Servicios de Auditoría de Seguridad

Q2 2026

Contenido

1. Introducción

Financial Strides, en colaboración con DataArt, ofrece una gama completa de soluciones para ayudar a las empresas a asegurar sus productos e infraestructura mediante un enfoque estructurado y una metodología consistente basada en las mejores prácticas de la industria y recursos asociados, como OSSTMM, OWASP, WASC. Ayudamos a nuestros clientes a identificar problemas de seguridad, sugerir soluciones de remediación y brindar soporte continuo al equipo técnico del cliente.

El objetivo de este documento es describir las tareas y metodologías típicas que Financial Strides y el equipo de seguridad de DataArt siguen durante las auditorías de seguridad, incluyendo:

- Prueba de penetración de red externa Black Box
- Prueba de penetración interna de red
- Prueba de penetración de aplicaciones web Grey Box
- Prueba de penetración nativa de aplicaciones Grey Box
- Revisión del código de seguridad White Box
- Revisión de la infraestructura de auditoría en la nube White Box

Por favor, consulte la sección de Enfoque y Metodología para una descripción detallada de estas actividades y herramientas utilizadas.

2. Enfoque y metodología

2.1. Prueba de Penetración de Red Externa (Caja Negra)

La prueba de penetración de redes externas se enfoca en sistemas y servicios accesibles desde Internet y tiene como objetivo determinar hasta qué punto estos sistemas pueden ser vulnerados por un atacante sin conocimiento interno pero con habilidad y motivación.

Metodología

Nuestra metodología para pruebas de penetración de redes externas (Black Box) consta de varias fases:

Mapeo de redes

Durante la fase de mapeo de red, realizamos varios escaneos para crear un mapa de red del entorno objetivo. Este esfuerzo también identifica sistemas, puertos, servicios accesibles y señala otros posibles puntos de entrada que un atacante podría atacar.

Clasificación del Sistema

Esta fase implica la clasificación de sistemas descubiertos usando varios métodos de huella digital. Después de clasificar cada sistema, el mapa de red se actualiza para reflejar la función y el sistema operativo de cada sistema.

Descubrimiento de vulnerabilidades

Durante la fase de descubrimiento de vulnerabilidades, analizamos todos los vectores de ataque potencialmente explotables. Durante este paso, utilizamos un amplio conocimiento práctico de técnicas de explotación, información pública y los resultados de la investigación privada de vulnerabilidades.

La siguiente lista ilustra algunas de las diferentes clases de vulnerabilidad que cubrimos durante esa fase. La lista no pretende ser exhaustiva y las pruebas reales que se realicen dependen de las especificidades de la organización que se está probando.

- Servicios IP visibles
- Uso de protocolos inseguros
- Reglas de firewall mal configuradas
- Fallas conocidas del sistema operativo/aplicación
- Parches de seguridad faltantes
- Configuración débil
- Vulnerabilidades de servidores web
- Debilidades de TLS
- Ejecución remota de código
- Desbordamientos de amortiguadores
- Divulgación de información

Operación

Durante la fase de explotación, nuestro equipo aprovecha las vulnerabilidades identificadas para lanzar sus propios ataques contra los sistemas objetivo. Los ataques buscan obtener acceso a datos restringidos, tomar el control de sistemas, suplantar usuarios y realizar otras acciones diseñadas para demostrar las posibles consecuencias de las vulnerabilidades descubiertas. Durante esta fase, también intentamos encadenar exploits para penetrar aún más en los sistemas objetivo, escalar privilegios de acceso e identificar vulnerabilidades adicionales.

