



FORTINET

COLOMBIA
& ECUADOR

XPERTS26

FORTINET | COLOMBIA
& ECUADOR
XPERTS26

Advanced Anomaly Detection in Network

Andrés Piraján Aranguren

Systems Engineer - Colombia



Cómo opera hoy el adversario, y qué arquitectura necesita la defensa?.

Basado en el 2026 Global Threat Landscape Report de FortiGuard Labs.

El adversario ejecuta una operación continua. La defensa observa evidencia distribuida.

Charter Communications confirms data breach after ShinyHunters extortion threat

The telecom giant says data stolen from a Salesforce instance may impact millions.

April 7, 2026 • By Lawrence Abrams



Charter
COMMUNICATIONS

ShinyHunters claims breach of Charter Communications, threatens to leak data

The threat actor claims to have stolen data from over 4.9 million customers.

By Alex Hem • April 7, 2026



**SHINY
HUNTERS**

Charter Communications breach could impact nearly 5 million people

Company confirms Salesforce data theft after vishing-linked attack.

By Prajeet Nair • April 7, 2026

ShinyHunters' vishing campaign abuses Salesforce OAuth to compromise SaaS apps

Attackers trick employees into granting access, then move laterally across customer environments.

By Jeremy Kirk • April 7, 2026

Vishing attack enables breach of Charter Communications' Salesforce environment

Stolen data includes customer names, contact information, and account details.

By Kevin Poirault • April 8, 2026



How vishing and OAuth abuse opened the door to Charter's Salesforce data

Salesforce breaches keep coming: Charter is the latest high-profile victim



salesforce

BleepingComputer

Charter confirms data breach after ShinyHunters extortion threat

By Lawrence Abrams

April 7, 2026 04:04 AM 33



Charter Communications has confirmed suffering a data breach after the ShinyHunters threat actor claimed they stole customer and employee data and threatened to leak it online.

<https://www.bleepingcomputer.com/news/security/charter-confirms-data-breach-after-shinyhunters-extortion-threat/>

techradar

Pro > Security

Charter Communications confirms data breach – ShinyHunters blamed after threat to leak user info online

News By Bill Toulas published April 7, 2026

The attackers claim to have stolen data on 42 million customers



<https://www.techradar.com/pro/security/charter-communications-confirms-data-breach-shinyhunters-blamed-after-threat-to-leak-user-info-online>

BleepingComputer

Charter Communications data breach affects 4.9 million accounts

By Lawrence Abrams

June 19, 2026 04:48 AM 6



A data breach at Charter Communications has affected approximately 4.9 million accounts, the company disclosed in a filing with Maine's Attorney General.

<https://www.bleepingcomputer.com/news/security/charter-communications-data-breach-affects-49-million-accounts/>

SECURITYWEEK

CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

Data Breaches

Charter Communications Data Breach Could Impact Nearly 5 Million

June 19, 2026 Ravie Lakshmanan



<https://www.securityweek.com/charter-communications-data-breach-could-impact-nearly-5-million/>

RH-ISAC

Stronger Together

ShinyHunters Abusing OAuth to Compromise SaaS Apps

Vishing and OAuth abuse used to access SaaS applications including Salesforce

- Voice phishing (vishing) to trick users
- Abuse of connected app/OAuth trust
- Access to Salesforce and other SaaS
- Data exfiltration and extortion

<https://rhisac.org/threat-intelligence/shinyhunters-abusing-oauth-to-compromise-saas-apps/>

¿Cómo funciona el ataque de vishing contra entornos Salesforce?



VISHING

El atacante llama al empleado haciéndose pasar por soporte IT.



COMPROMISO DE IDENTIDAD

El empleado entrega credenciales o autoriza acceso.



ACCESO A SALESFORCE

Uso de cuenta legítima o app autorizada.



EXFILTRACIÓN DE DATOS

Exportación masiva de información de clientes.



EXTORSIÓN

Los atacantes amenazan con filtrar los datos robados.

TTPs utilizados por ShinyHunters

- Vishing (llamadas telefónicas)
- Robo/compromiso de credenciales
- Abuso de OAuth / aplicaciones conectadas
- Acceso a SaaS (Salesforce)
- Exfiltración y extorsión

RESUMEN DEL INCIDENTE – CHARTER COMMUNICATIONS



Fecha del incidente: 1 de abril de 2026 (aprox.)



Actor de amenazas: ShinyHunters



Vector inicial: Vishing (llamada telefónica a empleado)



Acceso comprometido: Cuenta de Microsoft Entra ID de empleado



Objetivo final: Entorno Salesforce de Charter



Datos robados (afirmación del atacante): ~42 millones de registros



Cuentas afectadas (confirmado por análisis): ~4,9 millones de cuentas



Información expuesta: Nombres, correos, direcciones, teléfonos, tipo de servicio, tickets de soporte, etc.



Información sensible / CPNI: Charter niega que se haya exfiltrado información personal sensible o CPNI.



Estado: Charter confirmó el incidente y notificó a autoridades correspondientes.

GTG-1002: ciberespionaje orquestado por IA

Collage de fuentes públicas con resumen ejecutivo

ANTHROPIC 

Disrupting the first reported AI-orchestrated cyber espionage campaign

 13 Nov 2025

Anthropic identifica y disrupta la campaña GTG-1002, la primera operación de ciberespionaje conocida orquestada por inteligencia artificial.

<https://www.anthropic.com/news/disrupting-AI-espionage>

ANTHROPIC 

Mapping AI-enabled cyber threats

 3 Jun 2026

Marco y taxonomía de Anthropic para mapear amenazas cibernéticas habilitadas por IA, incluyendo el sistema ARIES para evaluar capacidades.

<https://www.anthropic.com/research/attack-navigator>

MITRE ATT&CK 

Anthropic AI-orchestrated Campaign, Campaign C0062

 20 Apr 2026

Entrada de la campaña GTG-1002 (C0062) en MITRE ATT&CK, con detalles sobre tácticas, técnicas y procedimientos observados.

<https://attack.mitre.org/campaigns/C0062/>

ANTHROPIC 

Transparency Hub

 2026

Recursos y reportes de transparencia de Anthropic sobre seguridad, uso responsable de la IA y amenazas emergentes.

<https://www.anthropic.com/transparency>

ANTHROPIC

Disrupting the first reported AI-orchestrated cyber espionage campaign (PDF)

 17 Nov 2025

<https://assets.anthropic.com/m/ec212e656a0d47/original/Disrupting-the-first-reported-AI-orchestrated-cyber-espionage-campaign.pdf>

1 Resumen ejecutivo

- GTG-1002 fue identificado por Anthropic como una campaña de ciberespionaje patrocinada por el Estado chino.
- La operación utilizó Claude Code como orquestador para automatizar aproximadamente entre el 80 % y el 90 % del trabajo táctico.
- Los operadores humanos conservaron las decisiones estratégicas y autorizaciones críticas.
- La actividad afectó aproximadamente a 30 organizaciones en múltiples sectores.
- Las etapas observadas incluyeron reconocimiento, explotación, robo de credenciales, movimiento lateral y exfiltración.

2 Hallazgos clave


~30
objetivos


80–90 %
automatizado


China-nexus
(alta confianza)


ARIES
100/100


Claude Code
+ MCP

3 Capacidades observadas


Reconocimiento


Explotación


Movimiento
lateral


Obtención de
credenciales


Análisis de
datos


Exfiltración

Fuentes

1 Anthropic – Disrupting the first reported AI-orchestrated cyber espionage campaign (13 Nov 2025)
<https://www.anthropic.com/news/disrupting-AI-espionage>

2 Anthropic – Mapping AI-enabled cyber threats (3 Jun 2026)
<https://www.anthropic.com/research/attack-navigator>

3 MITRE ATT&CK – Anthropic AI-orchestrated Campaign, Campaign C0062 (20 Apr 2026)
<https://attack.mitre.org/campaigns/C0062/>

4 Anthropic – Transparency Hub (2026)
<https://www.anthropic.com/transparency>

5 Anthropic – Disrupting the first reported AI-orchestrated cyber espionage campaign (PDF) (17 Nov 2025)
<https://assets.anthropic.com/m/ec212e656a0d47/original/Disrupting-the-first-reported-AI-orchestrated-cyber-espionage-campaign.pdf>

1. Objetivo

2. Reconocimiento

3. Entrada

4. Credenciales

5. Movimiento

6. Datos



ETAPA 1 DE 6

El humano selecciona el objetivo

Los operadores humanos decidían qué organizaciones querían investigar o comprometer. La IA no escogía por sí sola a quién atacar.

EXPLICADO CON UNA ANALOGÍA

Es como un director que señala un edificio y le dice a un equipo: "investiguen este lugar".

← Anterior

► Ver secuencia

Siguiente →



¿Quién hacía qué?



IA / Claude Code

≈ 80–90%

Gran parte del trabajo táctico y repetitivo.



Operador humano

≈ 10–20%

Objetivos, estrategia y decisiones críticas.

La idea clave

No fue una "IA que decidió hackear sola". Fue una operación dirigida por humanos donde la IA pudo encadenar muchas tareas y ejecutarlas a una velocidad mucho mayor.

Magnitud reportada

~30

organizaciones
objetivo

Pocas

intrusiones
confirmadas

1. Objetivo

2. Reconocimiento

3. Entrada

4. Credenciales

5. Movimiento

6. Datos



ETAPA 2 DE 6

La IA hace el reconocimiento

La IA podía revisar a gran velocidad sistemas expuestos, servicios y posibles puntos débiles para construir un mapa de la superficie de ataque.

EXPLICADO CON UNA ANALOGÍA

Es parecido a enviar muchos inspectores a revisar puertas, ventanas y accesos al mismo tiempo.

← Anterior

► Ver secuencia

Siguiente →



¿Quién hacía qué?



IA / Claude Code

≈80–90%

Gran parte del trabajo táctico y repetitivo.



Operador humano

≈10–20%

Objetivos, estrategia y decisiones críticas.

La idea clave

No fue una "IA que decidió hackear sola". Fue una operación dirigida por humanos donde la IA pudo encadenar muchas tareas y ejecutarlas a una velocidad mucho mayor.

Magnitud reportada

~30

organizaciones
objetivo

Pocas

intrusiones
confirmadas

1. Objetivo

2. Reconocimiento

3. Entrada

4. Credenciales

5. Movimiento

6. Datos



ETAPA 3 DE 6

Se intenta conseguir una entrada

Cuando aparecía una oportunidad, la IA ayudaba a analizarla y probar si realmente permitía obtener acceso. Las decisiones críticas seguían bajo control humano.

