DOCUMENTOS SiC
Nº 33
JUNIO 2021

RASP-IAST-SCA, LA TRIPLE APUESTA

Seguridad de Aplicaciones Unificada

Hdiv
BORN SECURE

Foto: Niko Iturralde

DevSecOps: la nueva forma de 'securizar' el software a la velocidad que exige el negocio

Daniel López
Sales Manager Hdiv Security

Detección temprana y precisa de vulnerabilidades en todo el SDLC

Protección de aplicaciones web y APIs en todo tipo de despliegues (*cloud* y *onpremise*)

La experiencia del cliente: automatizar procesos y reducir costos

ENTREVISTA

Roberto Velasco

CEO y Cofundador
Hdiv Security

Hdiv
BORN SECURE

Desde su fundación en 2016 se ha convertido en uno de los referentes mundiales en DevSecOps

Protegiendo las aplicaciones por defecto y a lo largo de su ciclo de vida

En sólo cinco años, la donostiarra Hdiv se ha hecho un hueco en el mercado global de soluciones de autoprotección (RASP) y detección de vulnerabilidades (IAST) gracias a una tecnología orientada a garantizar la seguridad de las aplicaciones heredadas o nuevas (a lo largo de su ciclo de vida) de forma fácil y en cualquier entorno, ya sea local o en nube. Prueba de ello es que entre sus clientes están algunos de los bancos y agencias federales más importantes de EE.UU., y una de las principales agencias de viaje a nivel internacional.

El mundo funciona gracias al software. Toda empresa u organización desarrolla software a medida de alguna u otra forma, ya sea creando código propio o consumiendo librerías *open-source* de terceros. Lo que resulta una herramienta imprescindible para nuestra vida digital y el negocio, sin embargo, también es el origen de gran parte de los incidentes de ciberseguridad que registran muchas compañías.

Se ha llegado a constatar en varias investigaciones que hasta siete de cada 10 aplicaciones presentan alguna vulnerabilidad por haberse enviado a producción sin la seguridad adecuada, primando la velocidad del negocio.

Para ayudar a las empresas a proteger las aplicaciones han surgido en los últimos años las herramientas de seguridad RASP (Runtime Application Self-Protection), que ganan cada vez más mercado por su eficacia ante las tradicionales soluciones WAF (Web Application Firewalls), según Gartner. ¿La razón? Permiten hacer frente de forma diferente y más acorde a la complejidad de las nuevas ciberamenazas.

Sede de Hdiv en Guipuzcoa.

Mercado internacional

Una situación que, de forma visionaria, supieron ver dos ingenieros donostiarras, Roberto Velasco y Gorka Vicente, hace dos décadas, cuando comenzaron a trabajar en el mundo de la ciberseguridad y se percataron de que la "ciberprotección no sabía de desarrollo de aplicaciones y viceversa. No había nadie en medio", explica Vicente. "Muchos equipos de desarrollo de software, ejecutivos y usuarios piensan que la seguridad es solo herramientas, criptografía, codificación, aplicaciones y varios dispositivos de hardware. Sin embargo, es un estado mental. Los equipos deben pensar seriamente en la cultura de protección para crear software verdaderamente seguro", destacan.

En 2008, ambos desarrollaron y pusieron a disposición de las empresas una herramienta de código abierto para implementar, desde su nacimiento, la seguridad en las aplicaciones. Era innovadora pero, sobre todo, eficaz y, de hecho, les sorprendió que comenzaran a usarla grandes corporaciones, un hecho que les confirmó su inquietud: había una demanda de soluciones de ciberseguridad que ofrecieran protección de las aplicaciones "desde la primera línea de código", recordó Vicente en la presentación del evento 'DevSecOps Spain'.

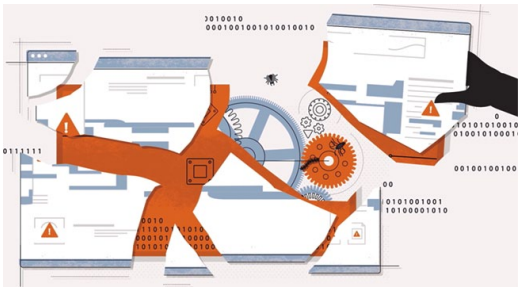
Esto les llevó a desarrollar una tecnología, actualmente patentada tanto en EE.UU. como en Europa, y a fundar en 2016 la compañía Hdiv, con sede en el parque tecnológico Miramón, en San Sebastián. Curiosamente, su primer cliente no fue, siquiera, europeo, sino un banco estadounidense: uno de los más grandes.

