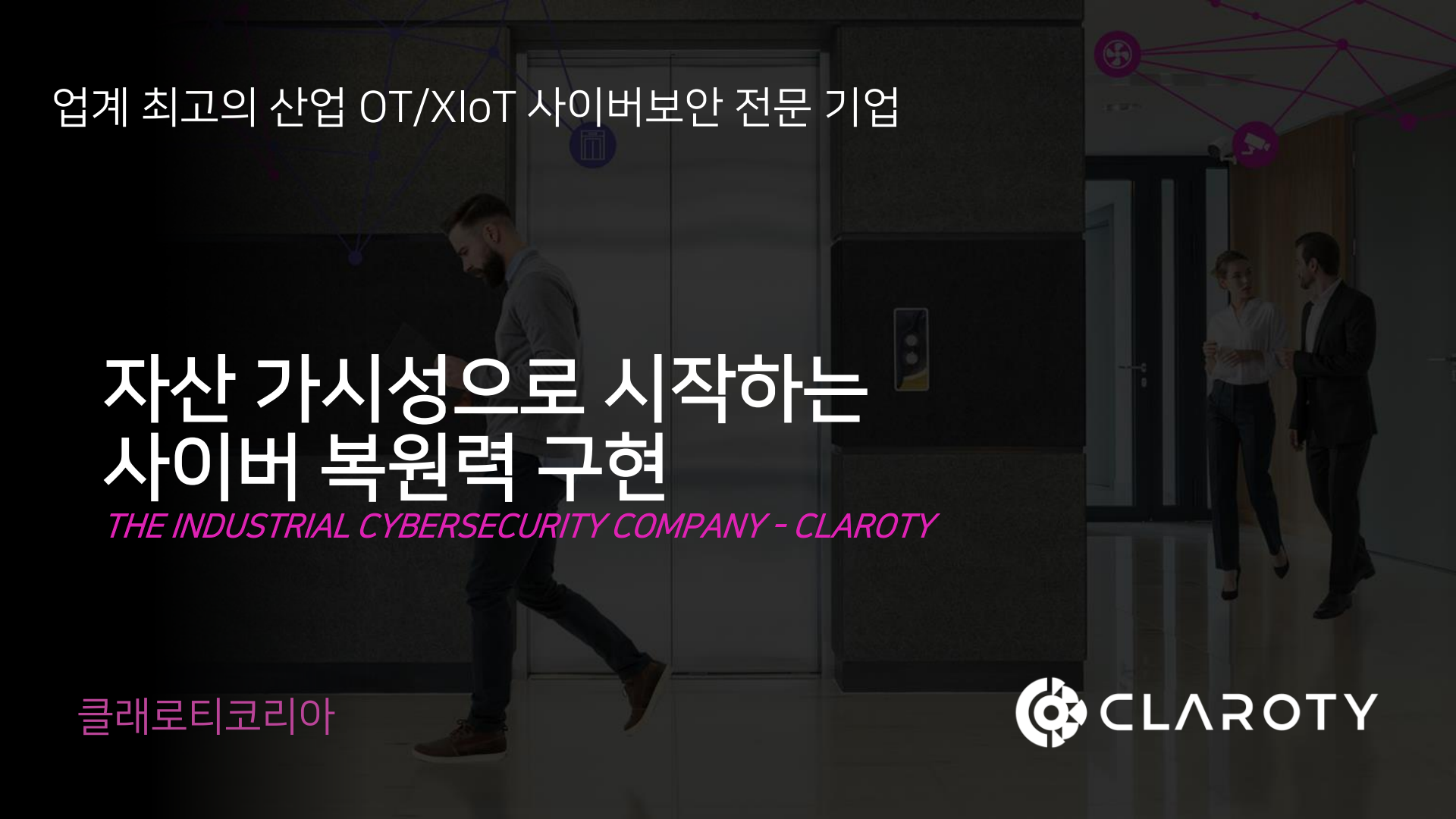


업계 최고의 산업 OT/XIoT 사이버보안 전문 기업

자산 가시성으로 시작하는 사이버 복원력 구현

THE INDUSTRIAL CYBERSECURITY COMPANY - CLAROTY

클래로티코리아

CLAROTY

정완채 수석 | OT/XIoT 사이버 보안팀 | 클래로티 코리아

EMAIL
Wanchae.j@claroty.com

[12년 이상 공장 자동화 (FA) 및 공정 자동화 (PA) 산업군 경력]
오일&가스 | 석유화학 | 철강 | 발전소 | 전력 그리드 | 식음료 | 수처리 | 자동차 | 빌딩 | 기계 | 선박 | 공항 | 디스플레이 | 물류 | 제조 | 해양 플랜트 외

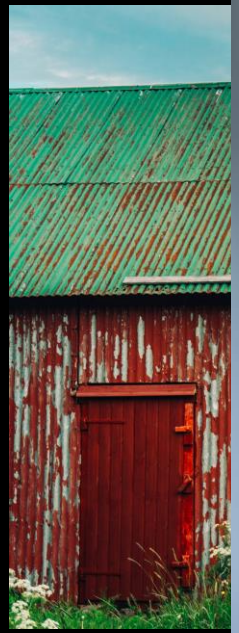
[주요 경력 사항]

클래로티 코리아	: 사이버 보안 솔루션 수석 엔지니어, 클래로티코리아
슈나이더 일렉트릭 코리아	: 안전 시스템 & 디지털 솔루션 기술 컨설턴트 크리티컬 & 안전 시스템 리드 엔지니어
한국 미쓰비시전기	: DCS, SCADA, PLC, HMI 기술영업 엔지니어

[자격 사항]
Functional Safety Engineer, SIS #13770/17　자격: TÜV Rheinland | Germany
사이버보안 표준 회원, ISA(국제자동화협회)

“

여러분이 강도로부터 집을 지켜야 한다면
가장 먼저 할 일은 어떤 것이 떠오르나요?



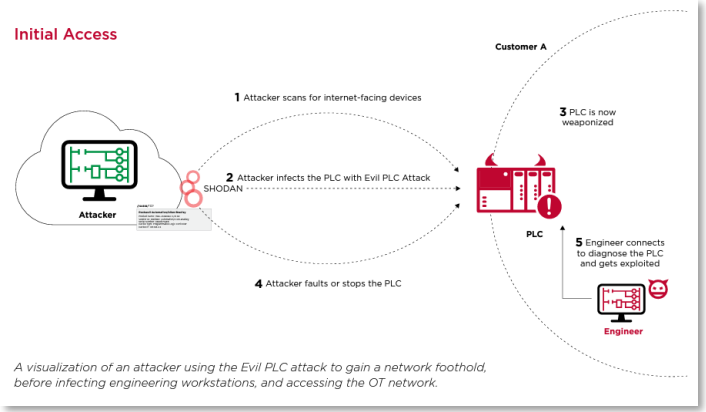
변화하는 사이버 공격 패러다임

사악한 PLC 공격 (Evil PLC Attack)

공격 시나리오1

1) 외부 공격자가 PLC에 악성코드 입력.

2) 감염된 PLC가 엔지니어링 컴퓨터를 (EWS) 감염.

