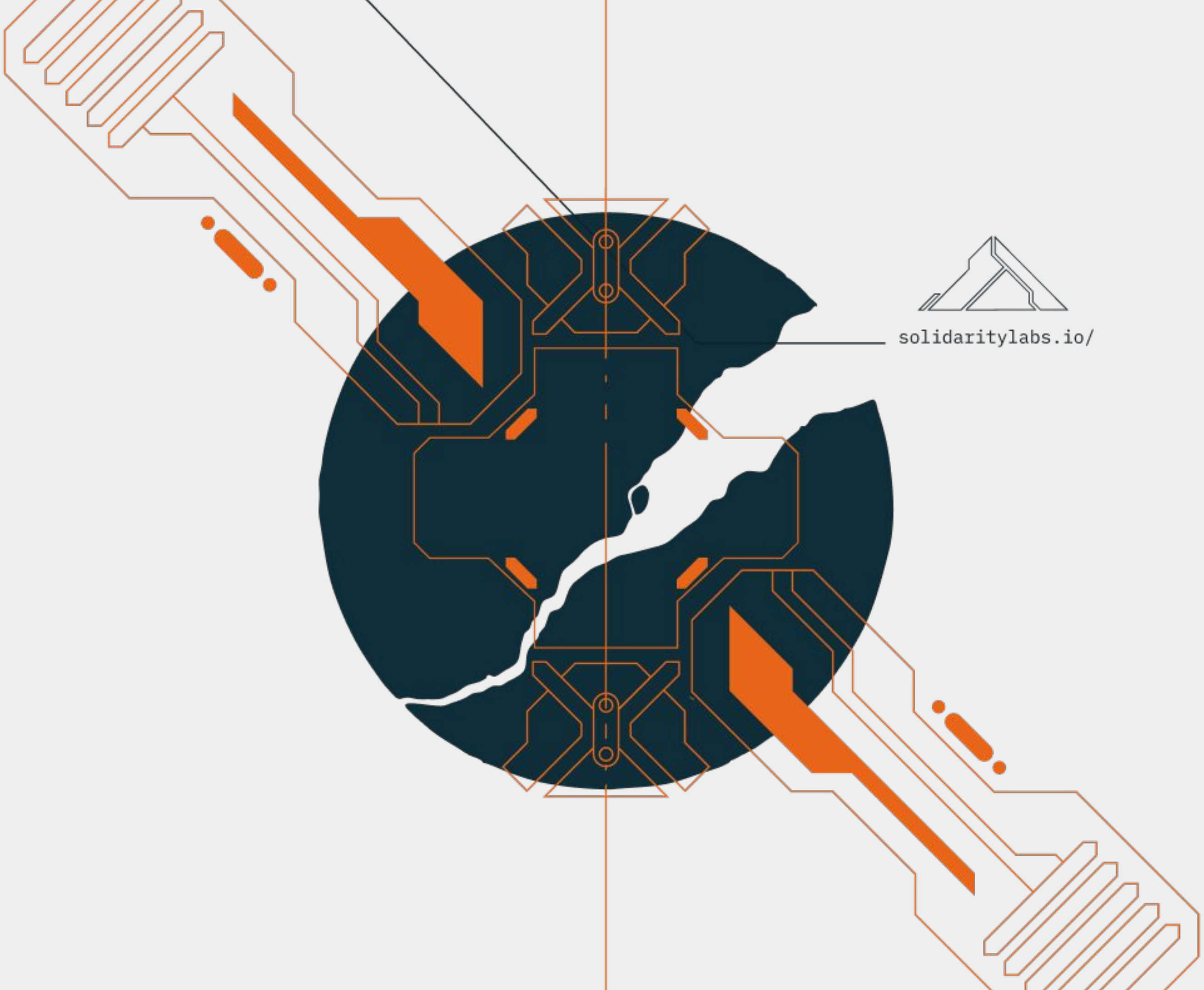


solidaritylabs.io/

Captura de IOCs en la Nube

solidaritylabs.io/

SECUREOT
CYBERSECURITY VILLAGE

EKOPARTY 2.0

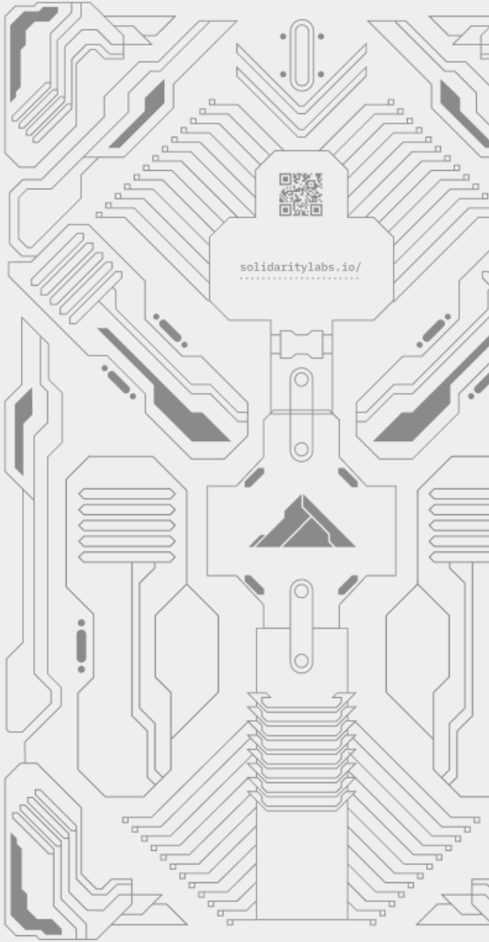
Matias Federico Manassero

Ex Policía Federal, experto en ICS enfocado en arquitecturas Onprem-Cloud

in /matiasmanassero

Tabla de Contenido

1. Introducción a OT
2. Desafíos de Seguridad OT
3. Continuidad Operativa y Seguridad
4. Integración de OT con AWS
5. Zero Trust con AWS
6. Arquitectura OT con AWS
7. Demo
8. Q&A



Introducción a OT

Tecnología de la Información

- IT se refiere a la gestión de datos, información y sistemas de cómputo en el mundo empresarial.
- Involucra computadoras, servidores, redes y software para almacenar, procesar y distribuir información en organizaciones.

Tecnología Operativa

- OT se centra en controlar y automatizar procesos industriales y físicos en sectores como la manufactura, la energía y el transporte.
- Implica tecnologías como controladores lógicos programables (PLCs) y sistemas de control industrial para garantizar la eficiencia y la seguridad en la producción.

