솔루션 개요

CLAROTY & ISA/IEC-62443-3-3

클래로티 산업 솔루션의 컴플라이언스 지원

목차

개요

조직들에 대한 보안 위협이 해마다 증가하면서 사이버 위협으로부터 중요 인프라와 제조 공정 및 관련 사이버 물리 시스템을 보호하는 것이 점차 중요해지고 있습니다. 산업 환경과 그 기반이 되는 운영 기술 네트워크가 매우 복잡하기 때문에 강력한 사이버보안 수단을 구축하는 일은 결코 만만치 않습니다. 이러한 복잡성은 지리적 조건, 여러 현장에 걸쳐 혼재해 있는 구형 및 신형 시스템, 온갖 특화 자산, 기존의 IT 보안 관행과 운영 고려사항 간에 존재하는 지식 격차 등 여러 가지 요인에서 비롯됩니다.

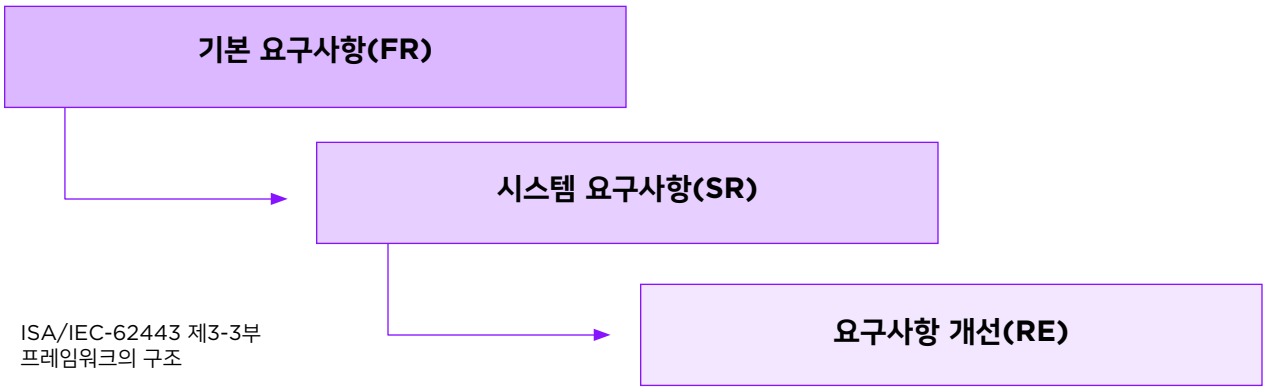
이 문제를 해결하기 위해 전 세계 조직들은 협업을 통해 국제자동화협회(ISA)가 개발하고 국제전기기술위원회(IEC)가 발행한 ISA/IEC-62443과 같은 사이버보안 표준을 제정합니다. ISA/IEC-62443은 사이버보안의 기술적 측면과 절차적 측면을 모두 아우르며 IACS의 보안을 위한 종합 프레임워크를 제시합니다.

오랫동안 중요 인프라 및 제조 소유자/운영자들이 자사의 복잡한 산업 자동화 및 제어 시스템 환경을 보호할 수 있도록 지원해온 클래로티는 이러한 기업들이 이 프레임워크의 다양한 요구사항을 충족하도록 도울 수 있는 독보적인 입지를 갖추고 있습니다. 클래로티 xDome, Continuous Threat Detection(CTD), Secure Remote Access(SRA)를 포함한 당사의 종합적인 산업 사이버보안 솔루션은 OT 네트워크 고유의 과제와 요구를 해결하도록 설계되었습니다. 본 문서는 업계의 다양한 조직들이 클래로티 산업 솔루션을 통해 ISA/IEC-62443-3-3 프레임워크를 어떻게 준수하고 있는지 소개합니다.

ISA/IEC-62443-3-3의 구조

ISA/IEC-62443 프레임워크는 적용 대상인 산업 자동화 및 제어 시스템(IACS) 분야의 다양한 청중 또는 중점 요소에 적용 가능한 4개의 그룹으로 구성됩니다. ISA/IEC-62443의 제3-3부는 목표 보안 등급을 만족하는 IACS를 구축하기 위한 시스템 보안 요건과 기능 수준을 정의하고 사용자가 자사의 보안 관행을 평가할 수 있는 방법을 제시합니다.

이 프레임워크는 7개의 기본 요구사항(FR)으로 구성되며 이들 기본 요구사항은 다시 다섯 가지 목표 보안 수준(SL) 중 하나에 도달하기 위해 사용할 수 있는 일련의 시스템 요구사항(SR)과 요구사항 개선(RE)을 포함합니다. 아래 도표는 이 프레임워크의 계층을 도식화한 것입니다.



ISA/IEC-62443 제3-3부 프레임워크의 구조

이 프레임워크의 5가지 보안 수준은 다양한 규모의 공격자에 대한 저항 수준을 나타냅니다. 보안 수준은 다음과 같습니다.

- **보안 수준 0:** 특별한 요구사항이나 보호가 필요하지 않음
- **보안 수준 1:** 의도적이지 않거나 우연한 오용으로부터 보호
- **보안 수준 2:** 적은 자원, 일반적인 기술 및 약한 동기를 가지고 간단한 수단을 이용하는 고의적 오용으로부터 보호
- **보안 수준 3:** 보통의 자원, IACS에 대한 지식 및 보통의 동기를 가지고 정교한 수단을 이용하는 고의적 오용으로부터 보호
- **보안 수준 4:** 방대한 자원, IACS에 대한 지식 및 강한 동기를 가지고 정교한 수단을 이용하는 고의적 오용으로부터 보호

본 문서의 구성

본 문서는 ISA/IEC-62443-3-3에 규정된 지침에 대해 클래로티 솔루션(클래로티 xDome, CTD, SRA)이 **솔루션 지원** 또는 **환경 지원**을 제공할 수 있는 영역을 식별합니다.

- **솔루션 지원:** IACS 환경에 어플라이언스/소프트웨어로서 배포된 클래로티 솔루션으로 시스템 요구사항(SR)을 충족합니다.
- **환경 지원:** 배포된 클래로티 솔루션을 통해 IACS 환경 전반에서 시스템 요구사항(SR)을 지원하여 현장 전체의 컴플라이언스를 유지하도록 보장합니다.

기본 요구사항 및 클래로티

이 섹션에서는 ISA/IEC-62443-3-3의 7가지 기본 요구사항(FR)과 기본 요구사항별 시스템 요구사항 및 요구사항 개선을 소개하고, 클래로티 산업 솔루션이 각 요구사항을 어떻게 지원하는지 알아봅니다. 클래로티 솔루션에 적용되지 않는 시스템 요구사항(SR)은 제외했습니다.

FR1 - 식별 및 인증 제어

제어 시스템 구성요소별로 사람, 소프트웨어 프로세스 및 장치를 포함한 종합적인 전체 사용자 목록을 마련하는 것은 FR1 - 식별 및 인증 제어 보호의 필수적인 수준을 보장하는 데 매우 중요합니다. 이 프로세스는 IACS를 보호하기 위한 기본 요소입니다. FR1 시스템 요구사항은 사용자에게 액세스 권한을 부여하기 전에 이들의 신원을 확인함으로써 무단 액세스와 잠재적 보안 위반을 예방하는 데 중요한 역할을 합니다. 또한 IACS 내 다양한 구성요소의 특정 요구에 따라 FR1 메커니즘을 맞춤화하는 것도 필수적입니다. 일부 구성요소는 강력한 인증 수단이 필요할 수 있지만 그렇지 않은 구성요소도 있기 때문에 FR1 시스템 요구사항을 만족하려면 다양한 용도에 맞게 조정할 수 있는 전략이 필요합니다. 이러한 접근법을 취하면 보안이 강화될 뿐만 아니라 다양한 환경에서 제어 시스템을 효율적이고 효과적으로 운영할 수 있습니다.

