



**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





IT는 모든 영역에 존재







오버헤드 컨베이어

로봇 팔

보일러

컨베이어 벨트

제조업 현황...



# 정유업 현황..



정제 타워

가열기

저장소

파이프

밸브



스마트 전력 분배 트랙

## 데이터센터 현황...

전기설비

전력 분배 시설

조명

공조 시스템

출입 통제

보안 카메라

사무실 현황...



# OT 보안 3가지 주요 경향

01

OT 사이버  
위협이 증가



OT

02

OT 보안  
책임이  
데이터 보안  
팀으로 전환



BMS

03

OT 보안  
규정이  
전 세계로  
확대



IoT



# OT 보안 구성 이해 및 개선 방향



# 일반적인 IT/OT 경계





# 실제 IT/OT 경계



# 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

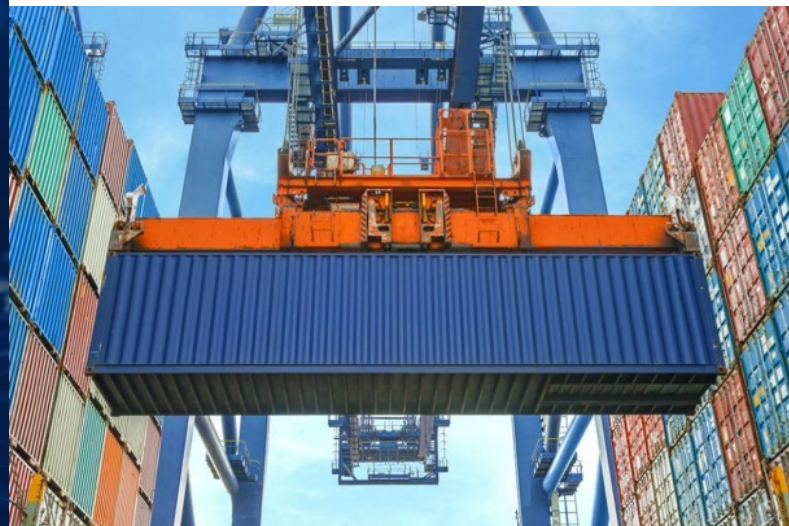
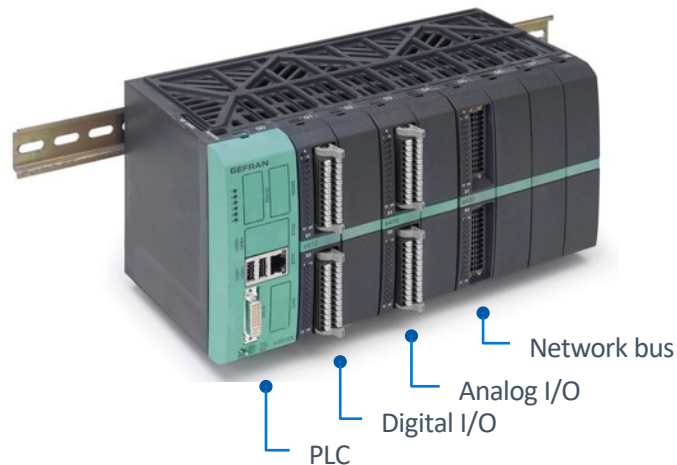
통합 관리(IT/OT취약점,설정 관련 오류)



# 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*

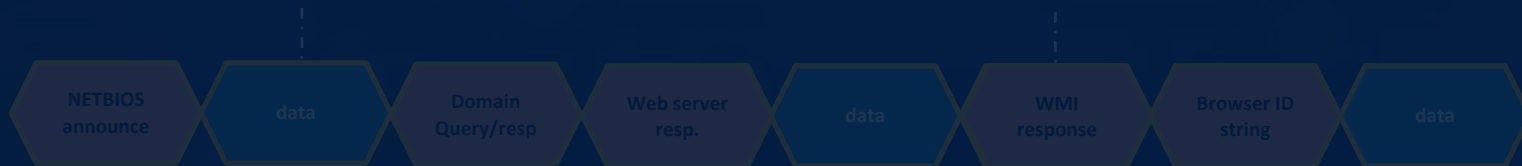
네트워크 미러링을  
통한 수동형 위협  
모니터링 방안 선택





# OT 네트워크 수동 분석 방식 - 문제

IT



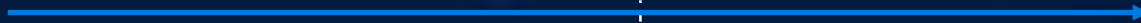
ID: "UNKNOWN"

