RAIJU DDoS

1. Cómo funciona

Raiju DDoS combina descubrimiento de infraestructura, simulación de ataques DoS/DDoS y generación de informes para mostrar, con datos, cómo responden las defensas configuradas y qué hay que mejorar.

La plataforma incorpora módulos de IA desde su diseño y registra las acciones durante las auditorías para asegurar trazabilidad completa.

Descubrimiento y validación de activos Verificación automática de dominios y servicios expuestos relevantes para DDoS, creando un mapa de activos priorizados según nivel de riesgo y exposición.	**Selección de escenarios de ataque** Con el mapa de activos, se seleccionan escenarios de ataque DoS/DDoS. Aportando al usuario una visión completa de riesgos potenciales según tipo de ataque
Configuración de Pruebas Permite personalizar y ajustar las pruebas que realmente de necesitan. Definiendo intensidad, duración, número de conexiones y ventanas horarias, ahorrando tiempo de configuración.	**Ejecución controlada y trazabilidad total** Lanza las simulaciones dejando constancia de usuarios y acciones para trazabilidad en las auditorías, teniendo el control de “quién, cuándo, cómo y contra que”.
Informes automáticos Genera métricas sobre las pruebas realizadas y estructura el resultado en informes configurables. Ordenando la información más relevante, reduciendo tiempos de preparación y análisis.	**De prueba puntual a validación continua** Permite repetir operaciones y pruebas tantas veces como sea necesario sin tener que volver a configurar la herramienta.

2. Servicio de auditoría a ofrecer

Fase 1 · Alcance y preparación Definición de activos, ventana autorizada, contactos, salvaguardas y criterios de parada. Se recomienda una reunión de kick-off y checklist previa.	**Fase 2 · Diseño de escenarios** Selección de vectores y campañas en función del activo: volumétricos, pps, low-and-slow, DNS, web/TLS o servicio específico.
Fase 3 · Ejecución controlada Lanzamiento supervisado, monitorización con Heartbeat y coordinación con cliente/NOC/SOC para verificar disponibilidad, degradación y mitigación.	**Fase 4 · Análisis y cierre** Interpretación de resultados, priorización de hallazgos, readout ejecutivo/técnico y propuesta de re-test o programa recurrente.

3. Tipos de auditorías

Servicio	Qué evalua	Qué incluye
Auditoría de Resiliencia ante DoS/DDoS	Evaluación controlada para medir la capacidad de la infraestructura frente a ataques DDoS. Incluye: • Descubrimiento y validación de activos expuestos. • Identificación de superficies de ataque • Simulación de ataques volumétricos, protocolarios y de capa 7. • Validación de controles de mitigación. • Informe de brechas y recomendaciones.	Constaría de 5-7 tipos de ataque cubriendo tipos de ataque volumétrico, Protocolario, DNS, paquetes malformados, capa 7 y ataques combinados. Cada prueba se realiza 3 veces para validar el ataque con niveles de carga bajo, medio y alto, para validación de capacidad de absorción, rate limiting, scrubbing y protección perimetral.

Servicio	Qué evalua	Qué incluye
Validación de Eficacia de Mitigaciones DDoS	Pruebas para verificar si los controles de protección realmente funcionan. Validación de: • Sistemas anti-DDoS • Firewalls • WAF • Rate limiting • Sistemas de scrubbing • Balanceadores y protección cloud	Se realizan pruebas con enfoque según protocolo, volumétrico, capa 7 y DNS. En cuanto a la carga se realiza mínimo 3 veces con niveles de carga bajo, medio y alto, pudiendo repetir pruebas, probando configuraciones distintas de los equipos a validar para evaluar la protección de los mismos.
Continuous DDoS Validation as a Service (DVaaS)	Validación continua gestionada **como servicio o como licencia**. Este servicio está enfocado para realizar pruebas programadas trimestrales/semestrales, simulación de escenarios, detección de degradaciones y reporting automático en la plataforma.	Se realizaría un plan de pruebas con 3 ataques fijos y 1 o 2 rotativos que van variando en cada prueba. Los ataques fijos de tipo volumétrico y de protocolo y rotando pruebas de aplicación (DNS), paquetes malformados y slow-rate attack. Se realizarían con 2 niveles de carga, bajo y alto para evaluar la seguridad ante cambios en la infraestructura y campañas semestrales de seguridad.
Red Team DDoS Simulation	Simulación avanzada de ataques realistas con escenarios de ataque. Incluye: • Diseño de escenarios personalizados • Ejecución controlada • Trazabilidad completa • Informe técnico y ejecutivo	Se realizan: SYN Flood, TCP/UDP Flood, DNS Amplification, HTTP/HTTPS Flood, Low&Slow (Slowloris), Multi-vector attacks. Este plan de pruebas se realiza con nivel bajo y/o medio de carga ya no se busca evaluar en nivel de carga soportado, si no la escalabilidad de este tipo de ataques.
Auditorías para certificaciones y normativas.	Facilita el cumplimiento regulatorio y de estándares de ciberseguridad con auditorías DoS completas y reportes generados mediante IA. Incluye descubrimiento de infraestructura, ejecución de ataques controlados e informes para presentarse a departamentos de auditoría interna de la organización.	Personalizado según necesidades de la certificación.
Formación y simulacros para SOC Training (como idea)	Ejercicios de simulacro realizando ataques controlados para evaluar la gestión de incidentes por parte del personal del SOC.	Personalizado según necesidades de la formación.