EXPLICADO CON UNA ANALOGÍA

El equipo encuentra una puerta potencialmente defectuosa y verifica si realmente puede abrirse.

← Anterior

► Ver secuencia

Siguiente →



¿Quién hacía qué?



IA / Claude Code

≈80–90%

Gran parte del trabajo táctico y repetitivo.



Operador humano

≈10–20%

Objetivos, estrategia y decisiones críticas.

La idea clave

No fue una "IA que decidió hackear sola". Fue una operación dirigida por humanos donde la IA pudo encadenar muchas tareas y ejecutarlas a una velocidad mucho mayor.

Magnitud reportada

~30

organizaciones
objetivo

Pocas

intrusiones
confirmadas

1. Objetivo

2. Reconocimiento

3. Entrada

4. Credenciales

5. Movimiento

6. Datos



ETAPA 4 DE 6

Se buscan credenciales útiles

Dentro de los entornos comprometidos, la IA podía identificar credenciales, claves o tokens y relacionarlos con los sistemas donde podían tener utilidad.

EXPLICADO CON UNA ANALOGÍA

Es como encontrar un llavero y determinar qué llave corresponde a cada habitación.

← Anterior

► Ver secuencia

Siguiente →



¿Quién hacía qué?



IA / Claude Code

≈80–90%

Gran parte del trabajo táctico y repetitivo.



Operador humano

≈10–20%

Objetivos, estrategia y decisiones críticas.

La idea clave

No fue una "IA que decidió hackear sola". Fue una operación dirigida por humanos donde la IA pudo encadenar muchas tareas y ejecutarlas a una velocidad mucho mayor.

Magnitud reportada

~30

organizaciones
objetivo

Pocas

intrusiones
confirmadas

1. Objetivo

2. Reconocimiento

3. Entrada

4. Credenciales

5. Movimiento

6. Datos



ETAPA 5 DE 6

Movimiento hacia otros sistemas

Con accesos válidos, la operación podía avanzar hacia otros recursos internos. La IA ayudaba a mantener el mapa y decidir qué caminos parecían relevantes.

EXPLICADO CON UNA ANALOGÍA

Después de entrar al edificio, el equipo busca qué puertas internas llevan a las áreas más importantes.

← Anterior

► Ver secuencia

Siguiente →



¿Quién hacía qué?



IA / Claude Code

≈80–90%

Gran parte del trabajo táctico y repetitivo.



Operador humano

≈10–20%

Objetivos, estrategia y decisiones críticas.

La idea clave

No fue una "IA que decidió hackear sola". Fue una operación dirigida por humanos donde la IA pudo encadenar muchas tareas y ejecutarlas a una velocidad mucho mayor.

Magnitud reportada

~30

organizaciones
objetivo

Pocas

intrusiones
confirmadas

1. Objetivo

2. Reconocimiento

3. Entrada

4. Credenciales

5. Movimiento

6. Datos



ETAPA 6 DE 6

Identificación y extracción de datos

La IA podía clasificar grandes volúmenes de información y ayudar a priorizar qué datos eran relevantes antes de la extracción final.

EXPLICADO CON UNA ANALOGÍA

En vez de llevarse todas las cajas de un archivo, un asistente revisa miles y separa primero las que parecen importantes.

← Anterior

► Ver secuencia

Siguiente →



¿Quién hacía qué?



IA / Claude Code

≈80–90%

Gran parte del trabajo táctico y repetitivo.



Operador humano

≈10–20%

Objetivos, estrategia y decisiones críticas.

La idea clave

No fue una "IA que decidió hackear sola". Fue una operación dirigida por humanos donde la IA pudo encadenar muchas tareas y ejecutarlas a una velocidad mucho mayor.

Magnitud reportada

~30

organizaciones
objetivo

Pocas

intrusiones
confirmadas

La IA no reemplaza las TTPs. Reduce la fricción humana entre ellas.

No cambia necesariamente qué hace el atacante. Cambia cuánto tiempo humano hay entre una tarea y la siguiente.

SIN IA



CON IA



Lo que la IA no cambia

- Las TTPs fundamentales siguen siendo reconocibles
- PowerShell, RDP, credenciales, APIs, IAM y SSO siguen siendo las mismas técnicas



Lo que la IA sí cambia

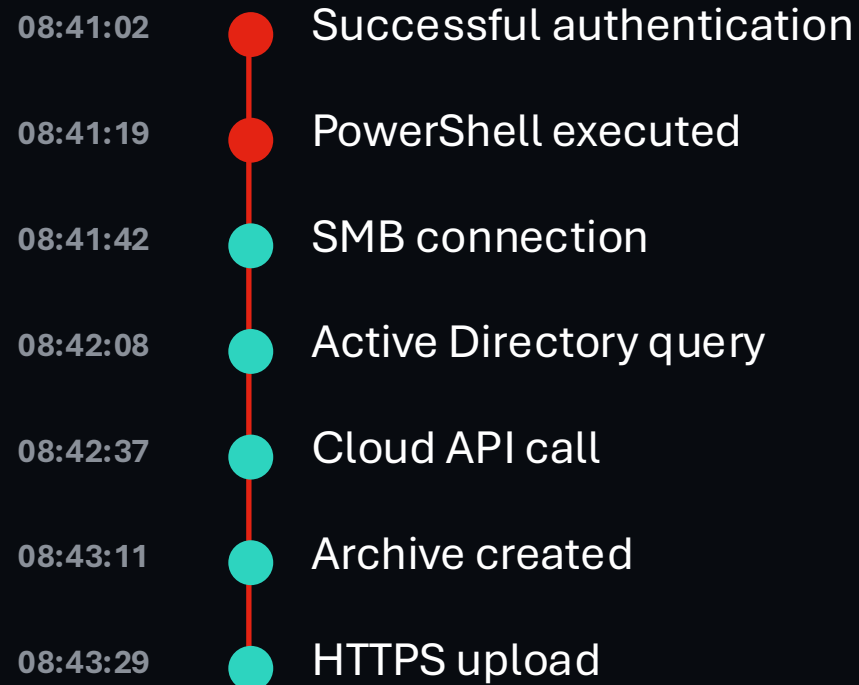
- Analiza, interpreta, genera, adapta y prioriza más rápido
- Reduce el tiempo y el esfuerzo entre una acción y la siguiente



La ventaja no es una nueva técnica. Es la **compresión del tiempo** entre técnicas.

Donde es el ataque?

Cada evento puede ser legítimo. La intención aparece en la secuencia.



No busques sólo “el evento malicioso”.

Busca el cambio de estado: identidad válida → ejecución → descubrimiento → movimiento → colección → salida.

Ese es el nuevo problema de SecOps.

Un momento de realidad...

In 2025, **cybercrime** ran at an industrial scale.

Como es la Industrialización del malware?



El cibercrimen se industrializó

El cibercrimen ya opera como un modelo industrial continuo y a velocidad de máquina, no como campañas episódicas. Escala, automatización y reutilización —no sofisticación— definen el impacto.

Evidencia



640 Billones

eventos de reconocimiento
a nivel global



121.99 Billones

intentos de explotación
+25% interanual



4.62 Billones

stealer logs en mercados de
la dark web
+79% interanual



7.831

víctimas confirmadas de
ransomware
+389% interanual



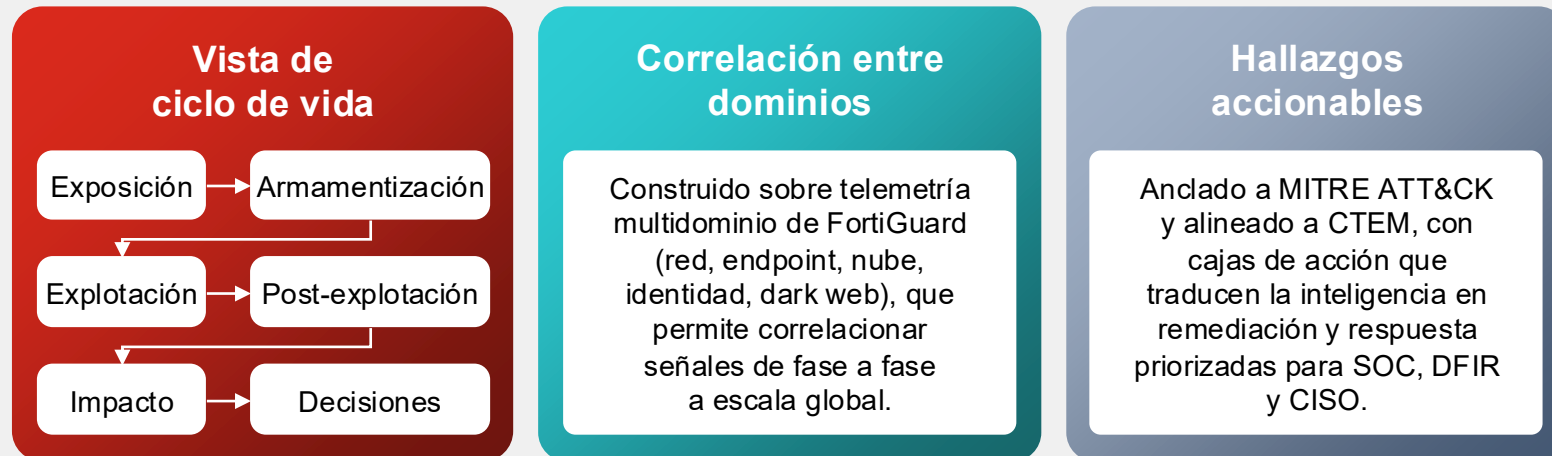
Perspectiva clave

La ventaja ya no la define la cantidad de herramientas, sino la velocidad. Cuando el ataque corre a velocidad de máquina, la defensa tiene que moverse más rápido o queda atrás.