설명	관련 클래로티 솔루션	클래로티 지원 내용
SR 1.1 – 사용자 식별 및 인증 제어 시스템은 모든 사용자를 식별하고 인증할 수 있는 기능을 제공해야 한다. 이러한 기능은 적용 가능한 보안 정책과 절차에 따라 직무 분리 및 최소 권한 사용을 지원하기 위해 제어 시스템에 대한 사용자 액세스를 제공하는 모든 인터페이스에서 식별과 인증을 시행해야 한다.	솔루션 지원 (xDome, CTD, SRA)	클래로티 솔루션에서는 특정 기능, 보기 전용 권한, 전체 관리 등 세분화된 역할 기반 액세스 제어(RBAC)를 통해 사용자 계정과 사용자 그룹을 구성하고 관리할 수 있습니다. 사용자 인증은 로컬로 수행하거나, 또는 액티브 디렉토리 또는 SAML 방식을 위한 LDAP over SSL 연결을 통해 수행할 수 있으며, 다중 인증(MFA)도 지원됩니다. 이렇게 세분화된 액세스 제어를 통해 클래로티 솔루션 내 광범위한 중요 네트워크 및 장치 데이터를 안전하게 보호할 뿐만 아니라 조직 내 역할에 따라 사용자 경험을 간소화할 수 있습니다.
SR 1.1 RE 1 – 고유 식별 및 인증 제어 시스템은 모든 사용자를 고유하게 식별 및 인증할 수 있는 기능을 제공해야 한다.	솔루션 지원 (xDome, CTD, SRA)	
SR 1.1 RE 2 – 신뢰할 수 없는 네트워크에 대한 다중 요소 인증 제어 시스템은 제어 시스템에 액세스하는 모든 사용자에게 다중 요소 인증을 적용할 수 있는 기능을 제공해야 한다.	솔루션 지원 (xDome, CTD, SRA)	

설명	관련 클래로티 솔루션	클래로티 지원 내용
SR 1.2 - 소프트웨어 프로세스와 장치의 식별 및 인증 제어 시스템은 모든 소프트웨어 프로세스와 장치를 식별하고 인증하는 기능을 제공해야 한다. 이 기능은 적용 가능한 보안 정책과 절차에 따라 최소 권한을 지원하기 위해 제어 시스템에 대한 액세스를 제공하는 모든 인터페이스에서 식별 및 인증을 시행해야 한다.	솔루션 지원 (xDome, CTD, SRA)	클래로티 솔루션은 모든 내부 소프트웨어 프로세스 외에도 연결된 구성요소(센서, CTD 서버, CTD Enterprise Management Console, xDome 컬렉터)를 식별하고 인증합니다. 이러한 구성요소들의 상태를 해당 솔루션에서 확인할 수 있으며, 이는 솔루션 가동시간과 문제 해결 작업을 보장하는 데 도움이 됩니다.
SR 1.3 – 계정 관리 제어 시스템은 계정의 추가, 활성화, 변경, 비활성화 및 삭제를 포함해 인가된 사용자가 보유한 모든 계정의 관리를 지원하는 기능을 제공해야 한다.	솔루션 지원 (xDome, CTD, SRA)	클래로티 솔루션은 액티브 디렉토리와 같은 서비스를 통해 세분화된 사용자 계정 관리 및 통합을 제공합니다. 사용자 계정은 그룹에 추가하거나 특정 권한을 할당하여 변경하거나 시스템 관리자를 통해 삭제할 수 있습니다. 또한 당사 솔루션 내에서 모든 사용자의 활동을 추적하고 감사 및/또는 검토를 위해 시스로그로 내보내거나 전달할 수 있습니다.
SR 1.4 – 식별자 관리 제어 시스템은 사용자별, 그룹별, 역할별 또는 제어 시스템 인터페이스별로 식별자의 관리를 지원하는 기능을 제공해야 한다.	솔루션 지원 (xDome, CTD, SRA)	클래로티 솔루션은 엄격한 RBAC 파라미터를 통한 사용자 및/또는 그룹 기능의 구성을 지원합니다. 이 파라미터들은 크게 보기 전용, 제한된 관리 및 전체 관리의 세 가지 권한 등급으로 분류됩니다. 이러한 제어는 클래로티 솔루션 내 데이터의 무결성을 높이고 조직 내 역할에 따라 사용자 경험을 간소화하는 데 도움이 됩니다.
SR 1.5 – 인증자 관리 제어 시스템은 다음과 같은 기능을 제공해야 한다. A. 인증자 내용의 초기화 B. 제어 시스템 설치 시 모든 디폴트 인증자의 변경 C. 모든 인증자의 변경/새로고침 D. 저장 및 전송 시 무단 공개와 변경으로부터 모든 인증자를 보호	솔루션 지원 (xDome, CTD, SRA)	클래로티는 최초 설치 후 모든 디폴트 사용자 계정을 반드시 변경하도록 요구하며, 자격증명을 일반 텍스트 형식으로 저장하지 않습니다. 플랫폼 구성요소는 액세스 권한을 프로비저닝하고 사용자와 데이터를 공유하기 위해 토큰을 통해 인증됩니다.

설명	관련 클래로티 솔루션	클래로티 지원 내용
SR 1.6 – 무선 액세스 관리 제어 시스템은 무선 통신에 참여하는 모든 사용자를 식별 및 인증하는 기능을 제공해야 한다.	환경 지원 (CTD, xDome)	클래로티 CTD와 xDome은 여러 검색 방법을 통해 네트워크 내에서 발견되고 작동하는 모든 무선 장치를 식별할 수 있는 종합 자산 목록을 제공합니다. 이러한 가시성은 무선 장치에 대한 추가 사이버보안 제어를 위한 기반을 제공합니다.
SR 1.7 – 패스워드 기반 인증의 강도 패스워드 기반 인증을 활용하는 제어 시스템의 경우, 해당 제어 시스템은 최소 길이 및 다양한 유형의 문자를 기반으로 설정 가능한 패스워드 강도를 강제하는 기능을 제공해야 한다.	솔루션 지원 (xDome, CTD, SRA)	클래로티 솔루션은 패스워드 기반 사용자 인증을 사용할 때 길이, 문자 유형 및 영숫자 제어에 따라 사용자 패스워드를 설정할 수 있는 기능을 제공합니다. 설정 후, 변경 주기, 재사용, 전체 초기화, 유효 기간 등에 관한 패스워드 규칙은 시스템 관리자가 설정할 수 있습니다. 이러한 세분화된 패스워드 규칙은 클래로티 솔루션의 무결성을 보장하는 데 효과적입니다.
SR 1.7 RE 1 – 사용자 패스워드 생성 및 사용기간 제한 제어 시스템은 한번 사용한 사용자 계정을 설정 가능한 특정 횟수 동안에는 재사용할 수 없도록 하는 기능을 제공해야 한다. 또한 제어 시스템은 사용자에 대해 패스워드의 최소 및 최대 사용 기간을 강제하는 기능을 제공해야 한다.	솔루션 지원 (xDome, CTD, SRA)	
SR 1.7 RE 2 – 모든 사용자 대상 패스워드 사용기간 제한 제어 시스템은 모든 사용자에게 패스워드의 최소 및 최대 사용 기간을 강제하는 기능을 제공해야 한다.	솔루션 지원 (xDome, CTD, SRA)	