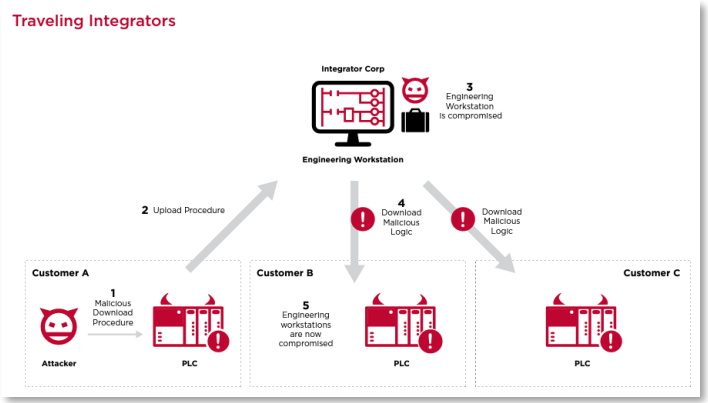


A visualization of an attacker using the Evil PLC attack to gain a network foothold, before infecting engineering workstations, and accessing the OT network.

공격 시나리오2

1) 감염된 PLC가 연결된 EWS 감염.

2) 감염된 EWS가 다른 설비 및 네트워크의 PLC로 악성 코드 전파.

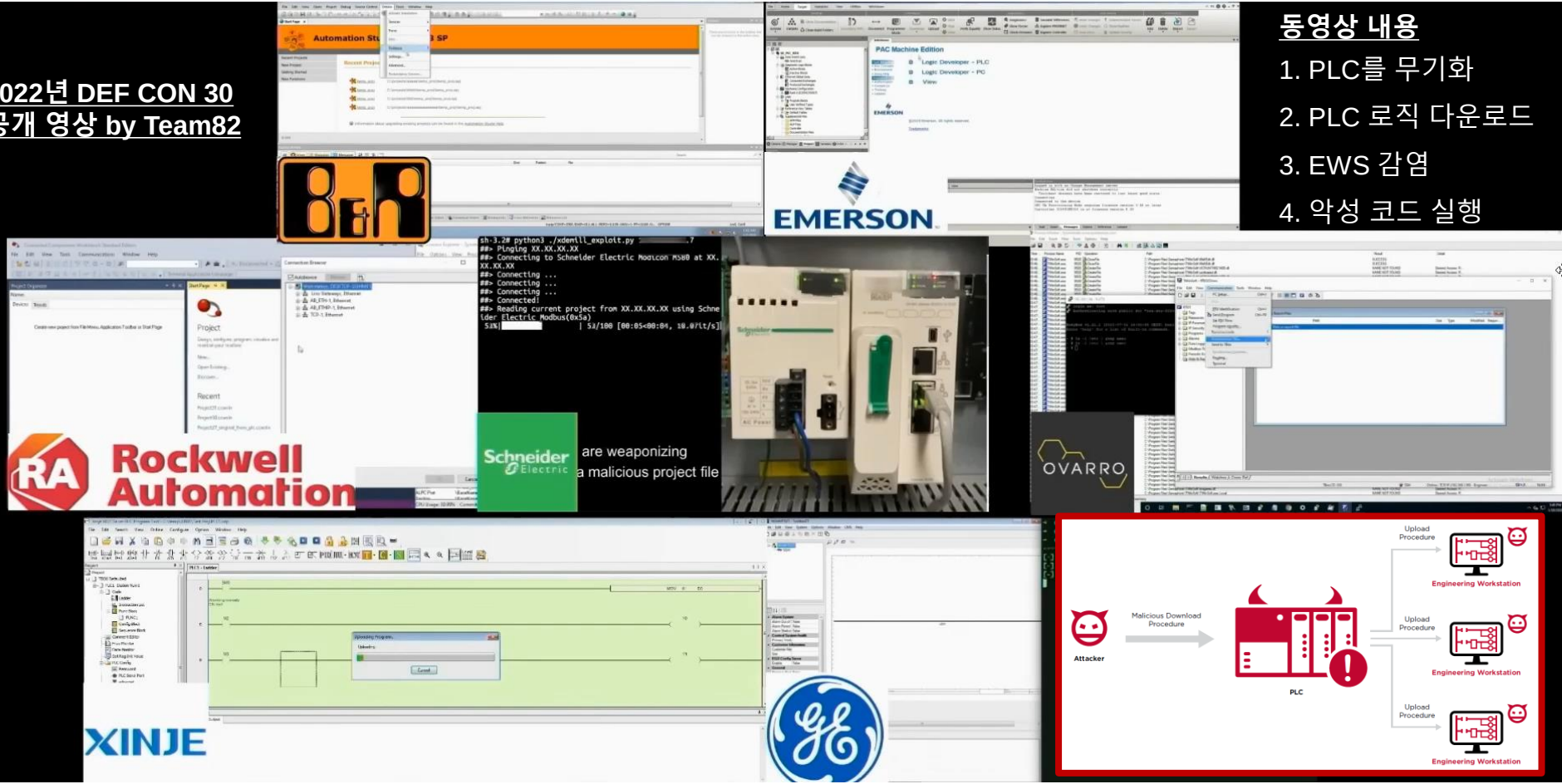


CLAROTY

2022년 DEF CON 30
공개 영상 by Team82

동영상 내용

1. PLC를 무기화
2. PLC 로직 다운로드
3. EWS 감염
4. 악성 코드 실행



잠재적인 보안 위험을 내포한 XIoT 자산들

State of XIoT Security Report – 1H 2022

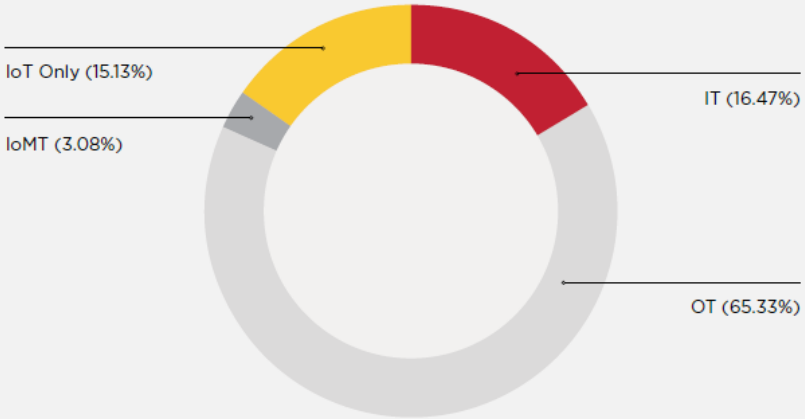
공개된 전체 취약점 수

747

영향 받은 제조사 수

86

XIoT 취약점 분류



위험 조치

71%

완전 조치 : 모든 제품은 패치 및 업데이트로 조치 가능

20%

부분 조치 : 일부 제품은 패치 및 업데이트 없음

9%

조치 불가 : 패치 및 업데이트 등 위험 최소화 방안 없음

T82 THE CLAROTY RESEARCH TEAM

CLAROTY

XIoT 사이버 보안 회사 클래로티의 연구 조직인 Team82는 고유의 위협 시그니처, 통신 프로토콜 분석, 산업/의료/상업 분야에서의 취약점 발견 및 공개를 개발한 것으로 유명한 OT 연구자 그룹입니다

운영 / 사이버 레질리언스(복원력)

단순 방어 개념에서 탈피, 지속적인 평가와 보완 필요

사이버 레질리언스를 얻기 위한 여정

가시성 → 조치 → 통합 → 최적화

1. 자산 식별

전사적 XIoT 자산 가시성 및 통신 프로파일링 기능을 제공

2. 취약점 & 위험성 관리

운영 네트워크의 취약성을 식별하고 위험성 해결 작업의 우선순위를 지정하여 지속적인 보안 상태 관리 및 규정 준수를 지원합니다.

