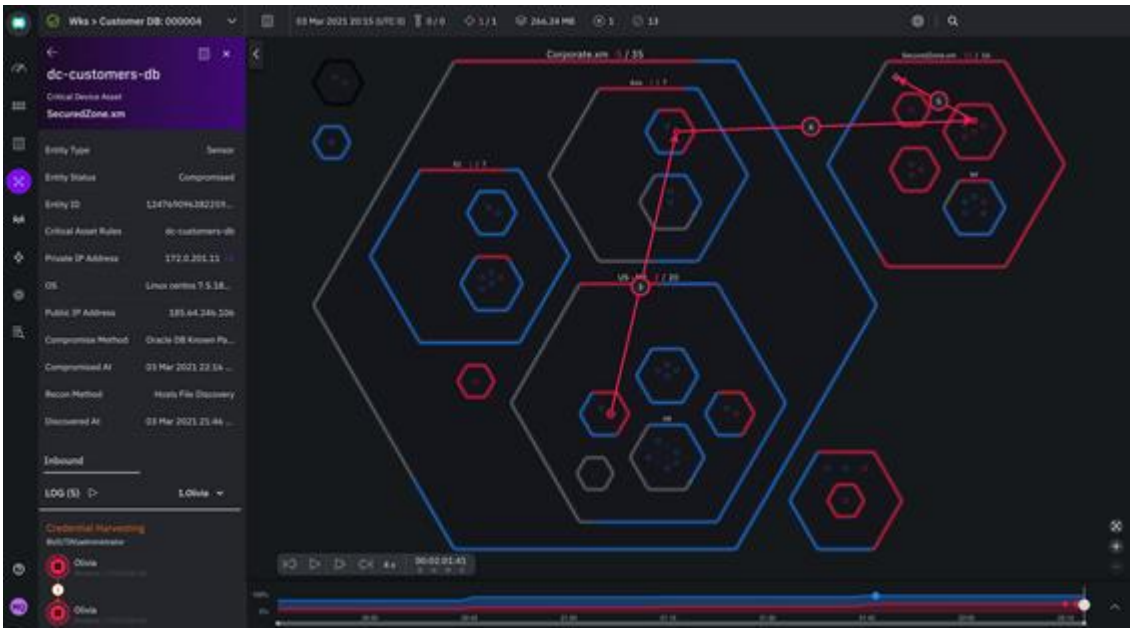
XM Cyber

XM Cyber는 고유한 위반 추정 방법론을 가지고 있습니다. 우리는 공격자가 가장 최적화된 보안 구성도 우회할 수 있으며 오늘날의 복잡하고 동적인 하이브리드 인프라에서는 이러한 손상이 불가피하다는 것을 알고 있습니다. 그러나 초기 거점보다 더 중요한 것은 공격자가 온프레미스 또는 클라우드 환경 내부에 있을 때 무엇을 달성할 수 있는지 이해하는 것입니다. 예를 들어……

- 내 환경의 장치가 랜섬웨어에 의해 손상된 경우 해당 공격의 폭발 반경은 얼마입니까?
- 내 네트워크의 어느 정도가 손상될 수 있습니까?
- 중요한 비즈니스 애플리케이션이 손상될 수 있습니까?
- 이 위험을 제거하거나 줄이기 위해 무엇을 할 수 있습니까? 어디서, 가장 적은 노력으로 가장 큰 보상을 얻을 수 있습니까?

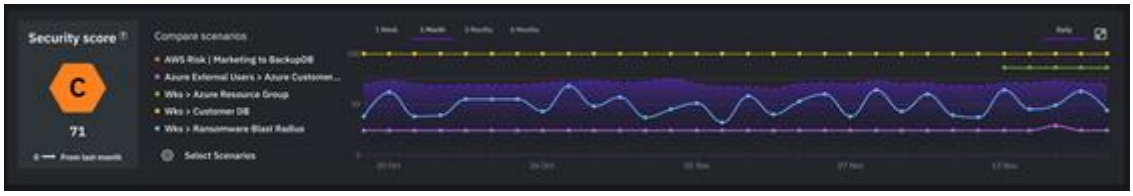
XM Cyber는 프로덕션 환경에 영향을 주지 않고 이러한 질문에 연중무휴로 지속적이고 안전하게 답변합니다. 전체 하이브리드 네트워크에서 모든 중요한 공격 경로에 대한 포괄적인 단일 보기를 제공하고 위험을 줄이는 데 가장 큰 영향을 미칠 수 있는 위치로 리소스를 보낼 수 있습니다.



특히 XM이 미래에 잠재적으로 가져올 수 있는 가치를 보여주는 다음 사용 사례를 확인했습니다.

