kaspersky

Kaspersky EDR Optimum:
포지셔닝 & 주요 솔루션 가치

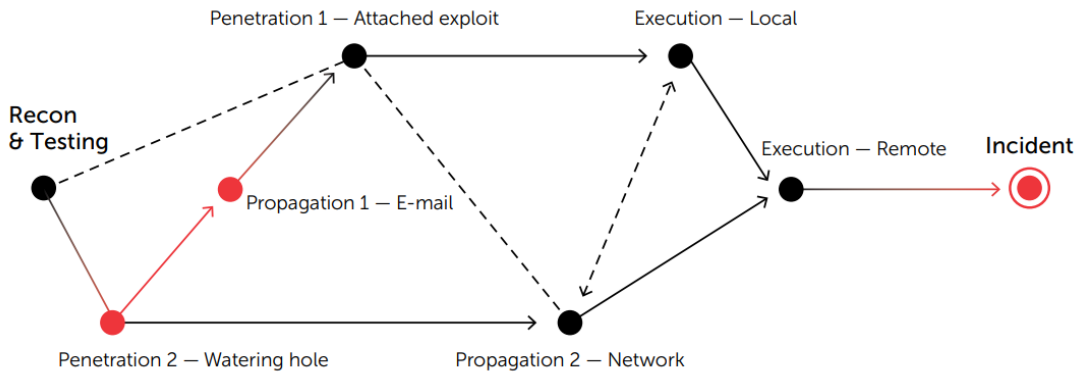
주요 내용

1. 보안 당면과제
2. 엔드포인트 방어 강화
3. EDR Optimum 소개
4. EDR Optimum 사용 사례
5. 카스퍼스키 통합 엔드포인트 보안 구축 제안
6. Kaspersky Sandbox 고급 동작 탐지 기능의 활용

보안 당면과제

최신 위협 환경

합법적 도구 및 파일리스 위협 활용	은밀함 & 모호함
기업은 해킹 공격의 좋은 수익원(예: 랜섬웨어 성행)	강력한 효과
다중 킬 체인 단계를 구성하고 이를 여러 차례 반복	복잡성 & 지속성



기업이 인식하는 문제점:

- 위협 건수 증가
- 공격 시나리오의 복잡성 증가
- 위협으로 인한 금전적 피해
- 규제 준수 문제 해결의 필요성

오늘날 기업의 당면과제

복잡한 위협에 대응할 수 있는 능력이 기업에 반드시 필요하지만...

...IT 보안 인력 및 전문지식의 전 세계적 부족 현상이 걸림돌

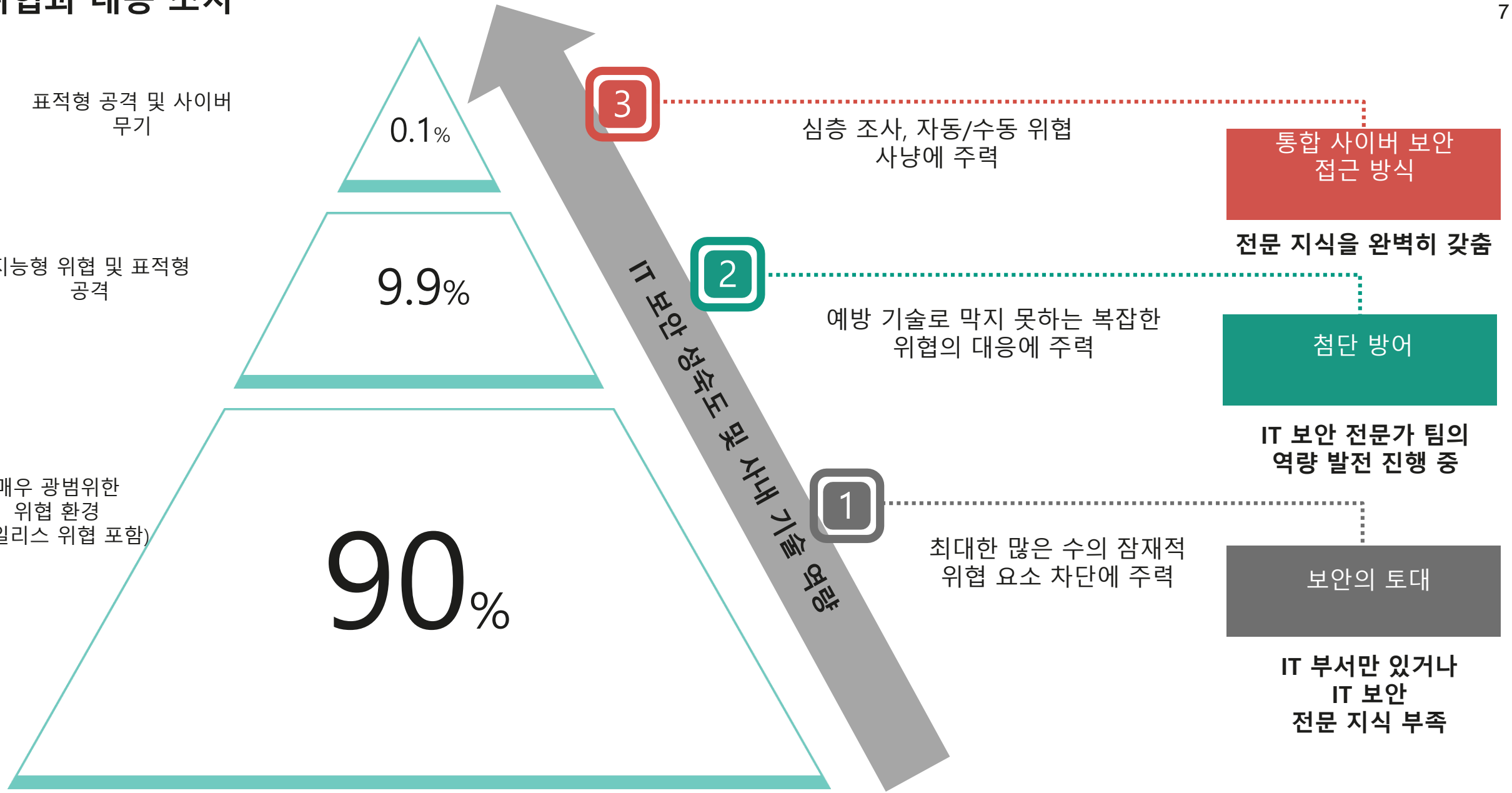
전체 기업 중 다양한 IT 보안 직무 숙련 인력 고용에 어려움을 겪는 기업의 비율*

리소스가 부족한 기업이 취해야 할 조치:

- 자동 기능 활용 극대화
- 귀중한 리소스는 중요하고 가치 있는 업무에 투입
- 최신 위협 환경에 대응할 수 있는 추가 역량 확보
- 관리형 서비스로 사내 인력 보강

*출처: Cybersecurity Through the CISO's Eyes PERSPECTIVES ON A ROLE(451 Research, 2019년)

위협과 대응 조치


표적형 공격 및 사이버 무기
0.1%
지능형 위협 및 표적형 공격
9.9%
매우 광범위한 위협 환경 (파일리스 위협 포함)
90%
IT 보안 성숙도 및 사내 기술 역량
3
심층 조사, 자동/수동 위협 사냥에 주력
통합 사이버 보안 접근 방식
전문 지식을 완벽히 갖춤
2
예방 기술로 막지 못하는 복잡한 위협의 대응에 주력
첨단 방어
IT 보안 전문가 팀의 역량 발전 진행 중
1
최대한 많은 수의 잠재적 위협 요소 차단에 주력
보안의 토대
IT 부서만 있거나 IT 보안 전문 지식 부족

