tenable

PASCON 2023
2023 공공 · 금융 · 기업 정보보안&개인정보보호 컨퍼런스

OT 환경 보안 강화를 통한 기업 환경 전반의 보안 운영 효율성 강화 방안

이준희(jolee@tenable.com)
Tenable Technical Sales Engineer

Sep 2023

목차

- OT 환경
- OT 보안 구성 및 개선 방향
- OT 보안 강화

OT는 모든 영역에 존재

tenable

제조업 현황...

tenable

정유업 현황..

데이터센터 현황...

tenable

사무실 현황...

tenable

OT 보안 3가지 주요 경향

01

OT 사이버 위협이 증가

02

OT 보안 책임이 데이터보안 팀으로 전환

03

OT 보안 규정이 전세계로 확대

OT

BMS

IoT

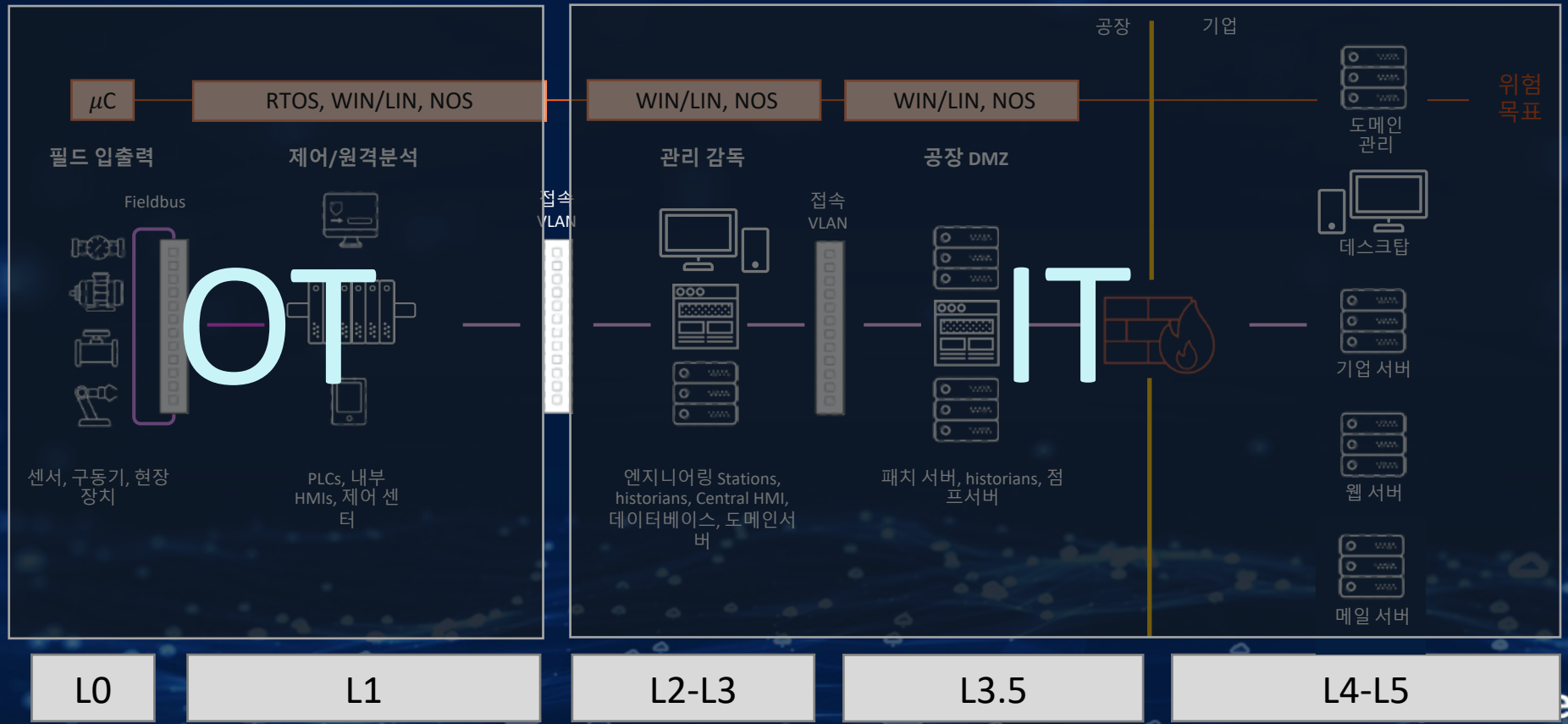
tenable

OT 보안 구성 이해 및 개선 방향

일반적인 IT/OT 경계


공장
기업
μC
RTOS, WIN/LIN, NOS
WIN/LIN, NOS
WIN/LIN, NOS
위험 목표
필드 입출력
제어/원격분석
관리 감독
공장 DMZ
도메인 관리
Fieldbus
접속 VLAN
접속 VLAN
데스크탑
OT
IT
기업 서버
웹 서버
메일 서버
센서, 구동기, 현장 장치
PLCs, 내부 HMIs, 제어 센터
