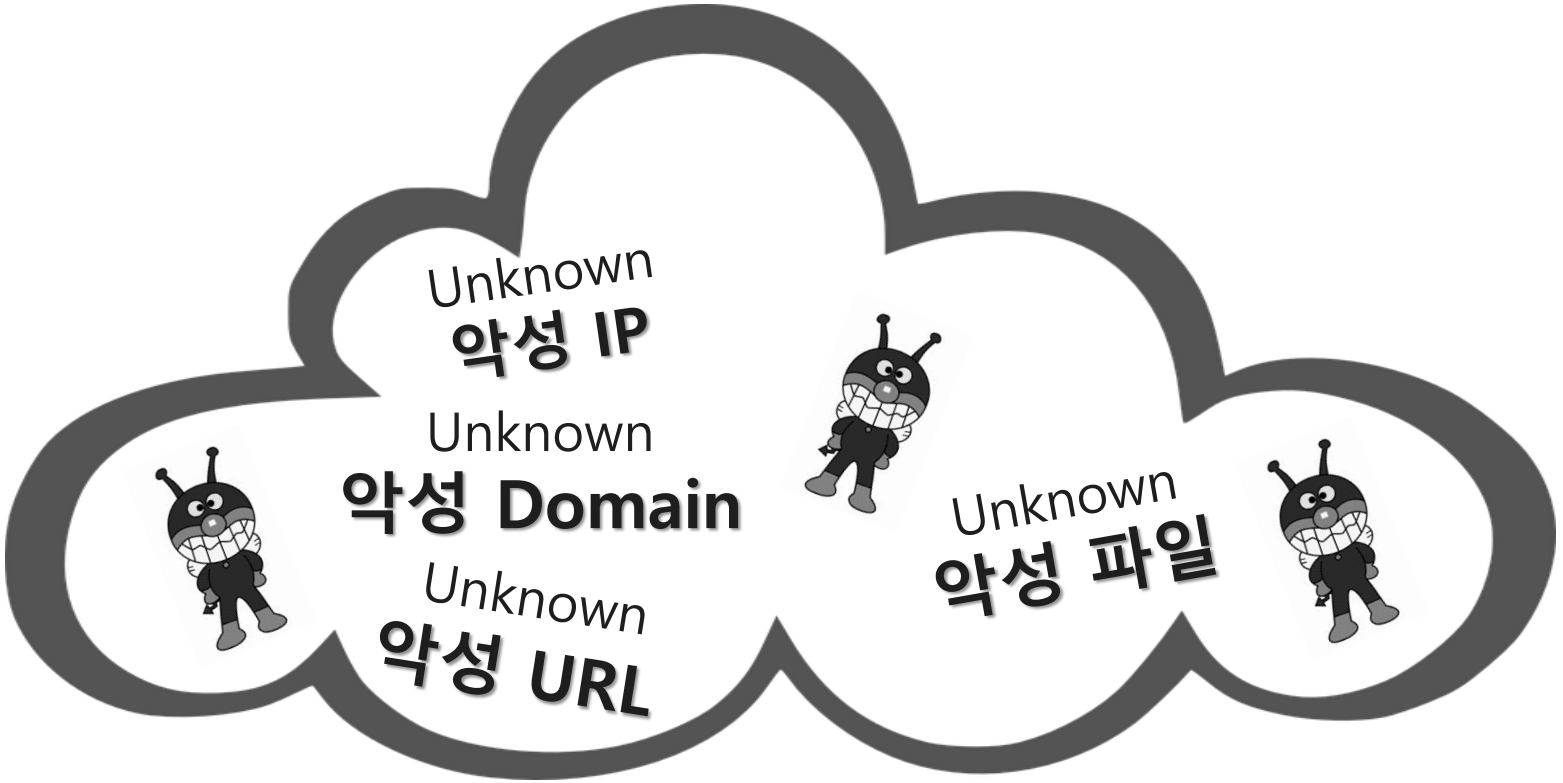
'증거를 기반하는 지식으로, 기업의 IT나 정보자산에 위협이 될 수 있는 부분에 실행가능한 조언을
컨텍스트나 메커니즘, 지표 등으로 제시하는 정보' – Gartner