Introducción a OT

Dominios

- Herramientas de escaneo de vulnerabilidades
- Equipos legacies
- Ventanas de mantenimiento
- Protocolos

Dominios

- Aplicación de parches
- Proveedores
- Gestión de riesgos

Orientada al Safety y Disponibilidad

Introducción a OT

PLC

SECUREOT
CYBERSECURITY VILLAGE

EKOPARTY
20

EtherNet/IP conformance tested
RS-485
RS-485
STATUS
RX
TX
Mod
Net
Powermonitor 1000
+
-
SHLD
ACT
LNK
AB
Allen-Bradley

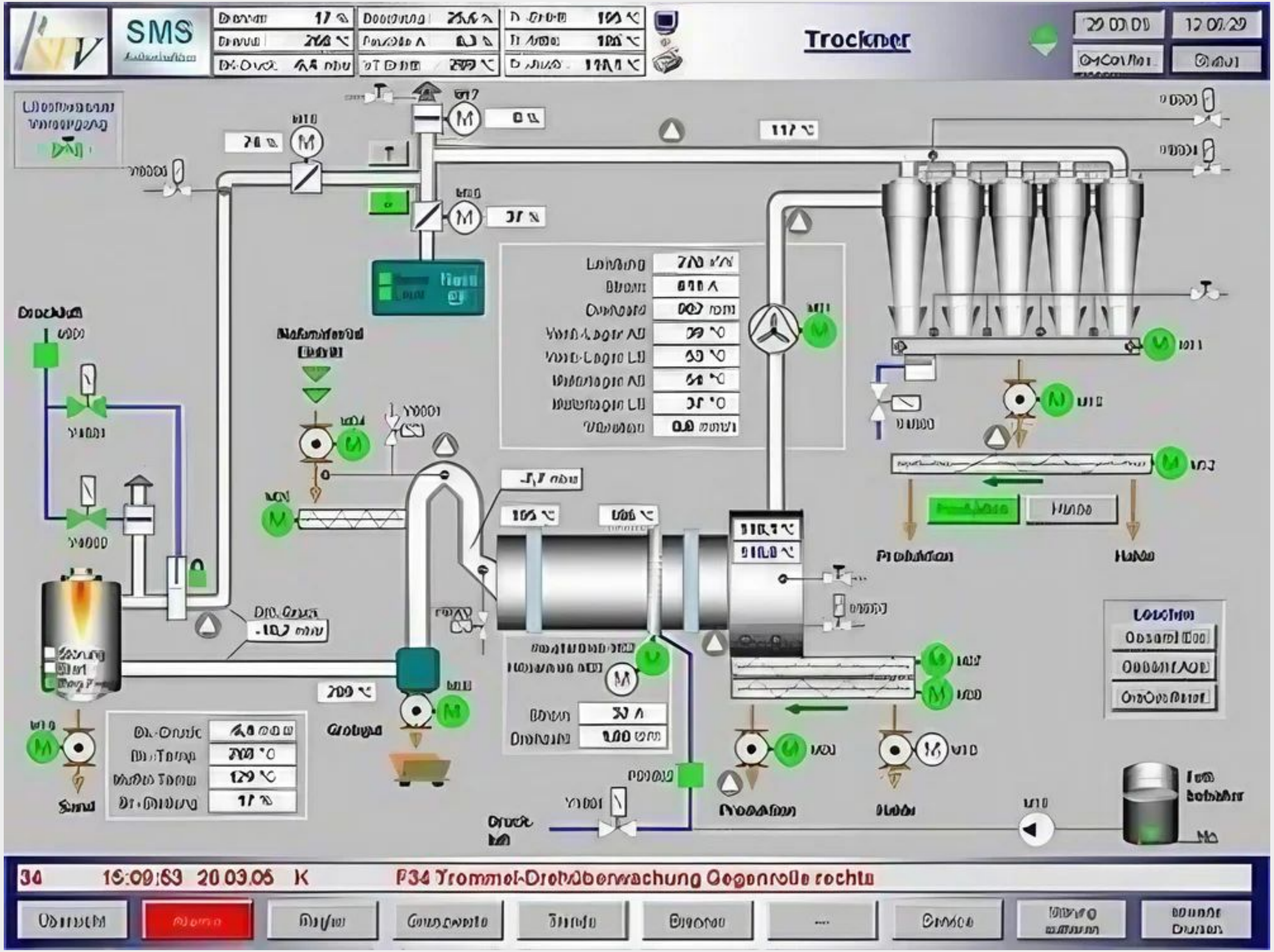
SIEMENS
SIMATIC
S7-1200
RUN / STOP
ERROR
MAINT
DI a
DI b
CPU 1214FC
DC/DC/DC
DQ a
DQ b

Introducción a OT

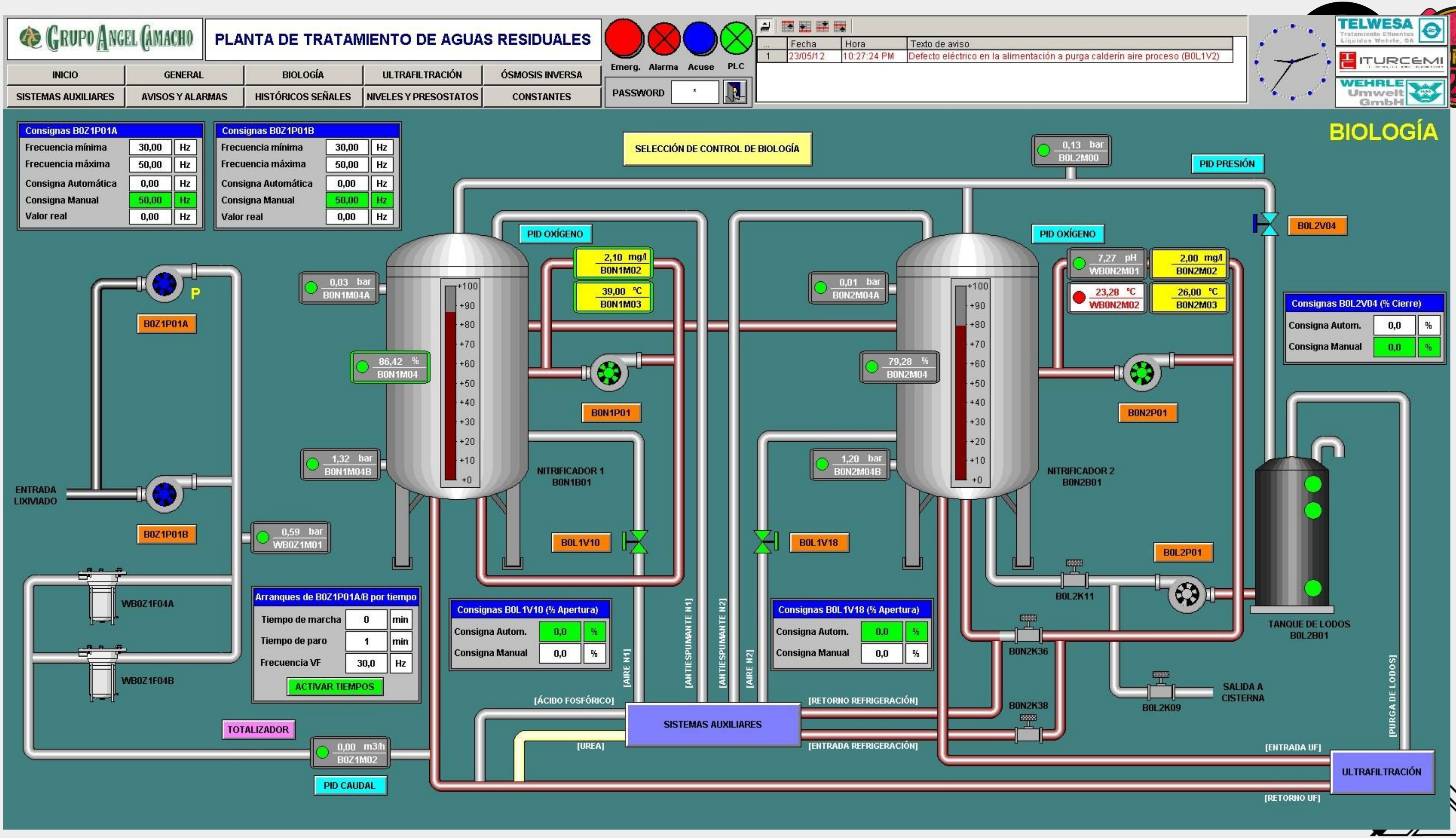
SCADA

SECUREOT
CYBERSECURITY VILLAGE

EKOPARTY
20



34 16:09:63 20.03.06 K P34 Trommel-Drehüberwachung Gegenrolle rechts



PLANTA DE TRATAMIENTO DE AGUAS RESIDUALES

...	Fecha	Hora	Texto de aviso
1	23/05/12	10:27:24 PM	Defecto eléctrico en la alimentación a purga calderín aire proceso (B0L1V2)