ID: "Windows 10"

PROBE



Data, time



OT

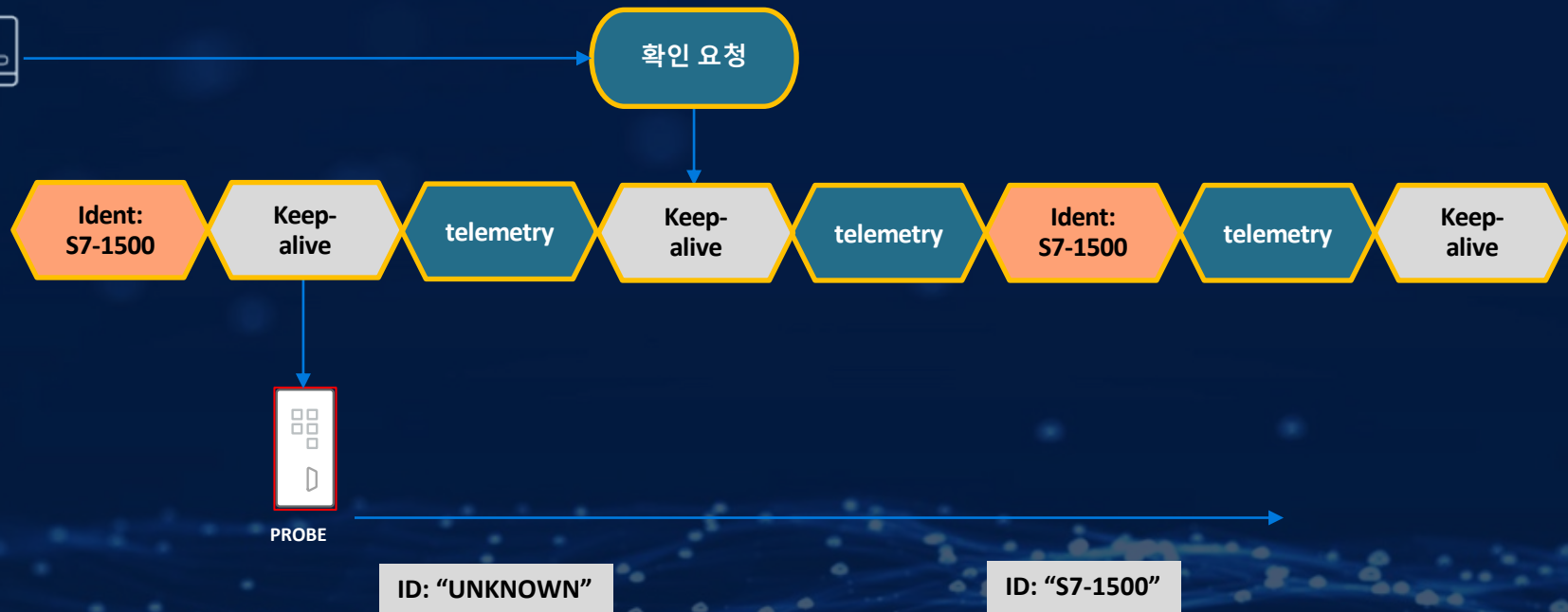


ID: "UNKNOWN"

ID: "UNKNOWN"

