Recorded Future®

DATA SHEET

보안운영(SecOps) 인텔리전스 모듈

조사 및 대응 가속화, 간소화

과제

공격 표면(attack surface)이 늘어나면서 보안 운영 및 사고 대응 팀이 날마다 확인해야 하는 보안 경고 또한 폭증하고 있습니다. 하지만 시간과 정보가 부족한 상황에서 무엇을 먼저 처리해야 하는지 파악하고 위험을 최소화하는 것은 쉬운 일이 아닙니다. 보안 분석가 는 공개된 웹사이트와 다크웹에서 관련 데이터를 찾는 데 소중한 시간을 투자하지만 필요한 정보의 극히 일부만 확인할 수 있습니다. 그 결과 놓치는 위협이 발생하고 대응이 느려집니다.

솔루션

레코디드 퓨처 보안운영(SecOps) 인텔리전스 모듈은 보안 운영 및 사고 대응 분석가들이 수작업을 통한 조사 없이도 알려지지 않은 위협을 파악하고 정확하게 대응할 수 있도록 해줍니다. 레코디드 퓨처는 방대한 오픈 소스, 다크웹, 기술 소스로부터 인텔리전스를 자동으로 수집, 분석, 생성합니다. 그리고 여기에 세계적인 수준의 연구원들이 전문 지식을 결합하여 대응을 가속화하도록 지원합니다. 이러한 엘리트 보안 인텔리전스를 기존 SIEM, SOAR, IR, TIP 툴에 바로 추가하여 경고 분류와 위협 탐지를 강화할 수 있습니다.

보안운영(SecOps) 인텔리전스 모듈은 고위험 지표 데이터 세트를 제공하여 분석가가 심각한 위협을 비즈니스에 영향을 미치기 전에 조기에 식별할 수 있도록 해줍니다. 또한 방화벽, 프록시, 안티바이러스, 기타 보안 로그에서 관찰되는 내부 네트워크에 뛰어난 컨텍스트를 추가합니다.

보안 운영 및 사고 대응 분석가는 실시간 위험 점수와 지표 관련 증거를 토대로 신속하게 오탐을 걸러내고 우선적으로 처리해야 하는 경고를 파악할 수 있습니다. 또한 추가 조사가 필요한 경우에 자세한 정보를 손쉽게 파악할 수 있습니다. 레코디드 퓨처의 보안운영(SecOps) 인텔리전스 모듈은 수작업을 통한 정보 집계, 상관관계 분석, 분류의 필요성을 제거함으로써 분석가가 실제 위협을 탐지, 조사, 대응하는 데 걸리는 시간을 대폭 단축합니다.

이점

- 50% 더 많은 경고 검토
- 오탐 감소
- 이전에 탐지하지 못한 위협 탐지
- 기존 보안 도구 투자 효과 극대화

주요 기능

- 가장 광범위한 소스 커버
- 실시간 위험 점수 및 컨텍스트
- SIEM, SOAR, IR, TIP 즉시 통합
- 포털 홈 화면: 최신 위협 토픽, 전문 연구 확인

결과*

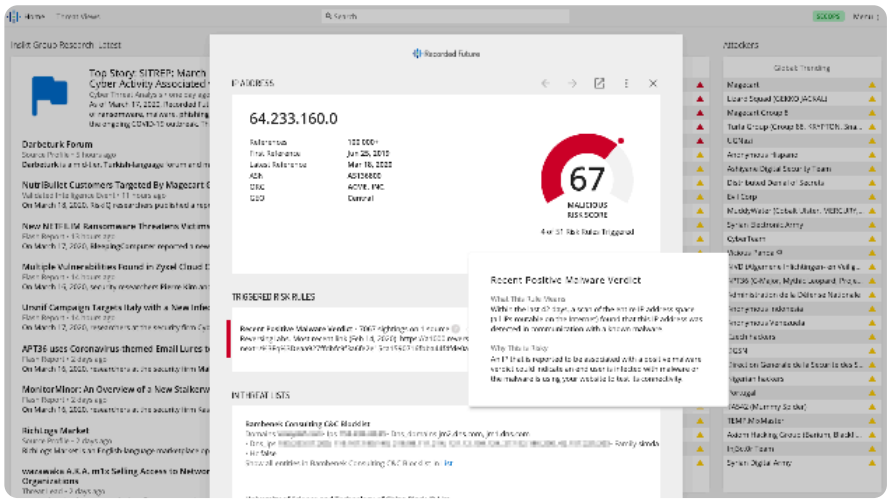
경고 선별 소요시간 32% 가속화
레코디드 퓨처의 보안운영(SecOps) 인텔리전스 모듈은 번거로운 수작업을 제거하며 단독으로 제공되는 위협 피드에 비해 훨씬 풍부한 컨텍스트를 제공합니다. 보안 운영 및 사고 대응 팀은 위험 점수와 주요 증거를 확인하여 신속하고 정확하게 결정을 내릴 수 있습니다.

피해 발생 전에 22% 더 많은 위협 식별
보안운영(SecOps) 인텔리전스 모듈은 위험 목록을 IP, 도메인, 해시, 멀웨어 관련 컨텍스트 및 내부 SIEM 데이터와 통합하고 상관 분석하여 정확한 위협 탐지와 신속한 대응을 지원하며 위험을 감소시킵니다.

**IDC 보고서에서 레코디드 퓨처가 어떤 비즈니스 가치를 제공하는지 자세히 확인해 보십시오.*

기능

- 10억 개 이상의 지표에 대한 종합적인 인텔리전스와 실시간 위험 점수
- 온라인 포털, 모바일 앱, 브라우저 확장, 보안 솔루션 통합 등 다양한 방식으로 인텔리전스 액세스
- 홈 화면 대시보드에서 최신 위협 소식, 전문 리서치 확인
- 주요 SIEM, SOAR, IR, TIP 등과 즉시 통합
- 전문가 인텔리전스 조사 보고서: 웹 포털에서 바로 확인 및 정기적인 고객 커뮤니케이션을 통해 제공
- 온보딩, 교육, 지속적인 지원을 위한 세계적 수준의 보안 인텔리전스 전문가 팀



Intelligence Card: 위험 점수, 전문 분석, 오리지널 소스 등 IP 주소에 대한 종합적인 인텔리전스를 보여줍니다.

레코디드 퓨처 소개

레코디드 퓨처(Recorded Future)는 세계 최대 엔터프라이즈 보안 인텔리전스 제공업체입니다. 레코디드 퓨처는 지속적이고 광범위한 자동 데이터 수집 및 분석에 전문가 분석을 결합하여 적시에 정확하고 실행 가능한 인텔리전스를 제공합니다. 레코디드 퓨처는 끊임없이 증가하는 혼란과 불확실성의 세계에서 조직이 위협을 신속하게 파악하고 탐지하는 데 필요한 가시성을 제공합니다. 조직은 이러한 가시성을 확보함으로써 선제적 대응을 통해 공격을 저지하고 사용자, 시스템, 자산을 보호하여 비즈니스를 안정적으로 수행할 수 있습니다. 레코디드 퓨처는 전세계 1,000개 이상의 기업과 정부 기관에서 신뢰받고 있습니다.

www.recordedfuture.com @RecordedFuture