THE WHOLE PACKAGE

ALL IN ONE SECURITY

Faraday

Acerca de Faraday

En Faraday ayudamos a las organizaciones a **gestionar su exposición al riesgo real.**

Combinamos tecnología propia con talento ofensivo para **identificar, priorizar y validar** vulnerabilidades antes de que se conviertan en incidentes. La seguridad no se trata de escanear más, sino de entender qué es explotable y actuar primero sobre lo que realmente importa.

Sólo hay dos formas de encontrar una vulnerabilidad: La encuentras tú o la encuentra alguien más. **En Faraday elegimos encontrarla primero.**

Faraday

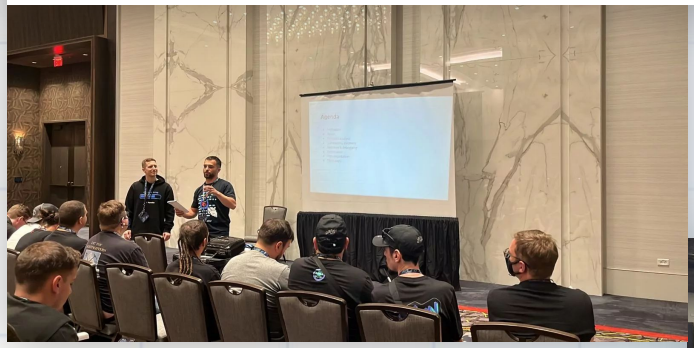
Presentación internacional

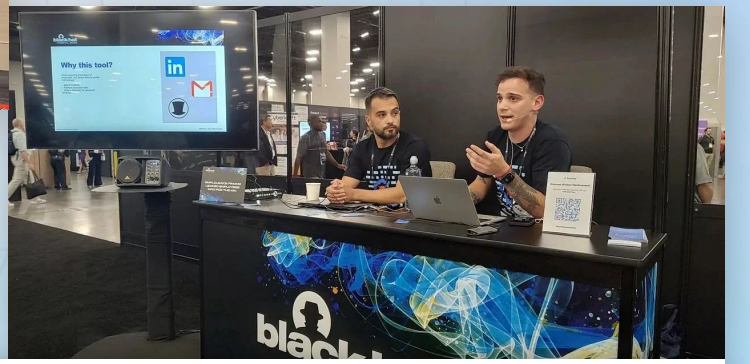
EKOPARTY SINCE 2001

TRAININGS 2025

DEF CON 32: Hackers argentinos exponen fallos de seguridad que afectan al menos a 500 mil routers DrayTek

- Se trata de una serie de problemas que pueden ser aprovechados para atacar redes corporativas y domésticas.
- Qué riesgos conlleva y cómo mitigarlos.





Black Hat USA 2025: presentan evilDoggie, un dispositivo para testear la seguridad de los autos modernos

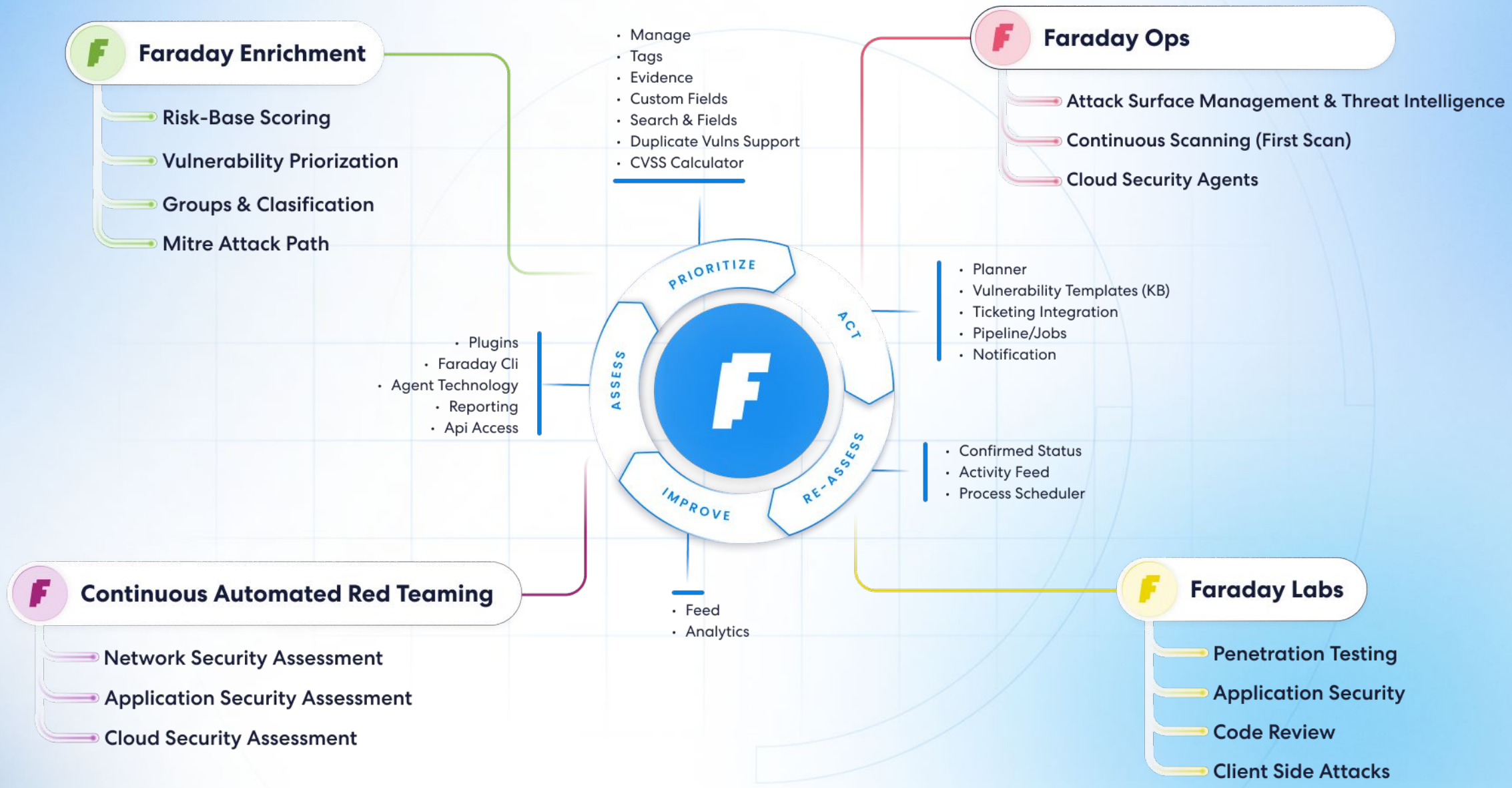
Día 2: dos argentinos hicieron un workshop para mostrar una herramienta de seguridad ofensiva automotriz. Además, el keynote de Nicole Perlroth y su llamado a la acción sobre la IA.

