

업계 최고의 산업 OT/IIoT 사이버보안 전문 기업

자산 가시성으로 시작하는 사이버 복원력 구현

THE INDUSTRIAL CYBERSECURITY COMPANY - CLAROTY

클래로티코리아



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 시나리오 1

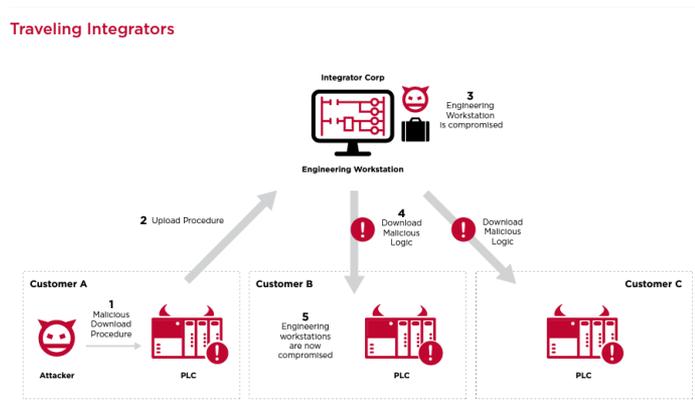
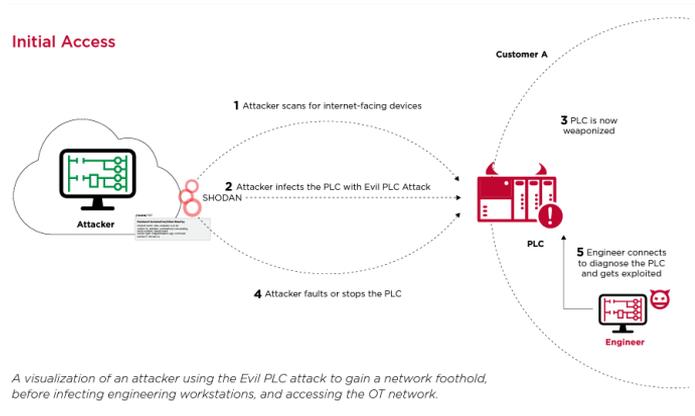
1) 외부 공격자가 PLC에 악성코드 입력.

2) 감염된 PLC가 엔지니어링 컴퓨터를 (EWS) 감염.

공격 시나리오 2

1) 감염된 PLC가 연결된 EWS 감염.

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



EVIL PLC ATTACK: WEAPONIZING PLCs

Team82, Clarity Research Team

Maksim Sujan, Ulf Katz, Fabian Muehle, Shantanu Dutta, Arne Probstinger

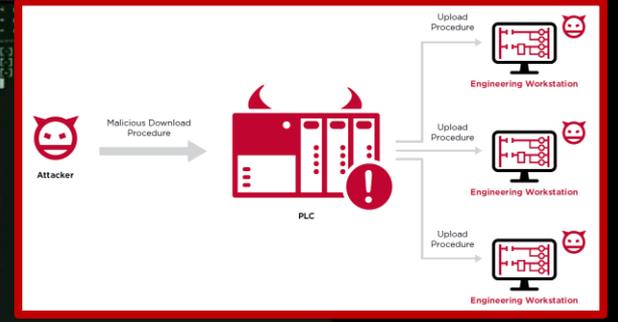
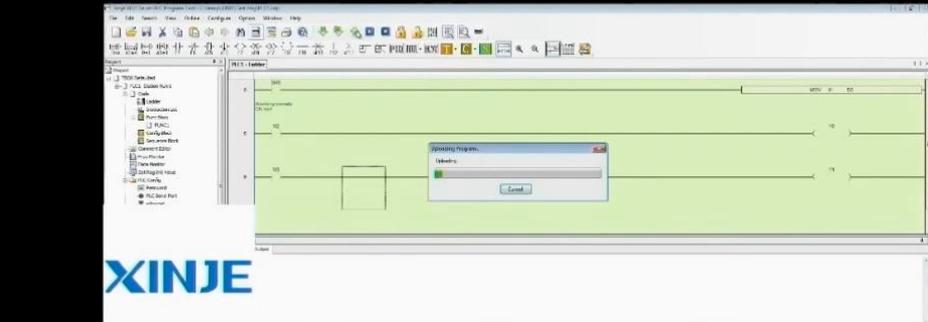
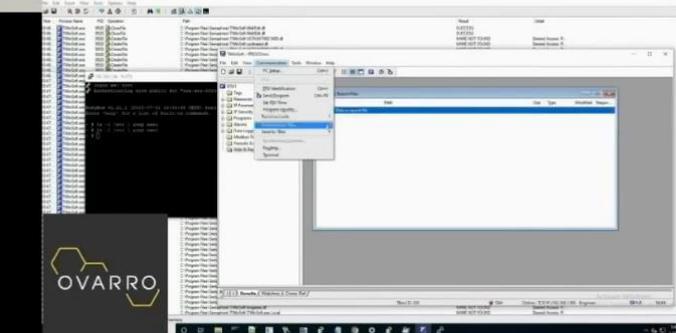
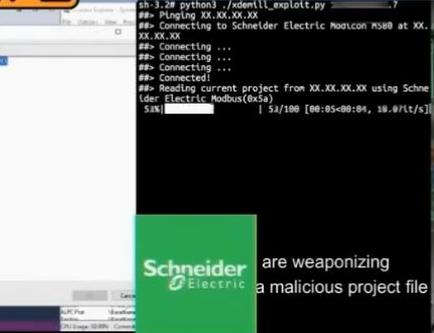


