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

VISIBILIDAD TOTAL

SEGURIDAD

AUTOMATIZACIÓN

Situación ?

- 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

¿identifica tu tipo de red?

ó

?

RED TIPO A

RED TIPO B

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

RED TIPO A

RED AUTOMATIZADA

Opciones ?

- ¿En la red local qué? «Access lists» del año 1995 (L4 OSI)?
- Vmware NSX, Cisco ACI-EM (DNA-C)= $
- NGFW+ ADS + Automatización


Palo Alto
Protección de perímetro y “endpoint”
Integración, visibilidad y control del SaaS
Inteligencia operacional (aka= Threat int)

Flowmon

- 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)

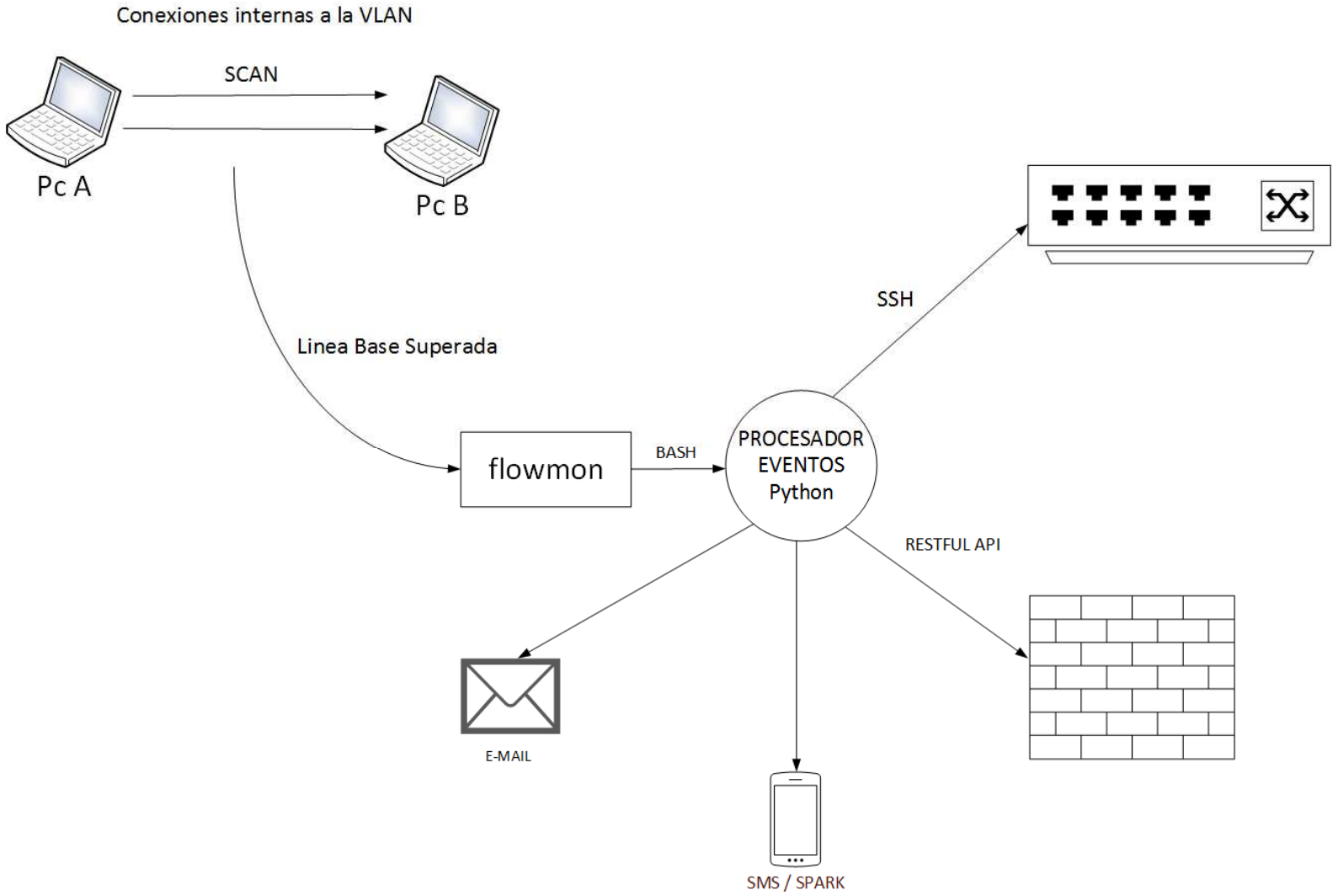
CASO DE USO

Automatización con micro segmentación de red local

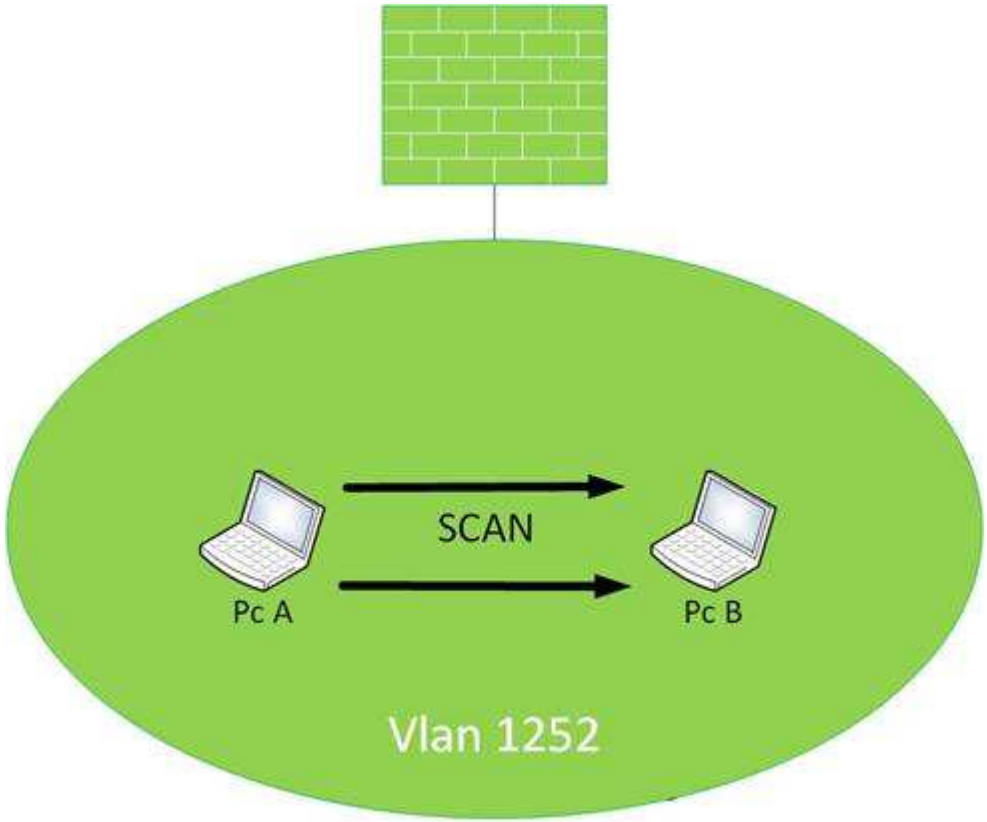
NETICS networks & services 10 AÑOS

Lógica de detección automatizada

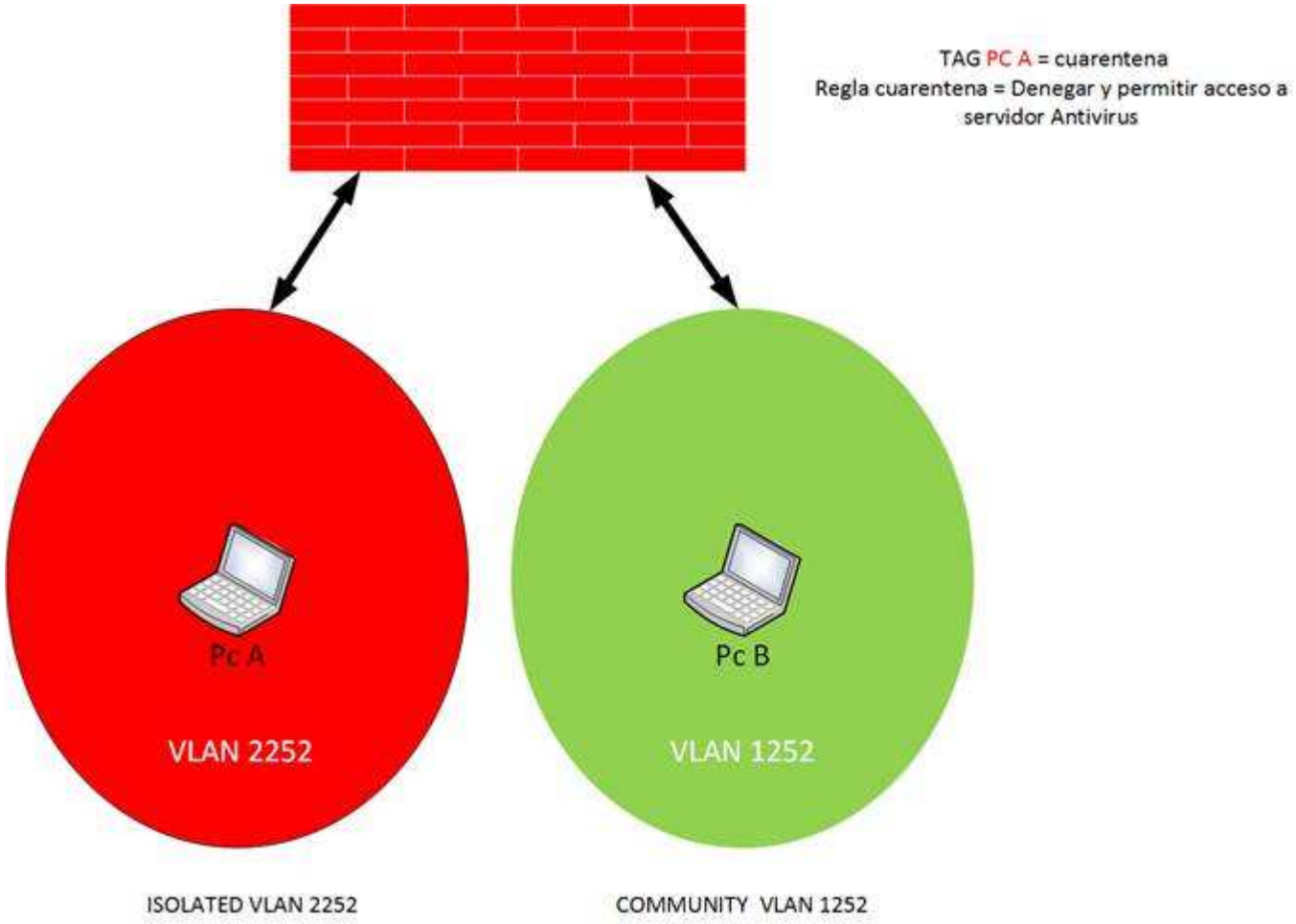
Diagrama del
Diagrama del caso de uso de Micro segmentación física y objetos dinámicos



