cybereason

헌팅 엔진의 기술

복잡한 IT 생태계를 보호한다는 것은 끊임없이 성장하는 다양한 사람들과 사물의 활동, 관계, 역할, 그리고 무엇이 좋으며 무엇이 나쁜지 파악하여 보호하고 발생하는 공격을 감지하며 피해가 발생하기전에 대응하는 것을 의미합니다.

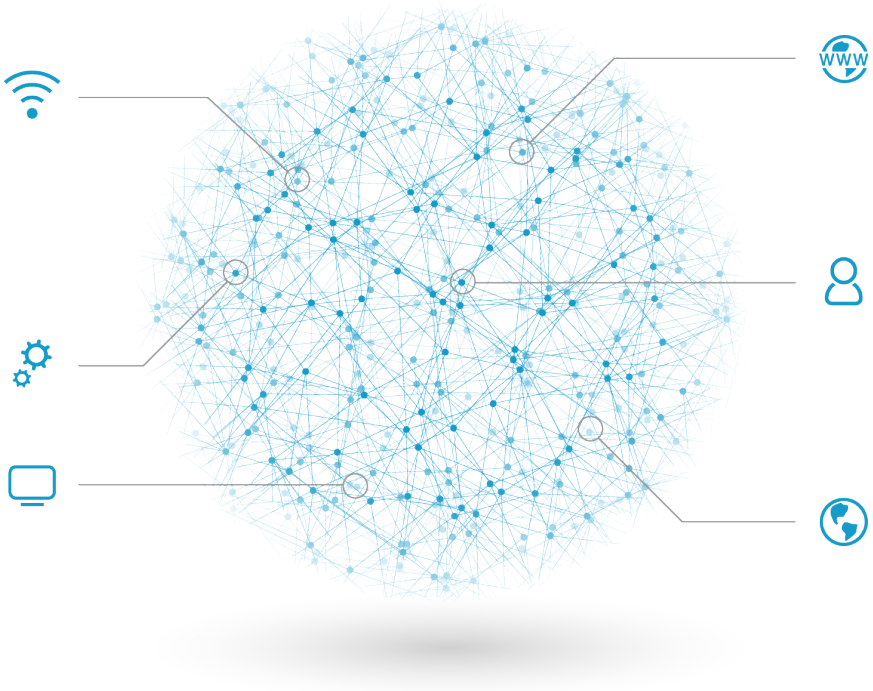


그룹 방어 : 공격에 대한 완벽한 방어

사이버리즌 헌팅 엔진은 스트리밍, 엔티티 상관 관계 분석을 수행하는 인메모리 데이터 저장소입니다. 헌팅 엔진은 매초 수백만 개의 데이터 조각을 가져오며 데이터 사이에 수천만 개의 관계를 분석하고 유지합니다.

헌팅 엔진은 빠르고, 확장할 수 있는 그래프 데이터베이스입니다. 그래프는 노드, 링크 및 속성을 사용하여 데이터와 해당 관계를 나타냅니다.

디스크에서 데이터를 검색하는 대신 메모리 내에서 실행됩니다. 메모리 작업은 디스크 요청보다 수천 배 빠른 속도로 수행되므로 헌팅 엔진이 훨씬 신속하게 쿼리에 응답 할 수 있습니다. 또한 최근의 컴퓨팅은 많은 양의 메모리를 비용 효율적으로 사용할 수 있게 하여 단일 시스템에서 대형 환경정보를 그래프로 표현할 수 있으며 여러 시스템이 함께 작동하여 데이터베이스 간 관계를 설정하고 표현할 수 있습니다.



©2018 Cybereason. All rights reserved.

악성 행위의 탐지와 시각화

헌팅 엔진은 끊임없이 진화하는 실시간 당신의 환경을 메모리 내에 유지하기 하기 위해 그 데이터에 대해서 매초마다 수만개의 쿼리를 수행하고 적응합니다.