설명	관련 클래로티 솔루션	클래로티 지원 내용
SR 1.8 – 공개키 인프라(PKI) PKI를 활용할 때, 제어 시스템은 일반적인 모범 관행에 따라 PKI를 운용하거나 기존 PKI로부터 공개키 인증서를 얻는 기능을 제공해야 한다.	환경 지원 (CTD, xDome)	클래로티는 PKI를 사용할 뿐만 아니라 외부 인증 기관(CA)도 이용할 수 있도록 지원하므로 사용자가 솔루션의 사용자 인터페이스에 액세스할 때 믿을 수 있는 자체 인증 기관(CA)을 이용할 수 있습니다.
SR 1.9 – 공개키 인프라(PKI)의 강도 공개키 인증을 활용하는 제어 시스템의 경우, 해당 시스템은 다음과 같은 기능을 제공해야 한다. A. 서명의 유효성을 검사하여 인증서를 검증 B. 허용된 CA에 대한 인증 경로를 구성하거나 자체 서명 인증서의 경우 배포 리프 인증서로 인증서를 검증 C. 인증서 해지 상태를 검사하여 인증서를 검증 D. 상응하는 개인키의 사용자 제어를 구축 E. 인증된 아이덴티티를 사용자에게 매핑	솔루션 지원 (xDome, CTD, SRA)	
SR 1.10 – 인증자 피드백 제어 시스템은 인증 과정에서 인증 정보의 피드백을 알아보기 어렵게 만드는 기능을 제공해야 한다.	솔루션 지원 (xDome, CTD, SRA)	클래로티 솔루션은 패스워드 입력을 위해 마스킹된 문자와 같은 인증자 피드백을 알아보기 어렵게 만드는 등 모든 인증 이벤트를 보호하고 암호화합니다.
SR 1.11 – 로그인 시도 실패 제어 시스템은 설정 가능한 시간 동안 사용자가 로그인 시도에 실패할 수 있는 횟수 한도를 강제하는 기능을 제공해야 한다. 제어 시스템은 이 한도가 초과되었을 때 특정 시간 동안, 또는 관리자가 잠금을 해제할 때까지 액세스를 거부하는 기능을 제공해야 한다.	환경 지원 (xDome, CTD, SRA)	클래로티 솔루션은 설정 가능한 횟수만큼 로그인에 실패한 경우 사용자 로그인을 비활성화하는 기능을 제공합니다. 또한 설정 가능한 시간 동안 접속하지 않은 사용자는 로그인이 비활성화될 수 있습니다. 클래로티 솔루션이 모니터링하는 네트워킹된 자산의 경우, 로그인에 여러 번 실패할 경우 솔루션에서 사용자가 처리할 수 있는 경보가 생성됩니다.

설명	관련 클래로티 솔루션	클래로티 지원 내용
SR 1.12 – 시스템 사용 알림 제어 시스템은 인증 전에 시스템 사용 알림 메시지를 표시하는 기능을 제공해야 한다. 시스템 사용 알림 메시지는 인가된 담당자가 설정해야 한다.	솔루션 지원 (xDome, CTD, SRA)	클래로티 솔루션은 인증 전에 솔루션 로그인 화면에서 시스템 사용 알림 및 사용자 동의 기능을 제공합니다. 이 로그인 메시지는 시스템 관리자를 통해 사용자 지정할 수 있습니다.
SR 1.13 – 신뢰할 수 없는 네트워크를 통한 액세스 제어 시스템은 신뢰할 수 없는 네트워크를 통해 제어 시스템에 액세스하는 모든 방법을 모니터링 및 제어하는 기능을 제공해야 한다.	환경 지원 (xDome, CTD, SRA)	클래로티 솔루션은 신뢰할 수 없는 네트워크에서의 사용자 또는 장치에 의한 모든 네트워크 액세스를 모니터링하고 경보를 발령합니다. 클래로티는 신뢰할 수 없는 네트워크를 통해 시스템 액세스를 모니터링 및 제어하는 SRA를 제공합니다.
SR 1.13 RE 1 – 명시적 액세스 요청 승인 제어 시스템은 할당된 역할에 의해 승인되지 않는 한 신뢰할 수 없는 네트워크를 통한 액세스 요청을 거부하는 기능을 제공해야 한다.	환경 지원 (SRA)	

FR2 - 사용 통제

각 사용자(사람, 소프트웨어 또는 장치)에게 적합한 수준의 권한만 부여되도록 하는 것은 IACS 보안에서 중요한 부분으로, 제어 시스템 자원에 대한 무단 작업을 방지하는 데 매우 중요합니다. 사용자가 식별되고 인증되면 시스템은 해당 사용자가 데이터 읽기/쓰기, 프로그램 다운로드, 구성 설정 등의 작업을 수행하는 데 필요한 권한이 있는지 검증해야 합니다. 따라서 자산 소유자와 시스템 통합 사업자는 시간, 위치, 액세스 방법 등 다양한 요소를 고려하여 사용자 권한을 신중하게 관리해야 합니다. FR2 - 사용 통제의 시스템 요구사항에 따르면 특히 구성요소마다 보안 요구사항이 각기 다른 환경에서 이러한 통제 메커니즘을 구현하는 것은 시스템과 데이터를 모두 보호하여 IACS의 운영 무결성과 보안을 유지하는 데 도움이 됩니다.

설명	관련 클래로티 솔루션	클래로티 지원 내용
SR 2.1 – 권한 부여 시행 모든 인터페이스에서 제어 시스템은 제어 시스템 사용을 통제하여 직무 분리 및 최소 권한 사용을 지원하기 위해 모든 사용자에게 할당된 권한을 시행하는 기능을 제공해야 한다.	솔루션 지원 (CTD, xDome) 환경 지원 (SRA)	클래로티 솔루션은 시스템 관리자가 설정할 수 있는 세분화된 역할 기반 액세스 제어(RBAC)를 통해 직무 분리를 지원합니다. 이 파라미터들은 크게 보기 전용, 제한된 관리 및 전체 관리의 세 가지 권한 등급으로 분류됩니다. RBAC 프로필을 그대로 사용하여 특정 자산, 구역 또는 현장에 액세스하도록 세분화 수준을 추가할 수 있으며, 액티브 디렉토리 서비스와의 통합을 통해 액세스 권한도 매핑할 수 있습니다. 또한 클래로티 SRA는 구성 다운로드나 OT 자산 변경과 같은 중요한 변경 작업을 수행할 때 이중 승인(Dual Approval)을 지원합니다.
SR 2.1 RE 1 – 모든 사용자 대상 권한 부여 시행 모든 인터페이스에서 제어 시스템은 제어 시스템 사용을 통제하여 직무 분리 및 최소 권한을 지원하도록 모든 사용자에게 할당된 권한을 시행하는 기능을 제공해야 한다.	솔루션 지원 (CTD, xDome) 환경 지원 (SRA)	
SR 2.1 RE 2 – 권한-역할 매핑 제어 시스템은 인가된 사용자나 역할이 모든 사용자에 대한 권한-역할 매핑을 정의 및 변경할 수 있는 기능을 제공해야 한다.	솔루션 지원 (CTD, xDome) 환경 지원 (SRA)	
SR 2.1 RE 3 – 감독자 재정의 제어 시스템은 설정 가능한 시간 또는 일련의 이벤트에 대한 현재 사용자 권한의 감독자 수동 재정의를 지원해야 한다.	환경 지원 (SRA)	
SR 2.1 RE 4 – 이중 승인 제어 시스템은 작업이 산업 공정에 심각한 영향을 끼칠 수 있는 경우, 이중 승인을 지원해야 한다.	환경 지원 (SRA)	

