NSM
Network Security Monitoring
(IDS – IPS – SIEM) y otras cosas...

Lucas González
lucasg@neuquen.gov.ar

MINISTERIO DE ENERGÍA
Y RECURSOS NATURALES
COORDINACIÓN TÉCNICA
ADMINISTRATIVA

JUNTOS
PODEMOS
MÁS

DÉFICIT DE ATENCIÓN POWER POINT

DEFAPP

Slides del expositor

Nomenclatura (Estados del oyente)

- TIENES TODA MI ATENCIÓN
- CREO QUE SIGUES TENIENDO MI ATENCIÓN
- OK, VOY A VER MI SMARTPHONE
- ¿QUÉ TENGO QUE HACER DESPUÉS DE ESTO?
- MIRA, EL TIPO SIGUE HABLANDO
- QUE ACABE YA, POR DIOS
- HIBERNACIÓN HUMANA

- – – – – CANTIDAD IDEAL DE SLIDES
- ——— CANTIDAD MÁXIMA DE SLIDES PARA LA CONSERVACIÓN DE LA ATENCIÓN AJENA.

CINISMOILUSTRADO.COM

MINISTERIO DE ENERGÍA Y RECURSOS NATURALES
COORDINACIÓN TÉCNICA ADMINISTRATIVA

JUNTOS PODEMOS MÁS

Territorio Comanche

"Para un reportero en una guerra, territorio comanche es el lugar donde el instinto dice que pares el coche y des media vuelta; donde siempre parece a punto de anochecer y caminas pegado a las paredes, hacia los tiros que suenan a lo lejos, mientras escuchas el ruido de tus pasos sobre los cristales rotos. El suelo de las guerras está siempre cubierto de cristales rotos. Territorio comanche es allí donde los oyes crujir bajo tus botas, y aunque no ves a nadie sabes que te están mirando."

Arturo Pérez Reverté...

Asumir:

Los Atacantes no juegan limpio.

Los Atacantes conocen mejor tu Sistema que Vos.

Los Atacantes ya se encuentran dentro de tu Sistema.

Los atacantes siempre encuentran la forma de entrar y comprometer el objetivo.

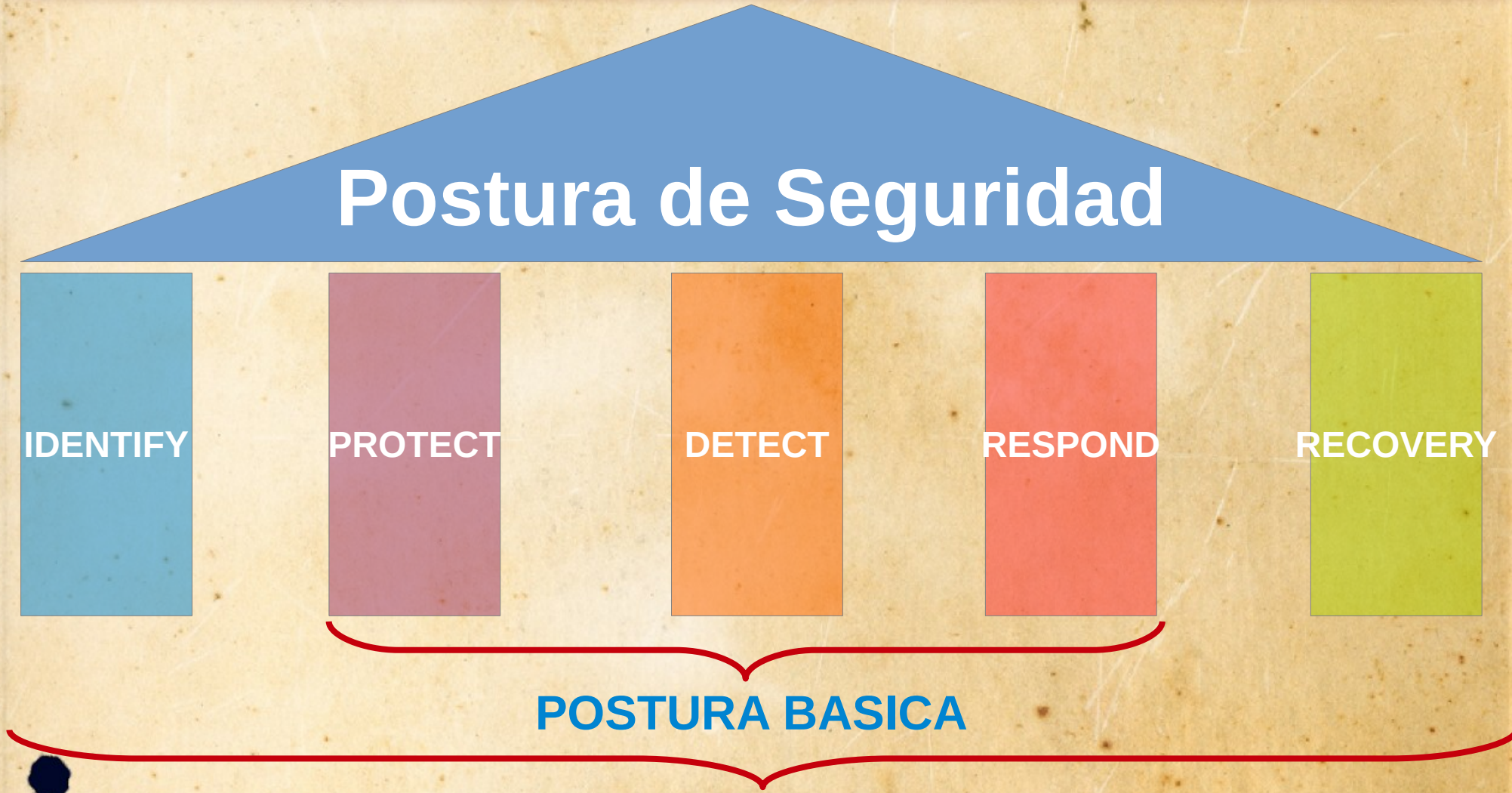
Nuestra Empresa siempre va a estar comprometida ó bajo amenaza

Los que Defienden deben tener en cuenta muchos factores. Los Atacantes necesitan solo uno.

La Seguridad es un proceso y no una operación táctica.

La Seguridad se degrada con el Tiempo.

