

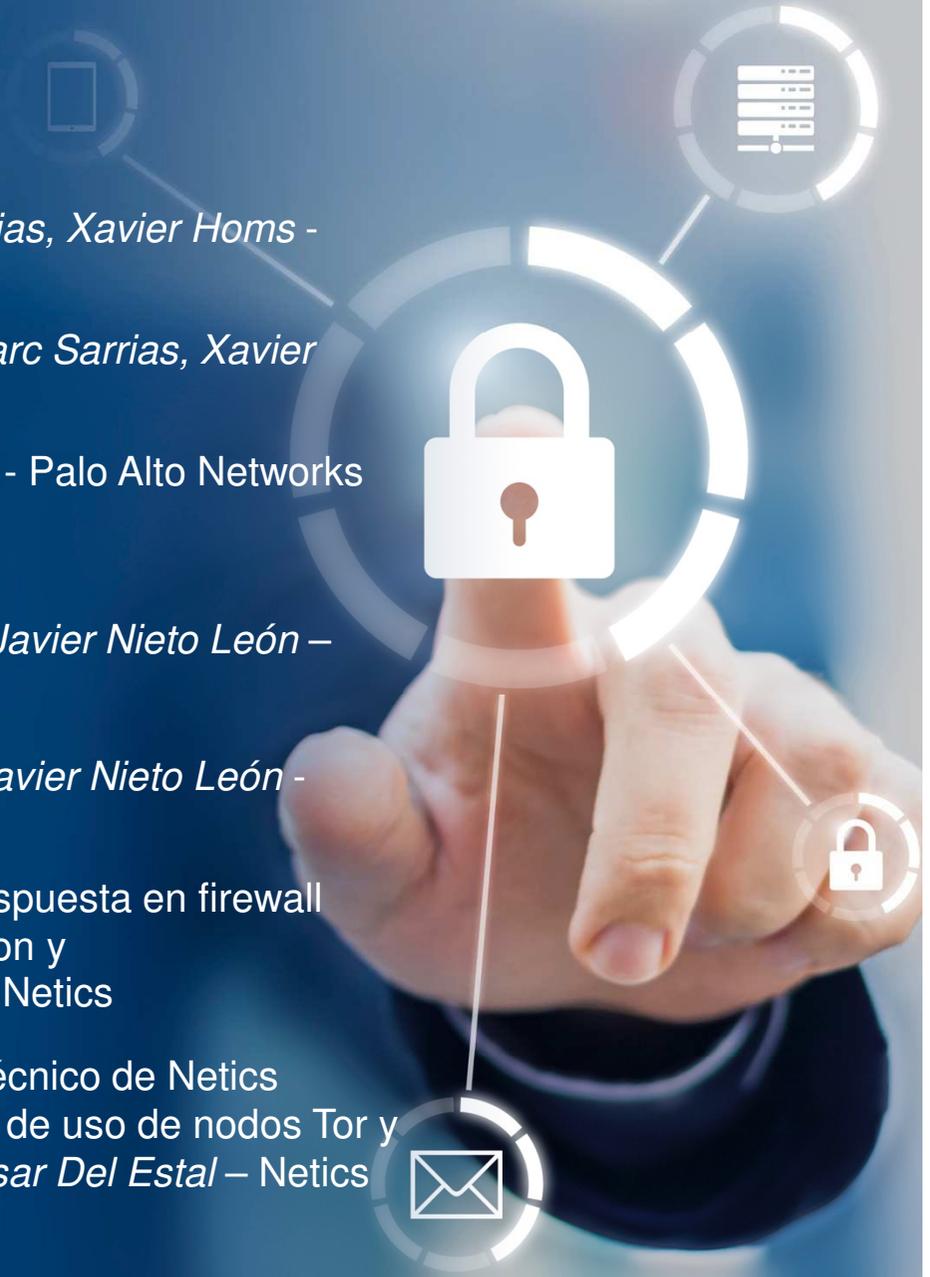
SEGURIDAD Y MONITORIZACIÓN DE RED CON NGFW Y NBA



Cèsar Del Estal Vendrell

AGENDA

- 09:45** Palo Alto NGFW (Panos 8) - *Marc Sarrias, Xavier Homs* - Palo Alto Networks
- 10:15** Protección del Endpoint con Traps - *Marc Sarrias, Xavier Homs* - Palo Alto Networks
- 10:45** Minemeld - *Marc Sarrias, Xavier Homs* - Palo Alto Networks
- 11:00** Descanso / Café
- 11:15** Presentación Flowmon ADS y DDOS- *Javier Nieto León* – Flowmon Networks
- 11:45** Módulos , NPM y APM de Flowmon - *Javier Nieto León* - Flowmon Networks
- 12:15** Demostración de automatización de respuesta en firewall Palo Alto a partir de eventos en Flowmon y microsegmentación - *Cesar Del Estal* - Netics
- 12:45** Servicios de valor añadido al soporte técnico de Netics (MMAAS -Minemeld as a service, caso de uso de nodos Tor y lista de servidores de Office 365) - *Cesar Del Estal* – Netics
- 13:00** Dudas y preguntas



```
if ($?) {  
    Write-Output "Operation successful"  
} else {  
    Write-Error "Operation failed"  
}
```

VISIBILIDAD TOTAL



SEGURIDAD

AUTOMATIZACIÓN



Situación ?

```
graph LR; A[Situación ?] --- B[Incremento del tráfico SSL, APT's..]; A --- C[Infección y rápida propagación interna a las vlans.. (movimiento lateral del Ransomware)]; A --- D[SDN y micro segmentación en redes corporativas compleja y cara];