'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



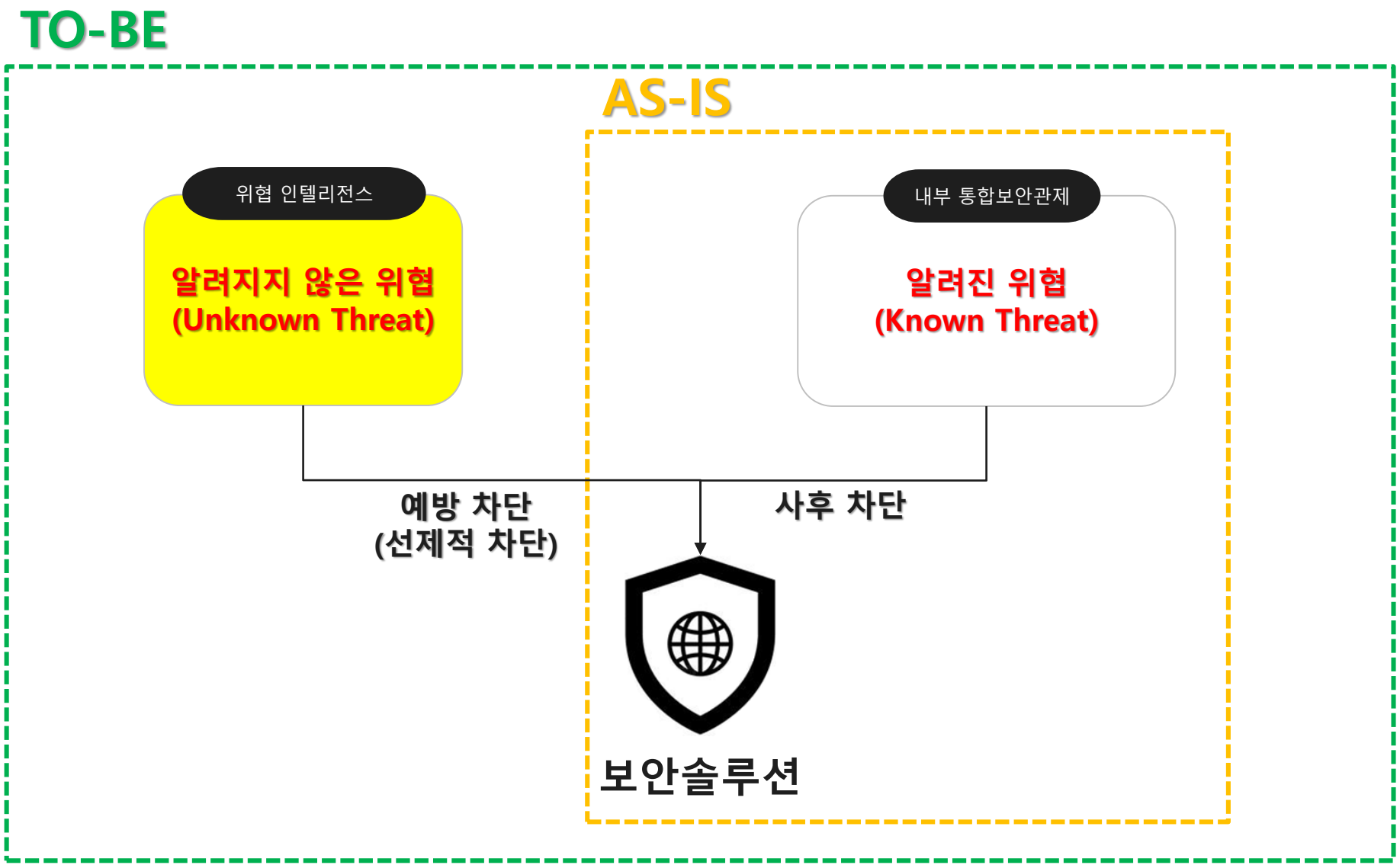
4. Idea of 선제 방어 전략



선제 접속 **차단**

선제 실행 **차단**

4. Idea of 선제 방어 전략



5. 구축/적용 진행 과정

검토/선정 (2018) › **구축 계획 수립 (2018)** › 단계별 개발 (~2019.09) › Bug-Fix/운영안정화 (~2019.12)

Global 6개 TI 대상 도입 검토/구축 계획 수립

평가 기준			평가 대상					
분류	항목	배점	C-TAS	A	B	C	D	E
정보 활용성	소계	100	70	55	65	28	23	33
	제공하는 정보수량	10	10	5	5	3	3	3
	자동화 활용가능한 정보수량	40	40	30	40	10	20	20
	참고 활용가능한 정보수량	20	20	0	20	15	0	10
	악성코드 Network단 탐지/차단	30	0	20	0	0	0	0
정보 신뢰성	소계	100	85	70	57	40	50	40
	운영 기관 공신력	30	30	30	200	10	10	20
	신뢰성/위험도 지표 제공	30	15	30	30	0	30	0
	정보 설명 제공	10	10	5	5	5	0	5
	정보 피드백 제공	10	10	0	0	10	0	0
	PoC간 치명적 오탐 미발생	10	10	0	0	10	10	10
	국내 레퍼런스	10	10	5	2	5	0	5
정보 최신성	소계	100	100	50	100	50	100	70
	정보 업데이트 주기	100	100	50	100	50	100	70
자동화 용이성	소계	100	40	100	70	10	40	20
	기존 보안장비 탐지 연동 지원	30	0	30	30	0	0	0
	기존 보안장비 차단 연동 지원	30	0	30	0	0	0	0
	정보 제공 방법(API/WEB/메일)	40	40	40	40	10	40	20
도입 비용	소계	100	85	80	45	65	85	85
	라이선스 비용(연간)	50	50	30	5	30	50	50
	H/W 운영 비용(연간)	30	30	30	30	30	30	30
	구축(개발) 비용(1회성)	20	5	20	10	5	5	5
총점		500	380	355	337	193	298	248
환산 총점(100점 만점 환산)		100	76	71	67.4	38.6	59.6	49.6

5. 구축/적용 진행 과정

검토/선정 (2018) → 구축 계획 수립 (2018) → **단계별 개발 (~2019.09)** → Bug-Fix/운영안정화 (~2019.12)

"SOA(Security Orchestration and Automation)" 관점에서의 단계별 개발 수행

1. 위협정보 집중화

외부 위협인텔리전스/내부 통합보안관제로부터
수집된 모든 위협 정보를 내부 위협인텔리전스로 집중화

2. 보안장비간 연동 자동화

수집된 위협정보를 내부 보안장비에 API를 통해 자동화 입력

개발 담당

김소천 (Socheon Kim)

Interest

보안,물류시스템,자동화,최적화,인공지능,머신러닝,딥러닝

5. 구축/적용 진행 과정

검토/선정 (2018) → 구축 계획 수립 (2018) → 단계별 개발 (~2019.09) → **Bug-Fix/운영안정화 (~2019.12)**

