Stay ahead of your adversaries

Kaspersky Threat Intelligence

kaspersky BRING ON THE FUTURE

Kaspersky Threat Intelligence

Kaspersky의 보안 인텔리전스는 세계 최고의 연구진과 분석가 팀이 제공하는 인텔리전스에 대한 액세스를 제공하여 사이버 위협을 완화할 수 있도록 합니다.

Kaspersky는 사이버 보안의 모든 측면에 관한 지식, 경험, 깊이 있는 인텔리전스를 보유하고 있으며, 인터폴과 같은 세계 최고의 법 집행기관 및 정부기관, 우수한 CERT의 든든한 파트너로 활동하고 있습니다. Kaspersky Threat Intelligence를 통해 전술, 운영, 전략 차원의 보안 인텔리전스를 즉시 이용할 수 있습니다.

Kaspersky Threat Intelligence는 당사의 전문가들이 인텔리전스 소스, 위협 데이터 피드, 내부 연구자료를 종합한 글로벌 위협 현황에 대해 전반적으로 살펴볼 수 있습니다.

Kaspersky Threat Intelligence가 힘이 되어 드립니다

위협의 선제 인식 및 예방

Kaspersky Threat Intelligence는 고객이 선제 조치로 시스템을 보호할 수 있도록 위협 및 취약성에 대한 최신 정보를 제공합니다.

디지털 발자국에 대한 시야 확보

Kaspersky Threat Intelligence는 공격 및 침해에 취약할 수 있는 자산을 포함하여, 디지털 발자국에 대한 포괄적인 시야를 제공합니다.

위협 탐지 역량 강화

Kaspersky Threat Intelligence가 제공하는 최신 위협 인텔리전스로 현재 사용하는 보안 솔루션을 강화하고, 정교한 위협 탐지 및 방지 역량도 키울 수 있습니다.

인시던트 대응 개선

Kaspersky Threat Intelligence는 인시던트에 신속하고 효과적으로 대응할 수 있도록, 새로운 위협과 침해 지표에 관한 정보를 실시간으로 제공합니다.

규정 및 기준 준수

모든 기업체는 업계의 다양한 규정과 기준을 준수해야 합니다. Kaspersky Threat Intelligence는 이러한 요구 사항의 준수를 지원합니다.

내부 전문성 강화

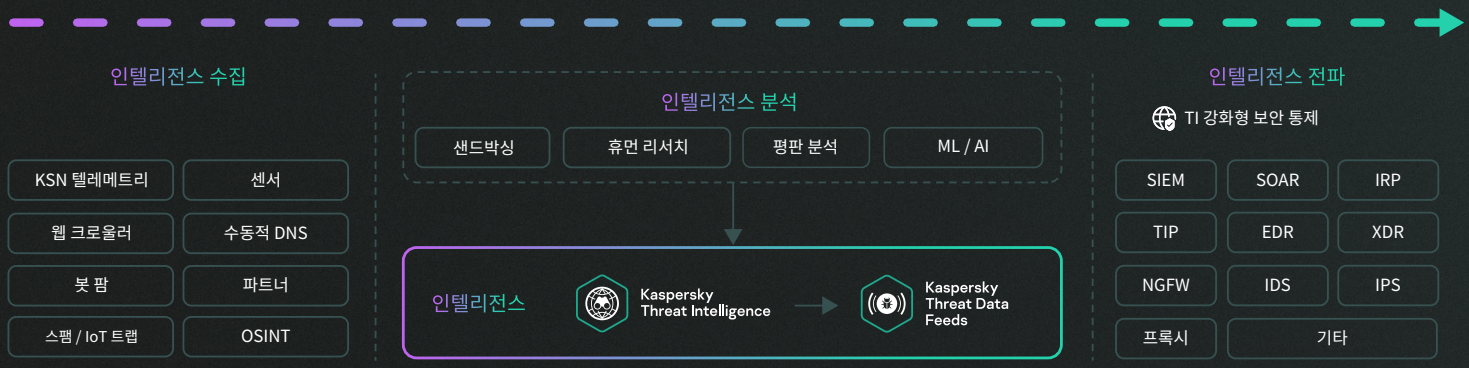
업계 최고 수준의 경험과 실력을 갖춘 Kaspersky의 전문가들이 고객의 정보 보안팀에 폭넓은 지식과 전문성을 제공합니다.

Kaspersky Threat Data Feeds

사이버 공격은 매일같이 일어나며, 사용자의 보안을 노리는 사이버 위협의 빈도, 복잡성, 난독화도 나날이 심화하고 있습니다. 공격자들은 복잡한 침입용 킬체인, 캠페인, 커스텀 TTPs(Tactics, Techniques and Procedures)를 활용하여 대상의 사업을 방해하거나 대상의 고객에게 피해를 줍니다. 이를 효과적으로 막으려면 위협 인텔리전스 기반의 새로운 접근법이 필요합니다.

보안 팀은 의심스럽거나 위험한 IP, URL, 파일 해시에 대한 정보가 담긴 최신 위협 인텔리전스를 SIEM, SOAR, 보안 인텔리전스 플랫폼과 같은 현행 보안 시스템에 연계함으로써 최초 경고 분류 체계를 자동화할 수 있으며, 이를 통해 분류 전문가들에게 충분한 컨텍스트를 제공하여 조사가 필요하거나 인시던트 대응팀에게 에스컬레이션하여 추가 조사나 대응을 진행해야 하는 경고 항목을 즉시 식별할 수 있습니다.

Kaspersky Threat Data Feed가 실시간으로 전송하는 위협 인텔리전스 정보를 통해 사이버 위협으로부터 네트워크와 시스템을 보호할 수 있습니다. 데이터 피드는 알려진 악성코드, 피싱 웹사이트, 최신화된 보안 취약점 및 익스플로잇, 기타 사이버 위협의 유형 등, 악성 트래픽 차단, 보안 소프트웨어 업데이트, 사이버 공격 방지 조치 수행에 도움이 되는 정보를 포함합니다.



컨텍스트 데이터

각 데이터 피드의 모든 기록은 실행 가능한 컨텍스트(위협의 이름, 타임스탬프, 지리적 위치, 감염된 웹 리소스의 IP주소를 변환된 IP 주소, 해시, 인기도 등)가 뒷받침합니다. 컨텍스트 데이터는 '더 큰 그림'을 볼 수 있게 해주어, 데이터의 폭넓은 활용을 가능하게 합니다. 이러한 데이터를 컨텍스트에 접목하면 '누가, 무엇을, 어디서, 언제'에 관한 정보를 더 쉽게 얻을 수 있어, 빠른 판단과 대응을 할 수 있습니다.

절차

1

Kaspersky Security Network, 자체 크로울러, 봇넷 위협 모니터링 서비스(봇넷 및 그 타겟을 24시간 추적), 스팸 트랩뿐만 아니라 연구기관, 파트너 등 신뢰할 수 있는 출처를 통해 데이터를 수집합니다.

2

수집된 모든 정보는 샌드박싱, 통계 및 휴리스틱 분석, 유사성 도구, 행동 프로파일링 및 전문가 분석 등 다양한 전처리 방법을 사용하여 실시간으로 신중하게 확인 및 정제됩니다.

3

데이터 피드를 활용하여 경고 또는 인시던트에 관한 위협 정보를 수집하고 자세한 내용을 파악할 수 있습니다. 또한 '누가? 무엇을? 어디서? 왜?'에 관한 답을 찾고 사이버 공격의 출처를 식별하여 신속한 결정을 내림으로써, 복잡한 위협으로부터 기업을 보호할 수 있습니다.

Kaspersky가 제공하는 피드 항목은 위협의 신속한 확인 및 우선순위 지정에 도움이 되는 컨텍스트 데이터를 포함합니다.

- 위협 이름
- 악성 웹 리소스의 IP 주소 및 도메인 이름
- 악성 파일의 해시
- 취약 개체 및 유출된 개체
- MITRE ATT&CK 분류에 따른 공격의 전술, 기술, 절차
- 타임스탬프
- 지리적 위치
- 인기도 등

Kaspersky Threat Data Feeds의 장점

더 강력하고 빠른 인시던트 대응 및 포렌식 역량 구축

이를 위해 초기 분류 프로세스를 자동화하고 보안 분석가에게 충분한 컨텍스트를 제공하여, 앞으로 조사가 필요하거나 인시던트 대응팀에게 에스컬레이션하여 추가 조사나 대응을 진행해야 하는 경고 항목을 즉시 식별할 수 있습니다.

보안 솔루션 강화

꾸준히 업데이트되는 침해 지표(IOC)와 실행 가능한 컨텍스트를 통해 사이버 공격에 대한 인사이트를 얻어 공격자의 의도, 역량, 목표에 대한 이해를 높이고, SIEM, 방화벽, IPS/IDS, 보안 프록시, DNS 솔루션, Anti-APT 등의 보안 솔루션을 강화할 수 있습니다. 주요 SIEM(ArcSight, IBM QRadar, MS Sentinel, Splunk 등) 및 TI 플랫폼을 완벽하게 지원합니다.

민감한 자산 및 지적 재산의 유출 방지

감염된 컴퓨터는 조직 외부로 자산을 유출할 수 있습니다. 감염된 자산을 빠르게 탐지하여 브랜드 평판을 보호하고 경쟁 우위를 유지하며 비즈니스 기회를 확보할 수 있습니다.