Cinco años después, la empresa, que ha duplicado su plantilla en el último año y espera alcanzar los 70 integrantes en 2022, cuenta con la confianza de más de 1.000 organizaciones de más de 120 países, incluidos Estados Unidos, China, Francia, España y Reino Unido. Además, entre sus clientes están desde muchas de las compañías del Fortune 500, a los que llegan a través de su amplia red de *partners*, integradores y mayoristas, que cubren los principales países donde opera Hdiv.

Estas entidades precisan dotar con la máxima seguridad a sus aplicaciones 'por defecto'. Y en esto se especializa Hdiv mediante sus tecnologías IAST, RASP y SCA, que brindan detección y protección desde la fase de diseño hasta cuando las aplicaciones están en producción y frente a las principales vulnerabilidades registradas,

Las capacidades de Hdiv se enfocan a la automatización de la seguridad de las aplicaciones para mejorar drásticamente la calidad del código y minimizar los tiempos de puesta en producción reduciendo, en el proceso, las revisiones cuando ya están en uso.

entre otras, por la Fundación OWASP.
A diferencia de las soluciones tradicionales, que basan su funcionamiento en analizar el código fuente durante la programación (SAST) y en escanear las webs para detectar problemas (Dynamic Application Security Testing, DAST), Hdiv ofrece en su plataforma el enfoque Interactive Application Security Testing (IAST), que monitoriza su ejecución. En cierto modo es similar a "poner un sensor en la aplicación y ver cómo se mueven los datos dentro de ella", explica Velasco. "Nuestra filosofía es permitir un software más seguro, no crear más software de seguridad. El enfoque tradicional siempre ha sido proteger las aplicaciones después de su desarrollo. Hdiv las protege desde el principio para resolver las causas fundamentales de los riesgos, así como después de que las aplicaciones se ponen en producción", destacan desde la compañía. Además de unificar estas dos funcionalidades en un único producto, Hdiv también es compatible con los enfoques de desarrollo más populares, como son las APIs REST y microservicios, e instalaciones en la nube, al integrarse de manera nativa con las aplicaciones.



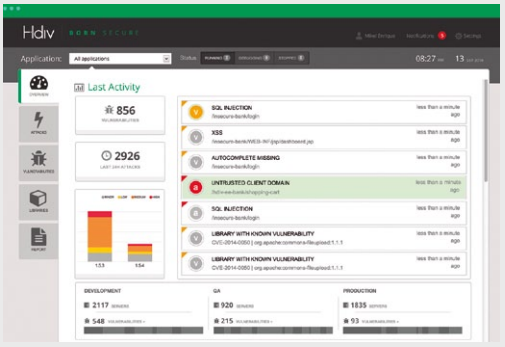
Su enfoque de automatización de la seguridad también logra mejorar la calidad del código al reducir los errores y minimiza los tiempos de puesta en producción, evitando revisiones una vez que las aplicaciones ya están siendo usadas. "Cuanto más desapercibido pasa un problema de software y más se tarda en localizar, más caro y 'perturbador' se vuelve", destaca Vicente.

Multientorno

La propuesta de Hdiv Security también destaca porque se despliega en las propias aplicaciones; por lo tanto, no requiere de ningún hardware adicional o cambios en las operaciones. Gracias a esta aproximación se elimina la necesidad de un punto específico de entrada, como en el caso de los WAF. Así, no hay cambios tampoco en el equipo de comunicaciones. Por ello, su aproximación no requiere de recursos adicionales y puede ejecutarse en los entornos ya provisionados para las aplicaciones. La solución no interfiere en su escalabilidad, ni requiere de inversiones en recursos específicos. Su tecnología trabaja de forma eficaz en cualquier escenario, incluyendo Amazon EC2, Microsoft Azure, Google App Engine, contenedores Docker e infraestructuras PaaS como Cloud Foundry.
Fruto del interés del mercado por su propuesta, Hdiv también ha atraído a numerosos inversores, como Adara Ventures, Wayra (Telefónica) o Prosegur Tech Ventures, que la han permitido incrementar su capital, acelerar su expansión internacional y seguir desarrollando sus productos con una fuerte inversión en I+D+i propio, siendo una de las *startups* españolas más innovadoras. Además, para ponerla en marcha, sus fundadores fueron cofinanciados por el Gobierno Vasco y la Unión Europea a través, entre otros, de los fondos Feder.
En definitiva, una de las claves es que "ofrecemos la única solución RASP capaz de proteger automáticamente las aplicaciones web y APIs de ataques dirigidos a la lógica de negocio", destaca Velasco a la vez que recuerda que "nuestra pasión siempre ha sido desarrollar productos que sean fáciles de utilizar por cualquier tipo de organización, y estamos comprometidos con absorber el ritmo de cambios que el mercado de la ciberseguridad demanda. Debido al aumento de velocidad con la cual los desarrolladores publican funcionalidad y la sofisticación de los ataques existentes, nos estamos dando cuenta de que los equipos de desarrollo valoran mucho la capacidad de contrarrestar ataques a nivel de aplicación de forma automática". ●

