cybereason

Cybereason Detection and Response Platform

Cybereason 실시간 공격 탐지 및 대응 플랫폼은 군대 수준 방어 기능을 기업에 제공하여 자동화된 탐지, 완벽한 상황 인식 및 공격자 활동에 대한 깊은 이해를 제공합니다.



공격 캠페인 자동 탐지



상세 공격정보 제공

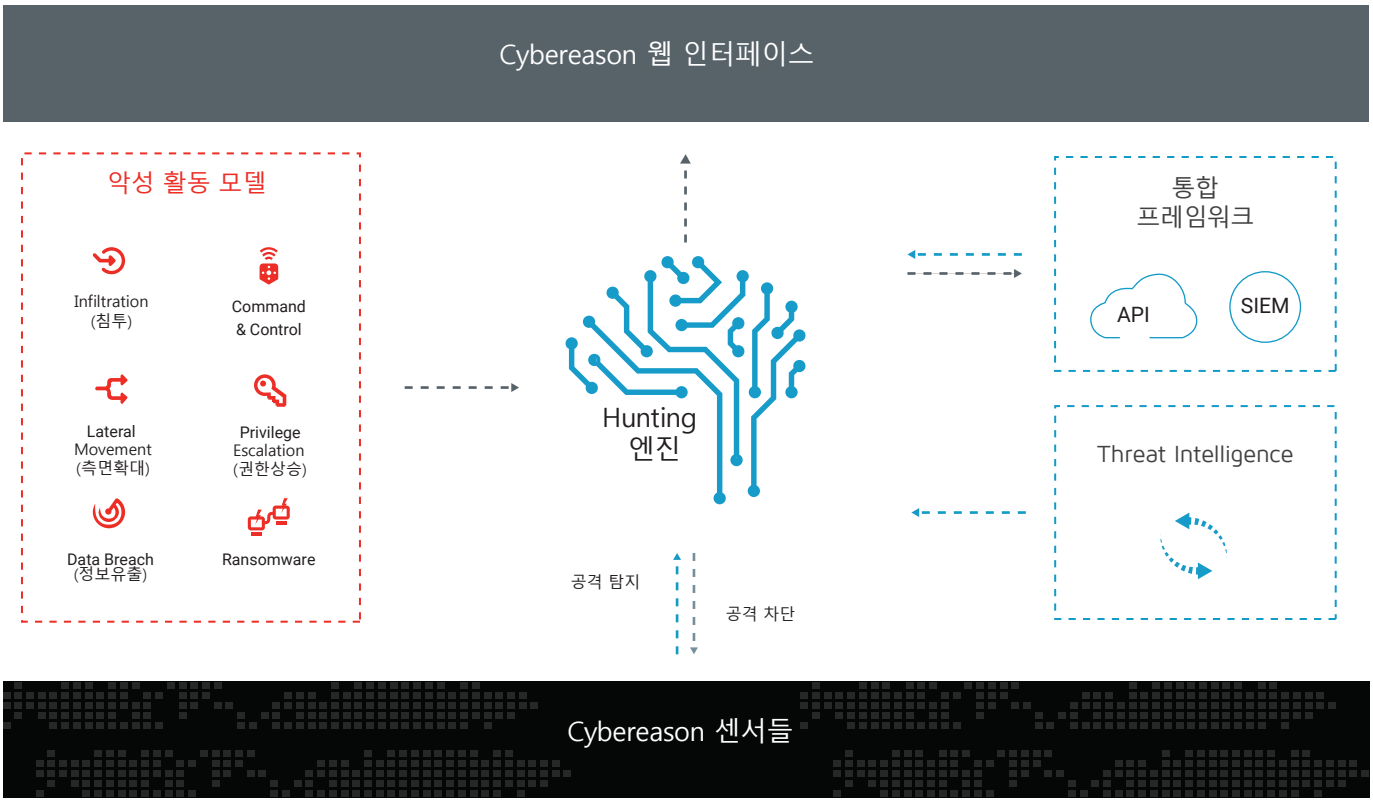


보안팀 스킬 향상

Cybereason은 악의적인 활동을 자동으로 탐지하여 직관적으로 제시하고 공격 캠페인의 종단간 컨텍스트를 제공하며 빠르고 쉽게 적용할 수 있어 24-48 시간 이내에 배포와 탐지를 시작할 수 있습니다.

지속적인 24/7 모니터링을 통해 Cybereason은 전체 IT 환경에 대해 완벽한 상황인지 기능을 제공하므로 언제든지 "지금 공격 받고 있습니까?"라는 질문에 대답할 수 있습니다.

©2018 Cybereason Inc. All Rights Reserved.



악의적인 활동을 완벽히 파악 할수 있습니다.

Cybereason 센서는 기업 전체의 모든 최종 사용자 시스템과 서버에서 상세 정보를 지속적으로 수집합니다. Hunting Engine은 중앙 집중식 메모리 내 분석을 수행하여 초기 침투, 명령 및 제어, 권한 상승 및 측면 이동과 같은 모든 악성 활동을 식별합니다.