MSSP 비즈니스 성장

고객에게 프리미엄 서비스의 형태로 업계 최고의 위협 인텔리전스를 제공할 수 있습니다. CERT로서의 사이버 위협 탐지 및 식별 역량을 강화하고 확장할 수 있습니다.

Kaspersky CyberTrace

위협 데이터 피드와 사용 가능한 위협 인텔리전스 소스가 꾸준히 증가하며, 기업 입장에서 중요한 정보가 무엇인지 직접 판단하기가 어려워지고 있습니다. 또한, 위협 인텔리전스는 형식이 다양한 데다 대량의 침해 지표(IoC)를 포함하므로 SIEM 및 기타 네트워크 보안 제어가 이를 소화하기 어렵습니다.

전산화된 최신 위협 인텔리전스를 SIEM 시스템, 보안 운영 센터와 같은 현행 보안 시스템과 연계함으로써 최초 경고 분류 체계를 자동화할 수 있으며, 분류 전문가들에게 충분한 컨텍스트를 제공하여 조사가 필요하거나 인시던트 대응팀에게 에스컬레이션하여 추가 조사나 대응을 진행해야 하는 경고 항목을 즉시 식별할 수 있습니다.

Kaspersky CyberTrace는 위협 데이터 피드를 SIEM 솔루션과 매끄럽게 통합하여, 보안 담당자들이 기존 보안 운영 워크플로의 위협 인텔리전스를 더 효과적으로 활용할 수 있게 해주는 위협 인텔리전스 플랫폼입니다. JSON, STIX, XML 및 CSV 형식의 모든 위협 인텔리전스 피드(Kaspersky, 기타 공급업체, OSINT, 자체 고객 피드 등)와 통합할 수 있으며 수많은 SIEM 솔루션 및 로그 소스를 대상으로 원활한 통합도 지원합니다.

도구

Kaspersky CyberTrace는 효과적인 위협 인텔리전스 운영에 필요한 도구를 제공합니다:

지표 데이터베이스는 완전한 텍스트 검색 및 고급 검색 쿼리 기능을 제공하며 컨텍스트를 포함한 모든 지표 필드에서 복잡한 검색을 지원합니다

피드 사용 통계를 이용해 통합 피드의 효율을 측정할 수 있으며, 피드 교차 매트릭스를 참고하여 가장 좋은 위협 인텔리전스 공급업체를 선택할 수 있습니다

IoC 태깅은 IoC 관리를 단순화합니다. 태그를 생성하고 가중치(중요도)를 지정한 다음, 이를 바탕으로 IoC에 태그를 수동 지정합니다. 이러한 태그와 가중치를 기준으로 IoC를 정렬하고 필터링할 수도 있습니다

연구 그래프는 CyberTrace에 저장된 데이터와 탐지 결과를 시각적으로 보여주므로, 위협 간의 공통점을 확인할 수 있습니다

지표 추출 기능을 통해 지표 세트를 정책 목록(차단 목록) 등의 보안 제어로 내보낼 수 있으며 위협 데이터를 Kaspersky CyberTrace 인스턴스 간이나 다른 TI 플랫폼과 공유

이력 상관관계 기능(레트로 스캔)은 최신 피드를 이용해 이전에 확인한 이벤트의 관찰 가능한 항목들을 분석하여, 이전에 발견되었던 위협을 찾아냅니다

멀티테넌시는 MSSP 및 대형 사업체의 사용 환경을 지원합니다

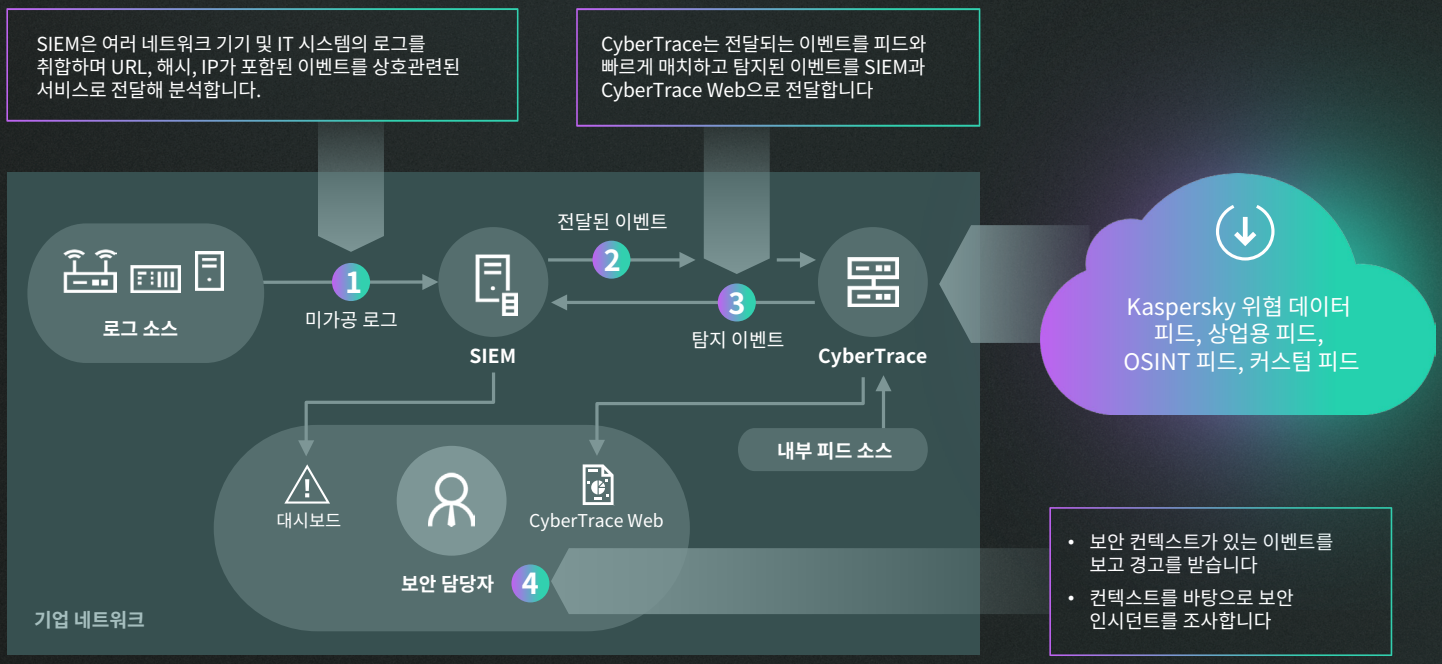
필터는 탐지 이벤트를 SIEM 솔루션으로 전송하여 분석가와 SIEM의 부담을 줄여줍니다

HTTP RestAPI로 위협 인텔리전스를 검색 및 관리할 수 있습니다

각 지표에 대한 자세한 정보가 있는 페이지에서 더 심층적인 분석도 확인할 수 있습니다. 각 페이지에는 위협 인텔리전스 공급업체 전체의 지표에 대한 모든 정보가 표시되므로(중복 제거), 분석가가 댓글을 통해 위협에 대해 논의하고 지표에 대한 내부 위협 인텔리전스도 추가할 수 있습니다

이 툴은 내장 프로세스를 사용해서 수신 데이터를 파싱 및 매칭하여 SIEM 워크로드를 크게 줄입니다. Kaspersky CyberTrace는 수신 로그와 이벤트를 파싱하고 결과 데이터를 피드에 신속하게 매칭하며 자체 위협 탐지 경고를 생성합니다.

아키텍처



Kaspersky CyberTrace와 Kaspersky Threat Data Feeds를 사용하면 고객의 보안 분석에 다음 효과를 더할 수 있습니다:

대량의 보안 경고를 효과적으로 정제하고 우선순위 지정

분류 및 초기 대응 절차 개선 및 가속

선제 인텔리전스 기반 방어 구축

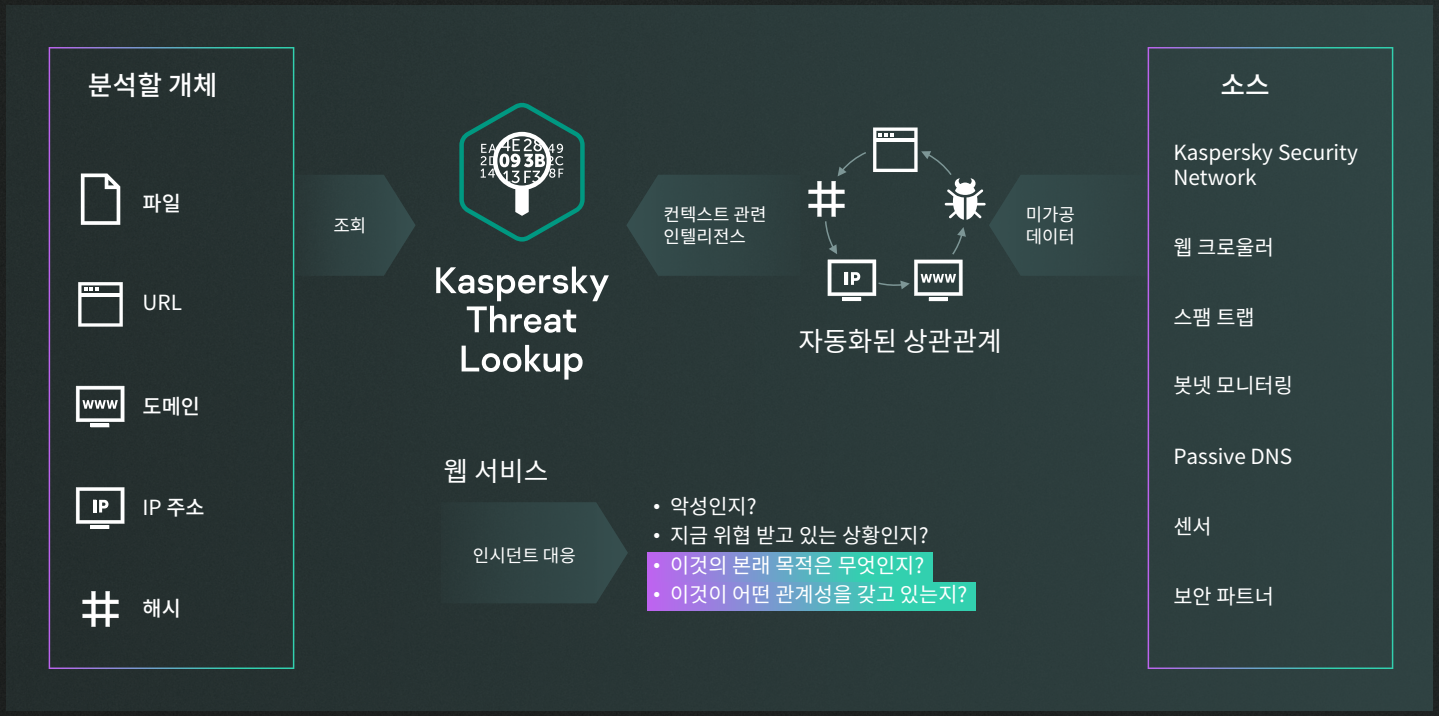
비즈니스에 치명적인 경고를 즉시 식별하고, IR 팀에 에스컬레이션할 항목을 더 신중하게 결정

Kaspersky Threat Lookup

사이버 범죄에는 경계가 없으며 기술적 수준도 빠르게 발전합니다. 사이버 범죄자들이 다크 웹 리소스를 사용함에 따라 사이버 공격도 점차 정교해지고 있으며, 사이버 보안 조치를 뚫는 새로운 수단들이 등장하면서 사이버 위협의 빈도와 복잡성, 난독화 역시 나날이 심화하고 있습니다. 사이버 범죄자들은 사업 방해나 자산 도용, 또는 고객에게 피해를 줄 목적으로 복잡한 킬 체인과 맞춤형 전술, 기술, 절차(TTPs)를 사용합니다.

Kaspersky Threat Lookup은 Kaspersky가 사이버 위협과 그 연관 관계에 관해 모은 모든 지식을 산출하여, 하나의 강력한 웹 서비스로 통합합니다. 보안 팀에 데이터를 최대한 많이 제공하여 사이버 공격을 미리 방지하는 것이 목표입니다. 이 플랫폼은 URL, 도메인, IP 주소, 파일 해시, 위협 이름, 통계/행동 데이터, WHOIS/DNS 데이터, 파일 속성, 지리적 위치 데이터, 다운로드 체인, 타임스탬프 등에 관한 최신 상세 위협 인텔리전스를 검색합니다. 이를 통해 새롭게 떠오르는 위협을 전반적으로 확인하여 조직을 보호하고 인시던트 대응력을 강화할 수 있습니다.

절차



주요 특징

신뢰받는 인텔리전스

Kaspersky Threat Lookup의 주요 특성은 실행 가능한 컨텍스트로 강화한 위협 인텔리전스 데이터의 신뢰성입니다. Kaspersky는 오탐이 거의 없는 최고의 탐지율로 당사 보안 인텔리전스의 독보적인 품질을 입증하며 악성 코드 방지 테스트 분야를 선도합니다.

위협 사냥

공격 선제 예방, 탐지 및 대응으로 공격의 영향과 빈도를 최소화합니다. 사이버 공격을 최대한 신속하게 추적하고 적극 제거하세요. 위협을 조기에 발견할수록 피해를 줄일 수 있고, 복구 및 네트워크 운영 정상화에 드는 시간도 단축됩니다.

쉬운 사용법

웹 인터페이스 또는 RESTful API. 웹 인터페이스(웹 브라우저)를 통해 수동 모드로 서비스를 사용하거나 간단한 RESTful API를 통해 액세스하는 등 원하는 방식으로 서비스를 이용할 수 있습니다.

다양한 내보내기 형식

IoC(침해 지표) 또는 실행 가능한 컨텍스트를 STIX, OpenIOC, JSON, Yara, Snort, CSV 등 널리 사용되는 체계적이고 전산화 가능한 공유 형식으로 내보낼 수 있습니다. 이를 통해 위협 인텔리전스의 장점을 극대화하거나, 운영 워크플로를 자동화하거나, SIEM과 같은 보안 제어와 통합할 수 있습니다.

Kaspersky Threat Lookup의 장점

고도로 검증된 위협 컨텍스트로 위협 지표에 대한 심층 검색을 수행하여, 공격의 우선순위를 정하고, 비즈니스 리스크가 가장 큰 위협의 처리에 집중

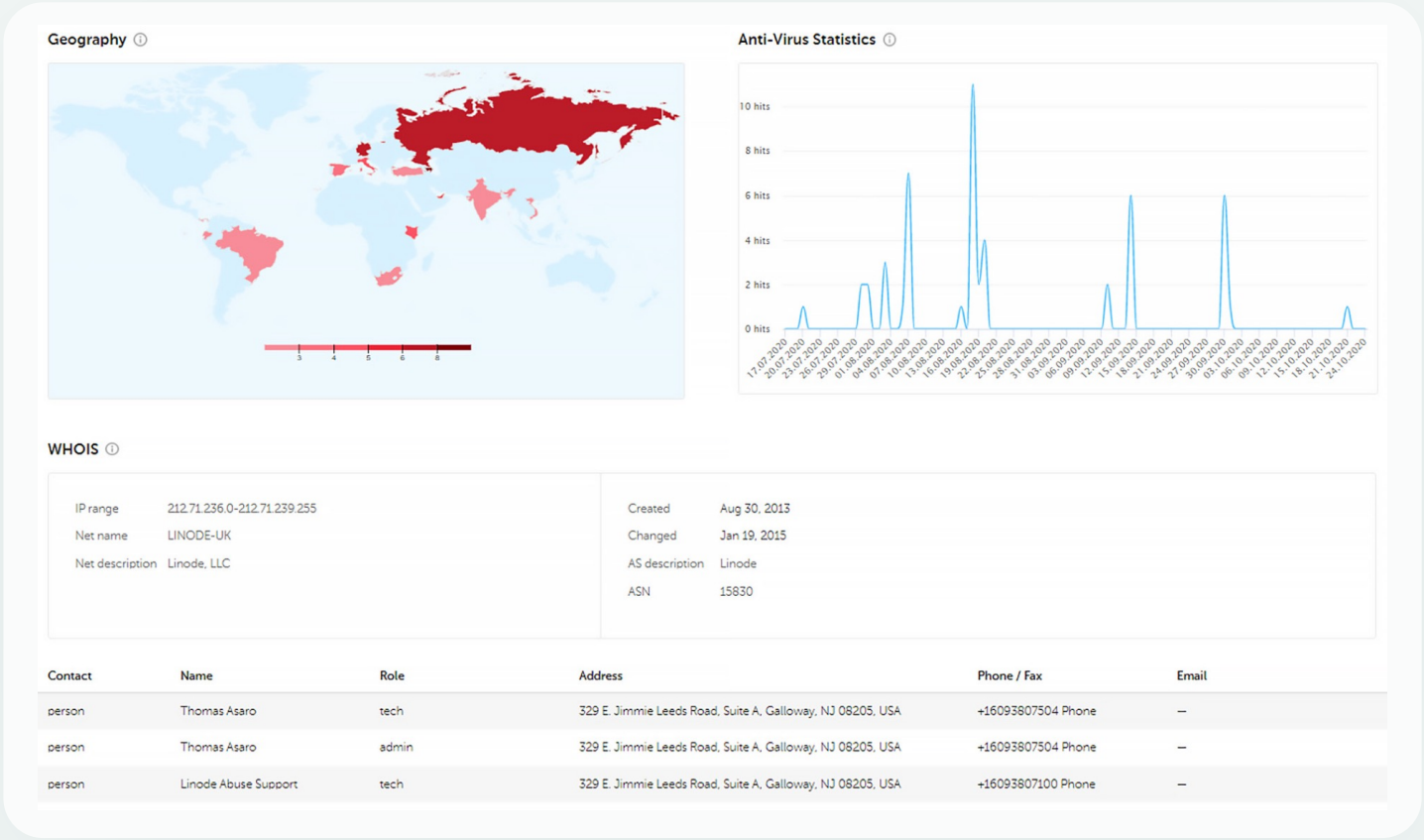
호스트와 네트워크의 보안 인시던트를 더 효율적으로 진단 및 분석하고, 내부 시스템의 알려지지 않은 위협에 대한 신호에 우선순위를 지정

