kaspersky

엔드포인트
보안을 위한
통합 솔루션

EDR Optimum
차세대 통합
엔드포인트 보안

kaspersky

자세한 내용은 kaspersky.co.kr 을 참조하십시오.
#bringonthefuture

소개

기업 규모, 위치, 분야에 관계없이 이제 모든 기업에게 사이버 공격은 발생 가능성 유무가 아니라 언제 발생할지를 걱정해야 할 문제가 되었습니다. 공격에 대해 안전하다고 장담하는 기업은 없을 것입니다.

그럼에도 불구하고 많은 기업이 현재의 위협과 보안 환경을 효과적으로 탐색할 수 있는 시간이나 리소스를 갖추지 못했을 뿐 아니라 보안에 대한 의지까지 부족한 경우가 많습니다.

정보 보안 분석가 자체도 수가 부족하지만 대부분의 인력이 이미 과중한 업무에 시달리고 있습니다. 이들은 신입 직원 및 직원 장비 지원, 신규 법률 및 규제 준수 문제 해결, 최신 위협 조사 등을 모두 처리한 후에야 실제로 주요 업무인 기업 보안 업무를 시작할 수 있습니다.

업무 시간 동안 신종 위협이나 흔치 않은 위협을 사냥하고 이에 대응하는 데에만 집중할 수 있는 보안 전문가는 거의 없다고 해도 무방합니다.

그래서 사이버 보안 제공업체와 보안 제품 및 솔루션이 필요합니다. 카스퍼스키의 역할은 일반적으로 비용이 많이 들고 확보하기 힘든 전문 지식을 시간 및 금전 등의 리소스 측면에서 최대한 낮은 비용으로 제공하여 각 기업이 인프라를 충분히 보호하고 사용자의 안전을 유지할 수 있도록 지원하는 것입니다.

문제점

먼저 오늘날의 IT 및 IT 보안 매니저가 겪고 있는 문제들을 살펴보겠습니다.

지능형 공격 또는 표적형 공격의 위협 증가

표적형 공격을 비롯한 복잡한 위협은 심각한 문제이며 발생 횟수도 증가하고 있습니다. 사이버 범죄 도구의 비용이 크게 낮아지고 손쉽게 확보할 수 있게 되면서 이제 기본적으로 컴퓨터만 있으면 누구나 지능형 공격을 시작할 수 있습니다. 즉, 스스로 지능형 위협의 '레이더망에서 벗어나' 있다고 생각하던 기업도 상황이 바뀌었다는 사실을 뼈저리게 느끼게 될 것입니다.

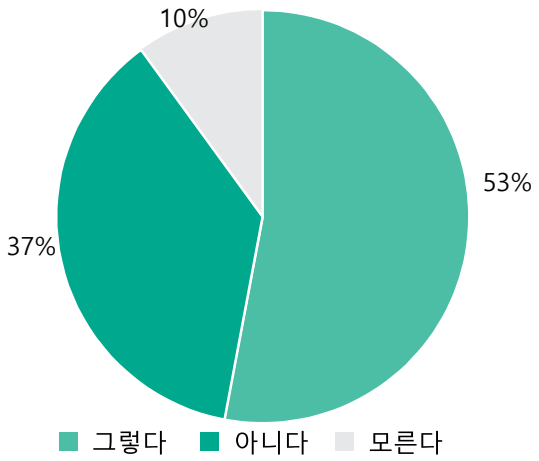
하지만 코모디티(범용) 위협도 양적 규모가 엄청나기 때문에 여전히 큰 골칫거리입니다.

사이버 위협의 대부분은 엔드포인트를 통해 침투하거나 엔드포인트에서 시작되도록 설계되어 있으며, 두 경우 모두 해당되는 위협도 있습니다.

따라서 자산을 보호하기 위한 방법 중 하나는 일단 엔드포인트를 보호하는 것입니다.