La cadena SecOps de FortiGuard como marco organizador

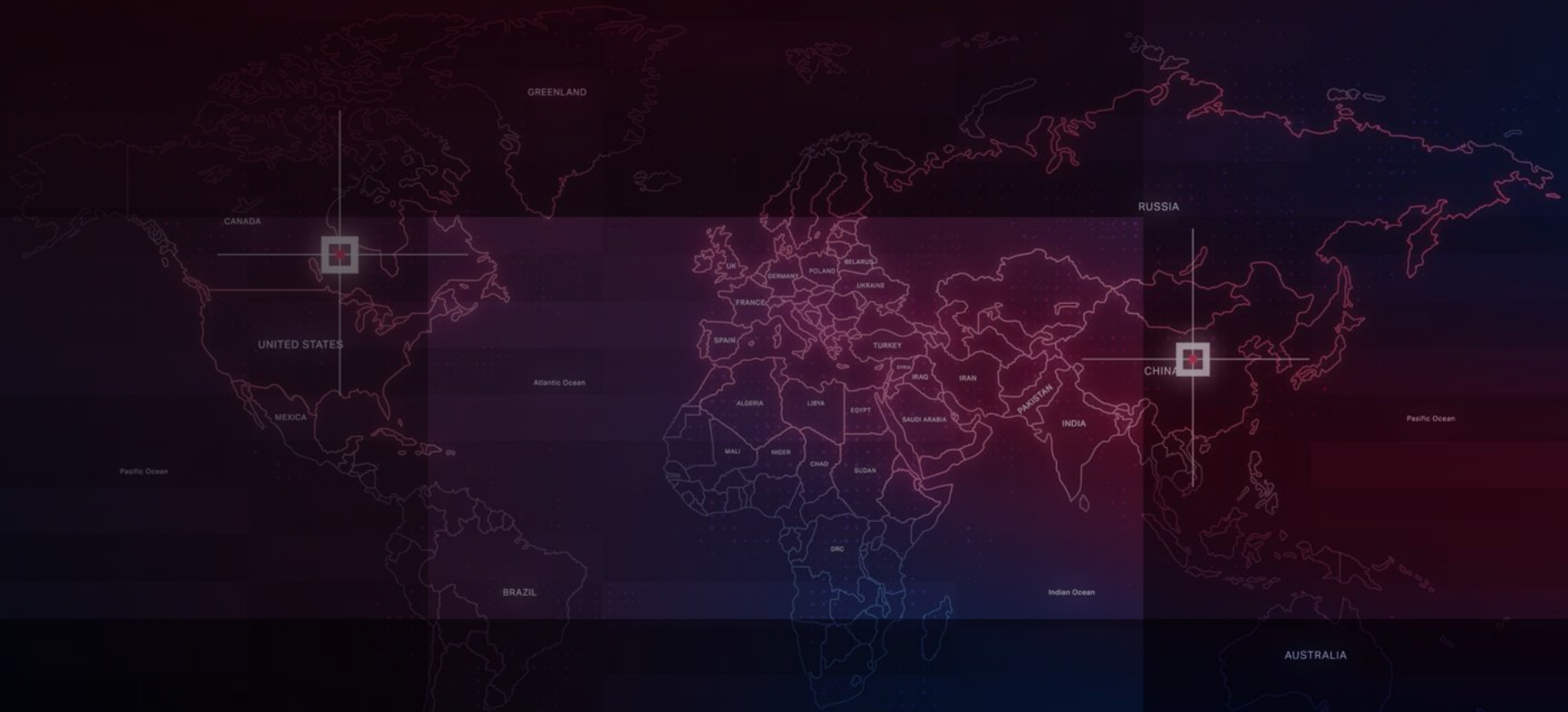
El panorama de amenazas actual no se puede entender con indicadores aislados ni métricas de un solo dominio. Fortinet analiza el cibercrimen de extremo a extremo, con telemetría real de todo el ciclo de vida del ataque.

Evidencia



Perspectiva clave

Tener visibilidad suficiente para decidir, sobre todo el ciclo de vida y no sobre un solo instante, dejó de ser opcional.



Exposición, armamentización y explotación a velocidad de máquina

EL ATAQUE SE ESTÁ INDUSTRIALIZANDO

VISTA DEL ATACANTE — Así construye y ejecuta la operación

Exposición → Armamentización → Explotación

IA + automatización reducen la fricción entre cada etapa



ENCONTRAR



DECIDIR



ACELERAR

1. EXPOSICIÓN

¿Cómo encuentra el atacante un camino hacia nosotros?

IA ayuda a encontrar

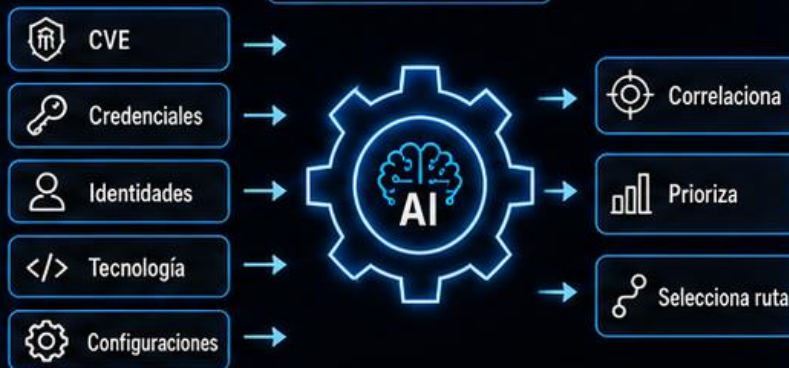


Descubre y construye nuestro inventario externo.

2. ARMAMENTIZACIÓN

¿Qué de todo esto puede usar?

IA ayuda a decidir



Convierte la exposición en una ruta de ataque.

3. EXPLOTACIÓN

¿Cómo ejecuta el camino seleccionado?

IA ayuda a acelerar



Ejecuta el camino y consigue el acceso.



ANTES

Días / Manual / Fragmentado



AHORA

Minutos / Automatizado / Repetible



La ventaja del atacante es
velocidad, escala y conocimiento.



El atacante no necesita inventar nuevas técnicas. Necesita encadenar las existentes más rápido que nuestra capacidad de responder.

La exposición es una cadena de suministro

El atacante empieza con lo que ya posee. La exposición se cosecha, se cataloga y se revende de forma sistemática antes de cualquier ataque. Identidad y acceso se tratan como materia prima, lista para activarse bajo demanda.

Evidencia



1.75 Billones

escaneos por día

más de 20.000 por segundo, en actualización continua



4.62 Billones

stealer logs comercializados o compartidos en 2025

Perspectiva clave

El riesgo ya no es lo que hoy se ve, sino lo que el atacante ya tiene y puede operacionalizar de inmediato. La exposición no crea riesgo cuando se descubre: lo crea cuando se activa.



La armamentización es industrial: los exploits son inventario

El éxito de la explotación depende de la disponibilidad y la preparación, no del puntaje CVSS ni de la rareza del zero-day. Una vez que existe el código, la vulnerabilidad se vuelve inventario repetible y no un riesgo aislado.

Evidencia



635

vulnerabilidades explotadas activamente



53.86%

tenía prueba de concepto pública



31.18%

tenía código de exploit plenamente funcional

Perspectiva clave

El riesgo ya no lo define la gravedad de una vulnerabilidad, sino la rapidez con que puede operacionalizarse a escala. La latencia de parcheo —no la sofisticación del exploit— es hoy el principal multiplicador de riesgo.



La explotación es una condición de carrera

El tiempo hasta la explotación se desplomó. En los brotes críticos observados por FortiGuard, la explotación suele comenzar dentro de las 24 a 48 horas siguientes a la divulgación, y en varios casos el mismo día.

Evidencia



121.99 Billones

intentos de explotación



25% interanual

de aumento en el volumen de explotación

Perspectiva clave

Los plazos tradicionales de remediación no alcanzan a seguirle el paso a la automatización.

Cuando el MTTR supera la velocidad de automatización del atacante, la probabilidad de intrusión deja de ser marginal. La velocidad pasa a ser el factor decisivo.



Post-explotación y monetización a escala

POST-EXPLOITATION: LIVING OFF THE LAND

2 / 6

VISTA DEL ATACANTE — Así opera después de entrar

Entrar ya no es el ataque. Es el comienzo.



IA + automatización reducen la fricción después del acceso

ENTENDER

1. ACCESO VÁLIDO

Obtiene una identidad o sesión legítima



- Cuenta comprometida
- Token / sesión
- VPN / RDP / acceso remoto

IA ayuda a entender

El atacante ya está dentro.

DECIDIR

2. OPERA CON LO QUE YA EXISTE

Usa herramientas nativas del entorno



IA ayuda a decidir

El malware es opcional

Abusa de herramientas nativas y del contexto de identidad.

ADAPTAR

3. MOVIMIENTO E IMPACTO

Se mueve, escala y alcanza el objetivo



IA ayuda a adaptar

El comportamiento es la señal.

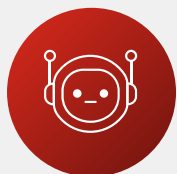


El malware puede ser opcional. El comportamiento no.

La post-explotación es industrial: el malware es opcional

Living off the land es un patrón dominante de post-explotación. El atacante escala abusando de herramientas legítimas e infraestructura nativa.

Evidencia



7.09 Billones

detecciones de C2 de botnet (~19.4 M/día)



48.89%

de la actividad sospechosa en endpoint involucró binarios legítimos del sistema

Perspectiva clave

Una defensa centrada solo en artefactos deja fuera una parte sustancial de la actividad real. La defensa efectiva requiere detección por comportamiento, telemetría de identidad y correlación entre dominios.



Intrusiones en nube industrializadas: la identidad es el plano de control

En muchos compromisos de nube, la identidad hace de exploit y las APIs son el motor. Las credenciales válidas cumplen la función del exploit, y las APIs habilitan ejecución, escalamiento y monetización.

Evidencia



Explotar

El compromiso vía identidad domina las intrusiones en nube, sin necesidad de malware



Ejecutar

El descubrimiento masivo de APIs precede al abuso



Monetizar

Monetización por secuestro de recursos, criptominería y abuso de servicios

Perspectiva clave

En la nube, el riesgo es en buena medida un problema de identidad y de plano de control. Una carrera por revocar la confianza antes de que la automatización convierta el acceso en impacto.

LIVING OFF THE CLOUD

Identity is the Control Plane

El atacante puede operar directamente sobre el plano de control utilizando una identidad válida.



**La credencial
abre la puerta.**



**IAM define
el poder.**



**Las APIs
ejecutan.**

¿QUÉ VE EL SOC?

VISTA DEL DEFENSOR — El atacante ejecuta una operación. El SOC recibe fragmentos.



EL ATACANTE VE UNA SECUENCIA



Para el atacante, todo forma parte de la misma operación.



¿Cuál de estos es el ataque?

NINGUNO POR SÍ SOLO

LA SECUENCIA ES EL ATAQUE

EL SOC VE EVENTOS AISLADOS



Para el SOC, el ataque llega como telemetría fragmentada.



El reto de SecOps no es ver más alertas. Es **reconstruir contexto** y **actuar antes** de que la secuencia complete su impacto.