2022년 DEF CON 30
공개 영상 by Team82



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

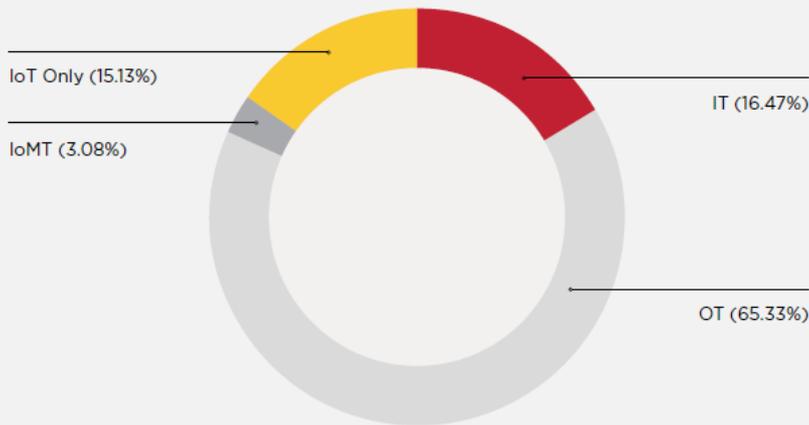
공개된 전체 취약점 수

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



XIoT 사이버 보안 회사 클래로티의 연구 조직인 Team82는 고유의 위험 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.

자산 식별

사이버 탄력성 여정의 시작



당면과제

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

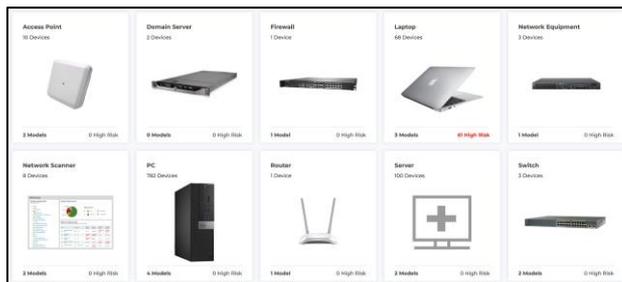
유연하고 간편한 XIoT 검색 옵션을 통해 구현 시간과 복잡성을 저감

산업계 전문성을 바탕으로 모든 자산에 대해 맹점을 없애고 완전한 가시성 확보

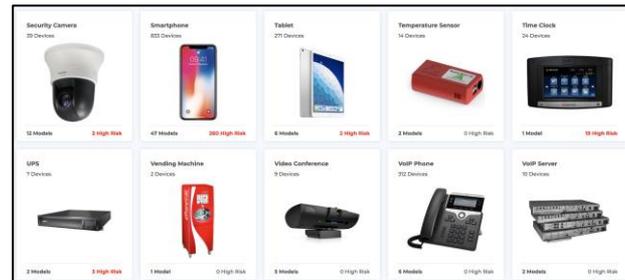
자산 관리 통합으로 전사적 자산 데이터베이스 보안 위생을 최적화

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

IT



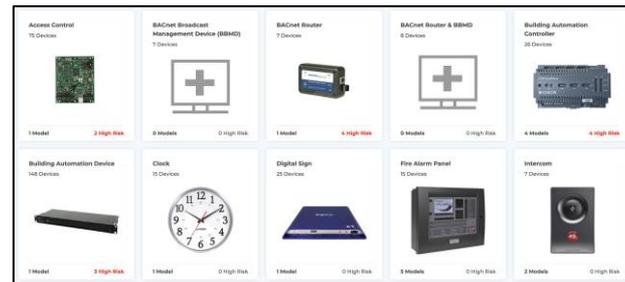
IoT



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.



