ANALYSIS, NETWORK REDESIGN, AND MONITORING OF AN INDUSTRIAL ENVIRONMENT FOR IMPROVING ITS SECURITY (APPLICATION TO AN INDUSTRIAL PROCESS CONTROL TESTBED)

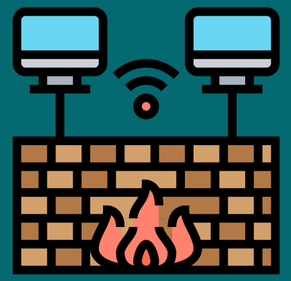
Valentín Santos Pérez

Contents

Project objectives

Network Redesign of the Industrial Environment

Development of a network architecture following industrial cybersecurity **best practices** and utilizing reference models



Industrial environment attacks

Execution of various **attacks** to verify the effectiveness of the measures applied in the environment and to test the monitoring of the system

Deployment of a monitoring solution

Implementation of a **monitoring** tool that provides visibility over system devices and detects threats in network communications

tenable®

Compliance with standards and regulations

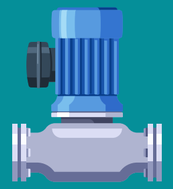
Use of the **IEC 62443** family of reference standards for industrial cybersecurity best practices

ISA™

Industrial environment used

Industrial four-variable testbed

Simulation of industrial processes through the control of four variables: level, flow, pressure, and temperature



Process circuit

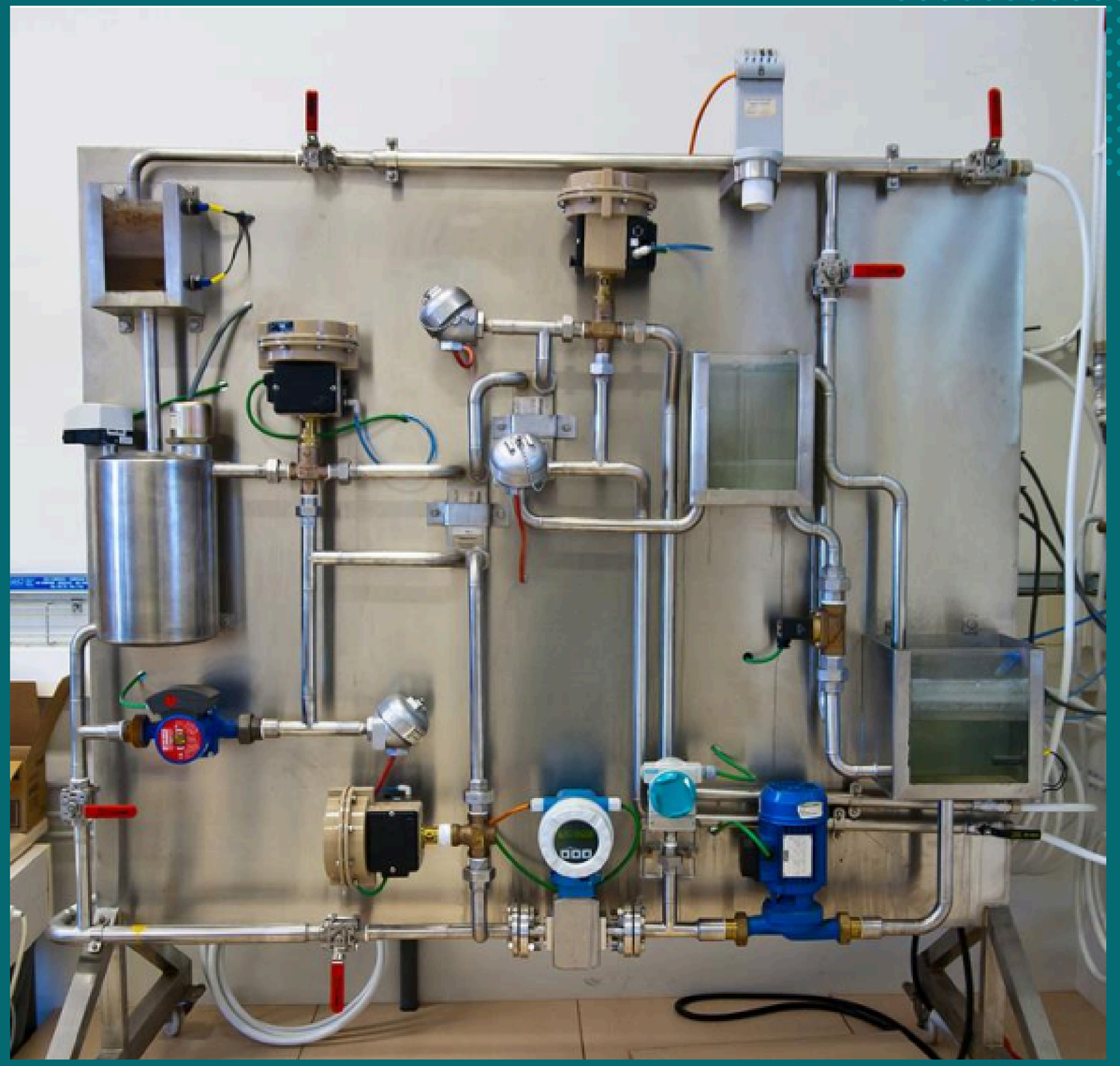
Fluid circulation between the tanks, with adjustable speed and flow rate