Faraday

¿Porque Faraday?

- **+20 años** combinando investigación, hacking ético y desarrollo de tecnología.
- Fundadores y speakers en conferencias como **DEFCON, Black Hat, and Ekoparty.**
- Investigación propia con **resultados publicados a nivel mundial.**
- ADN open-source y **enfoque ofensivo** desde el día uno.
- **Plataforma All-in-One** que integra ASM, PTaaS, VM y CyberSOC bajo un modelo de exposición continua.

Nuestros Servicios


Faradday Enrichment
Risk-Base Scoring
Vulnerability Priorization
Groups & Clasification
Mitre Attack Path
Manage
Tags
Evidence
Custom Fields
Search & Fields
Duplicate Vulns Support
CVSS Calculator
Faraday Ops
Attack Surface Management & Threat Intelligence
Continuous Scanning (First Scan)
Cloud Security Agents
PRIORITIZE
ACT
RE-ASSESS
IMPROVE
ASSESS
Plugins
Faraday Cli
Agent Technology
Reporting
Api Access
Planner
Vulnerability Templates (KB)
Ticketing Integration
Pipeline/Jobs
Notification
Confirmed Status
Activity Feed
Process Scheduler
Feed
Analytics
Continuous Automated Red Teaming
Network Security Assessment
Application Security Assessment
Cloud Security Assessment
Faraday Labs
Penetration Testing
Application Security
Code Review
Client Side Attacks

Pentest as a Service

Faraday

¿Sobre qué tecnologías trabajamos?

Nos enfocamos en las siguiente temáticas:

1. Pentesting Interno & Externo de Infraestructura.
2. Aplicaciones Web.
3. Nube (AWS, DO, GCP, Azure, Huawei).
4. Mobile (iOS & Android).
5. ATM (equipo de **research**).
6. Binarios y clientes de escritorio.
7. Campañas de Ingeniería Social.
8. Auditorías de Código Fuente.

¿Cómo lo podemos trabajar?

Esto queda a disposición del cliente para que elija una metodología *whitebox*, *greybox* o *blackbox*.

Faraday

Metodologías Cross-Service

Si bien para cada servicio el enfoque es diferente (negocio, impacto y riesgo), lo realizamos bajo una misma línea de trabajo:

1. Reconocimiento de la superficie (activos, puertos, servicios y de forma pasiva).
2. Entendimiento de la lógica de negocio.
3. Identificación de puntos de acceso e inyección.
4. Análisis de vulnerabilidades.
5. Fase de explotación *controlada*.
6. Impacto **ofensivo** (*¿hasta dónde puede llegar un atacante?*)
7. Entregables y plan de remediación.

La comunicación es constante. La visibilidad, en tiempo real.

Monitoreo continuo

Faraday

¿Qué es Continuous Scanning?

Tal como lo dice el nombre, corremos un set de herramientas elegidas por nosotros, donde buscamos identificar vulnerabilidades en distintos ambientes:

1. Internamente
2. Externamente
3. Aplicaciones Web
4. Infraestructura
5. Nube
6. Mobile

¿Qué le pedimos al cliente?

Acá podemos tomar 2 opciones, donde proponemos nosotros hacer un descubrimiento o bien, que el cliente nos pase su alcance.

Faraday

¿Qué herramientas usamos?

Combinamos herramientas para realizar un descubrimiento general de la infraestructura (de forma **pasiva** y **activa**) y un análisis de vulnerabilidades con un enfoque ofensivo.

1.

Reconocimiento pasivo

DNSdumpster / crt.sh / SecurityTrails → Recolección de subdominios, registros DNS públicos.

Shodan / Censys / zoomeye / FOFA → Búsqueda de servicios expuestos en internet.

Hunter.io / Email-Format.com / linkedint / crosslinked → Emails corporativos y estructura de naming.

theHarvester / Spiderfoot → Recopilación de OSINT automatizada.

Google Dorking → Recopilación de OSINT NO automatizada.

Subfinder / Assetfinder → Descubrimiento de subdominios de forma pasiva.

Amass (modo pasivo) → Mapeo de superficies externas.

Dig → AXFR.

Bagre / Emploleaks / intelx → Credenciales filtradas.

GrayHatWarfare → Plataforma para buscar buckets públicos en AWS y otros servicios cloud ya indexados.

Faraday

¿Qué herramientas usamos?

Combinamos herramientas para realizar un descubrimiento general de la infraestructura (de forma **pasiva** y **activa**) y un análisis de vulnerabilidades con un enfoque ofensivo.

