위협(Threat) 인텔리전스로 공격자 저지

광범위하고 종합적인 위협 환경 뷰 제공

지금까지는 자체 환경에 존재하는 위협을 조사하거나 다크웹에서 최신 공격 수법을 조사하려면 많은 시간을 들여 수작업으로 많은 개별 데이터 포인트를 수집, 분석, 연결하여 실행가능한 인텔리전스를 도출해야 했습니다. 이로 인해 다음과 같은 문제가 발생합니다

데이터 과부하

여러 시스템에서 위협 관련 데이터 포인트를 일일이 수동으로 수집, 연결, 분석하여 잠재적인 영향을 파악하는 것은 숙련된 보안 분석가조차도 힘든 작업입니다. 수작업 조사는 분석가의 귀중한 시간을 소모하며, 결과물 또한 정적이고 불완전한 인사이트에 국한되는 경우가 대부분입니다.

커뮤니케이션 단절

위협 분석가는 고립된 환경에서 작업하는 경우가 많습니다. 간단하고 효율적인 방법으로 실시간 평가와 인사이트를 다른 팀과 공유하는 것도 불가능합니다. 이로 인해 협업 효율이 떨어지고 이중 작업과 시간 낭비가 발생합니다. 보안 팀이 대응을 가속화하고 정보에 입각한 의사 결정을 통해 위협을 줄이기 위해서는 관련 인텔리전스를 공유할 수 있는 보다 효과적이고 동적인 방법이 필요합니다.

불완전한 분석

위협(Threat) 인텔리전스 프로그램의 성패는 위협을 신속하게 탐지하고 검증하는 역량에 달려있습니다. 하지만 분석가가 의심스러운 지표를 수작업으로 조사하기에는 시간이 부족한 경우가 대부분입니다. 이로 인해 분석이 제대로 이루어지지 못하고 위협을 놓치는 경우가 발생하며 조직이 위협에 노출되고 중요 위협과 최신 위협을 제대로 파악하지 못하게 됩니다.

폐쇄적인 다크웹

딥웹(Deep Web), 다크웹, 폐쇄된 웹 사이트들은 중요한 정보 소스이지만 이러한 소스를 모니터링하고 수집하는 것은 위험하고 시간도 많이 소요됩니다. 또한 해당 소스 중 상당수는 액세스조차 어렵습니다. 보안 분석가는 정보를 찾는 데 소중한 시간을 투자하지만 필요한 정보의 극히 일부만 확인할 수 있습니다. 그 결과 중대한 위협에 대한 대응이 지연됩니다.

레코디드 퓨처: 고급 위협(Threat) 인텔리전스

레코디드 퓨처는 타의 추종을 불허하는 가장 많은 수의 일반 웹, 다크웹, 기술 소스를 광범위하게 탐색하고 정보를 수집합니다. 이를 통해 분석가는 수작업 조사 필요 없이 실시간 인텔리전스를 확보할 수 있습니다. 레코디드 퓨처는 또한 조직과 관련된 위협 환경에 대한 다이나믹하고 종합적인 뷰를 제공합니다. 따라서 분석가는 수작업에 대한 부담 없이 전문적인 작업에 주력할 수 있습니다.

레코디드 퓨처는 특허 받은 알고리즘 프로세스와 세계적인 수준의 연구원들이 수행하는 전문 분석을 통해 수십억 개의 엔티티를 검색하고 인텔리전스를 분류, 연결, 분석하여 정제된 실시간 인사이트를 제공합니다. 이러한 인사이트는 기존 보안 시스템에 손쉽게 통합되어 4가지 위협(Threat) 인텔리전스 주요 사용사례를 지원합니다.

지능형 위협 조사 및 보고

레코디드 퓨처의 특허받은 알고리즘 프로세스와 자연어 처리 기술은 모든 언어로 된 방대한 소스에서 데이터를 자동으로 수집하고 분석합니다. 이러한 고속 자동 분석에 세계적 수준의 레코디드 퓨처 연구팀 전문가들의 인사이트가 결합되어 분석가의 위협 조사 워크플로우에 추가됩니다. 레코디드 퓨처는 각각의 위협 행위자 또는 침해 지표에 대한 단일 뷰를 제공합니다. 분석가는 동적 위험 점수와 풍부한 컨텍스트를 기반으로 현재의 위험을 신속하게 평가할 수 있습니다. 또한 고급 검색, 실시간 경고, 데이터 시각화 기능을 통해 조사 및 보고서 작성에 도움이 되는 관련 인텔리전스를 확보할 수 있습니다. 보안 팀은 분석가 노트를 통해 인사이트와 평가를 기업 전반에서 공유함으로써 고립된 분석 환경에서 탈피할 수 있습니다.

레코디드 퓨처 활용

레코디드 퓨처에서 동종 업계 위협에 대한 전문가 분석을 검색하고, 인텔리전스를 시각화하고, 관련 Intelligence Cards™를 검토하고, 고급 쿼리를 통해 심층적으로 알아볼 수 있습니다. 레코디드 퓨처 보안 인텔리전스 플랫폼에서 위협 보고서 뿐만 아니라 분석가 노트를 생성하여 분석과 인사이트를 보안 팀 전체가 쉽게 공유할 수 있으며, 이를 기반으로 더욱 확실하고 정보에 입각한 의사결정을 내릴 수 있습니다.