Cooling circuit

Circulation of coolant along with a plate heat exchanger for fluid cooling

Heating circuit

Water heating using electric resistors and a plate heat exchanger to transfer heat



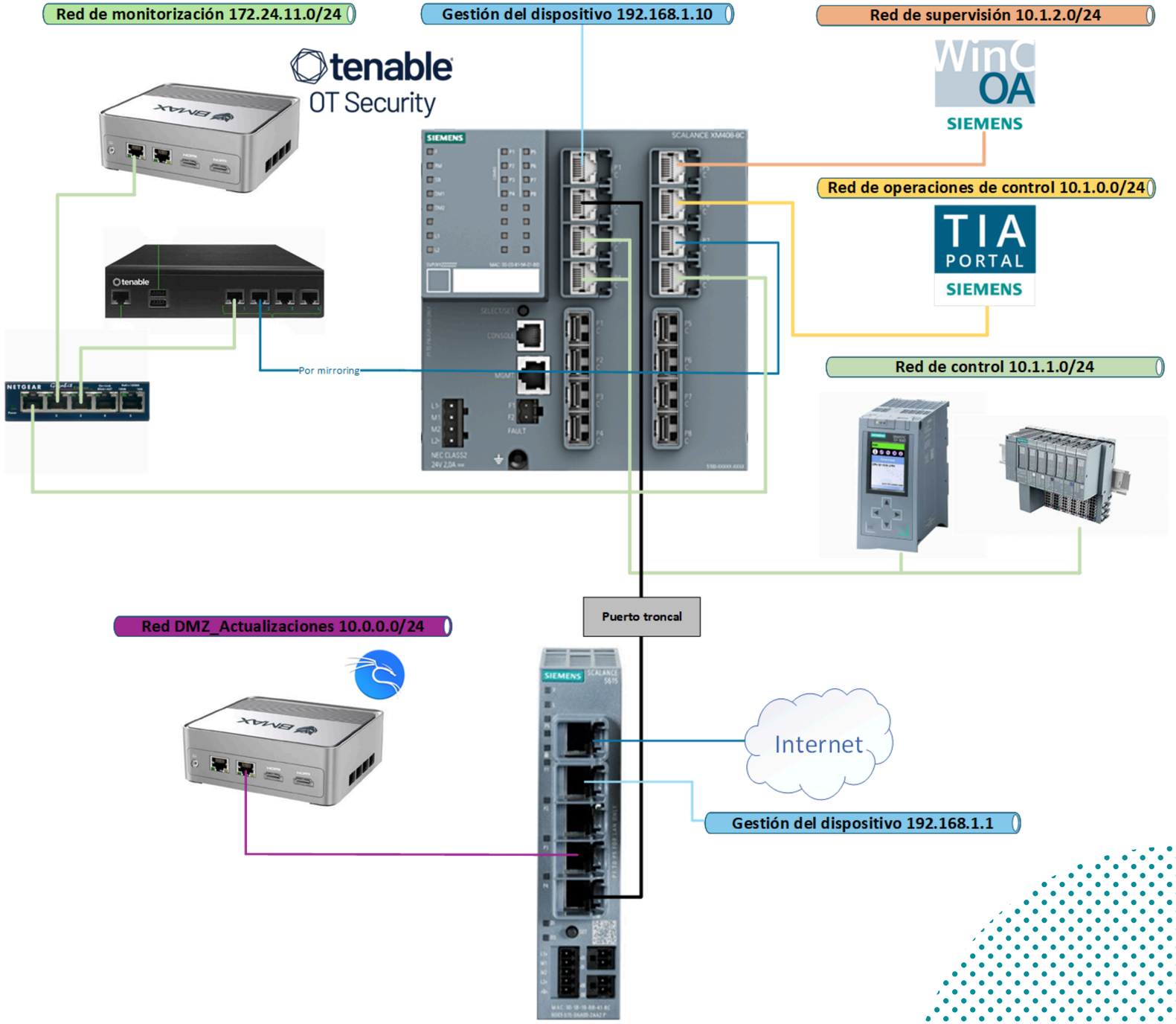
GRUPO SUPPRESS

SUPERVISIÓN, CONTROL Y AUTOMATIZACIÓN

universidad de león

Dispositivos del entorno indutrial

Industrial control systems	PLC SIEMENS S7-1516 SIEMENS ET-200SP SCADA SIEMENS WinCC
Comunication devices	SIEMENS SCALANCE S615 - Firewall SIEMENS SCALANCE XM408 - Switch
Monitoring tool	Tenable OT Security Sensor Tenable OT Security
Management software	SIEMENS TIA Portal - Windows 10
DMZ server	OpenSSH server - Kali Linux



