IBM Security Randori Recon: 공격 표면 관리

공격자 관점에서 공격의 표면을 관리하세요.

Randori™

공격자가 공격하기 좋은 위치를 알아내려면, 먼저 공격자의 시선으로 공격 표면을 보는 방법을 알아야 합니다.
IBM Security Randori Recon은 지속적으로 자산을 조사하고 공격자의 관점에서 이슈의 우선순위를 제공합니다.

공격표면이란?

기업 또는 조직의 공격 표면은 인터넷을 통해 접속 가능한 하드웨어, 소프트웨어, SaaS와 클라우드 자산으로 정보를 활용하고 저장하는 곳을 의미하며, 공격자에 의해서도 확인될 수 있는 지점을 의미합니다. 이 의미는, 공격 표면은 외부 자산 중 공격자에 의해 확인되고 공격이 가능한 지점을 의미하며, 이 지점을 발판으로 내부 환경으로의 공격에 활용될 수 있는 자산을 의미합니다.

공격표면관리 필요 이유

69%
의 조직이 인지하지 못한 외부 자산으로 인해서 침해가 발생되고 있음

73%
의 조직이 엑셀을 통해서 기업의 공격 표면(자산)을 관리하고 있음

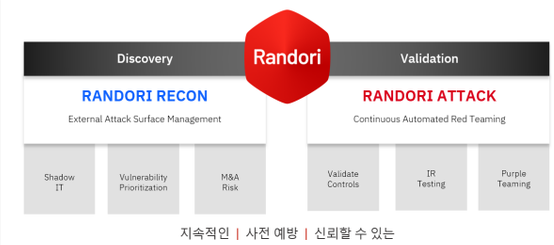
80시간+
공격 표면에 대해 인지하는 데까지 걸리는 시간

ESG, Security Hygiene & Posture Management Survey - 2H2021

IBM Security Randori

IBM Security Randori Recon은 공격 표면 관리 (Attack Surface Management)를 하나의 통합된 플랫폼으로 제공하여 지속적이고 적극적으로 진정한 공격 표면 관리 경험을 제공합니다. 클라우드 전환, 쉐도우 IT, 인수 합병 (M&A) 등을 통해 기업은 끊임없이 변화 하고 있습니다. 이러한 변화는 공격자에게도 기회가 됩니다. 기업의 변화로 인해 발생할 수 있는 위협을 Randori Recon으로 발견하십시오. IBM Randori Recon는 별도의 설치 또는 구성없이 공격 표면을 탐지합니다. 진짜 공격자의 입장에서 Randori Recon은 외부 공격 표면을 지속적으로 모니터하여, 눈에 보이지 않는 지점(blind Spot), 잘못된 구성, 그리고 그렇지 않으면 놓칠 수 있는 프로세스 실패를 감시합니다. Randori Recon은 블랙박스 분석을 통해 놓치기 쉬운 IPv6관련 자산 과 클라우드 자산까지 찾아냅니다. Randori는 자산 검색, 분류 및 우선 순위 지정, 문제 해결, 모니터링이라는 4가지 핵심 프로세스로 구성됩니다. 이를 통해 끊임없이 변화하는 디지털 공격 표면의 크기와 형태를 자동화된 방식으로 지속적으로 모니터링합니다. 이를 통해 보안 팀이 공격표면에 노출되어 있는 자산을 완벽하게 파악하고 이에 관한 최신 목록을 유지하도록 지원합니다.

위협 가능성 발견과 검증을 위한 통합 공격 보안 플랫폼



IBM Attack Surface Management – Randori Recon

- Randori는 사용자가 공격자의 관점을 이해할 수 있도록 지원
- 공격자가 실제 공격대상을 설정하고 공격에 활용하는 기술을 적용하여 활용
- 지속적이고 자동화된 공격 보안 플랫폼을 고객에게 제공
- 고객은 외부에 노출된 부분을 이해하고 실시간으로 방어를 최적화 하는데 사용

IBM Security Randori Recon 주요 특징

- **진정한 발견** 공격자는 인터넷 전체를 스캔하는 것으로 시작하지 않으며, 우리도 마찬가지입니다. 공격자와 같은 기술을 사용하여 놓치기 쉬운 IPv6및 클라우드 자산을 발견합니다.
- **지속적인 인사이트 확보** Randori는 항상 새로운 자산과 공격 표면의 변화를 찾고 있습니다. 공격자 트렌드에 기반하여 업데이트 되는 특허 출원 중인 목표 유혹 모델 (Target Temptation Model)과 IBM Randori Attack 데이터를 이용하여 문제를 빠르게 식별합니다.
- **적극적인 대응** 공격이 발생하기 전에 무엇이 노출되었는지, 어떠한 위험이 있고, 무엇을 해야 하는지 이해하십시오. 증거가 필요하십니까? Randori Attack과 함께 위험을 확인합니다.