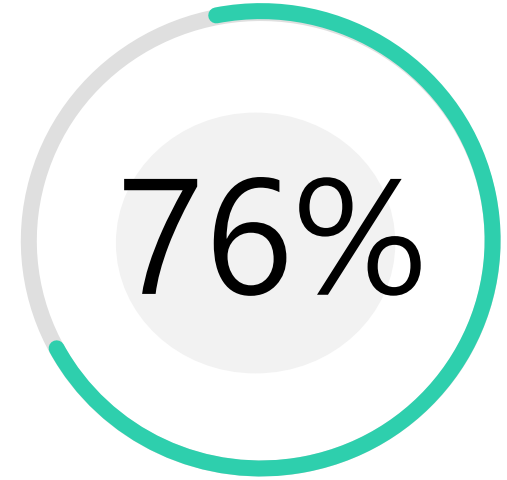
엔드포인트 방어 강화가 최우선

엔드포인트 보호의 중요성

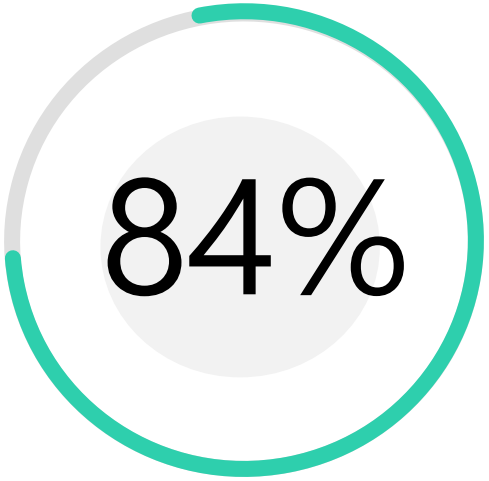
가장 취약한 요소이자 매우 보편적인 IT 인프라 진입점

차단 기준이 충분하지 않은 경우 엔드포인트를 핵심 데이터 출처로 하여 효과적인 사건 조사 가능

네트워크 트래픽 해독이 까다로운 TLS 1.3의 도입으로 인해 엔드포인트에 몰리는 관심 증가



등록된 전체 보안 이벤트의 76%가 엔드포인트로 인해 발생



여러 서버/워크스테이션이 관련된 사건의 비율

출처: The SANS 2018 Endpoint Protection and Response Survey

고객의 고민

전문 지식 부족

역량을 갖춘 전담 보안 전문가가
없는 경우

예산의 제약

전문 EDR 솔루션을 갖추기 위한
예산이 충분하지 않은 경우

복잡성 증가

다양한 관리 콘솔/에이전트

대응

자동화 수준은 어느 정도인가?
유사 이벤트 검색 능력을 갖추고
있는가?

새로운 차원의 엔드포인트 방어가 필요한 이유

갈수록
교묘해지는 공격

□ 보안 문제 자동 방지 이상의 보호 기능이 절실히 필요 – EPP 제어를 **피할 수 있도록 설계된 공격**에 대한 적절한 분석과 조사가 필수

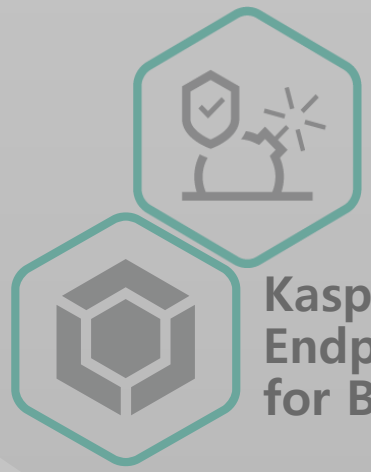
□ 엔드포인트 원격 분석 정보를 효과적으로 분석하면 IT 보안 인력이 사건을 전체적으로 파악하고 풍부한 정보를 바탕으로 의사결정을 내리며 규제 요건을 준수할 수 있음

이에 반드시 필요한 기능

엔드포인트
탐지 및 대응 (EDR)

카스퍼스키 솔루션: 성숙도 기반의 접근 방식

전담 보안 전문가 부족



Kaspersky Sandbox

Kaspersky Endpoint Security for Business

- IT 부서
- IT 부서 내 보안 팀
- 사무실이 분산되어 있고 업무 현장에 전담 보안 전문가가 없는 기업

전문 지식 역량 개발 진행 중

Kaspersky EDR Optimum

- 정보 보안이 IT 부서의 소관인 경우
- 소규모 보안 부서
- 보안 인력 추가 고용 계획이 없는 경우

안정적인 보안 실행

Kaspersky Anti Targeted Attack Platform

Kaspersky EDR Expert

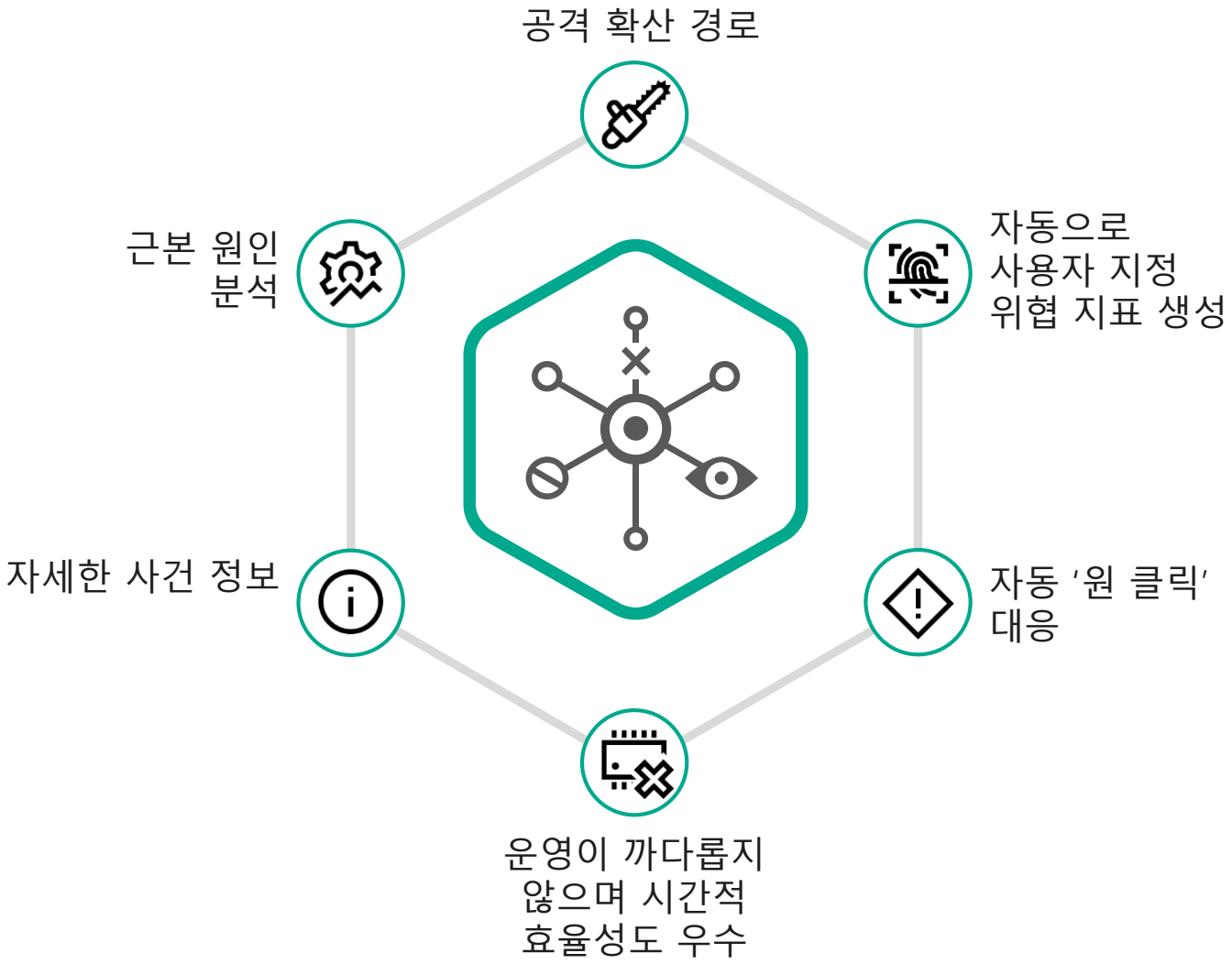
- 충분한 인력을 갖춘 보안 부서
- SOC/CERT/CSIRT
- 보안 위협 사냥 담당 팀

EDR Optimum 소개

Kaspersky EDR Optimum

주요 목표:

- 사건을 가시적으로 더욱 분명하게 확인 가능
- 솔루션 구축 관련 경비 절감
- 간단하게 사용할 수 있는 조사 도구 제공
- 복잡하고 모호한 위협에 신속하게 대응하여 더 큰 피해 발생 방지



가시성 및 분석 기능

공격 경로 가시화 – 사건과 관련된 모든 이벤트* 연결

- EPP 위협 탐지
- 코드 삽입
- 다른 프로세스를 생성하는 프로세스(Spawning)
- 파일 생성
- 네트워크 연결
- 레지스트리 수정

공격 증거에 대한 자세한 설명 – 사건 정보 카드를 통해 근본 원인 분석

감염된 서버와 워크스테이션을 **모두 파악할** 수 있는 능력

* EDR 에이전트는 전체 원격 분석을 KSC에 공유하지 않습니다(RCA에 필요한 해당 상세 데이터만 공유).