2.

Reconocimiento activo / Enumeración

Nmap (con scripts NSE) → Detección de servicios, versiones, SO, firewall.

Masscan → Scaneo rápido de puertos a gran escala.

Naabu → Scaneo de puertos TCP simplificado y paralelo.

httpx → Validación de hosts HTTP activos.

testssl → Detección de certificados, algoritmos, vulnerabilidades en SSL/TLS.

WhatWeb / Wappalyzer CLI → Identificación de tecnologías web.

ffuf / dirsearch → Fuzzing de directorios y archivos web.

Chaos-Client → Cliente del proyecto Chaos (Assetnote) para acceder a grandes datasets de subdominios.

Sudomy → Herramienta OSINT multipropósito con enfoque en subdomain enumeration.

sub.sh → Script ligero y automatizado para subdomain discovery desde múltiples fuentes.

Massdns → Resolver ultra-rápido para validación masiva de DNS.

ShuffleDNS → Wrapper que combina resolución con wordlists y Massdns para mayor cobertura.

CloudBrute → brute-forcer de assets cloud como subdominios, buckets, entornos GCP/Azure, etc.

BBOT → All in one tool

WP-Scan → Scanner de WordPress

Faraday

¿Qué herramientas usamos?

Combinamos herramientas para realizar un descubrimiento general de la infraestructura (de forma **pasiva** y **activa**) y un análisis de vulnerabilidades con un enfoque ofensivo.

3.

Escaneo de Vulnerabilidades

Nuclei → Scaneo basado en templates (CVE, tech stack, headers, etc).

Nikto → Scanner web de configuraciones inseguras.

OpenVAS / Nessus → Vulnerability scanners generalistas.

Searchsploit / ExploitDB → Revisión de exploits disponibles.

Vulners / CVE Search APIs → Verificación de versiones vulnerables.

Faraday

¿Cómo es la infra que usamos?

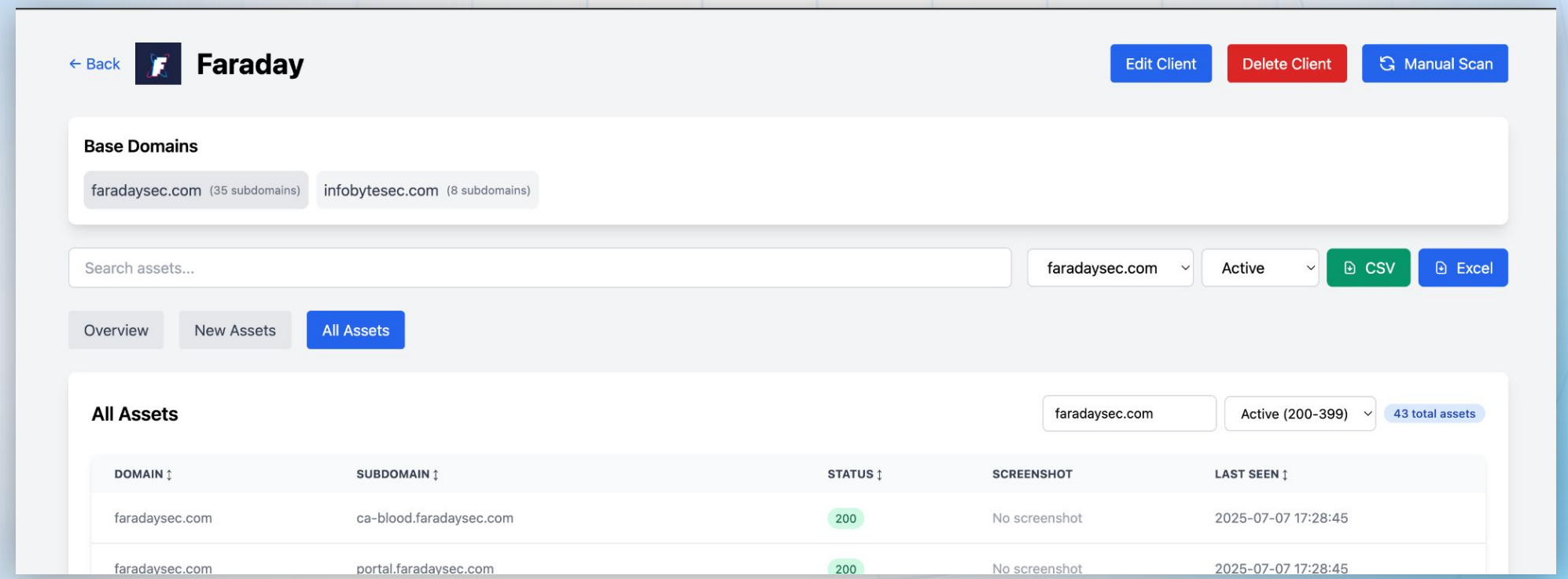
La arquitectura es relativamente simple, contando para la parte interna con un **servidor de scanning** y un colector central que es la plataforma de Faraday. Para la red externa, el servidor de **scanning es propio** y los resultados se almacenan en una instancia de la nube.

Attack Surface Managament

Faraday

¿De qué se trata el servicio?