```

Incremento del tráfico SSL, APT's..

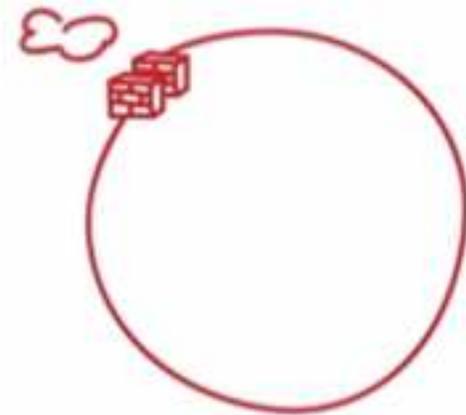
Infección y rápida propagación interna a las vlans.. (movimiento lateral del Ransomware)

SDN y micro segmentación en redes corporativas compleja y cara

```
if not isinstance(wirec_obj, MirrorObj):
    mirror_mod.wirec_object = mirror_obj

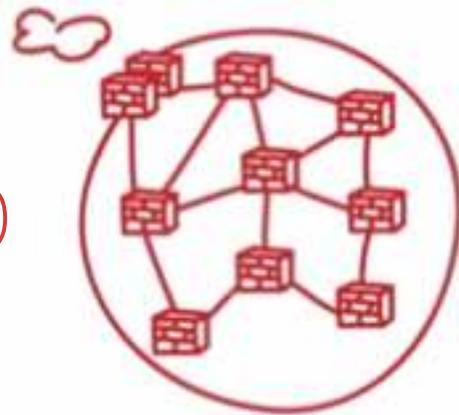
if operation == "Mirror X":
    mirror_mod.use_x = True
    mirror_mod.use_y = False
    mirror_mod.use_z = False
elif operation == "Mirror Y":
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif operation == "Mirror Z":
    mirror_mod.use_x = False
```

¿identifica tu tipo de red?



RED TIPO A

ó



RED TIPO B

?

```
def __init__(self, name, mirror_x):
    self.label = "Mirror X"

def __init__(self, context):
    self.wirec_context, active_object is not None
```

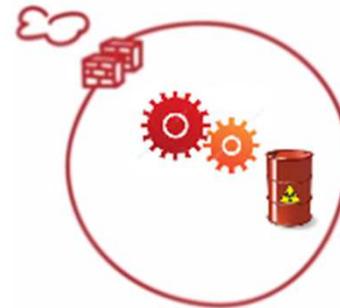
```
if self.active_object is None:
    mirror_mod.mirror_object = mirror_obj

if operation == "Mirror X":
    mirror_mod.use_x = True
    mirror_mod.use_y = False
    mirror_mod.use_z = False
else:
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True
```

¿Cómo abordamos una solución de protección completa en el segmento empresarial medio?