PASSWORD *

BIOLOGÍA

Consignas B0Z1P01A		
Frecuencia mínima	30,00	Hz
Frecuencia máxima	50,00	Hz
Consigna Automática	0,00	Hz
Consigna Manual	50,00	Hz
Valor real	0,00	Hz

Consignas B0Z1P01B		
Frecuencia mínima	30,00	Hz
Frecuencia máxima	50,00	Hz
Consigna Automática	0,00	Hz
Consigna Manual	50,00	Hz
Valor real	0,00	Hz

Consignas B0L2V04 (% Cierre)		
Consigna Autom.	0,0	%
Consigna Manual	0,0	%

Arranques de B0Z1P01A/B por tiempo		
Tiempo de marcha	0	min
Tiempo de paro	1	min
Frecuencia VF	30,0	Hz

ACTIVAR TIEMPOS

Consignas B0L1V10 (% Apertura)		
Consigna Autom.	0,0	%
Consigna Manual	0,0	%

Consignas B0L1V18 (% Apertura)		
Consigna Autom.	0,0	%
Consigna Manual	0,0	%

Medición	Valor
B0L2M00	0,13 bar
B0N1M04A	0,03 bar
B0N1M02	2,10 mg/l
B0N1M03	39,00 °C
B0N1M04	86,42 %
B0N1M04B	1,32 bar
WB0Z1M01	0,59 bar
B0Z1M02	0,00 m3/h
B0N2M04A	0,01 bar
WB0N2M01	7,27 pH
B0N2M02	2,00 mg/l
WB0N2M02	23,28 °C
B0N2M03	26,00 °C
B0N2M04	79,28 %
B0N2M04B	1,20 bar

Desafíos de Seguridad en OT

solidaritylabs.io/

SECUREOT
CYBERSECURITY VILLAGE

EKOPARTY
20

Desafíos de Seguridad en OT

Obsolescencia Tecnológica

Los sistemas OT suelen estar basados en tecnologías antiguas que no reciben actualizaciones regulares, lo que los hace vulnerables a ciberataques.

Falta de parches y actualizaciones

Los sistemas OT suelen estar basados en tecnologías antiguas que no reciben actualizaciones regulares, lo que los hace vulnerables a ciberataques.

Disponibilidad vs Seguridad

La implementación de medidas de seguridad adicionales puede comprometer la disponibilidad en sistemas OT críticos.

Arquitectura con redundancia

No tener redundancia en diferentes ubicaciones físicas podría comprometer todo el sitio en caso de un ataque.

Requerimientos

AWS

SECUREOT
CYBERSECURITY VILLAGE

EKOPARTY
20

Requerimientos AWS

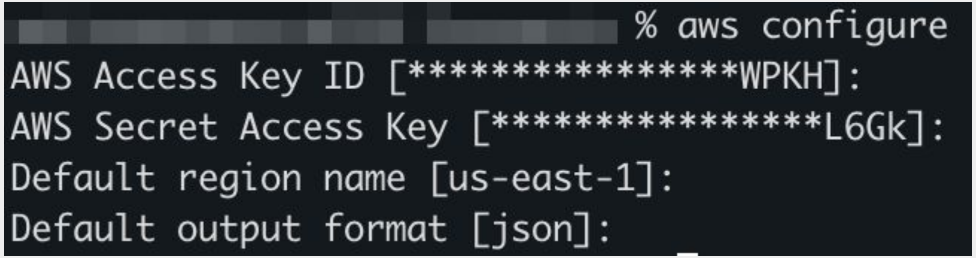
1. Crear una cuenta en AWS
2. Crear un usuario
3. Configurar MFA
4. Crear un grupo
5. Crear Access Key
6. Configurar una alerta de Billing

Requerimientos AWS

1. Instalar AWS CLI
2. Loguearse en AWS CLI

- aws configure

Resultado



```
[redacted] % aws configure
AWS Access Key ID [****************WPKH]:
AWS Secret Access Key [****************L6Gk]:
Default region name [us-east-1]:
Default output format [json]:
```

