PENTEST COMO SERVICIO - PTAAS

ITECH SAS

www.itechsas.com

2022

GESTION Y PRUEBAS DE PENETRACION COMO SERVICIO

Pentest moderno impulsado por IA y habilitada para SaaS

Con la pandemia del Covid-19, los incidentes de ciberseguridad se han incrementado exponencialmente lo que demuestra que debemos mejorar nuestras defensas de ciberseguridad. Pero hay algo positivo en todo esto: los incidentes han ayudado a sensibilizar al público sobre lo vulnerables que son los sistemas de tecnología de la información (TI) y tecnología operativa (OT). Han demostrado que las tecnologías de las que las empresas, los gobiernos y personas han llegado a depender se enfrentan a riesgos reales, y han reforzado el argumento comercial para la acción preventiva contra las violaciones de seguridad.

En otras palabras, han demostrado que la mejor defensa es una buena ofensiva. El creciente número de incidentes también ha alimentado la necesidad de realizar pruebas continuas de nuestros sistemas de defensa y conocer mejor a nuestro adversario.

Servicios de pruebas de seguridad: el modelo estándar

Las soluciones de pruebas de seguridad generalmente incluyen hasta tres capas sucesivas de defensa: **escaneo de vulnerabilidades**, **pruebas de penetración** (también conocidas como pen test) y formación de **Red Team o equipos rojos**.

Primer capa: El escaneo e identificación de vulnerabilidades es la primera capa, es un tipo de defensa pasiva. Es un medio automatizado de verificar los sistemas en busca de debilidades conocidas a intervalos establecidos y genera informes que resumen sus hallazgos.

Segunda capa: Las pruebas de penetración son la segunda capa, trae un elemento humano activo al ejercicio. Le asigna a uno o más expertos en ciberseguridad la tarea de trabajar de forma activa, más intensa y con una gama más amplia de herramientas para encontrar y explotar las debilidades de un sistema. Esos expertos buscan vulnerabilidades y las utilizan para penetrar en los sistemas, y sus hallazgos ayudan a los operadores de estos sistemas a encontrar y solucionar los puntos débiles, y luego implementar soluciones a largo plazo para protegerse contra las infracciones.

Tercer capa: Red team, en esta capa se expande e intensifica el elemento humano activo en los controles de seguridad. Es un ejercicio ofensivo que está diseñado para simular un ataque cibernético en evolución a un ecosistema o conjunto de sistemas, y a menudo se lleva a cabo para verificar el rendimiento de soluciones a largo plazo, como las que podrían adoptarse después de completar una campaña exitosa de pruebas de penetración. En consecuencia, los operadores que aún se encuentran en la etapa de prueba de penetración o que están considerando cómo responder a los resultados de la prueba de penetración pueden no participar en la formación de equipos rojos.

PTaaS: una forma moderna de hacer Pen Test

Esta nueva forma usa las pruebas penetración y la potencia de la nube como servicio (PTaaS), la cual brinda a los usuarios la capacidad de acceder a pruebas de pen test bajo demanda en un formato ágil y moderno. Esta opción representa una mejora en las pruebas de penetración tradicionales. Automatiza parte del proceso del pen test, lo que reduce la cantidad de especialistas necesarios para realizar las pruebas, los costos asociados y flexibiliza los horarios para realizar el trabajo. Permite programar las pruebas con software basado en la nube que se puede personalizar para adaptarse a las necesidades de cada usuario. Permite el monitoreo continuo de pruebas de penetración automatizadas y genera informes que los usuarios podrán ver los resultados de las pruebas en tiempo real.

El objetivo de PTaaS es ayudar a las organizaciones a crear programas de gestión de vulnerabilidades exitosos que puedan encontrar, priorizar y remediar las amenazas de seguridad de forma rápida y eficiente, aprovechando al máximo los recursos y presupuesto de seguridad.

Beneficios de las pruebas de penetración como servicio

Uno de los mayores beneficios de PTaaS es el control que le brinda al cliente. Las empresas con menos experiencia en la industria de la seguridad obtienen un socio y una plataforma que les proporciona todo lo que necesitan para desarrollar un programa exitoso de gestión de amenazas y vulnerabilidades.