다량의 위협정보 차단/연동 자동화에 따른 각종 오류 Bug-Fix 및 고도화 수행

1. 부가 기능 고도화
2. 보안장비에 다량 위협정보 연동에 따른 부하 이슈 해결 고도화
3. 예상치 못한 기타 발견된 이슈 Bug Fix 등

개발 담당

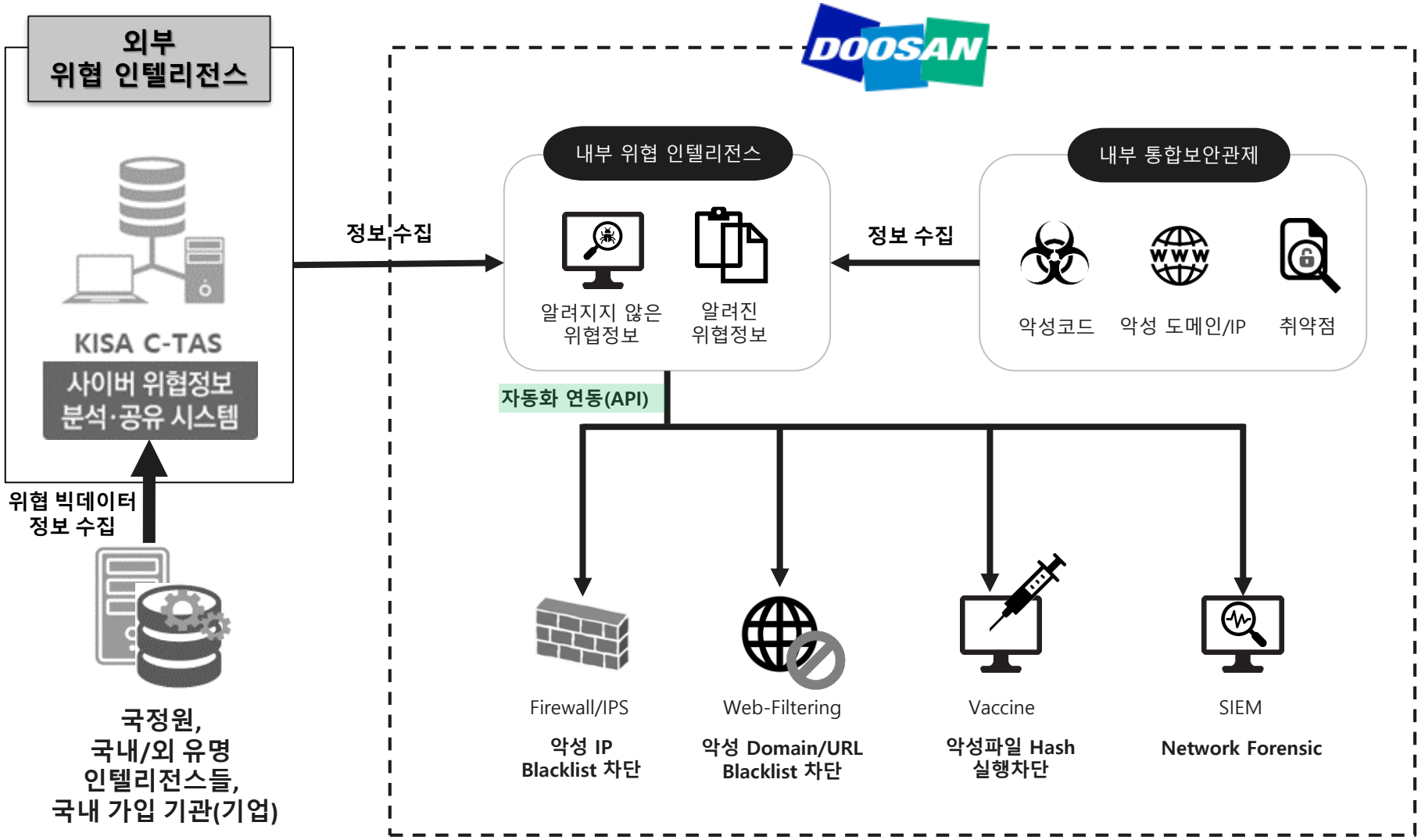
김소천 (Socheon Kim)