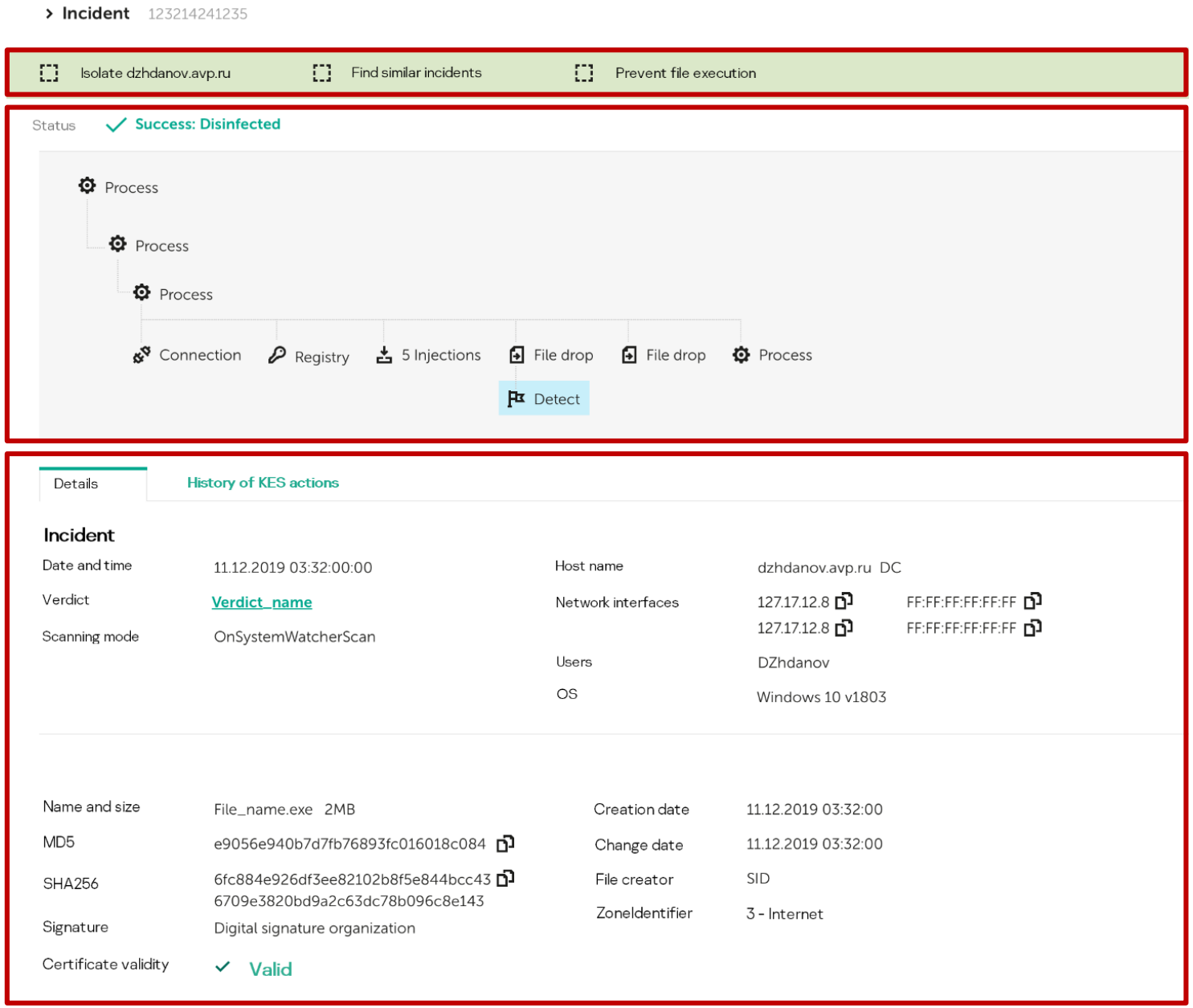
기존 KES 고객이 누리는 이점

기존에 **설치된 소프트웨어 에이전트에서** 샌드박스/EDR 기능 **이용**

TCO 절감: 사건 처리 간소화, 유지관리 비용 최소화, 인력 개입 최소화를 통한 총 소유 비용 절감

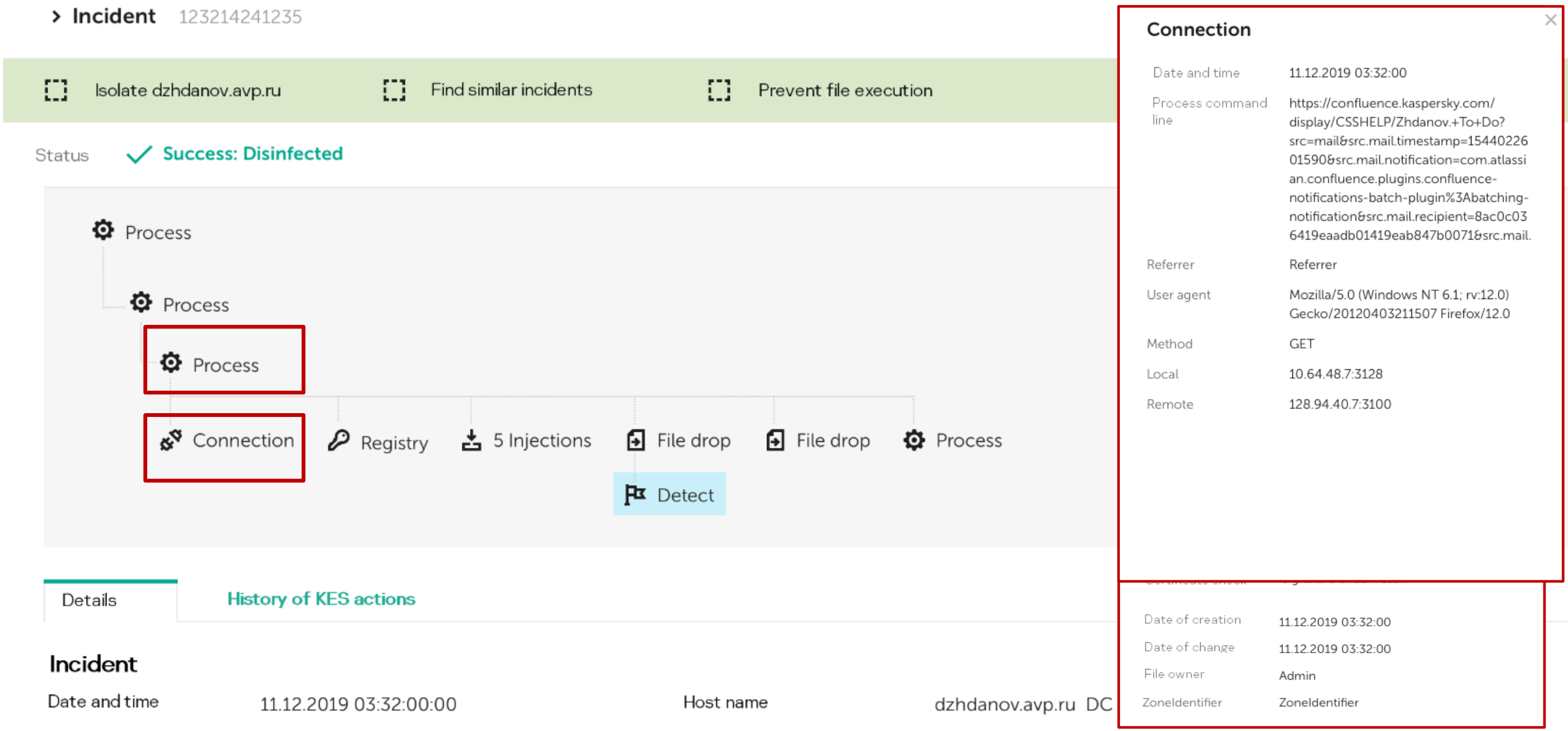
통합 콘솔: KSC 웹이 중앙 집중식 관리 콘솔의 역할을 함(온프레미스 및 클라우드)