Además de presentar el progreso y el estado de todos los compromisos abiertos, las plataformas en la nube de PTaaS facilitan a los clientes la solicitud y el alcance de nuevos compromisos. Otros beneficios incluyen:

- **Opciones de compra flexibles**: los servicios de prueba de penetración automatizados, manuales e híbridos se pueden presupuestar y adquirir a través de una suscripción mensual, trimestral o anual o según sea necesario.

- **Acceso continuo a datos en tiempo real**: a medida que una vulnerabilidad o exploit existente evoluciona con el tiempo, los datos relacionados con ella se actualizan.

- **Opciones de informes flexibles**: muchas plataformas de PTaaS pueden agregar y correlacionar hallazgos de múltiples fuentes y proporcionar conjuntos de resultados que satisfagan las necesidades de múltiples partes interesadas.

- **Automatización**: los flujos de trabajo automatizados hacen que el escaneo de vulnerabilidades para redes externas y aplicaciones web no autenticadas sea más fácil de realizar.

Los servicios de PTaaS ayudan a las empresas a probar, asegurar y proteger sus aplicaciones, la nube y la infraestructura, reducir los ataques a la cadena de suministro, prevenir filtraciones de datos y mantener los requisitos de cumplimiento.

Servicios disponibles

Pruebas de penetración de API

Pruebe sus microservicios y API para las vulnerabilidades SANS Top 25 y OWASP API Security Top 10. Simplemente cargue su esquema API en Postman, Swagger, GraphQL u otro formato. Cada prueba de penetración se proporciona con un SLA contractual de cero falsos positivos y garantía de devolución de dinero si hay un solo falso positivo en su informe. Detecte la escalada de privilegios, la omisión de autenticación y las vulnerabilidades de la lógica empresarial de la API.

Cada prueba de penetración se proporciona con evaluaciones de verificación de parches ilimitadas para que sus desarrolladores puedan solucionar los problemas y luego volver a ejecutar la prueba sin costo adicional. Descargue su informe en formato PDF o exporte los datos de vulnerabilidad a su SIEM o WAF a través de nuestras integraciones DevSecOps. Obtenga de acceso a nuestros analistas de seguridad si tiene alguna pregunta sobre el informe.

Gestión de superficie de ataque

Identifique su superficie de ataque externa simplemente ingresando el nombre de su empresa. El proceso de descubrimiento no intrusivo detectará, clasificará y calificará el riesgo rápidamente sus activos de TI ubicados en las instalaciones o en un entorno de nube. Encuentre software vulnerable, dominios que caducan y certificados SSL,

sistemas obsoletos o mal configurados e infraestructura de TI en la sombra. Detecte código desprotegido, imágenes de contenedores o instantáneas del sistema disponibles en repositorios de terceros. Visualice áreas geográficas y países donde se almacenan sus datos con fines de cumplimiento.

Configure alertas de correo electrónico granulares para su equipo sobre cualquier activo recién descubierto, configuraciones incorrectas, vulnerabilidades e incidentes de seguridad. Utilice grupos y etiquetas para el control y la gestión de activos detallados. Disfruta de un precio fijo mensual por empresa independientemente de la cantidad de activos de TI o eventos que tengas. Aproveche la API para sincronizar el flujo de datos directamente con sus sistemas de seguridad internos o exporte los hallazgos seleccionados a PDF o XLS.

Pruebas de penetración en la nube

Pruebe sus aplicaciones web, aplicaciones nativas en la nube, microservicios o API alojadas en AWS, Azure, GCP u otros proveedores de servicios en la nube con las pruebas de penetración por demanda. Detecte las vulnerabilidades OWASP Top 10 y SANS Top 25, así como las debilidades de OWASP API Top 10 y las configuraciones incorrectas específicas de la nube. Descubra lo que se puede hacer con los ataques de escalamiento de privilegios y pivote de IMDS en la nube mediante la explotación de permisos de acceso excesivos o políticas de IAM predeterminadas en su entorno de nube.

