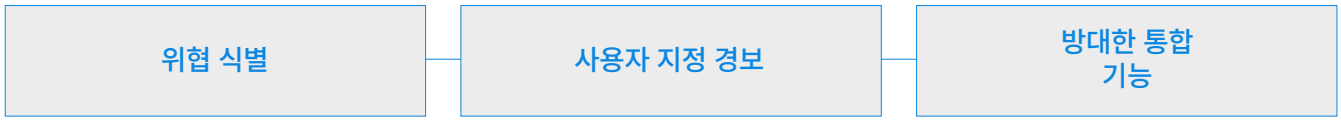
모듈 개요

이상 징후 및 위협 탐지

의료 분야의 위협 탐지 문제

의료 네트워크가 발전하면서 환자에게 제공하는 서비스 방식이 크게 달라졌습니다. 현재 의료 시스템의 인프라와 직원 및 워크플로는 확장형 IoT(XIoT)를 구성하는 다양한 커넥티드 디바이스에 상당 부분 의존하고 있습니다. 커넥티드 디바이스에 대한 임상 워크플로의 의존도가 점차 높아지면서 의료 서비스 기관(HDO)에게 운영 중단과 많은 비용을 초래하는 침해 또는 악의적 공격에 의한 사이버 사건이 발생할 위험이 더욱 커졌습니다.

통합 인사이트 및 경보 시스템은 디바이스 가시성과 교정 워크플로를 바탕으로 영향을 받는 디바이스에 대한 자동 모니터링, 우선순위 지정 및 대응 기능을 제공합니다. 오늘날 의료 서비스를 혁신하고 있는 커넥티드 디바이스는 알려진 위협과 새로운 위협에 더욱 많이 노출되고 있습니다. Medigate 플랫폼의 이상 징후 및 위협 탐지(ATD) 모듈은 이러한 문제를 해결하는 데 특화되어 있습니다.



Medigate 플랫폼 ATD 모듈

작동 원리

수동 심층 패킷 검사 기술과 업계에서 가장 광범위한 XIoT 프로토콜 커버리지 포트폴리오를 활용하는 Medigate 플랫폼은 의료 환경의 디바이스에 대해 고도로 중앙화된 상세 뷰를 제공합니다. Medigate 플랫폼은 네트워크 트래픽을 지속적으로 모니터링하여 비정상적인 행동과 침해 지표를 탐지함으로써 의료 서비스에 피해가 발생하기 전에 위협을 탐지하고, 우선순위를 지정하고, 대응 조치를 취합니다.

위협 식별

임상 워크플로의 고유한 특성과 더불어 위협 환경이 더욱 기승을 부리면서 병원 환경에 도사리는 사이버 위협의 찾아내기가 더욱 어려워질 수 있습니다. Medigate 플랫폼은 다음과 같은 기능을 이용해 병원 환경 전반에 걸쳐 알려진 위협과 새로운 위협을 모두 탐지합니다.

- **알려진 IoC 경보:** Medigate 플랫폼은 "알려진 정상" 행동 범위를 벗어나거나, 악성 IP와 통신하거나, 로그인 시도가 여러 번 실패하는 등 악의적 행동의 가능성을 보이는 디바이스에 대해 경보를 울립니다.
- **서명 기반 경보*:** Medigate 플랫폼은 Claroty Team82의 독점 연구와 공개 소스의 통합을 바탕으로 알려진 네트워크 서명 라이브러리를 구축하여 이전에 공개된 위협과 공격 기법을 탐지합니다.
- **ICS 프레임워크용 MITRE ATT&CK:** 알려진 전술과 기술을 사용해 위협 그룹화, 우선순위 지정 및 시각화를 실시하여 SOC 담당자의 경보 조사 및 시정 작업을 지원합니다.

사용자 지정 경보

의료 환경은 규모와 아키텍처, 사용자 기반 및 요구 사항이 저마다 다릅니다.
Medigate 플랫폼은 조직의 고유한 탐지 우선순위 및 목표에 기반한 위협 탐지 전략에 맞춰 경보를 사용자 지정할 수 있게 해줍니다.
사용자 지정 경보는 다음을 포함한 디바이스 매개변수의 다양한 측면을 아우릅니다.

- **사용자 지정 통신 경보*:** 네트워크 전반의 디바이스 통신 패턴을 파악하고 경보를 발령하여 XIoT 디바이스(예: 게스트 네트워크와 통신하는 BMS, 보안 장치가 없는 프로토콜을 사용하는 IoMT 디바이스)의 비정상적인 행동과 트래픽을 식별합니다.
- **디바이스 상태 변화 경보*:** 의료 환경의 디바이스에 발생한 중요한 변경 사항을 정확히 찾아냅니다. 오랜 기간 오프라인 상태였다가 다시 나타나거나, 위험 프로파일이 크게 변경되거나, 네트워크 상태 변경이 이루어진 디바이스의 경우에는 심층적인 조사가 필요할 수 있습니다.

강화된 SOC 기능 & 워크플로

보안 어플라이언스나 오케스트레이션 도구와 같은 기존 SOC 워크플로와의 통합을 통해 경보 및 보안 프로세스를 중앙화된 워크플로에 통합합니다. 또한 기존 인프라를 활용하고 기능을 확장하는 한편 위협 추적 및 시정에 필요한 수작업을 줄입니다.

- **기존 보안 인프라와의 통합:** Splunk, IBM Qradar, CrowdStrike와 같은 일반적인 SIEM 및 EDR 도구와의 통합을 통해 기존 워크플로를 강화하여 전체 의료 네트워크로 기능을 확장하는 동시에 복잡한 의료 기기 보안 학습 곡선을 제거합니다.
- **자동 경보:** 자동화된 경보 워크플로를 생성하여 다양한 디바이스 소유자와 그룹의 분류/시정을 최적화하고 중복을 줄이며 협업을 간소화함으로써 시스템 경보를 보다 효율적으로 관리합니다.

이상 징후 및 위협 탐지

Medigate 플랫폼 기본 모듈	Medigate 플랫폼 고급 모듈
ICS 경보 매핑용 MITRE ATT&CK을 이용한 행동 기준 설정, 이상 징후 탐지 및 사용자 지정 기능을 지원하는 강력한 위협 탐지 엔진	알려진 위협을 대상으로 한 서명 기반 탐지, 고유한 디바이스 행동에 대한 심층 모니터링 및 경보를 지원하는 사용자 지정 통신 경보, ICS 매트릭스용 MITRE ATT&CK의 추가적인 활용 등을 포함한 향상된 위협 탐지 기능

클래로티 회사 소개

클래로티는 산업, 의료 및 상업 조직이 각 환경에서 모든 사이버 물리 시스템, 즉 확장형 사물 인터넷(XIoT)의 보안을 강화할 수 있도록 지원합니다. 클래로티의 통합형 플랫폼은 고객의 기존 인프라와 통합되어 가시성, 위험 및 취약점 관리, 네트워크 보호, 위협 탐지 및 보안 원격 액세스에 대한 완전한 통제 범위를 제공합니다.

세계 최대의 투자기업 및 산업 자동화 벤더의 지원을 받는 클래로티는 전 세계 수백 개 기업에 소속된 수천 곳의 현장에 배치되어 있습니다. 뉴욕에 본사를 두고 있으며, 유럽, 아시아 태평양 및 라틴 아메리카 지역에서 지사를 운영하고 있습니다.

더 자세한 정보는 claroty.com을 방문하거나 claroty.com contact@claroty.com으로 이메일을 보내 주십시오.

** 고급 모듈에만 제공됨*

CLAROTY MEDIGATE by Claroty