Seguridad desde el corazón de la aplicación

Sin duda, Hdiv es una de las pioneras españolas en llevar la seguridad al ámbito del Desarrollo y Operaciones (DevOps), para convertirlo en DevSecOps, introduciendo la ciberseguridad en todo el ciclo de vida de las aplicaciones. Para ello, basa su tecnología en la detección y protección más proactiva, y en que sea fácil de usar y de desplegar, sin generar falsos positivos y pudiendo automatizar los procesos.



"Nuestras soluciones se usan durante el desarrollo del software para localizar los problemas y, una vez resueltos, podamos proteger esos sistemas tanto en entornos IT como en OT", recuerdan desde la compañía, que centra su apuesta en tres pilares:

• **Más protección** (**RASP**). Hdiv Protection (RASP) automatiza la protección de riesgos graves para que sus desarrolladores puedan ser productivos mientras 'lanzan' software seguro. El objetivo es proteger las aplicaciones de los fallos, tanto los detectables por herramientas, como los de lógica de negocio (detectables mediante *pen-testing* manual), sin necesidad de entrenamiento específico.

• **Mejor detección** (**IAST**). Gracias a Hdiv Detection (IAST), se fomenta la colaboración entre todos los equipos y se ofrece información precisa, que incluye detalles completos y consejos de remediación. Su solución es capaz de detectar los fallos en el código fuente propio antes de que sean explotados, usando una técnica de control del flujo de datos en ejecución, proporcionando el detalle del archivo y número de línea, así como la vista dinámica (URL y parámetro). En definitiva, esta solución aprovecha la instrumentación nativa y no requiere atacar la aplicación para encontrar vulnerabilidades de seguridad, simplemente analiza el tráfico existente. Esto simplifica la inclusión de la detección de vulnerabilidades de seguridad a lo largo del ciclo de vida de la aplicación.

• **Mejor detección de componentes vulnerables de terceros (SCA)**. Con esta herramienta Hdiv permite detectar las dependencias vulnerables incluidas en el software de las empresas y organizaciones, habitualmente librerías *open-source* disponibles en Internet. Para ello Hdiv dispone de un sistema capaz de detectar las versiones de las dependencias utilizadas, cotejándolas con la base de datos de vulnerabilidades que dispone Hdiv. Además de poder detectar aquellas vulnerabilidades ya publicadas (aquellas que dispongan de un CVE público), Hdiv es capaz de analizar el propio binario de la dependencia, pudiendo incluso detectar vulnerabilidades no publicas conocidas como *zero days*.

Roberto Velasco

CEO y Cofundador de Hdiv Security

Comenzó siendo un proyecto *open source* y hoy la donostiarra Hdiv da servicio a grandes organizaciones como American Express, agencias federales en EE.UU. y la Sociedad Informática del Gobierno Vasco (EJIE), entre otras. En 2022 espera consolidarse como uno de los principales fabricantes en IAST y RASP para ofrecer seguridad robusta en todo tipo de aplicaciones. Su CEO y cofundador, Roberto Velasco, desgrana cuáles son las claves del avance de la firma y cómo ha conseguido ganar mercado en un nicho tan competitivo.

"Nuestro objetivo es consolidarnos como un fabricante de referencia en IAST y RASP, y dar soporte a nuevas plataformas, como es el caso de Go"

– Hdiv inicia su andadura en 2008, aunque se crea en 2016, un proceso largo…

– Sí, la empresa fue creada hace cinco años, aunque su semilla germinó a partir de un proyecto *open-source*, cuya primera versión fue publicada en 2008. Concretamente, nace de nuestra experiencia previa en el mundo de la seguridad, donde pudimos ver que había un *gap* en el mercado para automatizar la protección, extendiendo los *frameworks* o marcos de trabajo utilizados por los desarrolladores.

De dicha solución *open-source*, el 17% de las descargas provenían del Fortune 500 y las primeras peticiones de soporte y funcionalidades adicionales fueron el origen de Hdiv Security, así como de nuestros primeros clientes en Estados Unidos.

– ¿Cómo resumiría lo que es hoy su compañía?