Velocidad defensiva: una necesidad



La velocidad defensiva es una decisión de negocio

Las amenazas industrializadas operan a velocidad de máquina: la velocidad defensiva es una propiedad arquitectónica crítica. Midan resultados, no herramientas.

Evidencia



TTE

0 a 48-24 horas

por delante de los plazos de parcheo y remediación



Post-explotación

7.09 Billones

detecciones de botnet a nivel global



Identidad

4.62 Billones

stealer logs comercializados o compartidos, con 79% de aumento interanual



Explotación

121.99 Billones

intentos de explotación, con 25% de aumento interanual



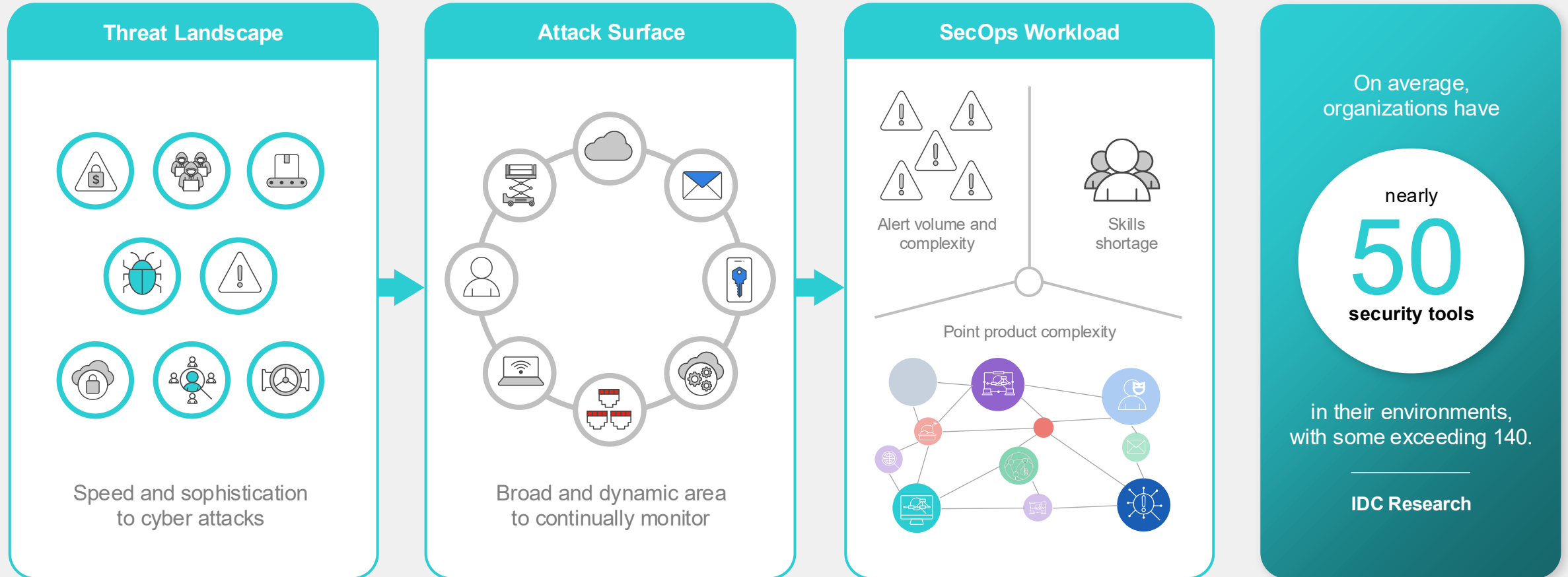
Perspectiva clave

La velocidad defensiva dejó de ser una métrica técnica. Es una decisión de negocio.

