CONSEJO DE LA MAGISTRATURA
ADMINISTRACION GENERAL
SUBDIRECCION DE CONTRATACIONES
SARMIENTO 877 - 7° PISO
C.P. 1041 - C.A.B.A
TEL 4370-2291 / 4370-2387
Mail: ag.oc@pjn.gov.ar

SELLAR CONFORME
LEY DE SELLOS CON $ .....
(SELLADO NACIONAL)

BUENOS AIRES, 5 DE SETIEMBRE DE 2024

ORDEN DE COMPRA N° 324/2024
EXPEDIENTE N° 1.703.100/2023
CONVOCATORIA: LICIT. PUBLICA 162/2024
DE FECHA 27 DE MARZO DE 2024
APROBADO POR RES. ADM.GRAL 3.111/2024
DE FECHA 3 DE SETIEMBRE DE 2024
VTO. PLAZO DE ENTREGA: 60 DIAS HABILES

SEÑOR(ES) KNOWLEDGE CONSULTING S.A.
JURAMENTO N°4874
C.P.: 1431 - CABA

T.E.: 62513130

SIRVASE REMITIR A: DIRECCION DE SEGURIDAD INFORMATICA
CON DOMICILIO EN: LAVALLE 1240- 1012 - CAPITAL FEDERAL -
LA PROVISION DE ELEMENTOS Y/O SERVICIOS QUE SE DETALLAN:

RENGLON	CANTIDAD	DESCRIPCION	PRECIOS EN $ UNITARIO	PRECIOS EN $ TOTAL
1 1	1	Provisión de un sistema de análisis de vulnerbilidades web estático y dinámico, con un plazo de ejecución de sesenta (60) días hábiles, a partir del día inmediato hábil siguiente a la notificación de la Orden de Compra.	323.028.000,00	323.028.000,00
2	5	Capacitación de la provisión del renglón 1, ítem 1.	3.199.400,00	15.997.000,00
		Renglón N°1, Item 3), Servicio de mantenimiento del sistema descripto en el renglón 1, ítem 1, a partir del día inmediato hábil siguiente a la recepción definitiva del ítem 1 y por un plazo de treinta y seis (36) meses. **RENGLON BONIFICADO**		
		IMPORTE TOTAL DE LA ORDEN DE COMPRA:		339.025.000,00 NETO
		SON: PESOS TRESCIENTOS TREINTA Y NUEVE MILLONES VEINTICINCO MIL		
		ORGANISMO SOLICITANTE: ========== DIRECCION GENERAL DE SEGURIDAD INFORMATICA, SITA EN LAVALLE 1240, C.A.B.A. EMAIL. dsi.direccion@pjn.gov.ar SUPERVISION: ========== LA SUPERVISION ESTARA A CARGO DE GABRIEL MILLARA TEL: 011-4124-4509. LUGAR DE ENTREGA: ========== LAVALLE 1240, CIUDAD AUTONOMA DE BUENOS AIRES Y SE DEBERA COORDINAR CON PERSONAL DESIGNADO POR LA DIRECCION GENERAL DE SEGURIDAD INFORMATICA INDICADO EN EL PUNTO X (ARTICULO 15) DEL PRESENTE ANEXO A LAS CLAUSULAS PARTICULARES. NOTA: ====		

IMPORTANTE: LA CONFORMIDAD DEFINITIVA DEBERA SER PRESTADA POR EL FUNCIONARIO TITULAR O SU REEMPLAZANTE NATURAL.