Cada prueba de penetración en la nube se proporciona con evaluaciones de verificación de parches ilimitadas para que sus ingenieros en la nube puedan corregir las fallas de seguridad y luego validar, sin costo adicional, que todo se haya solucionado correctamente. Descargue su informe pentest en la nube desde el tablero interactivo a PDF o exporte datos directamente a su SIEM o WAF a través de nuestras integraciones DevSecOps. Obtenga acceso a nuestros analistas de seguridad si tiene alguna pregunta sobre el informe o los hallazgos.

Gestión de la postura de seguridad en la nube

Obtenga una vista de helicóptero en su superficie de ataque de nubes múltiples. La gestión de la postura de seguridad en la nube detecta rápidamente sus activos en la nube visibles desde el exterior, incluidas las instancias informáticas, el almacenamiento de datos, las puertas de enlace, los equilibradores de carga, las bases de datos y otros servicios gestionados en AWS, Azure, GCP y más de 50 proveedores de servicios de nube pública. Además de evaluar su superficie de ataque en la nube en busca de varias configuraciones incorrectas, permisos de acceso excesivos o políticas de IAM predeterminadas, también mapeamos su almacenamiento de datos geográficos con fines normativos y de cumplimiento.

A diferencia de otros proveedores, no necesita proporcionarnos una cuenta de IAM en la nube, simplemente ingrese el nombre de su empresa para ejecutar el proceso de descubrimiento y el monitoreo de seguridad continuo. Detecte el almacenamiento en la nube en la sombra y el uso injustificado de la nube. Personalice las alertas para las personas relevantes de su equipo de DevOps. Aproveche nuestra API para sincronizar el flujo de datos con sus sistemas SIEM existentes o exporte los resultados a PDF o XLS. Disfrute de un precio fijo mensual por empresa independientemente del número de activos, pruebas o eventos en la nube.

Pruebas de penetración continua

Supere las pruebas de penetración tradicionales con las pruebas de penetración continuas las 24 horas del día, los 7 días de la semana. Detectamos rápidamente nuevos códigos o características en sus aplicaciones web y API y luego probamos los cambios en busca de vulnerabilidades de seguridad, cumplimiento o problemas de privacidad. Una vez que se identifica un problema, se le avisará de inmediato por correo electrónico, SMS o llamada telefónica. Para todos los clientes, ofrecemos un SLA

contractual de cero falsos positivos y garantía de devolución de dinero por un solo falso positivo.

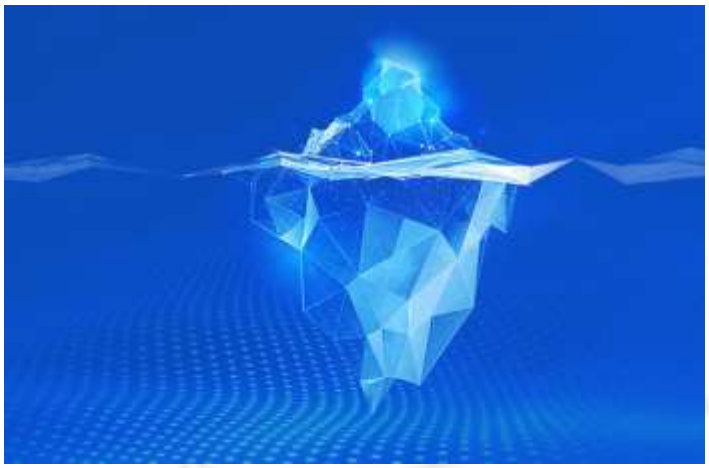
Aproveche nuestras integraciones con los principales proveedores de WAF para aplicar parches virtuales instantáneos a las vulnerabilidades descubiertas. Solicite una nueva prueba para cualquier hallazgo con un solo clic. Pregunte a nuestros analistas de seguridad sus preguntas sobre la explotación o la corrección de los hallazgos sin costo adicional. Obtenga un tablero en vivo con los hallazgos, descargue vulnerabilidades en PDF o aproveche nuestras integraciones de DevSecOps para exportar los datos a sus rastreadores de errores o sistemas SIEM.