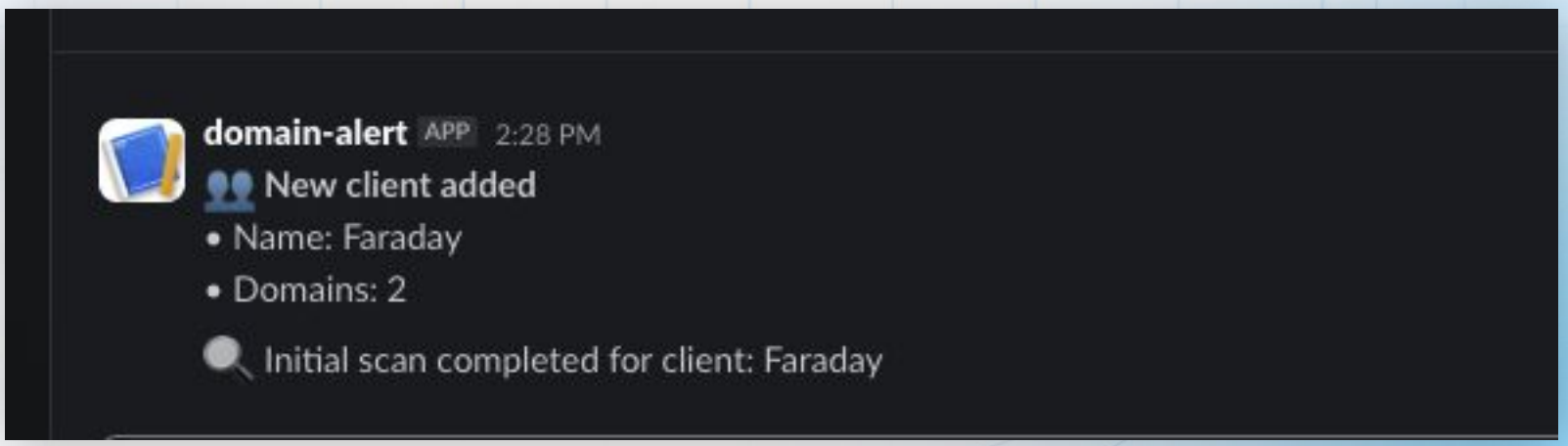
Dentro de este servicio nos enfocamos a hacer un relevamiento constante sobre lo que exponen **externamente.**
Hacemos la parte de descubrimiento constante (como así también de puertos y servicios externos).



Faraday

¿Qué buscamos?

Primero que nada, obtener nuevos subdominios de forma constante en base al **dominio base** del cliente. Este ejercicio corre **todos los días** y tiene múltiples integraciones para alertar automáticamente de que se descubrió algo nuevo.



Threat Intelligence

Faraday

¿De qué se trata el servicio?

Acá nos enfocamos a tareas de **inteligencia,** donde hacemos muchas tareas que no están relacionadas directamente con la búsqueda activa de vulnerabilidades, sino que es algo un poco más pasivo:

1. Recolección de credenciales filtradas en Internet.
2. Técnicas de *typosquatting* (en lugar de faradaysec.com, buscar faraadaysec.com)
3. Análisis de campañas de *phishing*.
4. Monitoreo de Marca (en redes sociales, portales de la *deep*)
5. Aplicaciones maliciosas simulando a la marca.

Offensive CyberSOC

¿De qué se trata el servicio?

En este caso, nos centramos en alguna tecnología que tenga el cliente de SIEM. Estos, recolectan información constantemente de servicios críticos de la empresa y mediante reglas de correlación el SIEM te permite detectar potenciales ataques en tiempo real.

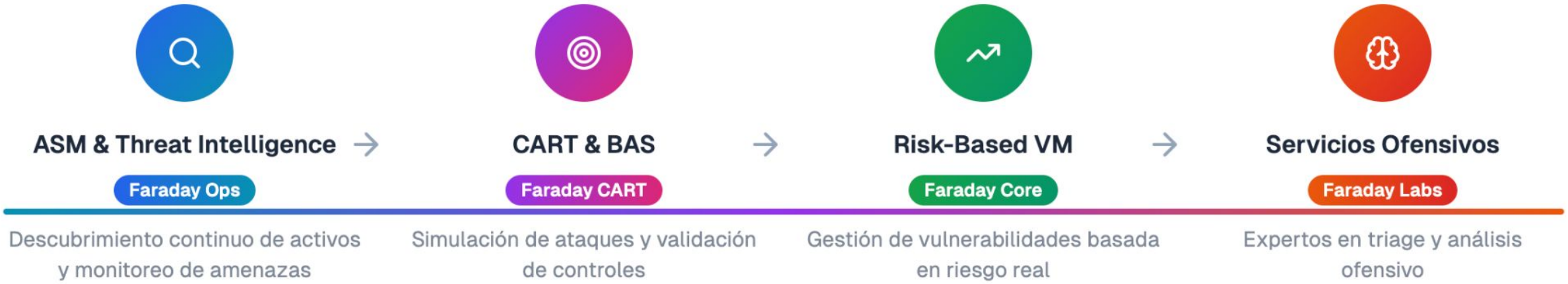
¿Cómo lo solemos trabajar?

Acá, tenemos que entender cuáles son los riesgos de los clientes, saber qué están monitoreando y en base a eso nosotros tomar decisiones. En nuestro caso de éxito, donde nosotros le damos un soporte activo a su plataforma llamada **QRadar**, y logramos bajar una cantidad de **~30** alertas por día, a **~10** por semana.