3. 네트워크 보호

맞춤형 권장 사항과 액세스 제어를 통해 네트워크를 세분화하여 운영 환경에서 제로 트러스트 아키텍처를 지원합니다.

4. 위협 탐지

위협을 탐지하고 기존 SOC 솔루션과 통합하여 운영에 영향을 미치기 전에 사이버 공격 위험을 완화합니다.

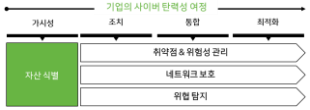
CLAROTY INDUSTRIAL

자산 식별

사이버 탄력성 여정의 시작

클래로티 xDome

자산 식별 – 자산 인벤토리 최신화



당면과제

- 모든 자산을 식별 가능?
- 모든 세부 정보를 수집 가능?
- 정확한 데이터인가?
- 단일 데이터베이스로 통합 가능?

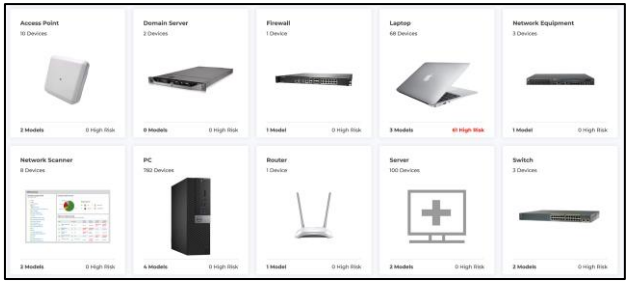
유연하고 간편한 XIoT 검색 옵션을 통해 **구현 시간과 복잡성을 저감**

산업계 전문성을 바탕으로 **모든 자산에 대해 맹점을 없애고 완전한 가시성 확보**

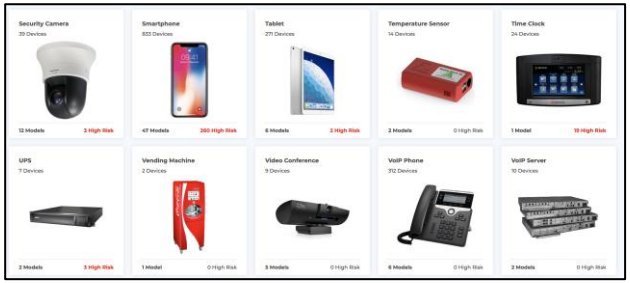
자산 관리 통합으로 **전사적 자산 데이터베이스 보안 위생**을 최적화

450개 이상의 프로토콜을 지원하여 보안 성숙도에 필요한 **모든 세부 정보 파악**

IT



IoT

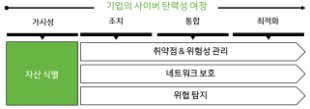


IoMT

BMS

클래로티는 XIoT의 자산 가시성에 있어 논란의 여지가 없는 선두 기업입니다. xDome은 SaaS 방식의 클라우드 플랫폼으로 새로운 장치가 출시되도 신속한 업데이트를 통해 자산 탐지 정확도를 100% 가까이 유지할 수 있습니다.

자산 식별 – 자산 정보 자동 수집



당면과제

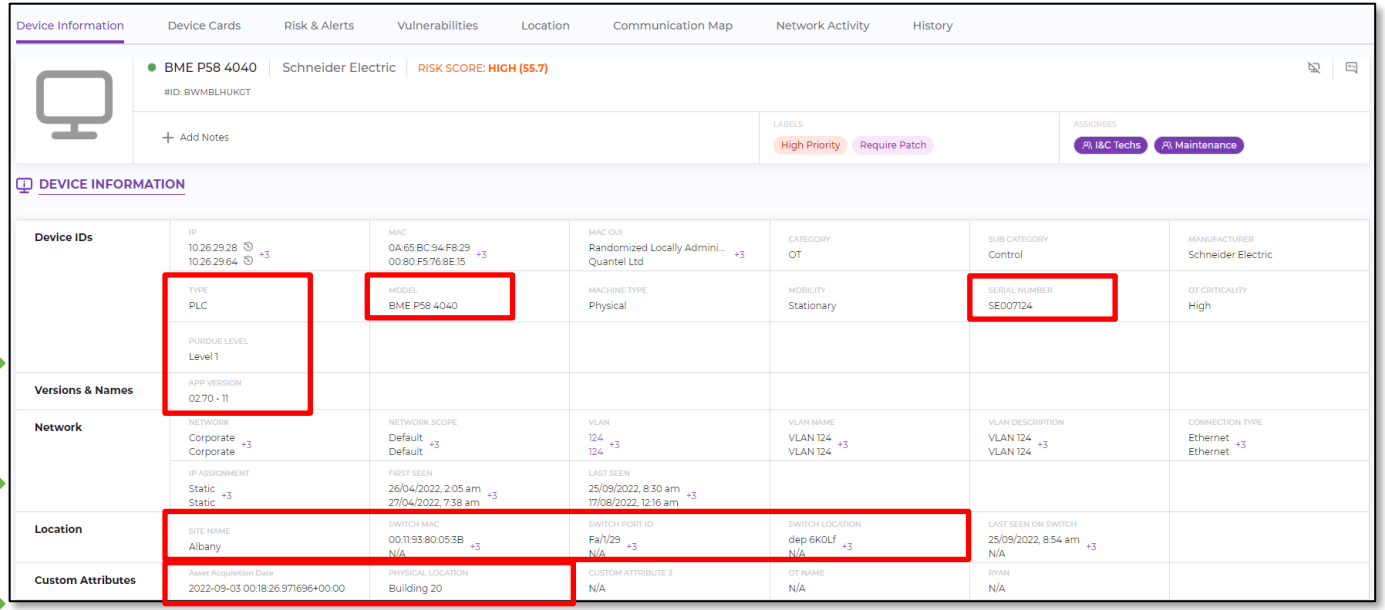
- 모든 자산을 식별 가능?
- 모든 세부 정보를 수집 가능?
- 정확한 데이터인가?
- 단일 데이터베이스로 통합 가능?

유연하고 간편한 XIoT 검색 옵션을 통해 **구현 시간과 복잡성을 저감**

산업계 전문성을 바탕으로 **모든 자산에 대해 맹점을 없애고 완전한 가시성 확보**

자산 관리 통합으로 **전사적 자산 데이터베이스 보안 위생**을 최적화

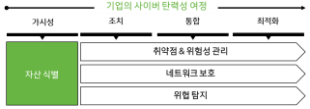
450개 이상의 프로토콜을 지원하여 보안 성숙도에 필요한 **모든 세부 정보 파악**



XIoT 자산의 장치 종류, 모델명, 시리얼 번호, 펌웨어 버전 등 상세한 정보를 기반으로 정확한 취약점, 제조사 서비스 지원 종료, 패치 및 업데이트 필요 여부 등 최적의 자산 관리가 가능합니다.