SANS Institute 의 연구에 따르면 [2] 전체 기업의 53%가 자사 엔드포인트가 침해된 사실을 알고 있으며 10%는 침해 여부를 확신하지 못했습니다.

엔드포인트 침해 발생률



전체 기업의 **91%**[1]가 한 해 동안 1 회 이상의 공격을 경험했습니다.

전체 기업의 **10 분의 1**[1]이 같은 기간 동안 표적형 공격을 받았습니다(인지된 공격에 한하여).

- 전체 기업의 **53%**[2]가 자사 엔드포인트가 침해된 사실을 알고 있습니다.
- 전체 기업의 **30%**[1]는 여전히 안티 맬웨어 소프트웨어가 충분히 구현되어 있지 않습니다.
- 침해 사건의 **56%**[3]는 여러 달 이상 지나서야 침해 사실을 알게 됩니다.

전체 기업의 **3 분의 2**[4]가 정보 보안 인력 부족 현상을 겪고 있습니다.

2021 년까지 **350 만**[5] 개의 사이버 보안 일자리가 충원되지 못한 상태일 것으로 예상됩니다.

1 The Kaspersky Lab Global IT Risk Report(카스퍼스키, 2019 년)

2 Next-Gen Endpoint Risks and Protections(SANS Institute, 2017 년)

3 2019 Data Breach Investigations Report(Verizon, 2019 년)

4 Cybersecurity workforce study((ISC)², 2019 년

5 Official Annual Cybersecurity Jobs Report (Cybersecurity Ventures, 2019 년)

사용자 실수

안타깝지만 공격받은 엔드포인트 중 대부분은 기업 인프라에서 가장 취약한 구성요소, 즉 '사용자'가 관련되어 있습니다. 직원이 개인 장치에서 원격으로 기업 데이터에 접근하는 일이 많아지고 온라인 이용 경험이 쌓이다 보면 나쁜 습관이 생길 수도 있고 스스로를 과신하게 될 수도 있습니다. 이러한 사용자 역시 다른 모든 구성요소와 마찬가지로 보호받아야 하는 대상입니다.

따라서 보안 전문가에게는 오늘날의 복잡한 IT 환경에서 위험한 사용자 행동을 탐지 및 방지하는 업무가 추가되는 셈입니다.

또한 IT 전문가도 결국은 사람이기에 실수할 수 있습니다. 이러한 실수로 인해 패치가 제때 적용되지 않은 기업 장치 또는 개인 장치의 취약점을 통한 공격이 발생하기도 합니다.

리소스 부족

IT 전문가가 해야 할 일이 많다는 것은 분명합니다.

기업 규모가 아무리 작아도 매일 검토, 분석, 대응해야 할 보안 이벤트의 수가 끊임없이 늘어나므로 항상 시기를 놓치지 않고 효과적으로 처리하기는 어렵습니다. 사이버 범죄자도 기업들이 이런 부분에서 어려움을 겪고 있다는 사실을 알고 있으며 이를 적극적으로 이용합니다.

운 좋게 자금이 넉넉한 기업도 있지만 전 세계적으로 숙련된 사이버 보안 전문가가 부족한 실정입니다. 이미 오래된 문제지만 해마다 양성되는 전문가의 수를 생각해볼 때 조만간 해결될 문제도 아닙니다.

이러한 환경에서 보안 전문가가 만족하며 업무에 집중할 수 있도록 지원하는 것은 사실상 불가능할 뿐 아니라 단순히 기업에 붙잡아 두는 것조차 쉽지는 않습니다. 극도의 피로감도 큰 문제입니다. 특히 기술이 뛰어나고 큰 비용을 들여 교육받은 직원들이 하루 종일 일상적 작업의 처리에 매달리고 있을 경우 더욱 심각합니다.

뿐만 아니라 재정이나 프로세서 성능이 부족한 문제도 있습니다. 또한 처리 속도, 직원 생산성, 사용자 만족도, 예산 등에 영향을 미치지 않고 보안 성능을 최적화하는 데 필요한 그 밖의 모든 요소도 무시할 수 없습니다.