Requerimientos AWS

1. Generar claves

- `ssh-keygen -t rsa -b 4096 -C "your_email@example.com"`

2. Linux/macOS

- `cat ~/.ssh/id_rsa.pub`

3. Windows

- `Get-Content ~/.ssh/id_rsa.pub`

Requerimientos

Terraform

SECUREOT
CYBERSECURITY VILLAGE

EKOPARTY
20

Instalación de Terraform

Descargar Terraform

Requerimientos
Workshop OT

SECUREOT
CYBERSECURITY VILLAGE

EKOPARTY
20

Repositorio del Workshop

- git clone <link>

Infraestructura

Despliegue

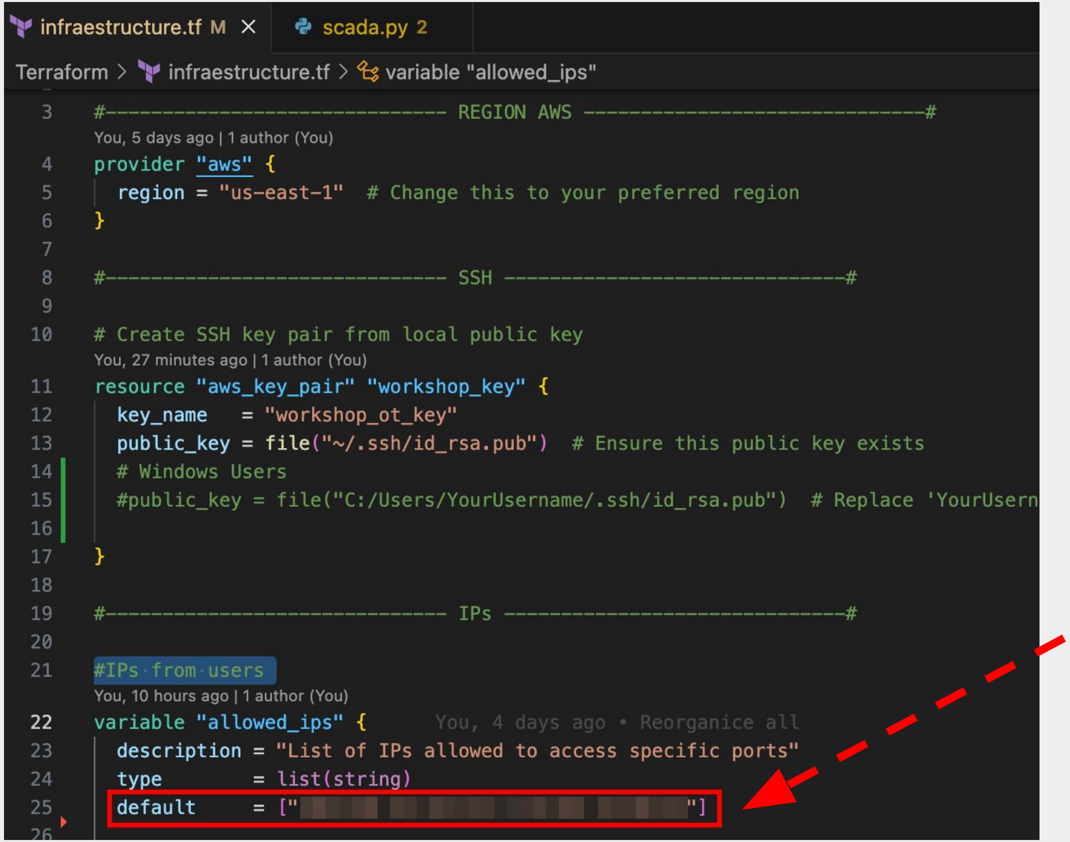
solidaritylabs.io/

solidaritylabs.io/

SECUREOT
CYBERSECURITY VILLAGE

EKOPARTY
20

Despliegue de IaC



infraestructure.tf M × | scada.py 2

Terraform > infraestructure.tf > variable "allowed_ips"

```
#------------------------------- REGION AWS -------------------------------#
You, 5 days ago | 1 author (You)
provider "aws" {
  region = "us-east-1"  # Change this to your preferred region
}

#------------------------------- SSH -------------------------------#

# Create SSH key pair from local public key
You, 27 minutes ago | 1 author (You)
resource "aws_key_pair" "workshop_key" {
  key_name   = "workshop_ot_key"
  public_key = file("~/.ssh/id_rsa.pub")  # Ensure this public key exists
  # Windows Users
  #public_key = file("C:/Users/YourUsername/.ssh/id_rsa.pub")  # Replace 'YourUsern

}

#------------------------------- IPs -------------------------------#

#IPs from users
You, 10 hours ago | 1 author (You)
variable "allowed_ips" {      You, 4 days ago • Reorganice all
  description = "List of IPs allowed to access specific ports"
  type        = list(string)
  default     = ["[redacted]"]
```