Posturas de Seguridad

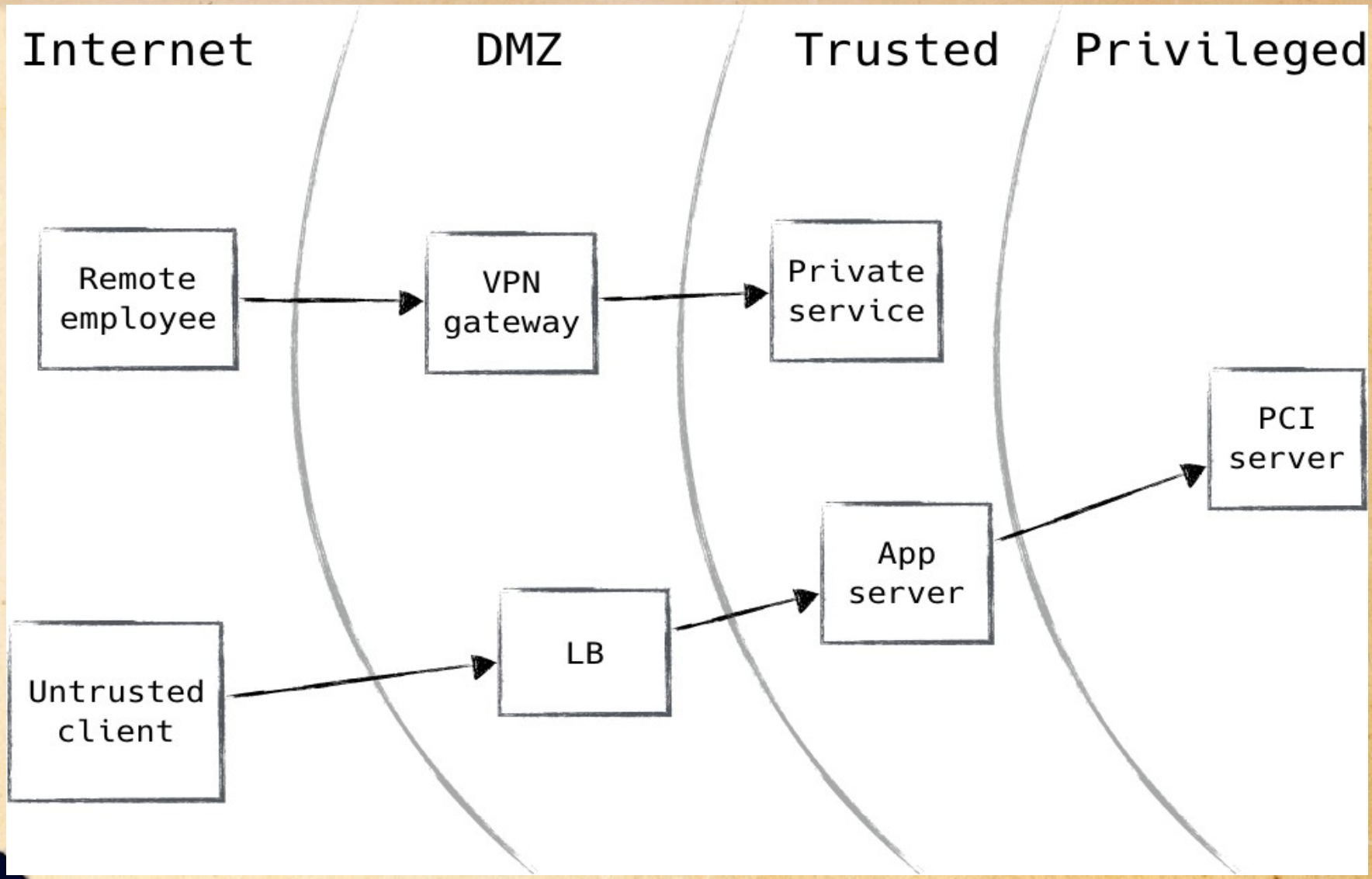


MINISTERIO DE ENERGÍA Y RECURSOS NATURALES
COORDINACIÓN TÉCNICA ADMINISTRATIVA

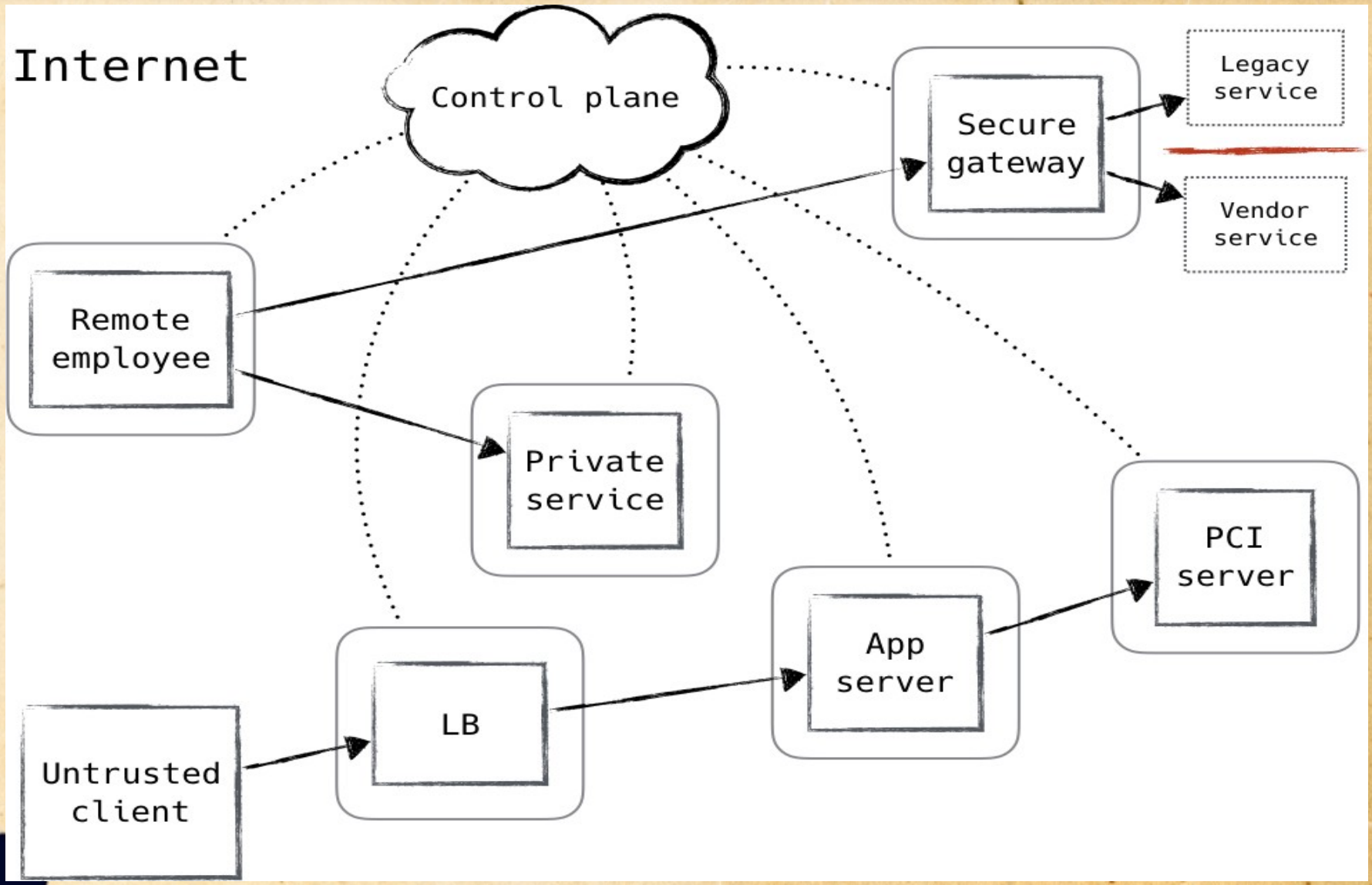
JUNTOS PODEMOS MÁS

Postura: Zero Trust

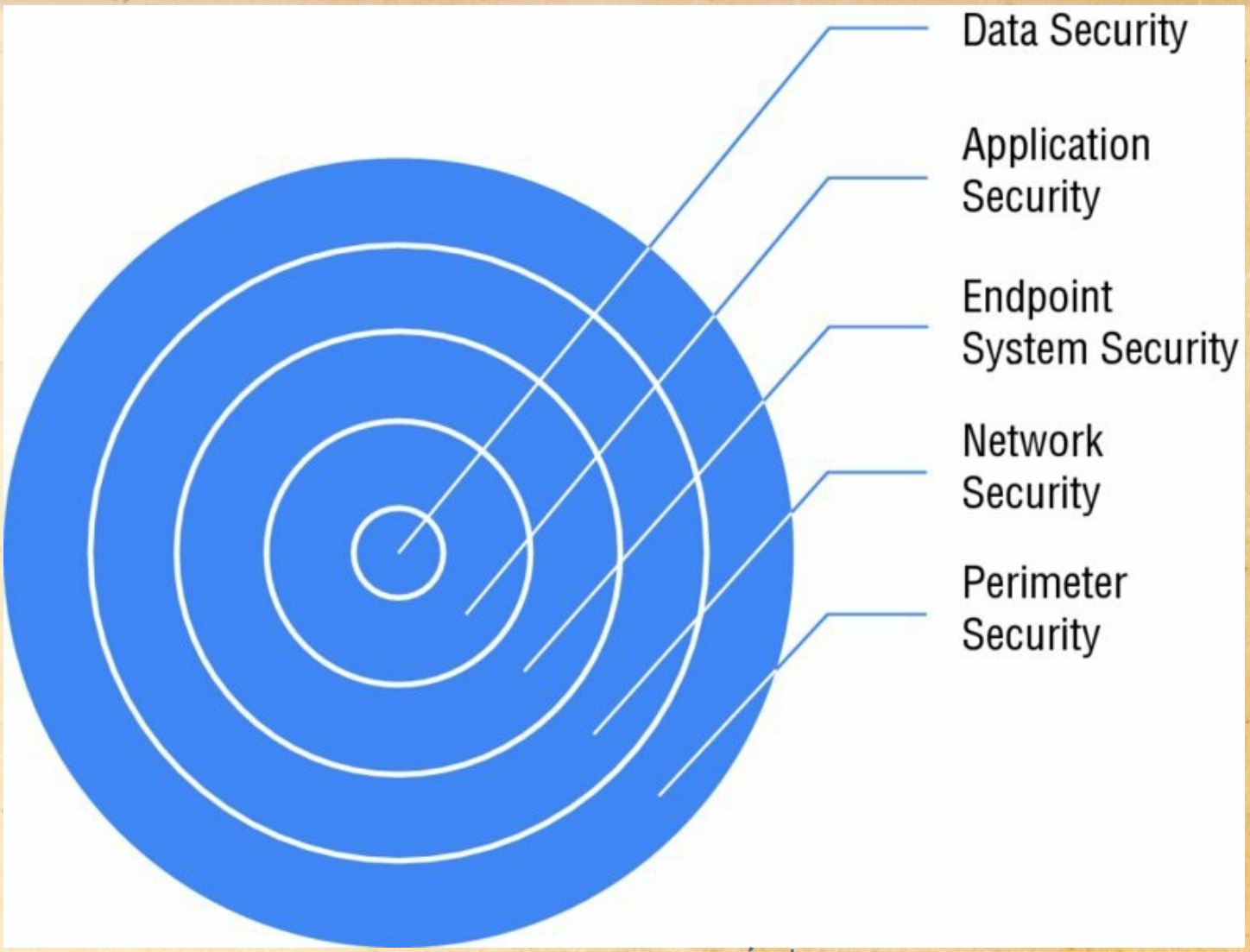
Postura:Zero Trust



Postura: Zero Trust