1 공격 유효성 분석

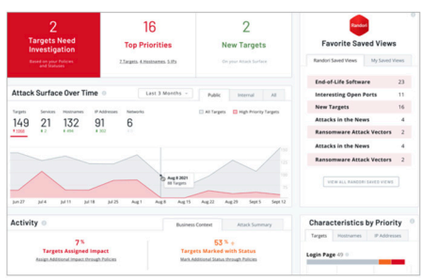
Target Temptation이 하는 것:

- 공격 표면을 공격자의 입장에서 관찰
- 위험 기반 취약점 관리 기법 적용
- 공격가능성에 따른 위험 평가
- 새로운 공격에 따르게 대응

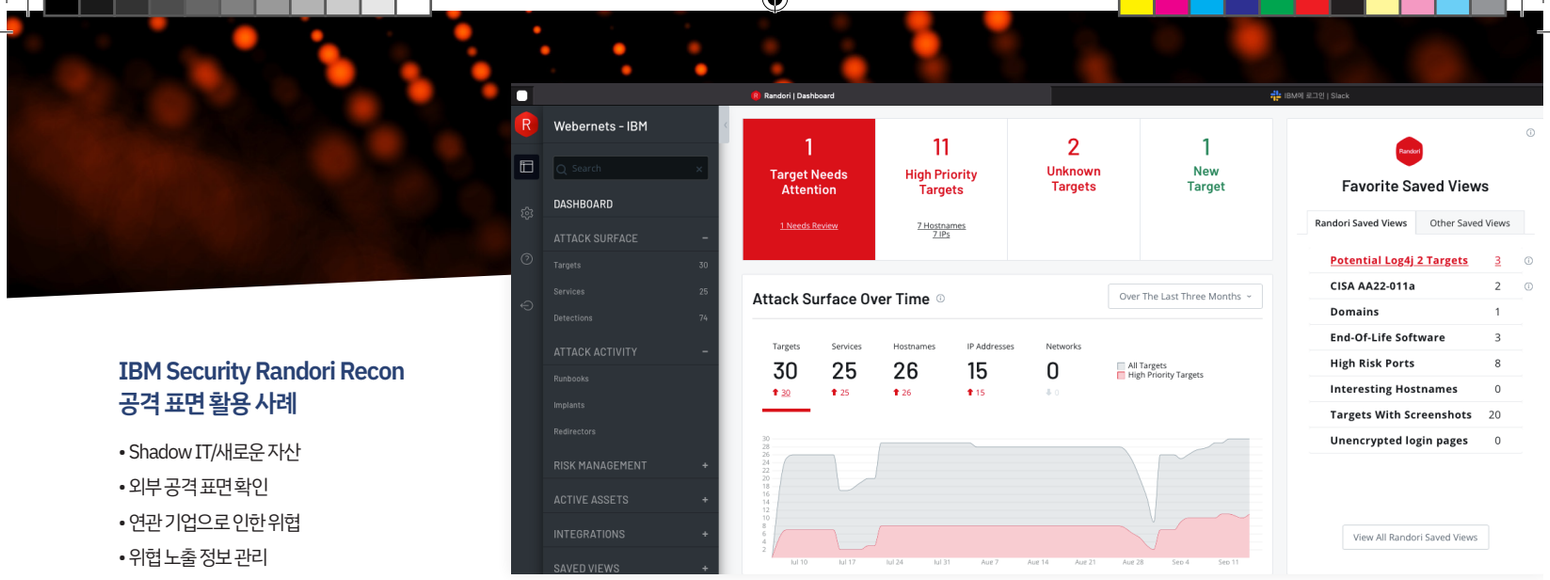
2 분석 정보 제공

Randori Demo my Data (DMD) 보고서 :

- 외부 공격 표면과 위험에 대한 관점 제공
- 중요하고 위험도 높은 이슈를 빠르게 확인하고 조치하도록 지원
- 공격자의 관점을 제공(Randori Target Temptation 엔진)



3 Randori 정보 수집 방안



IBM Security Randori Recon 공격 표면 활용 사례

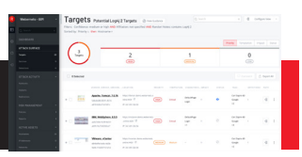
- Shadow IT/새로운 자산
- 외부 공격 표면 확인
- 연관 기업으로 인한 위협
- 위협 노출 정보 관리
- 위험 기반 취약점 관리