해결책

그렇다면 해결책은 과연 무엇일까요?

효과적인 보호

모든 것은 무엇보다도 **효과적인 엔드포인트 보안**에 달려 있습니다. 답은 간단합니다. 경고 발생 단계에 이르기 전에 엔드포인트 수준에서 위협을 차단하면 리소스 부담을 줄이고 공격이 이어질 위험을 완화할 수 있으며 비즈니스 운영도 원활하고 안전하게 지속할 수 있습니다.

이는 처리 시간의 대부분을 차지하는 코모디티 공격은 물론이고 공격 성공 가능성이 높고 매우 큰 피해가 발생하는 표적형 공격에도 모두 유효한 방법입니다. 카스퍼스키에서 권장하는 접근 방식은 코모디티 위협에 대한 강력한 기본 보호 기능인 **다계층 엔드포인트 방어** 체계를 구축하고 더욱 복잡한 최신 위협을 막아주는 계층화된 다각적 보안 기능을 결합하여 사용하는 것입니다.

EDR(Endpoint Detection and Response)은 그 다음으로 중요한 보안 계층을 제공합니다. EPP(Endpoint Protection Platform)을 통해 1 차 확인 및 보호 기능을 갖춘다면, EDR 은 우수한 가시성과 심층 분석 옵션을 제공하므로 공격이 시작된 경로와 현재 진행 단계를 파악할 수 있습니다. EDR 은 탐지 기능 외에 선제적 대응 옵션도 제공하므로 발견된 위협을 빠르고 효율적으로 진압할 수 있습니다.

EDR 은 강력한 보호 기반이 구축되어 있어야 효과를 발휘합니다. EPP 솔루션에서 먼저 차단해주는 사건 수가 많을수록 EDR 솔루션에서 처리해야 할 분량이 적어져 사건에 더 많은 리소스를 집중 투입할 수 있습니다.

사용자 행동 관리

사용자의 입장에서 볼 때 실수를 방지하는 가장 좋은 방법은 물론 **애플리케이션, 웹, 매체 제어**를 통해 실수가 발생할 기회나 유혹을 원천차단하는 것입니다. 효과적인 제어란 비즈니스 제약을 유발하는 조치가 아닙니다. 시간 낭비로 이어질 수 있고 잠재적 위험이 도사리고 있는 오락성 웹사이트, 소셜 미디어 등을 차단하여 실제로 생산성을 높일 수 있는 조치입니다.

하지만 그러려면 사용자 교육이 매우 중요합니다. 적절한 **사이버 보안 인식 교육**을 시행하면 직원 행동에 지대한 영향을 미쳐 기업 문화가 바뀌고 기업 위험이 크게 낮아지며 IT 부서 업무 부담도 대폭 줄일 수 있습니다.

투자 수익

결국 어떤 방식이든 ROI 측면에서 금전적 타당성을 입증할 수 있어야 하며 보안 전문가의 전문 지식을 비롯하여 여러 리소스가 한정된 환경에서 현재는 물론 향후에도 운영이 가능해야 합니다.

자동화 및 간소화

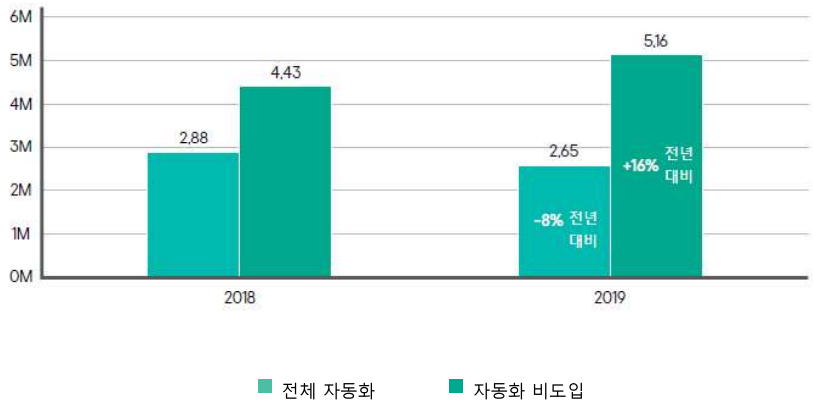
위협 규모가 점점 증가하고 업계 전반에 걸쳐 이러한 위협을 처리할 보안 전문가가 부족해지면서 **보안 작업 자동화**는 필수가 되었습니다. 이를 통해 보안 전문가의 귀중한 시간과 기술을 사람의 개입과 전문지식이 필요한 사건 처리에만 집중시킬 수 있어 결과적으로 업무 만족도가 높아지고 동기 부여가 강화됩니다.