예를들어 사이버리즌에서 수집하는 모든 요소(모든 사용자, 호스트, 프로세스, 네트워크 연결, 자동 실행 등등)가 헌팅 엔진에 공급됩니다. 요소 간의 관계는 링크를 사용하여 헌팅 엔진에 표시됩니다. 이러한 노드는 점점 더 많은 데이터가 헌팅 엔진에 공급됨에 따라 지속적으로 추가되며 더 많은 관계가 설정됩니다.

특정 사용자가 실행한 모든 프로세스를 이해하려는 경우에 헌팅 엔진은 해당 사용자와 그 사용자가 실행한 모든 프로세스 사이에 연결성이 있으므로 쉽게 처리 할 수 있습니다. 마찬가지로, 특정 프로세스에 의해 만들어진 모든 연결성을 이해하고자한다면 프로세스와 모든 네트워크 연결 사이에 연결성이 있기 때문에 이는 또한 간단하게 알수 있습니다.

과거에는 확장성 제약으로 발생하는 문제를 해결하기 많은 노력을 했습니다. 특히 관계형 데이터베이스는 부적절한 것으로 입증되었으며, 많은 사람들이 Hadoop®, 컬럼 데이터베이스 및 기타 NoSQL 엔진과 같은 기술을 사용하여 문제를 해결하려고 시도했습니다. 각각의 경우에 이러한 접근법은 데이터 처리, 분석 능력 및 스토리지 검색과 관련된 문제로 인해 확장할 수 없었습니다.

사이버리즌 헌팅 엔진은 악의적인 활동을 식별하고 논리적인 방식으로 확장하여 헌팅 엔진은 단순히 수집 된 데이터를 저장하지 않습니다. 사전 구성된 탐지 모델을 사용하여 공격자가 해킹 캠페인을 실행하는 동안 사용하는 악성 활동 및 도구, 전술 및 절차 (TTP)를 검색합니다. 당신은 룰을 구성하고 튜닝하는데 시간을 허비할 필요가 없습니다. 당신은 즉시 위협을 탐지할 수 있습니다.

©2018 Cybereason. All rights reserved.

사이버리즌 악성 활동 탐지 모델

이 모델은 공격의 초기 침입, C&C, 측면 이동, 권한 상승 및 정보 유출 또는 피해등 일련의 전체공격 라이프사이클 탐지 합니다. 사고를 가장 효과적으로 탐지하기 위해 사이버리즌은 아래와같이 수집하고 분석하는 데이터를 정의하고 구성합니다.



Facts는 사이버리즌 센서가 수집 한 원시 정보이며 프로세스, 사용자, 호스트, 메모리, 레지스트리 및 기타 이벤트의 변경을 결정하는 데 사용되는 상세한 정보입니다.



Evidence는 사이버리즌 헌팅 엔진이 흥미롭고 변칙적이거나 공격이 진행되고 있다고 암시하는 사실의 모음입니다. 추가적으로 연루된 데이터가 없을 경우에 분석가의 상세 조사를 필요로 하지는 않습니다.



Suspicions은 헌팅 엔진이 보다 악성일 가능성이 있다고 판단하는 활동입니다. 때로는 연결성이 없는 독립적인 의심스러운 활동일 수도 있으며 여러개의 관련 증거가 모여서 야기되는 경우도 있습니다. Suspicions가 되는 증거 판단의 임계치는 공격을 놓칠 가능성을 최소화하기 위해 의도적으로 낮습니다.