COPIA DE CONTROL

RENGLON	CANTIDAD	DESCRIPCION	PRECIOS EN $	
			UNITARIO	TOTAL
		LA PRESENTE ORDEN DE COMPRA ESTA EN UN TODO DE ACUERDO CON LA PROPUESTA DEL ADJUDICATARIO Y EL PLIEGO DE BASES Y CONDICIONES. SE DEJA CONSTANCIA QUE EN LA PRESENTE ORDEN DE COMPRA SE INCORPORO EL RENGLON 1, ITEM 3 DENTRO DEL RENGLON 1, ITEM 2, PORQUE AL ESTAR BONIFICADO, NO TIENE UN IMPORTE Y EL SISTEMA NO PERMITE GENERAR RENGLON SIN IMPORTE. NOTA: CON LA PRESENTACION DE FACTURAS, EL ADJUDICATARIO DEBERA ACREDITAR SU SITUACION IMPOSITIVA ANTE LA A.F.I.P. MEDIANTE LA CORRESPONDIENTE CONSTANCIA DE INSCRIPCION, Y PRESENTAR, DE POSEER, LOS CERTIFICADOS DE EXENCION IMPOSITIVA SOBRE LAS RETENCIONES EN CONCEPTO DE IMPUESTO A LAS GANANCIAS, I.V.A. O SISTEMA INTEGRAL DE JUBILACIONES Y PENSIONES *QUE PUDIERAN PROCEDER AL MOMENTO DE LOS RESPECTIVOS PAGOS.* FACTURACION: NO SE DARA CURSO A LA FACTURACION QUE NO SE PRESENTE ACOMPAÑADA DE LA CERTIFICACION DE RECEPCION DEFINITIVA, LA QUE DEBERA SER OTORGADA POR FUNCIONARIO, CON SELLO ACLARATORIO Y ANTEPONIENDO A LA LEYENDA "PROVISION PRESTADA DE CONFORMIDAD", LA FECHA DE RECEPCION Y DE OTORGAMIENTO DE LA RECEPCION DEFINITIVA (RES. C.S.J.N. NRO. 151 Y 543/90). LA/S MISMA/S DEBERA/N SER PRESENTADA/S EN LA MESA DE ENTRADA DE LA DIRECCION DE ADMINIST.FINANCIERA,SITA EN LA CALLE SARMIENTO 877 - PLANTA BAJA - CAPITAL FEDERAL. IVA: A LOS EFECTOS DE SU FACTURACION, EL CONSEJO DE LA MAGISTRATURA DEBERA SER CONSIDERADO IVA NO ALCANZADO. GARANTIA DEL CUMPLIMIENTO DEL CONTRATO: SI EL IMPORTE DE ESTA O/C SUPERA LA SUMA DE $ 1.000.000- DEBERA REMITIR A LA DIRECCION GENERAL DE ADMINISTRACION FINANCIERA LA PERTINENTE GARANTIA DE ADJUDICACION POR EL 10% DEL MONTO ADJUDICADO (RESOL.CM Nro. 254/2015 Y MODIFICATORIAS). LA MISMA DEBERA CONCRETARSE: HASTA LA SUMA DE $3.000.000- EN EFECTIVO O MEDIANTE PAGARE A SOLA FIRMA, LA QUE DEBERA ESTAR CERTIFICADA POR ENTIDAD BANCARIA A MENOS QUE DICHO DOCUMENTO HUBIERA SIDO SUSCRIPTO ANTE AUTORIDAD JUDICIAL QUE EXIGIERA LA ACREDITACION DE LA IDENTIDAD Y VINCULO CON LA EMPRESA POR PARTE DEL FIRMANTE. EL IMPORTE FALTANTE, HASTA CUBRIR EL REQUERIDO 10% SE PODRA COMPLETAR MEDIANTE AVAL O POLIZA DE CAUCION (CON FIRMA CERTIFICADA ANTE ESCRIBANO PUBLICO) O FIANZA BANCARIA. LA RUBRICA DEL ESCRIBANO DE AMBITO PROVINCIAL, *CERTIFICANTE DE LAS FIRMAS DE LA POLIZA DE CAUCION,* DEBERA ENCONTRARSE LEGALIZADA POR EL COLEGIO DE ESCRIBANO DE LA JURISDICCION. SI EN EL PRESENTE CONTRATO SE HA ESTIPULADO EL PAGO ANTICIPADO DE LA PROVISION O PRESTACION, DEBERA SER EXTENDIDA POR EL 100% DEL MONTO TOTAL ADJUDICADO. LA DOCUMENTACION ARRIBA CITADA DEBERA SER INGRESADA DENTRO DE LOS 5 DIAS CONTADOS A PARTIR DE LA FECHA DE NOTIFICACION DE LA ORDEN DE COMPRA, BAJO APERCIBIMIENTO DE RESCISION CONTRACTUAL. EL SIGUIENTE GASTO SERA APROPIADO A LA/S CUENTA/S: 05010000 020002 3 4 600000 11.3 15.997.000,00 05010000 020097 4 8 100000 11.3 323.028.000,00 DEL PRESUPUESTO GENERAL DE GASTOS, PARA EL EJERCICIO FINANCIERO DEL AÑO 2024.		

CONSEJO DE LA MAGISTRATURA Subdirección de Contrataciones

IMPORTANTE: LA CONFORMIDAD DEFINITIVA DEBERA SER PRESTADA POR EL FUNCIONARIO TITULAR O SU REEMPLAZANTE NATURAL.

COPIA DE CONTROL

María [illegible] Castro
SUBDIRECTORA GENERAL
CONSEJO DE LA MAGISTRATURA DE LA NACIÓN

CABA, 27 de marzo de 2024

CONSEJO DE LA MAGISTRATURA - PODER JUDICIAL DE LA NACION
LICITACION PUBLICA 162/24

CONSEJO DE LA MAGISTRATURA
ADMINISTRACIÓN GENERAL
SUBDIRECCIÓN DE CONTRATACIONES

La presente cotización se encuentra amparada en lo establecido por el Reglamento de Contrataciones del Consejo de la Magistratura aprobado por Resolución N° 254/15 y sus modificatorias y Resolución A.G. N° 77/18 y sus modificatorias.