또한 작업 자동화로 사용자 실수 발생 위험도 줄어듭니다. 한 예로 시스템 취약점 패치의 우선순위 지정 및 실행을 자동화하면 운영 인력이 직접 처리하는 것보다 훨씬 효과적일 것입니다.

간단한 구축과 효율적인 중앙집중식 **관리 콘솔**도 시간 및 리소스 절약에 도움이 되는 장점입니다. 작업마다 콘솔을 바꾸고 명령 키를 찾으면 시간이 걸리고 번거로울 뿐 아니라 관리상의 실수 및 누락이 발생할 가능성이 생깁니다.

보안 자동화를 도입하지 않은 기업은 위협 진압 비용이 16%[6] 증가했으나 자동화를 도입한 기업은 해당 비용이 8%[6] 감소했습니다.

비용
보안 자동화 수준에 따른 비용 비교
(M: 백만)



6 Cost of a Data Breach Report 2019(Ponemon Institute, 2019 년)

다계층 보안 관련 참고 사항

앞에서도 언급했지만 어떤 솔루션이든 지능형 공격과 표적형 공격을 포함하는 모든 유형의 사이버 위협 차단을 목표로 한다면 다계층 솔루션으로 구성해야 합니다.

기본적으로 솔루션은 엔드포인트 제어(웹, 애플리케이션 및 장치 차단 및 제한 기능), 강화된 안티 맬웨어 엔진 등의 **강력한 기본 엔드포인트 보호** 기능을 제공해야 합니다. 또한 자동 패치 관리 및 취약점 평가 기능도 갖추는 것이 좋습니다. 이를 통해 이러한 선별 분류 작업에 소모되는 IT 인력의 시간과 노력을 절약할 수 있습니다.

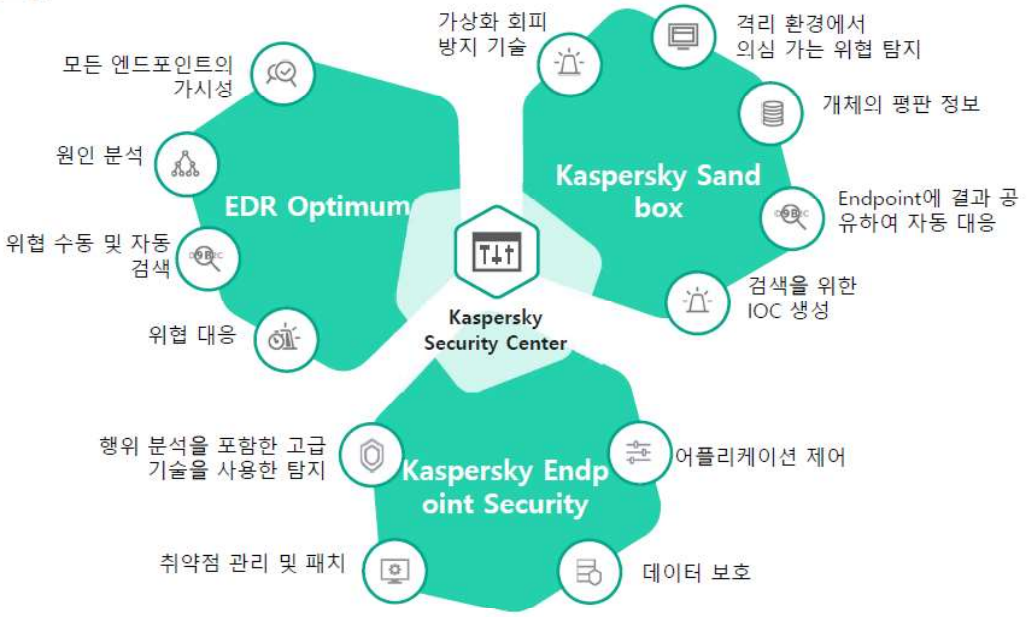
그러나 지능형 악성 코드 때문에 추가 보안 계층이 필요하다는 또 다른 문제가 발생합니다. 악성 코드는 아무리 정교한 엔드포인트 보안 메커니즘이라 해도 피할 수 있도록 특별히 설계되어 적절한 공격 개시 기회가 생길 때까지 숨어서 휴면 상태를 유지합니다. 해결책은 안전하고 제어된 환경에서 악성 코드가 스스로 모습을 드러내고 활성화되도록 하는 것입니다. 이런 경우 **샌드박스**를 이용합니다. 최근 일부 샌드박스의 경우에는 탐지한 위협에 대해 신속한 자동 대응 기능을 제공하기도 합니다.