RED TIPO A



RED AUTOMATIZADA

```
self.mirror = self.mirror_obj
self.label = "Mirror X"

self.inspect()
def insi(self, context):
    if context.active_object is not None:
```

Opciones ?

```
graph LR; A[Opciones ?] --- B(( )); A --- C(( )); A --- D(( )); B --- B1[¿En la red local qué? «Access lists» del año 1995 (L4 OSI)?]; C --- C1[Vmware NSX, Cisco ACI-EM (DNA-C)= $]; D --- D1[NGFW+ ADS + Automatización];
```

¿En la red local qué? «Access lists» del año 1995 (L4 OSI)?

Vmware NSX, Cisco ACI-EM (DNA-C)= \$

NGFW+ ADS + Automatización

Palo Alto

```
graph LR; A[Palo Alto] --- B(Protección de perímetro y "endpoint"); A --- C(Integración, visibilidad y control del SaaS); A --- D(Inteligencia operacional aka= Threat int);
```

Protección de perímetro y “endpoint”

Integración, visibilidad y control del SaaS

Inteligencia operacional (aka= Threat int)

Flowmon

```
graph LR; A[Flowmon] --- B[Visibilidad externa e interna de la red (interna a la vlan)]; A --- C[Modelo "offline", no añade retardo de proceso al tráfico de producción]; A --- D[Permite detectar Anomalías];
```

Visibilidad externa e interna de la red (interna a la vlan)

Modelo "offline", no añade retardo de proceso al tráfico de producción

Permite detectar Anomalías

Netics

Integración de herramientas de Palo Alto y Flowmon con electrónica de red Cisco, HP, Juniper, etc...

Integra NGFW Palo Alto y Traps

Integra Flowmon

Protege mediante automatización e interacción con red local (Python)

CASO DE USO

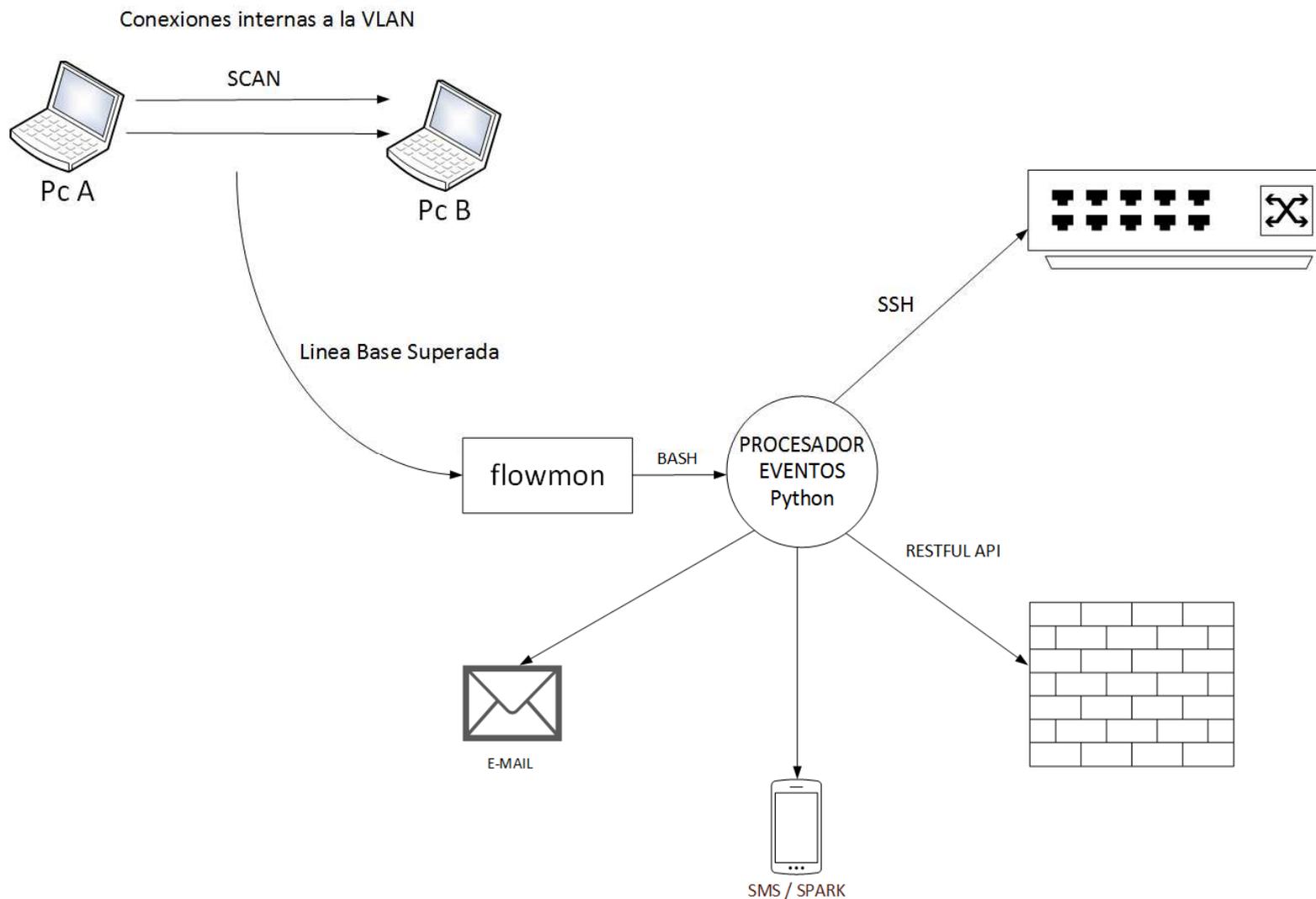
Automatización con micro segmentación de red local