Faraday

El proceso OSOC y sus módulos

Un enfoque integrado que combina detección, simulación y remediación para una seguridad ofensiva completa



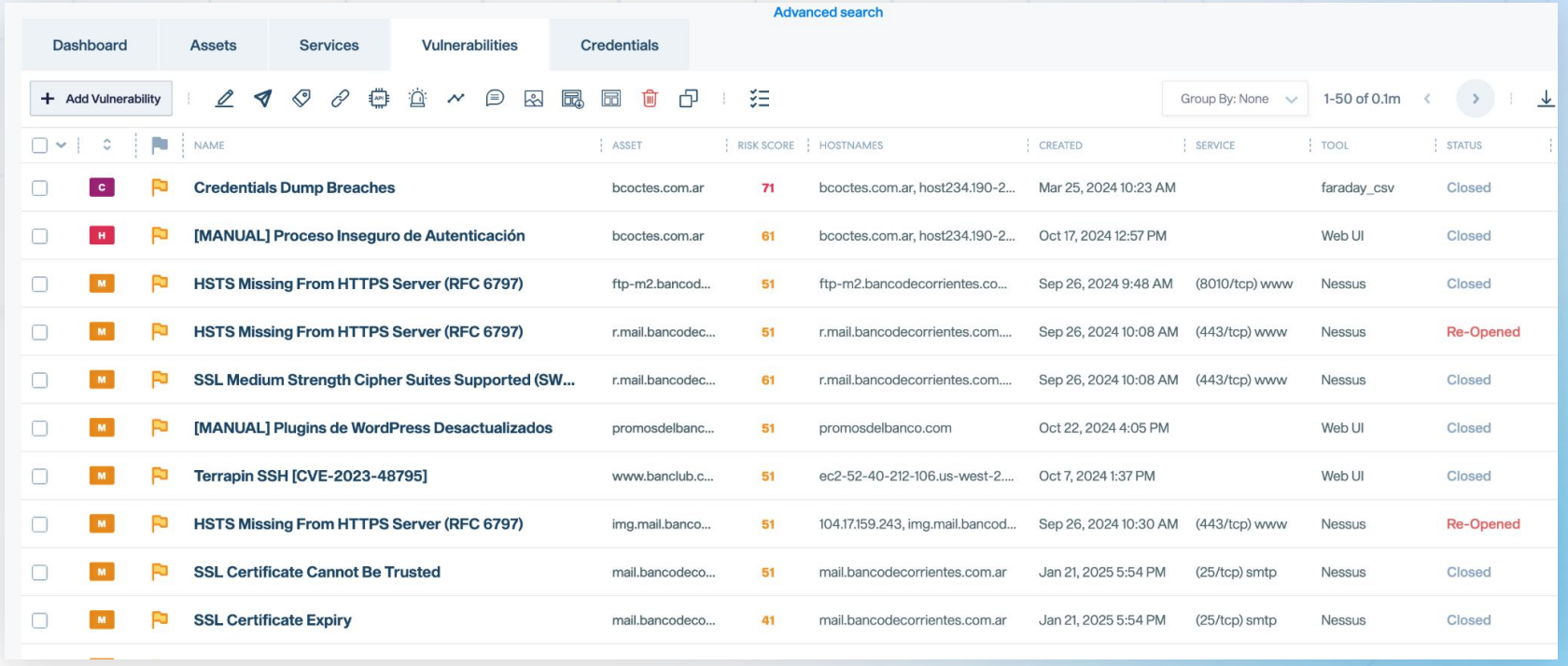
Postura de Seguridad Ofensiva Mejorada

All in One

¿De qué se trata el servicio?

Sí, básicamente es todo lo que vimos antes (sumandole **Pentest as a Service**). También, para hacer el *delivery* continuo utilizamos nuestra plataforma Faraday.

¿Cómo es que se visualiza la información?