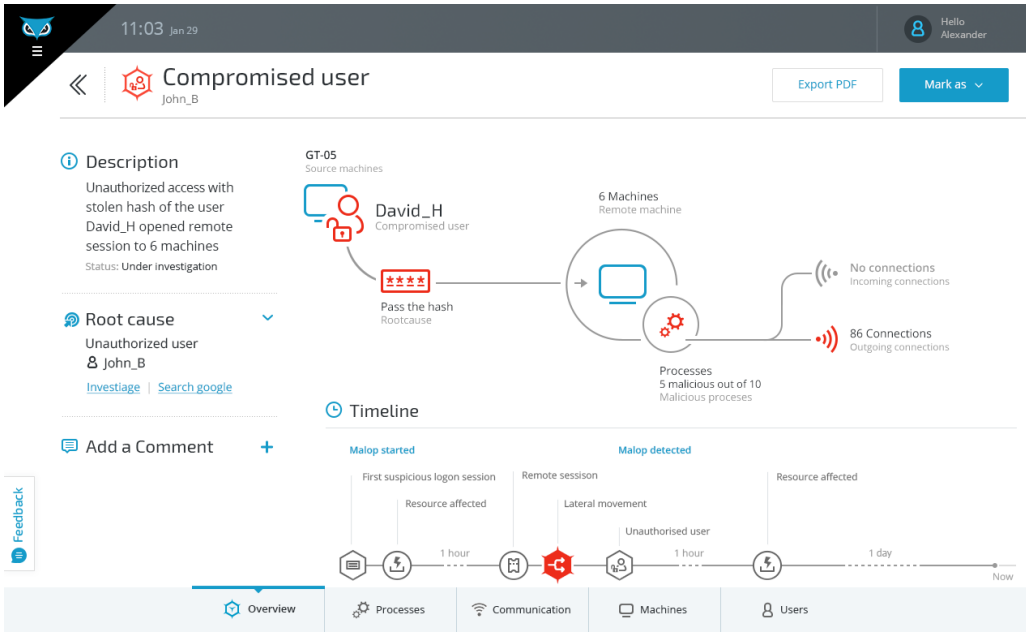
악의적인 조작 또는 "Malop"은 사이버 공격에 대한 완전한 스토리입니다. 전체 상황 분석가는 조직의 보안 사고를 식별해야합니다. Malop은 보안 사고의 일부일 가능성이 있는 의심스러운 활동의 모음입니다. Malop은 분석가가 불필요한 분석과 과탐에 허비하는 시간을 최소화하도록 고안되었습니다.

©2018 Cybereason. All rights reserved.

분석가에게 전체 컨텍스트 즉시 제공

헌팅 엔진은 수집하는 모든 데이터 간의 관계를 유지하기 때문에 Malop은 Malop이 경고를 발생시킨 전후의 상황을 정확하게 분석하기 위해 분석가가 드릴 다운 할 수있는 모든 관련 데이터 요소를 단일뷰에서 결합하여 나타냅니다.

또는 분석가가 다른 보안 솔루션에서 발생한 경고를 조사하고 특정 사용자, 컴퓨터, 프로세스 또는 네트워크 세션을 검색하는 경우 의심되는 문제가 진정으로 악의적인지 또는 양성인지를 전체 그림으로 신속하게 파악할 수 있습니다. 활동이 실제로 악의적인 경우 분석가는 모든 관련 요소의 그림을 쉽게 이해할 수 있습니다.
공격자가 한개의 경고를 발생시키면 헌팅 엔진은 공격 라이프 사이클의 모든 단계에서 언제 어떤 일이 일어 났는지에 대한 전체 이야기를 작성하여 제공합니다.



©2018 Cybereason. All rights reserved.

DISRUPT

THE ADVERSARY

LET THE HUNT BEGIN

cybereason

Cybereason은 사이버 공격에 대한 탐지 및 대응에 혁신적인 변화를 목적으로 전직 군인 사이버 보안 전문가 팀이 2012년에 설립했습니다. Cybereason Malop Hunting Engine은 빅 데이터, 행동 분석 및 머신러닝을 사용하여 시그니쳐 및 비 시그니쳐 공격을 식별합니다. 웹 대응 콘솔은 보안팀에게 공격 타임라인, 근본 원인, 억성 행위 및 도구, 영향을 받는 엔드포인트와 사용자는 물론 해커가 사용하는 인바운드 및 아웃 바운드 통신을 포함한 완벽한 공격 스토리를 직접 볼 수 있는 기능을 제공합니다 . 이를 통해 수동 조사가 필요 없어 보안팀의 응답 시간이 크게 단축됩니다. 이 플랫폼은 설치형 또는 클라우드 기반 서비스로 제공됩니다. Cybereason의 본사는 보스턴에 있으며 텔 아비브 및 도쿄에 사무소가 있습니다.

© All Rights Reserved. Cybereason 2018