설명	관련 클래로티 솔루션	클래로티 지원 내용
SR 2.2 – 무선 사용 통제 제어 시스템은 일반적으로 통용되는 보안 업계 관행에 따라 제어 시스템으로의 무선 연결에 대한 사용 제한을 승인, 모니터링 및 강제하는 기능을 제공해야 한다.	환경 지원 (CTD, xDome)	클래로티 CTD와 xDome은 네트워크 내에서 발견되고 작동하는 모든 무선 장치를 식별할 수 있는 종합 자산 목록을 제공합니다. 이 솔루션은 통신 정책을 그룹화 및 생성하고 네트워크에 속한 이러한 장치들을 모니터링하는 기능을 제공합니다. 할당된 정책을 위반하는 무선 장치는 솔루션에서 경보를 생성하는데, 이러한 경보는 내부적으로 처리하거나 조사 및 복구를 위해 통합 SOC 솔루션으로 전달할 수 있습니다.
SR 2.2 RE 1 - 인증되지 않은 무선 장치의 식별 및 보고 제어 시스템은 제어 시스템의 물리적 환경 내에서 전송하는 인증되지 않은 무선 장치를 식별 및 보고하는 기능을 제공해야 한다.	환경 지원 (CTD, xDome)	
SR 2.5 – 세션 잠금 제어 시스템은 설정 가능한 시간 동안 유휴 상태가 지속된 후에 세션 잠금을 시작하거나 수동으로 세션 잠금을 시작하여 추가 액세스를 방지하는 기능을 제공해야 한다. 세션 잠금은 해당 세션을 소유한 사용자 또는 또 다른 인가된 사용자가 적합한 식별 및 인증 절차를 통해 액세스 권한을 재구축하기 전까지 유효상태를 유지해야 한다.	솔루션 지원 (xDome, CTD, SRA) 환경 지원 (SRA)	클래로티 솔루션은 유휴 상태가 일정 시간 지속된 후에 시스템에서 자동으로 로그아웃하는 기능을 제공합니다. 유휴 시간은 사용자가 설정할 수 있습니다.
SR 2.6 – 원격 세션 종료 제어 시스템은 설정 가능한 시간 동안 유휴 상태가 지속된 후 자동으로, 또는 세션을 시작한 사용자가 수동으로 원격 세션을 종료하는 기능을 제공해야 한다.	환경 지원 (SRA)	클래로티 SRA는 시스템 관리자/감독자가 현재의 원격 세션을 언제든지 종료할 수 있도록 지원합니다.
SR 2.7 – 동시 세션 제어 제어 시스템은 특정 사용자의 인터페이스별 동시 세션 개수를 설정 가능한 세션 개수로 제한하는 기능을 제공해야 한다.	솔루션 지원 (xDome, CTD, SRA)	클래로티 산업 솔루션은 GUI를 통한 솔루션 액세스를 위한 동시 세션 제어를 지원합니다.

설명	관련 클래로티 솔루션	클래로티 지원 내용
SR 2.8 – 감사 이벤트 제어 시스템은 액세스 제어, 요청 오류, 운영 시스템 이벤트, 제어 시스템 이벤트, 백업 및 복구 이벤트, 구성 변경, 잠재적 정찰 활동, 감사 로그 이벤트 등의 범주에 대한 보안 관련 감사 기록을 생성하는 기능을 제공해야 한다. 개별 감사 기록에는 타임 스탬프, 소스(원본 장치, 소프트웨어 프로세스 또는 사용자 계정), 범주, 유형, 이벤트 ID 및 이벤트 결과가 포함되어야 한다.	환경 지원 (xDome, CTD, SRA)	클래로티 솔루션은 솔루션 자체와 솔루션이 모니터링하는 네트워킹된 장치 모두에 대한 상세 정보를 제시하는 감사 기록을 제공합니다. 클래로티 솔루션의 시스템 상태 기록은 시스템 상태, 경보, 자산 변경, 시스템 백업 및 이벤트, 업데이트 등에 관한 상세 정보를 중앙에서 제공합니다. 클래로티 솔루션은 이러한 정보 등을 외부 시스로그 서버, SIEM, SOAR 및 기타 중앙화된 수집을 위한 대상으로 내보낼 수 있는 시스로그 통합을 지원합니다.
SR 2.8 RE 1 – 중앙 관리형 시스템 전체 감사 추적 제어 시스템은 감사 이벤트를 중앙에서 관리하고 제어 시스템 전반의 여러 구성요소로부터 얻은 감사 기록을 시스템 전체(논리적 또는 물리적)에 대한 시간 연계 감사 추적으로 컴파일하는 기능을 제공해야 한다. 제어 시스템은 보안 정보 및 이벤트 관리(SIEM)와 같은 표준 상용 로그 분석 툴을 이용한 분석을 위해 이러한 감사 기록을 업계 표준 형식으로 내보내는 기능을 제공해야 한다.	환경 지원 (xDome, CTD, SRA)	
SR 2.9 – 감사 저장 용량 제어 시스템은 로그 관리 및 시스템 구성에 대해 널리 인정되는 권장 사항에 따라 감사 기록 저장 용량을 충분히 할당해야 한다. 제어 시스템은 이러한 저장 용량이 초과될 가능성을 줄여주는 감사 메커니즘을 제공해야 한다.	환경 지원 (xDome, CTD, SRA)	클래로티 솔루션은 감사 로그를 내부에 저장하고 백업을 위해 적시에 스냅샷을 생성하는 기능을 제공합니다. 시스템 상태 검사는 내부 디스크 공간 사용에 관한 정보를 포함합니다.
SR 2.9 RE 1 - 감사 기록 저장 용량 임계치 도달 시 경고 발령 제어 시스템은 할당된 감사 기록 저장 용량이 설정 가능한 최대 감사 기록 저장 용량 비율에 도달하면 경고를 생성하는 기능을 제공해야 한다.	환경 지원 (xDome, CTD, SRA)	