ANEXO I

Sres. _____

_____

Calle _____

_____

SANDRA M. BLAZQUEZ
FIRMA FUNCIONARIO AUTORIZADO

RENGLON	ITEM	DESCRIPCION	CANT	C. UNITARIO $ (número y letras)	C. TOTAL $ (número y letras)
1	1	Provisión de un sistema de análisis de vulnerabilidades web estático y dinámico,con un plazo de ejecución de 60 días hábiles contados a partir del dia inmediato hábil siguiente a la notificación de la orden de compra, de acuerdo al Pliego de Bases y Condiciones.	1	**$ 323.028.000,-** Son pesos trescientos veintitrés millones, veintiocho mil. Incluye IVA	**$ 323.028.000,-** Son pesos trescientos veintitrés millones, veintiocho mil. Incluye IVA
	2	Capacitación de la provisión del renglón 1, ítem 1, de acuerdo al Pliego de Bases y Condiciones.	5 agentes	**$ 3.199.400,-** Son pesos tres millones ciento noventa y nueve mil cuatrocientos. Incluye IVA	**$ 15.997.000,-** Son pesos quince millones novecientos noventa y siete mil. Incluye IVA
	3	Servicio de mantenimiento del sistema descripto en el renglón 1, ítem 1, a partír del día inmediato hábil siguiente a la recepción definitva del ítem 1, si esta fuera posterior, y por el plazo de 36 meses, de acuerdo al Pliego de Bases y Condiciones.	36 meses	**BONIFICADO**	**BONIFICADO**
					$ 339.025.000,- Son pesos trescientos treinta y nueve millones veinticinco mil. Incluye IVA

OFERTA N° 1
MARINA HERNANDEZ
PROFESIONAL ADMINISTRATIVA
SUBDIRECCIÓN DE CONTRATACIONES

APERTURAS
SUBD. DE CONTRATACIONES
408

ALEJANDRO R. GARCÍA ROMÁN
KNOWLEDGE CONSULTING S.A.
CUIT: 30-71374700-5
PRESIDENTE

KCLATAM

Folio 149

Costo Total (Nro y letras)	**Son Pesos $ 339.025.000,- Son pesos trescientos treinta y nueve millones veinticinco mil. Incluye IVA**
Costo Global (Nro y letras) * Bonificación por adjudicación integra	NO APLICA
	ORGANISMO SOLICITANTE: DIRECCION GENERAL DE SEGURIDAD INFORMATICA. LA PLANILLA DE COTIZACION FORMA PARTE DEL PLIEGO DE BASES Y CONDICIONES

ALEJANDRO R. GARCÍA ROMÁN
KNOWLEDGE CONSULTING S.A.
CUIT: 30-71374700-5
PRESIDENTE

SUBD. DE CONTRATACIONES
APERTURAS
409

Solución Propuesta: Micro Focus Fortify

Introducción a la seguridad de Micro Focus

Micro Focus Security, es un proveedor líder de soluciones de seguridad para las organizaciones que desean mitigar el riesgo en un entorno híbrido y defenderse contra amenazas avanzadas. Basada en productos líderes en el mercado de ArcSight, Fortify y Voltage, la plataforma Micro Focus Security Intelligence and Risk Management (SIRM) permite a la organización adoptar un enfoque proactivo de la seguridad que integra la correlación de la información, el análisis profundo de las aplicaciones y los mecanismos de defensa a nivel de red, unificando los componentes de un programa de seguridad completo y reduciendo el riesgo en toda su empresa.

Micro Focus Security y la solución Micro Focus Security Fortify son ampliamente reconocidos como líderes en el mercado de pruebas de seguridad de aplicaciones.

Fortify fue clasificado como líder en el último cuadrante mágico de pruebas de seguridad de aplicaciones de Gartner. Fortify, ha estado presente en forma ininterrumpida como Líder en el cuadrante de Application Security Testing (AST) de Gartner desde su creación, en 2013 (9 años hasta la fecha), además de los cuadrantes relacionados previos desde el año 2009 (13 años en total hasta la fecha).

Según Gartner, "*Micro Focus tiene una de las ofertas de AST más completas, con excelentes capacidades para todas las principales tecnologías de AST, así como buenas capacidades para las nuevas áreas adicionales de AST.*

... Fortify es conocido por la profundidad y precisión de sus resultados, lo que satisface las necesidades de los clientes empresariales..."