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 위생을 최적화

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

| Device Information | | | | | | |
|---|--|---|---|--|---|--|
| <p>● BME P58 4040 Schneider Electric RISK SCORE: HIGH (55.7)</p> <p>#ID: BWMBLHUKGT</p> <p>+ Add Notes</p> <p>High Priority Require Patch</p> <p>ASSIGNERS: I&C Techs Maintenance</p> | | | | | | |
| DEVICE INFORMATION | | | | | | |
| Device IDs | IP 10.26.29.28 10.26.29.64 +3 | MAC 0A:65:BC:94:F8:29 00:80:F5:76:8E:15 +3 | MAC OUI Randomized Locally Admini... Quantel Ltd +3 | CATEGORY OT | SUB CATEGORY Control | MANUFACTURER Schneider Electric |
| | TYPE PLC | MODEL BME P58 4040 | MACHINE TYPE Physical | MOBILITY Stationary | SERIAL NUMBER SE007124 | OT CRITICALITY High |
| | PURDUE LEVEL Level 1 | | | | | |
| Versions & Names | APP VERSION 0270 - 11 | | | | | |
| Network | NETWORK SCOPE Corporate Corporate +3 | | VLAN 124 +3 124 | VLAN NAME VLAN 124 VLAN 124 +3 | VLAN DESCRIPTION VLAN 124 VLAN 124 +3 | CONNECTION TYPE Ethernet Ethernet +3 |
| | IP ASSIGNMENT Static +3 Static | FIRST SEEN 26/04/2022, 2:05 am 27/04/2022, 7:38 am +3 | LAST SEEN 25/09/2022, 8:30 am 17/08/2022, 12:16 am +3 | | | |
| Location | SITE NAME Albany | SWITCH MAC 00:11:95:80:05:3B N/A +3 | SWITCH PORT ID Fa1/29 N/A +3 | SWITCH LOCATION dep 6KOLJ N/A +3 | LAST SEEN ON SWITCH 25/09/2022, 8:54 am +3 | |
| Custom Attributes | Asset Acquisition Date 2022-09-03 00:18:26.971696+00:00 | PHYSICAL LOCATION Building 20 | CUSTOM ATTRIBUTE 2 N/A | OT NAME N/A | RYAN N/A | |

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.



당면과제

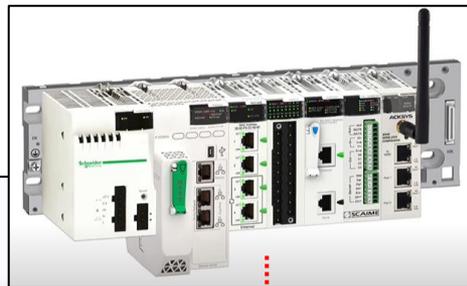
- 모든 자산을 식별 가능?
- 모든 세부 정보를 수집 가능?
- 정확한 데이터인가?
- 단일 데이터베이스로 통합 가능?