클래로티 xDome

자산 식별 – 모듈 단위의 가시성



당면과제

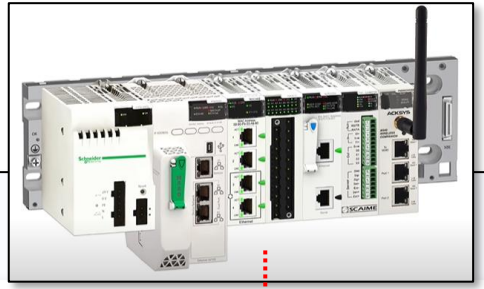
- 모든 자산을 식별 가능?
- 모든 세부 정보를 수집 가능?
- 정확한 데이터인가?
- 단일 데이터베이스로 통합 가능?

유연하고 간편한 XIoT 검색 옵션을 통해 **구현 시간과 복잡성을 저감**

산업계 전문성을 바탕으로 **모든 자산에 대해 맹점을 없애고 완전한 가시성 확보**

자산 관리 통합으로 **전사적 자산 데이터베이스 보안 위생**을 최적화

450개 이상의 프로토콜을 지원하여 보안 성숙도에 필요한 **모든 세부 정보 파악**



오직 클래로티만 가능

DEVICE CARDS

Device Cards (6)

Slot 0 - Empty	Slot 1 - Empty	Slot 2 - Network Card 2	Slot 3 - Network Card 3	Slot 4 - Network Card 4	Slot 5 - Empty	Slot 6 - Network Card 6	Slot 7 - Network Card 7	CARD NAME Network Card 7	CARD TYPE Network Card	Slot 8 - CPU 8	CARD NAME CPU 8	CARD TYPE CPU
								CARD MODEL TM221CE16R	CARD MANUFACTURER Schneider Electric		CARD MODEL BME P58 4040	CARD MANUFACTURER Schneider Electric
								CARD APP VERSION 1.5.0.1	CARD SERIAL NUMBER SE007125		CARD APP VERSION 02.70 - 11	CARD SERIAL NUMBER SE007130
								CARD IP 10.26.29.64	CARD MAC 00:80:F5:76:8E:15		CARD OS Proprietary	CARD SLOT NUMBER 8

xDome은 PLC 같은 컨트롤러를 구성하는 개별 모듈 정보까지 수집할 수 있습니다. 제조사와 모델명 뿐 아니라 펌웨어, 시리얼 번호까지 취득할 수 있기 때문에 모듈 단위의 취약점, 제품 단종 또는 서비스 종료 같은 자산 관리도 가능해집니다.

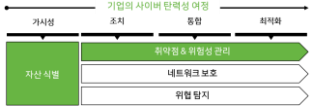
CLAROTY INDUSTRIAL

취약점 & 위험관리

사이버 탄력성 여정의 2단계

클래로티 xDome

취약점 & 위험 관리 – 조치 우선 순위 결정



당면과제

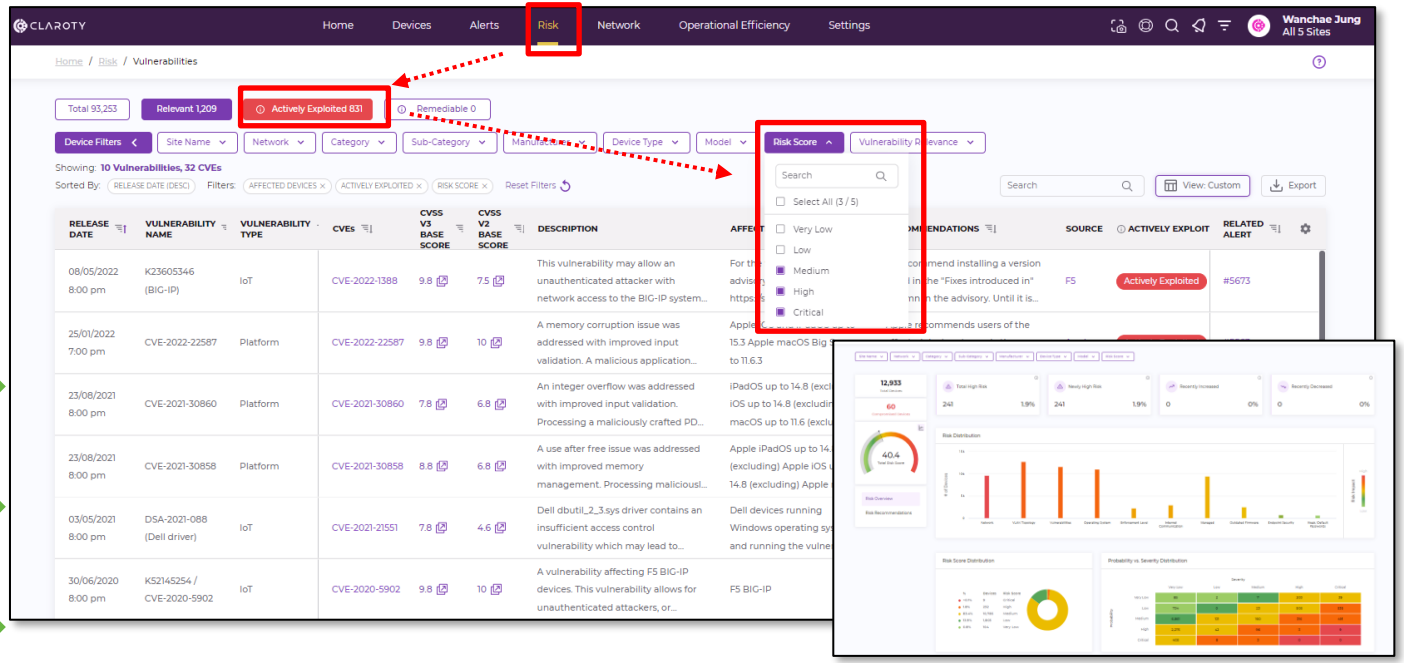
- 취약점 식별 및 조치 우선 순위?
- 간단한 절차로 사전조치 방식?
- 산업환경에 적합한 분석 툴?
- 조직에 맞는 위험성 산정 기준?

Team82의 심도 있는 취약점 연구 데이터로 산업 환경 전반에 걸쳐 **잠재된 위험을 식별**

3rd Party 취약점 통합으로 **OT 환경안의 IT 위험성을 쉽게 파악**

다중 요소 위험 스코어로 악용될 가능성이 가장 높은 자산의 **조치 우선 순위 결정**

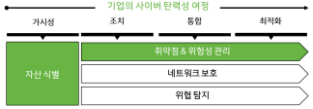
유연한 작업절차 및 보고서 옵션을 통해 **문제 해결 작업을 간소화**



특정 산업 환경에서는 해결해야 할 취약성이 수천 개에 달할 수 있습니다. xDome은 현재 적극적으로 악용되고 있는 알려진 취약성을 표시 가능 합니다. 따라서, 실제 발생할 가능성이 높은 위험을 파악하고 효과적인 대응 우선 순위를 정할 수 있습니다.

