NIS2 컴플라이언스 달성 전략

NIS2(개정된 네트워크 및 정보 보안 지침)의 정의 및 클래로티가 적용 대상 조직의 NIS2 컴플라이언스 달성을 지원하는 방법

서론

NIS2 지침은 EU(유럽연합) 내 핵심 인프라의 사이버 탄력성 강화라는 목표 아래 모든 EU 회원국이 각국의 적용 대상 조직에 부과해야 하는 최소한의 사이버 보안 요건을 규정한 법안입니다. 기존 NIS 지침을 대체하는 NIS2는 최근 몇 년간 증가한 EU 핵심 인프라에 대한 사이버 공격의 빈도 및 영향에 대응할 수 있도록 확장된 범위와 추가 요건이 특징입니다.

본 솔루션 개요는 NIS2에 대한 높은 수준의 개요와 함께 클래로티 포트폴리오가 NIS2 컴플라이언스를 위해 제공하는 지원에 대한 상세한 설명 및 EU 및 기타 지역의 보안 및 위험 업무 담당자를 위한 관련 지침을 제공합니다.

NIS2 기본 정보

범위

회원국은 다음 NIS2 요건을 식별하고 관할권 내 모든 적용 대상 조직에게 이를 부과해야 합니다.

1. 최소 50명의 직원을 고용하거나 최소 €10,000,000의 매출을 창출*해야 합니다.
2. EU의 건강, 안전 및/또는 안정성에 '필수적'이거나 '중요'하다고 간주되는 서비스를 제공합니다. 적용 대상이 되는 필수 및 중요 조직은 다음 분야의 조직을 포함합니다.

필수	중요
• 에너지 • 교통 • 은행 및 금융 인프라 • 의료 • 식수 및 폐수 • 디지털 인프라 • 공공 행정 • 우주	• 우편 및 배송 서비스 • 용수 관리 • 화학 물질 제조, 생산, 유통 • 식품 생산, 가공, 유통 • 의료, 전자, 운송 또는 관련 장비 제조 • 디지털 공급업체 • 연구

**회원국은 해당 인력 또는 매출 기준에 부합하지 않지만 EU의 건강, 안전 및/또는 안정성 지원과 관련해 중요한 역할을 담당하고 있는 조직을 대상으로 NIS2 요건을 확장 적용할 수 있습니다.*

NIS2 컴플라이언스 요건

적용 대상 필수 및 중요 조직에 부과되는 NIS2 컴플라이언스 최소 요건은 다음과 같습니다.

- **사이버 보안 위험 관리 조치:** EU 내 필수/중요 서비스 제공과 관련된 네트워크, 시스템 및/또는 기타 디지털/물리적 자산에 발생하는 사이버 위험의 관리 및 완화를 위한 10가지 주요 조치를 실행해야 합니다. 주요 조치는 다음과 같습니다.
    1. 위험 분석 및 정보 시스템 보안 관련 정책
    2. 사고 처리(예방, 탐지, 대응)
    3. 백업 및 복구 관리 등 위기 관리 및 비즈니스 연속성
    4. 각 조직과 공급업체 또는 서비스 제공업체 간 관계를 포괄하는 공급망 보안
    5. 취약점 처리 및 공개를 포함한 네트워크 및 정보 시스템 확보, 개발 및 유지관리 관련 보안
    6. 사이버 보안 위험 관리의 효과를 평가하는 정책 및 절차
    7. 기본 사이버 하이진(hygiene) 관행 및 사이버 보안 교육
    8. 암호화 기법 및 해당하는 경우 암호화 사용 관련 정책 및 절차
    9. 인적 자원 보안, 액세스 제어 정책, 자산 관리
    10. 다단계 인증 또는 지속 인증 솔루션, 보안 음성, 영상, 문자 통신 및 안전한 비상 통신 시스템의 사용
- **사고 보고 요건:** 다음 기준에 따라 지정된 CSIRT(컴퓨터 보안 사고 대응팀) 또는 기타 국가 기관에 사이버 사고를 보고해야 합니다.
    - 탐지 후 24시간 이내: 사건에 대해 알려진 상세 정보를 전달해야 합니다.
    - 탐지 후 72시간 이내: 사고, 심각도, 영향 및 침해 지표에 대한 평가를 포함한 전체 통지 보고서를 전달해야 합니다.
    - 탐지 후 30일 이내: 사건에 대한 최종 보고서를 전달해야 합니다.