Reportes

Durante la fase de reporte, creamos un informe detallado que incluye una visión general de los hallazgos y los pasos sugeridos para remediar. El informe incluirá las siguientes secciones:

- Resumen ejecutivo
- Metodología de pruebas de penetración
- Alcance de la prueba de penetración
- Visión general prioritaria de los hallazgos
- Recomendaciones para mejorar
- Datos y cifras de apoyo

Herramientas

- Nmap
- Nessus Professional
- Metasploit
- Nikto
- Fiddler
- SSLScan
- Wireshark
- Nexpose
- Herramientas de IA (Claude Enterprise, OpenAI Codex, Microsoft Copilot, cuando sea factible y permitido por el cliente)
- Cualquier otra herramienta según sea necesario

2.2. Prueba de Penetración de Red Interna

Durante la prueba interna de penetración, emulamos a un empleado malicioso e intentamos obtener un acceso no autorizado a los datos y recursos de la organización. La prueba indica si la empresa impide eficientemente que los usuarios o atacantes que obtuvieron acceso a nivel de usuario eleven sus privilegios o comprometan la seguridad organizacional de otras maneras.

Metodología

La metodología de la prueba de penetración interna es similar a la prueba de penetración de red externa; sin embargo, el atacante tiene acceso a la red local de la empresa y a las credenciales de un empleado sin privilegios.

La siguiente lista ilustra algunas clases adicionales de vulnerabilidad L2/L3 que cubrimos durante las pruebas de penetración internas. La lista no pretende ser exhaustiva y las pruebas reales que se realicen dependen de las especificidades de la organización que se está probando.

- Cambio de VLAN
- Envenenamiento de caché ARP
- Redirección de propiedad intelectual
- Debilidades del DHCP
- Fuzzing de protocolo
- Secuestro/repetición de sesión
- Captura de contraseñas
- Control de acceso insuficiente
- Protección de datos insuficiente
- Desbordamientos de amortiguadores
- Abuso de funcionalidad
- Divulgación de información

Herramientas

- Nmap
- Nessus Professional
- Metasploit
- Nikto
- Wireshark
- Nexpose
- Distribución Kali Linux
- Herramientas de IA (Claude Enterprise, OpenAI Codex, Microsoft Copilot, cuando sea factible y permitido por el cliente)
- Otras herramientas según sea necesario

2.3. Prueba de penetración de aplicaciones web (Grey Box)

El propósito de esta prueba es determinar si un atacante podría comprometer aplicaciones web corporativas para obtener acceso no autorizado a recursos de la empresa o a datos de otros usuarios.

Durante la prueba de penetración de la aplicación, imitamos a un atacante externo sin conocimiento previo del entorno, o a un atacante con acceso a nivel de usuario dentro de la aplicación. Intentamos eludir los controles de seguridad aprovechando las vulnerabilidades descubiertas mediante técnicas automatizadas y manuales.

Metodología

Nuestros proyectos de pruebas de penetración de aplicaciones involucran una metodología compuesta por las siguientes cinco fases: planeación de actividades del proyecto, recopilación de información, descubrimiento de vulnerabilidades, explotación de vulnerabilidades e informes. El proceso está diseñado para identificar problemas de seguridad y vulnerabilidades en aplicaciones objetivo, y para proporcionar a los clientes una visión clara del estado de seguridad de su aplicación, así como posibles formas de cómo podría ser comprometida por atacantes reales.

Planificación

Como primer paso, Financial Strides define y documenta los objetivos, el alcance y las reglas de enfrentamiento de la evaluación. Financial Strides y DataArt realizan entrevistas con las partes interesadas para obtener una comprensión profunda de los objetivos y necesidades del cliente, requisitos de seguridad y cumplimiento, riesgos de negocio, alcance de la evaluación y otros factores relacionados.

Recopilación de información

Durante la fase de recopilación de información, los ingenieros de pruebas de DataArt recopilan y examinan información clave sobre la aplicación y su infraestructura: funcionalidad de la aplicación, casos de uso, roles de usuario, arquitectura, mecanismos de seguridad, áreas críticas para la seguridad, entorno de hospedaje y más. Esa información permite a los ingenieros de pruebas apuntar correctamente al software de escaneo automatizado, enfocar mejor el proceso manual de pruebas e investigar posibles vectores de ataque.