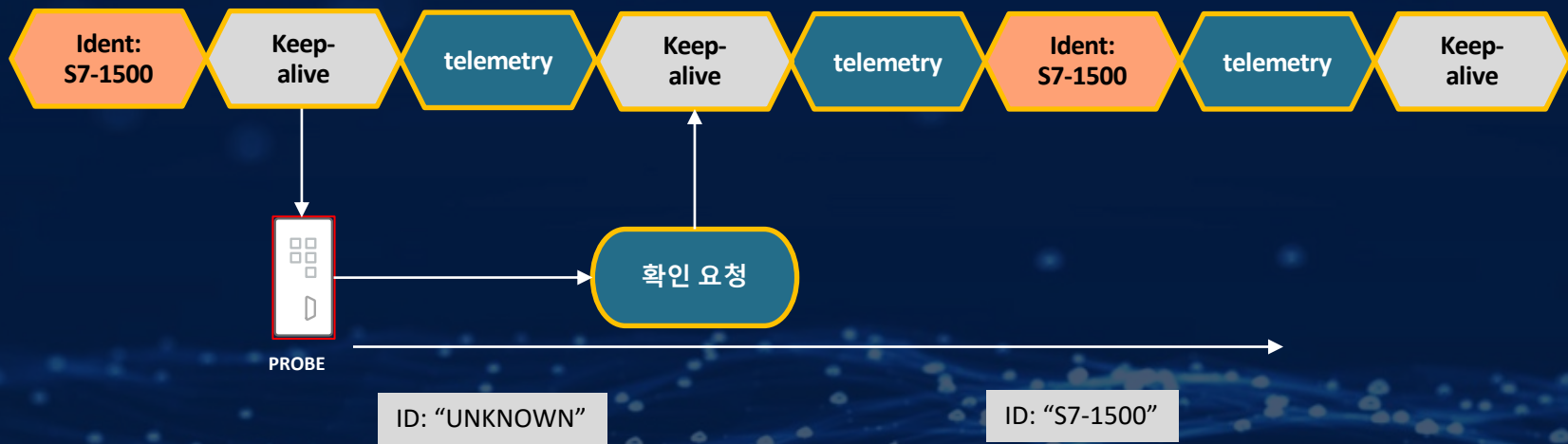
# OT 네트워크 수동 분석 방식 - 개선 방안

TIA Portal





# OT 네트워크 수동 분석 방식 - 개선



## 수동 분석 방식의 한계점

**전체 OT 자산 분석의 어려움**

수동 분석 가능 구역

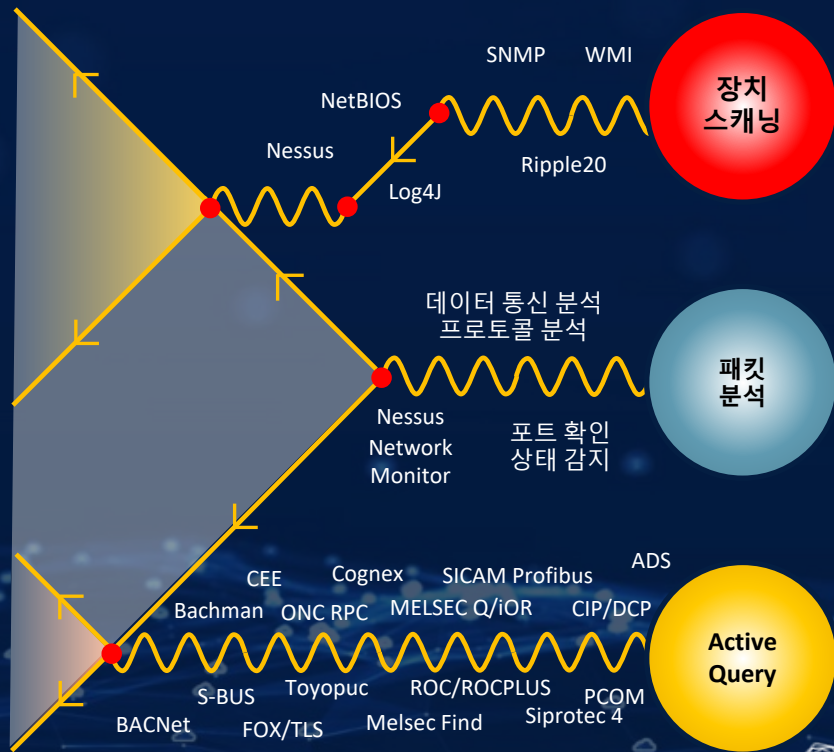
수동 분석 불가능 구역

# OT 보안 강화 방안

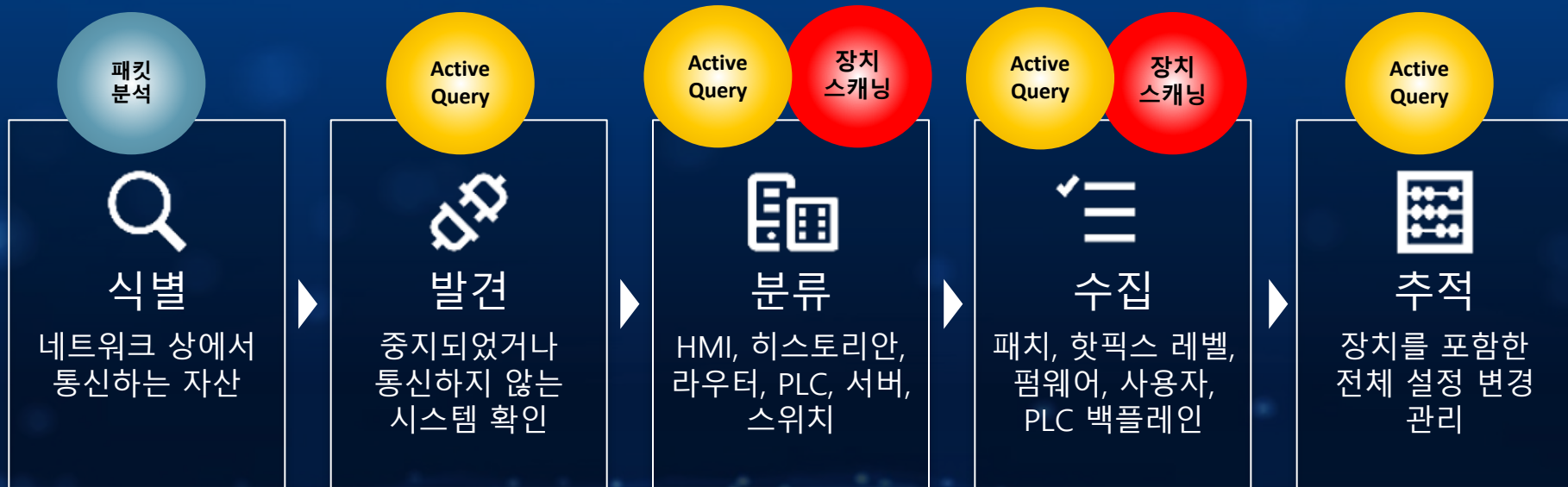


# OT 위험 분석 방안 – 하이브리드 방안 필요

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



# 하이브리드 분석을 통한 빠른 자산 확인



# 하이브리드 분석을 통한 설정 정보 분석

## VERSION 1

- 초기 기준점

## VERSION 2

- 주기적인 스냅샷
- 변경사항 없음

## VERSION 3

- 행위 발생
- PLC 프로그램 언어상의  
변화 감지(PLC Ladder  
Logic)

## VERSION 4

- 초기 기준선으로  
재설정

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

tenable.ot  
Powered by Indrigo

Europe Central - HQ > MII > Inventory

10:41 AM - Monday, Jan 6, 2020

MIIL

DASHBOARD

EVENTS

POLICIES

INVENTORY

CONTROLLERS

NETWORK ASSETS

RISK

NETWORK

GROUPS

REPORTS

IMS SETTINGS

Assembly\_Line\_B #7

Controller

ADDRESS

10.100.102.33 | 10.100.102.34 | 10.100.101.156

STATE

Unknown

VENDOR

Siemens

FAMILY

Siemens 57-400

MODEL

CPU 412-2 Fx/DP

FIRMWARE

V5.6.2

LAST SEEN

4:21:05 PM - Jan 14, 2019

CRITICALITY RATING (ACR)