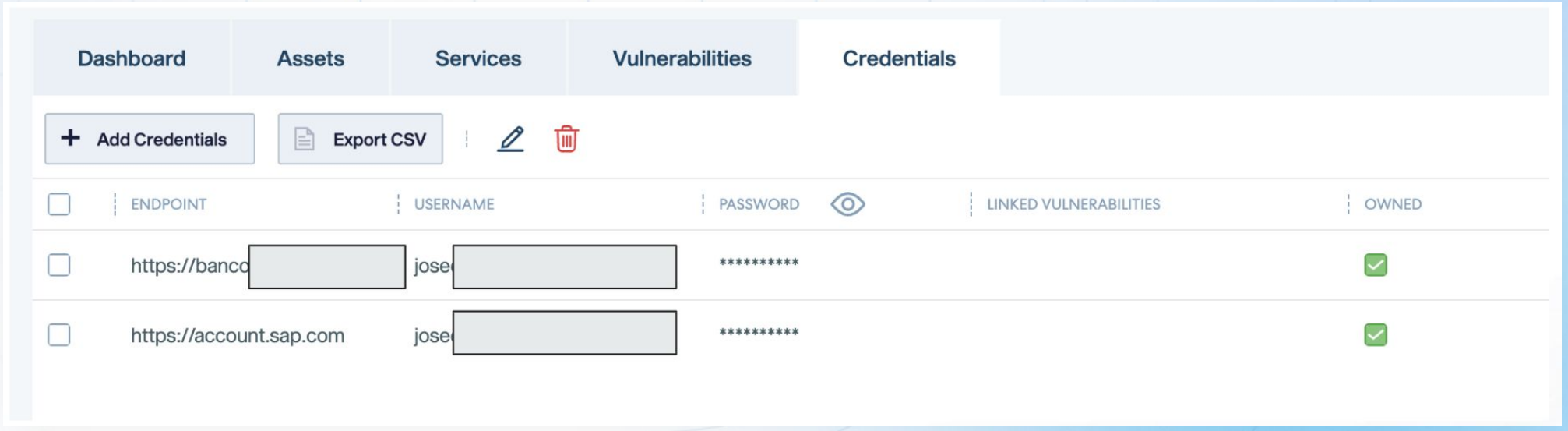


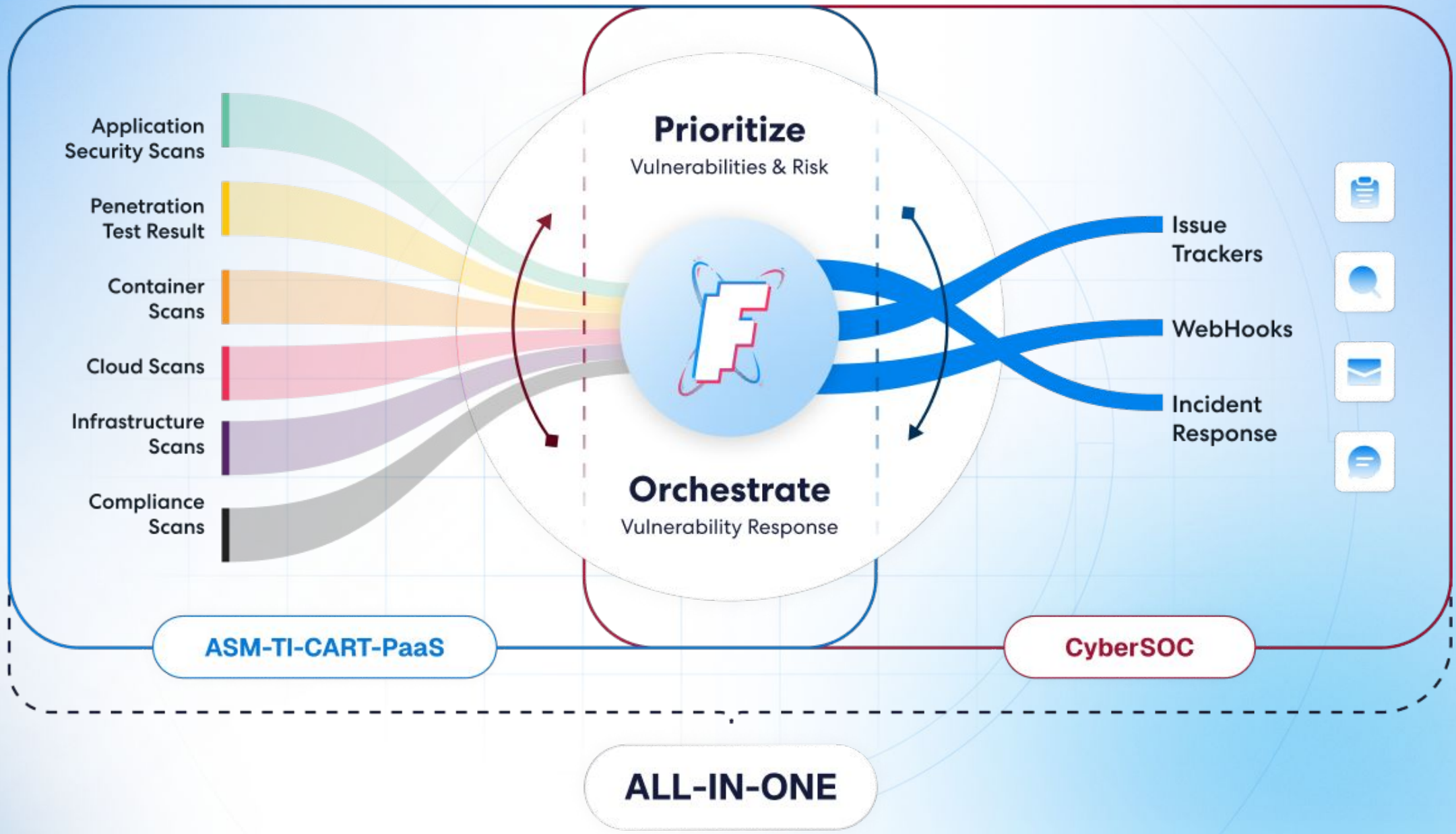
	NAME	ASSET	RISK SCORE	HOSTNAMES	CREATED	SERVICE	TOOL	STATUS
C	Credentials Dump Breaches	bcoctes.com.ar	71	bcoctes.com.ar, host234.190-2...	Mar 25, 2024 10:23 AM		faraday_csv	Closed
H	[MANUAL] Proceso Inseguro de Autenticación	bcoctes.com.ar	61	bcoctes.com.ar, host234.190-2...	Oct 17, 2024 12:57 PM		Web UI	Closed
M	HSTS Missing From HTTPS Server (RFC 6797)	ftp-m2.bancod...	51	ftp-m2.bancodecorrientes.co...	Sep 26, 2024 9:48 AM	(8010/tcp) www	Nessus	Closed
M	HSTS Missing From HTTPS Server (RFC 6797)	r.mail.bancodec...	51	r.mail.bancodecorrientes.com....	Sep 26, 2024 10:08 AM	(443/tcp) www	Nessus	Re-Opened
M	SSL Medium Strength Cipher Suites Supported (SW...	r.mail.bancodec...	61	r.mail.bancodecorrientes.com....	Sep 26, 2024 10:08 AM	(443/tcp) www	Nessus	Closed
M	[MANUAL] Plugins de WordPress Desactualizados	promosdelbanc...	51	promosdelbanco.com	Oct 22, 2024 4:05 PM		Web UI	Closed
M	Terrapin SSH [CVE-2023-48795]	www.banclub.c...	51	ec2-52-40-212-106.us-west-2....	Oct 7, 2024 1:37 PM		Web UI	Closed
M	HSTS Missing From HTTPS Server (RFC 6797)	img.mail.banco...	51	104.17.159.243, img.mail.bancod...	Sep 26, 2024 10:30 AM	(443/tcp) www	Nessus	Re-Opened
M	SSL Certificate Cannot Be Trusted	mail.bancodeco...	51	mail.bancodecorrientes.com.ar	Jan 21, 2025 5:54 PM	(25/tcp) smtp	Nessus	Closed
M	SSL Certificate Expiry	mail.bancodeco...	41	mail.bancodecorrientes.com.ar	Jan 21, 2025 5:54 PM	(25/tcp) smtp	Nessus	Closed