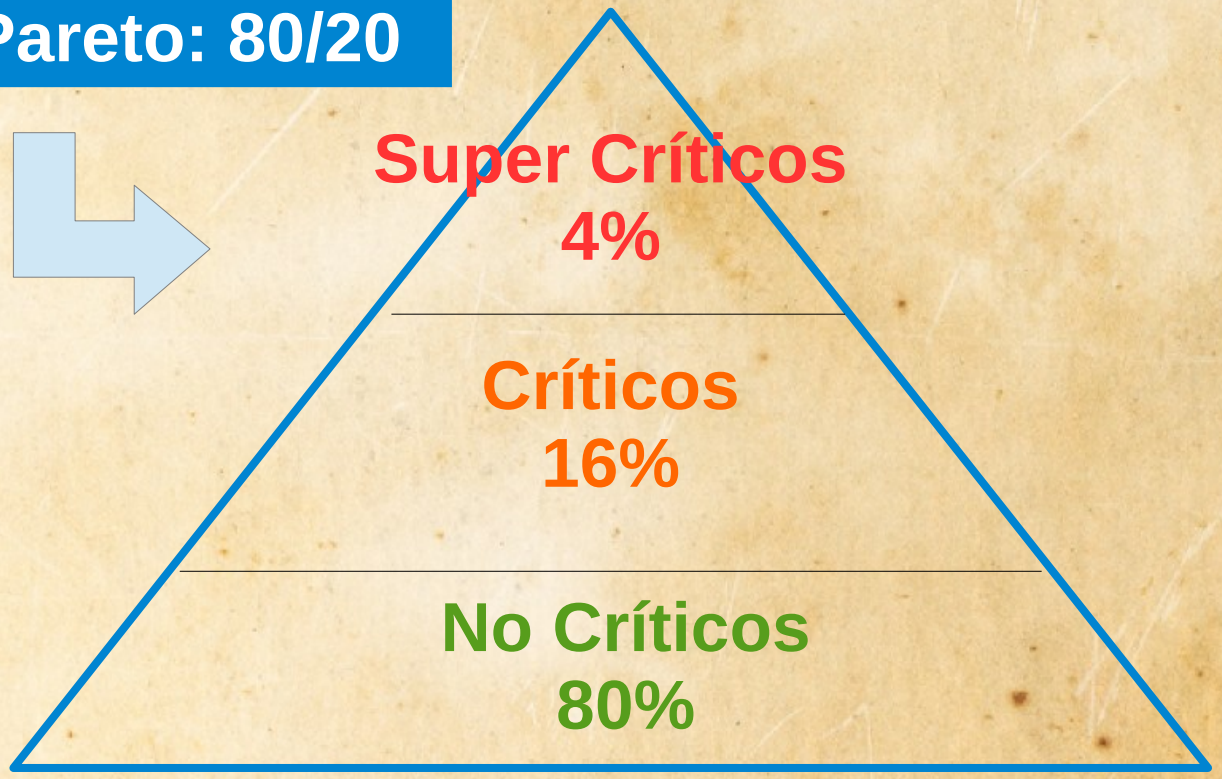
Postura: Defensa en Profundiad - Defense in Depth



Postura: Datos Críticos

Priorizar los Datos ó el atacante lo hará por vos

Ley de Pareto: 80/20



Postura: Zonas Sacrificables

Servidor Web

Servidor de Dominio

Postura: Seguridad Ofensiva

(Bombita Zip para Script Kiddies Incautos)

