Recorded Future®

보안운영(SecOps) 인텔리전스로 공격자 저지

신속한 조사와 대응으로 조직 방어

공격 표면(attack surface)이 늘어나면서 보안 운영 및 사고 대응 팀이 날마다 확인해야 하는 보안 경고 또한 폭증하고 있습니다. 이로 인해 보안 분석가의 경고 피로가 누적되고 있으며, 내부 환경에 대한 정보만으로는 조직을 겨냥한 진짜 위협을 식별하고 분류, 대응하기가 어려운 상황입니다. 문제는 다음과 같습니다.

너무 많은 경고, 부족한 시간

수천개의 개별적인 원시 데이터(raw data)를 조사하는 것은 숙련된 보안 분석가조차도 힘든 작업입니다. 시간이 부족하고 정보가 제한된 상황에서는 어떤 경고가 중대한 사고를 나타내는지, 어떤 것이 중복된 경고이고 오탐인지를 파악하기 어렵습니다. 따라서 무의미한 경고들을 걸러내는 데 귀중한 시간을 낭비하고 정작 중요한 경고를 놓칠 수 있습니다.

외부 상황에 대한 정보 부족

컨텍스트와 무관한 위협 데이터 피드와 개별 시스템들로부터 내부 경고를 받을 경우, 올바른 의사결정에 필요한 중요한 외부 위협 정보가 누락될 수 있습니다. 외부 위협 지표를 사용하더라도 무료 피드, 검증되지 않은 소스 등은 신뢰성이 떨어지며 오탐과 사각지대를 유발할 수 있습니다.

수작업 탐지

자사 및 동종업계 관련 외부 위협을 수작업으로 검색하는 것은 많은 시간이 소요될 뿐만 아니라 비효율적입니다. 보안 분석가는 공개된 웹 사이트와 다크웹에서 관련 데이터를 찾는 데 소중한 시간을 투자하지만 필요한 정보의 극히 일부만 확인할 수 있습니다. 그 결과 진짜 위협에 대한 대응이 지연됩니다.

비효율적인 차단 방식

위협 지표가 계속 증가하고 변화하기 때문에 네트워크 경계에서 방화벽, 이메일 보안, 엔드포인트 솔루션으로 진짜 위협을 식별하고 차단하기가 매우 어렵습니다. 또한 오탐으로 인한 빈번한 차단은 비즈니스 운영을 방해하고 직원 생산성을 저해합니다.

레코디드 퓨처:
고급 보안운영(SecOps) 인텔리전스

레코디드 퓨처는 방대한 데이터에서 광범위한 수집과 분석을 통해 신속한 위협 대응에 필요한 고급 보안 인텔리전스를 생성합니다. 레코디드 퓨처는 실시간으로 계속 업데이트되는 중앙 인텔리전스를 제공함으로써 보안 운영 및 사고 대응 분석가들이 알려지지 않은 위협을 파악할 수 있도록 해줍니다. 분석가는 레코디드 퓨처 솔루션을 통해 수작업 검색 필요 없이 실행 가능한 컨텍스트를 즉시 확인하여 정확하게 대응할 수 있습니다.

레코디드 퓨처는 특허 받은 알고리즘 프로세스와 세계적인 수준의 연구원들이 수행하는 전문 분석을 통해 방대한 범위의 오픈 소스, 다크웹, 기술 소스, 조사 보고서를 검색합니다. 이를 통해 정제된 실시간 인사이트를 모든 언어로 제공합니다. 이러한 인사이트는 기존 보안 시스템에 통합되어 보안 운영 및 사고 대응을 위한 4가지 주요 사용사례를 지원합니다.

경고 선별 분류

레코디드 퓨처는 모든 언어로 된 방대한 소스를 검색하고 분석합니다. 이를 통해 제공되는 고급 인텔리전스와 주요 컨텍스트는 분석가가 실시간으로 업데이트되는 위험 점수와 명확한 증거를 기반으로 경고를 선별할 수 있도록 해줍니다. 따라서 분석가는 신속하게 오탐을 가려내고 가장 중대한 위협을 식별하여 즉각적으로 대응할 수 있습니다. 또한 10종 이상의 SIEM 및 SOAR과 신속하게 통합되어 기존 보안 솔루션에 실시간 보안 인텔리전스를 추가할 수 있습니다.