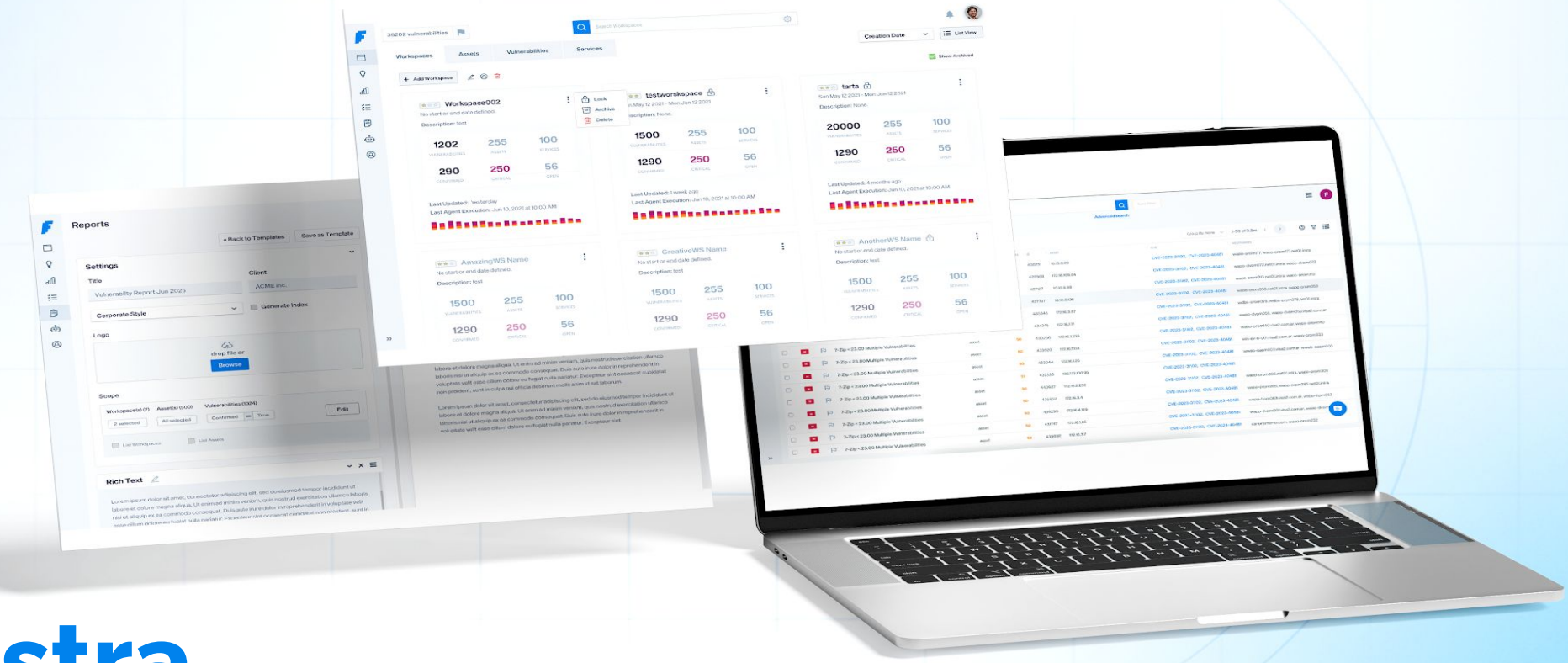
¿De qué se trata el servicio?

Sí, básicamente es todo lo que vimos antes (sumandole **Pentest as a Service**). También, para hacer el *delivery* continuo utilizamos nuestra plataforma Faraday.

¿Cómo es que se visualiza la información?




Application Security Scans
Penetration Test Result
Container Scans
Cloud Scans
Infrastructure Scans
Compliance Scans
Prioritize
Vulnerabilities & Risk
Orchestrate
Vulnerability Response
Issue Trackers
WebHooks
Incident Response
ASM-TI-CART-PaaS
CyberSOC
ALL-IN-ONE

