Recorded Future®

취약점(Vulnerability) 인텔리전스로 공격자 저지

주요 취약점을 신속하게 파악하여 우선 대응 실행

취약점은 비즈니스를 공격의 위험에 빠뜨립니다. 날마다 새로운 취약점이 출현하기 때문에 모든 것, 모든 곳을 다 패치하는 것은 불가능합니다. 그래서 대부분의 보안 팀과 IT 운영 팀이 우선순위에 따라 취약점을 선별하고 패치하는 데 많은 시간과 자원을 소비하고 있습니다. 위험을 줄이기 위해 어디에 치료 노력을 집중할 것인지 효과적으로 판별하지 못한다면 다음과 같은 과제에 직면하게 됩니다.

쏟아지는 취약점, 부족한 컨텍스트

IT 운영 팀은 전통적인 자산 중요도 및 심각도[1]에 따라 분류된 막대한 수의 취약점에 압도당하고 있습니다. 2019년 한 해에만 17,000개 이상의 새로운 취약점이 게시되었습니다. 이 중 거의 60%가 심각도가 높거나 매우 중요한 것으로 분류되었습니다. 대부분의 조직이 이러한 심각도 수준을 기준으로 패치를 실행합니다. 하지만 실제로 악용(exploit)되는 것은 전체 취약점 중 5.5%에 불과합니다.[2] 따라서 익스플로잇 정보에 대한 컨텍스트가 없으면 기업은 위험도가 낮은 취약점을 패치하는 데 자원을 낭비하고 정작 가장 중요한 취약점을 간과하게 됩니다.

제한된 가시성

NIST(National Institute of Standards and Technology)의 NVD(National Vulnerability Database)에 아직 게시되지 않은 취약점에 대해서는 대부분의 조직이 거의 알지 못합니다. 취약점이 처음 발생하고 NVD에 최초로 게시되기까지의 지연으로 인해 조직은 자체 환경에서 어떤 영역이 위험에 처해 있는지 파악하기 어렵습니다. 설상가상으로 조직 내에 어떤 취약점이 존재하고 아직 패치되지 않은 것이 무엇인지 추적하는 것도 쉽지 않습니다. 이로 인해 공격자에게 허점을 노출하게 됩니다.

부족한 시간

위협 행위자들의 취약점 익스플로잇 속도가 계속 빨라지고 있습니다. 오늘날 취약점이 발견된 후 익스플로잇이 출현하기까지 약 15일이 걸립니다. 즉, 보안 팀이 새로운 취약점에 대응하기 위해 시스템을 패치하거나 피해 완화 계획을 수립할 수 있는 시간이 약 2주 밖에 없다는 뜻입니다.

[1] https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/2020_VT_Trends-Report-reduced.pdf
[2] https://www.zdnet.com/article/only-5-5-of-all-vulnerabilities-are-ever-exploited-in-the-wild/

Recorded Future®

레코디드 퓨처:
컨텍스트화된 인텔리전스로 대부분의 위험을 감소시킴

레코디드 퓨처는 활성화된 익스플로잇과 익스플로잇 킷 가용 여부를 기반으로 취약점 위험 점수를 실시간 제공합니다. 이를 통해 IT 운영 팀이 패치 우선 순위를 정하고 공격을 방지하는 데 필요한 컨텍스트를 제공합니다. 위험 점수를 매기는 데 사용되는 소스를 투명하게 공개하여 더욱 빠르고 정확한 결정을 내릴 수 있도록 지원합니다.

레코디드 퓨처는 정교한 알고리즘과 세계적 수준의 전문가들의 분석을 통해 타의 추종을 불허하는 방대한 오픈 소스, 다크웹, 기술 소스, 자체 조사를 종합합니다. 레코디드 퓨처는 실시간으로 인텔리전스를 연결, 분류, 업데이트하여 손쉽게 다른 보안 도구와 통합되어 다음과 같은 취약점 관리 사용 사례를 지원하도록 해줍니다.