인시던트 대응 및 위협 사냥 기능을 강화하여 중요한 시스템과 데이터에 피해가 가지 전에 킬 체인 중단

웹 기반 인터페이스 또는 RESTful API를 통해 위협 지표 조회

인증서, 흔히 사용하는 이름, 파일 경로 또는 관련 URL을 포함한 고급 세부 정보를 검사하여 새로운 의심스러운 개체 발견

발견된 개체가 이미 널리 퍼졌거나 고유한 개체인지 확인하고, 악성 개체로 판단하는 원인 파악

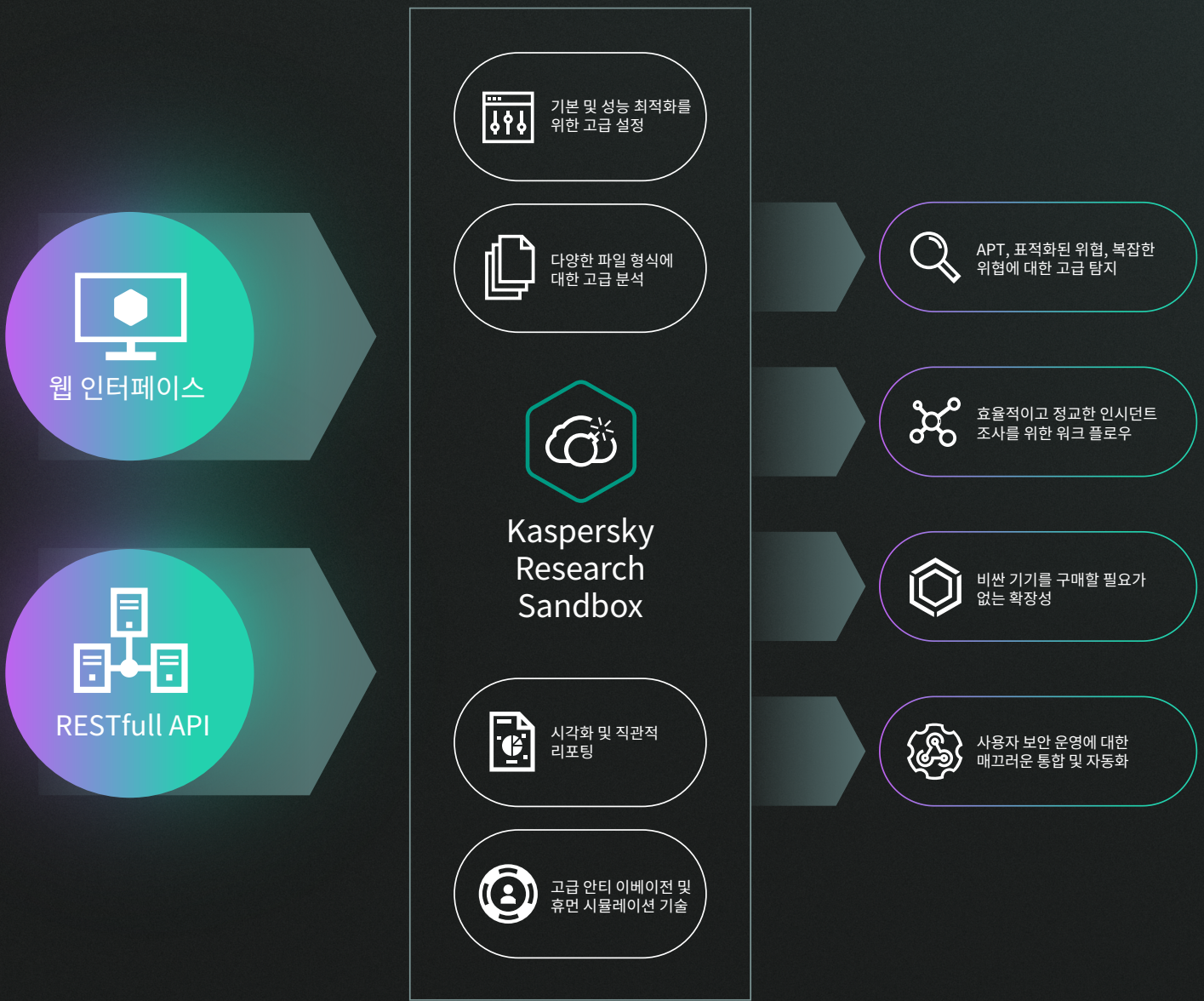


Kaspersky Research Sandbox

기존 AV툴만으로는 표적 공격을 예방할 수 없습니다. 안티바이러스 엔진으로 막을 수 있는 것들은 알려진 위협과 그 변종뿐입니다. 정교한 위협 인자는 매우 다양한 기술로 자동 탐지를 회피합니다. 정보 보안 인시던트에 따른 손실이 계속 증가하는 만큼, 즉각적인 위협 탐지 역량으로 신속하게 대응하여 피해가 발생하기 전에 위협에 차단하는 것이 중요합니다.

정교한 최신 맞춤형 표적화 위협을 파악하는 최적의 방법은 프로세스 메모리, 네트워크 활동 등을 동시 분석하면서 파일의 동작을 기반으로 신중한 판단을 내리는 것입니다. 통계 데이터에는 최근에 바뀐 악성코드의 정보가 부족할 수 있지만, 샌드박싱 기술은 파일 샘플 출처 조사, 행동 분석 기반의 IOC 수집, 발견된 적 없던 악성 개체 탐지를 지원하는 강력한 도구입니다.

Kaspersky Research Sandbox를 사용하면 파일 샘플의 출처를 조사하고, 행동 분석을 기반으로 IOC를 수집하고, 발견된 적 없던 악성 개체를 탐지할 수 있습니다. 이 솔루션은 페타바이트 규모의 통계 데이터(Kaspersky Security Network 및 기타 독자 시스템으로 구현)에서 수집한 위협 인텔리전스, 행동 분석 및 강력한 우회 방지 기능을 자동 클릭, 문서 스크롤, 더미 프로세스와 같은 인간 시뮬레이션 기술과 결합한 하이브리드 접근 방식을 제공합니다.



선제 위협 탐지 및 완화

악성코드는 다양한 방법으로 위장하여 탐지를 피합니다. 시스템이 필요한 매개 변수를 충족하지 않으면, 악성코드도 대개 흔적 없이 사라집니다. 악성코드가 실행되려면 샌드박싱 환경이 정상적인 최종 사용자의 동작을 정확하게 모방할 수 있어야 합니다.

Kaspersky Research Sandbox는 페타바이트 규모의 통계 데이터(Kaspersky Security Network 및 기타 독자 시스템으로 구현)에서 수집한 위협 인텔리전스, 행동 분석 및 강력한 우회 방지 기능을 자동 클릭, 문서 스크롤, 더미 프로세스와 같은 인간 시뮬레이션 기술과 결합한 하이브리드 접근 방식을 제공합니다.

이는 당사의 샌드박싱 랩에서 개발하여 10년 이상 발전시켜온 서비스입니다. 25년간 지속해온 위협 연구로 얻은 악성코드 행동에 대한 모든 지식이 이 기술에 포함되어 있습니다. 덕분에 매일 40만 개 이상의 새로운 악성코드를 탐지하며 고객에게 업계 최고의 보안 솔루션을 제공하고 있습니다.

Kaspersky Research Sandbox는 클라우드 기반 중앙 관리 플랫폼과 에어 갭 환경의 오프라인 콘솔에서 관리할 수 있으며, 위협 인텔리전스를 활용하고 커스터마이징 분석 기능도 포함되어 있습니다.

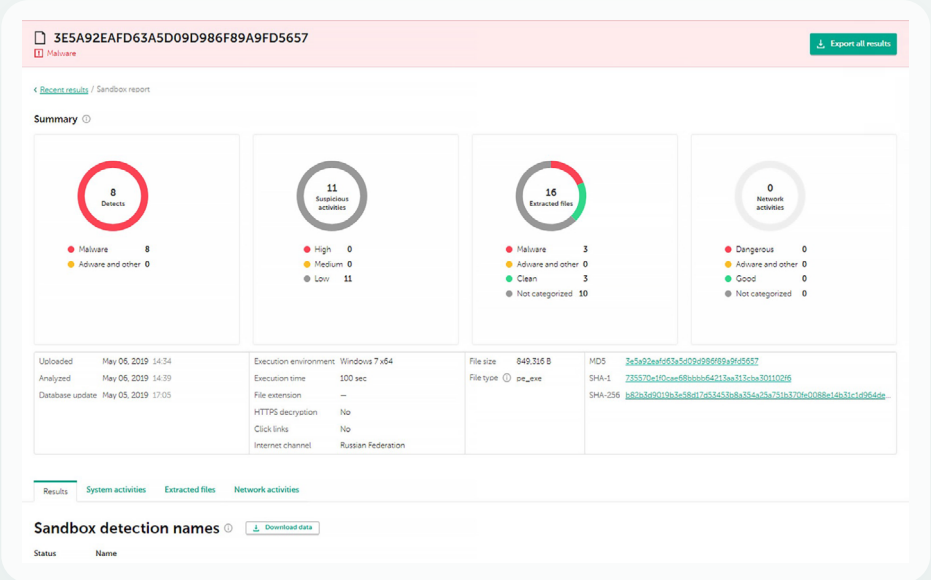
Threat Intelligence Portal의 일부인 Kaspersky Research Sandbox는 고객의 위협 인텔리전스 워크플로의 최종 구성 요소입니다. Threat Lookup이 URL, 도메인, IP 주소, 파일 해시, 위협 이름, 통계/행동 데이터, WHOIS/ DNS 데이터 등에 대한 최신 상세 위협 인텔리전스를 검색하는 반면, Research Sandbox는 그 결과 값을 분석된 파일로 생성한 IOC와 연결합니다.