엔지니어링 Stations, historians, Central HMI, 데이터베이스, 도메인서버
패치 서버, historians, 점프서버
L0
L1
L2-L3
L3.5
L4-L5

실제 IT/OT 경계


μC
RTOS, WIN/LIN, NOS
WIN/LIN, NOS
WIN/LIN, NOS
공장
기업
위험 목표
필드 입출력
제어/원격분석
관리 감독
공장 DMZ
도메인 관리
Fieldbus
접속 VLAN
접속 VLAN
데스크탑
OT
IT
기업 서버
웹 서버
메일 서버
센서, 구동기, 현장 장치
PLCs, 내부 HMIs, 제어 센터
엔지니어링 Stations, historians, Central HMI, 데이터베이스, 도메인서버
패치 서버, historians, 점프서버
L0
L1
L2-L3
L3.5
L4-L5

OT 보안 목표

01 OT 가시성 확보
OT 시스템 통합 관리

02 OT 취약점 관리
위험도 기반

03 설정 관리
운영 관리팀을 위한

04 위협 탐지
및 완화 방안

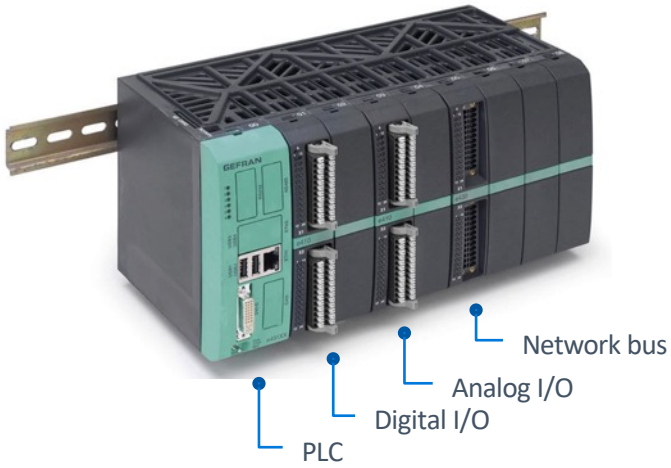
05 통합 대시보드
통합 관리(IT/OT취약점,설정 관련 오류)

tenable

OT 가시성 확보 어려움

오래된 생각 *컨트롤러 관련 문제*

- 현장 사용 년한이 길다.
- 취약점 점검에 민감할 수 있다.
- 중요 시스템 제어한다.
- 장애 발생시 영향이 크다.