– Como lema, destacaría el concepto de 'Unified Application Security', que refleja nuestra capacidad de cubrir todas las necesidades en la seguridad de aplicaciones desde un único proveedor. Inicialmente, comenzamos como proveedor de RASP y actualmente nuestro portafolio se ha complementado con soluciones IAST y SCA.

– Desde el principio, apostaron por productos y servicios fruto de un I+D+i propio, ¿Qué ha sido lo más complicado?

– Hablamos en ambos casos de productos que se integran en el software de los clientes y que, por tanto, deben garantizar propiedades como la escalabilidad o el rendimiento de los sistemas.

– ¿Integran tecnologías de terceros para complementar sus capacidades?

– Sí, por supuesto. Es algo que ya hacemos, por ejemplo, con productos de diferente tipología como soluciones *build*, CI (integración continua), *ticketing* de tareas, SIEMs, IDEs (entornos de desarrollo integrado)… que esperamos ampliar en el futuro.

– ¿Cómo han mejorado sus soluciones para hacer frente a los retos actuales, la evolución de las ciberamenazas y los nuevos entornos de desarrollo (contenedores, entornos 'sin servidor'…)?

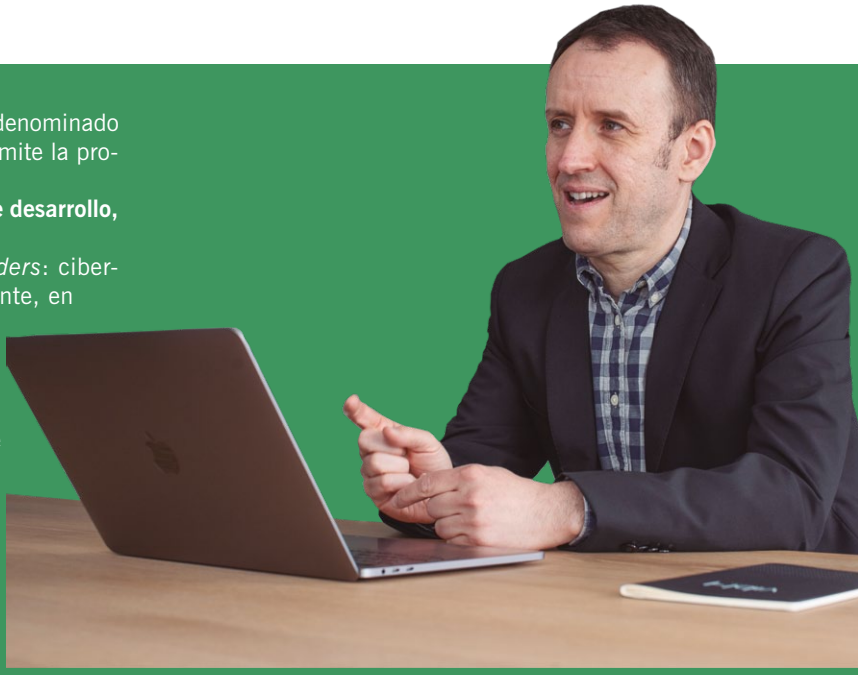
– Principalmente, con nuestro enfoque *plug&play* de instalación, tanto en lo que toca al nivel del entorno de ejecución como al de *build*, ya que nos facilita en gran medida poder adaptarnos a diferentes tipos de despliegue en la nube o basados en contenedores.

– Reconocida como una de las empresas más representativas del mercado global RASP por Gartner, ¿en qué sectores están más presentes y con qué clientes?

– Nuestra solución de detección IAST está generando mucho interés, sobre todo debido al malestar del mercado con las soluciones más tradicionales. Contamos con grandes clientes internacionales, como American Express, agencias federales en EE.UU., y, a nivel local, con eDreams y EJIE, entre otros.

– ¿Qué riesgos asociados a los entornos de desarrollo todavía son difíciles de encontrar y con qué enfoque los encara Hdiv?

– Los más complejos son aquellos solo detectables mediante auditorías manuales, como los problemas de lógica de negocio, conocidos como *business logic flaws* o



design flaws. En Hdiv ofrecemos un nuevo enfoque denominado *contract enforcement* (validación positiva), que permite la protección frente a ellos.

– No es fácil salvar el aislamiento de los entornos de desarrollo, de operaciones y de seguridad.