미준수 시 부과되는 제재

- **필수 조직:** 최대 €10,000,000 또는 해당 조직이 속한 기업이 이전 회계연도에 달성한 전 세계 연간 총 매출의 최소 2%(둘 중 더 높은 금액)를 벌금으로 부과합니다.
- **중요 조직:** 최대 €7,000,000 또는 해당 조직이 속한 기업이 이전 회계연도에 달성한 전 세계 연간 총 매출의 최소 1.4%(둘 중 더 높은 금액)를 벌금으로 부과합니다.

연대표 및 기한

- NIS2는 **2023년 1월 16일**에 발효되었습니다.
- 회원국은 **2024년 10월 17일**까지 NIS2를 국내법으로 전환해야 합니다.
- 회원국은 **2025년 4월 17일**까지 적용 대상 필수/중요 조직을 식별 및 등록해야 합니다.

클래로티의 NIS2 컴플라이언스 지원 방법

사이버-물리 시스템(CPS)의 역할

클래로티의 사이버-물리 시스템(CPS) 사이버 보안 포트폴리오는 강력한 보호, 모니터링 및 기타 사이버 위험 관리 제어 기능을 모든 CPS(NIS2 적용 대상으로 간주되는 EU 제공의 필수/중요 서비스를 뒷받침하는 CPS 포함)로 확장하여 NIS2 컴플라이언스 지원 및 간소화를 동시에 구현합니다.

CPS는 많은 중요 인프라 조직, 기타 산업, 의료, 상업 및 공공 분야의 조직이 간과하는 위험 사각지대입니다. CPS 보안은 NIS2 및 기타 규정에서 요구하는 것이기도 하지만 사회의 건강, 안전 및 안정성의 기반이 되므로 필수적인 구현이 필요합니다. 일반적인 CPS 유형은 다음과 같습니다.

- 발전 및 제조 프로세스를 구동하는 PLC(프로그래머블 로직 컨트롤러) 등 **운영 기술(OT)** 자산
- 안전하고 편안한 병원 환경을 위한 보안 카메라, 동작 센서 등 **사물 인터넷(IoT)** 및 **산업용 IoT(IIoT)** 디바이스
- 공기 정화 및 건물 내 편리한 이동을 위한 디지털화된 HVAC 컨트롤러, 엘리베이터 등 **건물 관리 시스템(BMS)** 장비
- **의료 사물 인터넷(IoMT)** 및 활력 징후 모니터링, 질병 진단 및 건강 유지를 위한 주입 펌프, MRI 등 기타 임상 디바이스

상기 언급된 CPS 유형 및 기타 CPS 유형은 대부분 기존의 보안 도구 및 접근 방식과 호환되지 않으므로 기본적으로 NIS2 컴플라이언스 등의 보안을 구현하기가 매우 어렵습니다. 클래로티는 모든 CPS를 대상으로 보호, NIS2 및 기타 규제 요건 지원을 제공할 수 있도록 특별히 설계된 포괄적이면서도 유연한 사이버 보안 포트폴리오를 이용해 이러한 문제를 해결합니다.

클래로티 포트폴리오 소개

클래로티는 CPS 사이버 보안 여정 전반에 걸친 모든 사용 사례 및 목표를 지원합니다. 포트폴리오 내 솔루션에는 다음이 포함됩니다.

Claroty xDome

Claroty xDome은 전체 산업 사이버 보안 여정의 모든 사용 사례 및 CPS 유형을 위해 특별히 설계된 유연한 SaaS 플랫폼입니다.

Medigate by Claroty

Medigate by Claroty는 환자 치료용 디바이스에 대한 보호를 제공하는 SaaS 기반 의료 사이버 보안 플랫폼입니다.

Claroty SRA

Claroty SRA(Secure Remote Access)는 내부 및 외부 OT 직원에게 원활하고 안정적이며 안전한 원격 액세스를 제공합니다.

Claroty CTD

Claroty CTD(Continuous Threat Detection)는 산업 환경을 위한 강력한 온프레미스 사이버 보안 제어 기능을 제공합니다.

NIS2 요건과 클래로티 기능의 연결을 통한 사이버 보안 위험 관리

다음 표는 클래로티 포트폴리오의 솔루션이 제공하는 다양한 기능과 NIS2 지침에 규정된 사이버 보안 위험 관리 요건과의 연결 범위를 개략적으로 설명합니다.