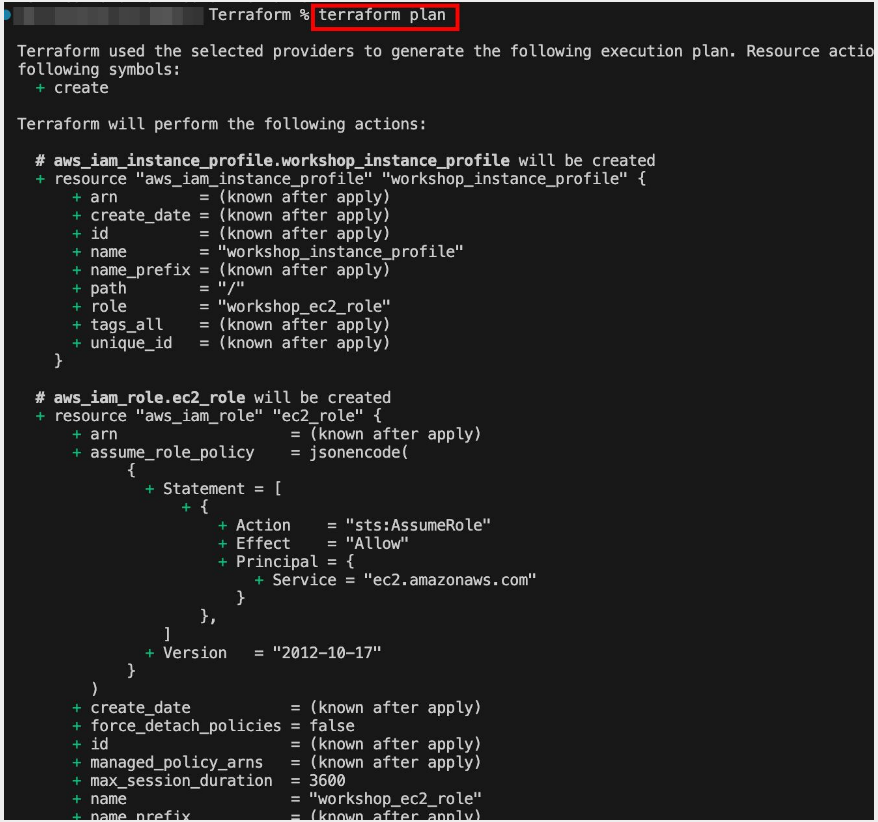
Comandos

- terraform plan
- terraform apply

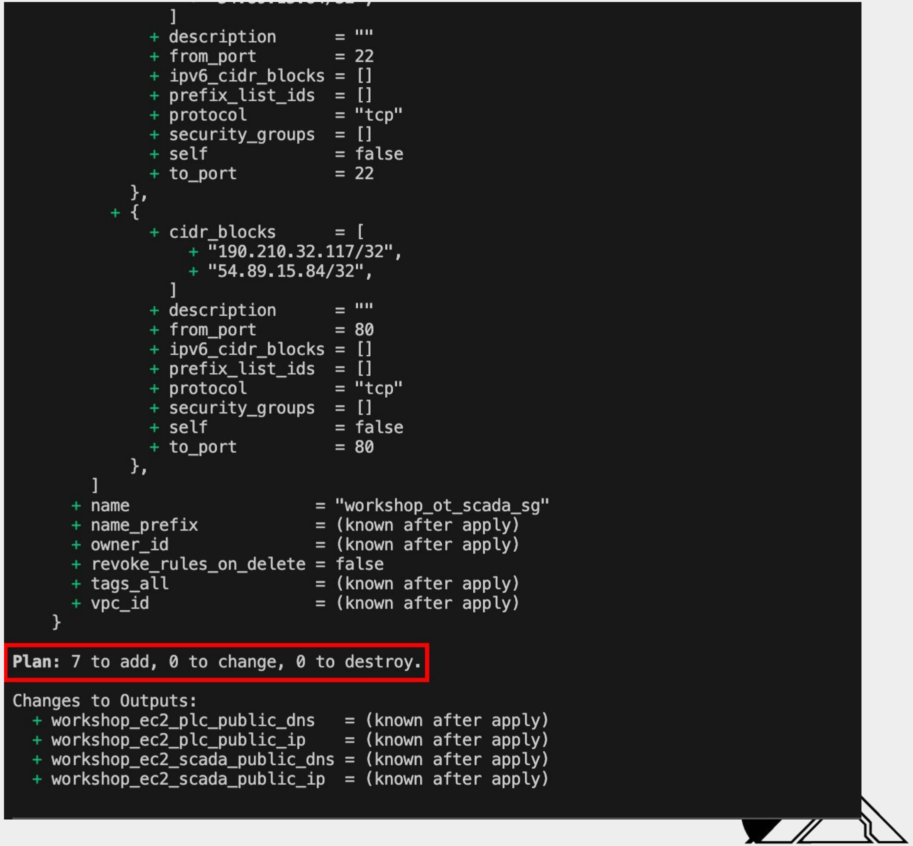
Comandos

- variable allowed_ips
- IPs from SCADA

Terraform plan

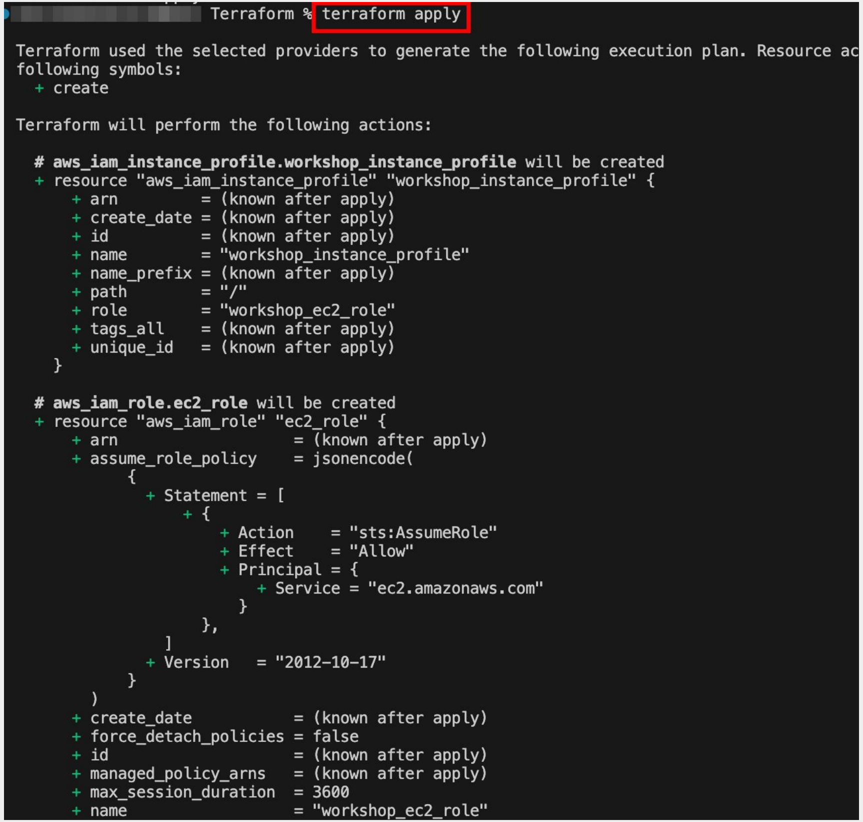


```
[redacted] Terraform % terraform plan

Terraform used the selected providers to generate the following execution plan. Resource actio
following symbols:
  + create

Terraform will perform the following actions:

  # aws_iam_instance_profile.workshop_instance_profile will be created
  + resource "aws_iam_instance_profile" "workshop_instance_profile" {
      + arn         = (known after apply)
      + create_date = (known after apply)
      + id          = (known after apply)
      + name        = "workshop_instance_profile"
      + name_prefix = (known after apply)
      + path        = "/"
      + role        = "workshop_ec2_role"
      + tags_all    = (known after apply)
      + unique_id   = (known after apply)
    }

  # aws_iam_role.ec2_role will be created
  + resource "aws_iam_role" "ec2_role" {
      + arn                   = (known after apply)
      + assume_role_policy    = jsonencode(
            {
              + Statement = [
                  + {
                      + Action    = "sts:AssumeRole"
                      + Effect    = "Allow"
                      + Principal = {
                          + Service = "ec2.amazonaws.com"
                        }
                    },
                ]
              + Version   = "2012-10-17"
            }
        )
      + create_date           = (known after apply)
      + force_detach_policies = false
      + id                    = (known after apply)
      + managed_policy_arns   = (known after apply)
      + max_session_duration  = 3600
      + name                  = "workshop_ec2_role"
      + name_prefix           = (known after apply)
```

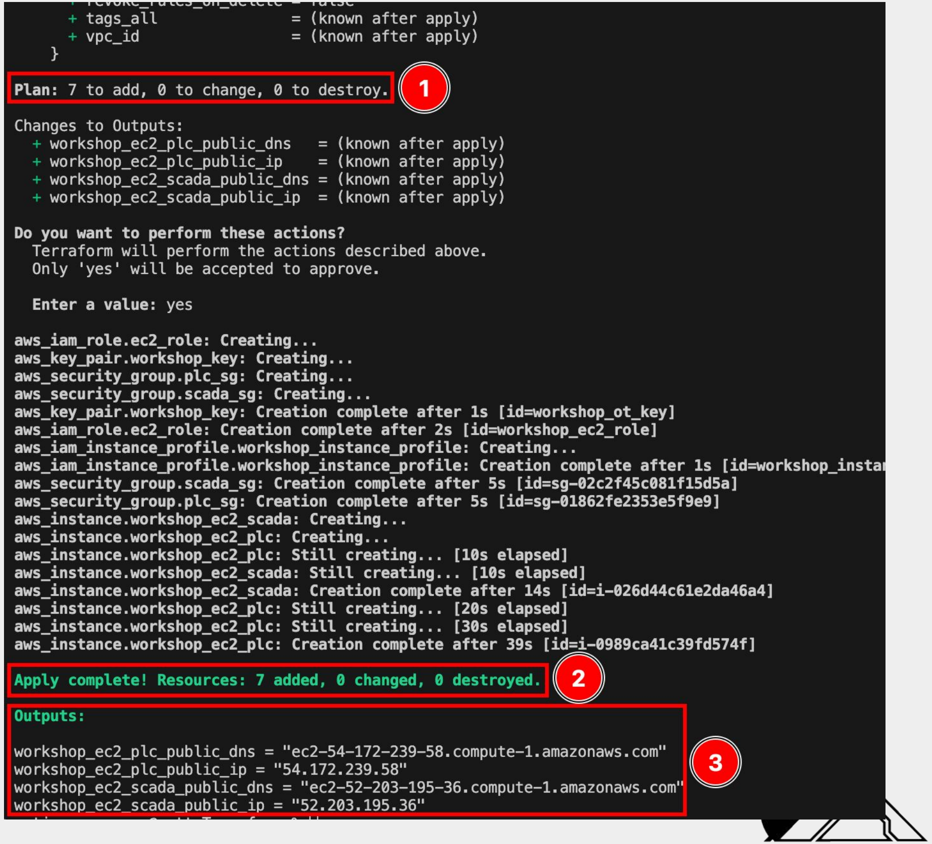


```
                ]
              + description      = ""
              + from_port        = 22
              + ipv6_cidr_blocks = []
              + prefix_list_ids  = []
              + protocol         = "tcp"
              + security_groups  = []
              + self             = false
              + to_port          = 22
            },
          + {
              + cidr_blocks      = [
                  + "190.210.32.117/32",
                  + "54.89.15.84/32",
                ]
              + description      = ""
              + from_port        = 80
              + ipv6_cidr_blocks = []
              + prefix_list_ids  = []
              + protocol         = "tcp"
              + security_groups  = []
              + self             = false
              + to_port          = 80
            },
        ]
      + name                   = "workshop_ot_scada_sg"
      + name_prefix            = (known after apply)
      + owner_id               = (known after apply)
      + revoke_rules_on_delete = false
      + tags_all               = (known after apply)
      + vpc_id                 = (known after apply)
    }

Plan: 7 to add, 0 to change, 0 to destroy.

Changes to Outputs:
  + workshop_ec2_plc_public_dns   = (known after apply)
  + workshop_ec2_plc_public_ip    = (known after apply)
  + workshop_ec2_scada_public_dns = (known after apply)
  + workshop_ec2_scada_public_ip  = (known after apply)
```

Terraform apply



```
[redacted] Terraform % terraform apply

Terraform used the selected providers to generate the following execution plan. Resource ac
following symbols:
  + create

Terraform will perform the following actions:

  # aws_iam_instance_profile.workshop_instance_profile will be created
  + resource "aws_iam_instance_profile" "workshop_instance_profile" {
      + arn         = (known after apply)
      + create_date = (known after apply)
      + id          = (known after apply)
      + name        = "workshop_instance_profile"
      + name_prefix = (known after apply)
      + path        = "/"
      + role        = "workshop_ec2_role"
      + tags_all    = (known after apply)
      + unique_id   = (known after apply)
    }

  # aws_iam_role.ec2_role will be created
  + resource "aws_iam_role" "ec2_role" {
      + arn                   = (known after apply)
      + assume_role_policy    = jsonencode(
            {
              + Statement = [
                  + {
                      + Action    = "sts:AssumeRole"
                      + Effect    = "Allow"
                      + Principal = {
                          + Service = "ec2.amazonaws.com"
                        }
                    },
                ]
              + Version   = "2012-10-17"
            }
        )
      + create_date           = (known after apply)
      + force_detach_policies = false
      + id                    = (known after apply)
      + managed_policy_arns   = (known after apply)
      + max_session_duration  = 3600
      + name                  = "workshop_ec2_role"
```