고급 탐지 및 확인

레코디드 퓨처의 광범위한 수집 및 분석은 일반 웹과 다크웹, 기술 소스 전반의 데이터 포인트를 연결합니다. 이를 통해 공격자, 멀웨어, 관심 트래픽에 대한 중요한 컨텍스트를 제공합니다. 레코디드 퓨처 Intelligence Cards™는 위협 행위자나 지표에 대한 알려진 모든 정보를 한 곳에 중앙화함으로써 분석가가 스마트하고 신속하게 사고에 대응할 수 있도록 해줍니다. 또한 조직은 위협 헌팅 패키지로 고급 분석을 실행하여 이를 네트워크, 엔드포인트, 멀웨어 보안 솔루션에 간단히 추가할 수 있습니다. 그리고 YARA 및 SNORT 스크립트를 통해 자체 환경에 존재하는 위협을 식별할 수 있습니다.

레코디드 퓨처 활용

APT33과 같은 위협 행위자에 대한 레코디드 퓨처 위협 헌팅(Threat Hunting) 패키지를 엔드포인트 솔루션에 추가하여 조직 내 해당 위협 행위자 TTP에 대한 지속적인 실시간 모니터링과 상관분석을 수행하십시오. 이상 활동이 탐지되면 즉시 경고와 컨텍스트가 제공되어 사고 대응을 가속화할 수 있습니다.

다크웹 조사

수작업으로 다크웹에서 인텔리전스를 수집하고 분석하기란 시간, 전문성, 리소스 측면에서 거의 불가능합니다. 레코디드 퓨처는 해커, 범죄자, 극단주의 포럼을 비롯한 폐쇄적인 다크웹 소스들로부터 즉각적으로 인텔리전스를 수집하고 처리합니다. 레코디드 퓨처의 Insikt Group이 이러한 분석을 수행합니다. Insikt Group의 세계적인 수준의 분석가, 언어학자, 보안 연구원들은 오랜 정부 경험, 광범위한 업계 지식, 모국어 수준의 외국어 역량을 갖추고 있습니다. 그들의 연구와 레코디드 퓨처의 방대한 소싱 및 자연어 처리 기술이 결합되어 종합적이고 실행가능한 실시간 보안 인텔리전스를 제공합니다.

레코디드 퓨처 활용

고급 쿼리 빌더를 사용하여 다크웹 포럼에서 최신 익스플로잇 킷을 검색하십시오. 경고가 트리거될 때 이메일 또는 레코디드 퓨처 모바일 앱으로 경고가 발송되도록 쿼리 기반 경고를 설정할 수 있습니다. 보안 팀 전체 공지 전에 해당 익스플로잇 킷에 대한 추가 정보를 Intelligence Cards™로 쉽게 전환할 수 있습니다.

최신 공격을 방어하려면 실시간으로 업데이트되고 시의성있는 인사이트가 필요합니다. 레코디드 퓨처는 특허받은 알고리즘 프로세스와 세계적 수준의 전문가 분석을 결합하여 정제된 위협(Threat) 인텔리전스와 종합적인 위협 환경 뷰를 제공합니다. 분석가는 이를 통해 공격자를 저지하고 위험을 신속하게 감소시킬 수 있습니다.

주요 기능

- 광범위한 사이버 저장소와 10억 개 이상의 Intelligence Cards
- 기술 포럼, 공개 웹, 폐쇄 웹, 딥웹, 다크웹 소스를 모두 아우르는 방대하고 다양한 소스
- 광범위한 자동 수집과 세계적 수준의 전문가 분석이 결합된 실시간 보안 인텔리전스
- 맞춤 조사를 위한 고급 검색 기능
- 확실한 의사결정과 대응을 지원하는 동적 위험 점수 및 컨텍스트
- 멀웨어 규칙과 위협 헌팅 패키지가 포함된 레코디드 퓨처 전문 연구 그룹의 정제되고 완성된 인텔리전스 제공

주요 이점

IDC는 레코디드 퓨처가 조직에 다음과 같은 이점을 제공한다고 보고했습니다.

- 위협 식별 10배 가속화
- 영향을 받기 전에 22% 더 많은 위협 파악
- 보고서 작성에 소요되는 시간 34% 단축
- 보안팀 업무 효율 32% 증대

Recorded Future®

www.recordedfuture.com

@RecordedFuture

레코디드 퓨처 소개

레코디드 퓨처(Recorded Future)는 컨텍스트 기반의 실행 가능한 인텔리전스로실시간 의사결정을 지원하여 보안 및 IT 팀의 효율성을 강화하는 보안 인텔리전스를 제공합니다. 레코디드 퓨처는 일반 웹 사이트는 물론 다크웹과 딥웹까지 광범위한 소스의 데이터를 분석하여 위협 정보, 디지털 브랜드 위험, 취약점, 써드파티 위험, 지정학적 위험 등에 대한 단일 뷰를 제공합니다.