Interest

보안,물류시스템,자동화,최적화,인공지능,머신러닝,딥러닝

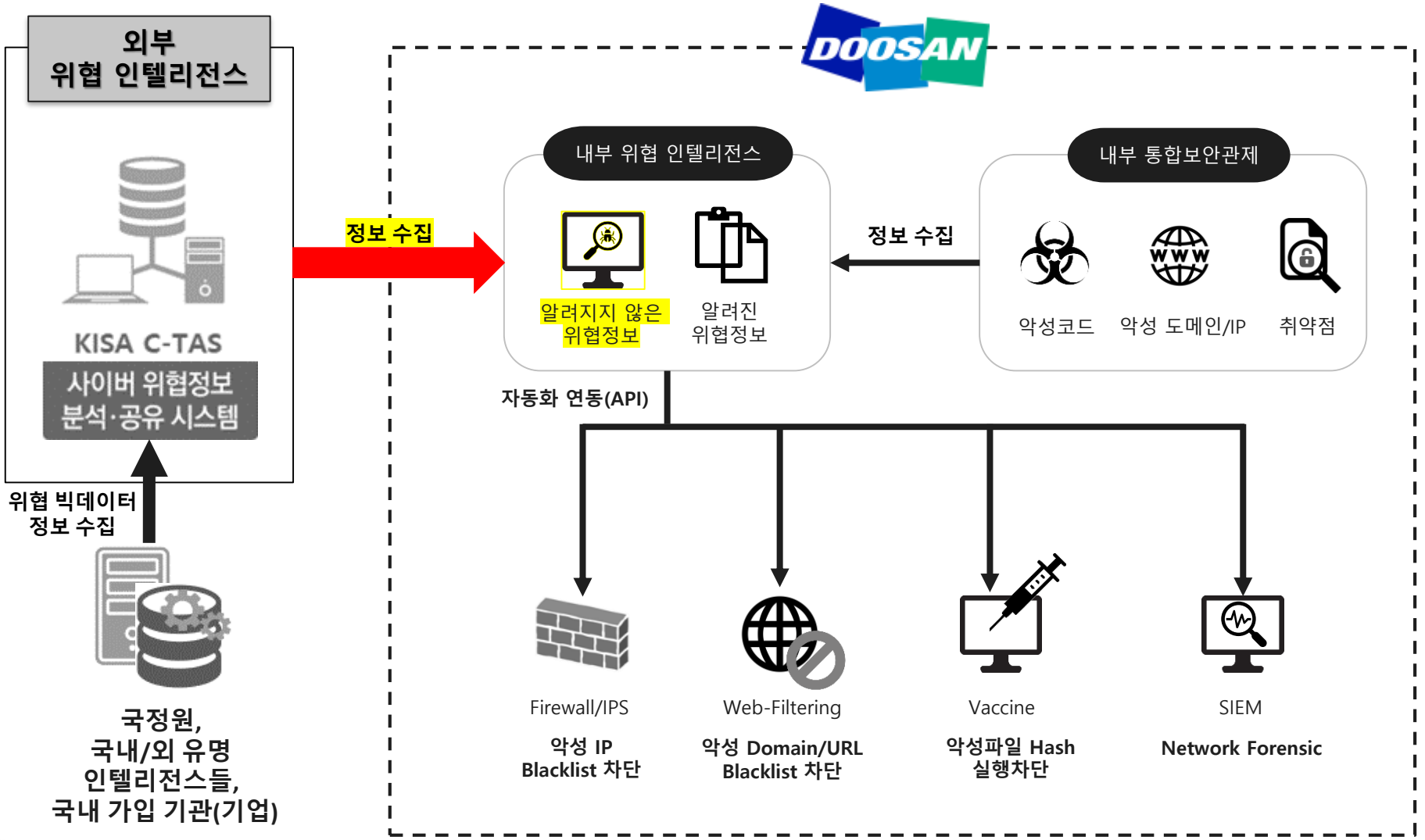
6. 위협 인텔리전스 적용 사례

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



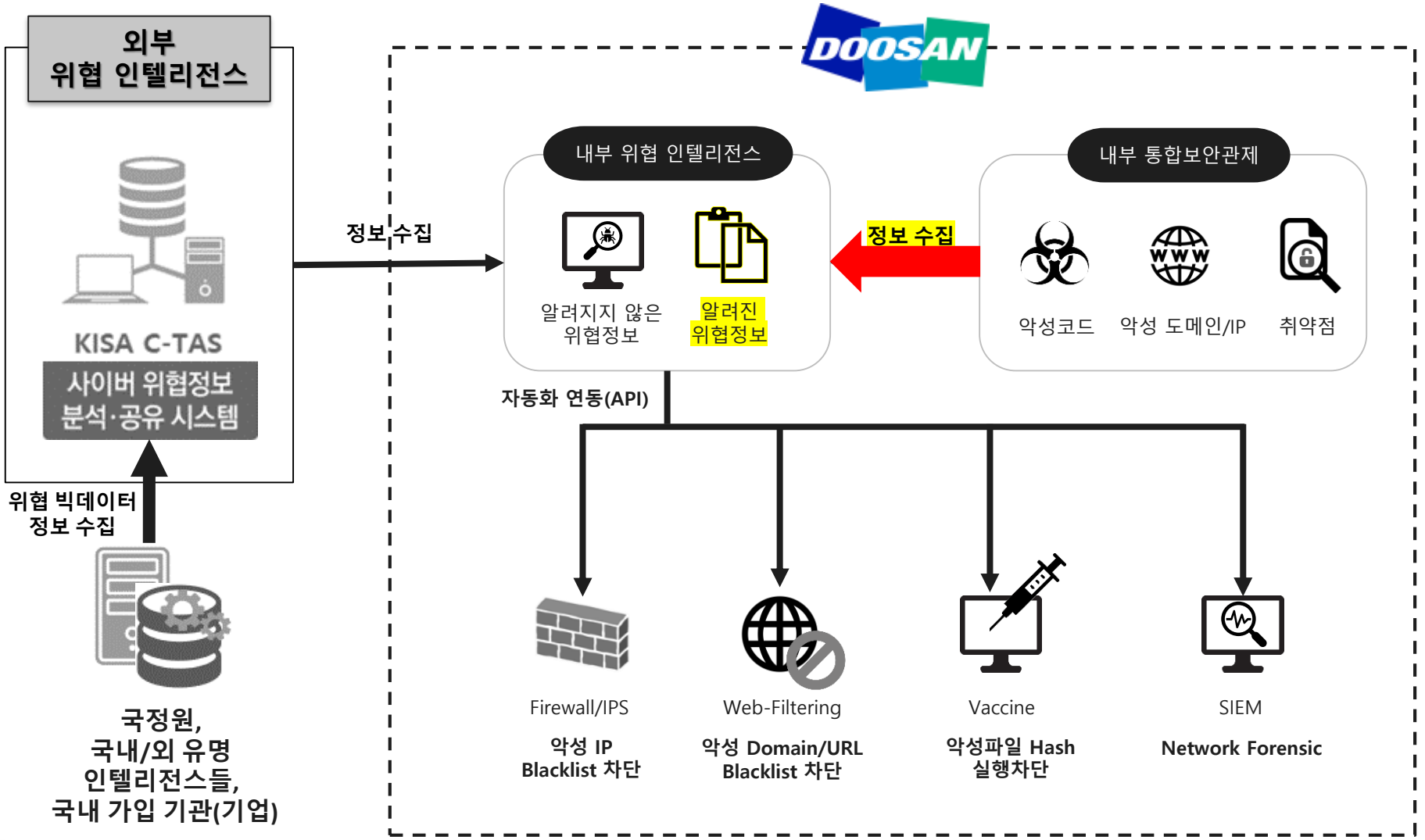
6. 위협 인텔리전스 적용 사례

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