Descubrimiento de vulnerabilidades

Durante la fase de descubrimiento de vulnerabilidades, nuestro equipo utiliza tanto herramientas automatizadas como técnicas manuales para inspeccionar el entorno objetivo e identificar minuciosamente las vulnerabilidades de las aplicaciones. Las

herramientas automatizadas se usan inicialmente para enumerar los recursos de la aplicación y seleccionar los problemas más comunes. Después de eso, pruebas manuales exhaustivas identifican cualquier problema restante que a menudo es pasado por alto por muchos competidores.

Las pruebas manuales se enfocan en vulnerabilidades que incluyen, pero no se limitan a:

Autenticación y Control de Acceso	• Política de contraseñas débiles • Inicio de sesión por fuerza bruta • Transmisión de credenciales inseguras	• Debilidades en la recuperación de contraseñas • Fallas en la implementación de SSO • Controles de acceso rotos
Gestión de Sesiones	• Generación insegura de tokens • Transmisión insegura de tokens • Envenenamiento por galletas	• Secuestro de sesiones • Fijación de sesiones • Terminación de sesión insegura
Fallas de Inyección de Comandos	• Inyección SQL • Inyección Xpath • Inyección de comandos del sistema operativo • Inyección de código	• Manipulación de caminos • Desbordamiento de búfer • Scripting entre sitios
Fallas tecnológicas del lado del cliente	• Dependencia de la validación del lado del cliente • Almacenamiento local de datos inseguro • Política de origen similar	• Fallas en AJAX/servicio web • Objetos Java/ActiveX/Flash/Silverlight
Fallas en la lógica de aplicación	• Escalada de privilegios • Divulgación de información sensible • Defectos de implementación de E/S de archivos • Uso inseguro de la criptografía	• Falsificación de solicitudes entre sitios • Validación de datos débil • Condiciones de la carrera • Funciones intensivas en CPU

Divulgación de Información	• Banners del servidor • Mensajes de error verbosos • Comentarios de código del lado del cliente • Divulgación del código fuente	• Enumeración de cuentas • Contenido web en caché • Problemas de privacidad local
Configuración incorrecta de la plataforma	• Contenido predeterminado • Credenciales administrativas predeterminadas	• Configuración incorrecta del servidor web • SSL y debilidades en la capa de transporte
Vulnerabilidades de LLM	• Inyecciones rápidas • Manejo inseguro de salidas • Cadena de suministro • Problemas de permisos	• Divulgación de información sensible • Agencia excesiva • Plugins y agentes inseguros

Los siguientes estándares de seguridad serán referenciados como parte de esta evaluación: OWASP Top 10, OWASP API Security Top 10, OWASP TOP 10 LLM

Explotación de vulnerabilidades

Durante esta fase, cualquier vulnerabilidad potencial encontrada es investigada, investigada manualmente y se intenta explotarla. Al explotar vulnerabilidades, intentaremos obtener acceso no autorizado al sistema objetivo o extraer datos sensibles de él. Un exploit se considera exitoso si logramos cualquiera de estos objetivos.

Para aplicaciones que aprovechan Grandes Modelos de Lenguaje, realizamos evaluaciones de seguridad integrales destinadas a identificar riesgos potenciales que podrían llevar a la exposición de datos sensibles o acceso no autorizado al sistema. Nuestros expertos evalúan áreas críticas como manipulación de entradas, inyección de prompts y vulnerabilidades de plugins para descubrir debilidades en el diseño, configuración e integración del LLM con sistemas externos.

Cada sistema comprometido será examinado para detectar la existencia de datos y archivos críticos. Si encontramos que dichos datos son accesibles, una muestra de estos datos será descargada del sistema y almacenada de forma segura por nosotros hasta la presentación de los entregables.

A medida que los sistemas o aplicaciones se vean comprometidos, los contactos clave de seguridad de nuestros clientes serán notificados. En ese momento, los contactos del cliente tendrán la oportunidad de decidir si el sistema en particular debe someterse a pruebas adicionales. Si deciden que continuemos, se usarán técnicas adicionales para penetrar aún más el sistema objetivo y el entorno en general. Esto puede incluir la instalación de detectores de red, herramientas de gestión remota, herramientas de conectividad, etc.