또한 엔드포인트에서의 복잡한 동작 탐지는 **EDR** 의 주력 기능이기도 합니다. EPP 와 마찬가지로 EDR 도 다양한 도구의 자동화 및 시각화 기능을 완벽하게 함께 갖추어 필요한 경우 인력 개입을 지원해줄 수 있어야 합니다. 보안 분석가는 사건에 대한 근본 원인 분석을 수행하고 각종 위협을 수동으로 또는 자동 대응 옵션을 활용하여 시기 적절하게 대응할 수 있어야 합니다.

EPP, 샌드박스, EDR 기술을 함께 사용하면 코모디티 악성 코드를 빠르고 효율적으로 처리할 수 있을 뿐 아니라 사용자 실수 발생 가능성이 낮아지고 알려지지 않은 신종 위협, 제로데이 위협도 탐지 및 대응하므로 지능형 공격 또는 표적형 공격의 성공 위험을 줄일 수 있습니다.

이 모든 기능이 통합된 솔루션을 갖추면 다양한 도구 간에 해커와 공격자가 악용할 수 있는 빈틈도 사라집니다.

카스퍼스키
엔드포인트 보안



카스퍼스키 솔루션

Kaspersky Endpoint Security 은 엔드포인트 보호 및 제어 기능, 자동 샌드박스, EDR 로 구성되어 있는 고도로 자동화된 통합 솔루션이며 보완 옵션으로 사이버 보안 인식 교육 플랫폼이 마련되어 있습니다.

강력한 기본 엔드포인트 보호 기능

Kaspersky Endpoint Security for Business 는 매우 안정적인 솔루션으로 랜섬웨어, 파일리스 공격 등에 대한 보호 기능을 포함하는 대단히 강력한 EPP 를 제공하며 업계 최다 테스트 시행, 최다 수상 경력을 갖춘 안티 맬웨어 엔진을 활용하고 있습니다.

Kaspersky Endpoint Security for Business 는 다음과 같은 엔드포인트 보호 계층을 제공합니다.

- 수상 경력을 갖춘 안티 맬웨어 엔진
- 랜섬웨어 탐지 및 차단
- 동작 탐지 및 자동 롤백 - 파일리스 악성 코드, 관리자 계정 가로채기를 비롯한 지능형 위협의 파악 및 차단, 이미 수행된 변경 사항 역변경
- 모바일 위협 방어 및 EMM 통합
- IPS/HIPS
- 방화벽 및 OS 방화벽 관리
- Kaspersky Security Network 위협 인텔리전스
- 암호화 - OS 내장 암호화 관리 기능 포함
- 보안 어드바이저 - 최적화된 보안 설정의 수정 여부 모니터링
- 자동 취약점 및 패치 관리
- OS 및 타사 소프트웨어 설치
- SIEM 시스템 통합