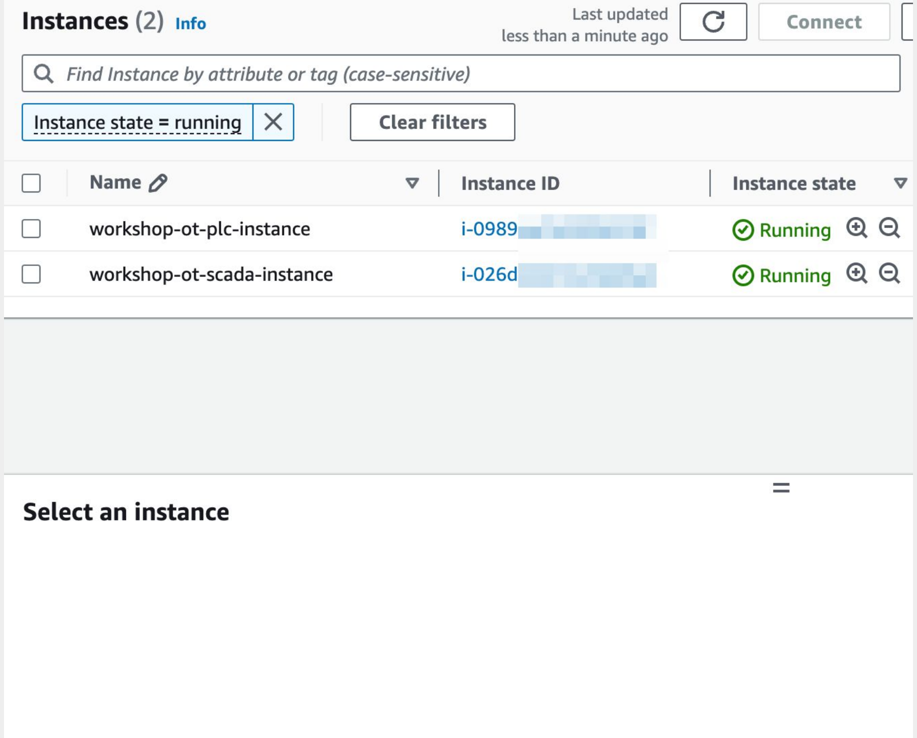


```
      + revoke_rules_on_delete = false
      + tags_all               = (known after apply)
      + vpc_id                 = (known after apply)
    }

Plan: 7 to add, 0 to change, 0 to destroy.

Changes to Outputs:
  + workshop_ec2_plc_public_dns   = (known after apply)
  + workshop_ec2_plc_public_ip    = (known after apply)
  + workshop_ec2_scada_public_dns = (known after apply)
  + workshop_ec2_scada_public_ip  = (known after apply)

Do you want to perform these actions?
  Terraform will perform the actions described above.
  Only 'yes' will be accepted to approve.

  Enter a value: yes

aws_iam_role.ec2_role: Creating...
aws_key_pair.workshop_key: Creating...
aws_security_group.plc_sg: Creating...
aws_security_group.scada_sg: Creating...
aws_key_pair.workshop_key: Creation complete after 1s [id=workshop_ot_key]
aws_iam_role.ec2_role: Creation complete after 2s [id=workshop_ec2_role]
aws_iam_instance_profile.workshop_instance_profile: Creating...
aws_iam_instance_profile.workshop_instance_profile: Creation complete after 1s [id=workshop_instar
aws_security_group.scada_sg: Creation complete after 5s [id=sg-02c2f45c081f15d5a]
aws_security_group.plc_sg: Creation complete after 5s [id=sg-01862fe2353e5f9e9]
aws_instance.workshop_ec2_scada: Creating...
aws_instance.workshop_ec2_plc: Creating...
aws_instance.workshop_ec2_plc: Still creating... [10s elapsed]
aws_instance.workshop_ec2_scada: Still creating... [10s elapsed]
aws_instance.workshop_ec2_scada: Creation complete after 14s [id=i-026d44c61e2da46a4]
aws_instance.workshop_ec2_plc: Still creating... [20s elapsed]
aws_instance.workshop_ec2_plc: Still creating... [30s elapsed]
aws_instance.workshop_ec2_plc: Creation complete after 39s [id=i-0989ca41c39fd574f]

Apply complete! Resources: 7 added, 0 changed, 0 destroyed.

Outputs:

workshop_ec2_plc_public_dns = "ec2-54-172-239-58.compute-1.amazonaws.com"
workshop_ec2_plc_public_ip = "54.172.239.58"
workshop_ec2_scada_public_dns = "ec2-52-203-195-36.compute-1.amazonaws.com"
workshop_ec2_scada_public_ip = "52.203.195.36"
```

Infraestructura

AWS

Validación AWS

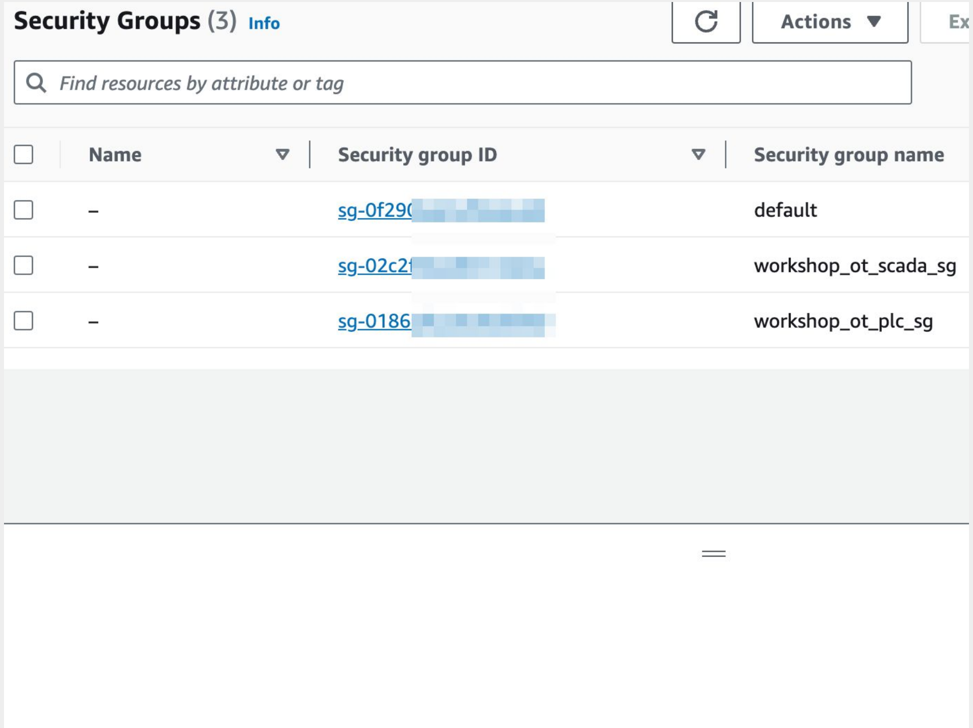


Info
Last updated less than a minute ago
Connect
Find Instance by attribute or tag (case-sensitive)
Instance state = running
Clear filters

Instances (2)