클래로티 xDome

취약점 & 위험 관리 – 위험 완화 작업



당면과제

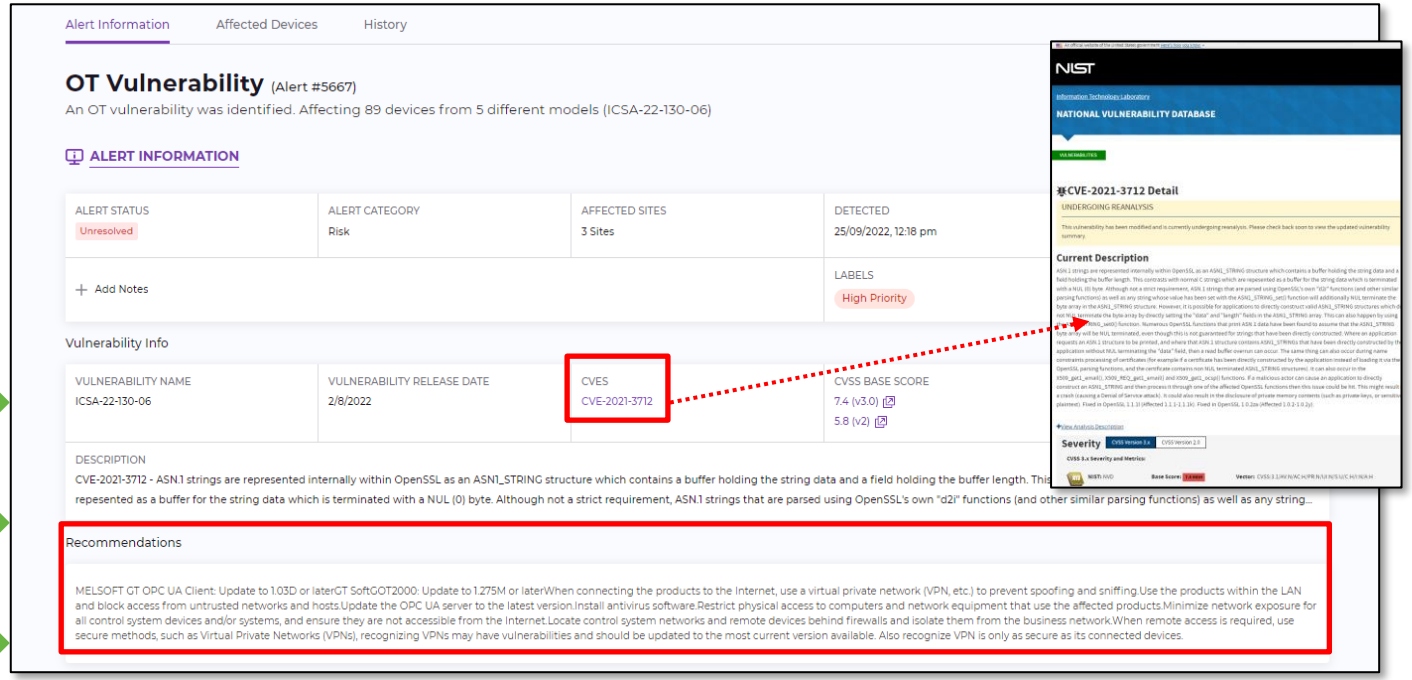
- 취약점 식별 및 조치 우선 순위?
- 간단한 절차로 사전조치 방식?
- 산업환경에 적합한 분석 툴?
- 조직에 맞는 위험성 산정 기준?

Team82의 심도 있는 취약점 연구 데이터로 산업 환경 전반에 걸쳐 **잠재된 위험을 식별**

3rd Party 취약점 통합으로 **OT 환경안의 IT 위험성을 쉽게 파악**

다중 요소 위험 스코어로 악용될 가능성이 가장 높은 자산의 **조치 우선 순위 결정**

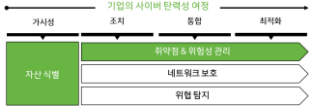
유연한 작업절차 및 보고서 옵션을 통해 **문제 해결 작업을 간소화**



xDome은 CISA, ICS 벤더 뿐 아니라 Team82가 공개한 방대한 양의 CVE DB를 기반으로 취약점별로 권장 조치사항을 제공합니다. 사용자는 취약점 정보 분석에 소요되는 시간을 절약하고 보다 효율적으로 대응할 수 있습니다.

클래로티 xDome

취약점 & 위험 관리 – 중대 취약점 공지



당면과제

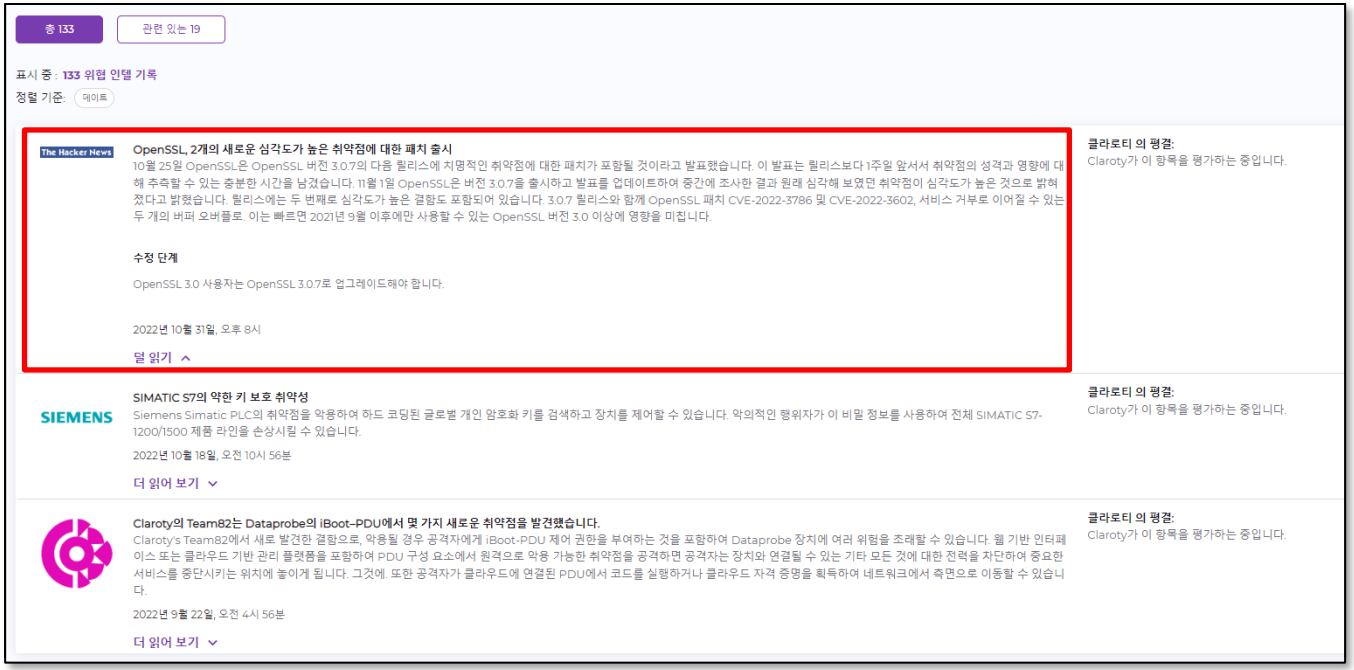
- 취약점 식별 및 조치 우선 순위?
- 간단한 절차로 사전조치 방식?
- 산업환경에 적합한 분석 툴?
- 조직에 맞는 위험성 산정 기준?