Network redesign

Network segmentation

Stage

00

Analysis of the initial situation

Stage

01

Initial segmentation

Stage

02

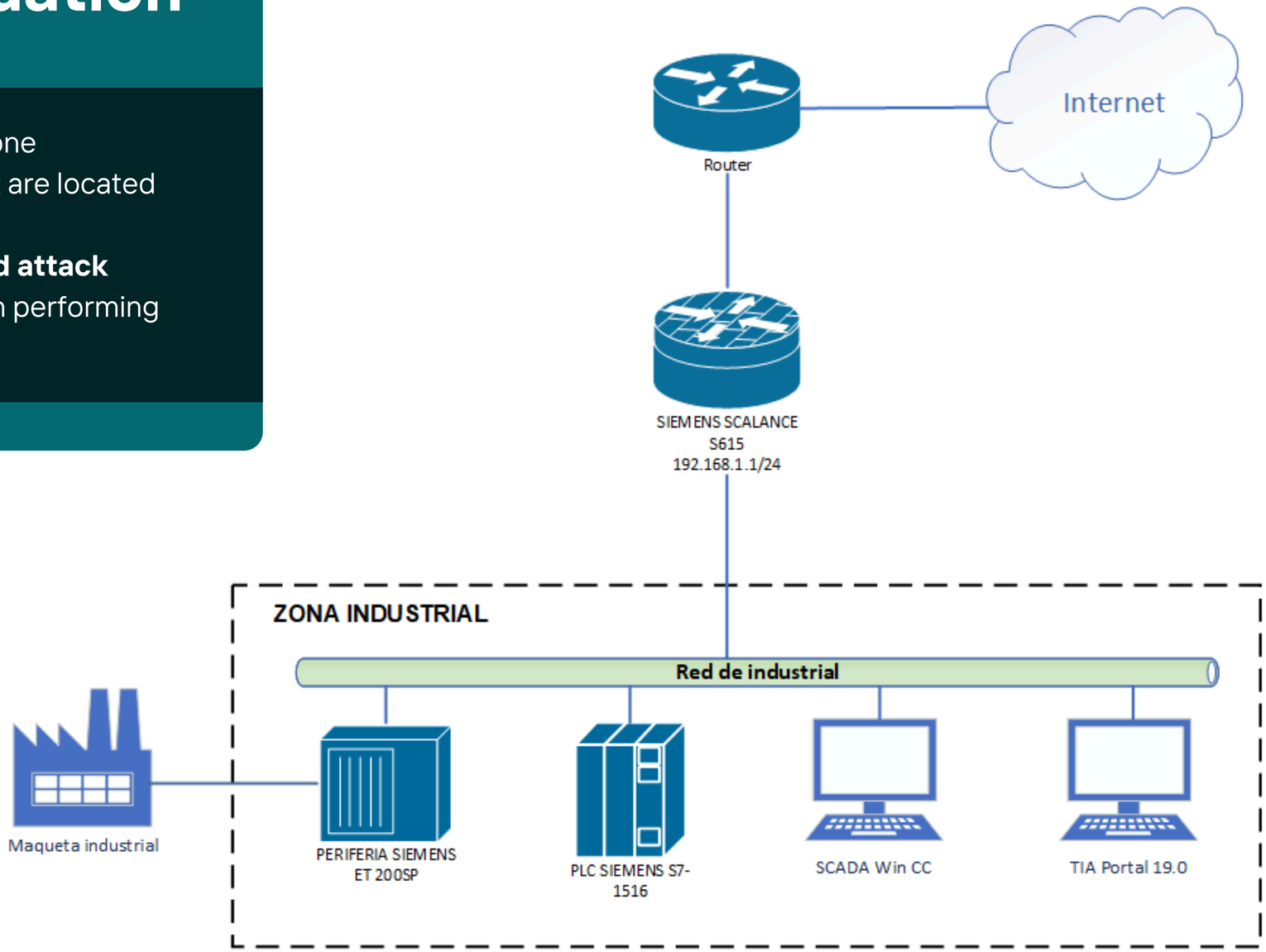
Segmentation aimed at maximum security

Through network segmentation, **zones** are created, where devices with similar characteristics or requirements are grouped. Communications between these zones are carried out through **conduits**.

The process of segmenting the network is carried out in several stages, implementing the changes **gradually**.