	NIS2 요건	클래로티 지원 기능 요약	솔루션
1.	**위험 분석 및 정보 보안 관련 정책**	클래로티는 CPS 환경에 존재하는 모든 자산, 시스템, 취약점, 사이버 및 운영 위험을 발견 및 평가하며, 광범위한 가시성을 바탕으로 이러한 위험 노출을 완화하는 정책을 자동으로 정의 및 시행합니다.	**Claroty xDome, Medigate, & CTD**
2.	**사고 처리**	클래로티는 전체 CPS 환경의 지속적인 모니터링을 통해 알려진/알려지지 않은 위협의 초기 지표를 찾고, 모든 경고의 맥락을 파악하여 대응을 최적화하며, SIEM, SOAR 및 관련 솔루션과의 통합을 바탕으로 기존 SOC 워크플로를 전체 CPS로 확장합니다.	**Claroty xDome, Medigate, & CTD**
3.	**위기 관리 및 비즈니스 연속성**	클래로티는 모든 CPS에 대한 포괄적인 실시간 인벤토리를 제공하고, 모든 자산/네트워크 변경 및 이상 징후를 기록하고, 사고 방어 및 예방을 위한 네트워크 세그멘테이션 정책 및 액세스 제어 기능을 정의 및 시행하며, 바로 이용 가능한 백업 및 복구 도구와의 통합을 제공합니다. 이러한 모든 기능은 전사적 위기 관리 및 연속성 활동을 촉진하고 개선합니다.	**Claroty xDome, Medigate, SRA, & CTD**
4.	**공급망 보안**	클래로티는 발견된 모든 자산과 최신 CVE 및 기타 약점의 상관 관계를 파악하고, CPS 환경 내 위험을 지속적으로 평가하며, 모든 내부 및 외부 사용자에게 OT에 대한 안전하면서도 원활한 원격 액세스를 제공함으로써 고객이 공급망 전반에 걸쳐 외부 위험을효과적이고 효율적으로 평가, 관리 및 완화할 수 있도록 합니다.	**Claroty xDome, Medigate, SRA, & CTD**
5.	**네트워크 및 정보 시스템 보안**	클래로티는 발견된 모든 자산과 최신 CVE, 구성 오류 및 기타 약점의 상관 관계를 실시간으로 파악하고, 전체 CPS 환경 내 위험 노출을 지속적으로 평가하며, 모든 내부 및 외부 인력에게 OT에 대한 안전하면서도 원활한 원격 액세스를 제공함으로써 고객이 환경에 걸쳐 사이버 위험을 효과적이고 효율적으로 평가, 관리 및 완화할 수 있도록 합니다.	**Claroty xDome, Medigate, SRA, & CTD**
6.	**사이버 보안 위험 관리의 효과를 평가하는 정책 및 절차**	클래로티는 사용자 지정 위험 점수 산정 메커니즘, 위험 시정 조치 영향 시뮬레이션, 각 제어 조치가 시간 경과에 따라 전사적 위험 태세에 미치는 영향을 측정하는 선제적 모니터링 및 과거 이력 평가, 다양한 분야의 이해관계자를 위한 정보의 전달을 단순화하는 유연한 보고 기능을 제공합니다.	**Claroty xDome, Medigate, & CTD**
7.	**기본 사이버 하이진(hygiene) 관행 및 사이버 보안 교육**	클래로티의 위험 보고 및 시뮬레이션 기능은 사이버 하이진 및 교육 관련 요구 사항에 대한 정보를 얻는 데 도움이 되는 시정 권장 사항을 포함합니다. 또한 클래로티의 SRA 솔루션은 내부 및 외부 인력 모두를 대상으로 RBAC, 비밀번호 정책 및 기타 사이버 하이진 관행을 손쉽게 시행할 수 있도록 합니다.	**Claroty xDome, Medigate, SRA, & CTD**
8.	**암호화 기법 및 암호화 관련 정책 및 절차**	클래로티는 NIS2, GDPR 및 기타 규제 요건에 따라 모든 사용자, CPS 및 기타 시스템 관련 데이터를 암호화합니다. 또한 개인 건강 정보(PHI)와 같은 민감 데이터가 정책에 어긋나는 방식 등으로 처리되는 이벤트에 대한 경고를 제공하여 고객이 잠재적인 데이터 노출과 관련된 사고를 방지할 수 있도록 합니다.	**Claroty xDome, Medigate, SRA, & CTD**
9.	**인적 자원 보안, 액세스 제어, 자산 관리**	클래로티의 위험 완화 권고는 사이버 하이진 및 액세스 제어 정책에 대한 정보 획득 및 우선순위 지정에 도움을 줍니다. 또한 클래로티의 SRA 솔루션은 내부 및 외부 인력 모두를 대상으로 RBAC, 비밀번호 정책 및 기타 사이버 하이진 관행을 손쉽게 시행할 수 있도록 합니다. CMDB, CMMS 및 관련 솔루션과의 원활한 통합을 바탕으로 기존 자산 관리 워크플로를 조직 내 모든 CPS로 간단히 확장할 수 있습니다.	**Claroty xDome, Medigate, SRA, & CTD**
10.	**다단계 인증 및 보안 통신**	클래로티 SRA는 모든 내외부 OT 인력을 위한 세분화된 RBAC 및 MFA 등 제로 트러스트 기반 액세스 제어 기능과 함께 고가용성, OT를 위해 특별 구축된 UX, 감사, 포렌식 및 관련 사용 사례를 지원하는 기록 기능을 추가하여 고가용성, OT 환경 내 모든 CPS에 대한 안전한 원격 및 현장 액세스를 제공합니다.	**Claroty xDome, Medigate, SRA, & CTD**