4. Entregables y cierre al cliente

Resumen ejecutivo	Informe técnico

Conclusiones, impacto observado, activos prioritarios, mensaje de riesgo y quick wins para dirección o patrocinador del servicio.	Campañas ejecutadas, cronología, comportamiento de mitigación, métricas relevantes y recomendaciones accionables.
Paquete de evidencias Capturas, exportaciones, referencias de campañas, datos de Heartbeat y trazabilidad de ejecución.	**Sesión de readout** Reunión ejecutiva/técnica para explicar resultados, resolver dudas y acordar re-test o plan continuo.

5. Tiempos orientativos y modelos de servicio

Servicio	Qué incluye	Tiempo orientativo
Onboarding y configuración	Alta de cliente, usuarios, roles, 2FA, proyecto, naming, gobierno básico y guía de acceso.	2–4 h
Formación funcional	Sesión de adopción para equipos de red, seguridad o gestión: flujo de uso, buenas prácticas, lectura de resultados y operación segura.	3–4 h
Assessment inicial	Descubrimiento y validación de dominios, subdominios y servicios expuestos; revisión manual de alcance y priorización de activos. Planning de pruebas a realizar.	3–4 h
Auditoría estándar	Diseño de campañas, configuración de pruebas, ejecución supervisada, war-room y captura de evidencias.	1 día
Auditoría ampliada	Auditoría estándar con más activos y con mayor número de pruebas y de ataques combinados para poner a prueba los sistemas de seguridad	2-3 días
Informe y readout	Resumen ejecutivo, detalle técnico, matriz de hallazgos, recomendaciones y sesión de devolución con próximos pasos.	0,5–1,5 días
Re-test / validación continua	Repetición selectiva de campañas tras remediación o cambios en la defensa para demostrar mejora continua. *Incluye informe	0,5–1 día
Servicio recurrente	Prueba de validación continua periódica. Con un plan de pruebas personalizado, informe de ejecutivo e informe técnico con el seguimiento periódico de las pruebas realizadas.	0,5–1 día (Mensual / trimestral)

Referencias operativas observadas: análisis automático de subdominios en torno a 5–10 min, duración típica de prueba de 2 min ampliable hasta 20 min, arranque de contenedores de ataque de 20–30 s y generación automática de informe por IA en unos 5 min.

Nota comercial: Las auditorías son totalmente personalizables en cuanto a número de ataques y tipo de los mismos.

Una auditoría estándar serían 12-15 ataques con 3 niveles de carga en cada uno.

Anexo: Tipos de ataques soportados

DNS:
- DNS WATER TORTURE
- DNS INVALID PAYLOAD FLOOD
- DNS QUERY FLOOD
- DNS MIX QUERY-TYPE EXISTANT FLOOD
- DNS MIX QUERY-TYPE NON EXISTANT FLOOD

ICMP:
- ICMP FRAG FLOOD
- ICMP PULSE WAVE DDOS
- ICMP ECHO REPLY FLOOD
- ICMP RANDOM PACKET FLOOD
- ICMP PING OF DEATH
- ICMP BLIND PING FLOOD
- ICMP TIME EXCEEEDED FLOOD
- ICMP FLOOD
- ICMP REDIRECT FLOOD
- ICMP PARAMETER PROBLEM FLOOD
- ICMP UNREACHABLE FLOOD
- ICMP Targeted Local