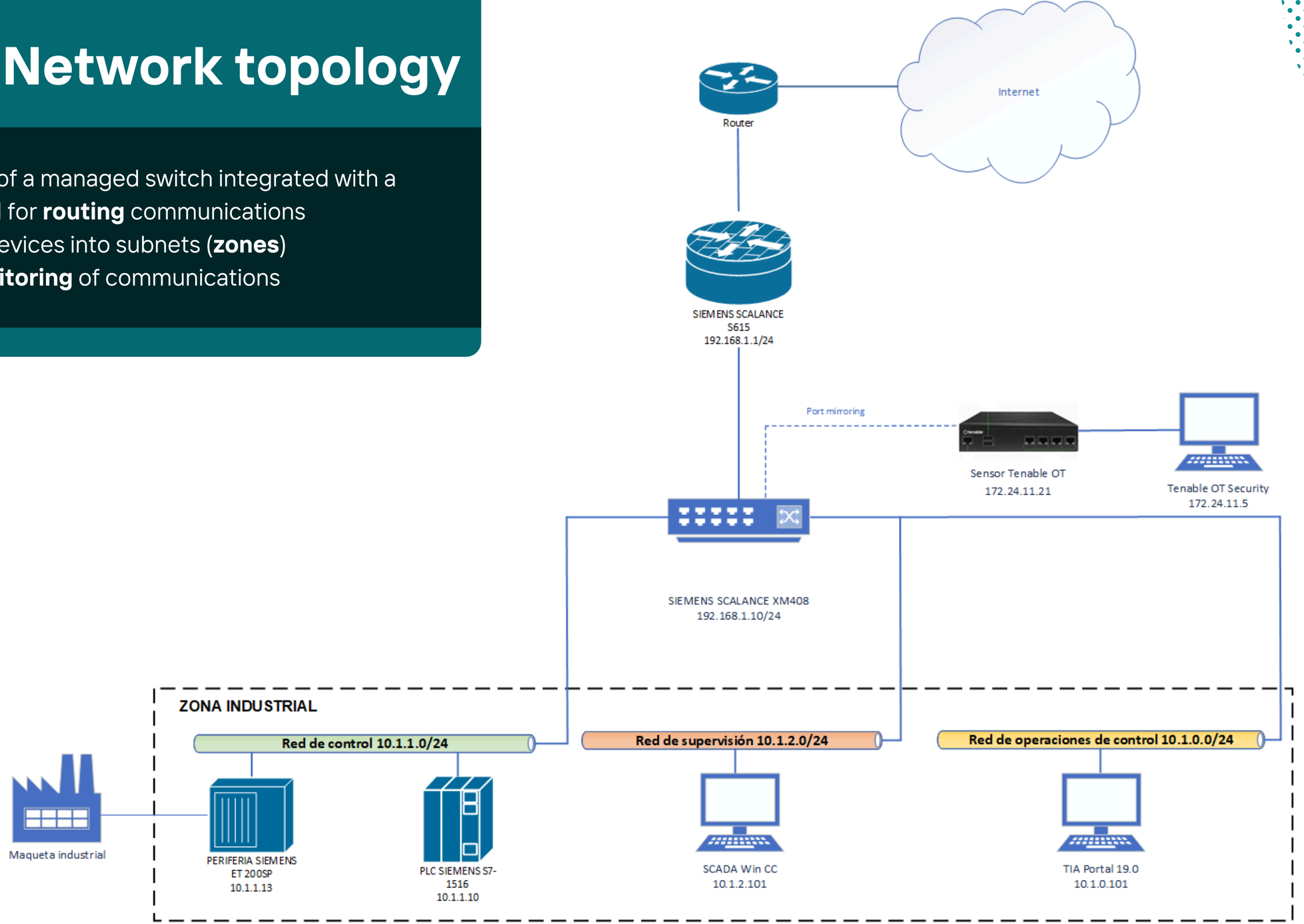
Stage 0: Initial situation

- **Internet connection** in the industrial zone
- All devices in the industrial environment are located within the **same network**
- Large number of associated risks: **broad attack surface**, **lateral movement**, difficulty in performing **security monitoring** of the system...