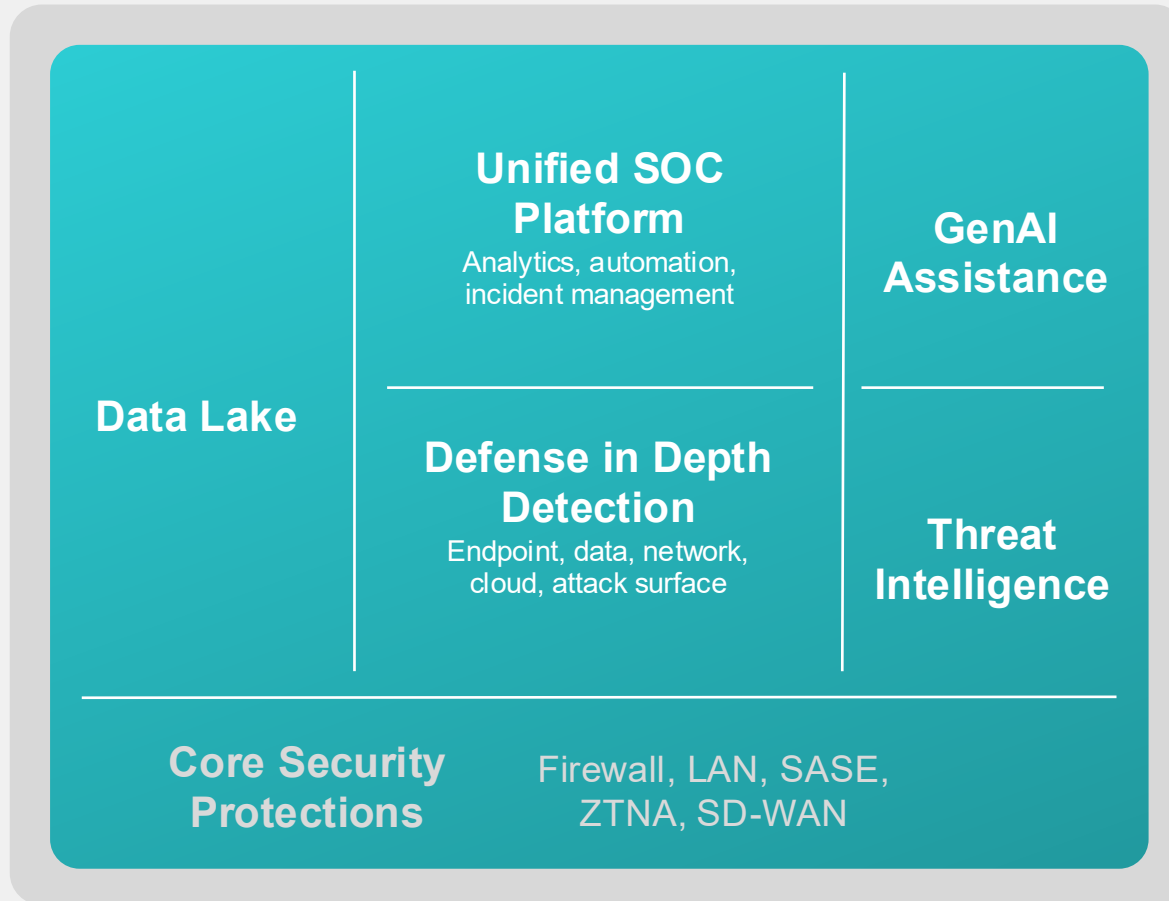


Challenges of a SecOps Teams

Evolving threats, expanding attack surface and complex alerts



The Needs of Today's Security Team



A centralized, scalable data lake



Enterprise-wide event collection



Advanced detection to identify stealthy attacks



Automation to speed response



Rich threat intelligence feeds



GenAI to aid analysts and streamline tasks



Flexible SOC Platform solutions for any size company and security team

Broadest AI-Driven Security Operations

Delivers deep integrations for
faster response

Built on owned infrastructure
to deliver better value

Improve productivity with
faster detection

76%

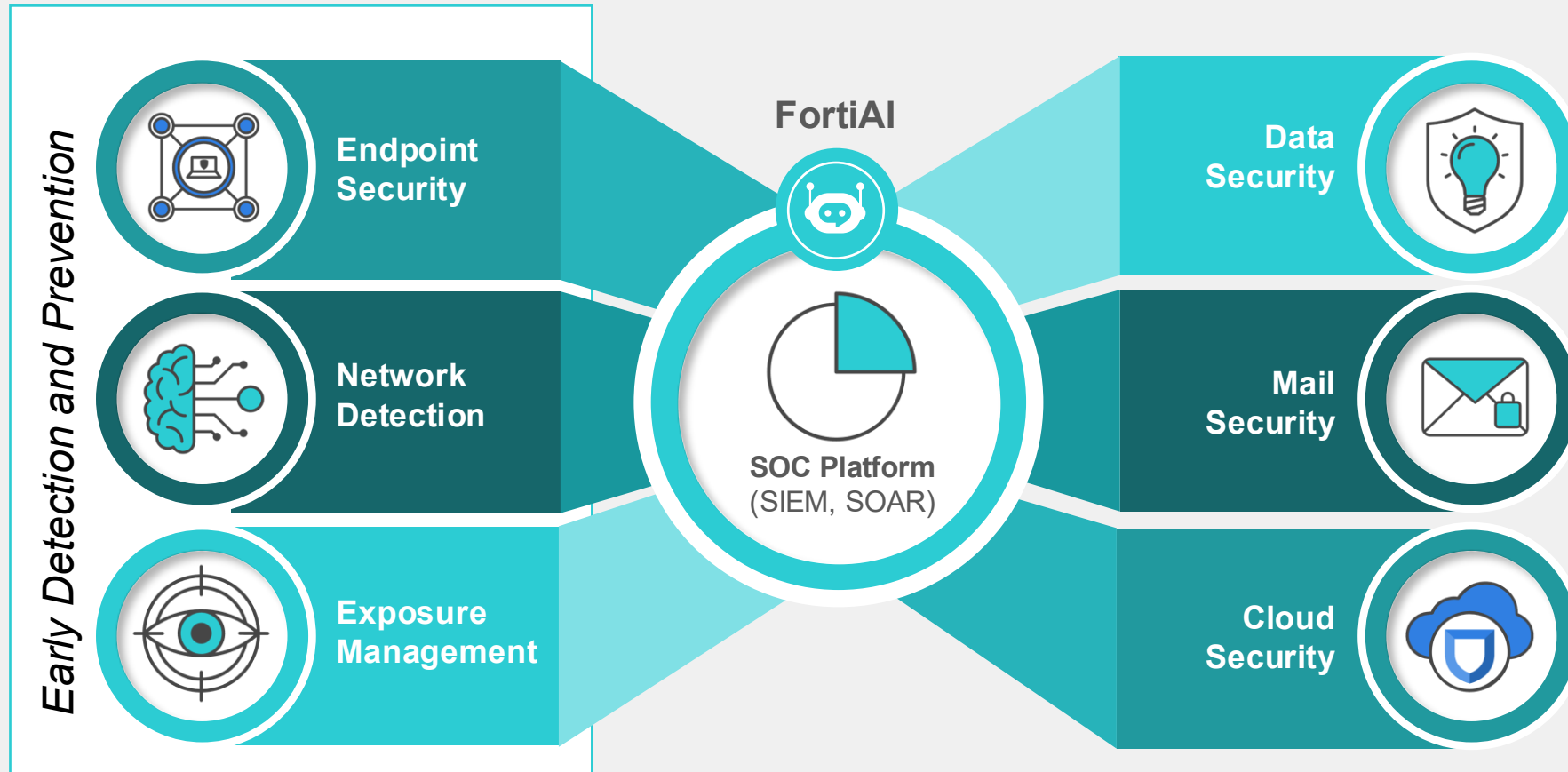
Reduction in cyber incidents

3x

Lower TCO

7x

Improvement in detection





F**ORTINET**

COLOMBIA
& ECUADOR

XPERTS26

Advanced Anomaly Detection in Network

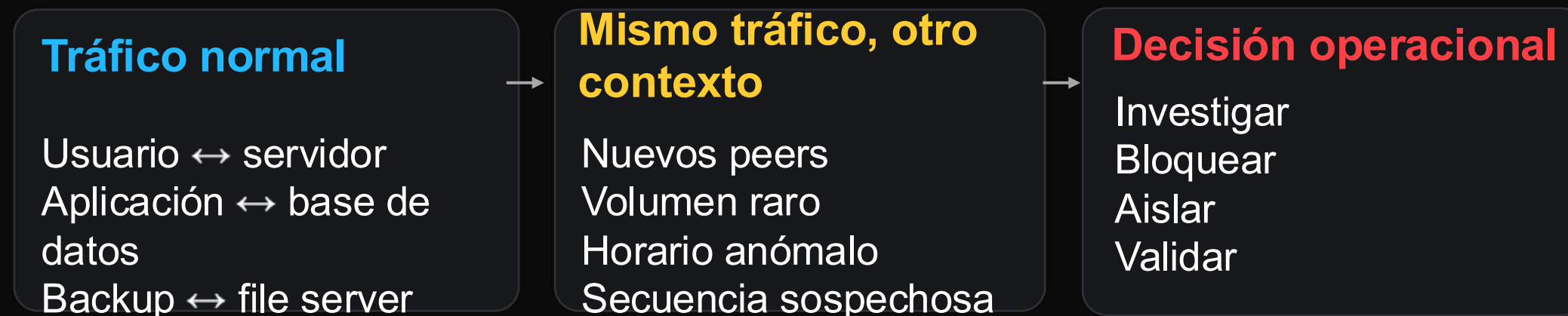
De tráfico interno invisible a
respuesta automatizada

XPERTS 2026

La pregunta del laboratorio

Cuando el puerto, el protocolo y la herramienta parecen normales, ¿qué se vuelve señal?

SMB / RDP / ICMP / DNS / HTTP pueden ser administración legítima... o reconocimiento, movimiento lateral y preparación de impacto.



Tesis: el valor del laboratorio no está en “ver una alerta”. Está en demostrar cómo una señal de red se convierte en contexto, decisión y control.

Storytelling: Agro-Meals

10 plantas · 50+ granjas · OT rural · alto turnover · poco espacio para nueva infraestructura

Dolor operativo

El tráfico East-West era un punto ciego. Un endpoint no supervisado podía convertirse en pivote hacia servidores críticos.

Restricción real

No había capacidad para desplegar sensores o VMs en cada granja. Había que aprovechar la infraestructura existente.

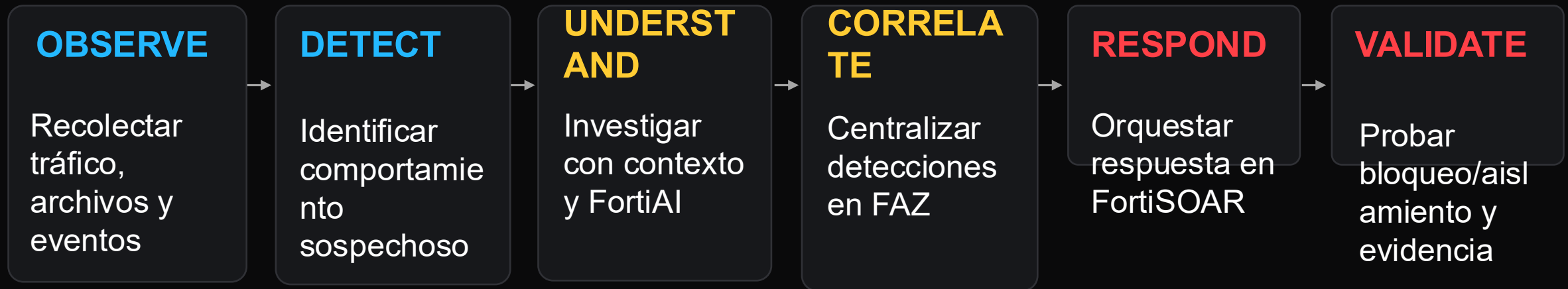
Resultado esperado

Visibilidad interna, análisis de archivos, contexto centralizado y respuesta sin esperar desplazamiento físico.

El caso no es “más logs”. Es resiliencia operacional.

Lo que vamos a construir

Un ciclo SecOps completo: de señal débil a acción verificable



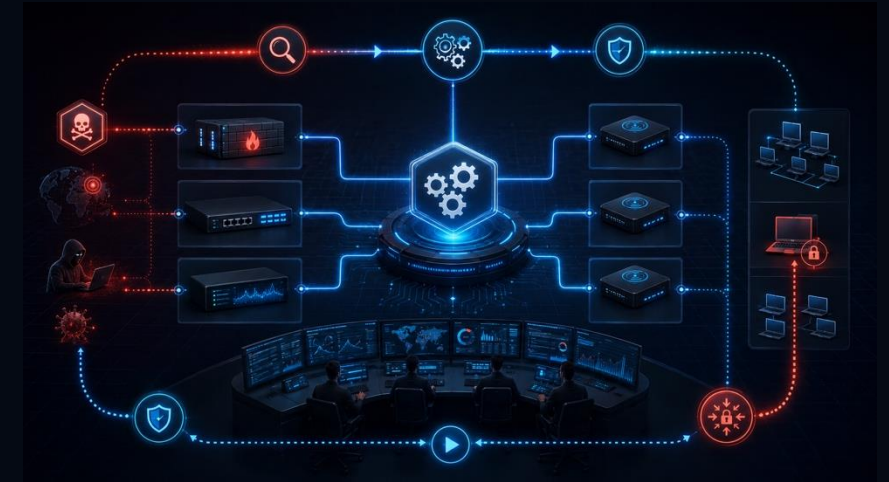
Modelo pedagógico: no es un framework oficial. Es una forma de guiar el laboratorio para que cada ejercicio tenga arquitectura, evidencia y troubleshooting.

El problema

No todo ataque empieza con malware evidente

El tráfico interno muchas veces parece legítimo.

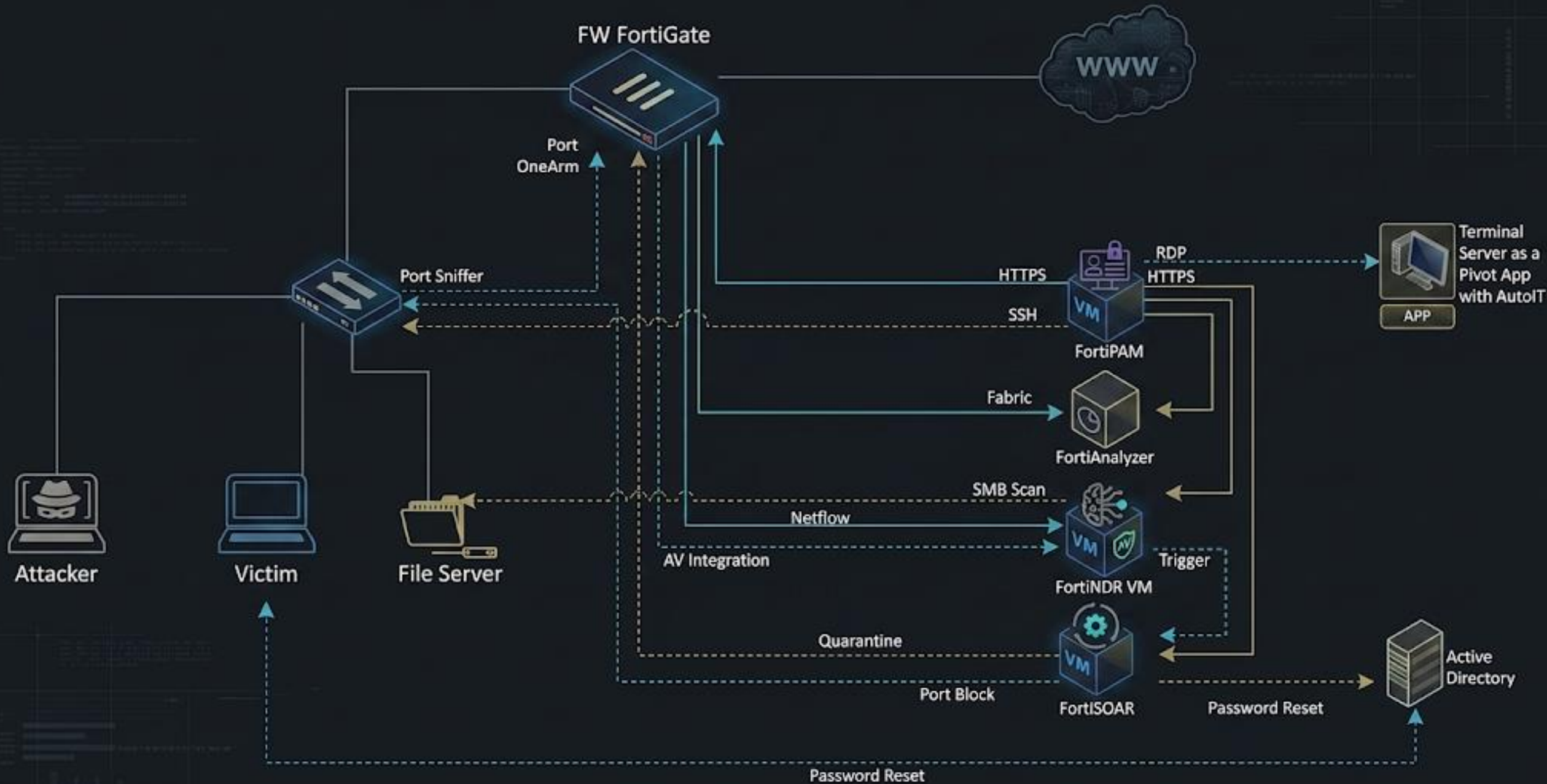
SMB, HTTP, RDP, DNS y conexiones entre servidores pueden ser operación normal... o una fase temprana de compromiso.