Reportes

Tras la finalización del proyecto de evaluación de seguridad, entregamos un informe detallado basado en los hallazgos del equipo. Para cada hallazgo, también incluimos un resumen detallado, evidencia (capturas de pantalla), análisis del posible impacto y recomendaciones accionables para remediación o mitigación.

Herramientas

- Escáneres de vulnerabilidades (Nessus Professional, ActiveScan++, BurpBountyPro)
- Plataformas de Pruebas de Seguridad (Burp Suite Pro, OWASP Zap)
- Herramientas de enumeración (dirsearch, gobuster, Wfuzz, findomain)
- Herramientas de prueba de inyección (SQLmap, XSSStrike, XSSHunter)
- Herramientas de fuerza bruta (hashcat, john, hydra, WebSocket BF)
- Herramientas de explotación (phpgcc, ruby marshaling, ysoserial, graphql-voyager, herramienta JWT)
- Herramientas de pruebas de seguridad CMS (wpscan, droopscan, joomscan)
- Repositorios de cargas útiles y shells (SecLists, PayloadsToTheThings)
- Herramientas de análisis SSL/TLS (sslscan, testssl)
- Herramientas de IA (Claude Enterprise, OpenAI Codex, Microsoft Copilot, cuando sea factible y permitido por el cliente)
- Otras herramientas según sea necesario

2.4. Prueba de Penetración de Aplicaciones Nativas

Dicha prueba está dirigida al mismo objetivo, que la prueba de penetración de aplicaciones web: identificar si un atacante podría comprometer aplicaciones nativas de escritorio o móviles para obtener acceso no autorizado a información personal o corporativa, recursos de la empresa o datos de otros usuarios. Sin embargo, el enfoque se ha desplazado a romper la privacidad local y a eludir las APIs y mecanismos específicos de la plataforma usados para la protección de datos.

Al realizar pruebas de penetración en aplicaciones nativas, imitamos a un atacante externo sin conocimiento previo del entorno, o a un atacante con acceso físico al dispositivo de la víctima y acceso a nivel de usuario dentro de la aplicación. Intentaremos eludir tanto los controles de seguridad de aplicaciones como de plataformas aprovechando las vulnerabilidades descubiertas mediante técnicas automatizadas y manuales.

Metodología

Nuestro enfoque para las pruebas de penetración de aplicaciones nativas consiste en los mismos pasos principales descritos en la sección anterior : planificación, recopilación de información, descubrimiento de vulnerabilidades, explotación de vulnerabilidades e reportes, pero las técnicas son diferentes. Durante la fase de descubrimiento de vulnerabilidades, nos enfocamos en la ingeniería inversa de la lógica de aplicación y sus controles de seguridad, análisis dinámico de aplicaciones e inspección de datos almacenados localmente. Analizamos todas las comunicaciones de la aplicación con servicios remotos y aseguramos la seguridad de cualquier dato transmitido. Durante la prueba, analizamos la aplicación desde el punto de vista del atacante y tratamos de idear y lanzar ataques.

Las pruebas nativas de aplicaciones se enfocan en posibles vulnerabilidades en la lógica de aplicaciones móviles, buscando problemas que incluyen, pero no se limitan a:

- Almacenamiento local de datos
- Caché y archivos temporales
- Tala
- Cuestiones de privacidad
- Fuga de información
- Vulnerabilidades de WebView
- SSL y debilidades en la capa de transporte
- Defectos de autenticación y gestión de sesiones
- Código no gestionado y acceso a memoria
- Fugas de memoria

También descubrimos las APIs del lado del servidor usadas por las aplicaciones, y estas APIs pasan por pruebas de penetración de aplicaciones web, como se describió en la sección anterior. Si las aplicaciones nativas exponen varios widgets o usan módulos externos de terceros, como bibliotecas estáticas o dinámicas, también se prueban, y los problemas encontrados ahí también se incluyen en el informe final.