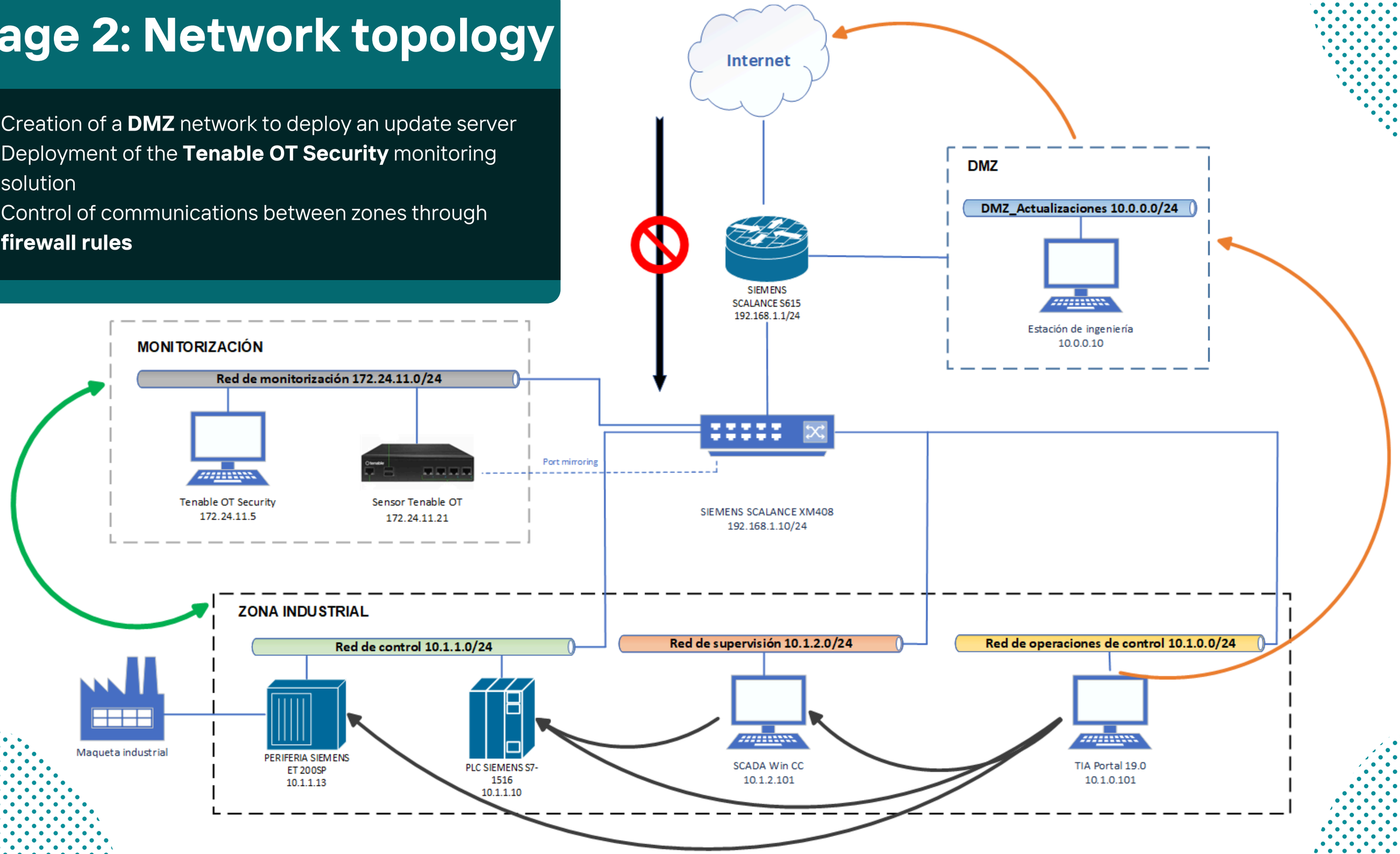
Stage 1: Network topology

- **Deployment** of a managed switch integrated with a router/firewall for **routing** communications
- Grouping of devices into subnets (**zones**)
- **Passive monitoring** of communications



Stage 2: Network topology

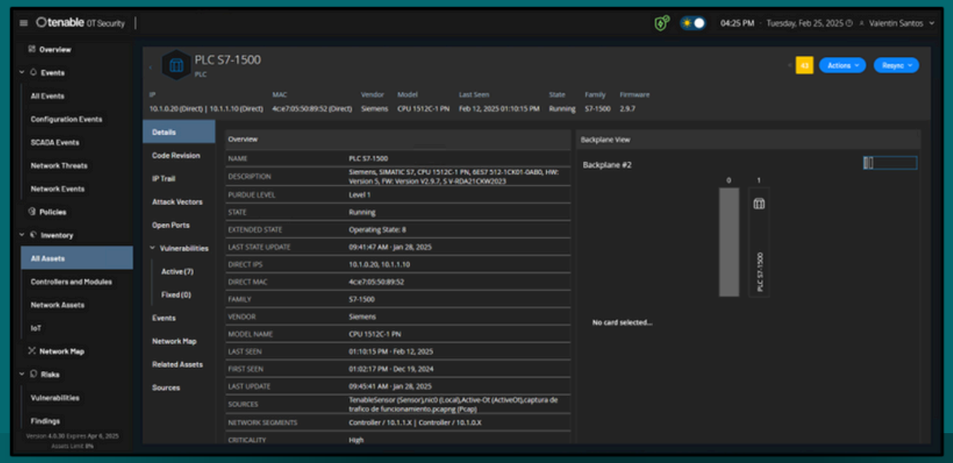
- Creation of a **DMZ** network to deploy an update server
- Deployment of the **Tenable OT Security** monitoring solution
- Control of communications between zones through **firewall rules**



Monitoring solution

tenable®
OT Security

tenable
OT Security



Information about assets

Through **passive monitoring** and **active queries**, detailed information about the devices in the industrial environment has been collected.