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 위생을 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 | Slot 8 - CPU 8 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|------------------|----------------|-------------------------|-------------------------|-------------------------|----------------|-------------------------|--|----------------|----------------|-----------|--------------|------------|------------|-------------------|--------------------|------------------|---------|--------------------|----------|---------|-------------|----------|-------------------|---|-----------|-------|-----------|-----|------------|--------------|-------------------|--------------------|------------------|------------|--------------------|----------|---------|-------------|------------------|---|
| | | | | | | | <table border="1"> <tr> <td>CARD NAME</td> <td>Network Card 7</td> <td>CARD TYPE</td> <td>Network Card</td> </tr> <tr> <td>CARD MODEL</td> <td>TM22ICE16R</td> <td>CARD MANUFACTURER</td> <td>Schneider Electric</td> </tr> <tr> <td>CARD APP VERSION</td> <td>1.5.0.1</td> <td>CARD SERIAL NUMBER</td> <td>SE007125</td> </tr> <tr> <td>CARD IP</td> <td>10.26.29.64</td> <td>CARD MAC</td> <td>00:80:F5:76:8E:15</td> </tr> </table> | CARD NAME | Network Card 7 | CARD TYPE | Network Card | CARD MODEL | TM22ICE16R | CARD MANUFACTURER | Schneider Electric | CARD APP VERSION | 1.5.0.1 | CARD SERIAL NUMBER | SE007125 | CARD IP | 10.26.29.64 | CARD MAC | 00:80:F5:76:8E:15 | <table border="1"> <tr> <td>CARD NAME</td> <td>CPU 8</td> <td>CARD TYPE</td> <td>CPU</td> </tr> <tr> <td>CARD MODEL</td> <td>BME P58 4040</td> <td>CARD MANUFACTURER</td> <td>Schneider Electric</td> </tr> <tr> <td>CARD APP VERSION</td> <td>02.70 - 11</td> <td>CARD SERIAL NUMBER</td> <td>SE007130</td> </tr> <tr> <td>CARD OS</td> <td>Proprietary</td> <td>CARD SLOT NUMBER</td> <td>8</td> </tr> </table> | CARD NAME | CPU 8 | CARD TYPE | CPU | CARD MODEL | BME P58 4040 | CARD MANUFACTURER | Schneider Electric | CARD APP VERSION | 02.70 - 11 | CARD SERIAL NUMBER | SE007130 | CARD OS | Proprietary | CARD SLOT NUMBER | 8 |
| CARD NAME | Network Card 7 | CARD TYPE | Network Card | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CARD MODEL | TM22ICE16R | CARD MANUFACTURER | Schneider Electric | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CARD APP VERSION | 1.5.0.1 | CARD SERIAL NUMBER | SE007125 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CARD IP | 10.26.29.64 | CARD MAC | 00:80:F5:76:8E:15 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CARD NAME | CPU 8 | CARD TYPE | CPU | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CARD MODEL | BME P58 4040 | CARD MANUFACTURER | Schneider Electric | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CARD APP VERSION | 02.70 - 11 | CARD SERIAL NUMBER | SE007130 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 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.

취약점 & 위험관리

사이버 탄력성 여정의 2단계



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

The screenshot shows the CLAROTY Risk Management interface. At the top, there are navigation tabs: Home, Devices, Alerts, Risk (highlighted), Network, Operational Efficiency, and Settings. Below the navigation, there are summary statistics: Total 93,253, Relevant 1,209, Actively Exploited 831, and Remediable 0. A dropdown menu for 'Risk Score' is open, showing options: Very Low, Low, Medium, High, and Critical. The main table displays a list of vulnerabilities with columns for Release Date, Vulnerability Name, Vulnerability Type, CVEs, CVSS V2 Base Score, CVSS V2 Base Score, Description, Affected Devices, and Recommendations. An inset window shows a detailed risk analysis dashboard with various charts and graphs, including a risk score distribution and a probability of severity distribution.

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.



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

총 133 관련 있는 19

표시 중: 133 위험 인덱스 기록 정렬 기준: (메이트)

The Hacker News **OpenSSL, 2개의 새로운 심각도가 높은 취약점에 대한 패치 출시**

10월 25일 OpenSSL은 OpenSSL 버전 3.0.7의 다음 릴리스에 치명적인 취약점에 대한 패치가 포함될 것이라고 발표했습니다. 이 발표는 릴리스보다 1주일 앞서서 취약점의 성격과 영향에 대해 추측할 수 있는 충분한 시간을 남겼습니다. 11월 1일 OpenSSL은 버전 3.0.7을 출시하고 발표를 업데이트하여 중간에 조사한 결과 원래 심각해 보였던 취약점이 심각도가 높은 것으로 밝혀졌다고 밝혔습니다. 릴리스에는 두 번째로 심각도가 높은 결함도 포함되어 있습니다. 3.0.7 릴리스와 함께 OpenSSL 패치 CVE-2022-3786 및 CVE-2022-3602, 서비스 거부로 이어질 수 있는 두 개의 버퍼 오버플로. 이는 빠르게 2021년 9월 이후에만 사용할 수 있는 OpenSSL 버전 3.0 이상에 영향을 미칩니다.

수정 단계

OpenSSL 3.0 사용자는 OpenSSL 3.0.7로 업그레이드해야 합니다.

2022년 10월 31일, 오후 8시

덜 읽기 <

클라로티의 평가:
Clarity가 이 항목을 평가하는 중입니다.