설명	관련 클래로티 솔루션	클래로티 지원 내용
SR 2.10 – 감사 처리 실패 시 대응 제어 시스템은 감사 처리 실패 시 담당자에게 경보를 발령하고 필수 서비스와 기능의 손실을 방지하는 기능을 제공해야 한다. 제어 시스템은 일반적으로 통용되는 산업 관행과 권장 사항에 따라 감사 처리 실패에 대한 조치를 지원하는 기능을 제공해야 한다.	솔루션 지원 (xDome, CTD, SRA)	솔루션의 가용 저장 공간이 특정 한계에 도달하면 경보 생성과 같은 중요한 기능을 계속 실행하기 위해 저장 공간을 확보하기 시작합니다.
SR 2.11 – 타임 스탬프 제어 시스템은 감사 기록 생성에 사용할 타임 스탬프를 제공해야 한다.	솔루션 지원 (xDome, CTD, SRA)	클래로티 솔루션은 이벤트를 실시간으로 식별하고 기록된 모든 이벤트에 대해 타임스팟을 제공하며, 외부 NTP 서버에 연결하는 옵션을 추가로 제공합니다. 시스템 내 시간 소스는 관리자 액세스 권한이 있는 사용자만 구성할 수 있습니다.
SR 2.11 RE 1 - 내부 시간 동기화 제어 시스템은 설정 가능한 주파수로 내부 시스템 클럭을 동기화하는 기능을 제공해야 한다.	솔루션 지원 (xDome, CTD, SRA)	
SR 2.11 RE 2 - 시간 소스 무결성 보호 시간 소스가 무단으로 변경되지 않도록 보호해야 하며, 변경 시 감사 이벤트가 시작되어야 한다.	솔루션 지원 (xDome, CTD, SRA)	
SR 2.12 – 부인 방지 제어 시스템은 특정 사용자(사람, 소프트웨어 프로세스, 또는 장치)가 특정 작업을 수행했는지 여부를 판별하는 기능을 제공해야 한다.	솔루션 지원 (xDome, CTD, SRA)	클래로티 솔루션은 경보 해결/구성, 보고서 일정 관리, 시스템 변경, 위협 탐지 설정, 구역 규칙 등 솔루션 내에서 발생하는 모든 사용자 활동에 대한 상세 로그를 제공합니다. 모든 사용자 작업/변경은 내보내기 가능한 로그로 캡처됩니다.

FR3 - 시스템 무결성

IACS에 대한 엄격한 테스트 및 유지관리는 믿을 수 있고 안전한 운영을 보장하는 데 매우 중요합니다. 이러한 시스템은 생산을 개시하기 전에 시스템이 제대로 작동하는지 확인하기 위해 장치 테스트, 공장 인수 테스트(FAT), 현장 인수 테스트(SAT), 인증, 시운전 등 다양한 테스트 단계를 거칩니다. 잠재적인 문제를 식별하고 수정하여 운영 시 비용이 많이 들거나 잠재적으로 위험한 고장을 방지하려면 이렇게 철저한 테스트 프로세스가 반드시 필요합니다. 일단 운영이 시작되면 IACS의 무결성을 유지하는 것은 자산 소유자의 몫입니다. 여기에는 위험 평가 방법을 이용하여 IACS 내 여러 시스템, 통신 채널 및 정보에 적합한 수준의 무결성 보호를 할당하는 작업이 포함됩니다. FR3 - 시스템 무결성에서 설명했듯이 IACS의 안전한 작동을 위해서는 시스템 무결성을 보호하기 위한 종합적인 접근법이 필수적입니다.

설명	관련 클래로티 솔루션	클래로티 지원 내용
SR 3.1 – 통신 무결성 제어 시스템은 전송된 정보의 무결성을 보호하는 기능을 제공해야 한다.	솔루션 지원 (xDome, CTD, SRA)	클래로티 솔루션은 연결된 모든 구성요소(센서, CTD 서버, CTD Enterprise Management Console, xDome 컬렉터) 간 통신을 보호하고 전송되는 데이터의 오류를 검사합니다. 또한 클래로티 솔루션은 비정상적인 동작이나 기준선과의 편차를 탐지하기 위해 자산 통신을 지속적으로 모니터링함으로써 ICS 환경에서 전송되는 데이터의 무결성을 보호하는 데 효과적입니다.
SR 3.1 RE 1 – 암호화 무결성 보호 제어 시스템은 암호화 메커니즘을 사용하여 통신 시 발생하는 정보 변경을 식별하는 기능을 제공해야 한다.	솔루션 지원 (xDome, CTD, SRA)	

설명	관련 클래로티 솔루션	클래로티 지원 내용
SR 3.2 – 악성 코드 차단 제어 시스템은 보호 메커니즘을 사용하여 악성 코드 또는 승인되지 않은 소프트웨어의 영향을 방지, 탐지, 보고 및 완화하는 기능을 제공해야 한다. 제어 시스템은 보호 메커니즘을 업데이트하는 기능을 제공해야 한다.	환경 지원 (CTD, xDome)	클래로티 솔루션은 어떠한 자산에 안티바이러스 또는 EDR 솔루션이 배포되었는지 여부를 식별하고 알려진 위협 서명을 탐지하기 위해 해당 자산을 지속적으로 모니터링하여 환경 내 악성 코드의 전송 및/또는 실행을 탐지하고 보호하도록 도와줍니다. 이러한 네트워크 서명은 클래로티 솔루션의 UI에서 관리할 수 있으며, 사용자는 이를 통해 해당 서명을 편집, 활성화 또는 비활성화할 수 있습니다.
SR 3.2 RE 1 – 진입점과 출구점에서 악성 코드 차단 제어 시스템은 모든 진입점과 출구점에서 악성 코드 차단 메커니즘을 사용하는 기능을 제공해야 한다.	환경 지원 (CTD, xDome)	
SR 3.2 RE 2 - 악성 코드에 대한 중앙 관리 및 보고 제어 시스템은 악성 코드 차단 메커니즘을 관리하는 기능을 제공해야 한다.	환경 지원 (CTD, xDome)	