세분화된 제어

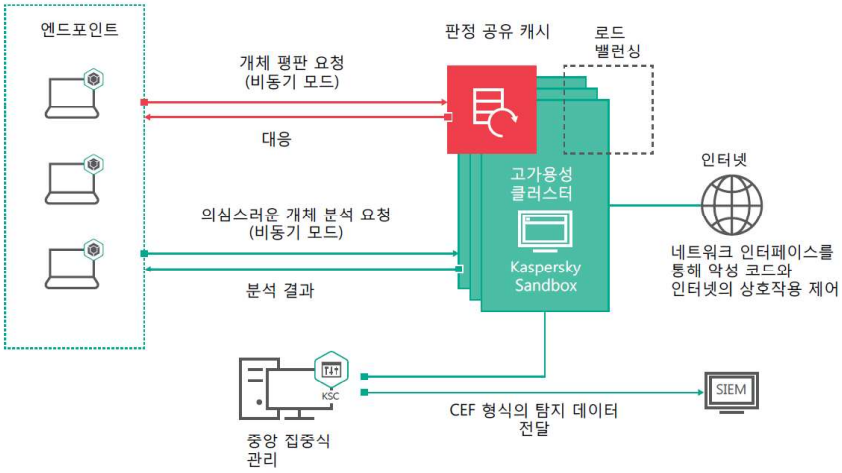
다음과 같은 제어 기능을 통해 시스템 강화 및 사용자 실수 완화

- 카테고리 기반 화이트리스트 작성 기능을 사용한 애플리케이션 제어
- 적응형 이상 제어 - 자동으로 보안 수준을 기업 내 모든 사용자에게 적절한 최고 수준으로 상향 조정
- 매체 제어 – 외부 장치 플러그인 제어 및 차단
- 웹 제어 – 잠재적 위험성 또는 시간 낭비 우려가 있거나 부적절한 사이트 접근 차단 또는 제한

Kaspersky Endpoint Security for Business 에 대해 자세한 내용은 다음을 참조해주시기 바랍니다.
https://www.kaspersky.com/small-to-medium-business-security/endpoint-advanced

자동 샌드박스

Kaspersky Sandbox 는 엔드포인트 보호 기능을 피할 수 있도록 설계된 위협을 자동으로 탐지하고 대응하므로 사람의 개입이 필요하지 않습니다.



Kaspersky Sandbox 워크플로

검사할 개체는 워크스테이션을 시뮬레이션하는 격리된 가상 시스템에서 클러스터형 샌드박스 서버를 통해 실행됩니다.

샌드박스는 데이터에 악성 동작 및 의심스러운 동작이 나타나는지 분석하여 검사를 요청한 엔드포인트 에이전트와 작업 캐시에 판정을 전달하므로 검사한 개체에 관련된 정보를 다른 호스트에서 다시 분석하지 않고 신속하게 검색할 수 있습니다.

악성 파일이 탐지되면 침해 지표(IoC)를 활용하여 자동 복원 작업을 시작할 수 있고 이를 통해 네트워크 내의 다른 모든 컴퓨터에서 해당 파일을 삭제합니다.

Kaspersky Sandbox 에는 다음과 같은 기법이 사용됩니다.