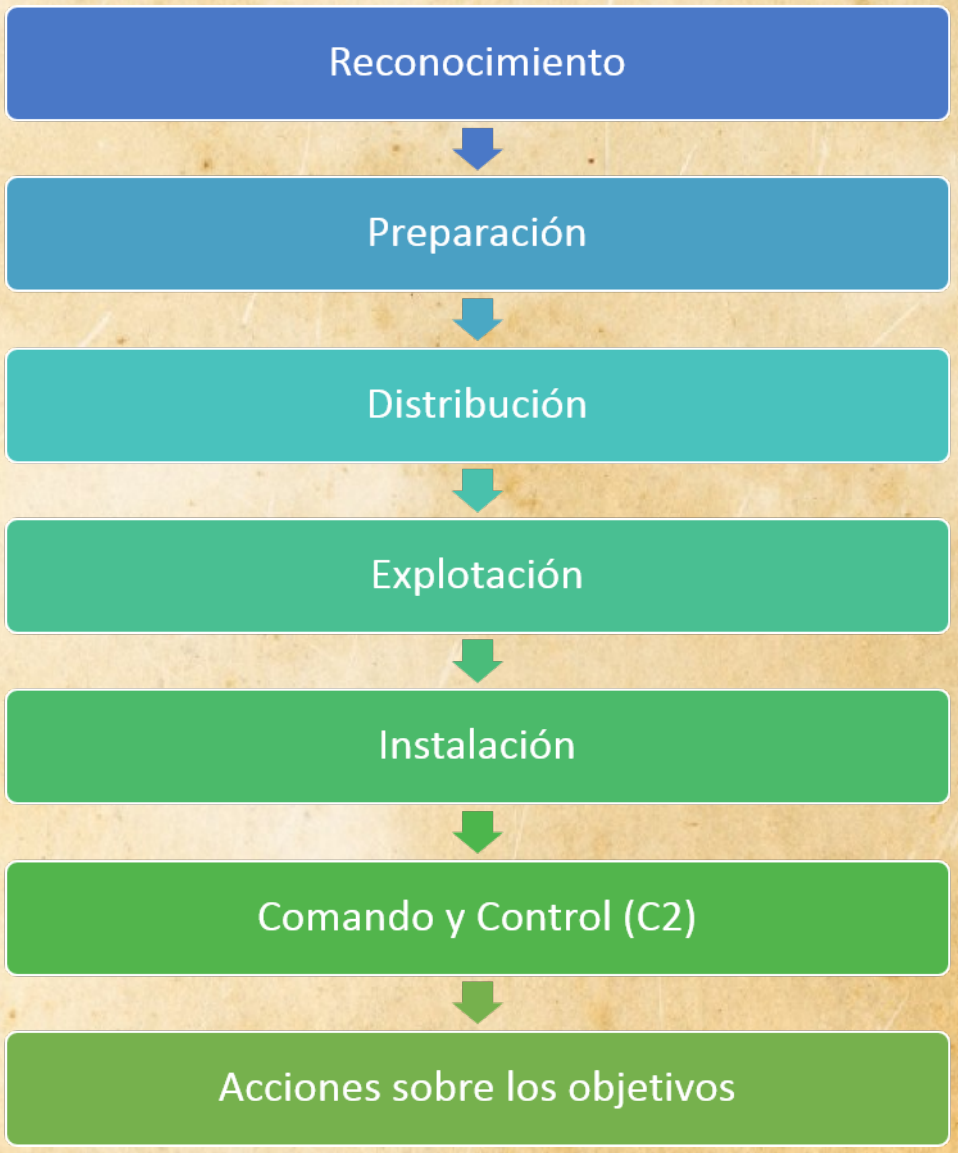
```
<?php
$agent = lower($_SERVER['HTTP_USER_AGENT']);

//check for nikto, sql map or "bad" subfolders which only exist on wordpress
if (strpos($agent, 'nikto') !== false || strpos($agent, 'sqlmap') !== false || startswith($url,'wp-')
|| startswith($url,'wordpress') || startswith($url,'wp/'))
{
    sendBomb();
    exit();
}

function sendBomb(){
      //prepare the client to recieve GZIP data. This will not be suspicious
      //since most web servers use GZIP by default
      header("Content-Encoding: gzip");
      header("Content-Length: ".filesize('10G.gzip'));
      //Turn off output buffering
      if (ob_get_level()) ob_end_clean();
      //send the gzipped file to the client
      readfile('10G.gzip');
}

function startsWith($haystack,$needle){
   return (substr($haystack,0,strlen($needle)) === $needle);
}
```

Cyber Kill Chain



NSM (Network Security Monitoring)

Los Atacantes ya se encuentran dentro de tu Sistema.

Los atacantes siempre encuentran la forma de entrar y comprometer el objetivo.

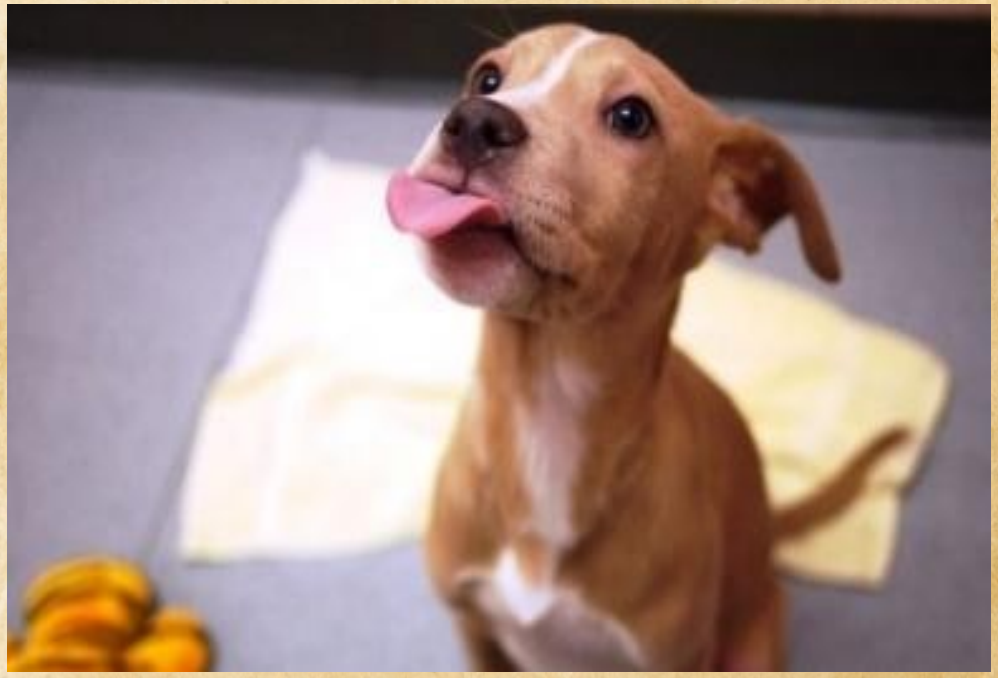
DETECTAR

CONTENER

RESPONDER

NSM

IDS / IPS



IPS

Intrusion Prevention Systems

IDS

Intrusion Detection Systems

MINISTERIO DE ENERGÍA
Y RECURSOS NATURALES
COORDINACIÓN TÉCNICA
ADMINISTRATIVA

JUNTOS
PODEMOS
MÁS

IDS – IPS Libres y Gratuitos

IDS: Clasificación

ENFOQUE	ORIGEN DE DATOS	ESTRUCTURA	COMPORTAMIENTO
Detección de Anomalías	NIDS	Centralizados	Activos
Detección De Usos	HIDS	Distribuidos	Pasivos
Híbridos	Híbridos		