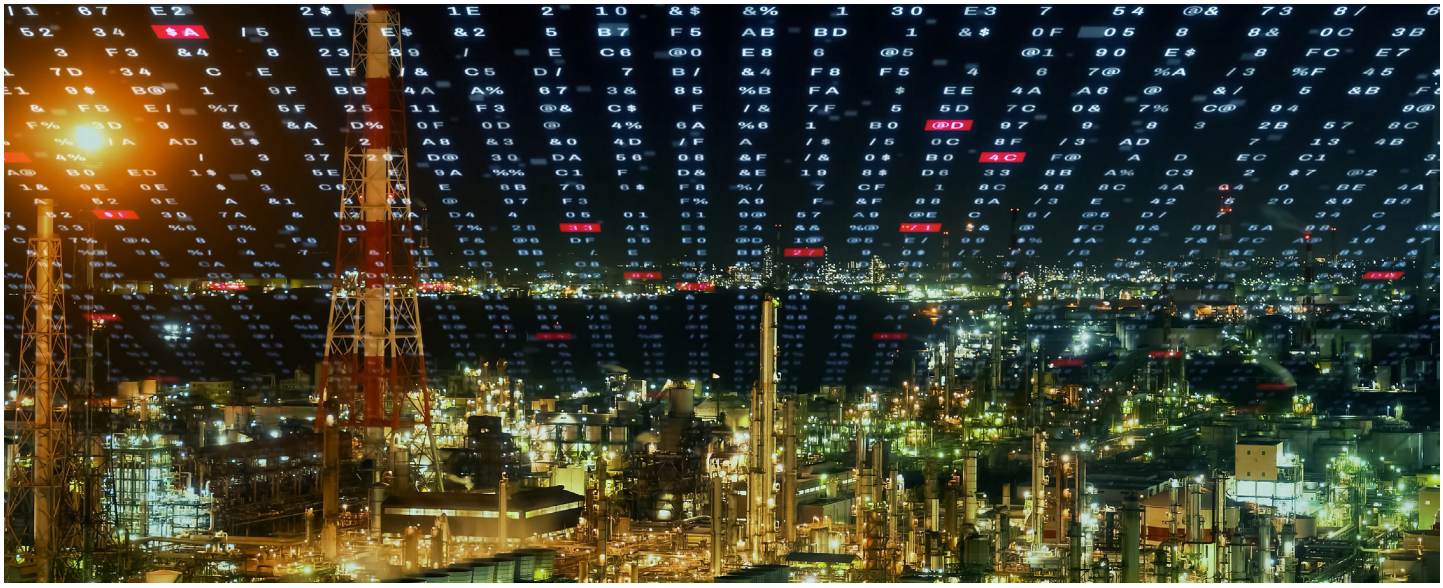
설명	관련 클래로티 솔루션	클래로티 지원 내용
SR 3.3 – 보안 기능 검증 제어 시스템은 보안 기능의 의도된 작동을 검증하고 FAT, SAT 및 계획 정비 시 이상이 발견될 경우 이를 보고하는 기능을 제공해야 한다. 이러한 보안 기능은 본 표준에 명시된 보안 요구사항을 지원하는 데 필요한 모든 요소를 포함해야 한다.	솔루션 지원 (xDome, CTD, SRA)	클래로티는 PoV, FAT 및 SAT와 계획 정비 시 보안 기능 검증을 위해 당사 플랫폼에 대해 엄격한 테스트를 수행합니다. 또한 클래로티는 알려진 위협 경보 대응을 테스트하는 방법으로, 알려진 자산에서 EICAR 테스트 파일, 호스트 및 포트 스캔을 테스트하여 경보를 생성하고 자동으로 해결하는 메커니즘을 제공합니다. 잠재적 오탐에 대한 시스템의 허용오차를 조정하기 위해 이러한 경보를 수동으로 조정할 수 있습니다.
SR 3.3 RE 1 – 보안 기능 검증을 위한 자동화된 메커니즘 제어 시스템은 자동화된 메커니즘을 사용하여 FAT, SAT 및 계획 정비 시 보안 검증 관리를 지원하는 기능을 제공해야 한다.	솔루션 지원 (xDome, CTD, SRA)	
SR 3.3 RE 2 – 정상 운영 중 보안 기능 검증 제어 시스템은 정상 운영 중 보안 기능의 의도된 작동에 대한 검증을 지원하는 기능을 제공해야 한다.	솔루션 지원 (xDome, CTD, SRA)	
SR 3.4 – 소프트웨어 및 정보 무결성 제어 시스템은 소프트웨어 및 저장 중인 정보에 대한 무단 변경을 탐지, 기록, 보고 및 차단하는 기능을 제공해야 한다.	환경 지원 (CTD, xDome)	클래로티 솔루션은 CPS 환경의 모니터링 중인 자산 내에서 소프트웨어 또는 유휴 정보가 변경될 경우 이를 식별하고 경보를 발령합니다. 이러한 경보는 자산 구성, 프로그램 또는 기능에 대한 무단 변경으로부터 시스템을 보호하는 데 효과적입니다. 대표적인 경보는 다음과 같습니다. • 구성 다운로드 • DCS 구성 변경 • 펌웨어 다운로드 • 모드 변경 • 메모리 초기화 • 온라인 편집 • 의심스러운 파일 전송 • 기타... 장치 변경 경보에 관한 전체 목록은 클래로티 사용자 설명서를 참조하십시오.
SR 3.4 RE 1 – 무결성 위반에 대한 자동화된 알림 제어 시스템은 무결성 검증 과정에서 불일치가 발견된 경우 설정 가능한 수의 수신자에게 알림을 제공하는 자동화된 툴을 사용하는 기능을 제공해야 한다.	환경 지원 (xDome, CTD, SRA)	

설명	관련 클래로티 솔루션	클래로티 지원 내용
SR 3.8 – 세션 무결성 제어 시스템은 세션의 무결성을 보호하는 기능을 제공해야 한다. 제어 시스템은 유효하지 않은 세션 ID의 사용을 거부해야 한다.	솔루션 지원 (CTD, xDome) 환경 지원 (SRA)	클래로티 솔루션은 신규 세션마다 고유 토큰을 생성하고, 로그아웃하거나 세션창을 닫아 세션을 종료한 후 토큰을 무효화함으로써 세션의 무결성을 보호합니다. 이 메커니즘은 클래로티 SRA를 사용하여 IACS 자산에 원격으로 액세스할 때도 적용되므로 세션 보안을 강화하는 데 효과적입니다.
SR 3.8 RE 1 – 세션 종료 후 세션 ID 무효화 제어 시스템은 사용자 로그아웃 또는 기타 세션 종료(브라우저 세션 포함) 시 세션 ID를 무효화하는 기능을 제공해야 한다.	솔루션 지원 (CTD, xDome) 환경 지원 (SRA)	
SR 3.8 RE 2 – 고유 세션 ID 생성 제어 시스템은 세션별 고유 세션 ID를 생성하고 예기치 않은 모든 세션 Id를 무효로 처리하는 기능을 제공해야 한다.	솔루션 지원 (CTD, xDome) 환경 지원 (SRA)	
SR 3.8 RE 3 – 세션 ID의 무작위성 제어 시스템은 일반적으로 통용되는 무작위 소스를 통해 고유 세션 ID를 생성하는 기능을 제공해야 한다.	솔루션 지원 (CTD, xDome) 환경 지원 (SRA)	
SR 3.9 – 감사 정보 보호 제어 시스템은 무단 액세스, 변경 및 삭제로부터 감사 정보와 감사 툴(존재하는 경우)을 보호해야 한다.	솔루션 지원 (xDome, CTD, SRA)	클래로티 솔루션은 세분화된 역할 기반 액세스 제어(RBAC) 설정을 통해 모든 감사 및 네트워크 정보를 보호합니다.

FR4 - 데이터 기밀성

IACS가 생성하는 정보의 중요성을 고려할 때 특정 통신 채널과 데이터 저장소에는 도청과 무단 액세스를 차단하기 위한 강력한 보호 조치가 필요합니다. 보안 조치를 시행하는 것은 데이터 유출, 운영 중단 또는 더 심각한 결과를 초래할 수 있는 잠재적 보안 위반을 방지하기 위한 중요한 활동입니다. 이러한 보호는 데이터 프라이버시를 보호하는 문제일 뿐만 아니라 각종 산업 및 인프라 운영에서 중요한 역할을 하는 제어 시스템의 전반적인 안정성과 신뢰성을 보장하기 위한 필수 요소입니다.

설명	관련 클래로티 솔루션	클래로티 지원 내용
SR 4.1 – 정보 기밀성 제어 시스템은 명시적인 읽기 권한이 지원되는 유휴/전송 정보의 기밀성을 보호하는 기능을 제공해야 한다.	솔루션 지원 (xDome, CTD, SRA)	클래로티 솔루션은 SSH 및 SSL 프로토콜을 이용하여 IACS 환경에서 수집되는 유휴/전송 정보를 보호합니다. 구역 경계를 넘어 자산에서 수집된 정보는 네트워크를 통과할 때 정보의 기밀성을 보장하기 위해 암호화를 함께 사용합니다.
SR 4.1 RE 1 - 신뢰할 수 없는 네트워크를 통해 유휴/전송 정보의 기밀성을 보호 제어 시스템은 유휴 정보를 비롯해 신뢰할 수 없는 네트워크를 통과하는 원격 액세스 세션의 기밀성을 보호하는 기능을 제공해야 한다.	솔루션 지원 (xDome, CTD, SRA)	
SR 4.1 RE 2 - 구역 경계를 지나는 정보의 기밀성 보호 제어 시스템은 모든 구역 경계를 통과하는 정보의 기밀성을 보호하는 기능을 제공해야 한다.	솔루션 지원 (xDome, CTD, SRA)	
SR 4.2 – 정보 지속성 제어 시스템은 활성 서비스로부터 해제 및/또는 폐기되는 구성요소로부터 명시적 읽기 권한이 지원되는 모든 정보를 삭제하는 기능을 제공해야 한다.	솔루션 지원 (CTD, xDome)	클래로티 솔루션은 사용자 조작 또는 자동화된 보관 규칙을 통해 자산 정보와 경보를 삭제하는 메커니즘을 제공합니다. 이러한 규칙은 솔루션 관리자가 자산 정보의 보관 기간을 정하여 설정할 수 있습니다.
SR 4.3 – 암호화 사용 암호화가 필요한 경우 제어 시스템은 일반적으로 통용되는 보안 업계 관행과 권장 사항에 따라 암호화 알고리즘, 키 크기, 키 설정 및 관리 메커니즘을 사용해야 한다.	솔루션 지원 (xDome, CTD, SRA)	클래로티는 솔루션에 액세스하는 토큰에 대해 고급 암호화 표준(AES)을 적용합니다.