NIS2 요건과 클래로티 기능의 연결을 통한 사고 보고

다음 표는 클래로티 포트폴리오의 솔루션이 제공하는 다양한 기능과 NIS2 지침에 규정된 사고 보고 요건과의 연결 범위를 개략적으로 설명합니다.

	NIS2 요건	클래로티 지원 기능 요약	솔루션
1.	**24시간 이내:** **사건에 대해 알려진 모든 상세 정보를 전달해야 합니다.**	클래로티는 전체 CPS 환경에 대한 지속적인 모니터링을 통해 사고 가능성을 나타내는 초기 지표를 신속하게 탐지합니다. 동일 사건과 관련된 모든 이벤트는 손쉽고 빠른 내보내기 및 관련 당국과의 공유가 가능한 모든 관련 상세 정보를 포함한 맥락화된 단일 경고로 통합되어 해당 요건을 충족할 수 있도록 합니다.	**Claroty xDome, Medigate, & CTD**
2.	**72시간 이내:** **사고, 심각도, 영향 및 IoC에 대한 평가를 포함한 전체 통지 보고서를 전달해야 합니다.**	클래로티가 각 경고별로 제공하는 세분화된 상세 정보에는 일반적으로 사고의 IoC, 전체 근본 원인 분석, 관련이 있거나 영향을 받는 자산, 악용되는 취약점, 심각도 및 환경에 대한 위험, 완화 권고, 로그 등이 포함됩니다. 이러한 상세 정보는 추가적인 영향 평가를 지원하며 관련 당국과 빠르고 쉽게 공유하여 해당 요건을 충족할 수 있습니다.	**Claroty xDome, Medigate, & CTD**
3.	**30일 이내:** **사건에 대한 최종 보고서를 제출해야 합니다.**	상기 모니터링, 경고 강화 및 평가 기능 외에도 클래로티의 포트폴리오는 SIEM, SOAR, EDR, CMDB 및 기타 IT, 운영 및 보안 기술과의 원활한 통합을 제공합니다. 이러한 통합은 IT 및 CPS 환경 전반에 걸친 포렌식 조사, 감사 및 관련 워크플로를 추가적으로 지원하여 고객이 전체 조직 내 사고를 보다 효과적이고 효율적으로 평가하고 보고할 수 있도록 합니다.	**Claroty xDome, Medigate, SRA, & CTD**

결론

클래로티의 사이버 보안 포트폴리오는 NIS2 적용 대상이 되는 산업, 의료, 상업 및 공공 분야의 조직에서 보안 및 위험 업무를 담당하는 이들을 위한 이상적인 솔루션을 제공합니다. 특히 사이버-물리 시스템(CPS) 환경에서 NIS2 지침의 사이버 보안 위험 관리 및 사고 보고 요건에 대한 광범위한 지원을 제공합니다. 클래로티의 CPS 사이버 보안 솔루션을 고객의 기존 IT 보안 도구 및 워크플로와 병행하여 사용하고 원활하게 통합하면 전사적 IT 및 CPS 환경 전반에서 모든 NIS2 요건에 대한 완전한 커버리지 및 지원을 확보할 수 있습니다.

클래로티 회사 소개

클래로티는 산업, 의료, 상업 및 공공 분야의 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 기능을 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 지역에 지사를 운영하고 있습니다.