Herramientas

- Proxies (Burp Suite Pro, OWASP ZAP)
- Herramientas específicas de ingeniería inversa de plataforma (por ejemplo, Frida, Objection para iOS)
- Cadenas de herramientas y SDKs para aplicaciones nativas e híbridas (por ejemplo, gcc, clang y SDK de iOS)
- Herramientas para extraer secretos y contraseñas (por ejemplo, chainbreaker para macOS)
- Depuradores y modificadores de tiempo de ejecución (por ejemplo, gdb, cycript)
- Herramientas de IA (Claude Enterprise, OpenAI Codex, Microsoft Copilot, cuando sea factible y permitido por el cliente)
- Otras herramientas según sea necesario

2.5. Revisión del Código de Seguridad (Pruebas de Caja Blanca)

Una revisión de código de seguridad es una actividad de prueba de "caja blanca" destinada a analizar el código fuente de la aplicación y determinar posibles debilidades y fallas de seguridad en el mismo.

Metodología

Nuestros proyectos de revisión de códigos de seguridad incluyen análisis tanto estático como manual.

Análisis estático

Nuestro equipo utiliza varias herramientas de análisis estático para analizar el código fuente de las aplicaciones objetivo e identificar posibles vulnerabilidades. Estas herramientas son capaces de identificar los siguientes tipos de problemas:

- Algoritmos criptográficos débiles y funciones hash
- Parámetros de entrada no confiables
- Potencial de inyección SQL/HQL
- Inyección potencial de LDAP
- Recorrido potencial de trayectorias
- Posible inyección de comandos
- Inyección potencial de XPath
- Posible división de la respuesta HTTP
- Inyección potencial de plantillas
- XSS potencial
- Redirecciones no validadas
- Datos potencialmente sensibles en una cookie
- Cookies sin banderas HttpOnly y Secure
- Autenticación insuficiente del servidor SSL/TLS
- Violaciones de límites de fideicomiso
- Claves y contraseñas codificadas

Revisión Manual de Código

Para revisiones manuales, nuestro equipo adopta el proceso y las directrices descritas en la Guía de Revisión de Código OWASP V1.1. Además, hacemos referencia a la lista de requisitos de seguridad de aplicaciones del Estándar de Verificación de Seguridad de Aplicaciones OWASP 3.0 (nivel 3).

Nuestro equipo realizará las siguientes acciones como parte de esta tarea:

- Familiarízate con el propósito comercial de las aplicaciones

- Identificar diferentes tipos de agentes de amenaza y posibles vectores de ataque
- Identificar todas las entradas y salidas de la aplicación
- Realizar análisis dinámico y estático del flujo de datos
- Realizar análisis de transacciones de aplicaciones
- Revisar la implementación de los controles de seguridad de aplicaciones
- Rastrear el código fuente para detectar vulnerabilidades de seguridad específicas

La revisión manual de código cubre los controles de seguridad y áreas de vulnerabilidad más críticos, tales como:

- Manejo de entradas
- Validación de datos
- Autenticación
- Gestión de sesiones
- Autorización
- Criptografía
- Manejo de errores
- Tala
- Configuración de seguridad
- Defectos en la lógica de aplicación
- Emisiones de concurrencia
- Denegación de servicio a nivel de aplicación

Herramientas

- SAST (SonarQube, Semgrep y herramientas específicas del lenguaje)
- SCA y escaneo de contenedores (Snyk, Trivy)
- Escaneo Secreto (GitLeaks, TruffleHog)
- Escaneo IaC (Trivy, Checkov)
- Herramientas de IA (Claude Enterprise, OpenAI Codex, Microsoft Copilot, cuando sea factible y permitido por el cliente)

2.6. Auditoría en la nube (Revisión de la infraestructura White Box)

La auditoría en la nube es una revisión y actividad de prueba de infraestructura de "caja blanca" que se enfoca en los siguientes objetivos:

- Verifica que la infraestructura en la nube y los controles de seguridad estén implementados de acuerdo con las políticas de seguridad del cliente y las mejores prácticas comunes
- Encuentra brechas de seguridad no abordadas e identifica los problemas técnicos relacionados dentro de entornos en la nube y sugiere las mejoras

Metodología

Nuestro marco de evaluación en la nube consta de cuatro fases: recopilación de información, entrevistas, evaluación manual y automatizada, reportes.