□	Name	Instance ID	Instance state
□	workshop-ot-plc-instance	i-0989[redacted]	✓ Running
□	workshop-ot-scada-instance	i-026d[redacted]	✓ Running

Select an instance



Security Groups (3)

□	Name	Security group ID	Security group name
□	–	sg-0f29[redacted]	default
□	–	sg-02c2[redacted]	workshop_ot_scada_sg
□	–	sg-0186[redacted]	workshop_ot_plc_sg

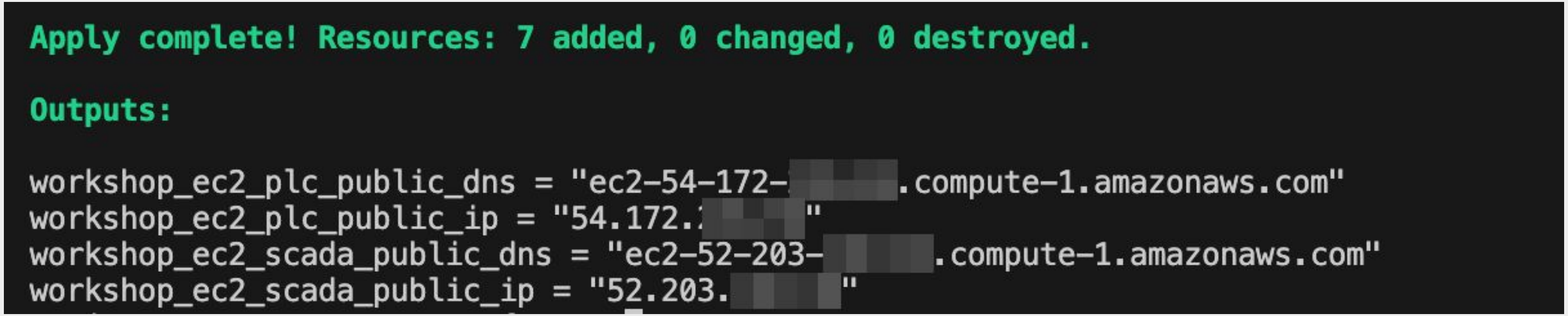
Conexión EC2

Conexión SCADA

```
- ssh -i ~/.ssh/id_rsa ec2-user@<IP-SCADA>
```

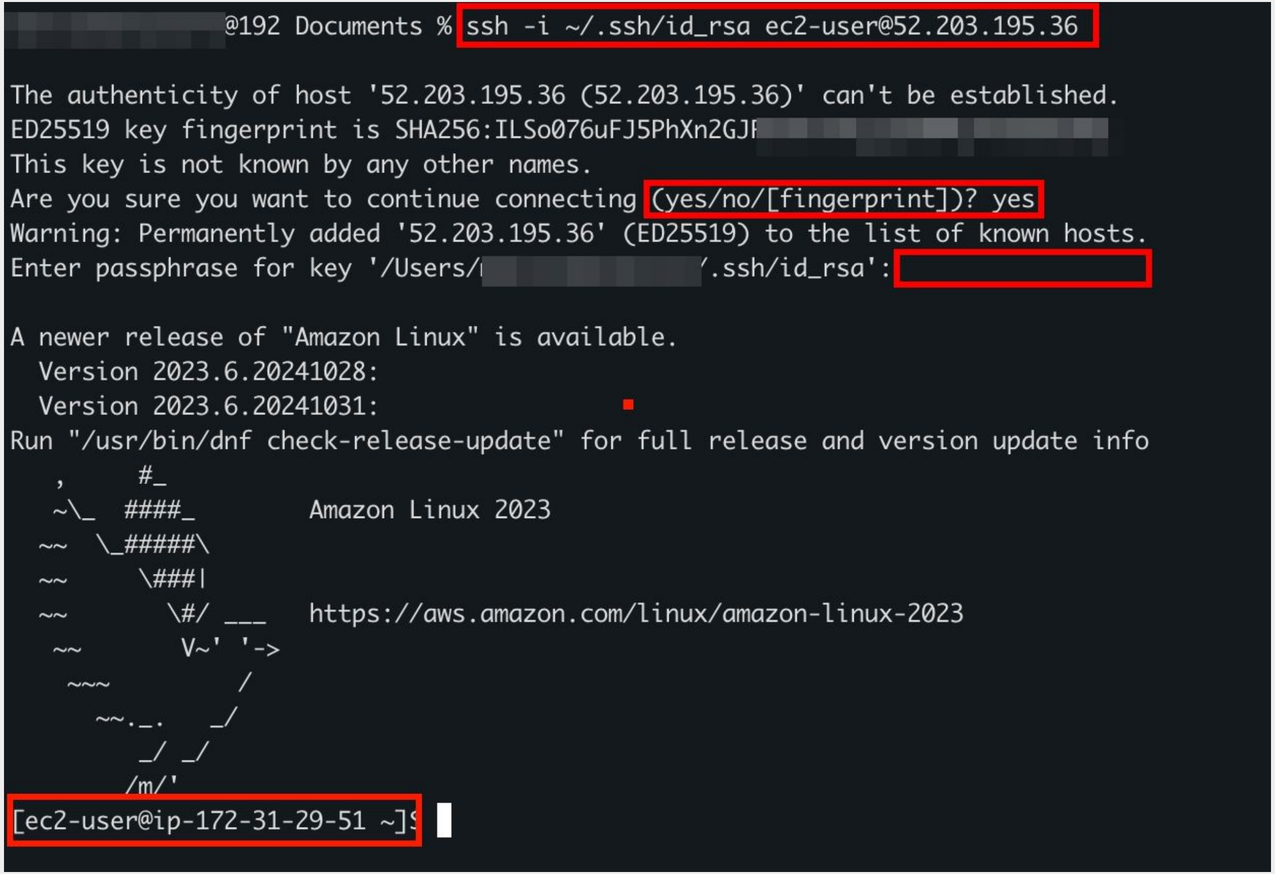
Conexión PLC

```
- ssh -i ~/.ssh/id_rsa ec2-user@<IP-PLC>
```



```
Apply complete! Resources: 7 added, 0 changed, 0 destroyed.

Outputs:

workshop_ec2_plc_public_dns = "ec2-54-172-[redacted].compute-1.amazonaws.com"
workshop_ec2_plc_public_ip = "54.172.[redacted]"
workshop_ec2_scada_public_dns = "ec2-52-203-[redacted].compute-1.amazonaws.com"
workshop_ec2_scada_public_ip = "52.203.[redacted]"
```

Conexión EC2



```
[redacted]@192 Documents % ssh -i ~/.ssh/id_rsa ec2-user@52.203.195.36

The authenticity of host '52.203.195.36 (52.203.195.36)' can't be established.
ED25519 key fingerprint is SHA256:ILSo076uFJ5PhXn2GJ[redacted]
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '52.203.195.36' (ED25519) to the list of known hosts.
Enter passphrase for key '/Users/[redacted]/.ssh/id_rsa':

A newer release of "Amazon Linux" is available.
  Version 2023.6.20241028:
  Version 2023.6.20241031:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-172-31-29-51 ~]$
```