Inteligencia de amenazas cibernéticas

Supervise el panorama de amenazas cibernéticas y los incidentes de seguridad. Simplemente ingrese el nombre de su empresa para detectar campañas de phishing en curso, nombres de dominio ocupados ilegalmente, cuentas falsas en redes sociales o aplicaciones móviles maliciosas que imitan su identidad. Reciba alertas instantáneas sobre menciones de su empresa o sus activos de TI en Dark Web, foros de piratería o mercados clandestinos. Detecte el indicador de compromiso (IoC) en sus sistemas locales o en la nube. Detecte e investigue si sus sistemas se agregan a varias listas negras por actividades sospechosas o de piratería.

Junto con la gestión de la superficie de ataque, la inteligencia de amenazas cibernéticas buscará automáticamente cualquier incidente que implique a cualquiera de sus sistemas, nombres de dominio, aplicaciones y usuarios. Envíe alertas instantáneas sobre nuevos hallazgos a las personas relevantes de su equipo mediante el uso de grupos y etiquetas en el tablero interactivo. Exporte los resultados a PDF o XLS, o envíelos directamente a su SIEM mediante la API. Disfruta de un precio fijo por empresa independientemente del número de activos, hallazgos o eventos.

Monitoreo de la web oscura



Descubra filtraciones de datos, credenciales robadas y documentos confidenciales en la Dark Web. El monitoreo de los mercados clandestinos y los foros de piratería se complementa con la vigilancia las 24 horas, los 7 días de la semana de los sitios web de pegado, redes sociales, IRC y canales de telegramas. A diferencia de los servicios de otros proveedores, nuestro monitoreo de Dark Web se incluye con la gestión de la superficie de ataque para detectar automáticamente todas las menciones de cualquiera de sus sistemas, nombres de dominio, aplicaciones o usuarios sin necesidad de ingresarlos todos manualmente.

Simplemente ingrese el nombre de su empresa para iniciar el descubrimiento y el monitoreo continuo que también llamará su atención sobre campañas continuas de phishing y ocupación ilegal de dominios, cuentas de redes sociales falsas, aplicaciones móviles maliciosas que usurpan su marca e indicadores de compromiso (IoC) en sus instalaciones. o activos de TI basados en la nube. Explore los hallazgos clasificados en el tablero interactivo, exporte los hallazgos a PDF o XLS, o use la API para sincronizar automáticamente los datos con sus sistemas SIEM o DFIR. Disfruta de un precio fijo mensual por empresa independientemente del número de incidentes de seguridad, menciones o filtraciones en la Dark Web.

Protección de marca digital

Detecte infracciones de marcas registradas y casos de uso indebido de marcas en Internet. En combinación con la gestión de la superficie de ataque, la protección de la marca rápidamente llama su atención sobre la ocupación ilegal de errores tipográficos y cibernéticos de todos los nombres de dominio nacionales o globales, campañas de phishing, cuentas falsas en redes sociales y aplicaciones móviles maliciosas

que imitan su marca o empresa. Detecta sitios web fraudulentos que imitan tu diseño con fines ilícitos.

Simplemente ingrese el nombre de su empresa para iniciar el monitoreo continuo. Disfruta de un precio fijo mensual por empresa independientemente del número de tus dominios, incidencias o campañas de phishing. Personalice las alertas para las personas relevantes de su equipo o envíe notificaciones a sus abogados directamente. Aproveche nuestra API para sincronizar el flujo de datos con sus sistemas internos o exporte los resultados a PDF o XLS.

Pruebas de penetración del RGPD

Realice pruebas de penetración periódicas de sus sistemas que almacenan o procesan datos personales según lo exigen las pautas de GDPR y EDBP. Cada prueba de penetración se proporciona con un SLA contractual de cero falsos positivos y garantía de devolución de dinero si hay un solo falso positivo en su informe. Detecte las vulnerabilidades de seguridad y las configuraciones incorrectas de OWASP Top 10 y SANS Top 25 en sus aplicaciones web y API. Obtenga valiosos consejos sobre configuraciones incorrectas de privacidad que pueden violar los requisitos reglamentarios o de cumplimiento.