EDR Optimum의 사건 정보 및 프로세스 실행

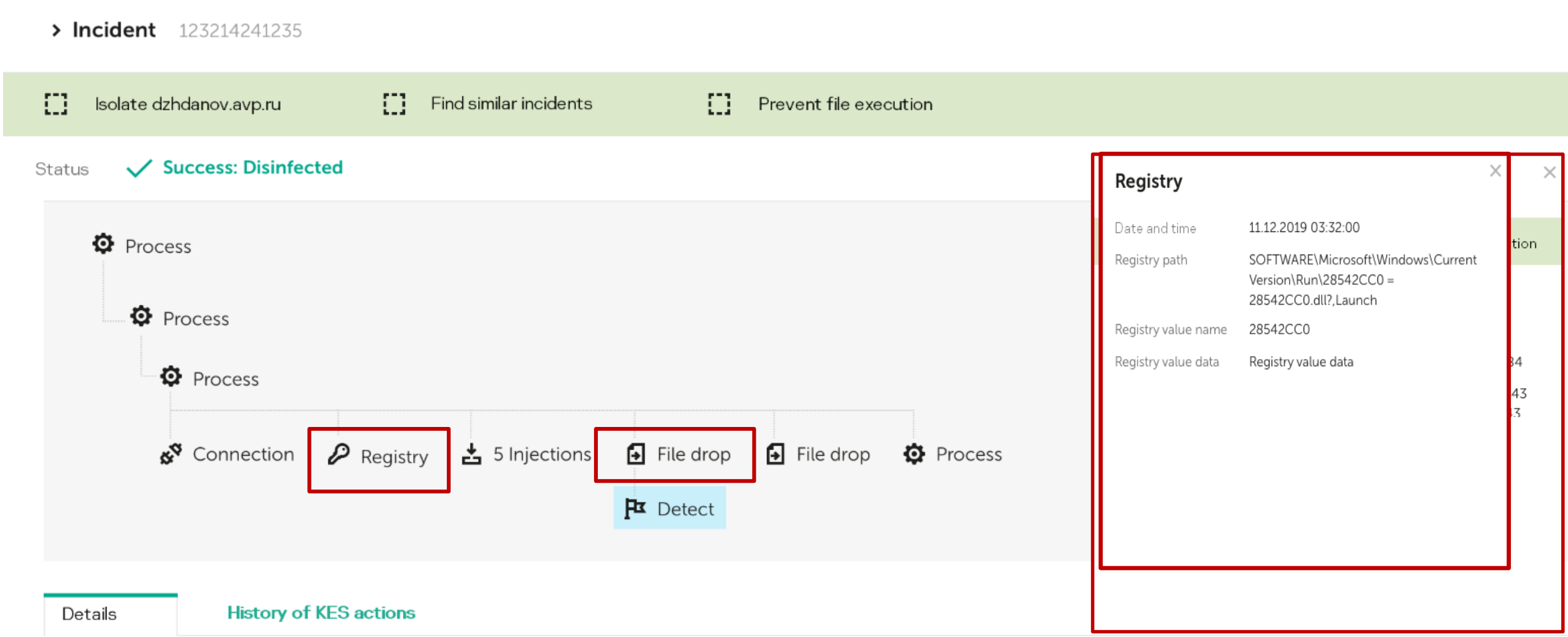


- 신속한 조치:
  - 격리
  - 유사 사건 검색
  - 파일 실행 차단
- 프로세스 실행 지도
- 사건 증거

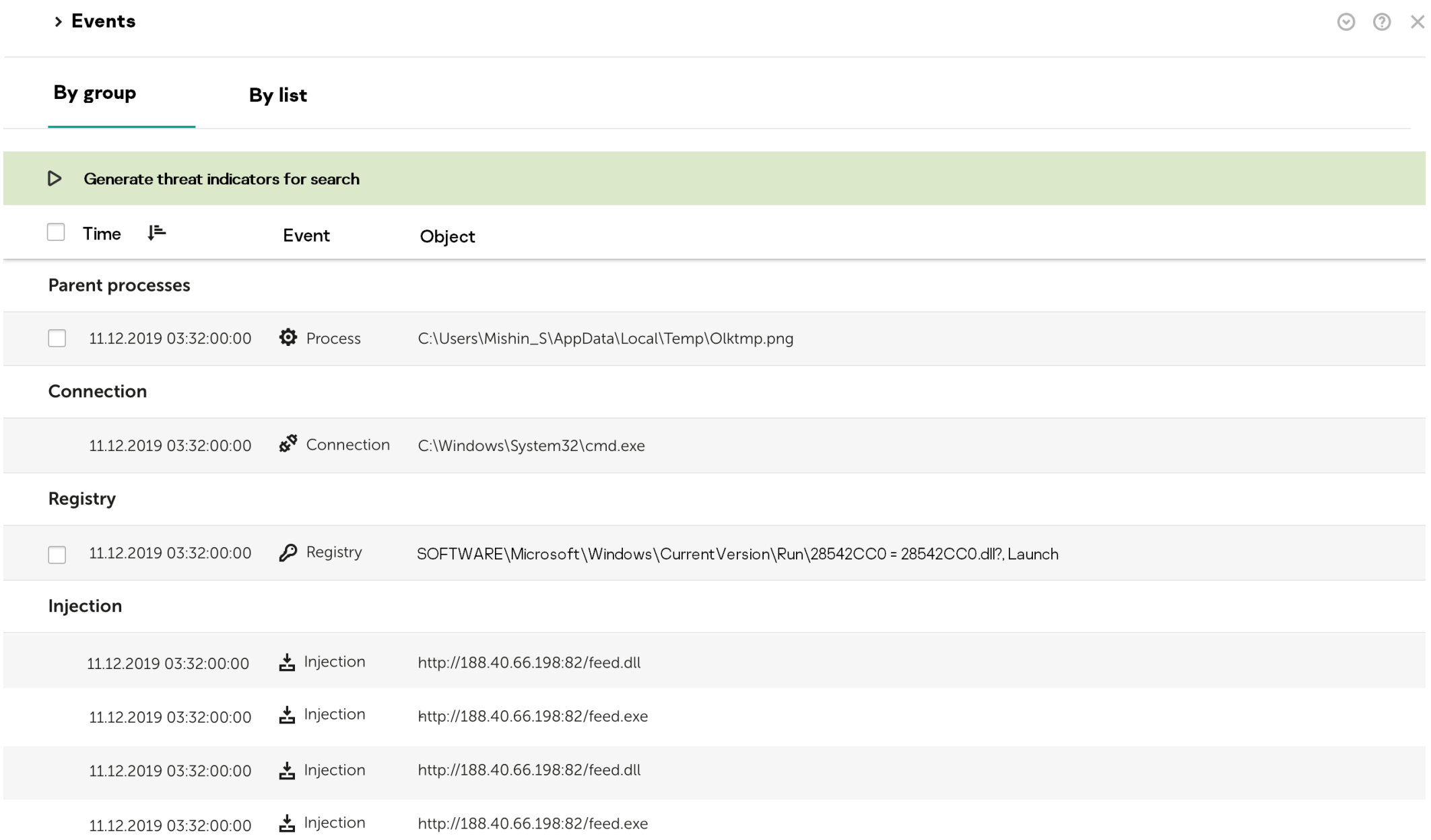
EDR Optimum의 사건 정보 및 프로세스 실행



EDR Optimum의 사건 정보 및 프로세스 실행



카테고리별 이벤트 분류(프로세스별, 레지스트리별 등)



사건 이벤트 목록

Events

By group | By list

Generate threat indicators for search

Time	Event	Object
11.12.2019 03:32:00:00	Process	C:\Users\Mishin_S\AppData\Local\Temp\Olktmp.png
11.12.2019 03:32:00:00	Connection	C:\Windows\System32\cmd.exe
11.12.2019 03:32:00:00	Registry	SOFTWARE\Microsoft\Windows\CurrentVersion\Run\28542CC0 = 28542CC0.dll?, Launch
11.12.2019 03:32:00:00	Injection	http://188.40.66.198:82/feed.dll
11.12.2019 03:32:00:00	File drop	C:\Users\Mishin_S\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\iexplore.exe
11.12.2019 03:32:00:00	File drop	-
11.12.2019 03:32:00:00	File.exe	C:\Users\Mishin_S\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\iexplore2.exe

대응 절차 간소화

다양한 대응 조치

- 호스트 격리
- 호스트 AV 검사 시작
- 파일 삭제/격리
- 프로세스 종료
- 파일 확보
- 파일 실행 차단
- 파일을 KES 화이트리스트에 추가/카스퍼스키로 전송하여 분석