포괄적인 보고

- 통합 위협 점수
- 의심스러운 시스템 활동과 상세 설명
- DLL 로드 및 실행
- 파일 생성, 변경, 삭제
- 프로세스 메모리 덤프 및 네트워크 트래픽 덤프(PCAP)
- 상호 확장(mutexes) 생성
- 레지스트리 키 수정 및 생성
- 실행 파일로 생성한 프로세스
- 네트워크 활동(SMB, SMTP, IP, TCP, UDP, DNS, SSL, FTP, IRC, POP3, SOCKS 세션, HTTP(s), 요청 및 응답)
- 공개된 모든 침해 지표(IOC)에 대한 실행 가능한 컨텍스트가 포함된 상세한 위협 인텔리전스
- MITRE ATT&CK 기술이 강조된 상세 실행 맵
- YARA로 탐지 및 트리거한 IDS 규칙(커스텀 규칙 포함)
- 특정 URL에 호스팅된 파일의 다운로드 및 분석
- Microsoft Office(Word, Excel, PowerPoint, Publisher, Outlook) 및 Adobe Reader용 문서의 링크 클릭
- 분석 세부 정보를 STIX, JSON, CSV 형식으로 내보내기 가능
- 모바일 OS(Android) 및 환경 커스터마이징 기능을 포함한 다양한 환경
- 커스텀 파일 실행 파라미터
- 다양한 인터넷 채널, 커스텀 VPN 채널을 통한 트래픽 라우팅 가능
- RESTful API
- 스크린샷 및 추가 기능

Kaspersky Research Sandbox를 사용하면 매우 효과적이고 복잡한 인시던트 조사를 실행하여 위협의 특성을 즉시 파악할 수 있고, 드릴 다운을 통해 위협 지표 간의 상호연관성을 파악하여 인사이트를 얻을 수 있습니다.

검사에는 리소스가 많이 필요할 수 있으며, 특히 다단계 공격에서 그러합니다. Kaspersky Research Sandbox는 인시던트 대응 및 포렌식 활동을 강화함으로써, 비싼 장비나 시스템 리소스에 관한 부담 없이도 파일을 자동 처리할 수 있는 확장성을 제공합니다.



Kaspersky Threat Attribution Engine

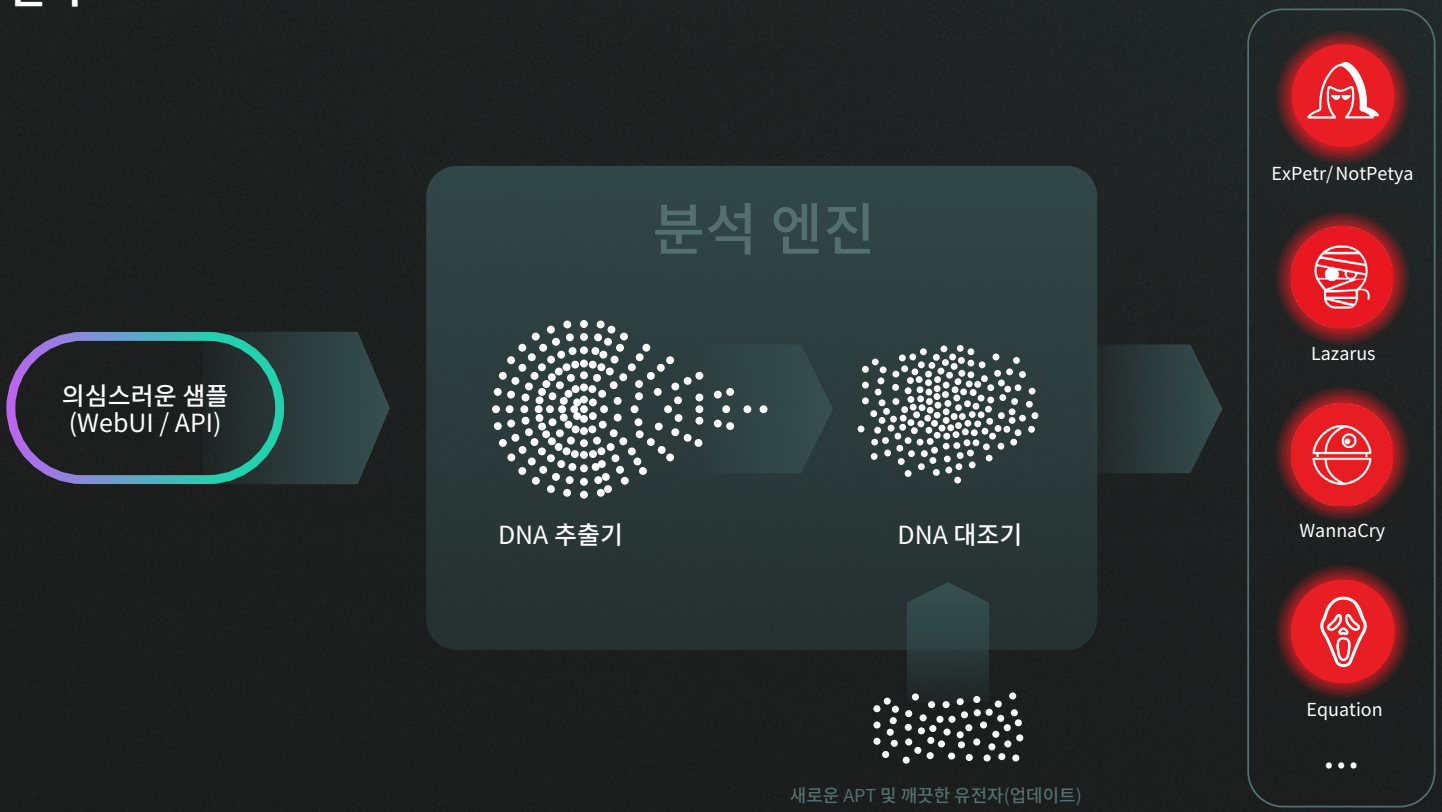
사이버 보안에서 위협 분석을 강조하는 데에는 그럴 만한 이유가 있습니다. 매우 정교한 위협은 복잡한 조사와 리버스 엔지니어링 프로세스를 수행해야 하므로 탐지 후에도 대응까지 시간이 오래 걸릴 수 있습니다. 그리고 사이버 공격은 대개 그 사이에 목적을 달성합니다. 정확하고 시기적절한 분석으로 사고 대응 시간을 몇 시간에서 몇 분으로 단축하고 오탐의 수도 줄일 수 있습니다.

표적 공격 식별, 공격자 프로파일링, 다양한 위협 인자 분석 요소 생성은 몇 년이나 걸릴 수도 있는 길고 복잡한 작업입니다. 또한 작동 가능한 분석을 생성하려면 오랜 시간 동안 축적된 대량의 데이터뿐만 아니라 관련 조사 경험과 뛰어난 능력을 갖춘 연구팀이 필요합니다. 일반적으로 이러한 연구자들은 여러 그룹의 활동을 추적하고, 수집된 모든 정보로 데이터베이스를 채웁니다. 이 데이터베이스는 툴의 형태로 공유할 수 있는 귀중한 리소스가 됩니다.

Kaspersky Threat Attribution Engine은 Kaspersky 전문가들이 25년 이상 수집한 APT 악성코드 샘플과 클린 파일로 구성된 데이터베이스를 바탕으로 하고 있습니다. 당사는 1,100개 이상의 위협 그룹 및 위협 행위를 추적하고 연간 120개 이상의 위협 인텔리전스 보고서를 발표하고 있습니다. 현재 진행 중인 연구는 약 83,000개의 파일이 포함된 APT 컬렉션을 지원합니다. 이를 통해 허위 플래그 탐지를 향상할 수 있으며, 자동화된 툴과 함께 사용 시 분석 정확도가 매우 높아집니다.

오탐을 거의 완벽하게 없애는 동시에 유사한 샘플을 비교하는, 차별화된 접근방식을 제공하는 제품입니다. 이를 이용하면 어떠한 새로운 공격이든 알려진 APT 악성코드, 과거의 표적 공격 및 해커 그룹과 신속하게 링크하여 고위험 위협과 심각도가 낮은 인시던트를 구분할 수 있으며 적시에 선제 조처를 하여 공격자가 시스템에 발판을 마련하지 못하게 할 수 있습니다.

절차



Kaspersky Threat Attribution Engine은 파일 간의 유사성을 검색하는 독자적인 방법을 사용하여 악성코드를 분석 개체에 연결합니다. 여기에는 다음이 포함됩니다:

1

샘플 유전 특질 분석을 위해 코드에서 다음 요소 추출:

- 유전자형 - 고유한 바이너리 코드 조각입니다.
- 문자열 - 고유한 문자 문자열입니다.

2

분석된 파일의 유전자형 및 문자열 자동 검색. 이전에 분석했거나 이미 속성 개체에 연결된 APT 샘플의 유전자형 및 문자열과 유사한 것으로 검색합니다.

3

분석된 샘플의 출처, 관련 속성 개체, 이 샘플과 알려진 APT 샘플 간의 유사성에 대해, APT 샘플에서 발견된 유사한 유전자형과 문자열을 기반으로 분석한 보고서를 제공합니다.

이 제품은 안전한 에어 갭 환경에 배포하여, 처리된 정보 및 제출된 개체에 제삼자가 액세스하지 못하도록 할 수 있습니다. 이 엔진은 API를 통해 다른 툴 및 프레임워크에 연결되며, 기존 인프라 및 자동화된 프로세스에 분석 작업을 적용합니다.