Ejecute evaluaciones ilimitadas de verificación de vulnerabilidades sin costo después del pentest, para que sus desarrolladores puedan validar fácilmente si los hallazgos se corrigieron correctamente. Explore un panel de múltiples funciones con los hallazgos, descargue vulnerabilidades en PDF o aproveche nuestras integraciones de DevSecOps para exportar los datos a sus sistemas de seguimiento de errores o SIEM. Aproveche nuestras integraciones con los principales proveedores de WAF para parchear virtualmente las fallas de seguridad con un solo clic.

Pruebas de penetración móvil

Detecte las 10 debilidades principales de OWASP Mobile en su aplicación móvil iOS o Android y descubra las 25 vulnerabilidades principales de SANS en los puntos finales de la aplicación móvil. Revise si los mecanismos de privacidad, cumplimiento y encriptación de su aplicación móvil se ajustan a las mejores prácticas de la industria. Cada prueba de penetración móvil está equipada con un SLA contractual de cero falsos positivos y una garantía de devolución de dinero si hay un solo falso positivo en su informe.

Ejecute una caja negra o pruebas autenticadas mediante SSO, MFA u OTP. Detecte la lógica empresarial y las vulnerabilidades de omisión de autenticación. Aproveche las evaluaciones de verificación de parches ilimitadas después de la prueba de penetración, para que sus desarrolladores de software puedan validar fácilmente si todos los hallazgos se han parcheado correctamente. Exporte datos de vulnerabilidad desde su tablero interactivo a PDF o directamente a su SIEM o sistema de seguimiento de errores para una reparación más rápida.

Escaneo de seguridad móvil

Detecte las 10 debilidades principales de OWASP Mobile. Simplemente ingrese el nombre de su empresa para iniciar un proceso de descubrimiento no intrusivo y obtener una lista completa de sus aplicaciones móviles iOS y Android disponibles en más de 30 tiendas públicas, como Google Play o Apple Store. Las pruebas automáticas de SAST, DAST y SCA se iniciarán automáticamente en las aplicaciones móviles descubiertas para detectar las 10 vulnerabilidades y debilidades de OWASP Mobile Top 10.

Posteriormente, puede cargar cualquier aplicación móvil que pertenezca a su empresa sin costo adicional en caso de que no se descubra automáticamente o no esté disponible en las tiendas de aplicaciones públicas. Además del escaneo de vulnerabilidades móviles,

también verá varios problemas de privacidad, como permisos de aplicaciones móviles excesivos o peligrosos, cifrado faltante o débil y comunicaciones externas de la aplicación móvil. Nuestros analistas de seguridad están disponibles para responder sus preguntas sobre los hallazgos. Todas las funciones, incluido el escaneo de seguridad ilimitado, están disponibles a un precio mensual fijo.

Evaluación de la seguridad de la red

Descubra sus servicios de red accesibles externamente que combina la gestión de la superficie de ataque con la evaluación de la seguridad de la red. Simplemente ingrese el nombre de su empresa para obtener una instantánea completa de sus servidores, dispositivos de red y otros activos de TI alojados en las instalaciones o en una nube. Cada puerto abierto se analiza cuidadosamente para tomar una huella digital del servicio en ejecución y su versión para brindarle una puntuación basada en el riesgo. A diferencia de las soluciones de escaneo de vulnerabilidades tradicionales, nuestra tecnología de escaneo segura para la producción no interrumpirá ni ralentizará sus servicios de red.