Recopilación de información

Presentamos a nuestros evaluadores al equipo de mantenimiento en la nube del cliente y les pedimos que proporcionen documentación relacionada con la seguridad y llenen un cuestionario especial que cubre los aspectos clave de la seguridad en la nube. El cuestionario incluye aspectos como autenticación, control y gestión de acceso, auditoría, seguridad a nivel de aplicaciones y red, mantenimiento y otros. La lista de artefactos requeridos incluye, pero no se limita a:

- Diagramas de red y arquitectura
- Catálogo de aplicaciones
- Resultados de escaneos previos de vulnerabilidades y reportes de herramientas de seguridad
- Varias configuraciones (aplicaciones, red, etc.)
- Ejemplos de registros de aplicaciones y rastreos de auditoría

Una vez que los artefactos y el cuestionario llenado se comparten con el equipo de evaluación, los revisamos y analizamos para identificar la arquitectura de la nube, los tipos de servicios desplegados, los controles de seguridad utilizados, así como las personas y procesos clave.

Entrevistas

Tras completar la fase anterior, organizamos varias entrevistas con las personas clave responsables de la nube: ingenieros de redes, arquitectos técnicos, líderes de equipos de soporte y mantenimiento, oficiales de seguridad y cumplimiento. Con base en la

información recopilada, los evaluadores preparan preguntas específicas para cada miembro del equipo y piden demostraciones rápidas y sesiones de compartición de pantalla, si es posible.

Si se descubren algunos puntos ciegos durante la evaluación, organizamos una ronda extra de entrevistas para aclarar puntos inciertos, hacer preguntas adicionales y obtener acceso a materiales adicionales.

Evaluación Manual y Automatizada

Nuestro equipo realiza una evaluación automatizada de la infraestructura en la nube para validar los controles de seguridad existentes usando listas de verificación predefinidas, identificar posibles problemas en sus configuraciones y traducirlos en reportes. El equipo de evaluación también inspecciona y analiza toda la configuración manualmente, ya sea a través de la consola web o de APIs proporcionadas por la nube, y recopila las evidencias de que los controles de seguridad funcionan como se describen en las políticas y mejores prácticas. También se registran todas las desviaciones respecto a las configuraciones recomendadas. Generalmente se examinan los siguientes aspectos:

- Límites de fideicomiso
- Autenticación de usuarios y control de acceso
- Separación de roles y deberes
- Medidas de protección de datos en tránsito y en reposo
- Acceso remoto y administrativo seguro
- Mecanismos de detección y respuesta a ataques
- Respaldos seguros y plan de recuperación ante desastres

Reportes

En el paso final de la auditoría, nuestro equipo colabora con el equipo de nube en hallazgos discutibles, define la criticidad de cada elemento y crea un informe de auditoría que incluye la sección de resumen ejecutivo, descripción de la metodología, definición del alcance de la auditoría y una visión prioritaria de los temas. Cada hallazgo se acomoda con grado de criticidad, descripción, evidencias (capturas de pantalla, enlaces a configuraciones, grabaciones de video y voz, etc.) y recomendaciones sobre remediación. Este informe se comparte con el equipo y se discute en una reunión de seguimiento.

Herramientas

- Suite de Exploradores, Merodeador
- PMapper, CloudSploit
- Kali Linux
- Herramientas de IA (Claude Enterprise, OpenAI Codex, Microsoft Copilot, cuando sea factible y permitido por el cliente)
- Otras herramientas según sea necesario

3. Entregables

Tras completar cada tarea, entregamos un informe detallado basado en los hallazgos del equipo. Los informes incluyen las siguientes secciones:

- Resumen ejecutivo (de manera no técnica, adecuado para alta dirección)
- Metodología de evaluación
- Alcance de la evaluación
- Narrativa de ataque (cuando aplica)
- Visión general prioritaria de los hallazgos
- Recomendaciones para mejorar
- Datos y cifras de apoyo

Todas las vulnerabilidades identificadas se clasifican por su causa y luego se priorizan según una calificación de riesgo estimada. Para cada hallazgo, también incluimos un resumen detallado, evidencia (capturas de pantalla), análisis del posible impacto y recomendaciones accionables para remediación o mitigación.