Descripción de la Solución

Micro Focus® Fortify ofrece seguridad de aplicaciones como software y/o como servicio, brindando a los clientes las pruebas de seguridad, la gestión de vulnerabilidades, la experiencia y el soporte necesarios para crear, complementar y expandir fácilmente un programa de Software Security Assurance. Con estas soluciones y servicios automatizados los clientes pueden abordar los desafíos clave:

- **Enterprise Application Risk Management**

  Comprender el riesgo es un primer paso importante en cualquier iniciativa de seguridad de aplicaciones.

  Un portal centralizado permite a los clientes de Fortify crear un programa integral de garantía de seguridad del software a lo largo del tiempo. Los Dashboards brindan visibilidad de todo el portafolio de seguridad de aplicaciones de una organización, lo que permite ver el riesgo del programa, abordar problemas de seguridad críticos de manera temprana y priorizar los esfuerzos de remediación en muchos equipos y aplicaciones.

- **Secure Development**

  Encontrar y solucionar los problemas de seguridad de las aplicaciones de manera temprana, durante el desarrollo, es mucho menos costoso que esperar hasta que se haya implementado una aplicación, por lo que es fundamental capacitar a los desarrolladores para crear software seguro desde el principio.

KCLATAM

A. EJANDRO R. GARCIA ROMAN
KNOWLEDGE CONSULTING S.A.
CUIT: 30-71374700-5
PRESIDENTE

NANCY V. FERNANDEZ
SECRETARIA
Comisión de Preadjudica
PODER JUDICIAL de la

Folio 94

Totalmente integradas dentro del IDE donde trabajan los desarrolladores, las evaluaciones estáticas brindan comentarios inmediatos al desarrollador. El análisis de componentes de código abierto se puede agregar para evitar incluir componentes vulnerables conocidos. Los resultados de análisis auditados, incluidos los detalles de la línea de código y los consejos de remediación, ayudan a impulsar las mejores prácticas de codificación segura. A medida que las organizaciones maduran y adoptan los principios de DevOps, las evaluaciones estáticas de Fortify se pueden integrar completamente en la cadena de herramientas de desarrollo de software.

- **Security Testing – Testeos de Seguridad**

  La evaluación de la aplicación en ejecución en un entorno de control de calidad, prueba o ensayo simula las técnicas de hacking y los ataques del mundo real empleados por los atacantes.

  Para las aplicaciones web y los servicios web, las evaluaciones dinámicas emplean una combinación de técnicas de prueba automáticas y manuales para rastrear la superficie de ataque de la aplicación e identificar las vulnerabilidades explotables antes de implementar una versión de la aplicación en producción.

  Las evaluaciones móviles de Fortify on Demand utilizan el binario de la aplicación compilada y emplean una combinación de técnicas automatizadas y manuales para identificar vulnerabilidades en los tres niveles del ecosistema móvil: dispositivo cliente, red y servicios de back-end.

Características de Fortify

Testeo Estatico de Aplicaciones - Static Application Security Testing (SAST)
Las evaluaciones estáticas ayudan a los desarrolladores a identificar y eliminar vulnerabilidades en código fuente, binario o bytecode para crear software más seguro. Con la tecnología de Micro Focus Fortify Static Code Analyzer (SCA), las evaluaciones estáticas detectan más de 1.220 categorías únicas de vulnerabilidades en 30 lenguajes de programación que abarcan más de 1.000.000 API individuales.

Las evaluaciones estáticas de Fortify on Demand también incluyen nuestra innovadora plataforma de aprendizaje automático Fortify Scan Analytics para eliminar los falsos positivos y garantizar la calidad general para que los equipos de desarrollo puedan maximizar sus esfuerzos de remediación al principio del ciclo de vida del software. Fortify on Demand se adapta perfectamente a los procesos ágiles o DevOps existentes de los clientes con IDE listo para usar, servidor de compilación, integración continua e integraciones de seguimiento de errores y resultados de evaluación automatizados disponibles en minutos.

Dynamic Application Security Testing (DAST)
Las evaluaciones dinámicas imitan las técnicas y los ataques de hacking del mundo real utilizando técnicas automáticas y manuales para proporcionar un análisis completo de aplicaciones y servicios web complejos. Utilizando Fortify WebInspect para el análisis dinámico automatizado, se ofrece una experiencia completa, ya que todos los análisis incluyen la creación de macros para la autenticación, además de poder incluir una auditoría completa de los resultados para eliminar los falsos positivos y para la calidad general. Nuestras pruebas se centran en los tipos de vulnerabilidades que explotan los atacantes, incluida la autenticación, el control de acceso, la validación de entrada, la gestión de sesiones y las pruebas de lógica empresarial.