SIEMENS **SIMATIC 57의 약한 키 보호 취약성**

Siemens Simatic PLC의 취약점을 악용하여 하드 코딩된 글로벌 개인 암호화 키를 검색하고 장치들 제어할 수 있습니다. 악의적인 행위자가 이 비밀 정보를 사용하여 전체 SIMATIC 57-1200/1500 제품 라인을 손상시킬 수 있습니다.

2022년 10월 18일, 오전 10시 56분

더 읽어 보기 >

클라로티의 평가:
Clarity가 이 항목을 평가하는 중입니다.

 **Clarity의 Team82는 Dataprobe의 iBoot-PDU에서 몇 가지 새로운 취약점을 발견했습니다.**

Clarity's Team82에서 새로 발견한 결함으로, 악용될 경우 공격자에게 iBoot-PDU 제어 권한을 부여하는 것을 포함하여 Dataprobe 장치에 여러 위험을 초래할 수 있습니다. 월 기반 인터페이스 또는 클라우드 기반 관리 플랫폼을 포함하여 PDU 구성 요소에서 원격으로 악용 가능한 취약점을 공격하면 공격자는 장치와 연결될 수 있는 기타 모든 것에 대한 전력을 차단하여 중요한 서비스를 중단시키는 위치에 놓이게 됩니다. 그것에 또한 공격자가 클라우드에 연결된 PDU에서 코드를 실행하거나 클라우드 자격 증명을 획득하여 네트워크에서 측면으로 이동할 수 있습니다.

2022년 9월 22일, 오전 4시 56분

더 읽어 보기 >

클라로티의 평가:
Clarity가 이 항목을 평가하는 중입니다.

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

네트워크 보호

사이버 탄력성 여정의 3단계



당면과제

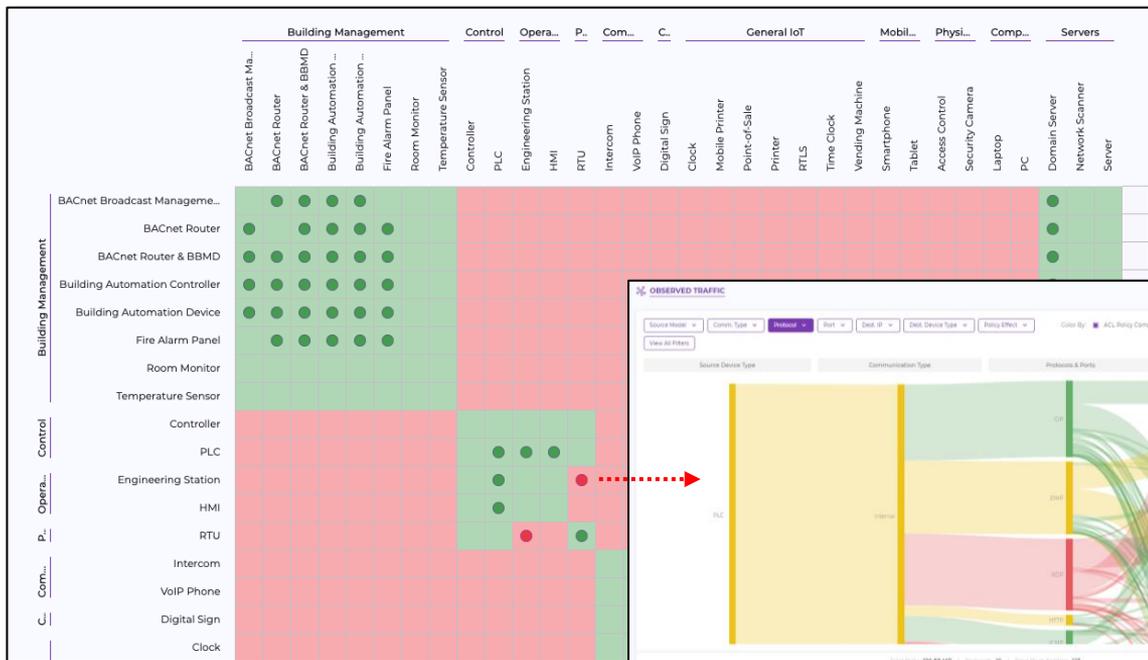
- 모든 취약점에 패치 및 수정불가.
- 네트워크 제어로 위험 완화 필요.
- 필수, 불필요한 통신의 구분.
- 적절한 네트워크 세분화.

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 액세스 제어 설정 적용 전 충분한 검증 작업을 돕습니다.