El cliente recibe una alerta inmediata sobre cualquier vulnerabilidad crítica detectada durante la auditoría, por lo que puede actuar de inmediato sin esperar el informe completo.

En caso de que se realice una nueva prueba, los problemas se actualizan con notas de reprueba que indican que las pruebas realizadas para validar las correcciones adecuadas han sido implementadas o no correctamente dentro del entorno.

Criterios para la calificación de riesgo

La asignación de calificaciones de riesgo a las vulnerabilidades identificadas es uno de los elementos clave de la evaluación de seguridad. Permite crear una lista prioritaria de hallazgos para que el cliente pueda iniciar la remediación de problemas que representan el mayor riesgo para su organización.

Nuestros analistas de seguridad realizan un análisis inteligente para determinar y asignar una calificación de riesgo a cada problema identificado. La siguiente información obtenida durante el proyecto de evaluación se considera en el cálculo de una calificación de riesgo:

- Probabilidad de ataque
- Impacto potencial de la explotación
- Nivel de habilidad requerido para ejecutar el ataque
- Número de instancias de la vulnerabilidad
- Controles de mitigación

La siguiente tabla describe las calificaciones de riesgos:

Calificación	Descripción
CRÍTICO	Problemas graves que pueden ser fácilmente explotados para impactar inmediatamente el medio ambiente.
ALTO	Problemas importantes que pueden ser explotados para impactar el medio ambiente, sin embargo, su aplicabilidad es limitada o se requiere esfuerzo adicional para su explotación.
MEDIO	Problemas de seguridad moderados que requieren cierto esfuerzo para impactar exitosamente el medio ambiente.
BAJO	Problemas de seguridad que tienen un impacto limitado o trivial en el medio ambiente.

4. Certificaciones de Equipos

Todos los miembros del equipo de prueba cuentan con una o más de las siguientes certificaciones:

OSCP (Profesional Certificado en Seguridad Ofensiva)

CEH (Hacker Ético Certificado)

CPTS (Especialista Certificado en Pruebas de Penetración)

Probador de Penetración Registrado en CREST

BSCP (Profesional Certificado en Burp Suite)

OSWE (Experto Web en Seguridad Ofensiva)

eCPPT (Probador Profesional Certificado de Penetración)

eCPTXv2 (Tester de Penetración Certificado eXtreme v2)

eWPTXv2 (Web Application Penetration Tester eXtreme v2)

eMAPT (Probador de Penetración Móvil)

5. Gestión de Proyectos

Financial Strides ofrece gestión de proyectos para sus servicios para reducir la cantidad de desafíos administrativos y otros presentes al realizar una evaluación.

El rol y la responsabilidad del gerente de proyecto son los siguientes:

- Planeación y alcance
- Reporta diariamente a todas las partes involucradas en el proyecto sobre todos los aspectos del mismo
- Establecer y mantener una comunicación segura entre los participantes
- Administrar el cronograma, presupuesto y expectativas del proyecto
- Definir y acercarse a grupos de servicio para responder a las necesidades del proyecto
- Recopilar y actualizar todos los informes de estado, preliminares y finales
- Gestionar los reportes financieros de proyectos, incluyendo hojas de tiempo y facturas
- Revisa el estado de todas las actividades de auditoría semanalmente.

Resumen de la participación

Nuestros proyectos de auditoría de seguridad involucran las siguientes fases:

- Planeación: nuestros expertos trabajan con el cliente para definir y documentar claramente los objetivos, el alcance y las reglas de enfrentamiento de la evaluación. Durante esa fase, el cliente proporciona las credenciales de acceso necesarias, detalles técnicos y otra información requerida para la tarea. Al final de la fase se realiza una reunión de inicio para finalizar las reglas de participación.
- Evaluación: nuestro equipo realiza evaluaciones de acuerdo con las metas establecidas durante la fase de planeación. Por lo general, se requiere ayuda del cliente, como resolver problemas técnicos, explicar ciertos aspectos, discutir cualquier problema crítico identificado, etc.
- Presentación del informe: entregamos los reportes de auditoría y presentamos los resultados generales a las partes interesadas del cliente.
- Soporte de remediación: podemos brindar apoyo puntual a los ingenieros del cliente durante la remediación de problemas.
- Re-pruebas: Si aplica, nuestros equipos pueden realizar nuevas pruebas de los problemas identificados y entregar una nueva revisión del reporte.