SIP:
- Sip Register FLOOD
- Sip Options FLOOD
- Sip Invite FLOOD

Other:
- Blacknurse Attack
- Sctp Abort Shutdown FLOOD
- Asp Session Open FLOOD
- Dccp Request FLOOD
- Sctp Init FLOOD
- Netbios Session FLOOD
- Sctp Out Of Bounds
- Adsp Connection FLOOD
- X225 Connection FLOOD
- X225 Synchronization Abuse
- Socks5 Auth Exhaustion
- Scp Virtual Session FLOOD
- SOCKS Connection FLOOD
- Zip Dos Query FLOOD
- X225 Session FLOOD
- Sockstress Attack
- Mqtt Connect FLOOD
- Amqp Large Message Dos
- Grpc FLOOD
- Ssh Login FLOOD
- Smtp Auth FLOOD
- Redis Memcached Abuse
- Smtp Helo FLOOD
- Amqp Connection Exhaustion
- Websocket FLOOD
- Soap FLOOD
- Ldap Bind FLOOD
- Graphql Introspection Dos
- Webrtc Data Abuse
- Rpc FLOOD
- Coap Observe Exhaustion
- Webrtc Signaling FLOOD
- Tiny Fragments Attack

VPN:
- GRE FLOOD
- IPSEC FLOOD
- AH FLOOD
- IKE FLOOD
- ESP FLOOD
- GRE UDP FLOOD

IP:
- IP UNKNOWN PROTOCOL FRAG FLOOD
- IP UNKNOWN RANDOM PROTOCOL FLOOD
- IP UNKNOWN PROTOCOL FLOOD
- Fragment Reassembly Timeout
- Overlapping Fragments Attack
- Tiny Fragments Attack

SLOW:
- SLOWLORIS RANGE
- SLOWLORIS RUDY
- SLOWLORIS READ
- SLOWLORIS HEADER

SSL/TSL:
- SSL CIPHER SUITE ATTACK
- SSL EXHAUSTION FLOOD ATTACK
- MALFORMED SSL PACKETS FLOOD
- SSL TLS HANDSHAKE FLOOD
- MALFORMED TLS DTLS RECORDS FLOOD
- DTLS MALFORMED FLOOD
- Adsp Connection FLOOD
- X225 Connection FLOOD
- SSL TLS RENEGOTIATION FLOOD
- SSL TLS SESSION RESUMPTION FLOOD
- TLS WEBDDOS - SINGLE KNOWN FINGEPRINT (Multiple Browsers)
- TLS WEBDDOS - RANDOMIZED UNKNOWN FINGEPRINT
- TLS WEBDDOS - SINGLE KNOWN FINGEPRINT
- TLS WEBDDOS – SING

TCP:
- TCP INVALID FLAGS FLOOD
- TCP RANDOM PACKET SIZE FLOOD
- TCP ACK FLOOD
- TCP SYN FLOOD
- SHREW ATTACK
- TCP FIN ACK FLOOD
- TCP FRAG RANDOM SIZE FLOOD
- TCP FRAG DELAYED SINGLE RANDOM PORT FLOOD
- TCP FRAG DELAYED X RANDOM PORTS FLOOD
- TCP DELAYED SINGLE RANDOM PORT FLOOD
- TCP DELAYED X RANDOM PORTS FLOOD
- TCP FRAG FLOOD
- XMAS ATTACK
- TCP RANDOM PORTS FLOOD
- TCP SYN ACK FLOOD
- TCP STATE EXHAUSTION FLOOD
- TCP RST FLOOD
- GENERIC CONNECTION FLOOD

UDP
- UDP RANDOM PACKET SIZE FLOOD
- UDP LONG BURST FLOOD
- UDP RANDOM PORTS FLOOD
- UDP DELAYED SINGLE RANDOM PORT FLOOD
- UDP FRAG DELAYED SINGLE RANDOM PORT FLOOD
- UDP FRAG DELAYED X RANDOM PORTS FLOOD
- Sctp Out Of Bounds
- Adsp Connection FLOOD
- X225 Connection FLOOD
- UDP DELAYED X RANDOM PORTS FLOOD
- UDP SHORT BURST FLOOD
- UDP FLOOD
- UDP FRAG RANDOM PACKET SIZE FLOOD
- UDP FRAG FLOOD

WEB:
- HTTP GET FLOOD
- HTTPS POST FLOODER
- ZHTTPS GET FLOOD