레코디드 퓨처 활용

레코디드 퓨처는 기존 SIEM 또는 SOAR 솔루션에 즉시 통합되어 실시간 인텔리전스를 강화합니다. 또한 우선순위에 따른 사고 에스컬레이션, 문제 해결 가속화, 분석가의 시간 절약에 필요한 컨텍스트를 제공합니다.

위협 탐지

보안 담당자는 매일 수많은 경고를 처리합니다. 그 중 대부분은 내부 네트워크 데이터와 관련 있는 외부 데이터를 기반으로 합니다. 그러나 해당 데이터에 컨텍스트나 시의성이 결여되어 있다면 해답 없는 경고만 쌓이게 됩니다. 레코디드 퓨처는 광범위한 수집과 분석을 통해 IP, 도메인, 해시, 멀웨어, 취약점에 대한 위험 목록과 중요한 컨텍스트를 제공함으로써 탐지와 자동 대응을 가속화하고 위험을 감소시킵니다.

레코디드 퓨처 활용

내부 데이터를 레코디드 퓨처 인텔리전스 및 위험 점수와 자동 매칭하여 잠재적 위협을 신속하게 파악하십시오. 레코디드 퓨처는 방화벽, 이메일 보안, 엔드포인트 솔루션의 내부 네트워크 관측에 중요한 컨텍스트를 추가함으로써 위협을 조기에 탐지하고 신속하게 대응할 수 있도록 해줍니다.

위협 방지

지표가 폭증하고 있는 상황에서 실행 가능한 인텔리전스를 제공하기 위해서는 위협 피드의 신뢰도와 충실도가 높아야 합니다. 레코디드 퓨처 Security Control Feeds는 조직이 대응을 자동화하고 위협을 선제적으로 방어하는 데 필요한 고품질 지표와 컨텍스트를 제공합니다. 조직은 추가적인 데이터 보강 필요없이 증거 기반 정보를 사용하여 방화벽, 이메일 보안, 엔드포인트 솔루션에서 고위험 지표를 자동으로 차단할 수 있습니다. 또한 맞춤 위험 피드를 써드파티 제품에 통합하여 에지(edge)에서 더 많은 위협을 차단하고 오탐으로 인한 차단을 최소화할 수 있습니다. 아울러 사고 대응을 자동화하고 전반적인 보안 태세를 향상시킬 수 있습니다.

레코디드 퓨처 활용

레코디드 퓨처 Security Control Feeds를 기존 경계 보안 솔루션에 통합하면 오탐을 줄이면서 고품질 경고 및 차단 목록을 생성할 수 있습니다. 악성 위협이 탐지되면 이메일 또는 레코디드 퓨처 모바일 앱을 통해 알림을 수신하고 엔드포인트 또는 방화벽에서 확인된 액티브 상태의 지표를 차단할 수 있습니다.

실시간으로 업데이트되는 인사이트는 보안 운영 및 사고 대응 팀에 적시에 적절한 정보를 제공하여 공격자를 저지하고 조직의 피해를 방지합니다. 정교한 알고리즘과 세계적 수준의 전문가 분석이 결합된 레코디드 퓨처 솔루션은 보안 분석가가 경고를 쉽게 탐지하고 해결하여 위험을 최소화할 수 있도록 지원합니다.

주요 기능

- 10억 개 이상의 Intelligence Cards™
- 공개 사이트, 다크웹, 기술 포럼 전반을 검색하여 실시간 위험 점수와 증거 제공
- 증거 기반의 탐지 및 차단 등급 지표
- Intelligence Goals Library에서 사용자 조직과 관련된 실시간 경고 제공
- 10여 가지 이상의 SIEM 및 SOAR과 신속하게 통합

주요 이점

- 50% 더 많은 경고 검토
- MTTD 향상: 10배 빠른 위협 파악
- MTTR 향상: 위협 해결 63% 가속화
- 영향을 받기 전에 22% 더 많은 위협 파악
- 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.