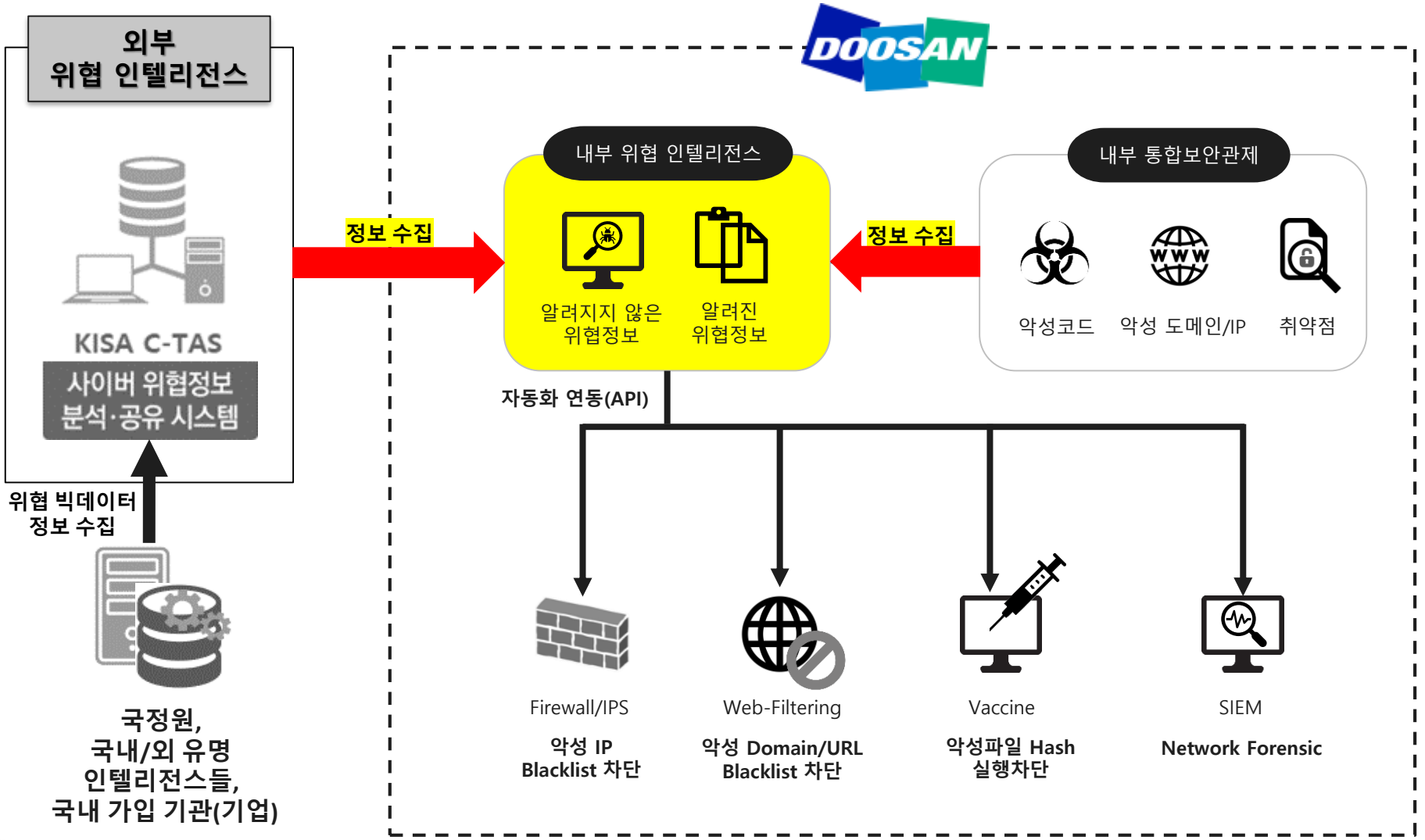
6. 위협 인텔리전스 적용 사례

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



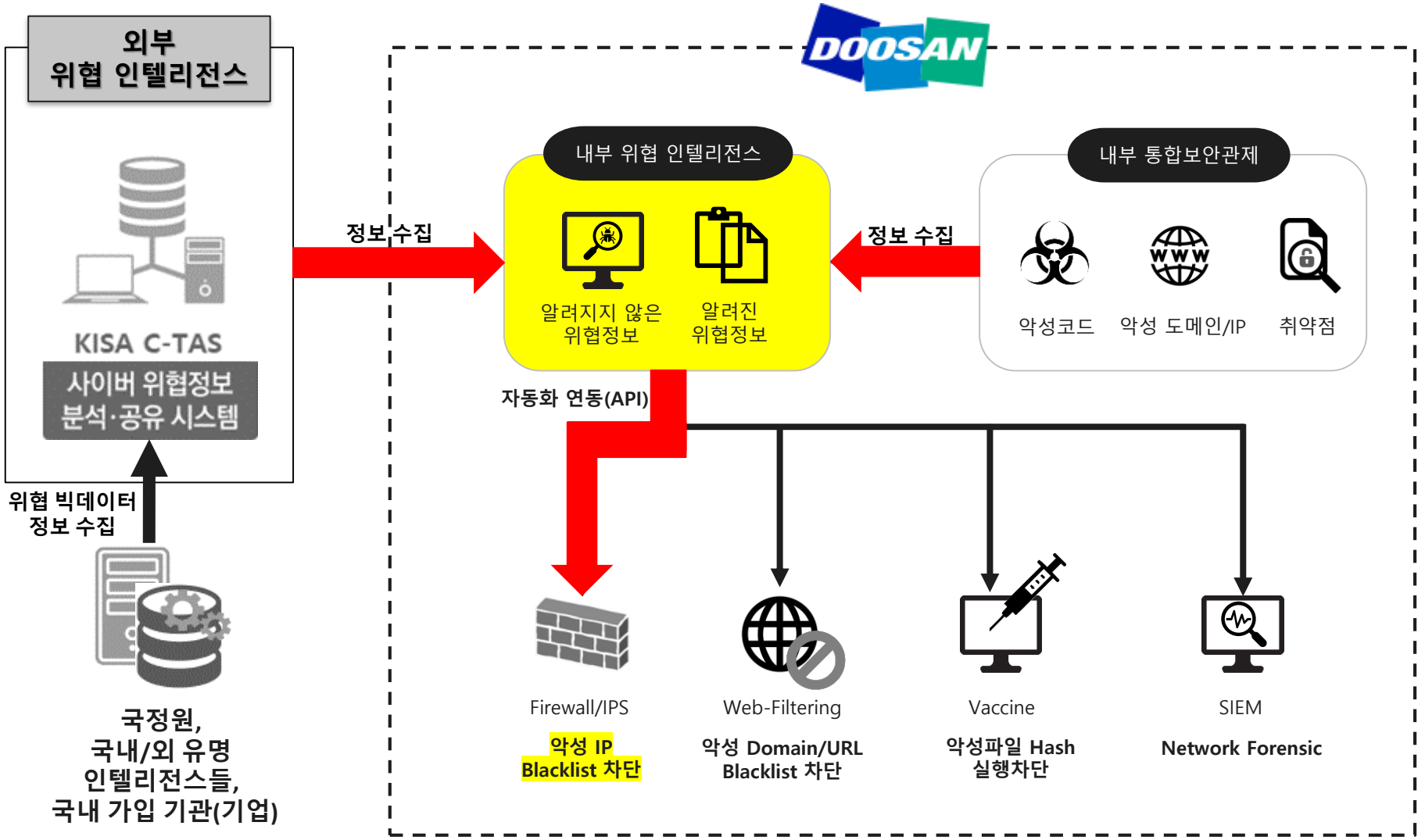
6. 위협 인텔리전스 적용 사례

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



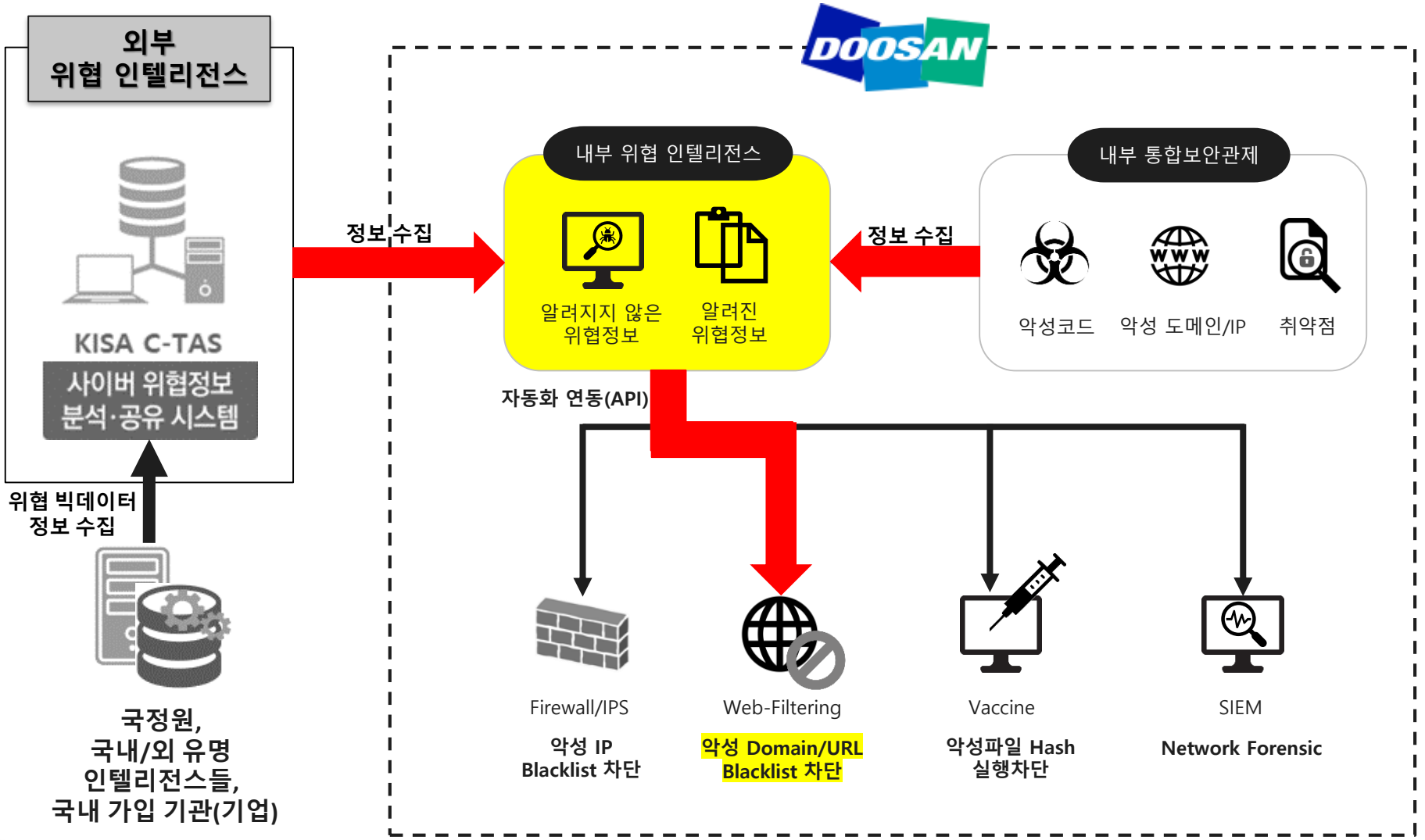