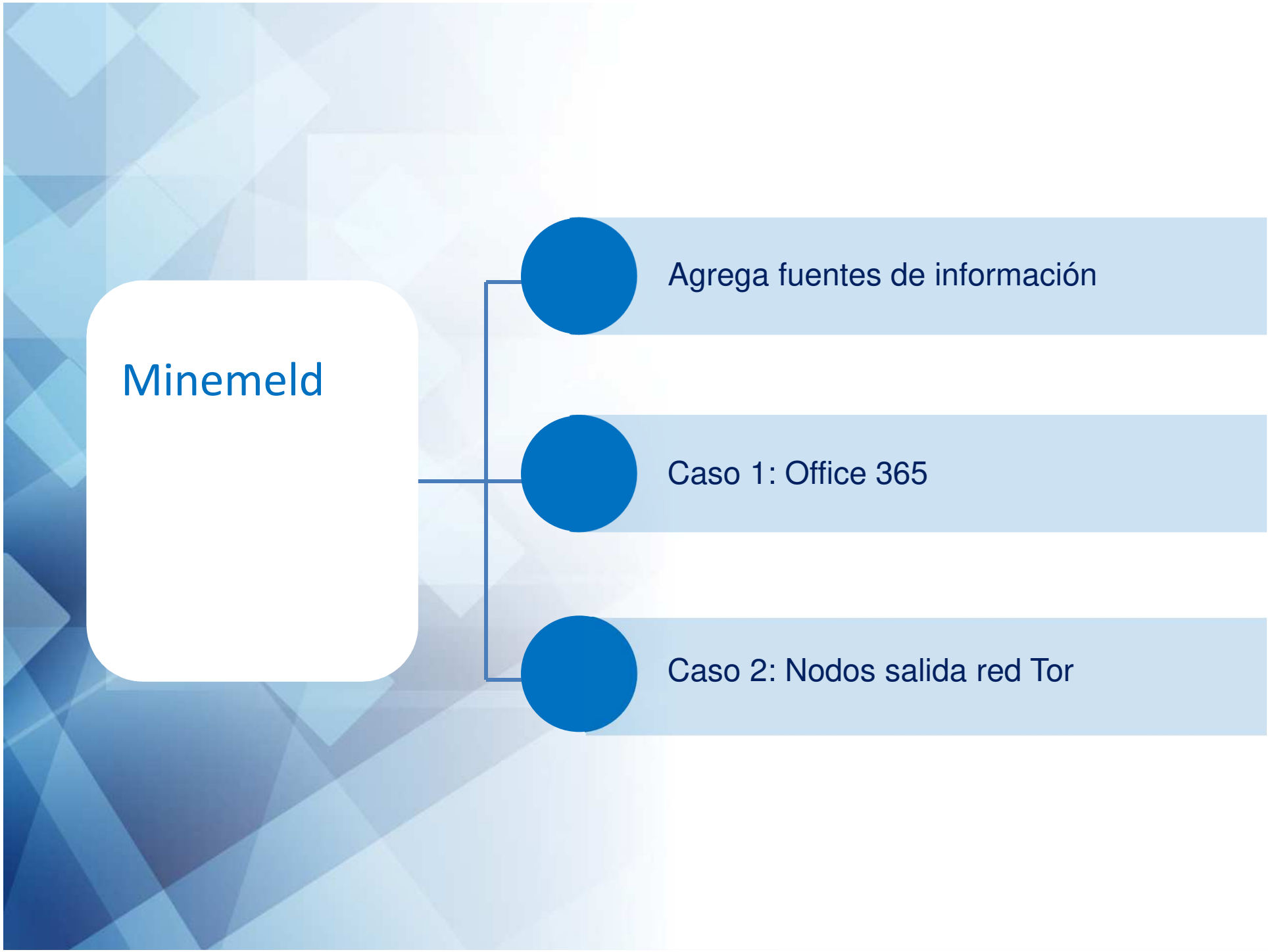
Generación y detección de tráfico anómalo en la vlan 1252 entre dos máquinas



Aislamiento por microsegmentación mediante vlans privadas



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


Minemeld
Agrega fuentes de información
Caso 1: Office 365
Caso 2: Nodos salida red Tor


Gracias