7

DETAILS

COMPONENTS

EVENTS

CODE REVISIONS

RISK

VULNERABILITIES

CVES

DIAGNOSTIC BUFFER

OPEN PORTS

IP TRAIL

ASSET MAP

VERSION 4

10:03 PM - FEB 15, 2019

Baseline

VERSION 3

7:36 PM - FEB 11, 2019

VERSION 2

11:42 PM - NOV 29, 2018

VERSION 1

9:25 AM - NOV 17, 2018

Version 4

Search

Compare to: Previous Version

Set Version as Baseline

Take Snapshot

NAME	SIZE	COMPILATION DATE
↳ LFI		4:32 AM - Oct 10, 2018
↳ Tags		4:32 AM - Oct 10, 2018
(int) Read	N/A	4:32 AM - Oct 10, 2018
(Message) MSG1	N/A	4:32 AM - Oct 10, 2018
(Message) MSG2	N/A	4:32 AM - Oct 10, 2018
(Sink) MSG_Read_Data	N/A	4:32 AM - Oct 10, 2018
(Sink) MSG_Read_Request	N/A	4:32 AM - Oct 10, 2018
(int) N7	N/A	4:32 AM - Oct 10, 2018
↳ MainTask		4:32 AM - Oct 10, 2018
↳ Programs		4:32 AM - Oct 10, 2018
↳ MainProgram		4:32 AM - Oct 10, 2018
↳ Tags		4:32 AM - Oct 10, 2018
(Sou) Button	N/A	4:32 AM - Oct 10, 2018
Routines		4:32 AM - Oct 10, 2018
(Ladder) Manoeuvre	108B	4:32 AM - Oct 10, 2018
↳ Floop		4:32 AM - Oct 10, 2018
↳ Programs		4:32 AM - Oct 10, 2018
↳ Tags		4:32 AM - Oct 10, 2018
(Count) Nopie	N/A	4:32 AM - Oct 10, 2018
Routines		4:32 AM - Oct 10, 2018

Version 4 Snapshots list

User Generated Snapshot

10:03 PM - FEB 15, 2019

Event Triggered Snapshot

10:03 PM - FEB 14, 2019

Periodic Query Snapshot

10:03 PM - FEB 14, 2019

User Generated Snapshot

10:03 PM - FEB 10, 2019

Event Triggered Snapshot

10:03 PM - FEB 4, 2019

Periodic Query Snapshot

10:03 PM - FEB 2, 2019

Periodic Query Snapshot

10:03 PM - FEB 1, 2019

Event Triggered Snapshot

10:03 PM - FEB 1, 2019

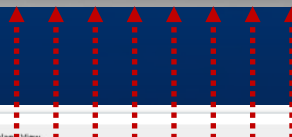
추가 정보

삭제 정보

Version 3.0 | Expires: Nov 17, 2020

# OT 위험 분석 예 - 네트워크 및 설정 정보 분석

구성 관리 데이터를 동시에 분석- 정확한 상황인지  
발생 이벤트에 대한 정확한 판단



Details

Code Revision

IP Trail

Attack Vectors

Open Ports

CVEs

Vulnerabilities

Events

Network Map

Device Ports

Overview

NAME	ROT
DESCRIPTION	Rockwell Automation 1756-L81E/B
LOCATION	SHEPHERDS-BUSH
PURDUE LEVEL	Level 1
STATE	Stopped
STATE UPDATE TIME	08:59:59 AM - Apr 6, 2021
DIRECT IPS	10.100.101.150
DIRECT MAC	00:1d9c:d4:c3:95
ASSOCIATED IPS	10.100.101.150   10.100.101.151   10.100.101.155
ASSOCIATED MACS	00:1d9c:d4:c3:95, 00:1d9c:d4:70:34, 00:1d9c:d4:2d:e9
FAMILY	ControlLogix 5580
VENDOR	Rockwell
MODEL NAME	1756-L81E/B
LAST SEEN	05:04:45 PM - Aug 10, 2021
FIRST SEEN	07:44:32 AM - Apr 6, 2021
NETWORK SEGMENTS	Controller / 10.100.101.X
RISK SCORE	24

Custom Fields

POINT OF CONTACT	eng134@eth.gov.uk
ASSET ID	44107

General

Backplane View

Backplane #44

0	1	2	3	4	5	6	7	8	9
ROT-COMM-PRI	GREEN-COMM	BLAU-COMM	ROT	GREEN	BLAU	ROT-COMM-SEC	GREEN-COMM		

Communication Module Details

NAME	ROT-COMM-PRI
RISK SCORE	24
TYPE	Communication Module
MODEL	1756-DNB/E
VENDOR	Rockwell
FW VERSION	12.005
ASSOCIATED IP'S	10.100.101.150   10.100.101.151   10.100.101.155
SLOT NUMBER	0
PURDUE LEVEL	Level 1

# 최종 목표 - 공격 경로 제거

모든 보안 위험은 악용이  
가능한 취약한 시스템에서  
시작

Attack vector generated on 11:30:47 PM · Oct 26, 2020

Export

Generate ▾



악용공격

초기 시작지점

ATTACKER  
ON-RAMP



ATTACKER  
OFF-RAMP

취약한  
시스템



http (tcp/80)



PAINT-HIST  
172.16.21.2

nntp (udp/123)



PLANTAD02.H2O.IO  
172.16.21.2

DNS (udp/53)