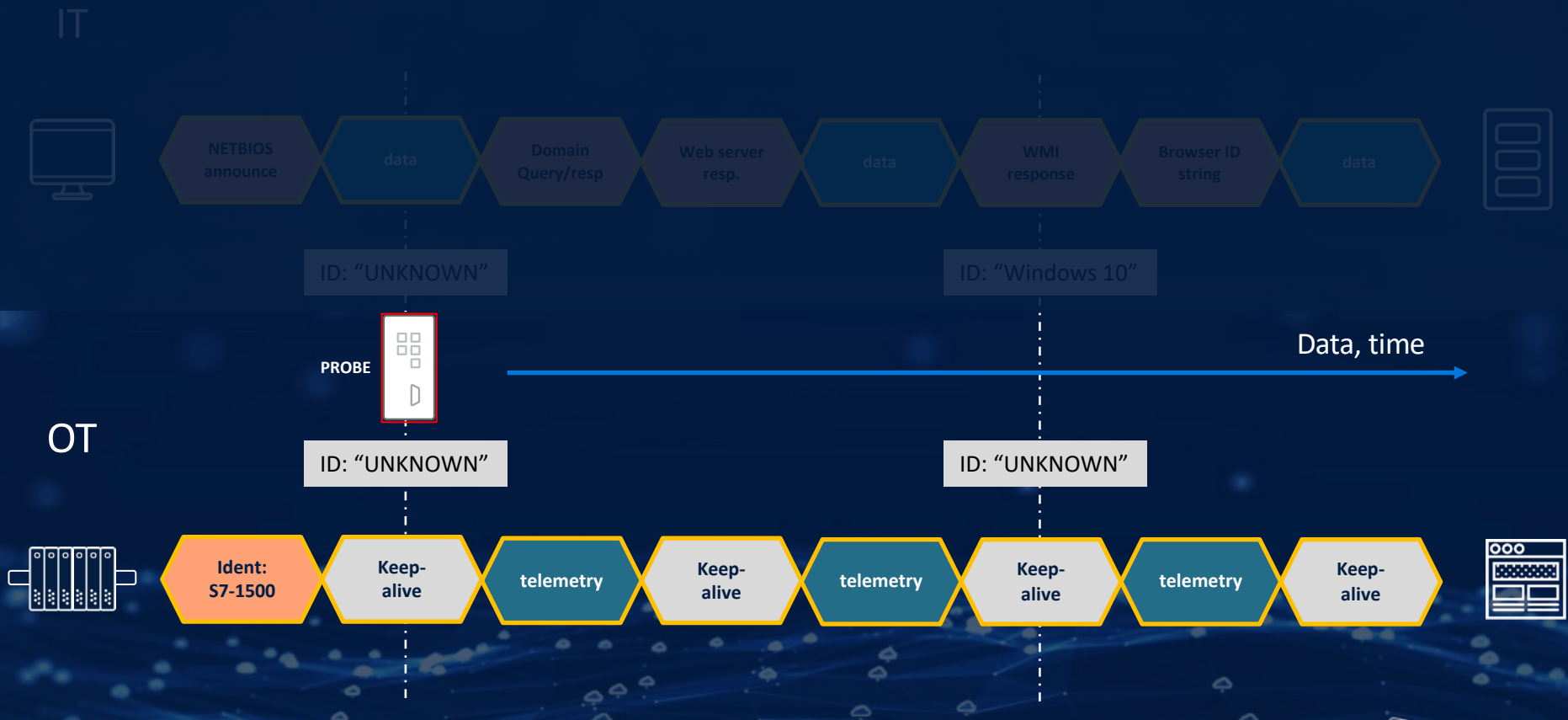


OT 가시성 확보 어려움

우리의 전략

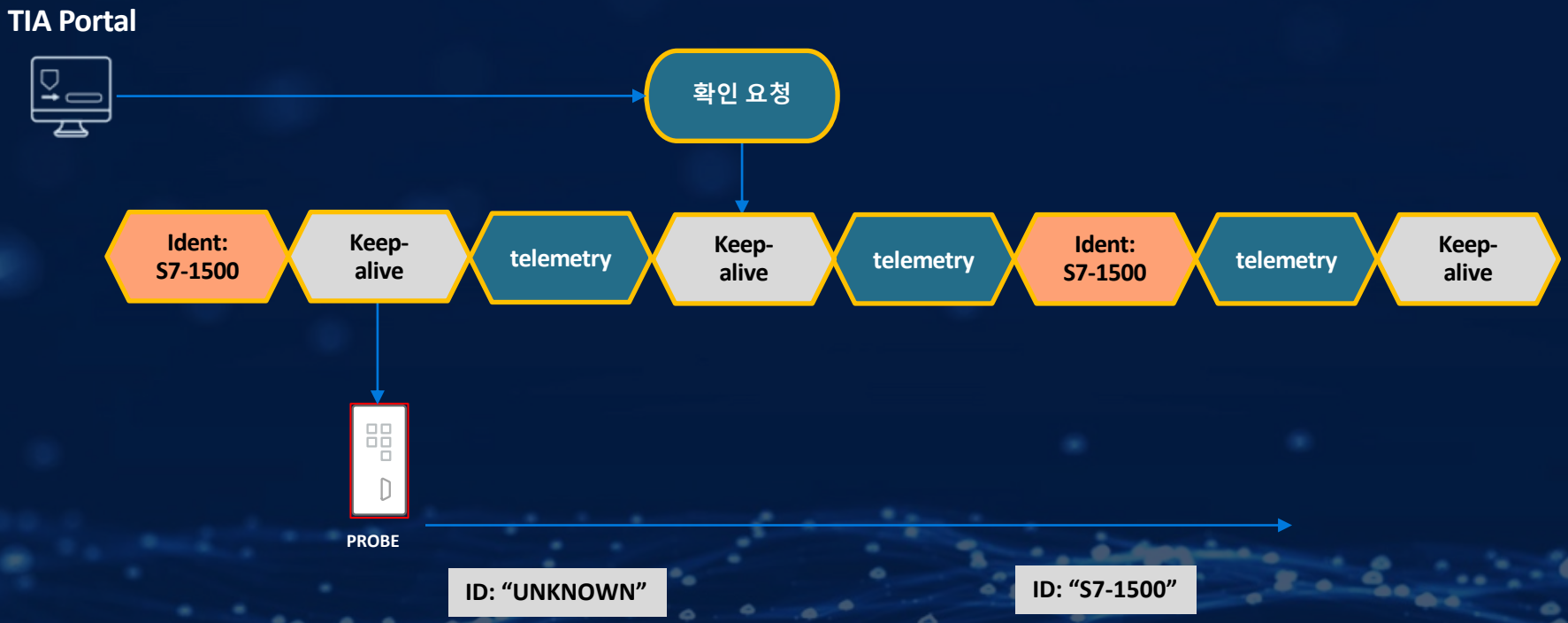
네트워크 미러링을 통한 수동형 위협 모니터링 방안 선택

OT 네트워크 수동 분석 방식 - 문제



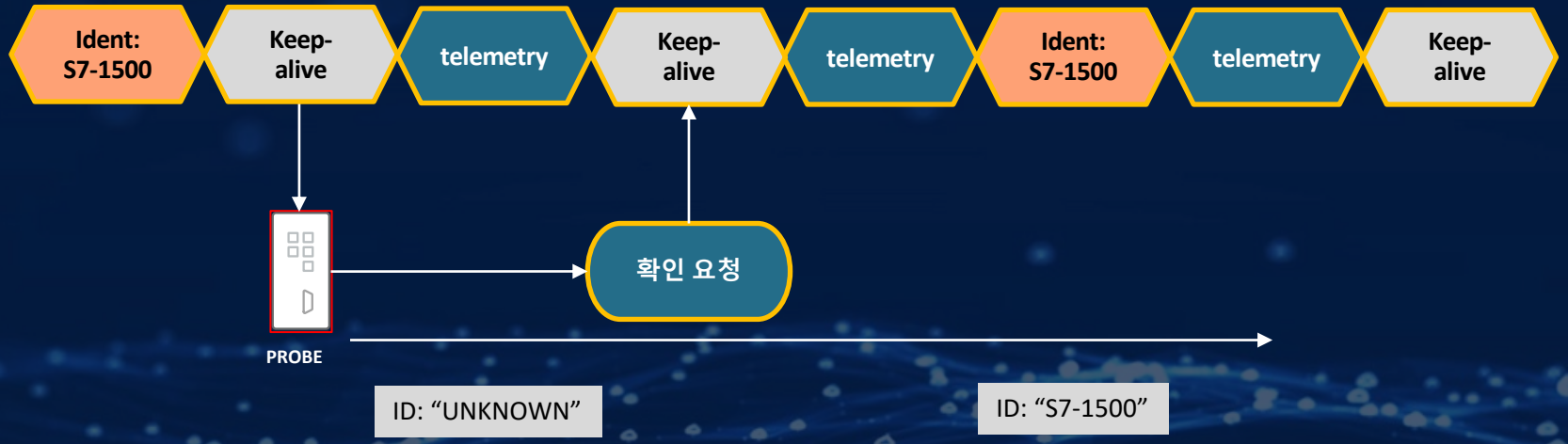
tenable

OT 네트워크 수동 분석 방식 – 개선 방안