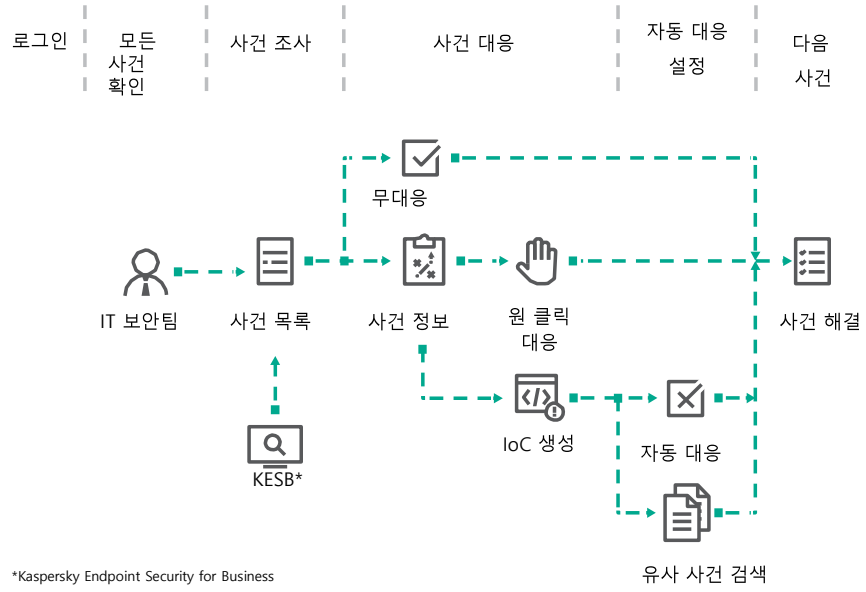
- 인터넷 리소스와의 상호작용 모니터링
- 모듈 로딩
- 동기화 및 비동기 검사 모드
- 역회피 기법
- 다양한 에뮬레이션 모드 적용
- 사용자 작업 모델링
- 자동 IoC 생성 및 인프라 검사
- 자동 방지

Kaspersky Sandbox 에 대해 자세한 내용은 다음을 참조해주시기 바랍니다.
https://www.kaspersky.com/enterprise-security/malware-sandbox

최적화된 EDR

Kaspersky EDR Optimum 은 엔드포인트 수준에서 발생하는 지능형 위협에 대해 자동 및 수동 분석과 대응 기능을 제공합니다.

비정상적 사용자 행동의 식별이 가능하여 모호한 위협, 특히 파일리스 위협이 일반적 동작을 모방하려 할 경우 자동으로 탐지하고 복원합니다. 또한 시각적 정보와 근본 원인 분석 수행 기능을 갖추고 있어 신속한 대응 및 무력화가 가능합니다.



Kaspersky EDR Optimum 워크플로

Kaspersky EDR Optimum 은 Kaspersky Endpoint Security 솔루션의 일부로 실행되며 다양한 기법을 사용하여 공격을 탐지하고 다음과 같은 흔적을 포함하여 공격 킬 체인에서 이를 시각화할 수 있습니다.

- 프로세스 인젝션
- 파일 드롭
- 레지스트리 키 수정
- 연결
- 사용자 행동 이상 징후

위협 탐지 후 대응 옵션은 다음과 같습니다.

- 호스트 격리
- 호스트 검사 시작
- 파일 삭제(격리)
- 프로세스 종료(Kill)
- 프로세스 실행 방지

Kaspersky EDR Optimum 은 IoC 가져오기 및 생성, 심층 검사 시작, 사건 대응 등을 포함하는 고도의 자동 기능과 원 클릭 수동 대응 옵션을 결합한 솔루션입니다.

Kaspersky EDR Optimum 에 대해 자세한 내용은 다음을 참조해주시기 바랍니다.
http://www.kaspersky.com/enterprise-security/edr-security-software-solution

관리 및 운영

카스퍼스키 솔루션의 모든 구성요소는 단일 코드베이스에서 사내 구축되고 동일한 단일 콘솔을 통해 관리하는 방식이며 동일한 다목적 엔드포인트 에이전트를 활용합니다. 따라서 일상적 관리가 중앙 집중식으로 이루어지며 간단하고 효율적입니다.

Forrester 의 분석에 따르면 [7] 보안 솔루션 구축 시 사용자에게 지장이 발생하지 않거나 극히 적어야 한다는 점이 대다수 기업의 주요 요구사항이라고 합니다. 그리고 이러한 원칙은 Kaspersky Endpoint Security 의 핵심이기도 합니다.