Shadow IT/새로운 자산 확인

문제점 CMDB와 자산 관리 솔루션은 이미 알고 있는 자산에 대한 부분만 확인하고 관리할 수 있음

위협 상황
- 30%의 외부 노출 자산에 대해 보안 팀에서는 모르고 있음
- 1/3의 유출이 이런 Shadow IT에서 발생

Randori 역할
- 공격자의 시선으로 위협을 확인
- Randori 역량을 통해 다른 분석에서 놓칠수 있는 부분을 분석
- Shadow IT 분석을 통해서 모르는 자산에 집중
- 새롭게 발견된 자산을 실시간으로 확인

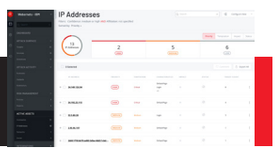


위협 관련 사항 관리 (예:Log4J)

문제점 문제 발생시 매 초가 중요한 상황, 관리자 및 보안팀은 빠르게 상황을 파악하고 대응할 수 있어야 함

위협 상황
- 공격이 발생하고 나서 인지하는 것은 의미가 없음
- 새로운 위협이 발생하는 경우 외부 노출 자산에 대한 파악이 중요

Randori 역할
- 최신의 위협에 노출된 환경을 분석
- 고객의 위협 환경을 최고의 해커 시각에서 분석
- 공격이 발생하기 전에 조치하도록 지원
- 새로운 공격에 대한 대응 사항 검증

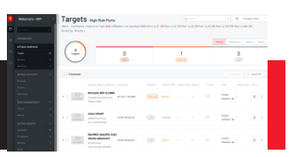


공격 표면 분석

문제점 기업의 공격 표면에 대한 전체 환경을 이해하고 확인하는데까지 오랜 시간이 소요됨

위협 상황
- 공격 표면은 지속적으로 변화되는데 반해 현재의 접근방식은 정적 데이터만을 분석하려고 함
- 전체 환경을 파악하는데 80시간 이상이 필요
- 파악이 되었을때 분석 환경은 이미 시효가 만료된 상태이고 침해를 당했을 위험이 존재(Log4j - 48 시간)

Randori 역할
- 지속적으로 공격 표면에 대한 가시성을 제공
- 변경 내역 확인, 자산 모니터링, 위험 관리



위험 기반 취약점 관리

문제점 패치는 중요 도구 중의 하나이지만 투자 이익율의 측면은 계속 나빠짐

위협 상황
- 새로운 취약점은 계속해서 나옴
- 20개의 취약점이 나올 때 단 하나 취약점 만이 악용됨

Randori 역할
- 취약점 관리팀에서 외부 위협 사항을 빠르게 파악하도록 지원
- Randori의 위협 분석 알고리즘(Target Temptation)을 통해 우선 위협 대응 관련 사항을 분류
- 공격이 확실하지 않은 항목에 대한 우선순위를 낮춤
- Randori Attack을 통해서 접속의 효율성 확인

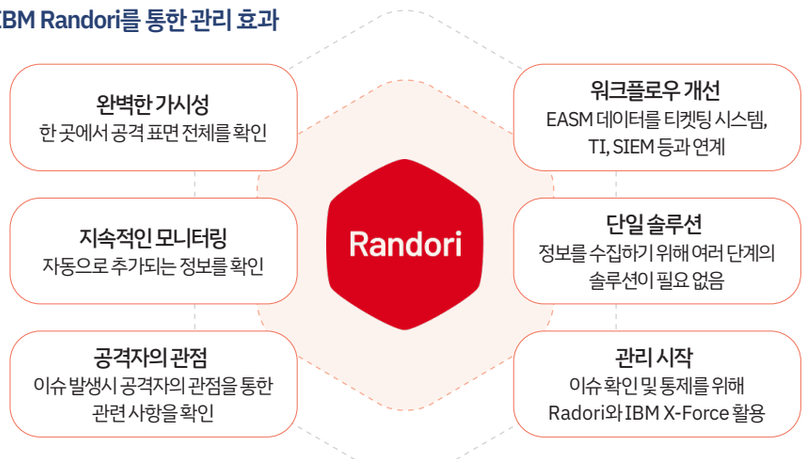
IBM Security Randori 혜택

1 알려지지 않은 위험 발견
공격자의 관점에서 잘못된 구성이나 프로세스 장애에 노출된 공격자처럼 파라미터를 발견합니다.

2 발견 사항에 대한 우선 순위 결정
공격자의 최상위 목표를 해커의 로직 기반으로 특허 출원중인 모델로 정확히 집어 냅니다.

3 공격 표면의 감소
쉐도우 IT, M&A, 예측하지 못한 변화에 한 발 앞서 새로운 위험을 알려줍니다.

IBM Randori를 통한 관리 효과



관련문의: IBM 보안 사업부 최교영 과장 (kyoyoung.choi@ibm.com / 02-3781-5090)