tenable

OT 네트워크 수동 분석 방식 – 개선



tenable

수동 분석 방식의 한계점

전체 OT 자산 분석의 어려움

수동 분석 가능 구역

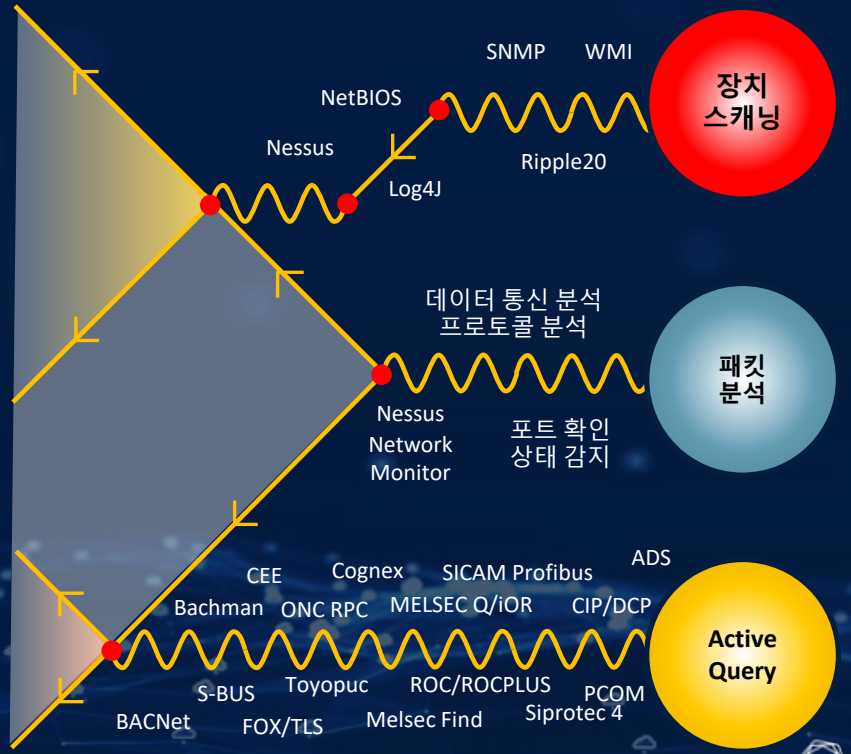
수동 분석 불가능 구역

tenable

OT 보안 강화 방안

OT 위험 분석 방안 – 하이브리드 방안 필요

퍼듀모델	운영시스템
LEVEL 5 ENTERPRISE	WIN / LIN VM / 서버
LEVEL 4 E.R.P.	WIN / LIN VM / 서버
LEVEL 3 SITE OPERATIONS	WIN CLIENT ENGINEER STN
LEVEL 2 SUPERVISORY	EMBED. WIN/LIN HMI
LEVEL 1 CONTROL	RTOS / LINUX CONTROLLER/RTU
LEVEL 0 PHYSICAL PROCESS	EMBEDDED / NONE FIELD DEVICE