– Nuestros productos los usan todos los *stakeholders*: ciberseguridad, operaciones y desarrollo. Tradicionalmente, en detección, el equipo de seguridad hace uso de un DAST (una herramienta de prueba de seguridad de aplicaciones dinámicas), mientras que el equipo de desarrollo utiliza un SAST (es decir, pruebas de seguridad de aplicaciones estáticas) en el mejor de los casos. Así pues, los distintos departamentos hacen uso de diferentes herramientas donde no es posible mapear ambas fuentes de información. Algo similar ocurre con la protección a través de *firewalls* de aplicaciones web (WAF), que son utilizados únicamente por el equipo de seguridad en los entornos productivos. En el caso de Hdiv, nuestras soluciones de detección y protección se emplean en cualquier entorno por todos los interesados.

– En un área de mercado tan activa, ¿qué marca la diferencia de Hdiv con competidores, en gran medida multinacionales?

– Depende del producto. En el caso de la detección (IAST), la principal diferencia frente a los SAST, cuyo análisis estático presenta muchas limitaciones, es evitar los falsos positivos y, en el caso de los DAST, aumentar su nivel de detección. IAST también está reemplazando a las herramientas de seguridad de aplicaciones tradicionales por su cobertura de 'testabilidad', pudiendo analizar el 100% de la aplicación sin pedir ningún requerimiento al usuario final (credenciales, especificaciones open-API, swagger para APIs, etc.).

En el caso de RASP, las principales aportaciones de valor frente a otras tecnologías estriban en el aumento de la protección, gracias, especialmente, a la protección de los problemas de negocio, la reducción de los falsos positivos y la integración nativa con los entornos *cloud*.

– En el capital de Hdiv participan fondos de inversión, como Adara Ventures, y entidades como Wayra (Telefónica). ¿Qué aportan?

– Además del capital, sin duda, muy importante en fases tempranas, es vital la experiencia previa en la creación de empresas. Fondos con alto bagaje en ciberseguridad, como es el caso de Adara, pueden ser clave a la hora de guiarte en los diferentes pasos a realizar por la empresa.

– Acaban de ingresar como miembros en la OWASP Foundation. La fuente abierta la llevan marcada a fuego.

– Como he comentado, nacimos como un proyecto *open-source* y somos firmes defensores del trabajo en comunidad. Para nosotros es clave que la compañía esté vinculada con OWASP y colaborar activamente con dicha Fundación.

– La evolución hacia el 5G, la IA, la IoT y la digitalización en grandes sectores y ámbitos (transporte, ciudades conectadas…) dará lugar a nuevas necesidades y nichos de mercado. ¿Son buenos escenarios para su compañía?

– Todos estos sistemas dependen directa o indirectamente de sistemas software y, por lo tanto, la protección de estos sistemas software es el punto donde encaja el papel de Hdiv.

– ¿Tienen patentada su tecnología?

– Sí, tanto en Estados Unidos, como en Europa. Son procesos pesados y lentos que requieren armarte de paciencia pero que recomiendo llevar a efecto a cualquier profesional que decida emprender un proyecto de tecnología, ya que puede ayudar a proteger la inversión.

– Para 2021 y 2022, ¿cuál será el gran reto de Hdiv, tanto de mercado como en materia de innovación?

– En primer lugar, gestionar el crecimiento de forma adecuada, ya que vamos a pasar de ser un equipo de 40 personas, en 2021, a tratar de llegar a 70 en 2022. Desde el punto de vista de innovación, nuestro objetivo es consolidarnos como uno de los principales fabricantes en el área de IAST y RASP, y dar soporte a nuevas plataformas, como es el caso de Go.

– Una sugerencia para un CISO…

– Centrarse en las cosas más sencillas pero que pueden tener un gran impacto en el fortalecimiento de la ciberseguridad como, por ejemplo, asegurarse de llevar a cabo las actualizaciones a las últimas versiones, *backups*, aislamiento de sistemas, etc.

En segundo lugar, y respecto a la protección de aplicaciones, que según datos de Verizon son la causa de casi la mitad de los incidentes, les aconsejaría empezar por la implantación de una solución de detección en primer lugar para, posteriormente, seguir por una revisión de sus arquitecturas de desarrollo. ●

"Los riesgos más complejos son aquellos que solo son detectables mediante auditorías manuales, como los problemas de lógica de negocio conocidos como *business logic flaws* o *design flaws*. En Hdiv ofrecemos un nuevo enfoque, conocido como *contract enforcement* (validación positiva), que permite la protección frente a ellos"

DevSecOps: la nueva forma de 'securizar' el software a la velocidad que exige el negocio

El reto de la transformación digital y, en particular, la creciente demanda por sacar aplicaciones al mercado, ha supuesto que los equipos que generan software se centren en la funcionalidad y la productividad, relegando en ocasiones la seguridad. Al mismo tiempo, los ataques son cada vez más sofisticados y dañinos. Esta combinación de factores es uno de los desafíos más serios a los que se enfrentan las organizaciones que producen software.