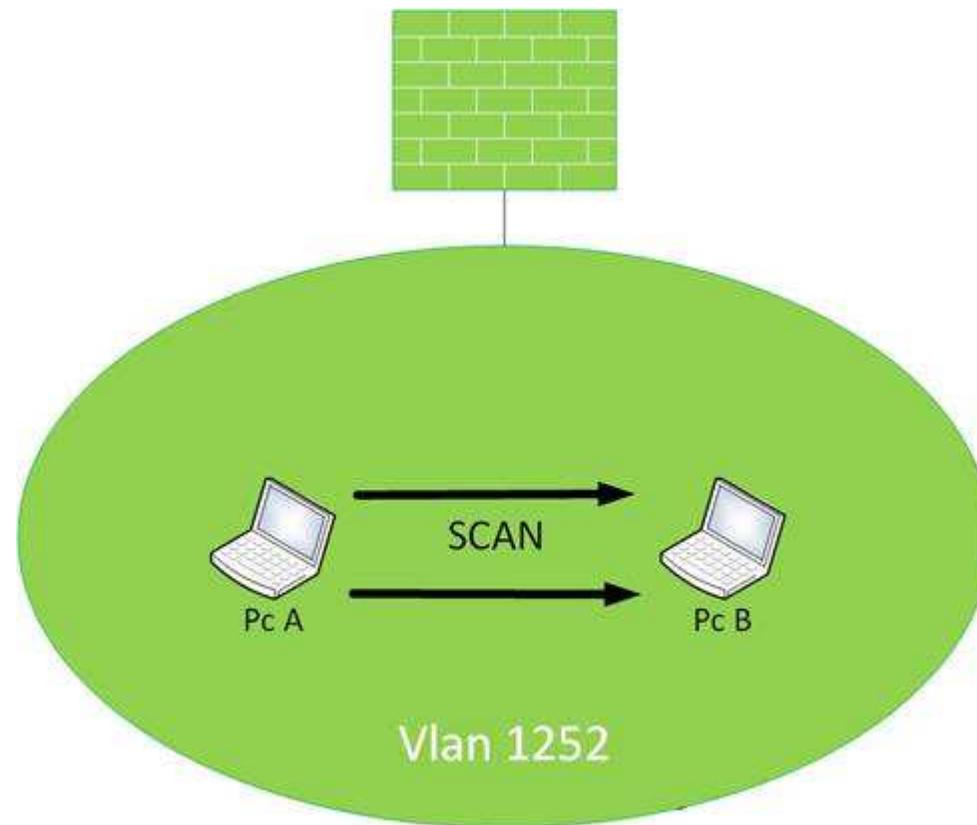
Lógica de detección automatizada



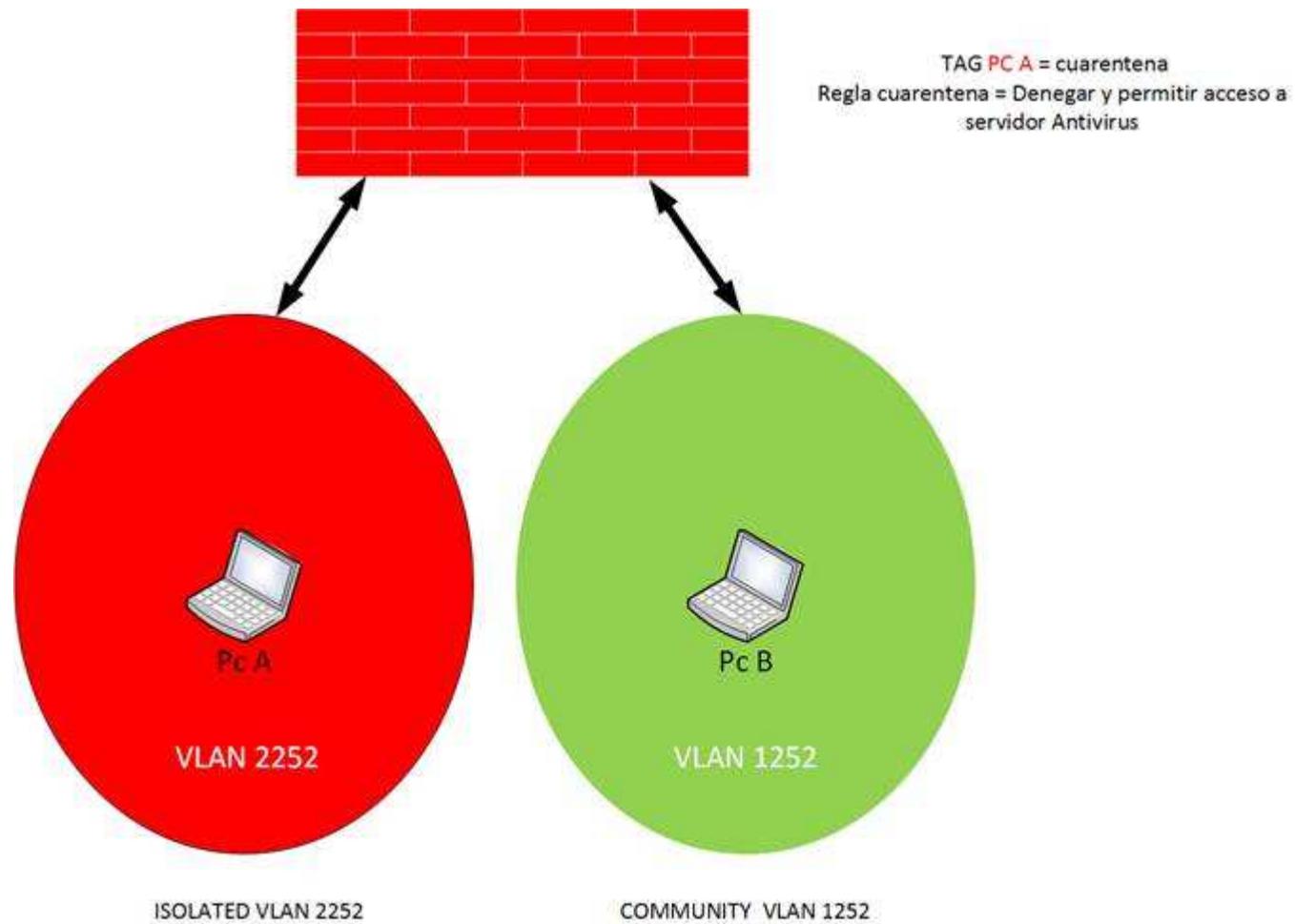
Diagrama del caso de uso de Micro segmentación física y objetos dinámicos



Generación y detección de tráfico anómalo en la vlan 1252 entre dos máquinas



Aislamiento por microsegmentación mediante vlans privadas



<https://tools.ietf.org/html/rfc5517>

Minemeld

```
graph LR; Minemeld --- A[Agrega fuentes de información]; Minemeld --- B[Caso 1: Office 365]; Minemeld --- C[Caso 2: Nodos salida red Tor];
```

Agrega fuentes de información

Caso 1: Office 365

Caso 2: Nodos salida red Tor

The background of the slide is an abstract composition of overlapping, semi-transparent blue geometric shapes, primarily squares and rectangles, in various shades of blue. These shapes are arranged in a way that creates a sense of depth and movement, with some appearing more prominent than others. The overall effect is a modern, clean, and professional aesthetic.

Gracias