tenable

하이브리드 분석을 통한 빠른 자산 확인

패킷 분석

식별

네트워크 상에서 통신하는 자산

Active Query

발견

중지되었거나 통신하지 않는 시스템 확인

Active Query | 장치 스캐닝

분류

HMI, 히스토리안, 라우터, PLC, 서버, 스위치

Active Query | 장치 스캐닝

수집

패치, 핫픽스 레벨, 펌웨어, 사용자, PLC 백플레인

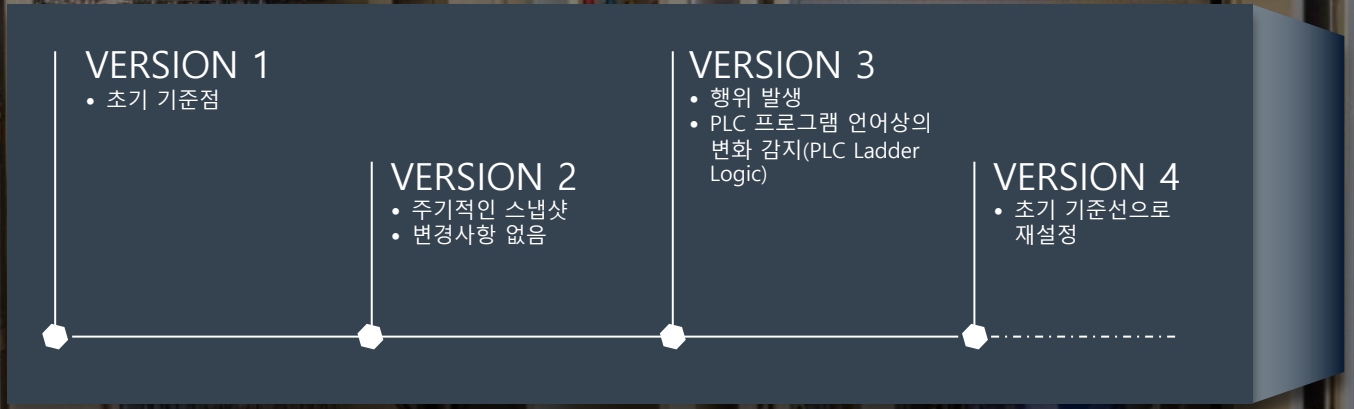
Active Query

추적

장치를 포함한 전체 설정 변경 관리

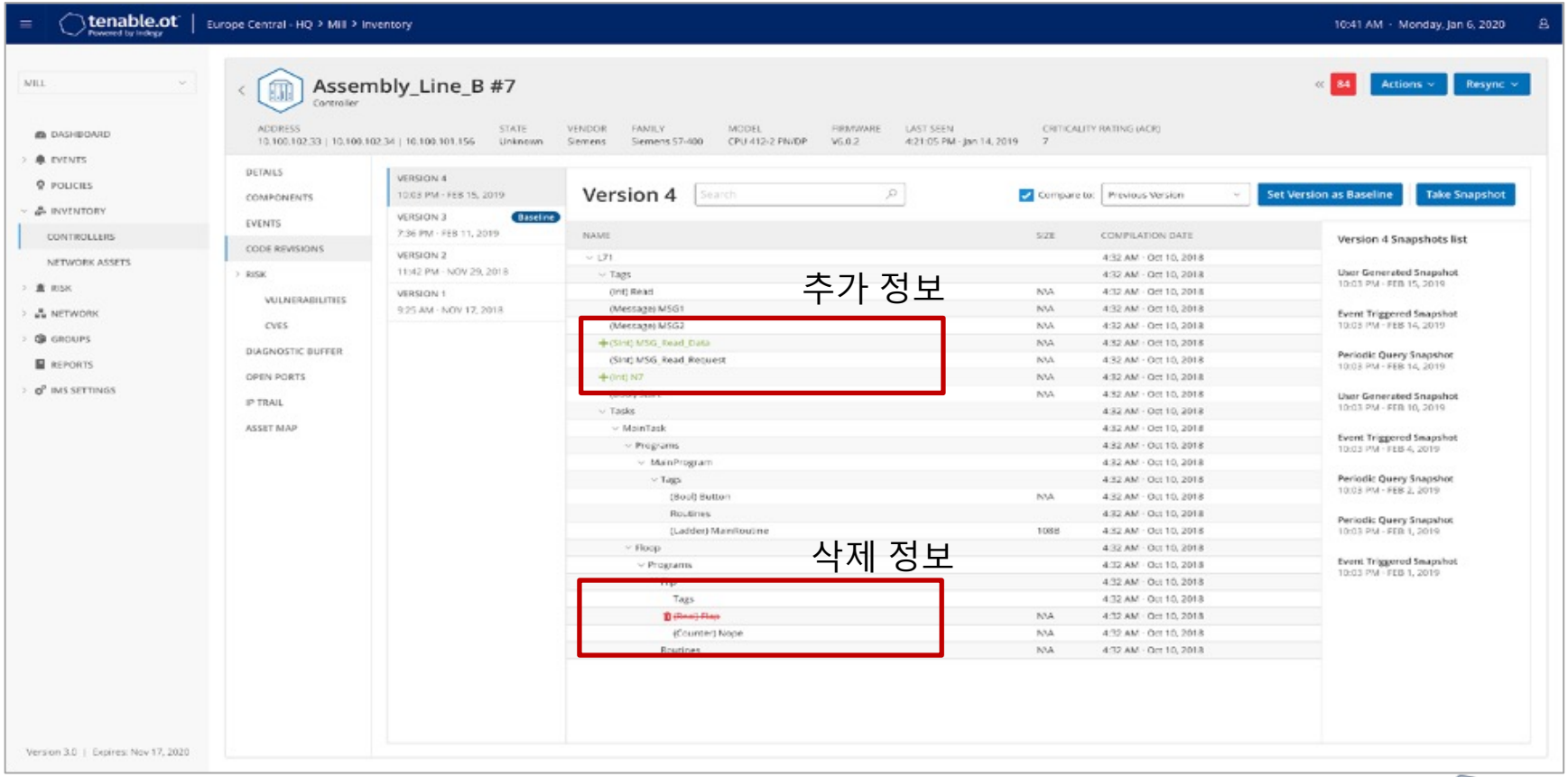
tenable

하이브리드 분석을 통한 설정 정보 분석



설정이 변경되는 것을 추적하고 확인하는 것은 모든 변경은 사용자나 악성 파일에 의한 것이기 때문이다. 네트워크를 통하거나 직접 통하는 모든 경우 동일