6. 위협 인텔리전스 적용 사례

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



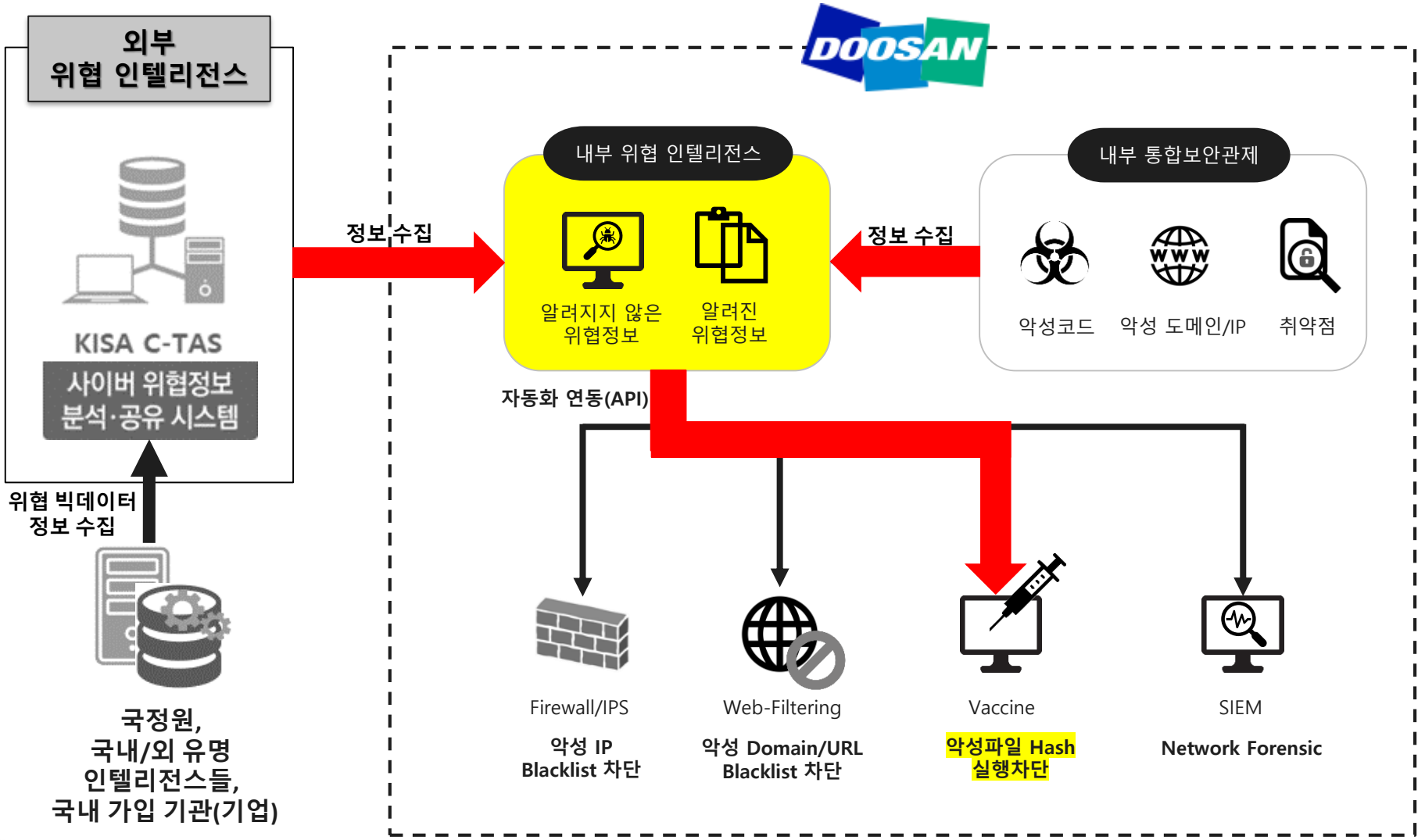
6. 위협 인텔리전스 적용 사례

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



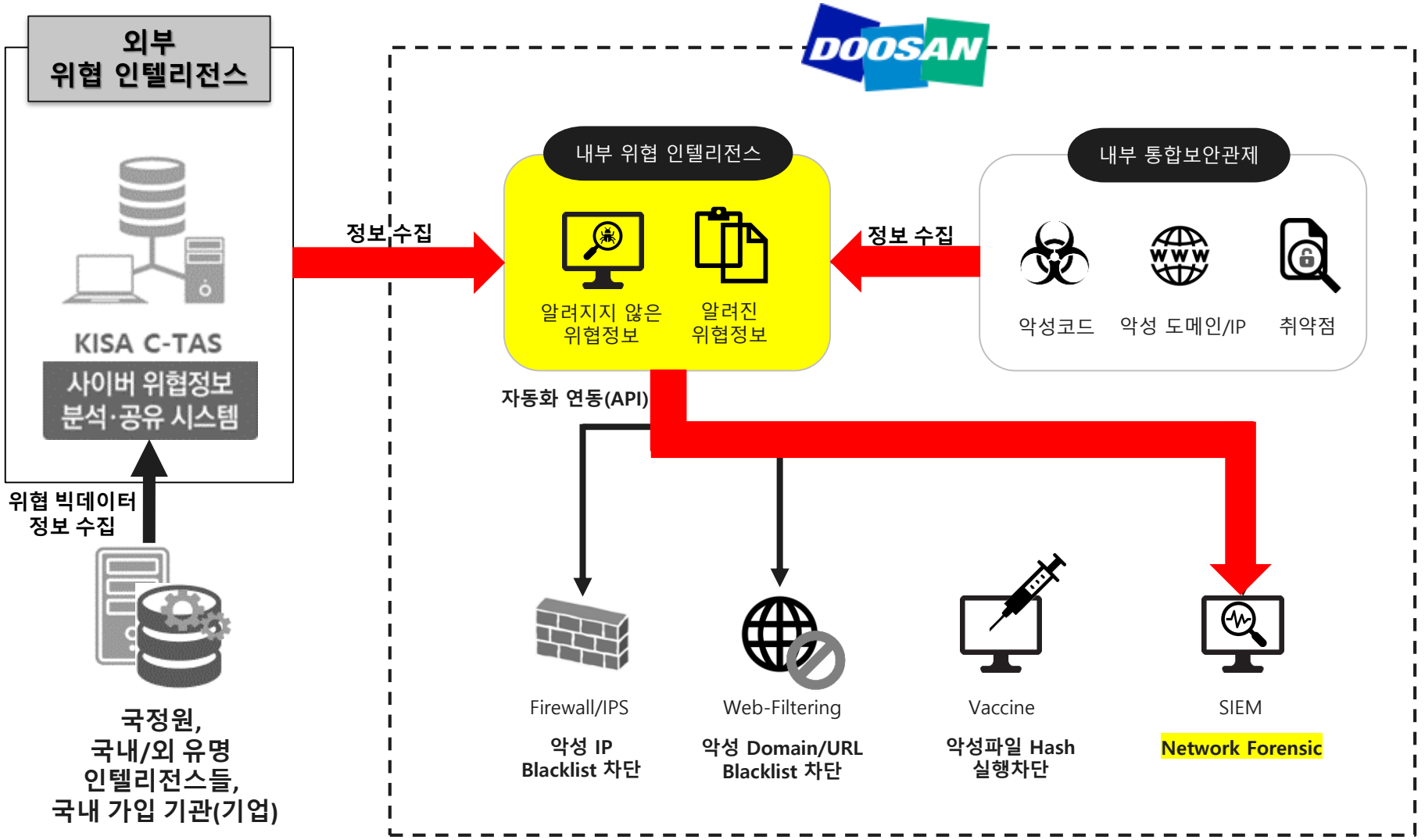
6. 위협 인텔리전스 적용 사례