6. Apéndice: Información de DataArt

DataArt es una empresa global de ingeniería de software que adopta un enfoque exclusivamente humano para resolver problemas. Con más de 20 años de experiencia, equipos de ingenieros altamente capacitados alrededor del mundo, profundo conocimiento del sector industrial e investigación tecnológica continua, ayudamos a los clientes a crear software personalizado que mejore sus operaciones y abra nuevos mercados.

Impulsados por nuestro principio People First, trabajamos con clientes a cualquier escala y plataforma, y nos adaptamos junto a ellos conforme evolucionan.

Integramos nuestra excelencia en ingeniería con valores profundamente humanos que impulsan nuestro negocio y nuestro enfoque hacia las relaciones: curiosidad, empatía, confianza, honestidad e intuición. Estas cualidades nos ayudan a ofrecer soluciones de alto valor y calidad en las que dependen nuestros clientes, y alianzas de por vida en las que creen.

Ubicaciones globales:

- Nueva York
- Londres
- Zúrich, Suiza
- Múnich, Alemania
- Europa del Este
- América Latina

Datos rápidos sobre DataArt:

- Fundada en 1997, transparente, de propiedad privada y rentable;
- Ofreciendo pruebas de auditoría de seguridad desde 2012;
- ingresos de $378 millones en 2022;
- 95% de los clientes recurrentes;
- 4.7 de duración promedio;
- Colaboramos con 400+ empresas líderes.
- Nuestros 20 principales clientes han trabajado con nosotros durante un promedio de 7+ años;
- 40+ ubicaciones globales;
- 5,000+ Consultores e Ingenieros;
- 87 % de retención de empleados en 2023;
- Certificado SOC 2 Tipo II, priorizando la seguridad tanto interna como para nuestros clientes;
- No hay litigios abiertos, el historial legal se limita a asuntos de cobranza.

7. Apéndice: Información sobre Avances Financieros

Financial Strides es una firma de consultoría FinTech con presencia en California y el Reino Unido.

Las principales áreas de experiencia de producto de Financial Strides son:

- Apertura de cuentas en línea y móviles: Proceso de Identificación del Cliente ("CIP"), AML/BSA y OFAC ("KYC"), Detección de fraude y señales de alerta:
- Protocolos de pago: Protocolos de pagos con tarjeta, Pagos rápidos: Push-to-Debit, RTP, Zelle, ACH
- Servicio de Cuentas en Línea y Móvil: Aplicaciones móviles nativas para iOS y Android, correo electrónico y gestión de mensajes push móviles y adaptadas a móviles
- Configuración y gestión de TI: Subcontratación y supervisión de servicios administrados, configuraciones basadas en la nube (AWS, Google, Azure), arquitecturas de TI optimizadas para cumplimiento PCI-DSS y GLBA, planes y procesos de continuidad de negocio y recuperación ante desastres

Ayudamos a los clientes a establecer su marco de cumplimiento mediante:

- Evaluar sus políticas y procesos existentes
- Creación de políticas personalizadas y procesos documentados donde sea necesario
- Capacitación del personal para cumplimiento regulatorio específico: AML/BSA & OFAC, UDAAP, Privacidad y GLBA, Robo de Identidad y Señales de Alerta, Reglamento E

Realizamos evaluaciones de seguridad y control de procesos mediante:

- Pruebas de penetración: "caja negra", "caja gris" según los estándares OWASP y PCI
- Asistencia PCI con cuestionarios de autoevaluación
- SOC 2, ISO 27001 trabajo de preparación antes de auditorías formales