IPS: Clasificación

ORIGEN DE DATOS

- HIPS
- NIPS
- WIPS
- NBA

Reglas: IDS – IPS
No es Magia

alert icmp any any -> any any (msg: "ICMP detected";)

#alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP Address Mask Reply undefined code"; icode:>0; itype:18; classtype:misc-activity; sid:2100387; rev:8; metadata:created_at 2010_09_23, updated_at 2010_09_23;)

#alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP Address Mask Request undefined code"; icode:>0; itype:17; classtype:misc-activity; sid:2100389; rev:8; metadata:created_at 2010_09_23, updated_at 2010_09_23;)

#alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP Alternate Host Address undefined code"; icode:>0; itype:6; classtype:misc-activity; sid:2100391; rev:9; metadata:created_at 2010_09_23, updated_at 2010_09_23;)

#alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP Datagram Conversion Error undefined code"; icode:>0; itype:31; classtype:misc-activity; sid:2100393; rev:9; metadata:created_at 2010_09_23, updated_at 2010_09_23;)

#alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP Datagram Conversion Error"; icode:0; itype:31; classtype:misc-activity; sid:2100392; rev:6; metadata:created_at 2010_09_23, updated_at 2010_09_23;)

Indicadores de Efectividad

VERDADERO POSITIVO – TP

Intrusión existente y correctamente detectada.

FALSO POSITIVO – FP

Intrusión no existente e incorrectamente detectada.

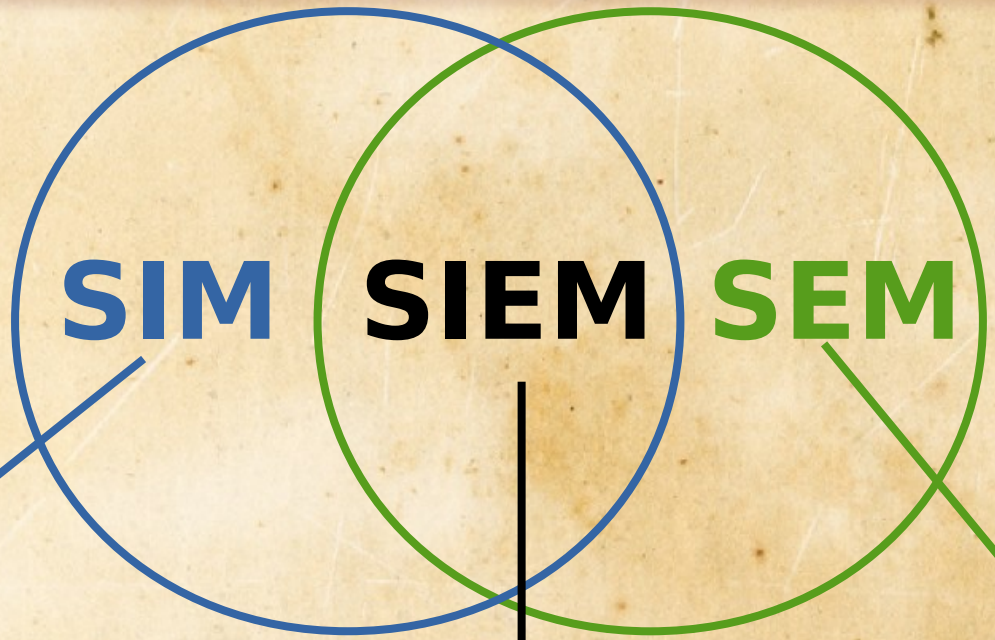
FALSO NEGATIVO – FN

Intrusión existente y no detectada.

FALSO POSITIVO – FP

Intrusión no existente y no detectada.

SIEM



Security Information Managment

Security Event Managment

Security Information and Event Managment

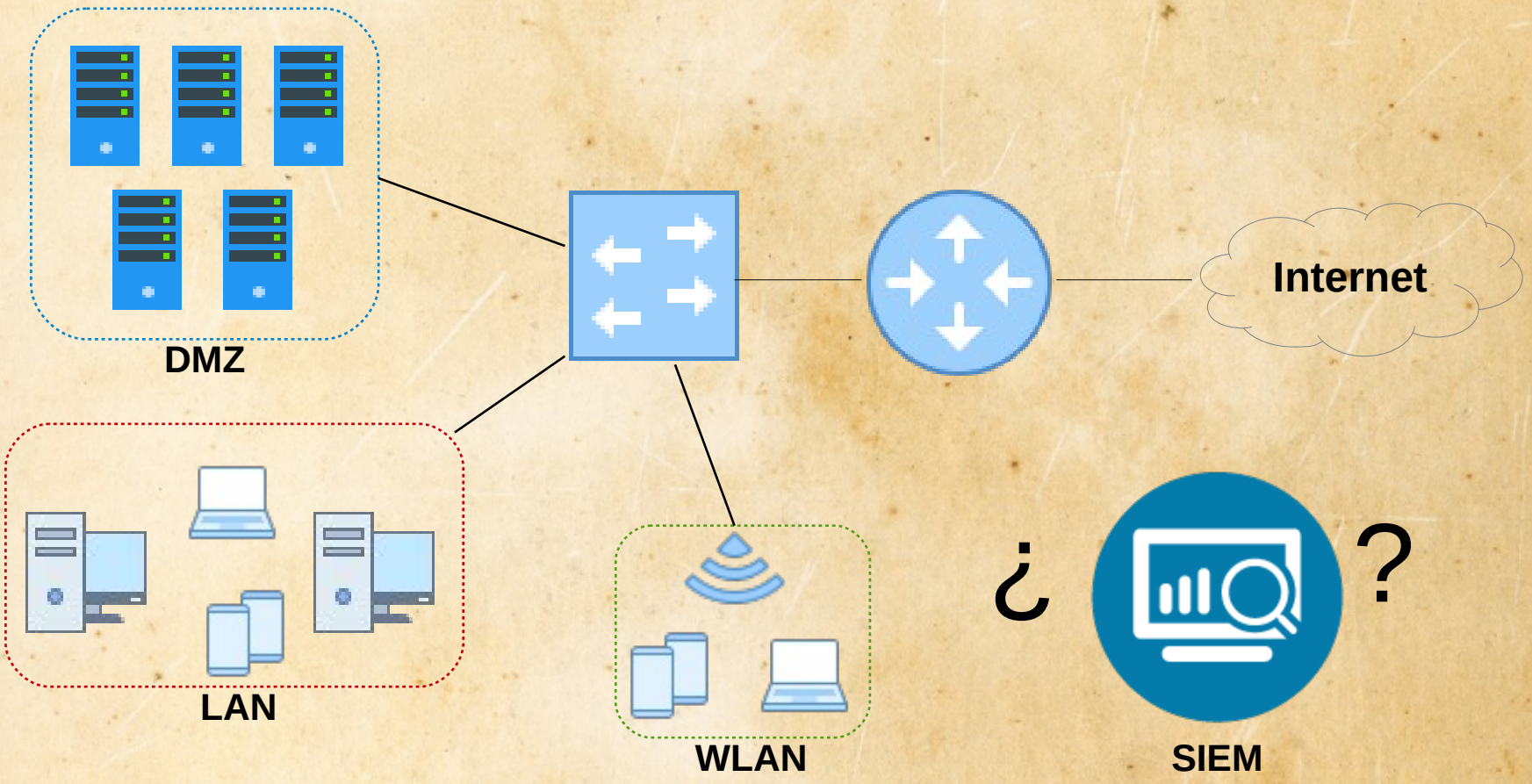
MINISTERIO DE ENERGÍA Y RECURSOS NATURALES
COORDINACIÓN TÉCNICA ADMINISTRATIVA

JUNTOS PODEMOS MÁS

¿Entonces?