El problema

Para responder a este reto, la industria de la seguridad ofrece cada vez más herramientas para que las empresas puedan defender sus activos frente a ciberataques. Sin embargo, en el ámbito de la protección de aplicaciones, la mayoría de los proveedores tradicionales cuentan en su catálogo con soluciones que pueden considerarse 'anticuadas', en el sentido de que no están evolucionando al ritmo que demanda el contexto en el que nos hallamos. Como dato que corrobora que algo no está funcionando lo suficientemente bien, basta recordar que, según el último informe de incidentes de Verizon, 'Data Breach Investigations Report (DBIR) 2020', **el 43% de las fugas de datos están relacionadas con la capa de aplicación.**

En Hdiv identificamos esta oportunidad de mejora y el resultado fue desarrollar nuestra oferta de productos basados en tecnologías IAST, RASP y SCA. Tal y como afirman Gartner y Forrester, entre otros, estas tecnologías suponen una evolución en la forma de entender la detección y la protección frente a vulnerabilidades. Como resultado, el *time-to-market* se acelera y la seguridad de las aplicaciones mejora.

Es obvio que las organizaciones que van a liderar la transformación digital son aquellas que mejor se adapten al desafío de **aunar** mayor productividad y mayor seguridad. Desde Hdiv, en colaboración con nuestros *partners* y distribuidores, tomamos este desafío como propio y, por tanto, nuestro objetivo es ayudar a las empresas en esta transformación ofreciendo soluciones que se adapten a la velocidad que requiere su negocio.

La solución: DevSecOps

DevOps, una metodología para mejorar la velocidad y la agilidad en la que empaquetamos, desplegamos y operamos el software, ha supuesto un cambio fundamental en la forma de crearlo. DevOps permite acelerar la publicación de software, pero la seguridad no forma parte explícita de ella y, frecuentemente, se traduce en actividades manuales que entorpecen la cadencia y producen software inseguro.

La solución es incluir la seguridad como parte integral del proceso DevOps y apostar por una evolución hacia **DevSecOps**.

Nuestra propuesta desde Hdiv Security para llegar a un modelo DevSecOps, además de mejorar la efectividad de las soluciones de detección y protección evitando falsos positivos y aumentando el nivel de detección, es **integrar la seguridad** de forma natural en las herramientas utilizadas por los diferentes grupos de trabajo:

- **Desarrollo**: herramientas de compilación, integración continua, entornos de desarrollo y gestión de tareas
- **Operaciones**: gestión de contenedores y configuración de servidores
- **Seguridad**: integración con sistemas SIEM y herramientas de gestión de tareas

En este contexto, Gartner* aconseja el uso de soluciones como las de Hdiv, concretamente el uso de IAST (Interactive Application Security Testing) en aquellos casos donde las organizaciones busquen implementar procesos DevSecOps. Concretamente, la firma analista recomienda: "Consider IAST when speed and accuracy are paramount especially in DevSecOps initiatives".

La necesidad de automatizar procesos, además de la de reducir costos y el *time-to-market,* responde a una dificultad todavía mayor, que es la falta de disponibilidad de personas expertas en ciberseguridad, perfiles cada vez más escasos en el mercado.

SEGURIDAD UNIFICADA DE APLICACIONES

La protección más fuerte contra OWASP Top 10

OWASP		Hdiv
A1	Inyección	✓
A2	Autenticación rota	✓
A3	Exposición de datos sensibles	✓
A4	Entidades externas XML (XXE)	✓
A5	Control de acceso roto	✓
A6	Configuración incorrecta de seguridad	✓
A7	Secuencias de comandos entre sitios (XSS)	✓
A8	Deserialización insegura	✓
A9	Uso de componentes con vulnerabilidades conocidas	✓
A10	Registro y monitorización insuficientes	✓

Funcionamiento

Hdiv aplica un enfoque diferente, tanto en la detección temprana de vulnerabilidades de seguridad, como en la protección proactiva contra ataques.

En el caso de la detección, a diferencia de las soluciones tradicionales como los SAST (Static Application Security Testing) que intentan simular la ejecución del código, en Hdiv Detection (IAST), pasamos de **adivinar** a, directamente, **observar** lo que ocurre gracias a la monitorización de la ejecución de las aplicaciones. Este cambio radical en el enfoque permite reducir los falsos positivos de los SAST e, incluso, aumentar el grado de detección que presentan. En lo que respecta a los DAST, la principal mejora es el aumento de las vulnerabilidades detectadas, gracias a la mayor información al ser una solución integrada dentro de las aplicaciones. Una evidencia objetiva de este nivel de efectividad es la nota obtenida por Hdiv en el test 'OWASP Benchmark', donde hemos llegado a alcanzar la máxima puntuación del 100%, dejando lejos a las soluciones tradicionales como los DAST o los SAST.