Cybereason 웹 인터페이스는 이러한 활동의 타임 라인을 그래픽으로 나타내며 근본 원인, 영향을 받는 엔드포인트와 사용자, 관련 통신 및 사용 된 도구에 대한 가시성을 제공합니다. Cybereason은 보안 분석가가 검색 및 조사 할 수 있도록관련 정보를 제공합니다.

Cybereason 센서들

차별화된 데이터 수집 에이전트인 Cybereason 센서는 엔드포인트와 서버에 배포되며 사용자 환경 전체에서 데이터를 수집합니다. 센서는 생산성에 전혀 영향을 미치지 않고 배포됩니다. Cybereason 센서의 고유한 기술은 커넬 레벨이 아닌 사용자 레벨에서 지속적으로 실행되므로 모든 작업을 완벽하게 볼 수있는 동시에 시스템을 중단(Blue Screen 등)시키는 것이 불가능하여 엔드포인트에서 실행중인 타 커넬 레벨의 솔루션들과 충돌이 없습니다.

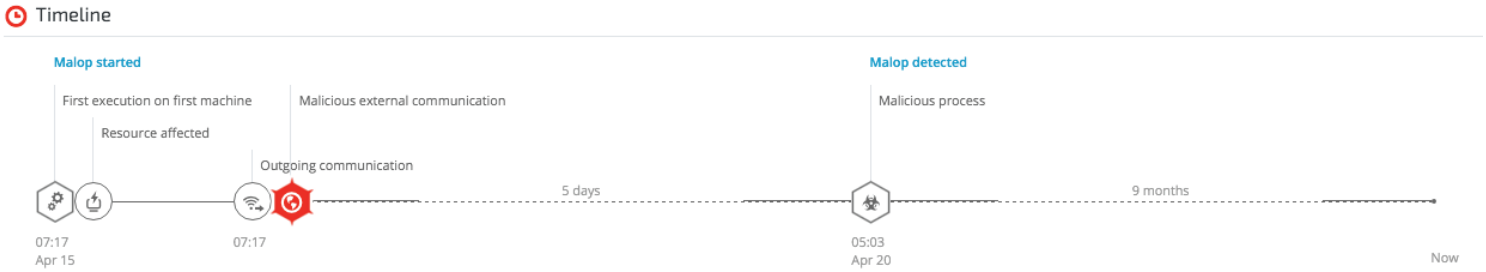
The Hunting 엔진

Hunting 엔진은 알려지지 않은 공격 요소와 새로운 공격 기법을 식별 할 수 있도록 설계된 광범위한 탐지 모델을 기본으로 제공합니다. 즉, Hunting 엔진이 센서에서 데이터를 수신하는 즉시 보안 위협을 감지하고 대응할 수 있습니다.

©2018 Cybereason Inc. All Rights Reserved.

악성 활동 탐지 모델

Cybereason에는 해킹 캠페인을 수행하는 동안 공격자가 사용하는 악성 활동 및 도구, 전술 및 절차를 찾는 모델 라이브러리가 탑재되어 있습니다. 규칙을 구성하고 조정하는 데 몇 주가 소요될 필요도 없습니다. 위협을 즉시 탐지 할 수 있습니다. Cybereason의 악성 활동 탐지 모델은 킬체인의 침입, C&C, 측면 이동, 권한 상승 및 피해를 탐지하여 전체 공격 라이프사이클를 분석합니다.



Cybereason 웹 인터페이스

Cybereason 웹 인터페이스는 플랫폼에서 수집 한 정보를 사용하여 쉽게 이해할 수있는 시각적 공격 이야기를 전달합니다. Cybereason 웹 인터페이스에서는:

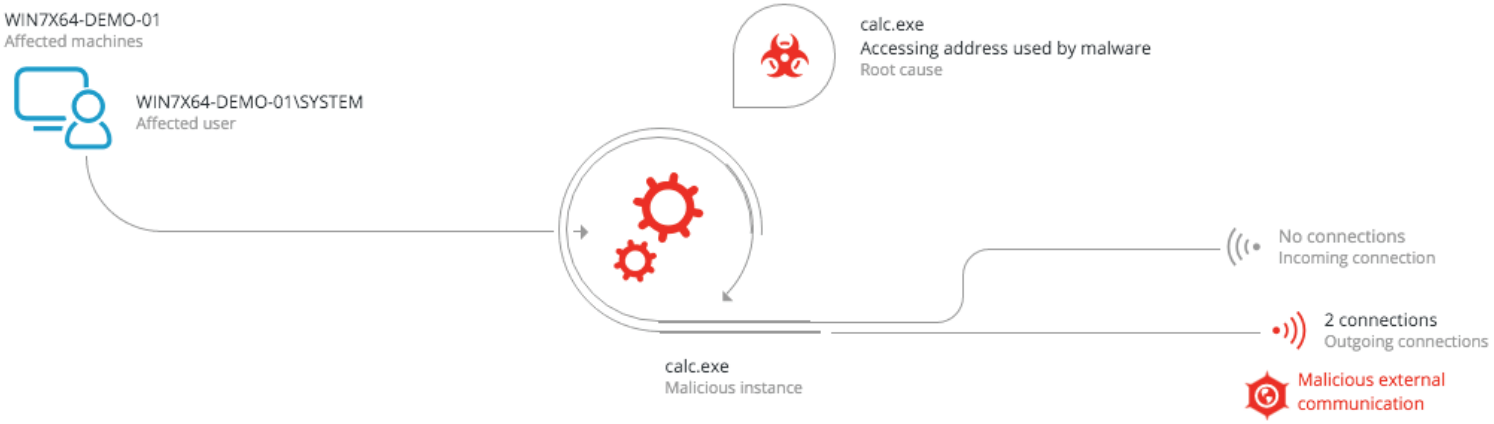
Malicious Operations Dashboard 엔드포인트 전체 상태를 한눈에 파악할 수 있습니다. 현재 진행중인 악의적인 활동에 대한 가시성과 얼마나 널리 퍼져 있는지 파악할 수 있으며 공격 정보를 공유할 수 있습니다.

Malop Visualizer 실시간으로 Cybereason에서 탐지한 악성 활동을 자동으로 연결하여 시각화합니다. 공격의 범위, 발생한 날짜의 타임 라인 및 진화하는 상황의 그림을 보여줍니다.

Investigation Workbench 분석가들에게 공격자의 활동에 대한 자세한 공격 컨텍스트를 제공합니다. 영향을 받는 사용자, 네트워크 연결, 시스템 및 프로세스를 기준으로 공격자의 활동, 도구 및 기법을 추적 할 수 있습니다.

Single-Click Guided Remediator 위협을 봉쇄하고 제거하는 프로세스를 자동화하여 프로세스를 중단하고 파일을 격리하며 레지스트리 키를 삭제할 수 있습니다.

Attack Blocker 자동으로 프로세스 실행을 차단하고 네트워크 통신을 차단하여 위협이 비즈니스를 손상시키는 것을 방지합니다.



©2018 Cybereason Inc. All Rights Reserved.

Cybereason Live Threat Intelligence

Cybereason Live Intelligence는 플랫폼에 내장된 실제적인 인텔리전스를 생성하여 악의적인 작업을 자동으로 탐지합니다. Cybereason의 전문가팀은 전세계의 적대 행위를 감시하여 임박한 위험에 대한 조기 경보를 얻습니다.

Cybereason의 Threat Ingelligence는 바이너리를 "블랙리스트" 또는 "화이트리스트"로 단순하게 판단하는 다른 솔루션들과 다르게, 악성 행위 구분을 위한 차별화된 행위 접근방식으로 분석할 만한 가치가 있는지를 판단하는 하나의 요소로 활용된다.

Cybereason Active Monitoring Team

Cybereason은 군인, 대학, 및 상업적 경험자들과 군대급 보안 전문가 군단을 모았습니다. 이 팀은 수십 년간 세계에서 가장 정교한 공격을 다루는 직접 경험을 가지고 있습니다. 포춘지 선정 500 대 기업을 대상으로 보안 운영 센터를 구축하고 Big Four 전문 서비스 조직 중 한 곳의 사고 대응 계획을 수립했습니다. 이 팀은 소규모 보안 팀에서부터 대규모 국제 조직에 이르기까지 수백 개의 조직에 보안 교육을 개발하고 제공하는 광범위한 경험을 갖추고 있습니다.

Cybereason Active Monitoring Team에서 구체적이고 실행 가능한 알림을 받으십시오.

우리는 아래 사항을 제공 할 수 있습니다. :

Active monitoring Cybereason 전문가는 사용자 환경에서 악성 활동을 모니터링하고 분석합니다. 악의적인 활동이 확인되면 Cybereason이 알려주고 위협을 제거하는 방법을 알려줍니다.

In-depth investigation 잠재적인 심각한 문제의 경우 Cybereason 전문가가 데이터를 조사하고 사건을 신고하고 대응 계획을 개발할지 여부에 대한 독립적인 조언을 제공합니다.

보안팀은 Cybereason 플랫폼에 대한 완전한 액세스 권한을 얻으며 Cybereason의 조사 결과에 대한 유효성 검사 및 추가 조사를 수행 할 수 있습니다. 따라서 플랫폼 및 데이터를 완벽하게 제어하면서 관리되는 모니터링에 대한 전문 지식을 얻을 수 있습니다.

Cybereason은 혁신적인 사이버 공격 탐지 및 대응을 위해 전직 군대 사이버 보안 전문가 팀이 2012 년에 설립했습니다.

Cybereason 본사는 보스턴에 있으며, 이스라엘 텔 아비브 및 일본 도쿄에 사무소가 있습니다.

cybereason

©2018 Cybereason Inc. All Rights Reserved.