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



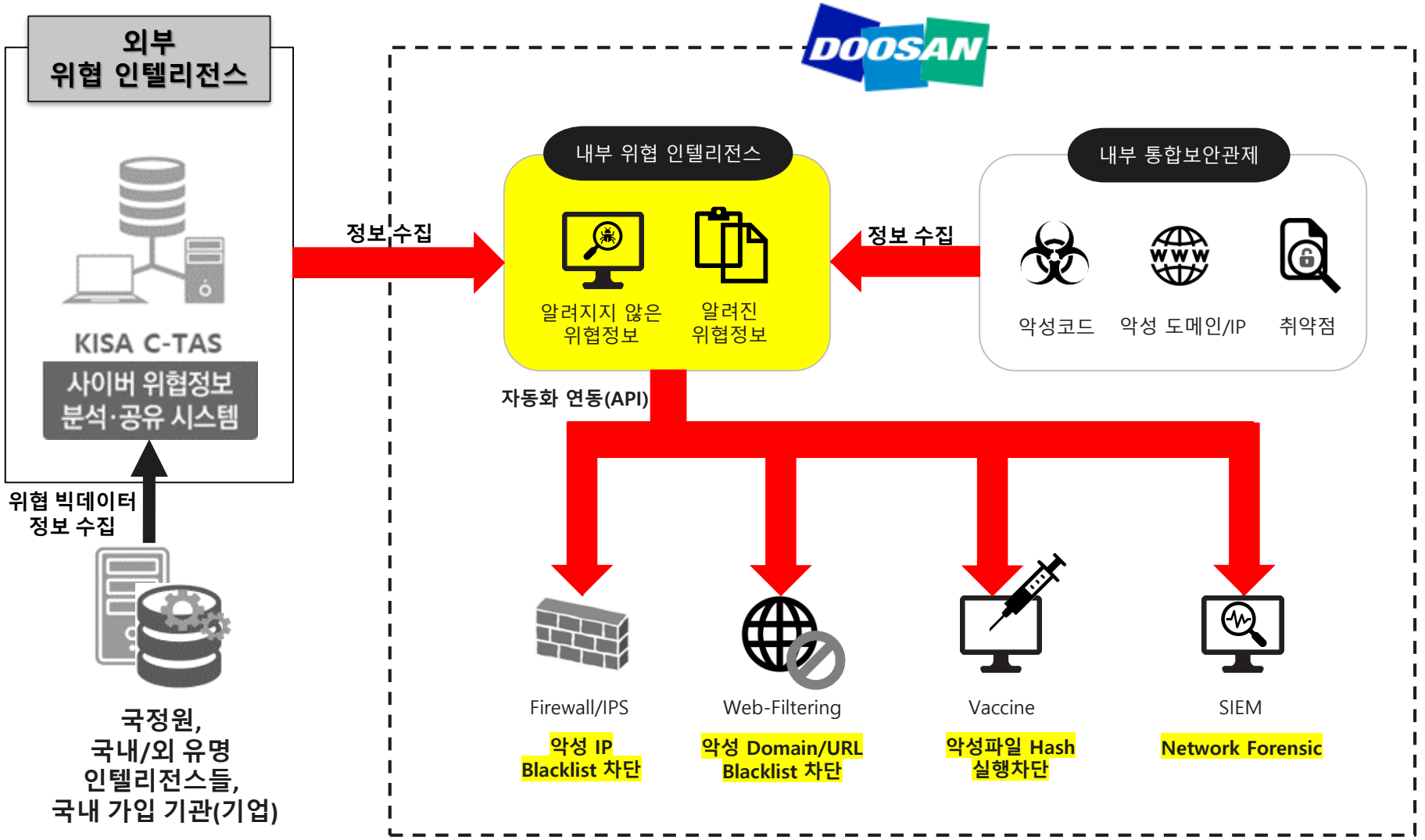
6. 위협 인텔리전스 적용 사례

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



6. 위협 인텔리전스 적용 사례

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



7. 위협 인텔리전스 적용 성과 (종합)