KCLATAM

ALEJANDRO R. GARCIA ROMAN
KNOWLEDGE CONSULTING S.A.
CUIT: 30-71374700-5
PRESIDENTE

NANCY V. FERNANDEZ
SECRETARIA
Comisión de Preadjudic.
PODER JUDICIAL de T.-Folio 95

OF I

Estrategia de implementación

Micro Focus Security Fortify ha utilizado la experiencia para desarrollar una metodología de implementación de 5 pasos como se describe a continuación.

Descubrimiento - Discover
El objetivo de la fase 'Descubrir' es identificar las aplicaciones web y móviles de las que la organización es responsable y realizar una clasificación de riesgo inicial de esos activos.

Esta información se carga en la plataforma de Fortify.

Parcheo - Patch
Esta fase consiste en utilizar las pruebas de seguridad de aplicaciones dinámicas de Fortify WebInspect para aplicaciones web y las pruebas de seguridad de aplicaciones móviles de FoD para aplicaciones móviles a fin de probar las aplicaciones de alto riesgo identificadas durante el "descubrimiento" y probar cualquier vulnerabilidad crítica.

Si se encuentran vulnerabilidades críticas, la organización puede optar por:

- Retirar o reemplazar la aplicación
- Bloquee la vulnerabilidad usando un WAF/IPS basado en el archivo de reglas generado por la prueba WebInspect
- Usar la información de la evaluación de Fortify para corregir la vulnerabilidad

Puerta de Seguridad - Security Gate
Para administrar de manera efectiva el riesgo de seguridad de las aplicaciones, las organizaciones deben probar y aprobar todas las aplicaciones antes de que entren en producción. El primer paso es definir una política de seguridad que defina un nivel de seguridad aceptable para las aplicaciones en función de su categoría de riesgo. Luego, esta política se incorpora a los estándares de desarrollo internos y se agrega a los contratos de proveedores externos. Para comunicar la política, debe incluirse en el programa de capacitación de concientización sobre seguridad de la organización.

Para hacer cumplir la política, la organización debe usar Fortify como una puerta de seguridad con el enfoque inicial en la prueba dinámica de todas las aplicaciones nuevas y las versiones principales de las aplicaciones existentes. La organización también debe establecer una fecha para probar y corregir las aplicaciones existentes.

Shift-Left - DevOps
La forma más rentable de entregar aplicaciones seguras es hacer que forme parte del ciclo de vida del desarrollo. Para hacer esto, las organizaciones deben integrar las pruebas de seguridad de aplicaciones estáticas Fortify en su SDLC. Las pruebas de seguridad de aplicaciones estáticas Fortify son adecuadas para todos los enfoques de desarrollo, desde la cascada tradicional hasta DevOps, pero la mayoría de los clientes están adoptando un enfoque DevOps.

DevOps está cambiando la forma en que se desarrollan las aplicaciones. Reúne a personas de negocios, desarrollo, operaciones y control de calidad en un solo equipo para entregar un proceso comercial en línea al mercado más rápidamente. La característica clave son los ciclos de liberación muy rápidos.

Para lograr estos ciclos de lanzamiento rápido, la automatización de la cadena de herramientas de desarrollo es clave.

KCLATAM

ALEJANDRO R. GARCIA ROMAN
KNOWLEDGE CONSULTING S.A.
CUIT: 30-71374700-5
PRESIDENTE

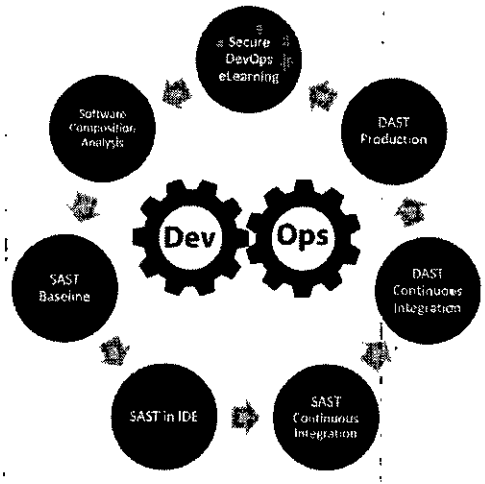
NANCY V. FERNANDEZ
SECRETARIA
Comisión de Preadjudic
PODER JUDICIAL de l
Folio 96

OF.

La seguridad se percibe como un inhibidor de este ciclo de liberación rápida. En particular, un enfoque de prueba de penetración es demasiado lento.

En general, se acepta que la mejor forma de ofrecer una aplicación segura es crear seguridad desde el principio. Con DevOps es la única forma de entregar aplicaciones seguras. Los equipos de DevOps deben implementar un ciclo de vida de desarrollo seguro que incorpore una variedad de controles de seguridad.