취약점 우선순위 지정

취약점 관리 팀이 신속하고 정확한 결정을 내리기 위해서는 취약점으로 인한 실제 위협과 패치 실행에 따른 지장을 빠르게 평가할 수 있는 방법이 필요합니다. 이를 위해 레코디드 퓨처는 모든 언어로 된 가장 방대한 소스에서 자동으로 데이터를 수집하고 분석합니다. 실제 익스플로잇 가능성을 기반으로 한 실시간 위험 점수는 이미 무기화되었거나 무기화될 가능성이 있는 취약점을 파악하여 우선적으로 패치하고 신속하게 위험을 줄일 수 있도록 해줍니다. 각 점수가 산정된 이유를 완전히 공개하여 기업이 꺼릴 수 있는 미션 크리티컬 패치에 대한 합당한 근거를 제공합니다.

단일 창에서 취약점 상세 정보를 통해 실시간으로 취약점 익스플로잇 및 무기화 상황을 모니터할 수 있습니다. 주요 취약점 관리 시스템과 바로 통합되므로 레코디드 퓨처의 엘리트 인텔리전스를 간편하게 활용하여 기존 워크플로우 내에서 빠른 조사와 우선 순위 분류가 가능합니다.

레코디드 퓨처 활용

귀사 환경에서 취약점을 스캔하십시오. 취약점 스캔 데이터와 함께 레코디드 퓨처의 실시간 위험 점수와 증거를 바로 확인하십시오. 고위험 취약점을 신속하게 선별하고 패치를 실행하여 위험을 최대한 줄일 수 있습니다. 또한 레코디드 퓨처 브라우저 확장 프로그램을 통해 CVE와 실시간 컨텍스트를 조사하고 중요한 오프사이클 패치에 대해 위험 기반의 정확한 결정을 내릴 수 있습니다.

기술 스택 내 취약점 모니터링

레코디드 퓨처는 기술, 산업, 회사 등을 기반으로 새로운 취약점에 대한 필수적인 실시간 컨텍스트를 제공합니다. NVD에 등재되기 약 11일 전에 새로운 익스플로잇을 실시간으로 파악합니다. 조직은 자산에 직접적인 영향을 미치는 새로운 취약점에 대한 실시간 경고를 수신하고 심층 분석과 우선 순위 지정을 위해 컨텍스트와 증거를 활용할 수 있습니다. 또한 보안 분석가가 수정 조치를 기록할 수 있으므로 조직 내 다른 사용자들이 패치 적용 여부를 쉽게 파악할 수 있습니다.

레코디드 퓨처 활용

레코디드 퓨처의 왓치리스트에 귀사의 핵심 기술을 추가하십시오. 기존 인프라에서 새로운 취약점이 발견되면 NVD에 게시되기 전이라도 이메일이나 레코디드 퓨처 모바일 앱을 통해 경고를 수신하고 위험 완화 조치를 취할 수 있습니다.

취약점 위험의 모니터링, 우선순위화, 대응을 위한 전략적인 접근을 실행하십시오. 레코디드 퓨처의 엘리트 보안 인텔리전스는 실시간으로 업데이트되는 인사이트를 통해 보안 팀과 IT 운영 팀에 필요한 취약점 정보를 적시에 제공하고 새로운 공격을 선제적으로 방어하도록 지원합니다.

주요 기능

- 익스플로잇 트렌드 기반의 위험 점수와 증거를 제공하여 빠르고 확실한 결정 지원
- 상세한 증거와 컨텍스트로 패치 정당화
- NVD 게재 약 11일 전에 취약점에 대한 인텔리전스 제공
- 레코디드 퓨처 브라우저 확장 프로그램을 통해 다양한 웹 기반 리소스에서 즉시 인텔리전스 액세스 가능
- ServiceNow Vulnerability Response와 같은 주요 취약점 관리 솔루션과 통합

주요 이점

IDC는 레코디드 퓨처가 조직에 다음과 같은 이점을 제공한다고 보고했습니다.

- 위협 식별 10배 가속화
- 전반적인 보안 팀 효율성 32% 증대
- 응답 시간 63% 향상
- 계획되지 않은 다운타임 86% 감소

www.recordedfuture.com

@RecordedFuture

레코디드 퓨처 소개

레코디드 퓨처(Recorded Future)는 컨텍스트 기반의 실행 가능한 인텔리전스로 실시간 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.