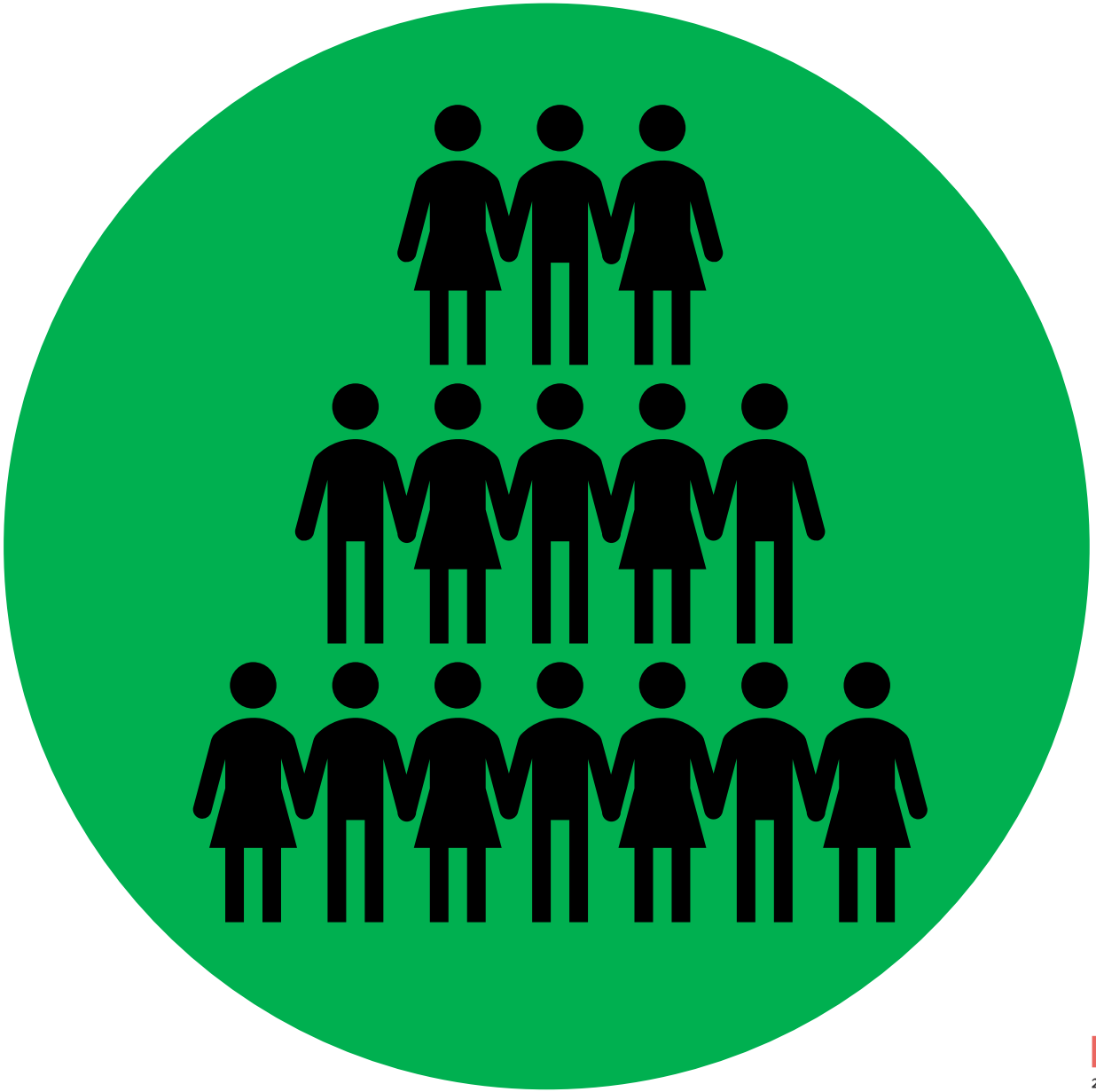
위협 인텔리전스 체계 적용/보안장비간 자동화 연동으로 인한 성과

① Unknown 위협 방어 : **60만건/월**

② Virus 유입 건 감소 : **15% 감소**

③ 위협 대응 속도 향상 : **48배 향상**

7. 위협 성공적인 방어를 위한 제언/맺음말



End Of Presentation

Questions

minkyo2.kim@doosan.com

kim@minkyo.net