- Agregación de Datos
- Administración de Logs de distintas Fuentes
- Correlación de Datos para buscar atributos comunes y relacionar eventos
- Alertas
- Cuadros de Mandos para Identificar actividades y reconocer patrones
- Elaboración de Informes
- Retención de Información para Análisis Forense

¿Dónde Va?



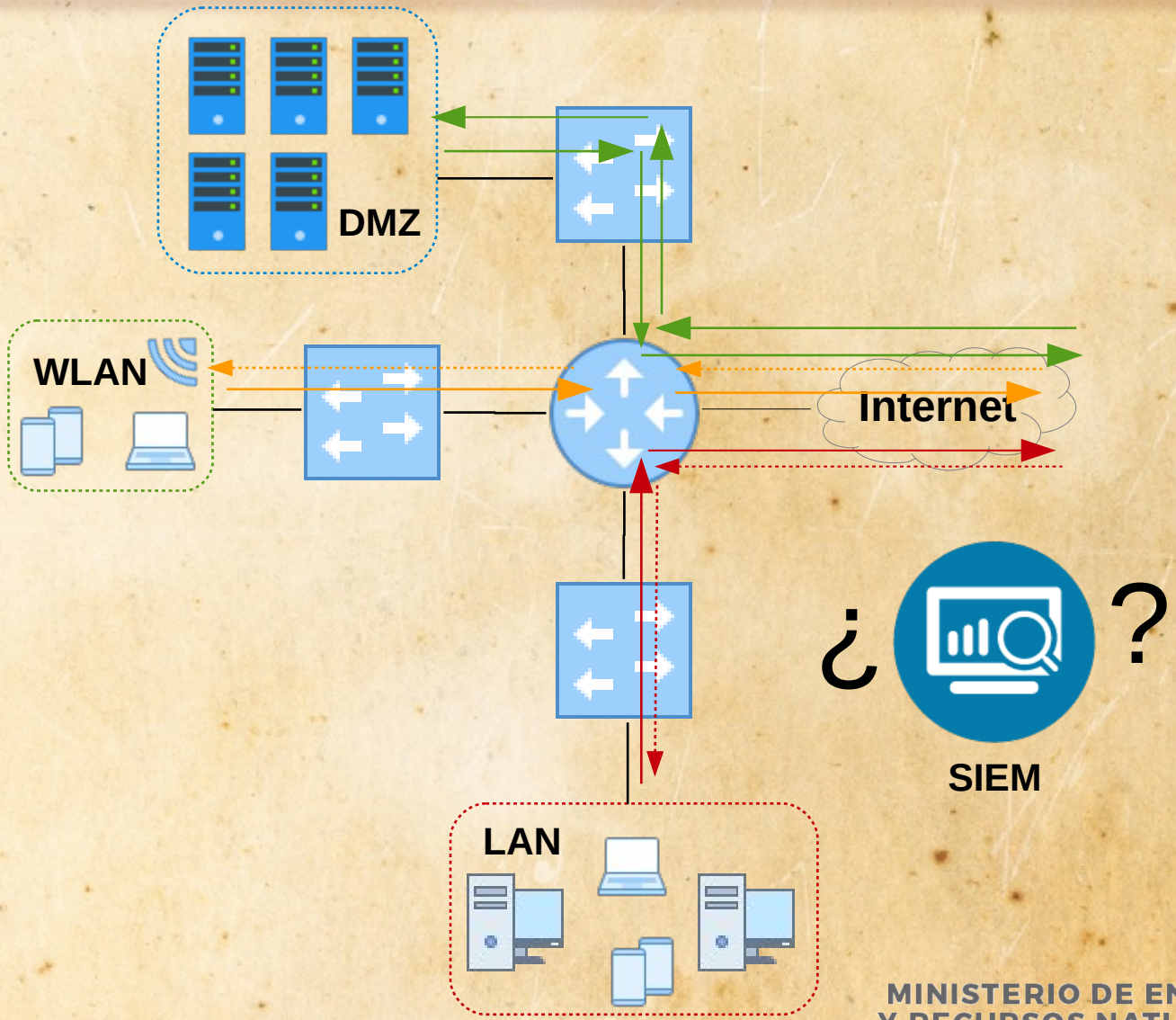
¿Dónde Va? - Factores

VISIBILIDAD

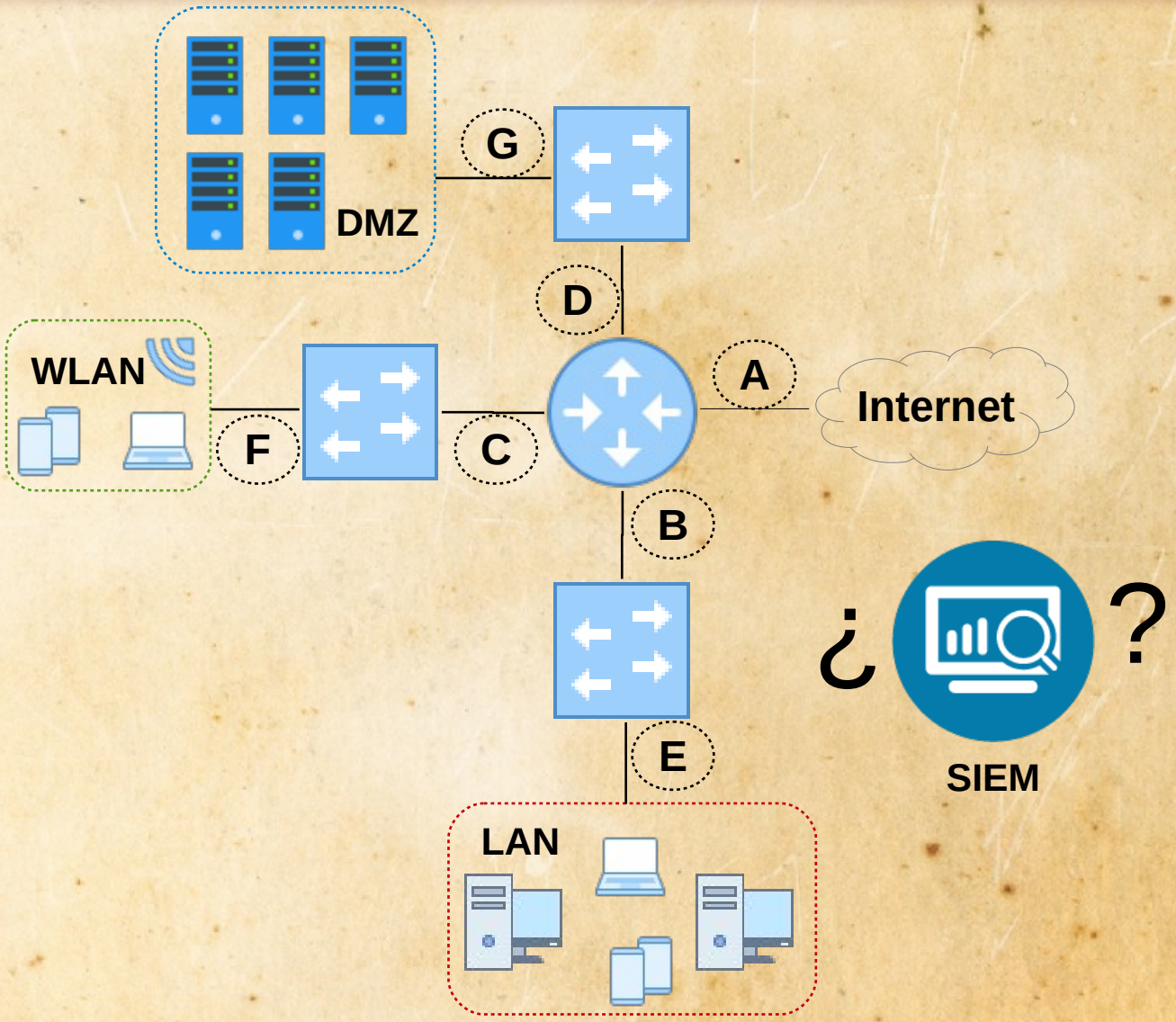
¿Tráfico a Monitorear?