Micro Focus Security Fortify proporciona todos estos controles de seguridad, disponibles bajo demanda y respaldados por expertos en seguridad.



Static Application Security Testing Baseline

La prueba de seguridad de aplicaciones estáticas (SAST) inspecciona el código fuente de la aplicación en busca de patrones de codificación inseguros que generen vulnerabilidades. La mayoría de los proyectos no comienzan desde cero, sino que se basan en un código base existente y es esencial que sea seguro.

Una evaluación de referencia de Fortify SAST realizará una prueba completa del código utilizando Fortify SCA, el producto SAST líder en la industria. Luego, los resultados son presentados nuevamente en el portal Fortify Software Security Center para facilitar una reparación rápida.

Static Application Security Testing in IDE

Ahora que la línea de base es segura, desea evitar que se agreguen nuevas vulnerabilidades al código base. Fortify Security Assistant es un complemento para el entorno de desarrollo integrado (IDE) que verifica el código en tiempo real a medida que el desarrollador escribe. Esto proporciona comentarios instantáneos para los desarrolladores sobre ciertos tipos de vulnerabilidades de seguridad.

Static Application Security Testing como parte de Integracion Continua (Continuous Integration)

ALEJANDRO R. GARCIA ROMAN
KNOWLEDGE CONSULTING S.A.
CUIT: 30-71374700-5
PRESIDENTE

NANCY V. FERNANDEZ
SECRETARIA
Comisión de Preadjudic
PODER JUDICIAL de la

Folio 97

No todas las vulnerabilidades de seguridad se pueden descubrir mediante la inspección de módulos de código individuales. También es necesario realizar un escaneo SAST completo con cada compilación.

Fortify on Demand se puede integrar a la perfección con herramientas de integración continua como Jenkins y Microsoft Azure DevOps para realizar un SAST completo para cada compilación. Para garantizar un tiempo de respuesta rápido, Fortify tiene un modo especial opcional que incorpora aprendizaje automático para minimizar los falsos positivos.

Testeo Dinámico de Seguridad de Aplicaciones - Dynamic Application Security Testing

El otro tipo de prueba de seguridad de aplicaciones es la prueba de seguridad de aplicaciones dinámicas (DAST). Las pruebas de seguridad de aplicaciones dinámicas intentan acceder a la aplicación en ejecución utilizando las mismas técnicas que utiliza un hacker. Por esta razón, se puede encontrar las vulnerabilidades que tienen más probabilidades de ser explotadas.

La mejor práctica de seguridad es probar dinámicamente cada versión antes de que entre en producción. Sin embargo, los rápidos ciclos de lanzamiento de DevOps a menudo significan que esto no es práctico. Por lo tanto, en su lugar, se debe usar DAST para cualquier versión crítica de seguridad y de forma periódica en producción.

Maduración - Mature

Todos los programas de seguridad deben evolucionar continuamente para gestionar el riesgo. Una vez que se implementan los controles básicos, las organizaciones deben comenzar a elevar la base de seguridad, por ejemplo, abordando la siguiente categoría de vulnerabilidades de gravedad. Además, el programa debe considerar las aplicaciones internas, no solo las externas.

También vale la pena señalar que, por lo general, solo en esta etapa las organizaciones han alcanzado la madurez suficiente para comenzar a transferir el costo total de la seguridad de la aplicación a sus terceros.

Descripción de componentes y servicio

Static Application Security Testing (SAST) y Infrastructure as Code (IaC)

Micro Focus Security Fortify Static Code Analyzer ayuda a las organizaciones a verificar que el software es confiable, reducir costos, aumentar la productividad e implementar las mejores prácticas de codificación segura. Static Code Analyzer escanea el código fuente, identifica las causas raíz de las vulnerabilidades de seguridad del software, correlaciona y prioriza los resultados, lo que le brinda orientación de línea de código para solucionar las vulnerabilidades de seguridad. Para verificar que los problemas más graves se aborden primero, correlaciona y prioriza los resultados para ofrecer una lista precisa y clasificada de riesgos.