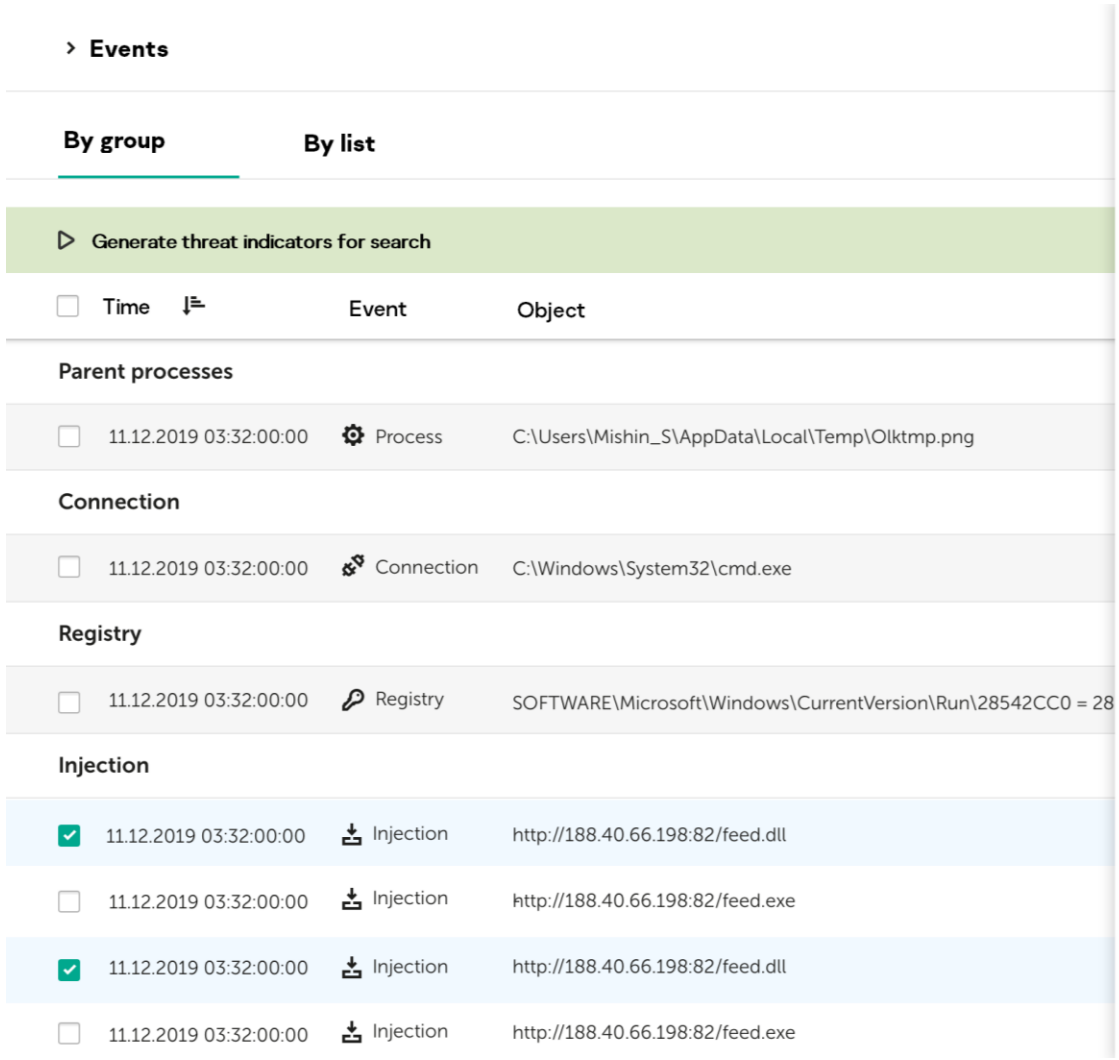
- 외부 지표 가져오기(위협 인텔리전스 공급업체/규제 기관)
- 실시간/예약 인프라 검사 - '원 클릭' 대응 기능을 갖춘 지표 기반 검사

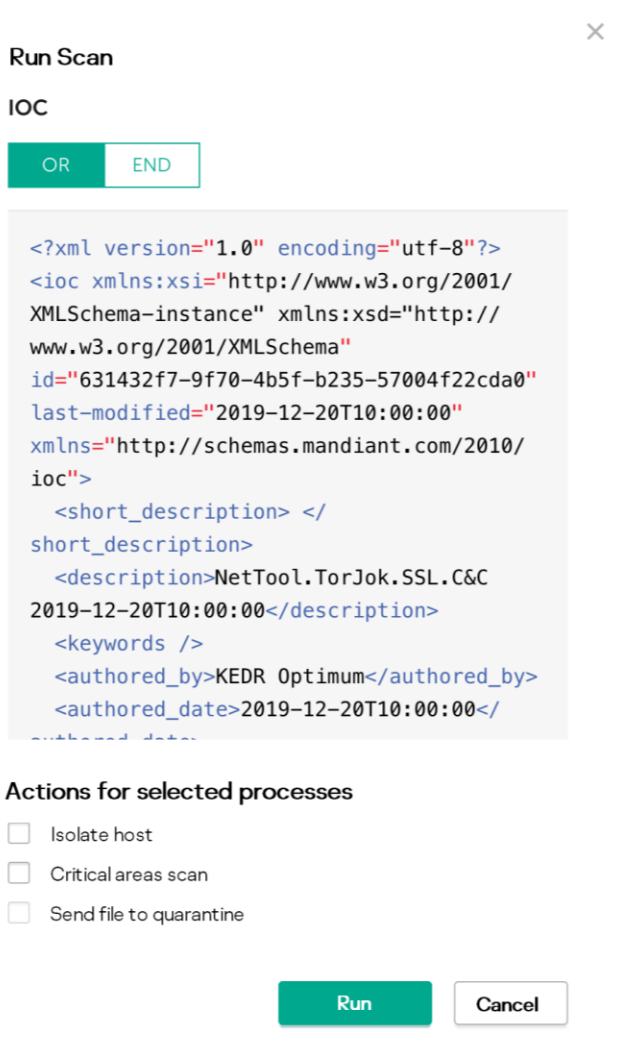
자동으로 사용자 지정 위협 지표 생성
- 자동 '교차 엔드포인트' 대응 기능 적용 가능

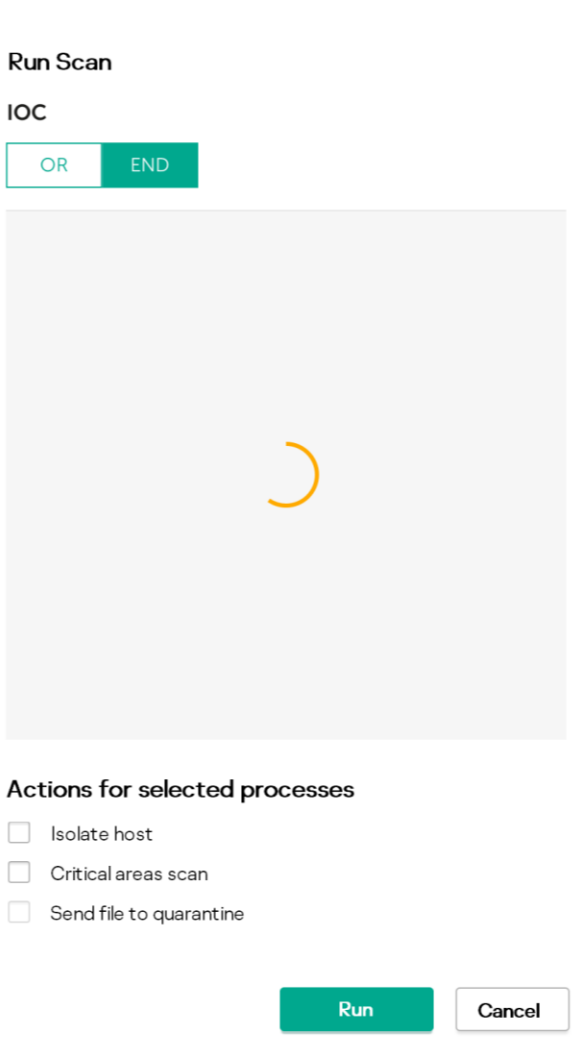
의심스러운 활동 탐지 시 EDR Optimum이 다른 호스트에서 유사 이벤트 검색 가능

* OpenIOC

사용자 지정 위협 지표 및 대응 옵션 선택







사건 정보 카드

호스트 정보

- 이름
- IP/MAC 어드레스
- 활성 사용자
- OS/사용하는 Active Directory

판정

- 탐지 유형(예: 실행 중)
- 대응 상태(격리/감염 제거)
- 탐지 기술

파일 발생 기록

- 최초 확인된 실행
- 실행 횟수
- 파일 변경 프로세스 경로 등

프로세스 세부 정보

- 파일 프로세스 경로
- 프로세스 명령
- PID
- 상위 프로세스 경로
- 사용자
- 로그온 세션 ID
- 세션 유형(대화식, 원격 등)
- 프로세스 무결성 수준
- 권한 있는 그룹의 사용자 멤버십