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

CLAROTY RECOMMENDED POLICIES

Showing: 15 Recommended Policies
Sorted By: MATCHING DEVICES (DESC)

| POLICY ID | POLICY SOURCE | POLICY NAME | APPLIED MODELS | MATCHING DEVICES | POLICY RULES | POLICY ACL |
|-----------|----------------|---|---|------------------|--------------|------------|
| #RD221 | Recommendation | PLC - Rockwell | 1747-L553/C C/13 - DC 3.54, 1756-ENBT/A, 1763-L16BWA B/14.00, 1794-AENT/B | 76 | 12 Rules | ACL |
| #RD144 | Recommendation | Clock - Primex - SNS | SNS Clock | | | |
| #RD147 | Recommendation | Time Clock - Kronos | InTouch 9100 | | | |
| #RD91 | Recommendation | Building Automation Controller - Johnson Controls | NAE, NCE | | | |
| #RD222 | Recommendation | HMI - Rockwell | PanelView Plus_7 Standard 700 | | | |

Policy 'PLC - Rockwell' - ACL

Alterations may be required to apply these rules to your network.

Wired Switch | WLC

```

1 remark CIP
2 permit tcp any any eq 44818
3 permit tcp any eq 44818 any
4
5 remark DHCP
6 permit udp any any eq 67
7
8 remark DNS
9 permit udp any any eq 53
10 permit tcp any any eq 53
  
```

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



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

Communicating Devices

| CONN. TYPE | IP | MAC | MANUFACTURER | TYPE | MODEL |
|------------|------------|-------------------|--------------|----------------------------|-------|
| + | 10.8.57.29 | 00:10:7F:B1:9CAE | CRESTFON | Building Automation Device | CPSN |
| + | 10.8.57.34 | 00:10:7F:73:B0:C1 | CRESTFON | Building Automation Device | CPSN |
| + | 10.8.57.37 | 00:10:7F:EC:91:6B | CRESTFON | Building Automation Device | CPSN |
| + | 10.8.57.43 | 00:10:7F:32:1E:22 | CRESTFON | Building Automation Device | CPSN |

[View 19 Matching Devices](#)

Russian Federation

| Communication Type Distribution | | | Communication Direction | Communicating Devices |
|---------------------------------|---------|------|-------------------------|-----------------------|
| Type | Data | % | Inbound | 23 Total |
| Internet | 0 Bytes | 0% | 611.82 KB | 12 OT |
| Endpoint Security | 0 Bytes | 0% | | |
| VPN | 0 Bytes | 0% | Outbound | 10 IoT |
| Manufacturer | 0 Bytes | 0% | | |
| Malicious | 1.24 MB | 100% | 656.43 KB | 1 IT |

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



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

Alert Information | Deviating Devices | Deviating Traffic | History

Out-of-Policy Communication (Alert #1000006)
Policy deviation was detected in PLC - Rockwell Policy by 3 Rockwell Automation 1756-ENBT/A devices

Suspicious Device Behavior (Alert #1000040)
A device was observed communicating to a substantial amount of malicious IP addresses

| ALERT STATUS | ALERT CATEGORY | AFFECTED SITES | DETECTED | UPDATED |
|--------------|----------------|----------------|---------------------|---------------------|
| Unresolved | Threat | Columbia | 04/11/2022, 1:06 am | 04/11/2022, 1:06 am |

DEVIATING TRAFFIC

| DEVIATING DEVICES | IP PROTOCOL | PROTOCOL | DST IPS | DEVICE PORTS | DST PORTS | DIRECTION | FIRST COMMUNICATION | LAST COMMUNICATION |
|-------------------|-------------|----------|---|--------------|-----------|-----------|---------------------|--------------------|
| 3 | UDP | NetBIOS | 10.134.159.76, 10.13.88.107, 10.223.240.156 | 137 | 137 | ↔ | 11/09/2022 | 08/10/2022 |

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

위험 탐지

자산 / 네트워크 / 데이터 가시성

유연한 배포

역할별 UX

통합 생태계

Historian RTU SCADA DCS

물리적 침입 보안카드 출입

자동화 설비 센서

엘리베이터 스마트 그리드

클라우드 서비스 공급망

HMI PLC CNC

카메라 조명 & 에너지

임베디드 장치 IIoT 게이트웨이

BMS/BAS HVAC

CAV

운영 기술 (OT)

사물 인터넷 (IoT)

산업용 IoT (IIoT)

스마트 빌딩

인더스트리 4.0



Thank you

ClarotyKR@claroty.com