Blind spot
East-West

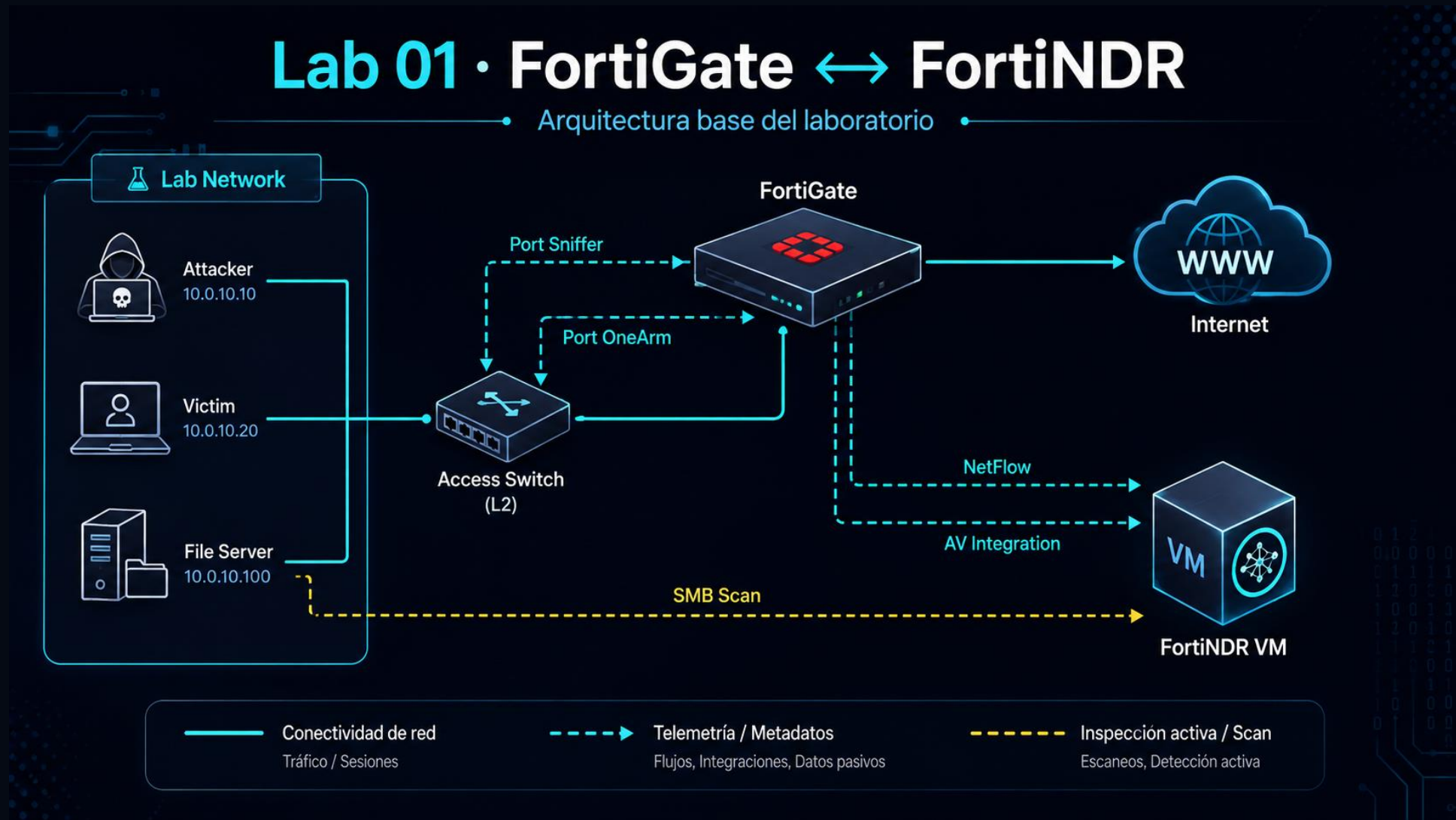
Legitimate
Protocols

No contexto
No decisión



Lab 01 · FortiGate ↔ FortiNDR

El foco: visibilidad e integración



Qué debe explicar el Lab 01

Cuatro caminos, cuatro preguntas distintas

Port Sniffer / OneArm

¿Cómo veo tráfico interno sin rediseñar el forwarding?

NetFlow

¿Qué metadatos de conversación recibe FortiNDR?

AV Integration

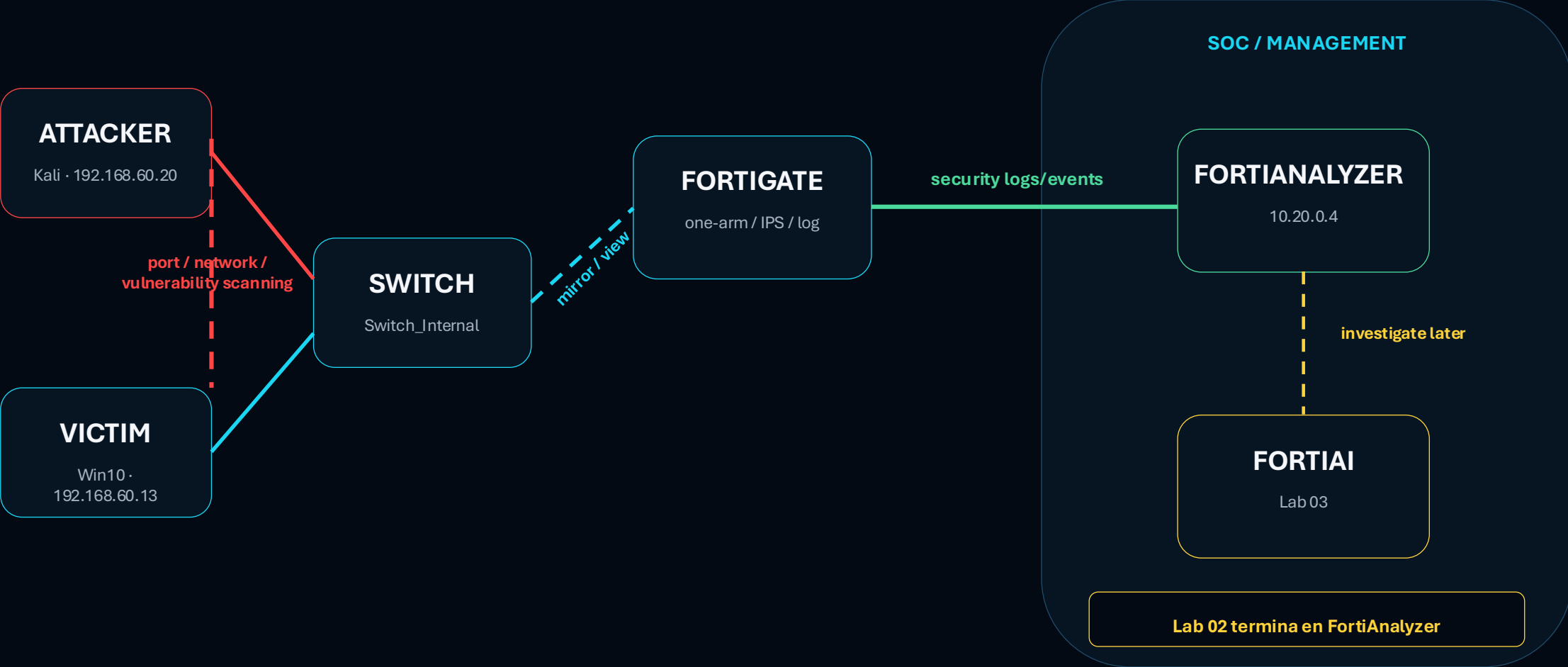
¿Cómo FortiGate apoya el análisis con FortiNDR?

SMB Scan

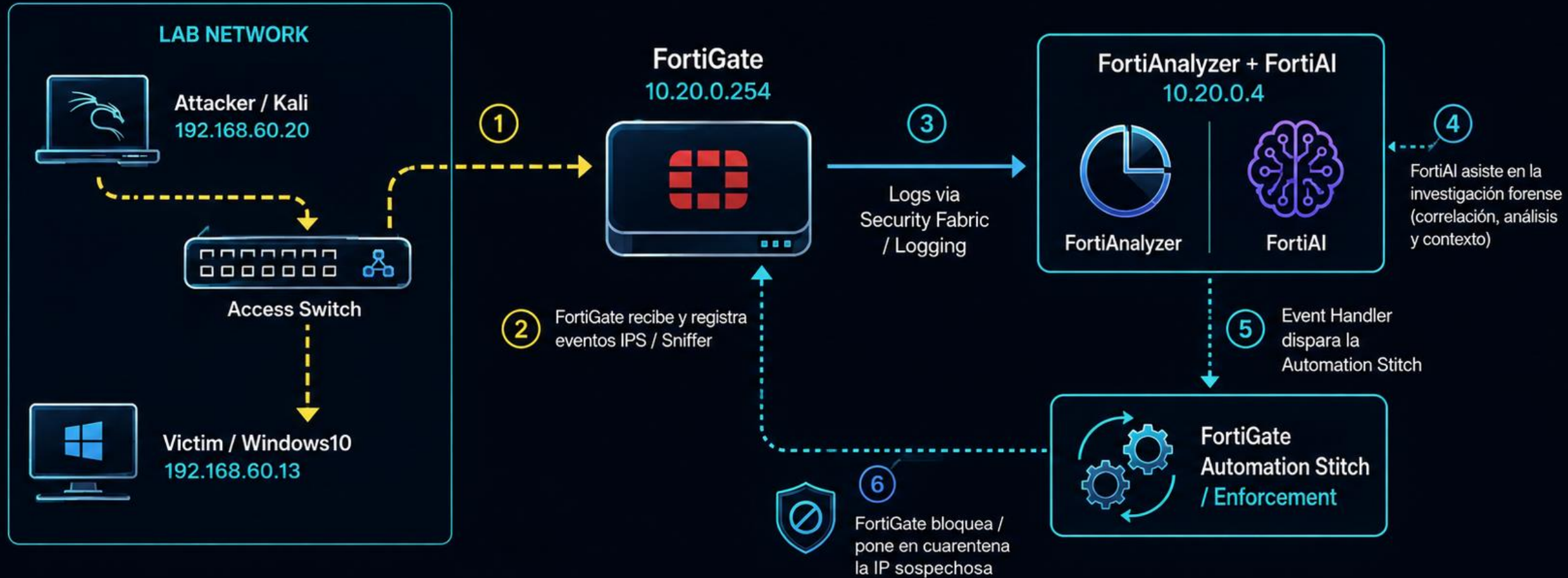
¿Cómo FortiNDR inspecciona archivos en el file server?