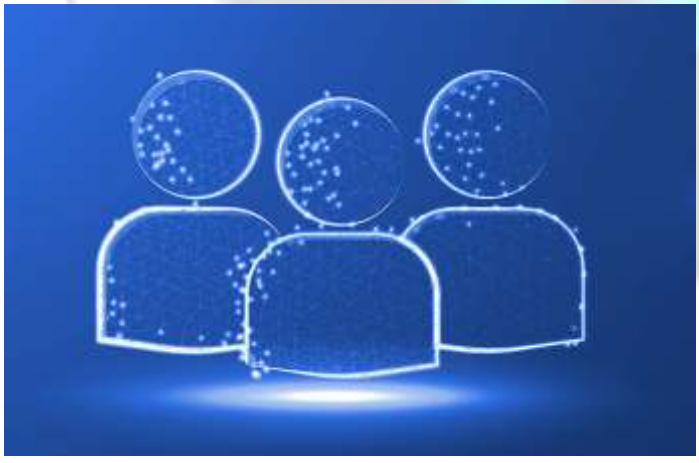
Detecte servidores ocultos, abandonados u olvidados y equipos de red con vulnerabilidades críticas. Reduzca la superficie de ataque de su red para acelerar y reducir los costos de las pruebas de penetración de la red. Envíe alertas instantáneas a las personas relevantes de su equipo mediante el uso de grupos, etiquetas y alertas en el tablero interactivo. Exporte datos de vulnerabilidad a través de la API u obtenga los hallazgos seleccionados en PDF o XLS. Disfruta de un precio fijo mensual por empresa independientemente del número de activos y servicios de la red.

Prueba de penetración PCI DSS

Realice pruebas de penetración periódicas de sus sistemas que almacenan o procesan datos de tarjetas de pago según lo exige PCI DSS . Detecte las vulnerabilidades de seguridad y las configuraciones incorrectas de OWASP Top 10, PCI DSS 6.5 List y SANS Top 25 en sus aplicaciones web, microservicios y API. Cada prueba de penetración se proporciona con un SLA contractual de cero falsos positivos y una garantía de devolución de dinero si hay un solo falso positivo en el informe.

Después del pentest, ejecute evaluaciones de verificación de vulnerabilidades ilimitadas sin costo, para que sus ingenieros de software puedan verificar fácilmente si los hallazgos del pentest se han solucionado de inmediato, según lo exige PCI DSS. Obtenga un panel multifunción con los hallazgos, descargue vulnerabilidades en PDF o aproveche nuestras integraciones de DevSecOps para exportar los datos directamente a sus sistemas de seguimiento de errores o SIEM. Aproveche nuestras asociaciones con los principales proveedores de WAF para aplicar parches virtuales con un solo clic a las vulnerabilidades de seguridad detectadas.

Ejercicio de equipo rojo



Aproveche PTaaS para los ejercicios Red Teaming adaptados a su estrategia de ciberseguridad y al panorama de ciberamenazas específico de su empresa. Al crear su proyecto, solo indique los escenarios de ataque, amenazas cibernéticas o actores maliciosos que desea simular. Puede adjuntar un escenario detallado o simplemente indicar brevemente los métodos y vectores de ataque clave que desea que probemos contra sus sistemas web. Nuestros analistas de seguridad y probadores de penetración revisarán cuidadosamente el plan de ataque y se comunicarán con usted en caso de preguntas o sugerencias sobre cómo expandirlo.

El informe Red Team elaborará las tácticas, técnicas y procedimientos de pentesting (TTP) y los resultados obtenidos equipados con una puntuación de riesgo consciente de las amenazas. Nuestros analistas de seguridad y probadores de penetración están a su disposición antes, durante y después del ejercicio Red Teaming sin costo adicional. El servicio se proporciona con un SLA contractual de cero falsos positivos y evaluaciones de verificación de parches ilimitadas para que sus desarrolladores puedan verificar que todas las fallas se solucionen correctamente.

Gestión de riesgos de terceros

Evalúe la higiene de TI, la ciberseguridad y la respuesta a incidentes de sus vendedores y proveedores críticos para el negocio. Simplemente ingrese el nombre de una empresa para obtener una instantánea completa de su superficie de ataque externa, sistemas y aplicaciones mal configurados o vulnerables, almacenamiento en la nube desprotegido, menciones en Dark Web y fugas de datos, campañas continuas de phishing o usurpación de dominio dirigidas a usted o su proveedor. Todo el proceso no es intrusivo y es seguro para la producción, lo que lo convierte en la opción perfecta para un programa de gestión de riesgos de terceros (TPRM).