FR5 - 데이터 흐름 제한

자산 소유자에 의한 위험 평가 방법은 IACS 내 정보 흐름에 대한 적합한 제한을 결정하는 데 유용하며, 맞춤형 조치를 시행하면 정보 흐름과 관련된 위험을 완화하는 데 도움이 됩니다. 제어 시스템 네트워크를 비즈니스 또는 퍼블릭 네트워크와 완전히 격리하는 것에서부터 방향 게이트웨어, 방화벽, DMZ와 같은 고급 기법을 사용하는 것까지 매우 다양한 조치가 수행될 수 있습니다. FR5 - 데이터 흐름 제한에 제시된 이러한 전략들은 무단 액세스를 방지할 뿐만 아니라 운영 효율과 강력한 보안 사이의 미묘한 균형을 유지하는 전략이기도 합니다.

설명	관련 클래로티 솔루션	클래로티 지원 내용
SR 5.1 – 네트워크 분할 제어 시스템은 제어 시스템 네트워크를 비제어식 시스템 네트워크와 논리적으로 분리하고 중요 제어 시스템 네트워크를 기타 제어 시스템 네트워크와 논리적으로 분리하는 기능을 제공해야 한다.	환경 지원 (CTD, xDome)	클래로티 솔루션은 우수한 가시성과 프로파일링을 활용하여 정상 운영 시 상호 통신할 수 있는 자산들로 구성된 논리적 그룹인 여러 구역으로 CPS를 가상으로 자동 분리합니다. 이러한 구역은 사용자 환경의 고유 통신 경로에 맞게 조정 가능하며, “정상” 네트워크 동작을 시각화하여 보여줍니다. 네트워크 분리 방법의 일환으로 클래로티 솔루션의 네트워크 보호 기능은 조직의 산업 사이버보안 태세를 강화하는 데 필수적인 제로 트러스트 관행을 위한 기반을 갖추는 데 유용합니다.
SR 5.1 RE 3 – 중요 네트워크의 논리적 및 물리적 분리 제어 시스템은 중요 제어 시스템 네트워크를 비중요 제어 시스템 네트워크와 논리적 및 물리적으로 분리하는 기능을 제공해야 한다.	환경 지원 (xDome, CTD, SRA)	

설명	관련 클래로티 솔루션	클래로티 지원 내용
SR 5.2 – 구역 경계 보호 제어 시스템은 구역 경계를 통과하는 통신을 모니터링 및 제어하여 위험 기반 구역 및 통신경로 모델에 정의된 구획화를 시행하는 기능을 제공해야 한다.	환경 지원 (CTD, xDome)	클래로티 솔루션은 위에 언급된 구역을 모니터링하여 통신 이상 현상과 정책 위반을 탐지할 수 있습니다. 이러한 이상이 탐지될 경우 시스템 관리자 및/또는 보안 담당자가 조사할 수 있도록 경보가 발령됩니다. 모니터링된 구역 통신은 정책 규칙으로 설정하여 기존 네트워크 인프라에서 시행되도록 내보낼 수 있습니다.
SR 5.2 RE 1 – 기본 거부 후 예외적 허용 제어 시스템은 기본적으로 네트워크 트래픽을 거부하고 예외적으로 네트워크 트래픽을 허용하는 기능(다른 말로 전체 거부, 예외적 허용)을 제공해야 한다.	환경 지원 (통합 - CTD, xDome)	

FR6 - 이벤트 적시 대응

보안 위반에 효과적으로 대응하기 위한 효과적인 통신 및 제어 라인을 구축하기 위해 자산 소유자는 FR6 - 이벤트 적시 대응에 설명된 대로 통신 및 보고에 대한 정책과 절차를 수립해야 합니다. 여기에는 포렌식 증거의 수집, 보고, 보존 및 상관 분석을 위한 지침 및 권장 사항의 수립이 포함됩니다. 시스템 보안을 유지하기 위해 모니터링 툴과 기법을 구현하는 것도 중요하지만 이러한 수단이 제어 시스템의 운영 성능에 부정적인 영향을 끼치지 않도록 관리하는 것도 그에 못지 않게 중요합니다. IACS 환경의 신뢰성과 효율성을 유지하려면 보안 태세와 운영 효율의 균형을 맞추는 것이 관건입니다.

설명	관련 클래로티 솔루션	클래로티 지원 내용
SR 6.1 – 감사 로그 접근성 제어 시스템은 인가된 사람 및/또는 툴이 읽기 전용으로 감사 로그에 액세스하는 기능을 제공해야 한다.	솔루션 지원 (xDome, CTD, SRA)	클래로티 솔루션의 감사 로그는 모든 사용자의 작업을 대상으로 하며 읽기 전용으로 제공됩니다.
SR 6.2 – 지속적인 모니터링 제어 시스템은 일반적으로 통용되는 보안 업계 관행과 권장 사항에 따라 모든 보안 메커니즘 성능을 지속적으로 모니터링하여 보안 위반을 적시에 탐지, 분석 및 보고하는 기능을 제공해야 한다.	환경 지원 (CTD, xDome)	클래로티 솔루션은 네트워크 트래픽의 패시브 모니터링을 통해 네트워크 자산을 지속적으로 모니터링합니다. 이러한 지속적인 모니터링을 통해 네트워크는 “정상” 네트워크 동작을 범주화하고 이상 동작, 알려진 위반 지표, 위협 서명 등 다양한 유형의 환경 위협을 추적할 수 있습니다. 설정 가능한 관련성 임계치를 만족하는 모든 이벤트는 사용자가 필요에 따라 조사하고 해결하도록 충분한 상황 정보가 포함된 경보를 자동으로 생성합니다.

FR7 - 자원 가용성

이 섹션의 주된 목표는 제어 시스템이 다양한 유형의 서비스 거부(DoS) 이벤트에 대한 탄력성을 갖추도록 하는 것입니다. 여기서 핵심은 제어 시스템 내 보안 사고가 안전계장시스템(SIS)이나 기타 안전 관련 기능을 침해하지 않도록 보장하는 것입니다. 탄력성을 확보하는 것은 IACS의 운영 무결성을 유지하는 것뿐만 아니라 시스템 장애 또는 중단으로 초래될 수 있는 잠재적 안전 위험을 차단하는 데에도 필수적입니다.