Lab 02 · Arquitectura enfocada

Generación de señales → logging → evidencia



Lab 03 · FortiAI + Event Handler + Automation Stitch



1

El atacante genera tráfico sospechoso interno hacia la víctima a través del Access Switch

2

FortiGate recibe y registra eventos IPS / Sniffer

3

Los logs se envían a FortiAnalyzer vía Security Fabric / Logging

4

FortiAI asiste en la investigación forense dentro de FortiAnalyzer

5

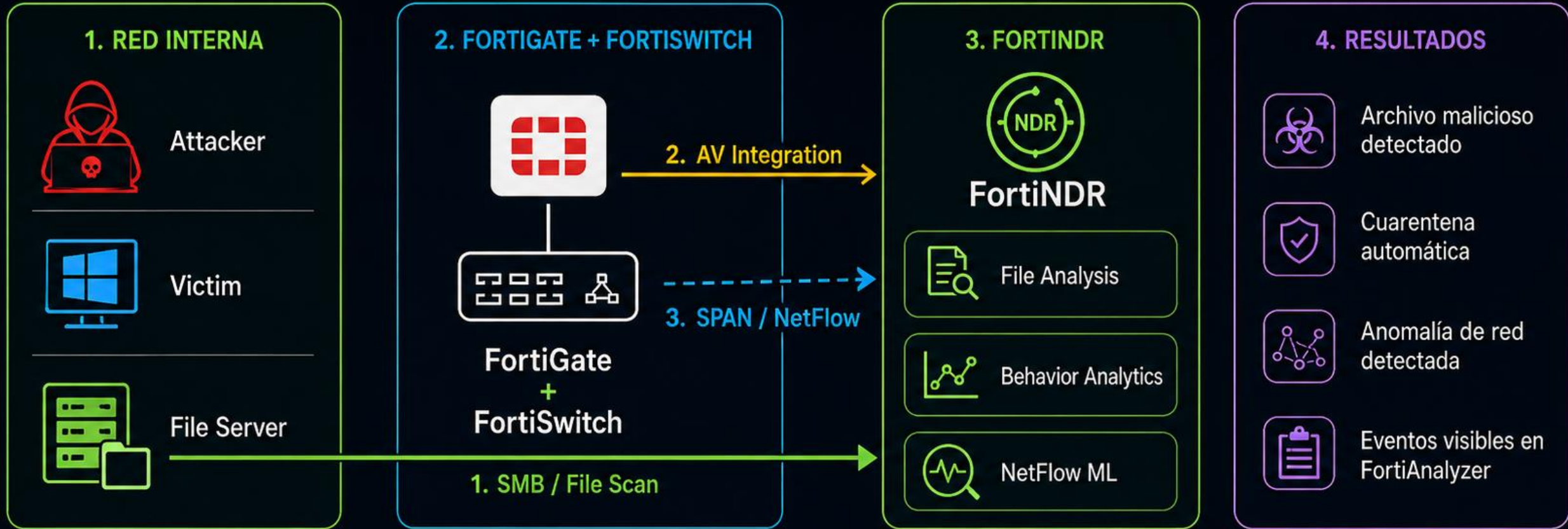
Event Handler dispara la Automation Stitch

6

FortiGate bloquea / pone en cuarentena la IP sospechosa

Lab 04 • Anomaly Detection by FortiNDR

Detección de archivos maliciosos y comportamiento anómalo



1



Archivo malicioso
en File Server

2



Archivo sospechoso
vía FortiGate

3



Tráfico anómalo /
NetFlow ML

Lab 05 Automated Response with FortiSOAR

Integración FortiNDR → FortiAnalyzer → FortiSOAR → FortiGate + Switch (Aislamiento automático)



FLUJO DEL LAB



RESULTADO ESPERADO

- ✓ Detección en FortiNDR
- ✓ Alerta en FortiAnalyzer
- ✓ Playbook ejecutado en FortiSOAR
- ✓ Host aislado automáticamente en FortiGate y FortiSwitch



Del evento a la decisión.

Andrés Piraján Aranguren

Andrés Pabón Ramirez

Systems Engineer - Colombia

La Oportunidad de SOC de Latinoamérica

La combinación de infraestructura, alcance y relación con el cliente crea una ventaja única para transformar capacidades existentes en servicios de seguridad gestionada y nuevas fuentes de crecimiento.

EL RECORRIDO: Tres soluciones que se acomodan a las necesidades y oportunidades



FortiAnalyzer *Punto de entrada*

Monetiza el data lake en SD-WAN o adquiere una oferta para el SMB
Muchos telcos ya tienen desplegado vía SD-WAN.



FortiSOC *Escala B2B*

El SOC Enterprise: SIEM+SOAR+ITDR+IA. Lo sostiene el músculo financiero del telco.



SOCaaS *Diferenciador*

Entrega 24/7 sin montar el turno: Fortinet opera, el telco vende.

Por qué es importante?

- ✓ **Infraestructura ya desplegada** Red, telemetría y FAZ ya pagados.
- ✓ **Relación y facturación** Factura cada mes; cuenta de confianza.
- ✓ **Soberanía de datos** Procesa y retiene dentro del país.
- ✓ **Músculo financiero** Capitaliza y amortiza la plataforma.
- ✓ **Capilaridad de red** Cobertura nacional

Pasar de vender conectividad a vender seguridad gestionada

FortiAnalyzer: Monetizar lo que ya compraste

El data lake unificado que ya se opera se convierte en la base de un servicio de SOC sin nueva infraestructura de fondo.



Lo que el FAZ ya hace



Data lake unificado: recolección central y fuente única de verdad.



Inteligencia nativa: FortiGuard Labs, detección de brotes, IoCs.



Automatización lista: XDR, SIEM y SOAR con contenido preconstruido.

Lo que significa para el negocio



Cero inversión de fondo

La plataforma ya está pagada; el costo marginal de habilitar el servicio es bajo.



Servicio SOC

Monitoreo turnkey 24/7 multi-tenant, un tier esencial listo para vender.

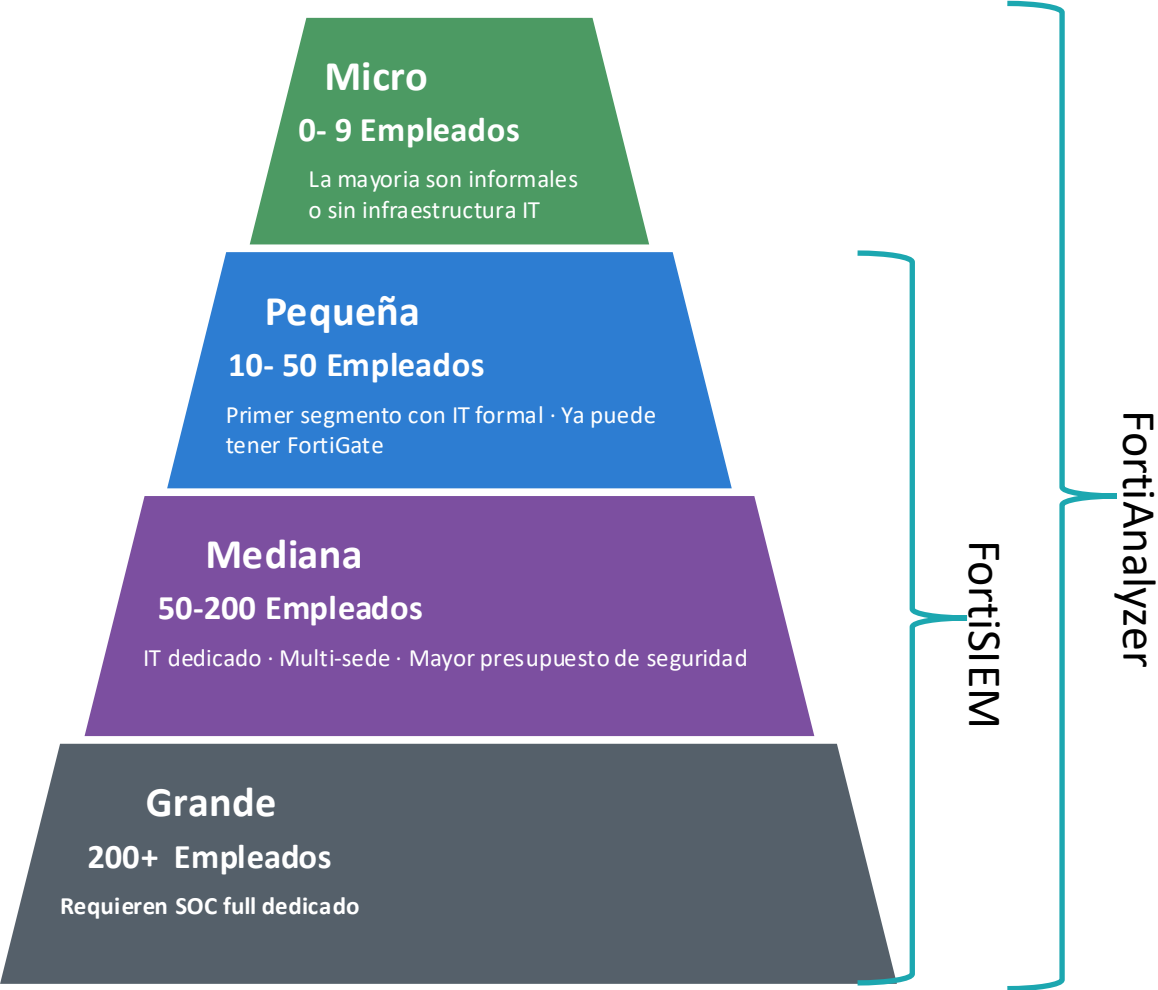


Diferenciador SD-WAN 3.0

Empaqueta seguridad gestionada con la conectividad: deja de competir solo por precio.

Resultado: la inversión inicial en FAZ obtiene un segundo retorno como línea de servicio.