En cuanto a la protección, la principal diferenciación de Hdiv, además de la integración nativa en entornos *cloud*, es el aumento de la seguridad gracias a la **visibilidad** total de lo que ocurre dentro de la propia aplicación. Este enfoque, más cercano a la aplicación, no está basado en la definición de un perímetro externo y permite la protección de riesgos no cubiertos por las soluciones de protección tradicionales como los WAFs. Entre estos riesgos cabe destacar los problemas de lógica de negocio (*business logic flaws*), *untrusted deserialization (*una vulnerabilidad que se produce cuando se utilizan datos que no son de confianza), Server Side Request Forgery (SSRF) y una mejora en la protección en los diferentes riesgos de inyección existentes, como SQL injection o XSS.

* **Gartner**: *Ciso PlayBook: embedding AST in the software development life cycle*, (Nov 2017).

Daniel López
Sales Manager
Hdiv Security

La integración de la seguridad en las aplicaciones para automatizar procesos y reducir costos

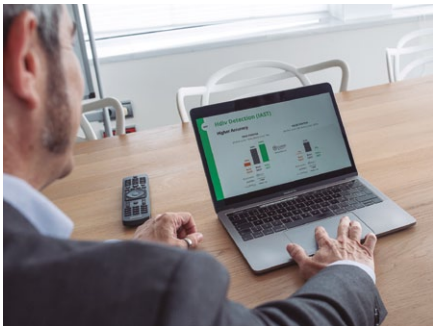
Contar con una buena idea de negocio no es sinónimo de éxito, ya que es igual de importante saber aplicarla a la realidad del mercado. La clave del crecimiento de Hdiv también ha sido comprender y dar respuesta a las necesidades de todo tipo de empresas y sectores que precisaban de una solución fácil de usar y que ofreciera una autoprotección de aplicaciones y prevención de vulnerabilidades, en tiempo real, incorporando la seguridad dentro del ciclo de vida del desarrollo de software. Por ello, en menos de un lustro, la firma vasca cuenta con clientes a nivel mundial en todo tipo de sectores, como banca, gobierno, comercio minorista, tecnología y aeroespacial, entre otros.

Protección de aplicaciones críticas

Y es que, desde sus comienzos, la tecnología de Hdiv traspasó fronteras, siendo grandes bancos y agencias federales estadounidenses las primeras en apostar por ella. Es el caso de **ASCR Federal**, entidad que ofrece servicios a diferentes agencias de la administración de EE.UU., especialmente al Departamento de Defensa y que "se convirtió en uno de los primeros clientes en adoptar nuestra solución RASP", explican desde Hdiv. La organización federal americana atiende a unos 10 millones de usuarios en 800 ubicaciones y, debido a su naturaleza de negocio, ejecuta aplicaciones particularmente sensibles, ya que pertenecen a los servicios sanitarios. Hdiv consiguió acelerar y mejorar los resultados de los procesos de prueba mediante la automatización de revisiones manuales, lo que resultó en un tiempo de comercialización más rápido.

Este éxito ha dado pie a que otras entidades gubernamentales europeas también apuesten por las soluciones de Hdiv. Es el caso de una agencia nacional de TI europea que, con un presupuesto de cientos de millones de euros y más de un centenar de desarrolladores, cuenta con miles de aplicaciones y servidores que utilizan soluciones SAST (de análisis de código estático) que requerían un largo proceso de personalización y configuración, con gran cantidad de falsos positivos.

Para solucionarlo, Hdiv Detection (IAST) se implementó en todo el ciclo de vida del desarrollo (SDLC) de la organización, incluidos



los entornos de los desarrolladores, el control de calidad, la puesta en marcha y las instancias de producción. Como resultado, los desarrolladores pueden escribir código seguro desde el principio, siendo conscientes de forma continua de la seguridad de las aplicaciones. "Hemos podido monitorizar la seguridad de nuestras 2.000 aplicaciones en minutos en lugar de meses", afirmaba Geoff, Director del Programa.

Evaluación proactiva de vulnerabilidades

En el mercado nacional, la compañía también cuenta como clientes con entidades públicas, como la Sociedad Informática del Gobierno Vasco (EJIE), a las que se les une grandes empresas privadas de ámbito internacional, como **eDreams Odigeo**, una de las agencias de viajes *online* más grandes del mundo y la mayor empresa cotizada de comercio electrónico de Europa.