Team82의 심도 있는 취약점 연구 데이터로 산업 환경 전반에 걸쳐 **잠재된 위험을 식별**

3rd Party 취약점 통합으로 OT **환경안의 IT 위험성을 쉽게 파악**

다중 요소 위험 스코어로 악용될 가능성이 가장 높은 자산의 **조치 우선 순위 결정**

유연한 작업절차 및 보고서 옵션을 통해 **문제 해결 작업을 간소화**



xDome은 긴급 대응이 필요한 최신 취약점 정보와 대응방안을 매우 빠르고 간결하게 제공합니다. 보안 담당자는 이를 토대로 적시에 대책을 마련할 수 있습니다.

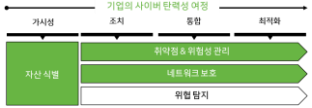
CLAROTY INDUSTRIAL

네트워크 보호

사이버 탄력성 여정의 3단계

클래로티 xDome

네트워크 보호



당면과제

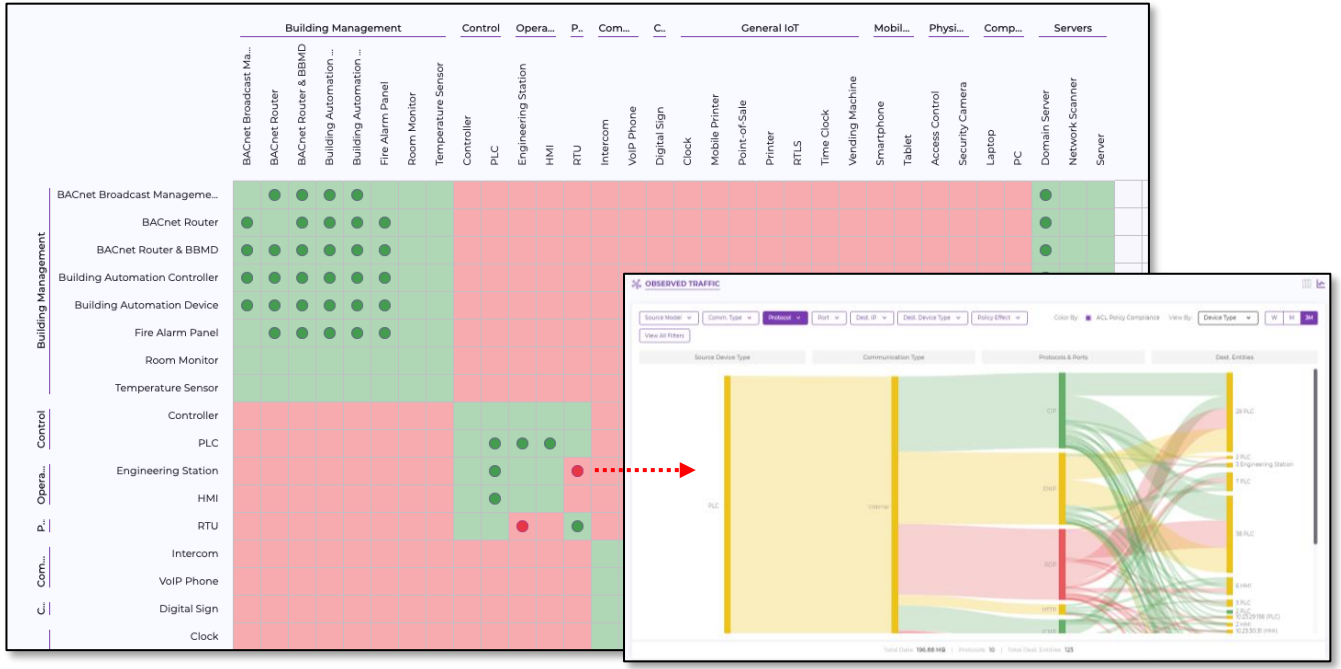
- 모든 취약점에 패치 및 수정불가.
- 네트워크 제어로 위험 완화 필요.
- 필수, 불필요한 통신의 구분.
- 적절한 네트워크 세분화.

운영 환경과 보안 조직의 정책에 의한 **네트워크 세분화 프로그램**

통신 정책을 손쉽게 정의하고 설정하여 **비인가 행위를 신속 탐지**

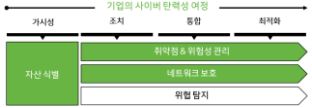
기존 인프라에서 세분화된 정책 적용을 통해 **위협으로부터 보호**

규제 및 조직의 규정 준수 모니터링



기존 IT 보안 툴은 자산 가시성이 충분하지 않아 방화벽/NAC 장치의 잘못된 룰 설정으로 오탐지나 과탐지로 설비 전체가 다운될 수 있습니다. xDome은 통신 정책 모니터링을 통해 엑세스 제어 설정 적용 전 충분한 검증 작업을 돕습니다.

네트워크 보호 - 권장 정책



당면과제

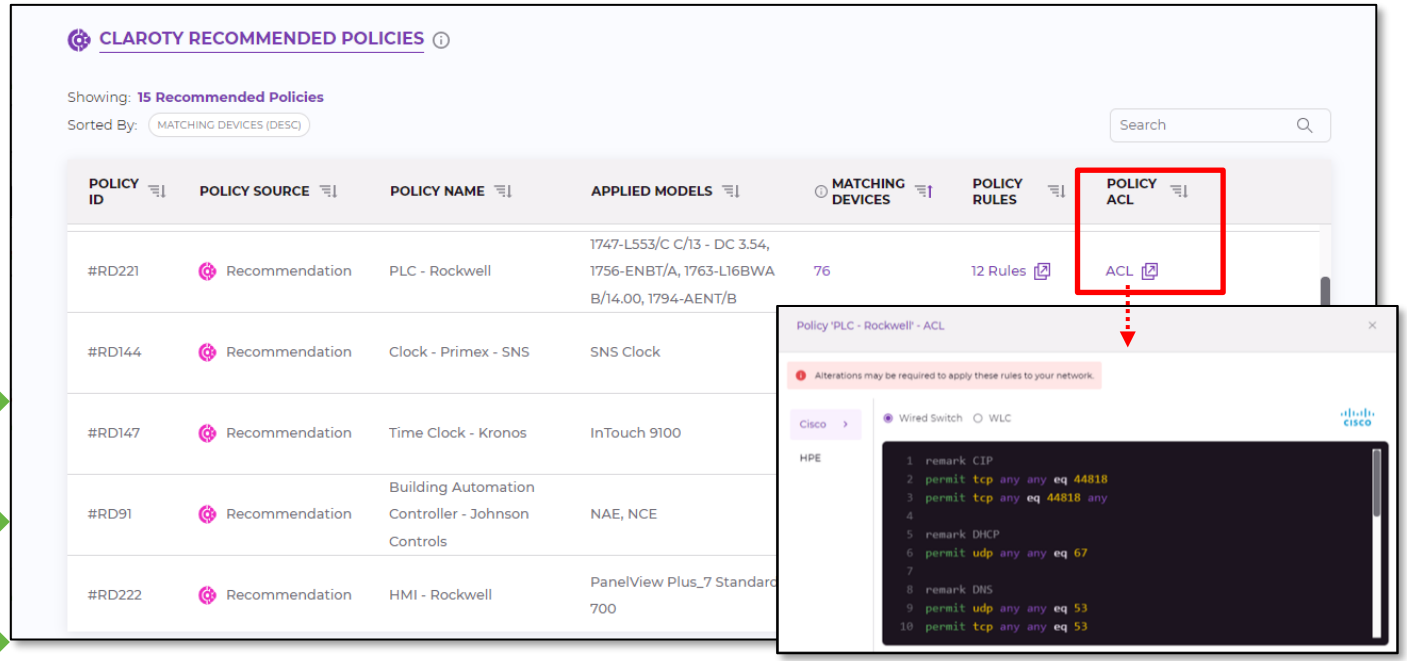
- 모든 취약점에 패치 및 수정불가.
- 네트워크 제어로 위험 완화 필요.
- 필수, 불필요한 통신의 구분.
- 적절한 네트워크 세분화.