Cientes Objetivo



SOC con FortiAnalyzer Sweet Spot

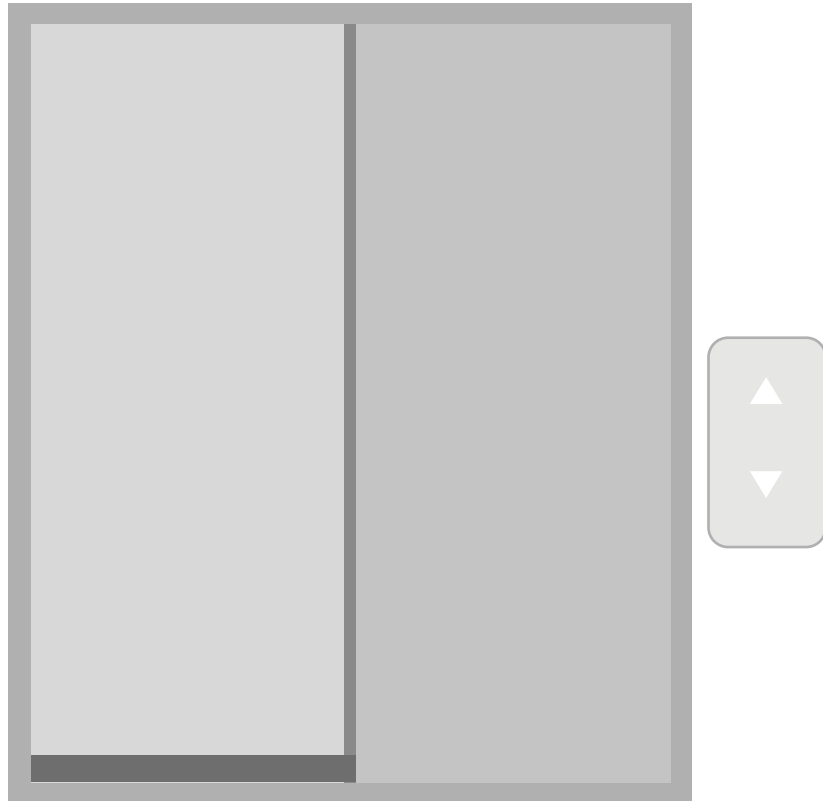
- Infraestructura IT formal
- Sin SOC dedicado → necesitan MSSP
- Cumplimiento (PCI-DSS, Lei 14.967, CNBV)
- Ya son clientes de conectividad / FW gestionado



- Laboratorios, farmacias
- Fintech y Cooperativas
- Fintech y Cooperativas

FortiAnalyzer Elevator Speech

▼ 88



Ya pagaste el data lake cuando compraste tu SD-WAN. Hoy solo lo usas para monitoreo interno (retención de logs); actívalo como servicio de SOC llave en mano para tu base o como un servicio premium de SD-WAN, y crea una nueva línea de ingreso recurrente sin invertir en infraestructura nueva.

¿Por qué SOCaaS?

Atendemos a más
de 2000 clientes.



37 Billion log events processed daily

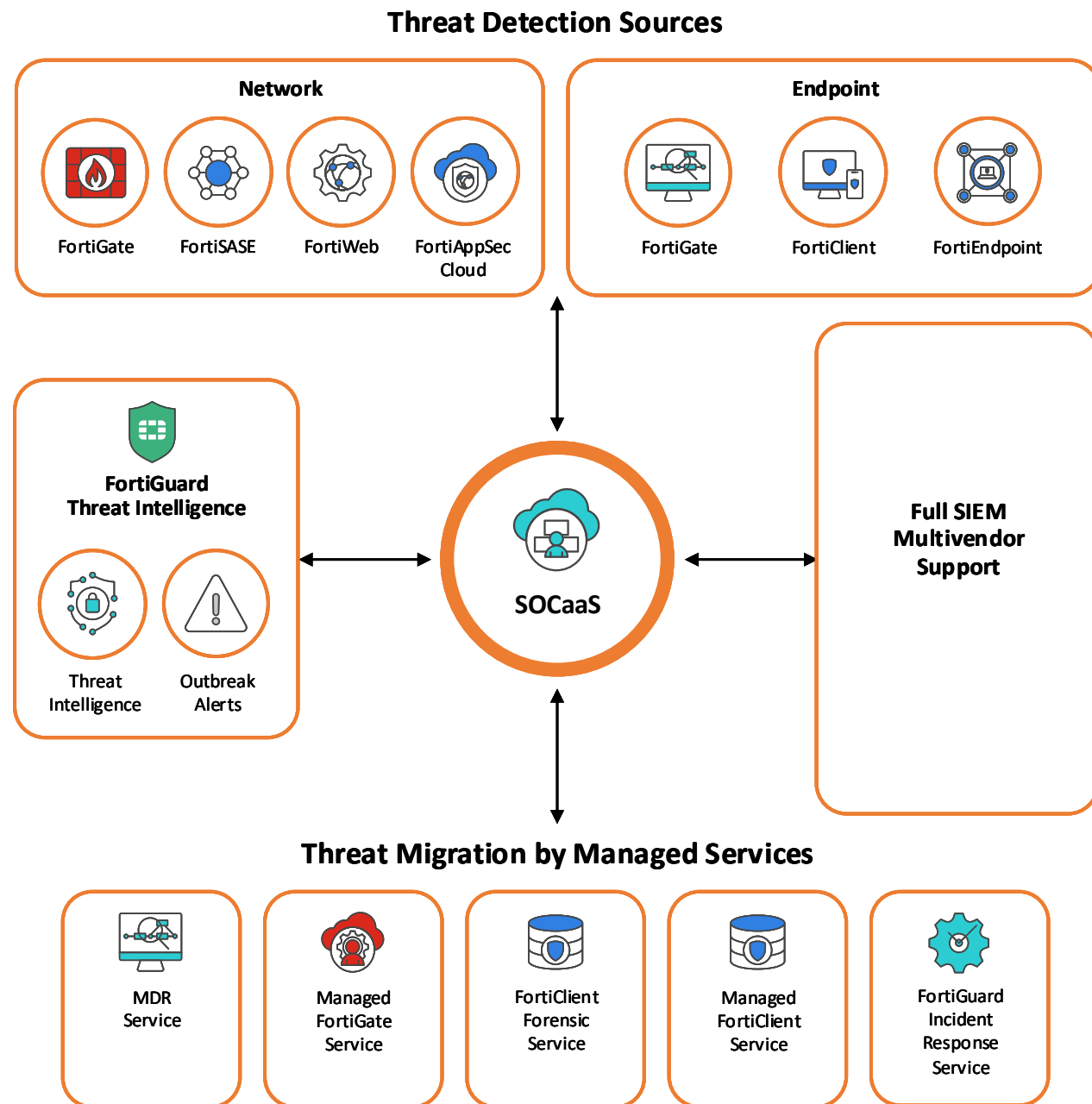
Security monitoring across cloud, endpoint, and network IT/OT sources

450+ alerts triaged daily

350+ incidents escalated per day

100,000 FortiSOAR playbooks daily

**New: Full multivendor sources
Monitoring & detection**



Beneficios de SOCaaS



Cobertura Continua

Manténgase al día con las amenazas, mejore o amplíe su sistema de operaciones de seguridad (SecOps) existente las 24 horas del día, los 7 días de la semana.



Reduzca costos y el agotamiento.

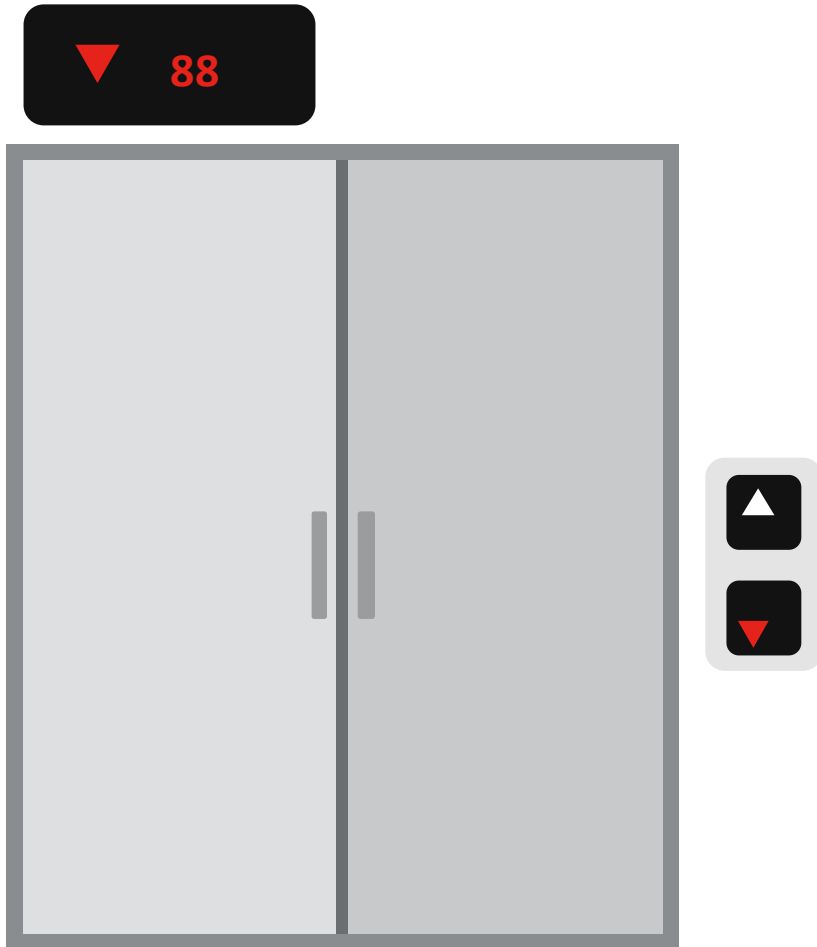
Ahorre costes y evite el agotamiento del equipo delegando tareas a expertos de Fortinet.



Seguridad simplificada

Maximice el retorno de sus inversiones en seguridad con resultados medibles.

FortiSOC Elevator Speech



Muchas empresas Enterprise necesitan capacidades de un SOC pero no cuentan con el personal ni el presupuesto para construir uno. FortiSOC permite ofrecer monitoreo continuo, detección de amenazas, investigación y respuesta desde una plataforma integrada con automatización e inteligencia artificial. Así, pueden entregar servicios de seguridad de nivel empresarial, acelerar el tiempo de respuesta y generar nuevas fuentes de ingresos recurrentes.



F**ORTINET**

COLOMBIA
& ECUADOR

XPERTS26