La seguridad de las aplicaciones de esta compañía que opera en Internet es, sin duda, una alta prioridad estratégica para ella, ya que cuenta con más de 17 millones de clientes en 45 mercados, y trabaja con más de 660 aerolíneas y 130 *partners*. Así pues, el objetivo de la firma es evitar riesgos del lado del cliente, como la protección contra el *malware* del navegador del usuario, como Magecart. Por ello, recurrió a Hdiv para contar con técnicas modernas de evaluación de vulnerabilidades que se adaptaran a metodologías ágiles como DevSecOps.

Aplicando la tecnología Hdiv Detection (IAST), eDreams complementó sus soluciones de prueba de seguridad de aplicaciones heredadas, como el análisis de código estático (SAST), que utilizaban sus equipos de desarrollo, los cuales, sufrían tiempos de escaneo cada vez más largos a medida que aumentaba la complejidad de los proyectos de software. La incorporación de Hdiv en todas las fases, pero en especial en la parte de la canalización CI/CD de la empresa (orquestadas por Jenkins e IntelliJ), les permitió disponer de protección contra errores de seguridad y fallos de lógica empresarial en todo el ciclo de vida de desarrollo de software (SDLC) de la compañía, además de con una evaluación de vulnerabilidades más precisa y eficiente, a través de la plataforma Hdiv Unified Application Security.

Cerrar la brecha entre seguridad y desarrollo

Hdiv además está presente en el sector asegurador en el que cuenta con clientes destacados. Se trata de entidades que basan su negocio en la "gestión de la información", por lo que la seguridad de las aplicaciones es una prioridad, precisando que sean fiables y protejan de forma eficaz los datos de los clientes.

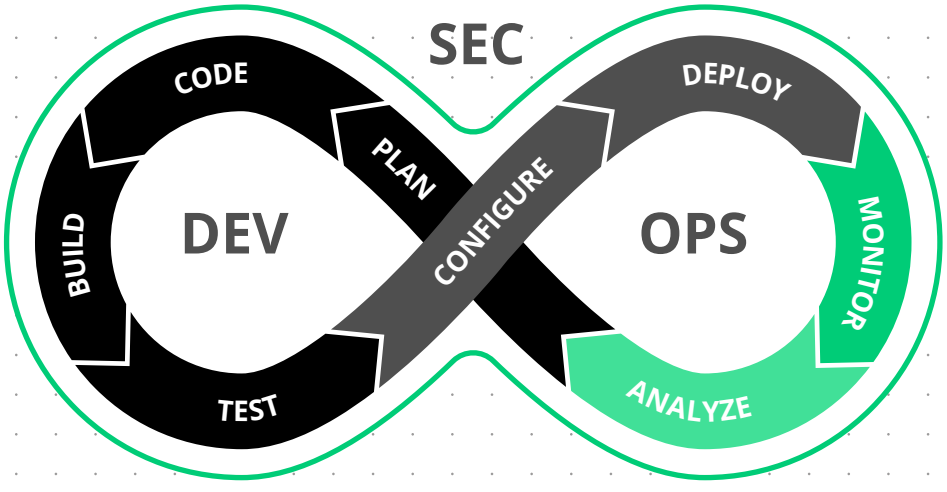
Para mejorar la ciberprotección de una destacada aseguradora, Hdiv ha implementado en sus sistemas su tecnología IAST, con un "enfoque moderno, que aprovecha la instrumentación para combinar puntos de vista estáticos y dinámicos". En términos de cultura de colaboración, la adopción de Hdiv Detection cerró la brecha entre los desarrolladores y el equipo de seguridad. Gracias a su tecnología, además, se consiguió una detección cinco veces mayor de los riesgos de seguridad del código, incluida la 'deserialización' insegura, logrando una reducción del 99,8% de falsos positivos, lo que se traduce en 'lanzamientos' de código más rápidos y con una disminución del 33% de las horas de prueba de lápiz manual debido a menos vulnerabilidades ●

BORN SECURE

Hdiv

¿Estás desarrollando **aplicaciones seguras?**

Automatiza la seguridad de tus **aplicaciones** y **APIs** durante todo el ciclo de vida del software



Hdiv Security ofrece la única plataforma de seguridad de aplicaciones de la industria para **DevSecOps** que se integra de forma nativa en todas las etapas del ciclo de vida del software, desde el desarrollo hasta producción.

Compruébalo solicitando una **demo gratuita**

hdivsecurity.com/demo