제품 하이라이트

- 수천 개의 APT 그룹, 샘플 및 광범위한 위협에 관한 선별된 데이터 저장소에 대한 즉각 액세스 제공(안티바이러스 엔진을 사용)
- 효율적인 자동 또는 수동 위협 우선순위 지정 및 경고 분류
- 비공개 그룹 및 샘플 추가. 고객의 비공개 컬렉션 내 파일과 유사한 샘플을 탐지하도록 제품을 교육
- 수동 샘플 업로드 지원 및 자동화된 워크플로와의 통합을 위한 향상된 REST API 기능 제공
- 아마존 웹 서비스(AWS)상의 배포 지원으로 하드웨어 투자 비용을 절감하고 신속하게 제품 설치
- YARA 룰로 쉽게 내보내고, 유사 파일에 대한 추가 자동 검색/스캔 또는 타사 솔루션과의 통합
- STIX 2.1 형식(TXT 및 JSON 형식도 지원)로 쉽게 내보내고, 보안 로그의 추가 자동 분석 또는 타사 솔루션/보안 제어와의 통합
- 사용자 지정 암호로 보호된 압축 파일의 압축 해제 지원
- 웹 인터페이스에서 문서 및 최종 사용자 사용권 계약(EULA)에 빠르게 액세스
- 단일 요청으로 분석에 필요한 병렬 파일의 속성 전송

Kaspersky Threat Attribution Engine의 장점

Kaspersky Threat Attribution Engine이 평판 점수를 계산

샘플의 평판 점수를 계산하고 유전 특질과 코드 분석을 밝혀냅니다. 이를 통해 샘플의 출처에 대한 인사이트를 얻을 수 있으며, 가능한 작성자를 분석할 수 있게 됩니다.

보안팀에서 자체 비공개 분석 개체 추가

관련 샘플도 Kaspersky Threat Attribution Engine 데이터베이스에 추가할 수 있습니다. 보안 팀은 이와 같은 방법으로 애플리케이션이 접수된 샘플을 상술한 비공개 분석 개체 및 샘플에 귀속하도록 교육할 수 있습니다.

이 분석 작업은 몇 초면 충분합니다

과거에는 몇 달, 몇 년이 걸렸던 분석 프로세스가 Kaspersky Threat Attribution Engine을 사용하면 단 몇 초 만에 완료됩니다.

Kaspersky Threat Attribution Engine 확장 및 강화

보안 운영 센터(SOC) 및 사이버 보안 기관이 효과적인 인시던트 관리 프로세스를 수립하도록 지원하여 해당 기관에 대한 Kaspersky 포트폴리오를 확장하고 강화합니다.

Kaspersky APT Intelligence Reporting

Kaspersky APT Intelligence Reporting은 발견되는 모든 APT 및 절대 공개되지 않는 위협에 대한 전체 기술 데이터(다양한 형식 지원)를 포함하여 고객에게 당사의 조사와 발견에 관한 차별화되고 지속적인 액세스를 제공합니다. 보고서에는 임원급을 대상으로 작성된 명료한 경영진 보고 요약이 포함되어 있습니다. 관련 APT에 대한 설명과 해당 APT 및 관련 IOC, YARA 룰에 관한 상세한 기술적 설명이 있어 보안 연구원, 악성코드 분석가, 보안 엔지니어, 네트워크 보안 분석가, APT 연구원이 위협에 빠르고 정확하게 대응할 실행 가능한 데이터로 활용할 수 있습니다.

사이버 범죄 그룹의 전술에서 변화가 발견되면 당사 전문가들이 즉시 알려드립니다. 또한 Kaspersky의 전체 APT 보고서 데이터베이스에 대한 액세스도 제공합니다. 더 강력한 보안을 위한 연구 및 분석에 큰 도움이 될 것입니다.

300+
위협 그룹

160+
연간 비공개 보고서 작성

12 000+
IoCs

400+
캠페인

700+
Yara 룰

Kaspersky APT Intelligence Reporting은 다음을 제공합니다

위협 그룹의 프로필

MITRE ATT&CK에 맵핑

핵심 요약

임원급 대상 정보

심층 기술 분석
- 공격 방법
- 사용된 익스플로잇
- 악성코드 정보
- C&C 인프라 및 프로토콜 설명
- 피해자 분석
- 데이터 유출 분석
- 분석

결론 및 제안

침해 지표(IOC) 및 YARA 룰

Kaspersky APT Intelligence Reporting의 장점

비공개 APT 정보

여러 가지 이유로 일반 대중에 공개하지 않는 사이버 위협에 관한 정보도 제공

특별 액세스

일반 대중에게 공개되지 않은, 조사 중인 최신 위협에 대한 기술적 설명을 제공

후향적 분석

서브스크립션 기간에 언제라도 이전에 발행된 비공개 보고서에 액세스

기술 데이터 액세스

OpenIOC 또는 STIX를 포함한 표준 형식으로 제공되는 확장된 IOC 목록, 당사 YARA 룰에 대한 액세스를 포함

위협 그룹 프로필 정보

출처로 의심되는 국가와 주요 활동, 사용된 악성코드 종류, 표적 산업 및 지역, 사용된 모든 TTP에 대한 설명, MITRE ATT&CK에 대한 매핑을 포함

매끄러운 통합 및 자동화

RESTful API와 고객 보안 워크플로의 매끄러운 통합 및 자동화

끊임없는 APT 캠페인 모니터링

조사가 끝나기 전에도 APT 배포, IOC, 명령 및 제어 인프라 등에 대한 정보를 활용하여 실행 가능한 인텔리전스에 액세스

MITRE ATT&CK

보고서에 설명된 모든 TTP를 MITRE ATT&CK에 매핑하여, 해당 보안 모니터링의 사용 사례 개발 및 우선순위 지정, 갭 분석 수행, 관련 TTP에 대한 현재 방어 테스트 등으로 탐지 및 대응 개선에 활용

Kaspersky Crimeware Intelligence Reporting

돈을 노리는 사이버 범죄는 특정 업계에만 국한되지 않습니다. ATM 및 PoS(Point of Sale) 디바이스와 같은 금융 인프라에 대한 공격이 계속되고 있는 가운데, 분야를 막론하고 모든 기업이 랜섬웨어의 위험에 노출되어 있습니다. 지난 몇 년 동안 다양한 유형의 위협과 위협 그룹 유형 간의 경계가 모호해졌습니다. 사이버 스파이 활동이 아닌 절도에 초점을 맞춘 지능형 지속적 위협(APT) 캠페인의 출현도 이에 해당합니다. 이렇게 훔친 돈은 ATP그룹의 다른 활동에 대한 자금으로 사용됩니다. 점점 더 정교해지는 크라임웨어의 위협을 과소평가해서는 안 됩니다.

Kaspersky Crimeware Intelligence Reporting은 악성코드 캠페인, 금융 기관 대상 공격, 은행, 대금 결제 서비스 회사 및 특정 인프라 공격에 사용되는 크라임웨어 툴에 대한 정보를 적시에 제공하여 고객의 방어 전략을 강화합니다.

Kaspersky Crimeware Intelligence Reporting은 다음을 제공합니다

- 자주 사용되는 잘 알려진 주요 악성코드에 대한 자세한 설명
- 신규 및 최신 악성코드 위협에 대한 정보를 포함하는 연구 노트/조기 경고
- 자주 사용되는 위험한 악성코드 캠페인 정보
- 금융 인프라 대상 위협과, 다양한 지역의 다크 웹에서 사이버 범죄자들이 개발 및 판매 중인 관련 공격툴에 대한 자세한 설명

Kaspersky Crimeware Intelligence Reporting의 장점

특별 액세스

일반 대중에게 공개되지 않은, 조사 중인 최신 위협에 대한 기술적 설명을 제공

후향적 분석

서브스크립션 기간에 언제라도 이전에 발행된 비공개 보고서에 액세스

매끄러운 통합 및 자동화

RESTful API와 고객 보안 워크플로의 매끄러운 통합 및 자동화

기술 데이터 액세스

OpenIOC 또는 STIX를 포함한 표준 형식으로 제공되는 확장된 IOC 목록, 당사 YARA 룰에 대한 액세스를 포함

크라임웨어 그룹 프로필 정보

출처로 의심되는 국가와 주요 활동, 사용된 악성코드 종류, 표적 산업 및 지역, 사용된 모든 TTP에 대한 설명, MITRE ATT&CK에 대한 매핑을 포함

Kaspersky ICS Threat Intelligence Reporting

Kaspersky ICS Threat Intelligence Reporting은 산업 조직을 표적으로 삼는 악성 캠페인에 대한 심층 인텔리전스와 폭넓은 인식을 제공하며, 가장 많이 사용되는 산업 제어 시스템 및 제반 기술에서 발견된 취약성 정보도 제공합니다. Kaspersky Threat Intelligence Portal을 통해 보고서를 제공하므로 즉시 서비스를 사용할 수 있습니다.