Infraestructura

Repositorios

solidaritylabs.io/

SECUREOT
CYBERSECURITY VILLAGE

EKOPARTY
20

Repositorio Workshop OT

Repositorio Dredge

solidaritylabs.io/

Configuración SCADA

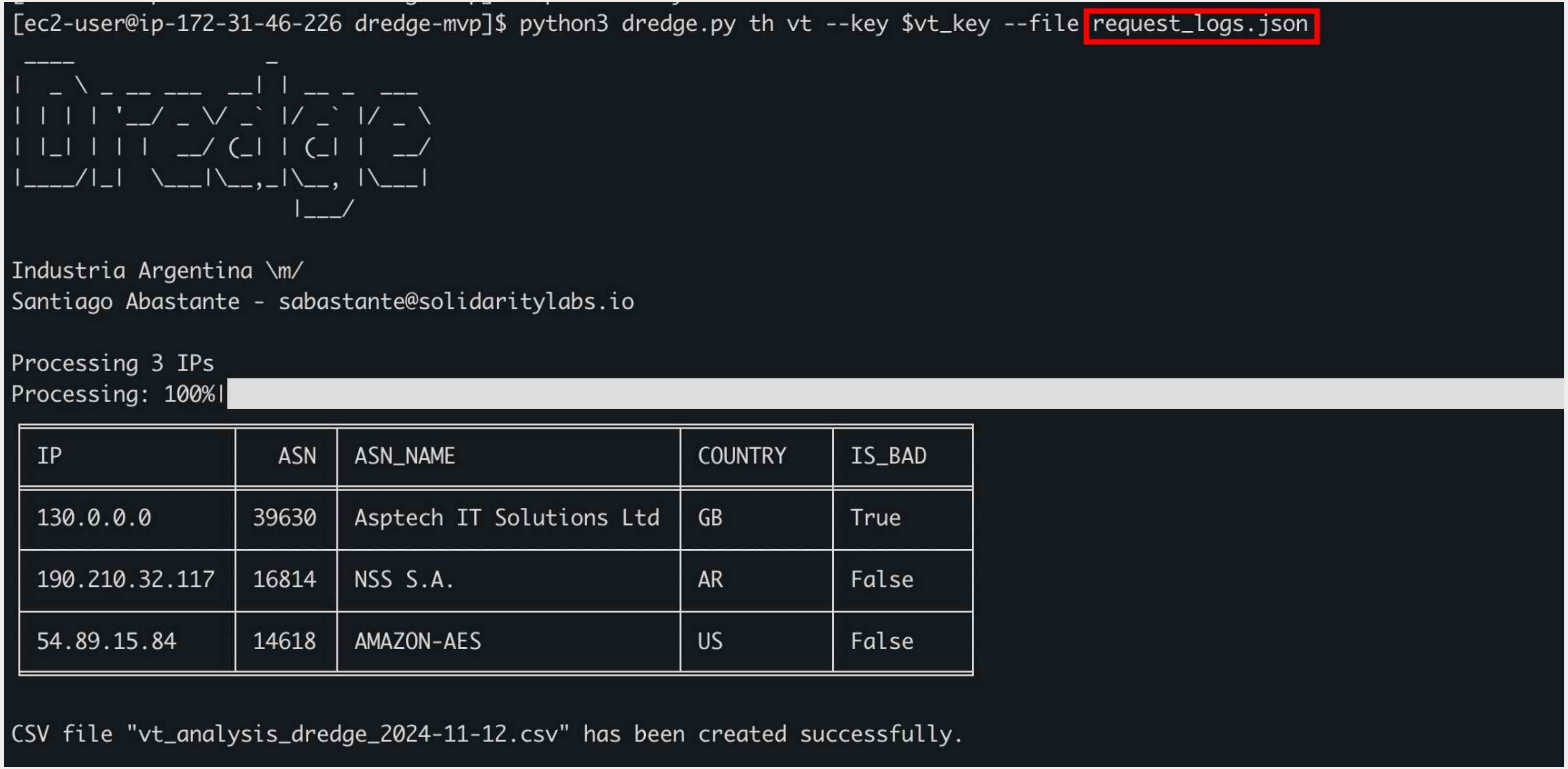
Configuración SCADA

Pasos para configuración del SCADA

1. Configurar SCADA para obtener datos del PLC
2. Configurar Security Group
3. Validar acceso Web al SCADA
4. Habilitar el Security Group para exponer el SCADA

Dredge

Dredge

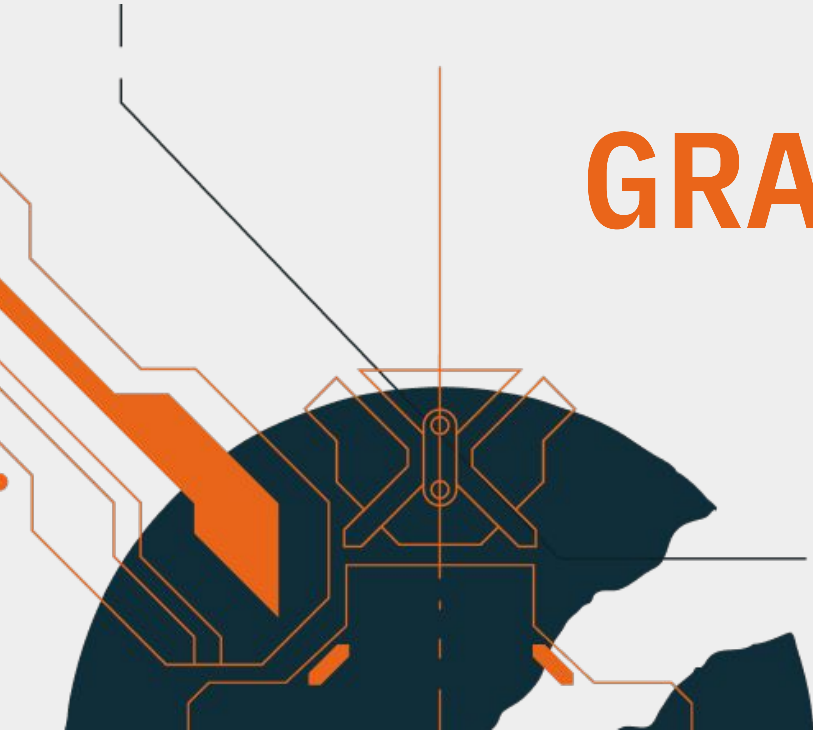


```
[ec2-user@ip-172-31-46-226 dredge-mvp]$ python3 dredge.py th vt --key $vt_key --file request_logs.json
 ____              _            
|  _ \ _ __ ___  __| | __ _  ___ 
| | | | '__/ _ \/ _` |/ _` |/ _ \
| |_| | | |  __/ (_| | (_| |  __/
|____/|_|  \___|\__,_|\__, |\___|
                      |___/      

Industria Argentina \m/
Santiago Abastante - sabastante@solidaritylabs.io

Processing 3 IPs
Processing: 100%|
╒═══════════════╤═══════╤═══════════════════════════╤═══════════╤══════════╕
│ IP            │   ASN │ ASN_NAME                  │ COUNTRY   │ IS_BAD   │
╞═══════════════╪═══════╪═══════════════════════════╪═══════════╪══════════╡
│ 130.0.0.0     │ 39630 │ Asptech IT Solutions Ltd  │ GB        │ True     │
├───────────────┼───────┼───────────────────────────┼───────────┼──────────┤
│ 190.210.32.117│ 16814 │ NSS S.A.                  │ AR        │ False    │
├───────────────┼───────┼───────────────────────────┼───────────┼──────────┤
│ 54.89.15.84   │ 14618 │ AMAZON-AES                │ US        │ False    │
╘═══════════════╧═══════╧═══════════════════════════╧═══════════╧══════════╛

CSV file "vt_analysis_dredge_2024-11-12.csv" has been created successfully.
```

Q&A

SECUREOT
CYBERSECURITY VILLAGE

EKOPARTY
20



GRACIAS

solidaritylabs.io/

/matiasmanassero