Vulnerabilities

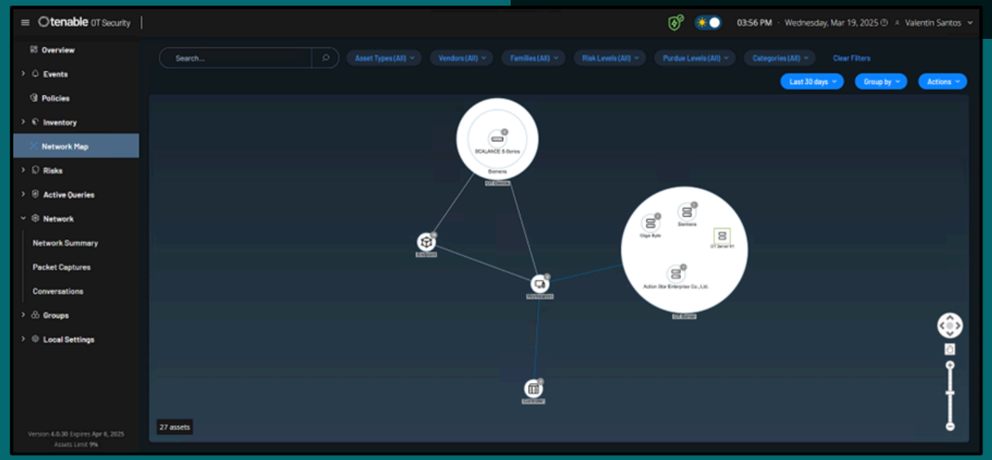
Alerts on device-associated vulnerabilities through Tenable OT Security database and information obtained from active scans

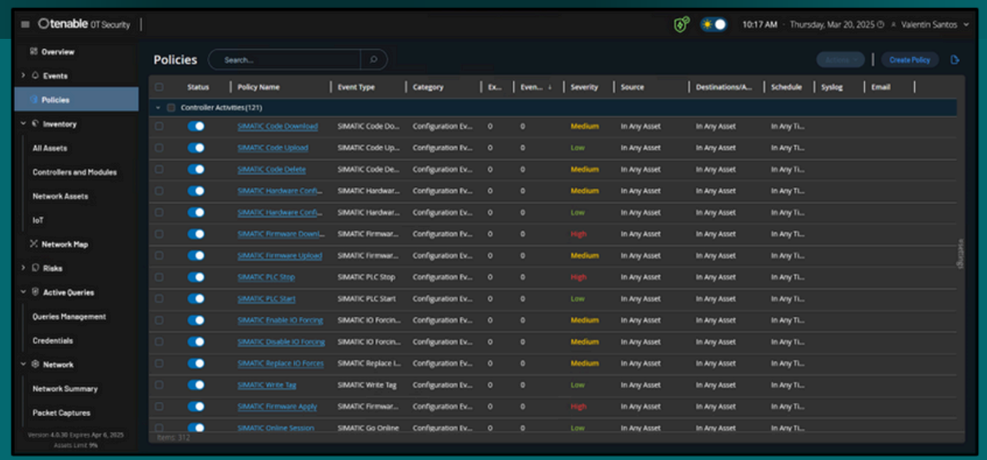
Visibility

Network map showing the **system topology**

Industrial IDS

Configuration of environment-specific **policies** to ensure proper reporting of security events in network communications





Attacks on the industrial environment

Some reported alerts

Not resol...	45	10:11:53 AM · Apr 1, 2025	Intrusion Detection	Medium	Scans - VNC	172.24.11.11	PLC S7-1500	10.1.1.10
Not resol...	44	10:11:35 AM · Apr 1, 2025	Intrusion Detection	Medium	Scans - NMAP	172.24.11.11	PLC S7-1500	10.1.1.10
Not resol...	43	10:11:35 AM · Apr 1, 2025	Intrusion Detection	Medium	Scans - NMAP	172.24.11.11	PLC S7-1500	10.1.1.10
Not resol...	42	10:03:14 AM · Apr 1, 2025	Intrusion Detection	Medium	Scans - VNC	172.24.11.11	MAQUETA2LAB-E2	10.1.2.101
Not resol...	41	10:03:13 AM · Apr 1, 2025	Intrusion Detection	Medium	Scans - NMAP	172.24.11.11	MAQUETA2LAB-E2	10.1.2.101
Not resol...	40	10:03:13 AM · Apr 1, 2025	Intrusion Detection	Medium	Scans - NMAP	172.24.11.11	MAQUETA2LAB-E2	10.1.2.101
Not resol...	39	10:02:00 AM · Apr 1, 2025	Spike in conversa...	Medium	Network Traffic Conversa...			
Not resol...	37	09:58:11 AM · Apr 1, 2025	Intrusion Detection	Medium	Scans - NMAP	172.24.11.11	PLC S7-1500	10.1.1.10
Not resol...	38	09:58:11 AM · Apr 1, 2025	Intrusion Detection	Medium	Scans - NMAP	172.24.11.11	PLC S7-1500	10.1.1.10
Not resol...	36	09:56:33 AM · Apr 1, 2025	ARP Scan	Medium	ARP Scan Detection	d4:be:d9:70:8c:0f		