- **Segmentation:** 공격자가 위치 A에서 위치 B로 이동할 수 있습니까? 사무실 A의 장치가 손상된 경우 예를 들어 공격자가 PCI/CDE 영역으로 이동할 수 있습니까?
- **Ransomware Readiness:** 공격자가 당신의 환경에 있다면, 이 공격의 폭발 반경은 얼마입니까? 얼마나 많은 네트워크가 손상될까요? 영향을 이해하고 공격에 앞서 문제 해결의 우선순위 지정
- **3rd Party/Supply Chain Risk:** 공격자가 타사에서 사용하는 장치, AD 계정 또는 클라우드 계정 리소스를 손상시킨 경우 중요한 자산을 손상시킬 가능성은 무엇입니까?

- **IT > OT:** IT에 발판을 마련한 공격자가 OT 환경으로 이동하여 중요한 시스템에 영향을 미칠 수 있습니까?
- **Mergers & Acquisitions:** 실사 단계의 일부로 XM Cyber는 새로운 비즈니스 내의 위험을 강조하고 인프라 통합을 가속화하고 위험을 제거하는 데 도움이 되는 명확한 수정 계획을 제공할 수 있습니다.
- **Cloud Security:** 공격자가 클라우드 내에서 이동하여 중요한 자산을 손상시킬 수 있도록 권한과 리소스가 함께 연결되는 클라우드에서 공격 경로를 신속하게 식별합니다. 공격자가 온프레미스에서 클라우드로 이동할 수 있습니까? 여러 구독 간에 이동할 수 있습니까?
- **Vulnerability Prioritisation:** 취약점이 존재하는지 여부뿐만 아니라 공격자가 취약점을 어떻게 활용할 수 있는지에 대한 진정한 이해를 얻으십시오. 공격 경로와 병목 지점을 따라 중요한 자산을 위험에 빠뜨리는 취약점의 우선 순위를 지정하고 단순한 패치 적용 이상으로 문제를 해결하는 방법에 대한 단계별 지침을 제공합니다. 예를 들어, Log4J를 사용하면 가장 취약한 위치와 이 취약성이 있는 시스템이 손상되어 중요한 자산에 위험을 노출할 수 있는지 파악합니다. 어떤 시스템을 우선적으로 패치해야 합니까?
- **Optimise Spend:** XM Cyber가 가장 큰 격차를 식별한 곳에 보안 전략을 집중하십시오. 지속적인 가시성을 위해 XM Cyber로 규모와 자동화를 주도하고 보다 전략적인 요구 사항에 대한 테스트를 예약하여 특정 시점 펜 테스트 및 Red Teaming 활동을 넘어 이동합니다.



How It Works

- Windows/Linux/Mac의 작은 특허 센서(CPU 0.02%, 재부팅 없음, 영향 없음)는 공격자가 잘못된 구성, 취약성, 사용자 행동 및 네트워크 세분화 부족 등을 악용할 수 있는 조건을 수집하여 XM Cyber SaaS로 전송합니다. 플랫폼. 가치를 얻기 위해 보안 도구와 복잡한 통합을 할 필요가 없습니다. 공격자의 관점에서 위험을 볼 수 있는 유일한 진정한 방법은 장치에 있는 것입니다. 공격자가 소프트웨어를 설치하고 있음을 기억하십시오!
- 사용자/리소스에 대한 IAM 기반 정보와 클라우드에서 에스컬레이션에 사용되는 방법을 수집하는 모든 AWS, Azure 및 GCP 구독에 연결할 읽기 전용 감사자 계정(API 기반)
- 생산에 영향을 미치지 않는 지속적인 24/7 안전 시뮬레이션. 우리는 공격이 언제든지 발판이 될 수 있다는 것을 알고 있으므로 매년, 매월 또는 심지어 매주 위험을 식별하는 것은 더 이상 중요한 비즈니스 기능이 위험에 처하지 않도록 하는 옵션이 아닙니다.
- 사용자를 가장 위험에 빠뜨리는 장치/계정/클라우드 리소스(초크 포인트)에 중점을 둔 우선 순위가 지정된 단계별 수정. 소규모 팀과 대규모 팀 모두 최소한의 노력으로 위험을 제거하고 줄인 다음 공격자가 더 이상 이점을 누릴 수 없을 때 취한 조치의 영향을 확인할 수 있습니다.

What's Included

- 지속적인 공격 시뮬레이션을 실행하는 XM Cyber SaaS 기반 플랫폼
- 추가 비용 없이 Amazon Inspector, Tenable, Crowdstrike, Microsoft Defender, Blackberry Cylance, XSOAR, ServiceNow, Jira 및 기본 API와 같은 도구와 통합
- 표준 지원에는 고객 성공 기능, 기술 지원 제공, 온보딩 및 초기 설정, 정기적 케이던스, 지원 포털 및 Slack 커뮤니티가 포함됩니다.
- Mitre Att&ck의 광범위한 스펙트럼에 걸쳐 추가된 새로운 기술
- 새로운 제품 기능 및 업그레이드 표준

자세한 문의는 아래로 연락 주시기 바랍니다.

㈜한국밸런스 영업대표 김형덕
M) 010-7138-8889
E) hdkim@valence.co.kr
http://www.valence.co.kr