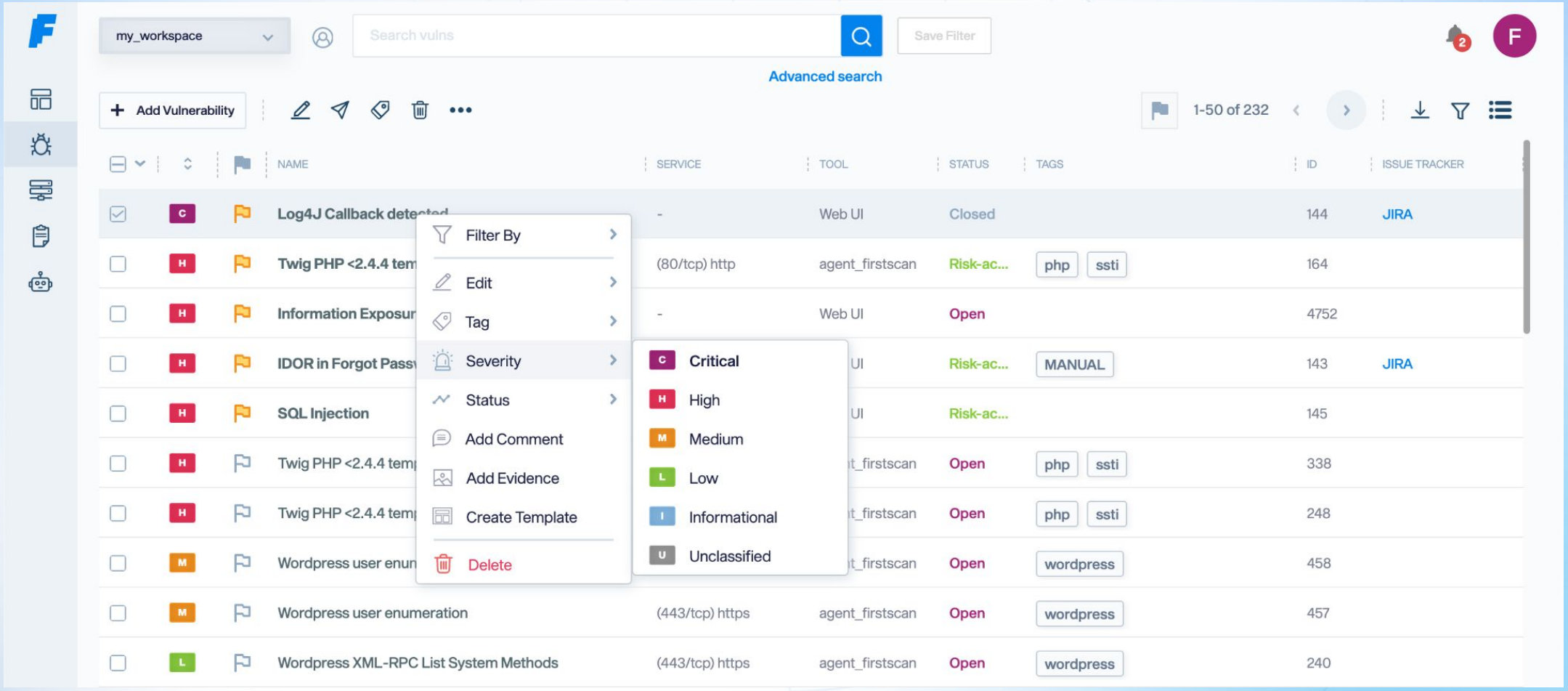


Nuestra Platforma

+180 Integraciones

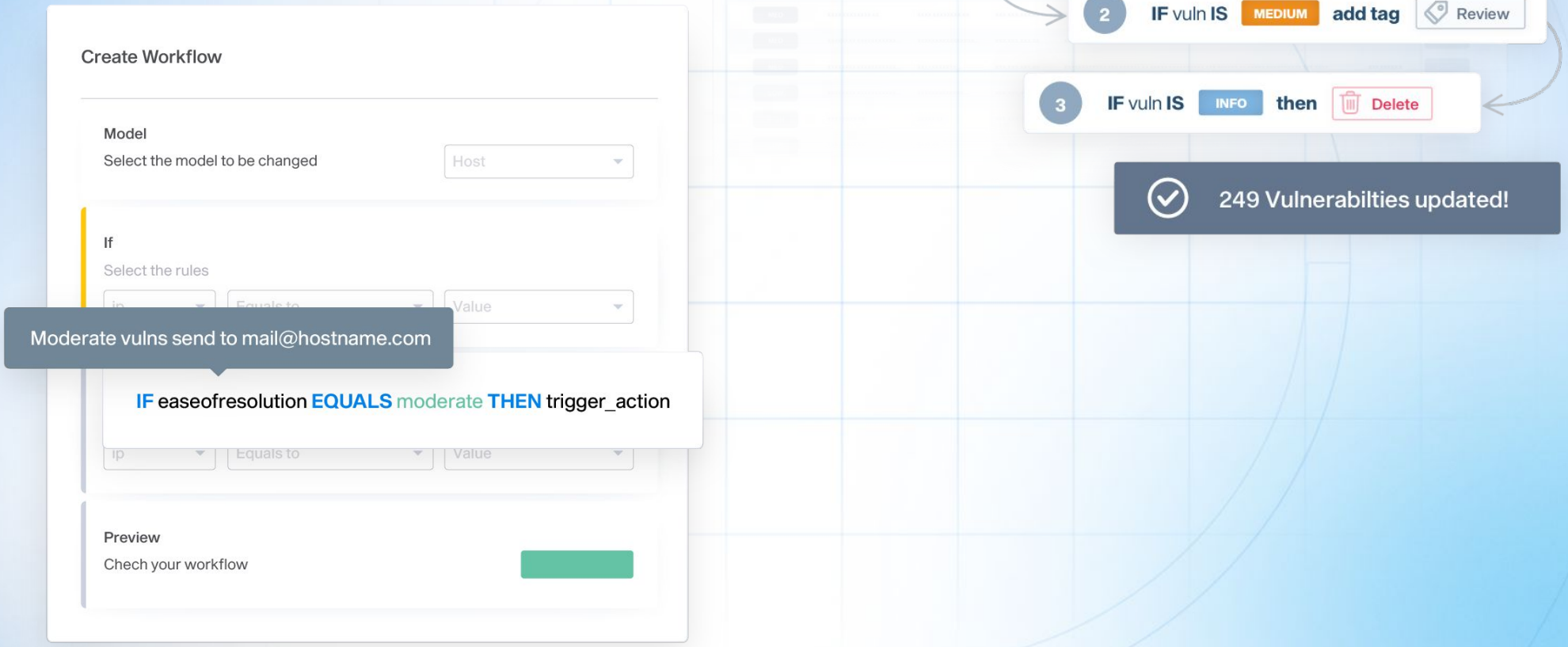
Faraday

Seguimiento de Riesgos y Triaje



Faraday

Automatización de tareas



Jira

servicenow

Faraday

+180 Integraciones

No nos oponemos al uso de otras herramientas, **lo facilitamos.**

Explora todas las Integraciones

Faraday

Clientes que confían en nosotros

@faradaysec

company/faradaysec

www.faradaysec.com