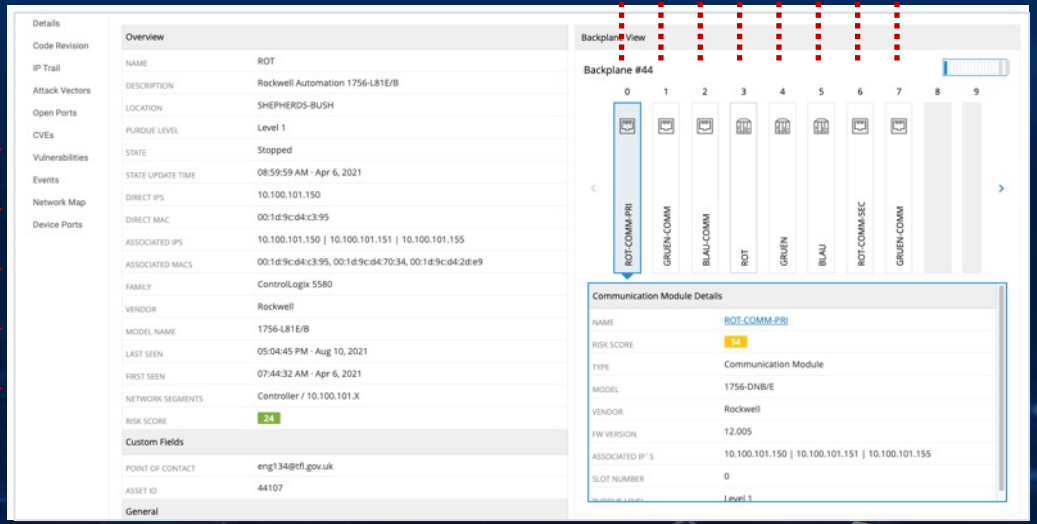
OT 위험 분석 예 – 설정 변경 모니터링



OT 위험 분석 예 – 네트워크 및 설정 정보 분석

구성 관리 데이터를 동시에 분석– 정확한 상황인지

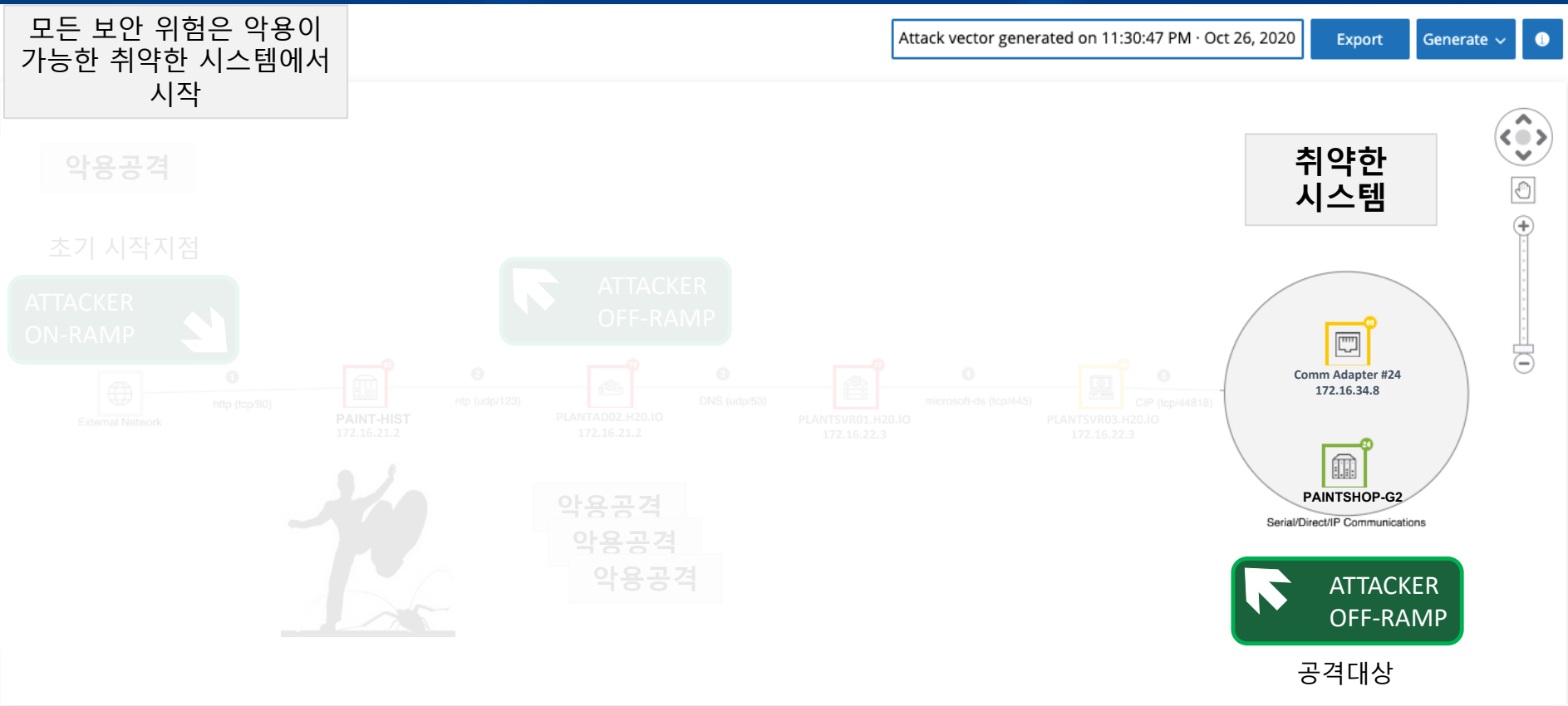
발생 이벤트에 대한 정확한 판단



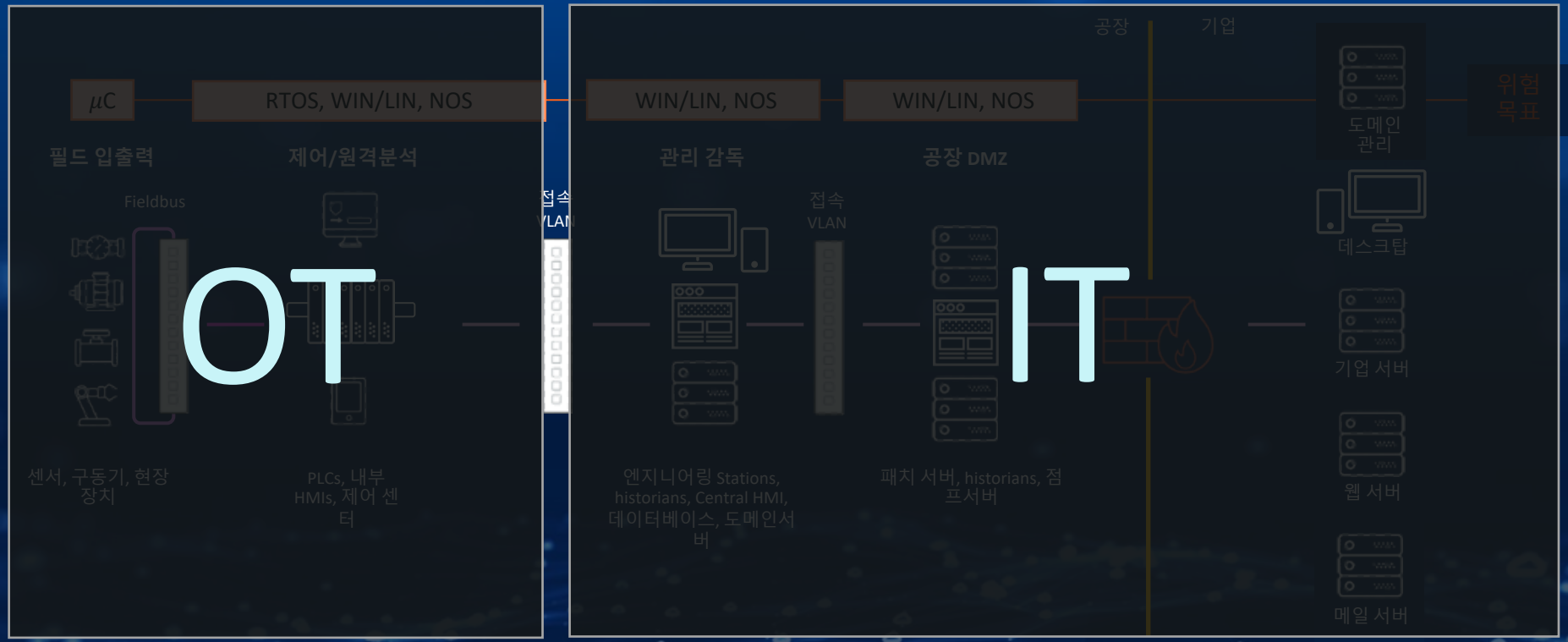
tenable

최종 목표 - 공격 경로 제거

모든 보안 위험은 악용이 가능한 취약한 시스템에서 시작



OT 보안 영역 재정의



L0	L1	L2-L3	L3.5	L4-L5

IT/OT 영역을 모두 잘 아는 솔루션이 필요


tenable OT Security
THANK YOU
https://tenable.com/products/tenable-ot 에서 필요한 정보를 확인 하실 수 있습니다