Beneficios principales

- Reducir el riesgo mediante la identificación de vulnerabilidades que representan la mayor amenaza
- Identificación y eliminación ágil de las vulnerabilidades explotables con un proceso repetible
- Reducción de costos de desarrollo mediante la identificación de vulnerabilidades al principio del ciclo de vida de desarrollo de software
- Educar a los desarrolladores en prácticas de codificación segura mientras trabajan

KCLATAM

ALEJANDRO R. GARCIA ROMAN
KNOWLEDGE CONSULTING S.A.
CUIT: 30-71374700-5
PRESIDENTE

NANCY V. FERNANDEZ
SECRETARIA
Comisión de Preadjudicación
PODER JUDICIAL de la

Folio 98

- Reunir a los equipos de desarrollo y seguridad para encontrar y solucionar problemas de seguridad

Con Fortify Static Code Analyzer se puede identificar las causas raíz de las vulnerabilidades de seguridad en el código fuente, recibir resultados priorizados ordenados por gravedad de riesgo y obtener orientación sobre cómo corregir vulnerabilidades en detalle de línea de código. Como resultado, se puede asegurar que el software sea confiable, reducir los costos de encontrar y corregir vulnerabilidades de aplicaciones y establecer las bases para las mejores prácticas de codificación segura.

Encontrando las vulnerabilidades

Para procesar el código, Fortify Static Code Analyzer funciona de manera muy similar a un compilador, que lee archivos de código fuente o una colección de archivos y los convierte en una estructura intermedia optimizada para el análisis de seguridad. Este formato intermedio se utiliza para localizar vulnerabilidades de seguridad. El motor de análisis, que consta de múltiples analizadores especializados, utiliza reglas de codificación segura para analizar la base de código en busca de violaciones a las prácticas de codificación segura. Fortify Static Code Analyzer también proporciona un generador de reglas para que pueda ampliar y ampliar las capacidades de análisis y poder incluir reglas personalizadas. Los resultados se pueden ver de varias maneras, dependiendo de la audiencia y la tarea.

Gestión de resultados

Las capacidades de colaboración basadas en web de Fortify Static Code Analyzer proporcionan un espacio de trabajo y un repositorio compartidos para que los profesionales, desarrolladores y administradores de seguridad de aplicaciones trabajen juntos en las revisiones de código y las actividades de corrección. Los profesionales de la seguridad y los desarrolladores pueden trabajar juntos de la manera que mejor se adapte a ellos, utilizando interfaces específicas para cada rol.

Diseñado específicamente para el profesional de la seguridad de aplicaciones, Audit Workbench de Fortify Static Code Analyzer proporciona los medios para analizar vulnerabilidades individuales, asignarlas para su corrección y realizar un seguimiento de las actividades hasta su finalización. Audit Workbench facilita a los clientes potenciales de seguridad investigar, verificar, comentar y establecer niveles de gravedad en los problemas a través de la navegación inteligente por código y las funciones intuitivas de la interfaz de usuario.

Los desarrolladores pueden abordar problemas en su entorno de desarrollo preferido mientras colaboran con el equipo de seguridad mediante complementos para Eclipse, Microsoft Visual Studio, Microsoft Visual Studio Code, IntelliJ o Android Studio. Con Fortify Static Code Analyzer, los desarrolladores aprenden sobre la codificación segura mientras corrigen vulnerabilidades. Para cada vulnerabilidad identificada, Fortify Static Code Analyzer proporciona información de referencia al desarrollador, describiendo el problema y las formas de solucionarlo en el lenguaje de programación específico del desarrollador. Esto ayuda a mitigar las vulnerabilidades de seguridad al principio del ciclo de desarrollo y refuerza las prácticas de codificación segura.

Con Fortify Static Code Analyzer, se puede verificar que el software que se ejecuta en la organización es confiable, reducir los costos de encontrar y corregir vulnerabilidades de aplicaciones, aumentar la productividad de los equipos de auditoría de seguridad y desarrolladores, mejorar los procesos de revisión de seguridad y sentar las bases para las mejores prácticas de codificación segura. Con Fortify Static Code Analyzer, se tiene una solución que convierte las políticas de seguridad únicas en

KCLATAM

ALEJANDRO R. GARCIA ROMAN
KNOWLEDGE CONSULTING S.A.
CUIT: 30-71374700-5
PRESIDENTE

NANCY V. FERNANDEZ
SECRETARIA
Comisión de Preadjudica
PODER JUDICIAL de l

Folio 99

código seguro, el código seguro en aplicaciones seguras y las aplicaciones seguras en procesos empresariales seguros.