ICS 관련 모든 위협 인텔리전스 연구는 전담팀인 Kaspersky ICS CERT가 수행합니다:

- 2016년 설립
- 상업 조직에서 만든 최초의 CERT 팀
- ICS 위협 및 취약성 연구, 인시던트 대응 및 보안 분석 분야의 우수한 전문가 약 20명

서브스크립션에 포함되는 보고서

APT 보고서

산업 조직 대상의 신규 APT 및 대규모 공격 캠페인 관련 보고서, 활성 위협에 관한 업데이트

취약점 발견

Kaspersky가 산업 제어 시스템, 산업용 사물인터넷 및 다양한 산업 분야의 인프라에 사용되는 인기 제품에서 식별한 취약점 보고서

취약점 분석 및 완화 방안

인프라 취약성을 식별하고 줄이는데 유용한 Kaspersky 전문가의 실행 가능한 권장 사항 제공

위협 환경의 진화

산업 제어 시스템의 위협 환경에 대한 중요한 변화, 새롭게 발견된 ICS 보안 수준에 영향을 미치는 중요 요소 및 위협에 대한 ICS 노출에 대한 지역, 국가 및 산업별 정보를 포함한 보고서 제공

위협 인텔리전스 데이터로 더 강력해지는

탐지 및 예방

기존에 보고된 위협에 대한 탐지 및 예방으로 소프트웨어 및 하드웨어 구성 요소 등의 중요 자산을 보호하고, 기술 프로세스의 안전과 연속성을 보장

취약성 평가

취약점의 범위와 심각도에 대한 정확한 평가를 기반으로 고객의 산업 환경 및 자산을 평가하여, 패치 관리에 대해 정보에 입각한 결정을 내리고 Kaspersky가 권장하는 기타 예방 조치를 이행

상관관계

산업 환경에서 탐지한 모든 악성 및 의심스러운 활동을 Kaspersky의 연구 결과와 연관지어, 해당 악성 캠페인에 대한 탐지 내용을 분석하고 위협을 식별하여 사고에 신속하게 대응

정보 활용

공격 기술, 전술 및 절차, 최근에 발견된 취약점 및 기타 중요한 위협 환경 변화에 대한 정보를 활용하여 다음을 수행할 수 있습니다.

- 보고된 위협 및 기타 유사한 위협에 따른 위험 식별 및 평가
- 생산 안전성과 기술 프로세스의 연속성 보장을 위한 산업 인프라 변경 계획 및 설계
- 실제 사례 분석을 기반으로 보안 인식 활동을 실행하여 직원 교육 시나리오를 만들고 레드팀 대 블루팀 훈련 계획
- 정보에 입각한 전략적 결정으로 사이버 보안에 투자하고 운영 회복력 보장

Kaspersky Digital Footprint Intelligence

비즈니스의 성장에 따라 IT 환경의 복잡성과 분포도 함께 증가하며, 직접적인 제어나 소유권 없이 광범위하게 분산된 디지털 자산을 보호해야 하는 새로운 어려움이 발생하고 있습니다. 기업은 동적이고 상호연결된 환경을 활용해 상당한 이익을 창출할 수 있습니다. 그러나 이러한 상호 연결성의 증가에 따라 공격 지점도 확대되고 있습니다. 공격자의 숙련도가 점차 올라가는 만큼, 조직의 온라인 상태에 대한 정확한 파악뿐만 아니라 변화를 추적하고 노출된 디지털 자산을 노리는 외부 위협에 대응할 능력도 중요합니다.

보안 운영을 위해 다양한 보안툴이 사용되고 있지만, 데이터 유출을 탐지 및 방지하고, 다크 웹 포럼에 있는 사이버 범죄자의 계획과 공격 전략을 모니터링하는 등 매우 구체적인 기능이 요구되는 디지털 위협이 여전히 존재합니다. 보안 분석가가 회사 리소스에 대한 공격자의 관점을 탐색하고, 공격자가 사용할 수 있는 잠재적 공격 벡터를 즉시 발견하고, 그에 따라 방어를 조정할 수 있도록 개발된 것이 바로 Kaspersky Digital Footprint Intelligence입니다.

Kaspersky Digital Footprint Intelligence는 다음을 제공합니다

네트워크 정찰

공격의 잠재적 진입점이 될 수 있는 고객의 네트워크 리소스 및 노출된 서비스를 식별합니다. CVSS 기본 점수, 공개 익스플로잇의 가용성, 모의 침투 테스트 경험, 네트워크 리소스(호스팅/인프라)의 위치를 기반으로 추가 평가 및 종합적인 위험 평가를 통해 기존 취약점에 대한 맞춤형 분석을 제공합니다.

브랜드 보호

온라인에서 회사 브랜드의 무단 사용을 모니터링하고 차단합니다. 회사 평판을 손상하거나 고객을 속일 수 있는 가짜 SNS 계정 및 애플리케이션, 피싱 웹사이트 및 기타 사기 활동을 식별합니다. 모바일 마켓플레이스에서 가짜 SNS 계정과 가짜 애플리케이션을 삭제합니다.

다크 웹 모니터링

다크 웹 리소스(포럼, 랜섬웨어 블로그, 메신저, 토르 사이트 등)를 지속해서 모니터링하여 회사, 고객 및 파트너와 관련된 모든 참고사항 및 위협을 탐지합니다. 현재 진행 중인 표적 공격 또는 계획 중인 공격 및 고객의 회사, 고객이 속한 산업계 및 운영 지역을 겨냥한 APT 캠페인을 분석합니다.

데이터 유출 확인

사이버 공격을 수행하거나 회사의 평판 위험을 초래하는 데 사용될 여지가 있는 직원, 파트너 및 고객 자격 증명, 은행 카드, 전화번호 및 기타 민감한 정보를 탐지합니다.

인텔리전스 소스

비즈니스의 외부 보안 태세를 종합적으로 파악하는 것은 중요합니다. 이를 돕기 위해, Kaspersky 보안 분석가는 다음의 인텔리전스 소스에서 정보를 수집하고 집계합니다.

구조화하지 않은 데이터

- IP 주소
- 회사 도메인
- 브랜드 이름
- 키워드

네트워크 경계 인벤토리

표층 웹, 딥 웹, 다크 웹

Kaspersky Knowledge Base

분석적 보고서

위협 경고

연간 10건의 삭제 요청

Kaspersky, OSINT, 표면 및 다크 웹 소스 전반을 대상으로 실시간 검색

절차

구성	수집	필터	대응
회사의 디지털 자산에 대한 정보 검색	표면 웹, 딥 웹 및 다크 웹과 Kaspersky 위협 인텔리전스 데이터베이스를 대상으로 자동화된 데이터 수집	분석가의 위협 탐지, 분석 및 우선순위 지정	완전한 인텔리전스의 전달

비즈니스 가치

Kaspersky Digital Footprint Intelligence는 강력한 혜택과 상당한 가치를 제공합니다.

브랜드 보호

잠재적인 위협을 실시간으로 탐지하여 브랜드 평판을 보호하고, 고객의 신뢰를 유지하며, 재정적 손실과 비즈니스 운영 손상의 위험을 줄일 수 있습니다.

사이버 리스크 저감

주요 이해 관계자(임원급 및 이사회)에게 기존 사이버 보안 투자 항목 간의 격차와 그에 따른 위험을 보여주어 어떤 사이버 보안 요소에 집중투자가 필요한지 알려줄 수 있습니다.

더 신속한 대응

보안 경고에 대한 추가 컨텍스트로 인시던트 대응을 개선하고 평균 응답 시간(MTTR)을 단축합니다.

공격 표면 축소

회사의 디지털 입지를 관리하고 외부 네트워크 리소스를 제어하여 공격에 사용될 수 있는 공격 벡터와 취약성을 최소화할 수 있습니다.

사이버 공격자들에 대한 이해

사이버 범죄자들이 다크 웹에서 회사에 대해 어떤 계획을 논의하고 있는지 파악하여 이에 대비할 수 있습니다.

지평 확장

사이버 공격을 견디고, 회사 보안 팀의 관할권 밖의 위협을 식별할 수 있도록 역량을 개발할 수 있습니다.

Kaspersky Takedown Service

사이버 범죄자는 회사와 브랜드를 공격하기 위해 악성 및 피싱 도메인을 생성합니다. 이러한 위협에 신속하게 대처하지 못하면 매출 손실, 브랜드 이미지 손상, 고객 신뢰 상실, 데이터 유출 등으로 이어질 수 있습니다. 그러나 이러한 도메인의 게시 중단을 관리하는 것은 전문 지식과 시간이 필요한 복잡한 프로세스입니다.

Kaspersky Takedown Service는 브랜드와 비즈니스에 피해가 발생하기 전에 악성 및 피싱 도메인의 위협을 신속하게 저감합니다. 전체 프로세스의 종단 간 관리로 고객의 소중한 시간과 리소스를 절약할 수 있습니다. 이 서비스는 전 세계를 대상으로 합니다.

Kaspersky는 매일 15,000개 이상의 피싱/스캠 URL을 차단하고, 해당 URL을 클릭하는 시도를 백만 건 이상 막고 있습니다. 수년간 악성 및 피싱 도메인 분석해온 만큼, 당사는 어떤 사이트가 악성인지 판단하는 데 필요한 모든 증거를 어떻게 수집하는지 잘 알고 있습니다. 당사는 고객이 다른 중요한 일에 집중할 수 있도록 고객의 게시 중단 관리 작업을 대신 처리하고, 신속한 조치를 통해 디지털 리스크를 최소화합니다.

Kaspersky는 국제기구, 국가 및 지역 법 집행 기관(인터폴, 유로폴, 마이크로소프트 디지털 범죄 유닛, 네덜란드 경찰청의 국가 하이테크 범죄 유닛(NHTCU), 런던 시경 등) 및 전 세계 컴퓨터 긴급 대응 팀(CERT)과 협력하여 고객의 온라인 서비스 및 평판을 효과적으로 보호하고 있습니다.