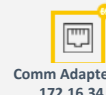
PLANTSVR01.H2O.IO  
172.16.22.3

microsoft-ds (tcp/445)



PLANTSVR03.H2O.IO  
172.16.22.3

CIP (tcp/44818)



Comm Adapter #24  
172.16.34.8



PAINTSHOP-G2

Serial/Direct/IIP Communications



ATTACKER  
OFF-RAMP

공격대상



악용공격

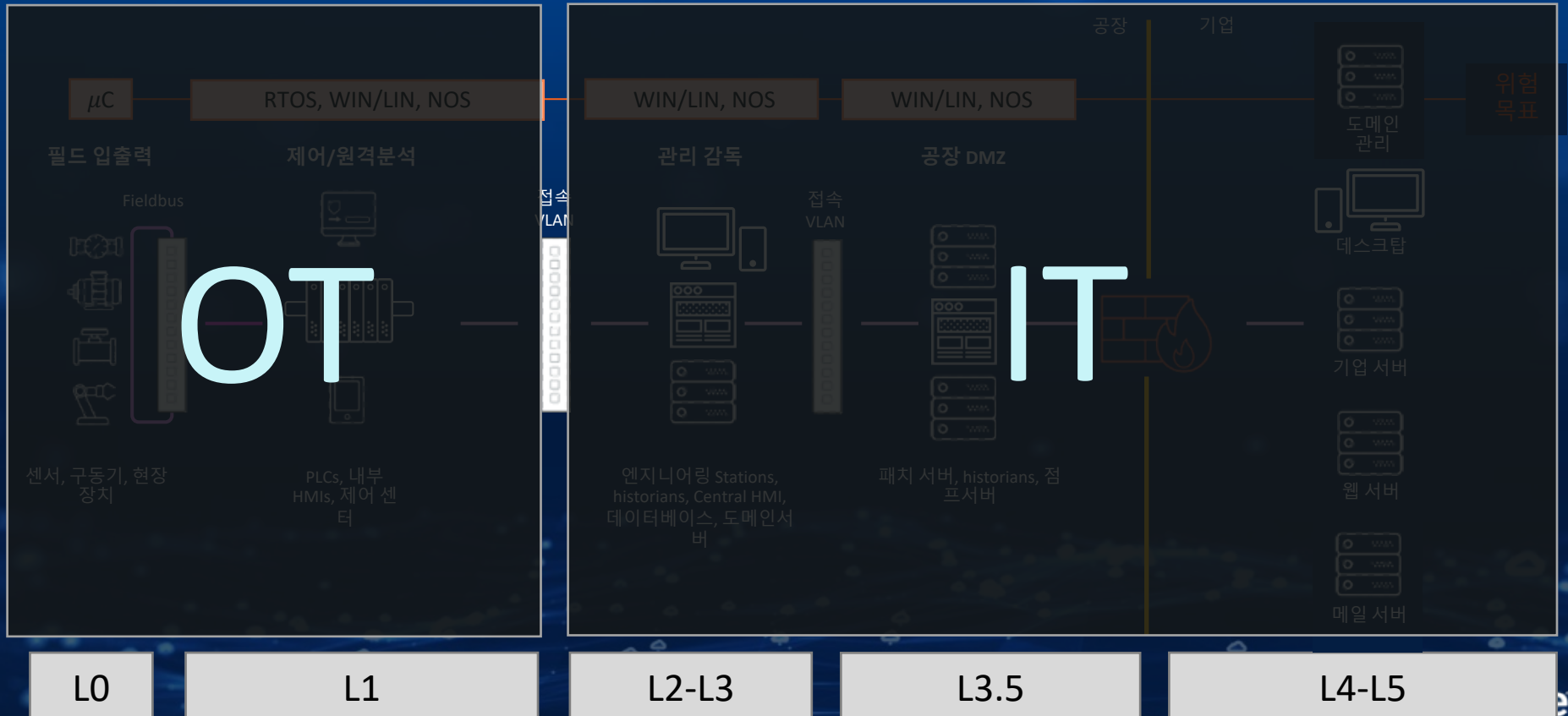
악용공격

악용공격





# OT 보안 영역 재정의



## IT/OT 영역을 모두 잘 아는 솔루션이 필요





**THANK  
YOU**

<https://tenable.com/products/tenable-ot> 에서 필요한 정보를 확인 하실 수 있습니다