FLUJO DE TRÁFICO

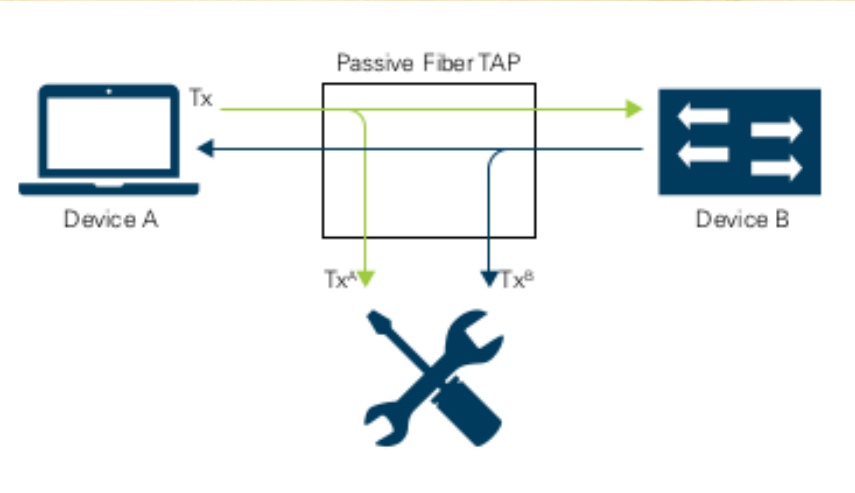
Flujo de Tráfico

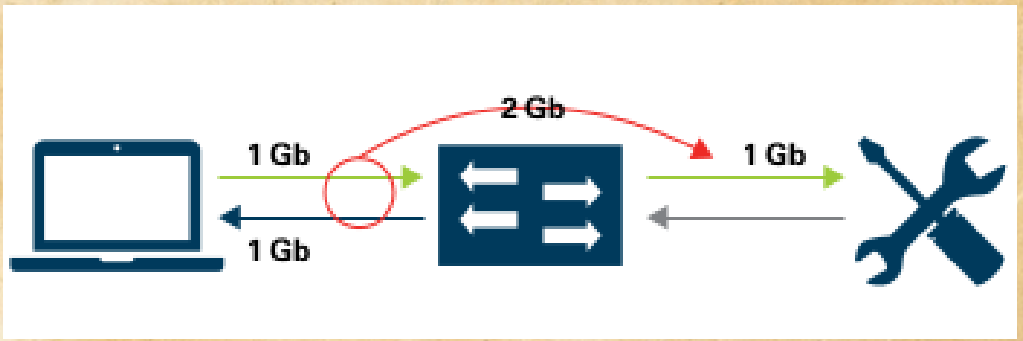


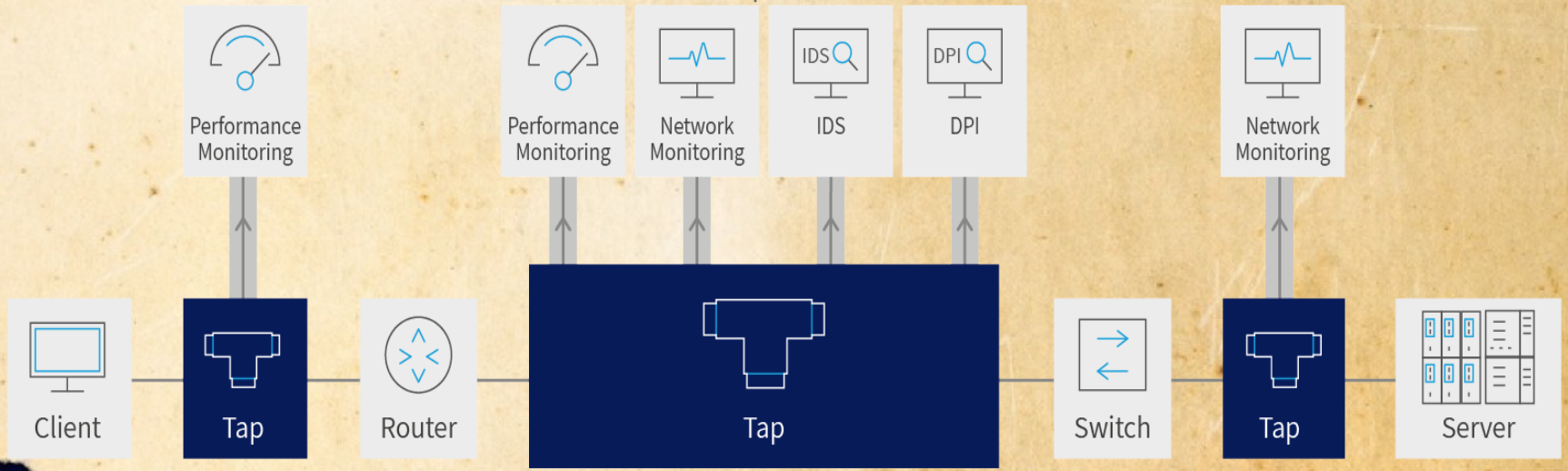
¿Dónde Va? - Debate



TAP vs SPAN





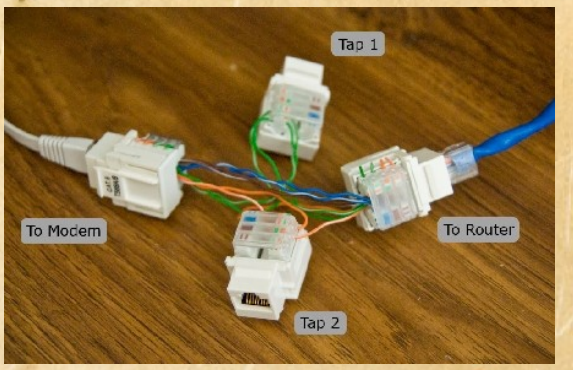


MINISTERIO DE ENERGÍA Y RECURSOS NATURALES
COORDINACIÓN TÉCNICA ADMINISTRATIVA

JUNTOS PODEMOS MÁS

TAP

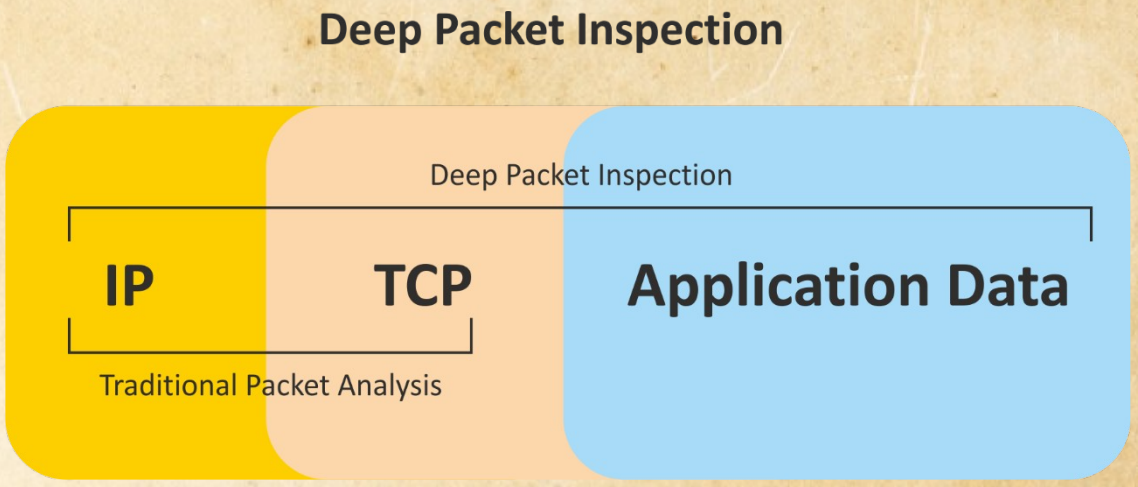

10/100/1000 Aggregation Tap
POWER
NETWORK
MONITOR
AGGREGATION
NON-AGGREGATION
USRobotics


Tap 1
To Modem
To Router
Tap 2


Optional 5V/1A
USB 3.0
PROFISHARK
1G
PROFITAP
Link/Activity
A
10
100
1000
B
Link/Activity


10 Gigabit Fiber Tap
Tx Rx
A
NETWORK
B
A
MON
B
USRobotics

DPI

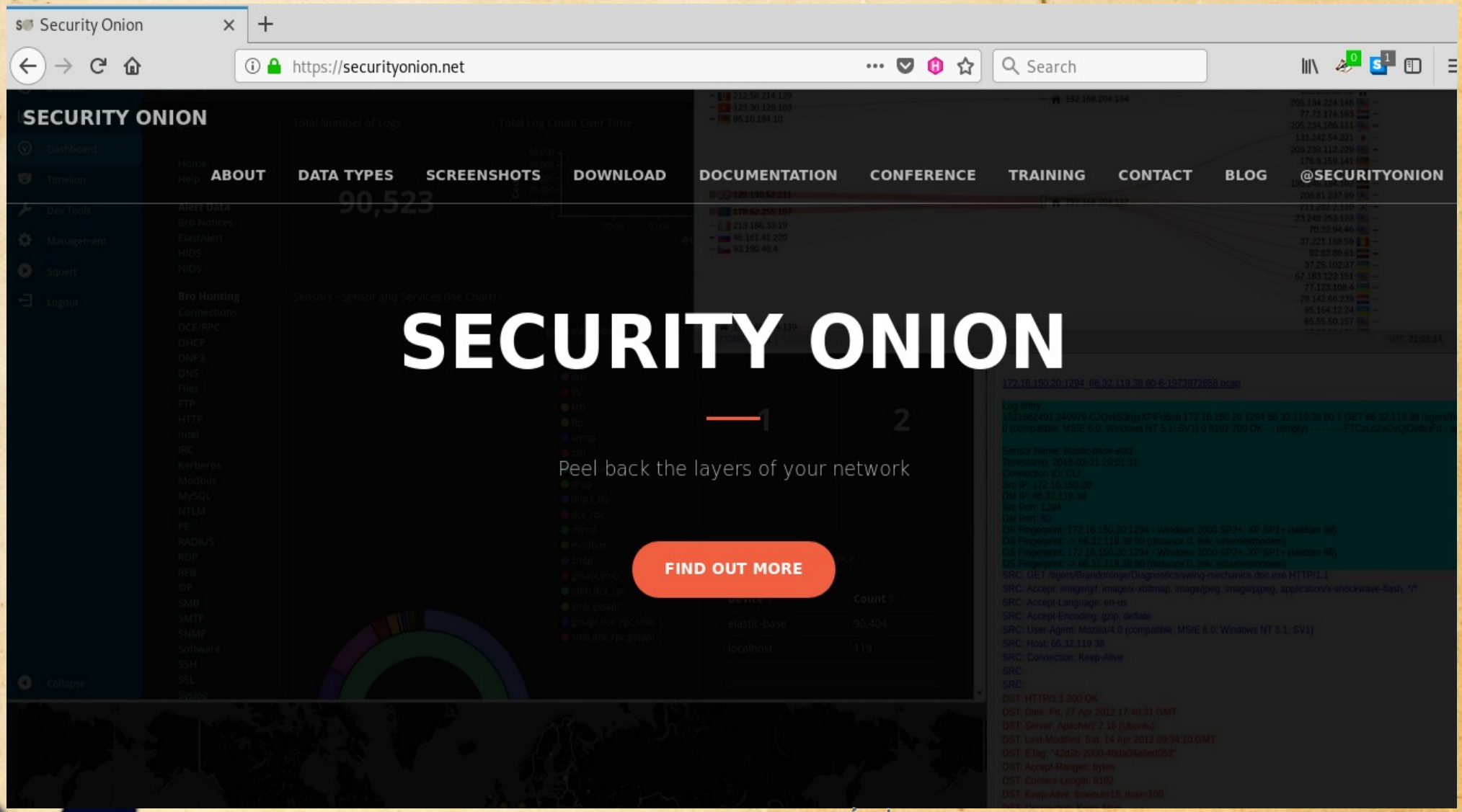

Deep Packet Inspection
Deep Packet Inspection
IP
TCP
Application Data
Traditional Packet Analysis

DPI - Producto

Tráfico encriptado (DPI-SSL) de inspección profunda de paquetes de SSL/TLS

Proteja su red en contra de amenazas encriptadas con la inspección profunda de paquetes de [redacted] de SSL/TLS y SSH. Estos servicios de seguridad complementarios están disponibles en todos los NGFirewalls y UTMs de [redacted] DPI-SSL brinda una protección profunda en contra de amenazas encriptadas, así como la desencriptación y desempeño de inspección sin límites. Aproveche el motor de la solución Reassembly-Free Deep Packet Inspection patentada de [redacted], un conjunto completo de tecnología de inspección y transmisión que analiza una amplia variedad de protocolos de encriptación incluyendo HTTPS, SMTPS, NNTPS, LDAPS, FTPS, Telnets, IMAPS, IRCS y POPS. Para tráfico intenso o despliegues altamente regulados, DPI-SSL puede excluir las fuentes confiables para optimizar el desempeño de la red y cumplir con los requerimientos de privacidad y/o legales.

SecurityOnion –
Un Vistazo



Terminamos...

Lucas González.

lucasg@neuquen.gov.ar

MINISTERIO DE ENERGÍA
Y RECURSOS NATURALES
COORDINACIÓN TÉCNICA
ADMINISTRATIVA

JUNTOS
PODEMOS
MÁS