전체적인 가시성

요청 등록부터 삭제 성공까지 단계마다 고객에게 알림 제공

종단 간 관리

당사가 전체 게시 중단 프로세스를 관리하여, 고객의 개입 최소화

글로벌 커버리지

Kaspersky는 악성 또는 피싱 도메인의 등록지와 무관하게, 관련 법적 권한이 있는 지역 기관에 해당 도메인의 삭제를 요청합니다.

Kaspersky Digital Footprint Intelligence와의 통합

Kaspersky Takedown Service는 별도 구매도 가능하지만, Kaspersky Digital Footprint Intelligence와 통합할 때 시너지 효과를 극대화할 수 있습니다. Kaspersky Digital Footprint Intelligence는 피싱 및 악성코드 도메인에 대한 실시간 알림을 제공합니다. 이 알림들은 필요하다면 Kaspersky Takedown Service에 즉시 전달하여 추가 차단할 수 있습니다.

절차

당사의 기업 고객 지원 포털인 Kaspersky Company Account를 통해 고객 요청사항을 제출할 수 있습니다. 당사는 필요한 모든 서류를 준비하여 도메인 폐쇄에 필요한 법적 권한을 가진 관련 지역/지역 당국(CERT, 등록기관 등)에 도메인 폐쇄 요청을 보냅니다. 당사는 요청된 리소스의 성공적인 삭제까지 단계마다 고객에게 알림을 제공합니다.

편리한 방지 조치

Kaspersky Takedown Service는 고객의 브랜드와 비즈니스에 피해가 발생하기 전에 악성 및 피싱 도메인이 제기하는 위협에 신속하게 대처합니다. 전체 프로세스의 종단 간 관리로 고객의 귀중한 시간과 리소스를 절약할 수 있습니다.

Kaspersky Ask the Analyst

사이버 범죄자들은 기업을 공격하는 정교한 방법을 끊임없이 개발하고 있습니다. 오늘날의 위협 환경은 빠르게 변화하고 성장하며, 사이버 범죄 기술도 점점 더 기민해지고 있습니다. 조직은 악성코드 없이 수행되는 공격, 파일리스 공격, 리빙 오프 더 랜드 공격, 제로 데이 익스플로잇, 그리고 이 모든 것이 결합된 복합 위협, APT 유사 공격 및 표적 공격 때문에 발생하는 복잡한 인시던트에 대처해야 합니다.

비즈니스를 위협하는 사이버 공격의 시대에 사이버 보안 전문가가 그 어느 때보다 중요하지만, 이러한 전문가를 찾고 사내에 유지하기란 쉽지 않습니다. 또한 사이버 보안 팀이 잘 구축되어 있더라도, 정교한 위협과의 전쟁에서 전문가 혼자 맞서 싸울 수는 없습니다. 따라서, 사내 사이버 보안 팀이 외부 전문가의 지원을 요청할 수 있어야 합니다. 외부 전문가는 복잡한 공격과 APT가 일어날 수 있는 경로를 제시하고, 이를 가장 결정적으로 제거할 방법에 대한 실행 가능한 조언을 제공할 수 있습니다.

지속적인 위협 연구 끝에, Kaspersky는 공격자와 사이버 범죄자가 자주 이용하는 전 세계의 폐쇄된 커뮤니티와 다크 포럼을 발견, 침투, 모니터링할 수 있는 역량을 개발했습니다. 당사의 분석가들은 이러한 액세스 권한을 활용하여 가장 피해가 크고 악명 높은 위협은 물론 특정 조직을 표적으로 삼는 맞춤형 위협을 선제로 탐지하고 조사합니다.

Kaspersky Ask the Analyst는 당사의 위협 인텔리전스 포트폴리오를 지원하여, 고객이 현재 직면하거나 관심이 있는 특정 위협에 대한 지침과 인사이트를 요청할 수 있도록 합니다. 이를 통해 Kaspersky의 강력한 위협 인텔리전스 및 연구 기능을 고객의 특정 요구 사항에 맞게 조정하여, 고객사를 표적으로 삼는 위협에 대해 탄력적인 방어 체계를 구축할 수 있습니다.

Kaspersky Ask the Analyst 제품(통합 요청기반 서브스크립션)

APT 및 크라임웨어

발표된 보고서 및 진행 중인 연구에 대한 추가 정보(APT 또는 크라임웨어 인텔리전스 보고 서비스 외)

위협, 취약점 및 관련 IoC에 관한 설명

- 특정 악성코드군에 관한 개괄적 설명
- 추가적인 위협 컨텍스트(관련 해시, URL, CnCs, 등)
- 특정 취약점 정보(치명도 및 해당 항목에 대해 Kaspersky 상품이 제공하는 보호 메커니즘)

ICS 관련 요청

- 발표된 보고서에 관한 추가 정보
- ICS 취약성 정보
- ICS 위협 통계 및 지역 / 산업계 추세
- 규제 또는 표준에 관한 ICS 악성코드 분석 정보

다크 웹 인텔리전스

- 특정 아티팩트, IP 주소, 도메인 이름, 파일 이름, 이메일, 링크 또는 이미지에 대한 다크 웹 조사
- 정보 검색 및 분석

악성코드 분석

- 악성코드 샘플 분석
- 추가 복구 활동 제안

절차

Kaspersky Ask the Analyst는 별도 구매할 수도 있고, 당사의 위협 인텔리전스 서비스에 추가하여 구매할 수 있습니다. 당사의 기업 고객 지원 포털인 Kaspersky Company Account를 통해 고객 요청사항을 제출할 수 있습니다. 이메일로 답변을 드리지만, 필요성이 인정되고 고객의 동의가 있으면 전화 회의 및 화면 공유 세션도 가능합니다. 고객 요청이 수락되면 처리 예상 기간을 알려 드립니다.

사용 사례

1. 사전에 게시된 위협 인텔리전스 보고서의 세부 정보를 명확화
2. 이전에 받은 IoC에 대한 추가 인텔리전스 획득
3. 취약점에 대한 세부 정보 및 취약점 악용을 막기 위한 제안을 확인
4. 고객이 관심 있는 특정 다크 웹 활동에 대한 추가 세부 정보 수신
5. 악성코드의 동작 및 잠재적 영향, Kaspersky가 관찰한 관련 활동에 대한 세부 정보가 포함된 악성코드군 개요 보고서 수신
6. 자세한 컨텍스트 정보 및 짧은 보고서로 제공된 관련 IoC에 대한 분류를 활용하여 경고/인시던트의 우선 순위를 효과적으로 지정
7. 탐지된 비정상적인 활동과 APT 또는 크라임웨어 인자와의 관련성에 대한 식별 지원 요청
8. 악성코드 파일을 제출하여 포괄적 분석을 수행하고, 이를 통해 이전에 제공한 샘플의 동작과 그 기능을 이해

Kaspersky Ask the Analyst의 장점

전문성 확장

비용을 치르고 풀타임 전문가를 고용할 필요 없이, 업계 전문가를 온디맨드 방식으로 이용

조사 가속화

맞춤형의 상세한 컨텍스트를 기반으로 인시던트의 범위를 효과적으로 지정하고 우선순위를 지정

신속한 대응

위협과 취약성에 빠르게 대응할 수 있도록 알려진 벡터를 통한 공격을 차단하는 당사의 지침을 제공

고객의 지식과 리소스 확장

Kaspersky Ask the Analyst를 사용해서 사례별 Kaspersky 핵심 연구원 그룹에 액세스할 수 있습니다. 이 서비스는 전문가 간의 포괄적인 커뮤니케이션을 제공합니다. 이를 통해 당사의 차별화된 지식과 리소스를 바탕으로 고객의 기존 역량을 확장할 수 있습니다.

결론

오늘날의 사이버 위협에 대응하려면 위협 그룹이 사용하는 전술과 툴에 대한 전방위적 이해가 필요합니다. 이러한 인텔리전스를 생성하고 가장 효과적인 대응책을 식별하려면 끊임없는 노력과 높은 수준의 전문성이 필요합니다. 전에 없던 사이버 공격에 대해 고객이 면역력을 유지할 수 있도록 페타바이트 규모의 풍부한 위협 데이터, 고급 머신 러닝 기술, 고유한 글로벌 전문가 풀을 통해 전 세계의 최신 위협 인텔리전스로 고객을 지원합니다.

주요 이점

글로벌 위협 가시성, 사이버 위협 적시 탐지, 보안 경고 우선순위 지정, 정보 보안 사고에 대한 효과적 대응 지원

다양한 산업과 지역의 위협 그룹이 사용하는 전술, 기술, 절차에 대한 차별화된 인사이트를 통해 표적화되고 복잡한 위협으로부터 고객을 선제로 보호

위협 완화 전략에 대한 실행 가능한 제안과 함께 보안 태세에 대한 포괄적인 개요를 통해, 주요 사이버 공격 표적으로 식별된 영역에 방어 전략을 집중

분석가의 번아웃을 방지하고 고객의 인력이 실제 위협에 집중할 수 있도록 지원

인시던트 대응 및 위협 헌팅 기능을 개선 및 가속하여 공격 '체류 시간'을 줄이고 피해를 최소화

Kaspersky Threat Intelligence

자세히 보기

www.kaspersky.co.kr

#kaspersky
#bringonthefuture