Obtenga hallazgos clasificados y clasificados por riesgo en el tablero interactivo donde sus proveedores pueden conectarse para ver los detalles y remediar rápidamente cualquier problema. Evite el aumento de ataques a la cadena de suministro llevando su programa de gestión de riesgos de proveedores al siguiente nivel. Cumplir con los requisitos reglamentarios para auditar sistemas de terceros que procesan datos personales, financieros o de salud. Disfruta de un precio fijo por empresa independientemente del número de activos TI, menciones en la Dark Web o número de incidentes de seguridad.

Pruebas de seguridad WAF

Valide la eficiencia y la resiliencia de su WAF u otros controles de seguridad con las pruebas de penetración. Descubra las vulnerabilidades de seguridad OWASP Top 10 y SANS Top 25 en sus aplicaciones web, microservicios y API y luego verifique si son explotables y cómo se puede omitir su configuración WAF actual. Pruebe si su WAF mitiga adecuadamente la explotación de las vulnerabilidades de la lógica empresarial. Obtenga todos los beneficios de nuestro SLA contractual de cero falsos positivos y garantía de devolución de dinero si hay un solo falso positivo en su informe.

Realice evaluaciones ilimitadas de verificación de parches después del pentest para verificar si los desarrolladores de software corrigen los hallazgos de manera adecuada. Obtenga los resultados en el tablero interactivo, exporte los datos de vulnerabilidad en formato PDF o XLS, u obtenga los resultados directamente en sus sistemas de seguimiento de errores o SIEM. Aproveche nuestras alianzas tecnológicas con los principales proveedores de WAF para obtener conjuntos de reglas de WAF listos para usar para todas las vulnerabilidades descubiertas.

Pruebas de penetración web

Detecte las vulnerabilidades OWASP Top 25, PCI DSS 6.5 List y SANS Top 25 en sus aplicaciones web, API RESTful y microservicios. Descubra vulnerabilidades sofisticadas de escalada de privilegios, omisión de autenticación y lógica empresarial. El servicio se proporciona con un SLA contractual de cero falsos positivos y una garantía de devolución de dinero si hay un solo falso positivo en su informe. Personalice las pruebas en Black Box o modo multiusuario autenticado mediante MFA, OTP o SSO.

Ejecute evaluaciones de verificación de vulnerabilidades ilimitadas después del pentest sin costo, para que sus desarrolladores de software puedan verificar fácilmente si los hallazgos del pentest se corrigieron correctamente. Obtenga un panel multifunción con

los hallazgos estructurados, descargue vulnerabilidades en PDF o aproveche nuestras integraciones de DevSecOps para exportar los datos directamente a sus sistemas de seguimiento de errores o SIEM. Aproveche nuestras alianzas con los principales proveedores de WAF para aplicar parches virtuales con un solo clic a cualquier vulnerabilidad detectada.

Escaneo de seguridad web

Obtenga un inventario completo de su software web comercial y de código abierto, incluidos CMS, bibliotecas de JavaScript y otras dependencias. Junto con la administración de la superficie de ataque, el escaneo de la aplicación web aprovecha nuestra tecnología avanzada de análisis de composición de software (SCA) para identificar de manera confiable su software y las versiones instaladas para identificar vulnerabilidades conocidas o divulgadas públicamente de la lista OWASP Top 10. A diferencia de los escáneres de vulnerabilidades tradicionales, todo el proceso es seguro para la producción y no ralentizará ni interrumpirá sus sitios web.

Simplemente ingrese el nombre de su empresa para iniciar el descubrimiento y el monitoreo de seguridad continuo de sus aplicaciones web externas, mejorado con pruebas continuas para el cumplimiento de los requisitos de PCI DSS, GDPR o NIST, cifrado TLS, WAF faltante y otras configuraciones incorrectas y debilidades. Envíe alertas instantáneas a las personas relevantes de su equipo mediante el uso de grupos, etiquetas y alertas en el panel interactivo. Exporte los resultados a PDF o XLS, utilice la API para enviar los datos directamente a sus sistemas de seguimiento de errores, SIEM o WAF. Disfruta de un precio fijo mensual por empresa independientemente del número de aplicaciones web y sitios web que tengas.