Reconnaissance scans – Nmap

```
└─# nmap 10.1.2.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-27 13:49 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --syst
em-dns or specify valid servers with --dns-servers
Nmap scan report for 10.1.2.101
Host is up (0.011s latency).
Not shown: 972 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
81/tcp    filtered hosts2-ns
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
443/tcp   open     https
444/tcp   filtered snpp
445/tcp   filtered microsoft-ds
902/tcp   filtered iss-realsecure
912/tcp   filtered apex-mesh
1217/tcp  filtered hpss-ndapi
1801/tcp  open     msmq
2103/tcp  open     zephyr-clt
2105/tcp  open     eklogin
2107/tcp  open     msmq-mgmt
3389/tcp  open     ms-wbt-server
3580/tcp  filtered nati-svrloc
4443/tcp  filtered pharos
4444/tcp  filtered krb524
5002/tcp  filtered rfe
5800/tcp  open     vnc-http
5900/tcp  open     vnc
7200/tcp  filtered fodms
8080/tcp  filtered http-proxy
8090/tcp  filtered opsmessaging
8888/tcp  filtered sun-answerbook
27000/tcp filtered flexlm0
48080/tcp filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 1.64 seconds
```

Brute-force attacks – Hydra

```
└─# hydra -L Brute_USERS -P Brute_PASS ssh://10.1.2.101
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-27 13:51:27
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 7579 login tries (l:53/p:143), ~474 tries per task
[DATA] attacking ssh://10.1.2.101:22/
```

Fuzzing attacks – boofuzz

```
boofuzz Fuzz Control                                         RUNNING
Total:       739   of  many
Request:     739   of  10,115  [====                    ]  7.306%
run time     27 sec
exec speed   27.1/sec
current      Request:[Request.Request-Line.Request-URI:684]
Pause
Test Case #                    Crash Synopsis
Test Case Log: 709    < 709 >  snap to current test case
[2025-02-27 13:42:49,543] Test Case: 709: Request:[Request.Request-Line.Request-URI:654]
[2025-02-27 13:42:49,543]     Info: Type: String
[2025-02-27 13:42:49,543]     Info: Opening target connection (10.1.1.10:80)...
[2025-02-27 13:42:49,547]     Info: Connection opened.
[2025-02-27 13:42:49,547]    Test Step: Monitor CallbackMonitor#140533314656864[pre=[],post=[],r
[2025-02-27 13:42:49,547]    Test Step: Fuzzing Node 'Request'
[2025-02-27 13:42:49,548]     Info: Sending 582 bytes...
[2025-02-27 13:42:49,548]     Transmitted 512 bytes (data truncated for database storage): 47 45
3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f
3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f
3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f
3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f
3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f
3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f b'GET
????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????
[2025-02-27 13:42:49,549]    Test Step: Contact target monitors
[2025-02-27 13:42:49,549]    Test Step: Cleaning up connections from callbacks
[2025-02-27 13:42:49,549]      Check OK: No crash detected.
[2025-02-27 13:42:49,549]     Info: Closing target connection...
[2025-02-27 13:42:49,550]     Info: Connection closed.
```

Conclusions

01 High level of cybersecurity achieved

02 The applied measures meet with reference standards and industrial security best practices

03 The importance of industrial security is highlighted thanks to the realistic nature of the work

Acknowledgements

GRUPO SUPPRESS

SUPERVISIÓN, CONTROL Y AUTOMATIZACIÓN

universidad de león

S21SEC

Cyber Solutions by Thales


¡THANK YOU!