운영 환경과 보안 조직의 정책에 의한 **네트워크 세분화 프로그램**

통신 정책을 손쉽게 정의하고 설정하여 **비인가 행위를 신속 탐지**

기존 인프라에서 세분화된 정책 적용을 통해 **위협으로부터 보호**

규제 및 조직의 규정 준수 모니터링



xDome은 자산 타입, 퍼듀 레벨, 통신 프로토콜 정보를 기반으로 방화벽, 스위치 또는 NAC에 의해 시행될 수 있는 정책을 자동으로 생성합니다. 네트워크 관리자는 정책 적용 전 커맨드 리뷰, 모니터링 후 간단히 적용할 수 있습니다.

위협 탐지

사이버 탄력성 여정의 4단계

위협 탐지 – 알려진 위협 탐지

당면과제

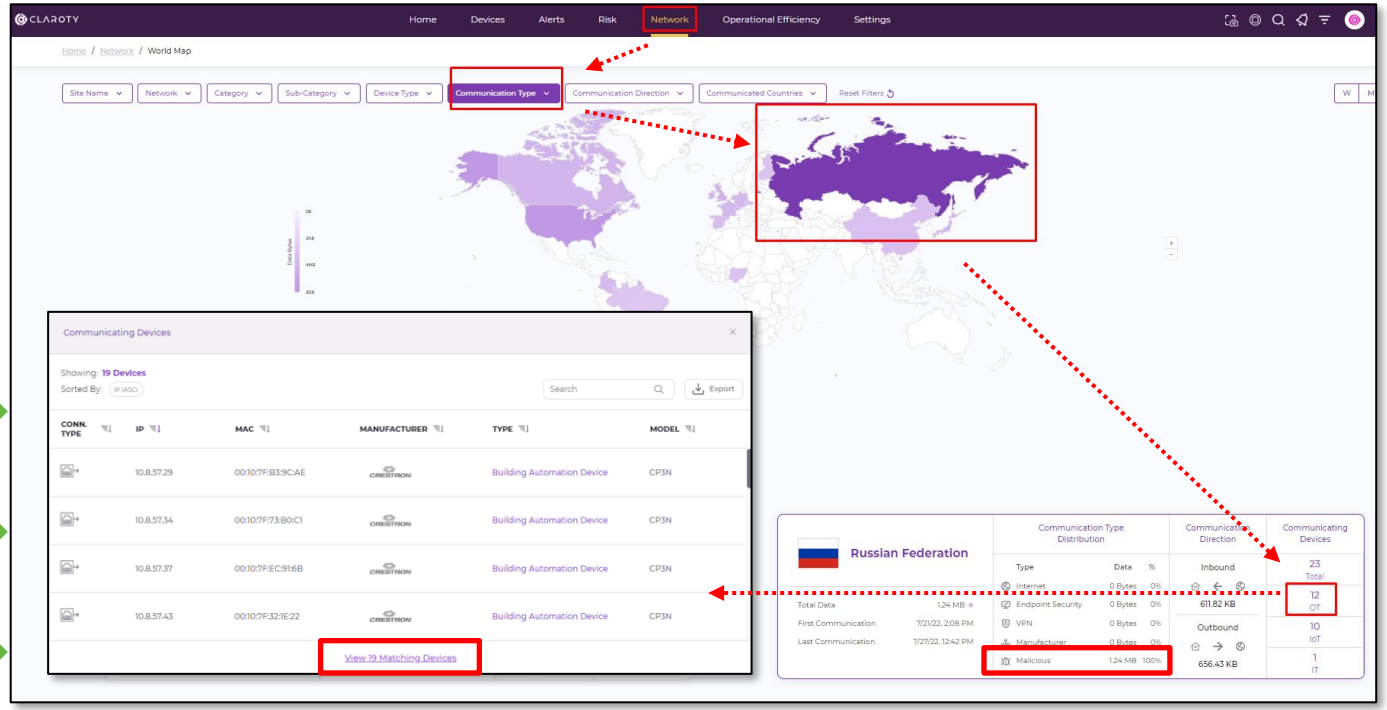
- OT환경의 위협요소 모니터링.
- OT환경에 부적합한 IT 보안 툴.
- 탐지되지 않는 새로운 위협.
- 기존 IT SOC 활용이 어려움.

악의적인 엔티티 (Entity)와의 통신을 식별하여 **공격 벡터 탐지**

솔루션 통합을 통해 알려진 위협을 탐지하고 **오탐지를 감소**

네트워크 정책 위반으로 인한 **알려지지 않은 위협 탐지**

기존 SOC 환경 (SIEM, SOAR 등)과 연동



xDome은 자체 위협 인텔리젼스과 다른 플랫폼의 위협 인텔리전스까지 활용해 IP, DNS, 악성 도메인 외에도 기타 알려진 지표로 수많은 알려진 위협을 탐지할 수 있습니다.