설명	관련 클래로티 솔루션	클래로티 지원 내용
SR 7.1 – 서비스 거부(DoS) 방지 제어 시스템은 서비스 거부(DoS) 이벤트 발생 시 성능 저하 모드로 작동하는 기능을 제공해야 한다.	솔루션 지원 (xDome, CTD, SRA)	클래로티 솔루션은 CPS에 대한 서비스 거부(DoS) 공격 발생 시 경보를 제공합니다. 관련된 모든 자산에 대한 요약과 영향 완화 방법에 대한 권장 사항을 포함하여 충분한 상황 정보를 제공하는 경보를 통해 이러한 공격의 영향을 제한할 수 있습니다.
SR 7.1 RE 2 – 서비스 거부(DoS)가 다른 시스템 또는 네트워크에 미치는 영향을 제한 제어 시스템은 모든 사용자(사람, 소프트웨어 프로세스 및 장치)가 다른 제어 시스템이나 네트워크에 영향을 끼치는 서비스 거부(DoS) 이벤트를 야기할 수 있는 능력을 제한하는 기능을 제공해야 한다.	솔루션 지원 (xDome, CTD, SRA)	클래로티 솔루션은 솔루션에 내장된 보안 제어의 일부로서 서비스 거부(DoS) 이벤트 발생 시 운영을 지속할 수 있습니다.

설명	관련 클래로티 솔루션	클래로티 지원 내용
SR 7.2 – 자원 관리 제어 시스템은 보안 기능을 통해 자원 사용을 제한하여 자원 고갈을 방지하는 기능을 제공해야 한다.	솔루션 지원 (xDome, CTD, SRA)	클래로티 솔루션은 시스템 상태 정보 인터페이스에서 디스크/CPU 사용에 대한 내부 자원 관리 옵션을 제공하여 보안 기능을 저해할 수 있는 자원 고갈을 방지하는 데 효과적입니다.
SR 7.3 – 제어 시스템 백업 제어 시스템은 정상적인 공장 운영에 영향을 주지 않고 중요 파일의 ID와 위치를 확인하고 사용자 수준 및 시스템 수준 정보를 백업할 수 있는 능력을 지원해야 한다.	솔루션 지원 (xDome, CTD, SRA)	클래로티 솔루션은 플랫폼을 통해 데이터의 일회성/예약 백업 생성을 지원합니다. 이러한 백업 데이터에는 시스템 구성, 데이터(자산, 인사이트, 경보 포함), 이벤트 및 PCAP 파일(필요 시)이 기본적으로 포함됩니다. 이러한 백업은 사용자가 정의한 시간 및 주기로 예약할 수 있습니다. 백업 파일은 로컬로, 또는 SMB 공유를 통해 저장할 수 있으며 중앙 인터페이스를 통해 생성할 수 있습니다.
SR 7.3 RE 1 – 백업 검증 제어 시스템은 백업 메커니즘의 신뢰성을 검증하는 기능을 제공해야 한다.	솔루션 지원 (xDome, CTD, SRA)	
SR 7.3 RE 2 – 백업 자동화 제어 시스템은 설정 가능한 주기로 백업 기능을 자동화하는 기능을 제공해야 한다.	솔루션 지원 (xDome, CTD, SRA)	
SR 7.6 – 네트워크 및 보안 구성 설정 제어 시스템은 제어 시스템 공급자가 제공한 지침에 설명되어 있는 권장 네트워크 및 보안 구성에 따라 구성되는 기능을 제공해야 한다. 제어 시스템은 현재 배포된 네트워크 및 보안 구성 설정에 대한 인터페이스를 제공해야 한다.	솔루션 지원 (xDome, CTD, SRA)	클래로티 솔루션은 유연한 배포 옵션을 유지하며 배포 환경에 따라 구성이 가능합니다. 클래로티는 사용자의 환경 평가를 바탕으로 해당 환경의 보안 정책과 목표에 적합한 구성을 사용자에게 추천합니다.

설명	관련 클래로티 솔루션	클래로티 지원 내용
SR 7.7 – 최소 기능 제어 시스템은 불필요한 특정 기능, 포트, 프로토콜 및/또는 서비스의 사용을 금지 및/또는 제한하는 기능을 제공해야 한다.	솔루션 지원 (xDome, CTD, SRA)	클래로티 솔루션은 관리자가 사용자 구성 및 테스트를 통해 플랫폼에서 불필요한 기능과 서비스 및 포트의 사용을 제한/금지하도록 지원함으로써 최소한의 기능 요구사항을 제공합니다.
SR 7.8 – 제어 시스템 구성요소 목록 제어 시스템은 설치된 구성요소 및 관련 속성에 대한 현재 목록을 보고하는 기능을 제공해야 한다.	환경 지원 (CTD, xDome)	클래로티 솔루션은 광범위한 CPS 프로토콜 라이브러리와 다양한 발견 방법(패시브, 안전 쿼리, 클래로티 Edge, 프로젝트 파일 분석 및 에코시스템 통합)을 활용하여 네트워킹된 자산에 대한 심층적이고 종합적인 목록을 생성합니다. 이렇게 다양한 스펙트럼의 자산 발견 방법을 통해 기존의 표준이나 IT 중심 발견 기법으로는 액세스하기 어려운 네트워크 영역도 찾아낼 수 있습니다.

결론

ISA/IEC-62443-3-3 프레임워크의 기본 요구사항(FR)과 시스템 요구사항(SR)은 날로 고조되는 사이버위협 환경 속에서 산업 자동화 및 제어 시스템(IACS)을 보호하는 사이버보안 수단의 역할을 조명하고 있습니다. 산업 환경과 운영 기술 네트워크의 복잡성에 대응하려면 이러한 맞춤형 사이버보안 접근법이 필요하다는 것을 이 프레임워크를 통해 알 수 있습니다. 클래로티 xDome, Continuous Threat Detection(CTD), Secure Remote Access(SRA)를 포함한 클래로티의 산업 사이버보안 솔루션은 ISA/IEC-62443-3-3 프레임워크의 다양한 기본 요구사항에 맞춰 OT 네트워크 고유의 과제를 해결하도록 설계되었습니다. 위의 섹션들은 클래로티의 산업 솔루션이 이 프레임워크의 기본 요구사항을 지원하기 위해 솔루션 지원과 환경 지원을 모두 제공하여 산업 시스템의 보호와 지속적인 운영을 어떻게 보장하는지 자세히 보여줍니다.

클래로티의 산업 사이버보안 솔루션 제품군에 관한 자세한 내용은 https://claroty.com/industrial-cybersecurity에서 확인하실 수 있습니다.

클래로티 소개

클래로티는 산업, 의료, 상업 및 공공 부문의 조직들이 자사 환경의 모든 사이버-물리 시스템(확장된 사물 인터넷, XIoT)을 보호하도록 지원합니다. 클래로티의 통합 플랫폼은 고객의 기존 인프라와 통합되어 가시성, 위험 및 취약점 관리, 네트워크 보호, 위협 탐지 및 보안 원격 액세스를 위한 총체적인 제어 기능을 제공합니다.

세계 최대 투자회사와 산업 자동화 업체가 후원하는 클래로티는 전 세계 수백 개 조직이 운영하는 수천 개의 현장에 배포되고 있습니다. 본사는 미국 뉴욕에 있으며 유럽, 아시아태평양 및 중남미 지역에서 지사를 운영하고 있습니다.

자세한 정보는 claroty.com에서 확인하실 수 있으며 이메일(contact@claroty.com)로 문의하셔도 됩니다.

CLAROTY