파일/의심스러운 프로세스 설명

- 파일 유형
- 파일 경로
- 해시(Md5/Sha256)
- 크기
- 생성/변경 날짜
- 소유자
- 특징
- ADS값
- 시그니처 등

네트워크 연결

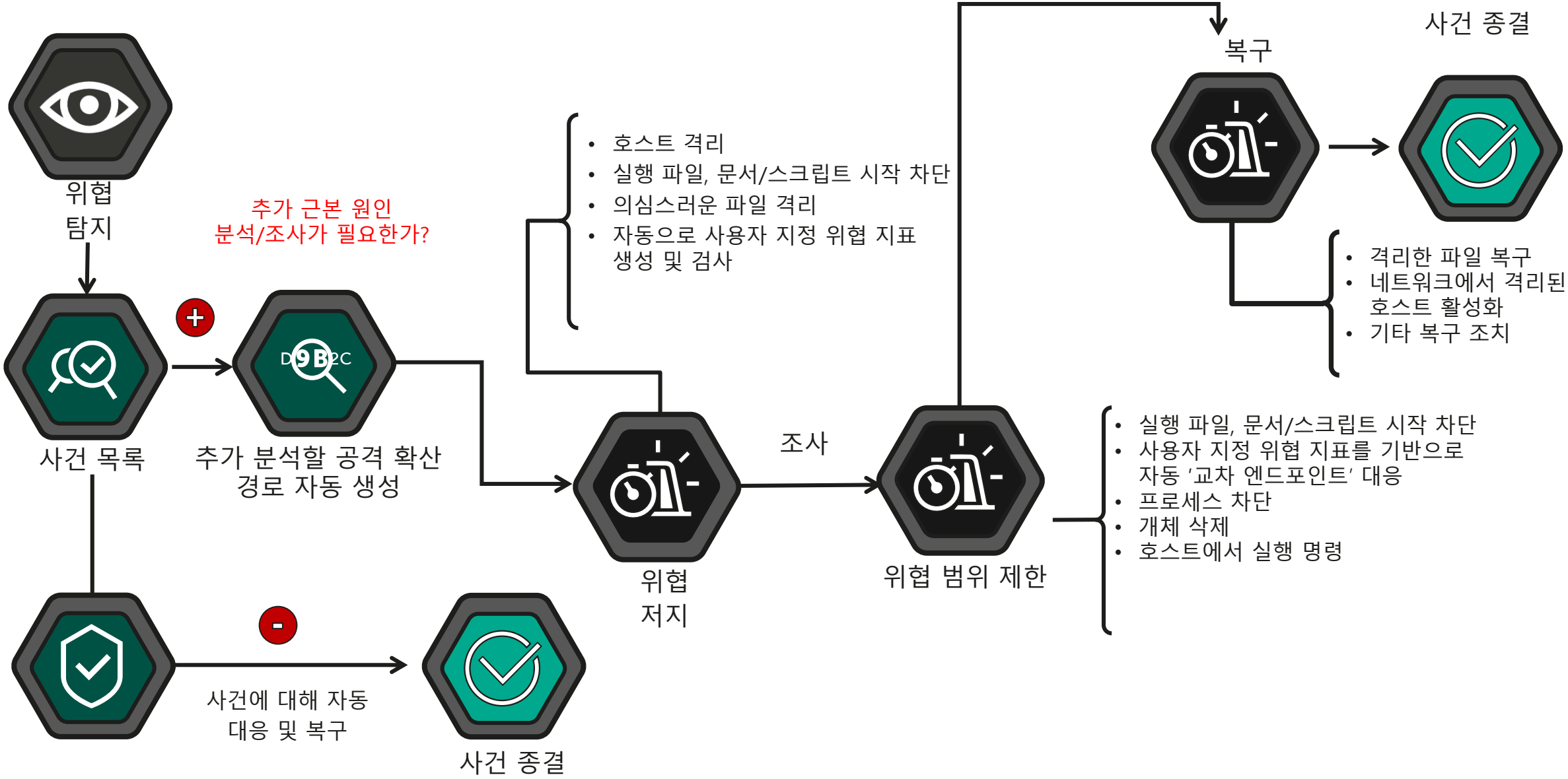
- URL
- 참조 페이지
- 사용자 에이전트
- 요청 유형(GET/POST)

Autorun 탐지

- 탐지된 개체 유형(서비스 이미지 경로, 레지스트리 키, WMI, lnk 등)
- 레지스트리 키 편집
- 서비스 설치 날짜 등

EDR Optimum 사용 사례

Kaspersky EDR Optimum의 사건 대응 프로세스



사용 사례 #1

합법적 프로세스의 메모리에서 악성 활동 탐지

IT 보안 전문가가 자동 생성된 사건 카드 데이터를 바탕으로 합법적 프로세스에 악성 코드를 삽입한 상위 프로세스를 확인

- 파일에서 악성 코드를 실행하지 못하도록 제품 인터페이스에서 바로 신속하게 차단
- 유사 감염 호스트를 모두 찾고 전체 감염 벡터를 원 클릭으로 차단

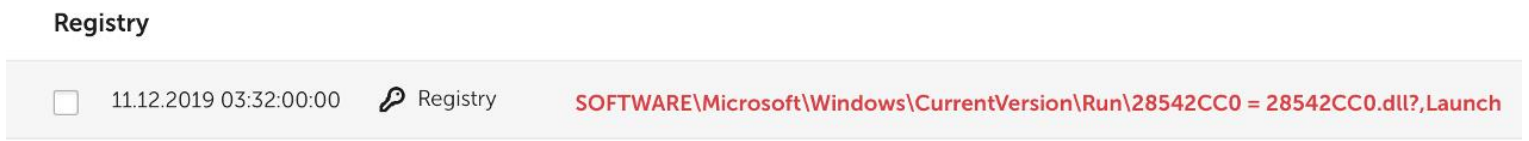
사용 사례 #2

KES/샌드박스를 통해 악성 파일이 탐지된 경우

이전 활동은 없었는가? 사건 범위는 어느 정도인가?

관련된 모든 호스트 활동은 에이전트를 통해 이미 기록되었으며 Kaspersky Security Center의 사건 카드에서 확인 가능하며 그 예는 다음과 같습니다.

- EDR-O를 사용하여 해당 악성 코드가 신뢰할 수 있는 그룹(예: 도메인 관리자)에서 확산된 것을 발견할 수 있음
- 시스템 바이너리 및 라이브러리를 활용하는 등, '활동이 눈에 띄지 않는' 기법을 사용했음
- 일부 모듈이 Autorun으로 추가되었거나 인코딩된 페이로드가 상주하도록 레지스트리에 저장되었음



즉, 호스트 또는 네트워크까지도 **감염된 상태**

위협 지표를 생성하여 네트워크 호스트 검사

탐지된 악성 코드 실행 방지

검사 시작

호스트 격리 (일부 경우)

사용 사례 #3

*.hta 파일로 연결되는 URL이 포함된 피싱 이메일을 받아 열어봄

HTA 파일을 열어 인터넷에서 애플리케이션을 다운로드하는 VBA/Powershell 스크립트를 실행

랜섬웨어(탐지 및 차단됨)

C&C 구성요소에 대한 상주 기능 추가

C&C 구성요소

(탐지되지 않음 – 확인 가능한 시그니처/평판이 없음)