클래로티 xDome

위협 탐지 – 새로운 위협 탐지

당면과제

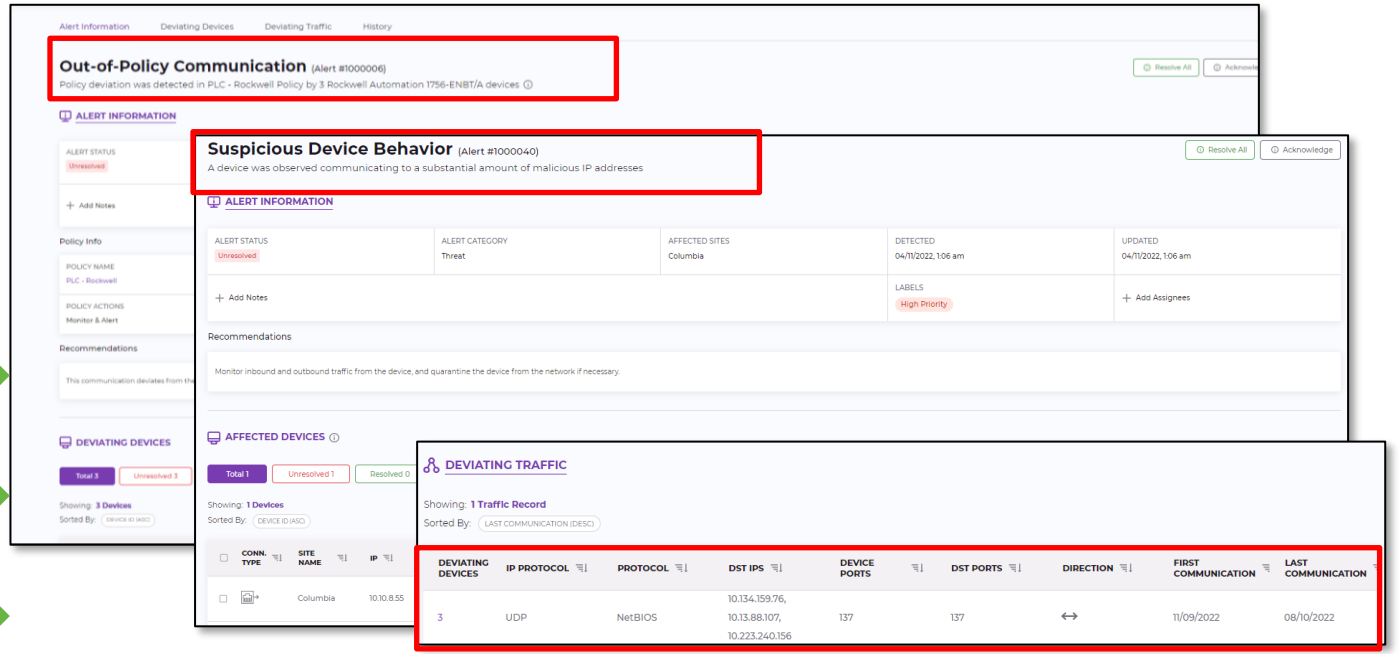
- OT환경의 위협요소 모니터링.
- OT환경에 부적합한 IT 보안 툴.
- 탐지되지 않는 새로운 위협.
- 기존 IT SOC 활용이 어려움.

악의적인 엔티티 (Entity)와의 통신을 식별하여 **공격 벡터 탐지**

솔루션 통합을 통해 알려진 위협을 탐지하고 **오탐지를 감소**

네트워크 정책 위반으로 인한 **알려지지 않은 위협 탐지**

기존 SOC 환경 (SIEM, SOAR 등)과 연동



xDome은 새로운 위협도 효과적으로 탐지합니다. 반복되는 로그인 실패나 운영상 관계 없는 자산 간의 의심스러운 행위 또는 통신 정책 위반 발생 시 경고를 발생 합니다.

클래로티 xDome

기업의 산업 사이버보안 여정을 위한 SaaS 기반의 클라우드 솔루션

취약점 및 위험 관리

네트워크 보호

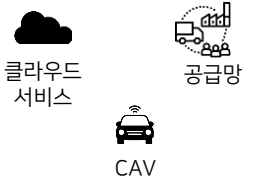
위협 탐지

자산 / 네트워크 / 데이터 가시성

유연한 배포

역할별 UX

통합 생태계



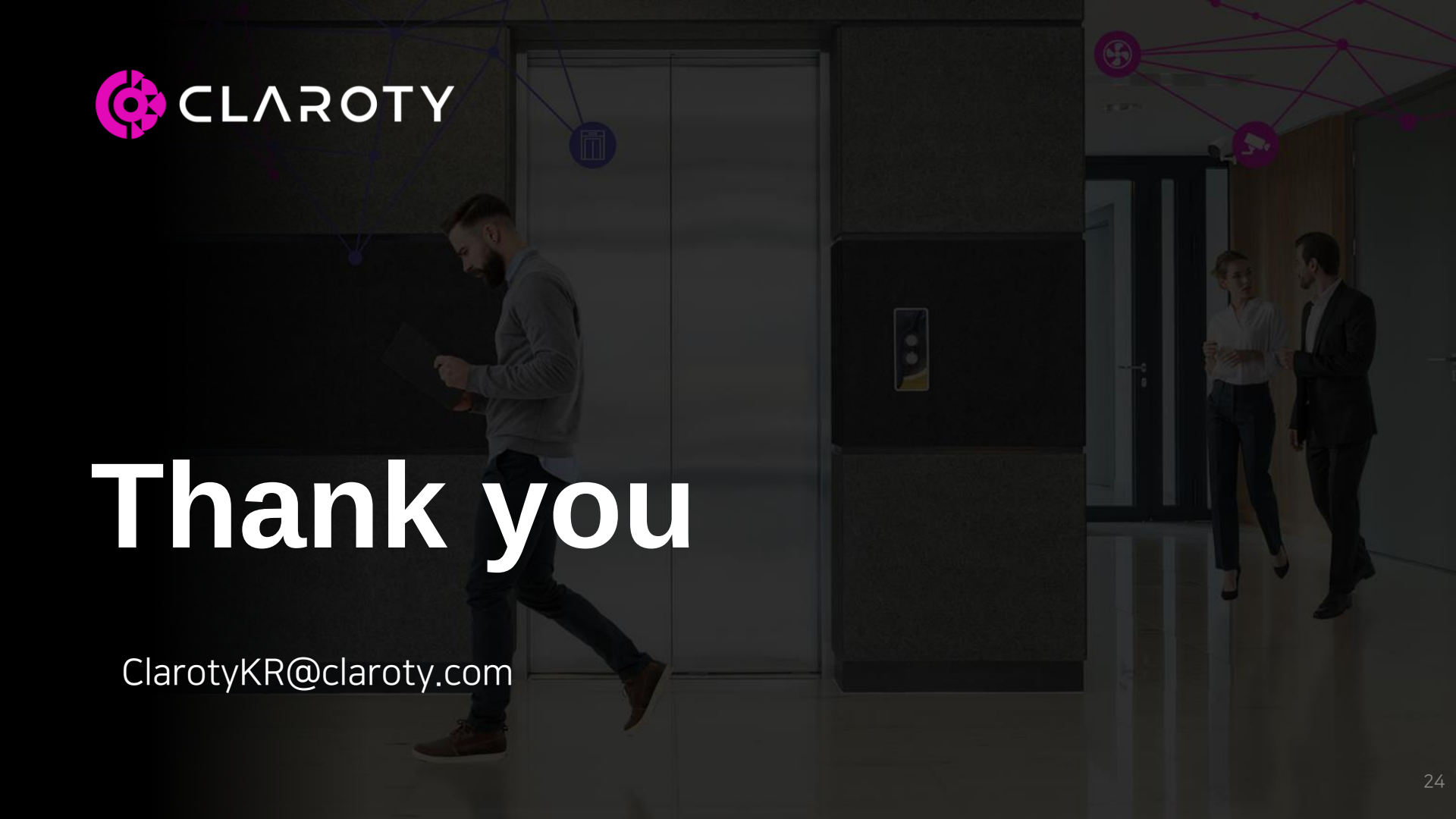
운영 기술 (OT)

사물 인터넷 (IoT)

산업용 IoT (IIoT)

스마트 빌딩

인더스트리 4.0



Thank you

ClarotyKR@claroty.com