C2 서버

x.x.x.x

감염의 직접적 원인 파악

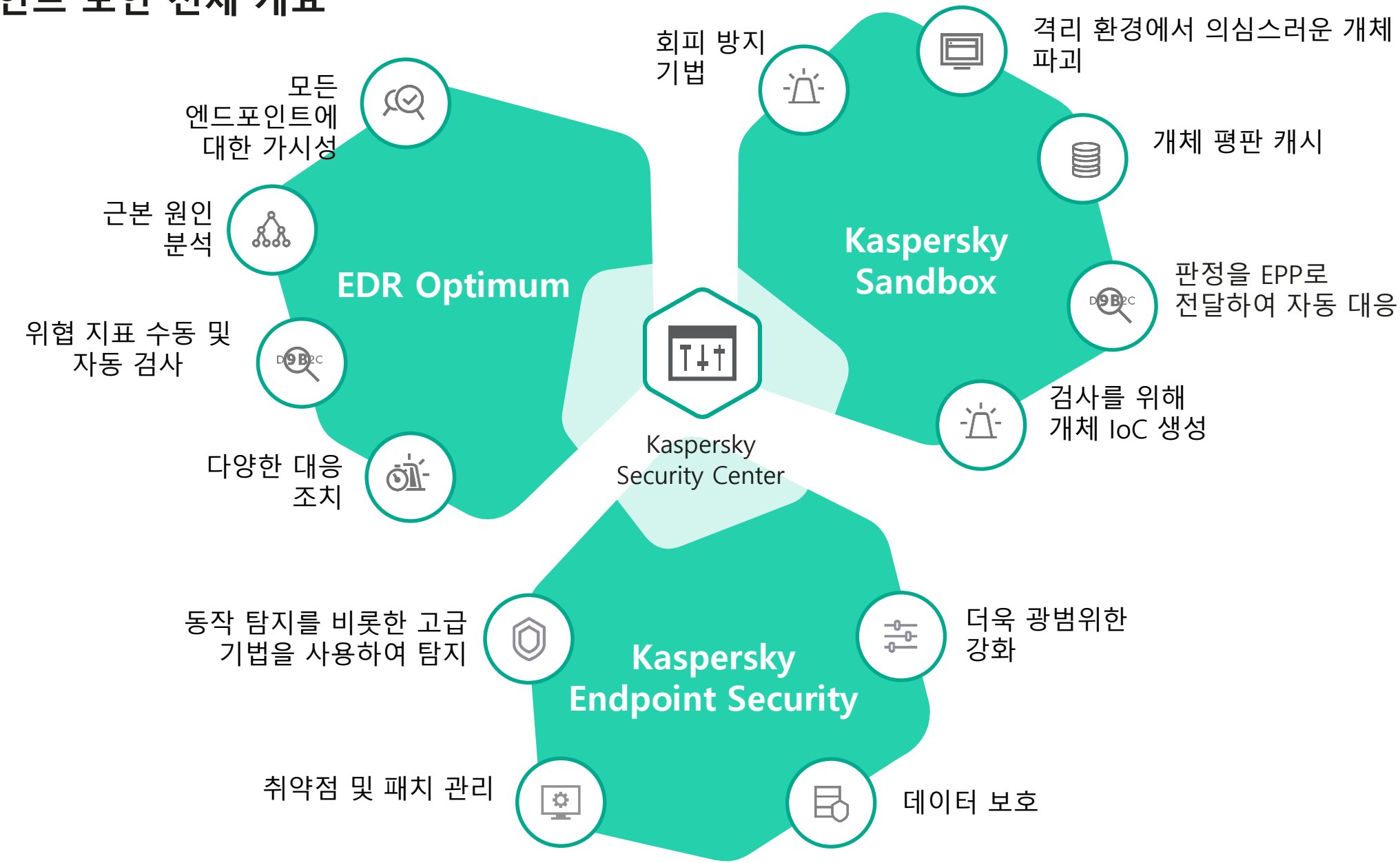
공격의 다른 부분 확인

- 파일/프로세스 실행
- 원격지 C2와의 커뮤니케이션

- 위협 지표를 생성하고 워크스테이션의 공격 징후 검사
- 호스트 격리/실행 방지/파일 삭제 등

카스퍼스키 통합 엔드포인트 보안 구축 제안

엔드포인트 보안 전체 개요



메인스트림 시장을 위한 통합 구축 제안

- 행동 탐지 및 머신 러닝
- 적응형 이상 행위 제어
- 익스플로잇 및 파일리스 공격 방지
- 취약점 평가 및 패치 관리
- 복원 엔진

- 엔드포인트 전체에 대한 가시성
- 자동으로 근본 원인 분석
- 위협 증거 탐색
- 심층 동적 분석 (자동 샌드박스 탐지)
- 다양한 대응 조치

자동 기능 극대화

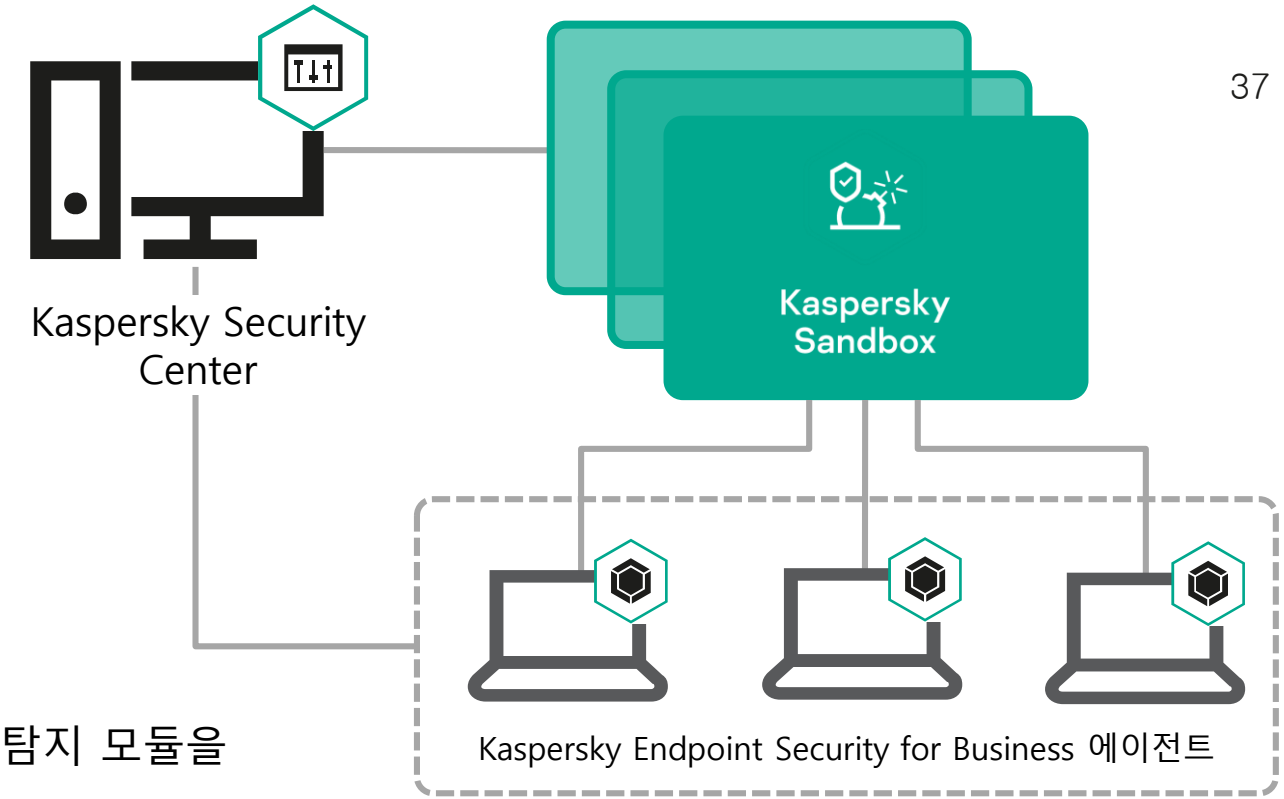
운영 간소화

Kaspersky Sandbox의 고급 동작 분석 활용

Kaspersky Sandbox

Kaspersky Endpoint Security for Business의 기능을 확대하여 복잡한 위협을 파악 및 차단:

- 지금까지 알려지지 않은 악성 코드
- 신종 바이러스 및 랜섬웨어
- 제로데이 익스플로잇 등

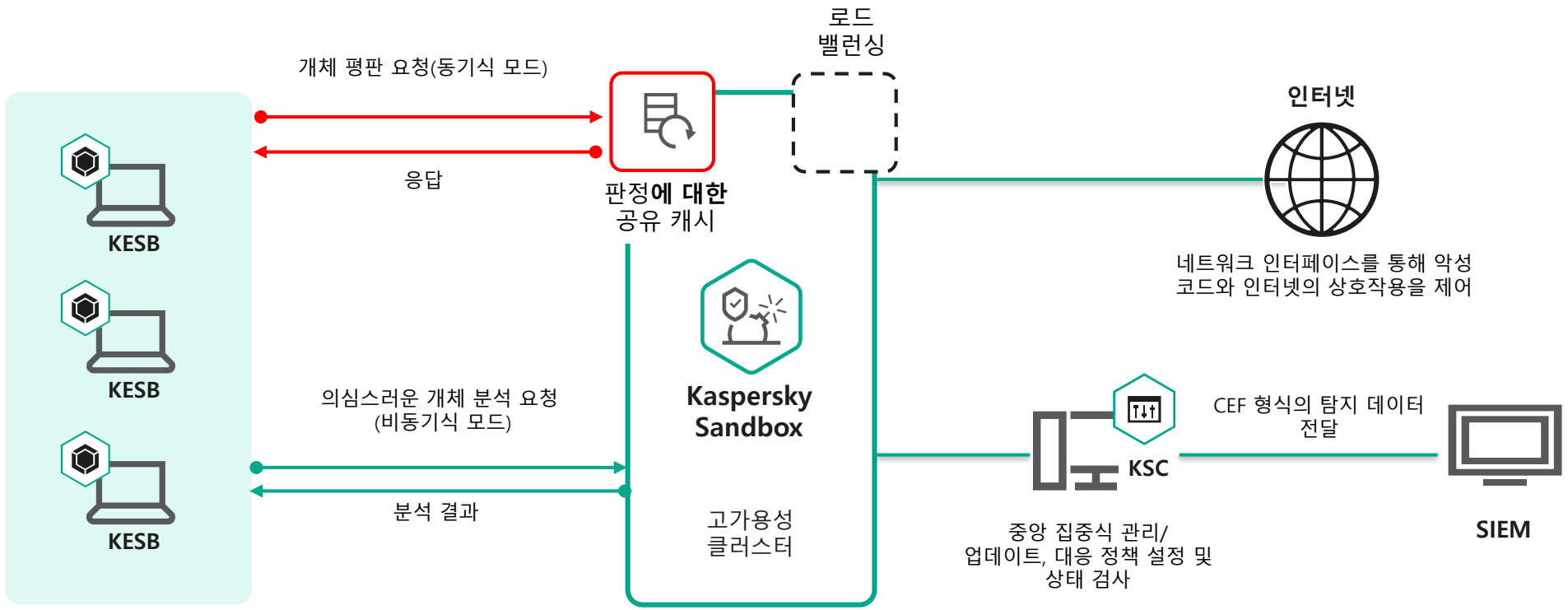


사용 사례

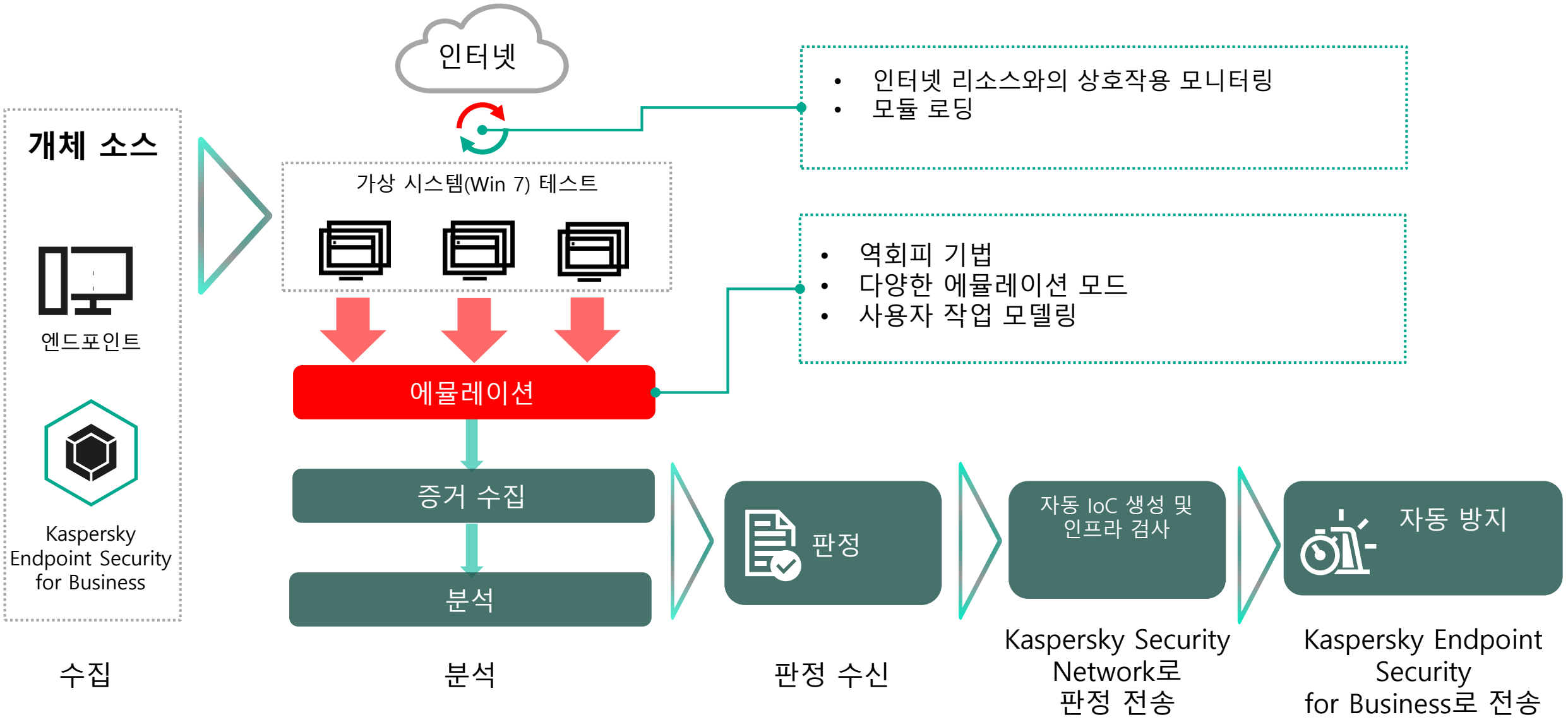
- Kaspersky Endpoint Security for Business의 행동 탐지 모듈을 종료한 상태에서도 고부하 터미널 서버를 보호
- Kaspersky Security Network와 연동 안 된 엔드포인트 보호
- API를 통해 고객 인프라의 타사 애플리케이션과 통합 가능

리소스 제약으로 인해
엔드포인트에서 수행할 수 없는 동작 기반 탐지에 대한 추가 탐지 계층

Kaspersky Sandbox 운영 체계



Kaspersky Sandbox 비동기식 모드



탐지율 증가

탐지율(DR) 증가의 이유는 다양합니다.

악성 코드 테스트
해킹 조직은 악성 코드를 실제로 유포하기 전에 반드시 신종 샘플을 테스트합니다.

눈에 띄지 않음
일부 샘플의 경우 보안 솔루션이 존재하는 것으로 판단되면 활동하지 않습니다. 이로 인해 AV 테스트를 거쳐도 악성 코드가 보호되지 않은 워크스테이션으로 전달될 수 있는 것입니다.

팜(farm)
해킹 조직은 팜을 갖추어 알려진 엔드포인트 보안 솔루션에 대한 위협 효과를 테스트하는 경우가 많습니다. 하지만 샌드박스와 같은 전용 도구는 보유하고 있지 않습니다.

격리된 환경

샌드박스 내의 활동과 증거는
샘플 실행과 관련 있으며
분석 가능합니다.

활동

모든 프로세스의 활동을 이용하여 간편하게 탐지할 수 있습니다. 엔드포인트 솔루션은 사용자의 작업 중단이 발생하지 않도록 주의 깊게 처리하는 신뢰할 수 있는 도구를 활용해야 합니다.

트래픽

샌드박스 실행 중 수집된 모든 트래픽은(발신 트래픽도 마찬가지) 종합적 Snort/Suricata 규칙을 사용하여 검사를 거칩니다.
샌드박스에서는 엔드포인트 보안 솔루션과 달리 트래픽을 자유롭게 해독할 수 있습니다.

덤프, 드롭/다운로드된 파일

메모리 덤프는 검사 가능합니다.
엔드포인트에서의 덤프 발생은 성능 문제가 원인일 수 있습니다. 드롭 및 다운로드는 원본 샘플과 밀접한 관계가 있습니다.

2019년 수상 경력 및 평가

Kaspersky Endpoint Security
NSS Labs: Advanced Endpoint Protection v.3 추천(Recommended) 등급

파일리스 위협 보호 테스트 최고 평가 달성

SE Labs AAA 어워드

SE Labs는 다양한 엔드포인트 보안 제품을 대상으로 발달된 기법을 사용하는 표적형 공격에 대한 테스트를 수행했습니다.
카스퍼스키가 실시간 탐지 및/또는 보호에 가장 효과적인 제품으로 인정받았습니다.

카스퍼스키는 MITRE 라운드 2 평가에 참여했습니다(APT29, Cozy Bear, The Dukes).

Radicati MQ 최우수 제품 선정: 엔드포인트 보안 부문

Forrester Wave 리더 그룹 선정: 엔드포인트 보안 제품

Gartner MQ EPP 부문 비저너리 그룹 선정

감사합니다.

Kaspersky Korea
www.kaspersky.co.kr
sales@kaspersky.co.kr

kaspersky