Static Code Analyzer (SCA) utiliza múltiples algoritmos y una amplia base de conocimientos de reglas de codificación segura para analizar el código fuente de una aplicación en busca de vulnerabilidades explotables. Esta técnica analiza cada ruta factible que la ejecución y los datos pueden seguir para identificar y remediar las vulnerabilidades. Fortify SCA identifica la causa raíz de las vulnerabilidades de seguridad en el código fuente, prioriza los problemas más graves al clasificarlos con el riesgo y proporciona una guía detallada sobre cómo solucionarlos para que los desarrolladores puedan resolver problemas con menos esfuerzo y en menos tiempo, todo mientras educan y crean conocimientos de codificación segura. Micro Focus Fortify SCA detecta más de 1.220 categorías de vulnerabilidad únicas, en 30 lenguajes de desarrollo, y cuenta con más de 1.000.000 API a nivel de componente. A continuación, el detalle de los lenguajes soportados por Fortify Static Code Analyzer:

Lenguaje	Versión	Plataforma	Fuente	Binario/Byte
.NET Framework	2.0 – 4.8	.NET	Sí	Sí
.NET	5.0 – 6.0	.NET	Sí	Sí
.NET core	2.0 - 3.1	.NET	Sí	Sí
ABAP/BSP	6	SAP	Sí	n/a
Action Script	3.0	Basado en plugins de navegador, por ejemplo, Flash Player	Sí	n/a
Apex	3.6	Visualforce	Sí	n/a
C#	5, 6, 7, 8, 9, 10	.NET	Sí	Sí
C/C++	C11, C++11, C++14, C++17, C++20	AIX, Linux, HP-UX, Mac OS, Solaris, Windows	Sí	No
ASP clásico (con VBScript)	2.0,3.0	Windows	Sí	n/a
Cobol	IBM Enterprise COBOL para z/OS 6.1 (y anteriores) con CICS, IMS, DB2, y IBM MQ Micro Focus Visual COBOL 6.0	IBM Enterprise COBOL con z/OS Micro Focus COBOL	Sí	no
Coldfusion	8, 9, 10	Diferentes plataformas	Sí	n/a
Go	1.12, 1.13, 1.14, 1.15, 1.16, 1.17	Windows y Linux	Sí	Sí
HCL Terraform	2.0	IaC	Sí	n/a
HTML	5 y anteriores	Explorador	Sí	n/a

KCLATAM

ALEJANDRO R. GARCIA ROMAN
KNOWLEDGE CONSULTING S.A.
CUIT: 30-71374700-5
PRESIDENTE

NANCY V. FERNANDEZ
SECRETARIO
Comisión de Preadjudicación
PODER JUDICIAL de la Nación

100

OF 1

Lenguaje	Versión	Plataforma	Fuente	Binario/Byte
Java (incluido Android)	7, 8, 9, 10, 11, 12, 13, 14, 17	[Independiente de la plataforma]	Sí	Sí
JavaScript/AJAX	ECMAScript 2015–2021	[Independiente de la plataforma]	Si	n/a
JSON	ECMA-404	[Independiente de la plataforma]	Sí	n/a
JSP	1.2, 2.1	Java	Sí	n/a
Kotlin	1.3.50, 1.4.20, 1.5.30	[Plataforma independiente]	Sí	No
MXML(Flex)	4	Basado en plugins de navegador	Sí	n/a
Objective-C	2.0	iOS	Sí	No
PHP	7.3, 7.4, 8.0	Diferentes plataformas, generalmente Unix / Linux / Windows	Sí	n/a
PL/SQL	8.1.6	Oracle, IBM DB2	Sí	n/a
Python	2.6 - 2.7, 3.x (3.9 y antes)	Diferentes plataformas, generalmente Unix / Linux / Windows	Sí	n/a
Ruby	1.9.3	Diferentes Plataformas	Sí	n/a
Scala	2.11, 2.12, 2.1.3	[Plataforma independiente]	Sí	No
Swift	5.4, 5.4.2, 5.5, 5.5.1, 5.5.2, 5.6, 5.6.1	iOS	Sí	No
T-SQL	SQL Server 2005, 2008, 2012	SQL Server 2005, 2008, 2012	Sí	n/a
TypeScript	2.8, 3.x, 4.0, 4.1, 4.2, 4.3, 4.4, 4.5	Diferentes Plataformas	Sí	n/a
VB.NET	11,14,15.x,16.0	.NET	Sí	Sí
Visual Basic (VB)	6.0	Windows	Sí	n/a
Visual Basic Script (VBS)	2.0, 5.0	Windows	Sí	n/a
XML	1.0	[Plataforma independiente]	Sí	n/a

KCLATAM

ALEJANDRO R. GARCIA ROMAN
KNOWLEDGE CONSULTING S.A.
CUIT: 30-71374700-6
PRESIDENTE

NANCY V. FERNANDEZ
SECRETARIA
Comisión de Preadjudicación
PODER JUDICIAL de la Nación

Folio 101

Lenguaje	Versión	Plataforma	Fuente	Binario/Byte
YAML	1.2	Diferentes Plataformas	Sí	n/a

Diferenciadores de Fortify Static Code Analyzer

- Uno de los más precisos del mercado y detecta una amplia gama de vulnerabilidades.
- Se integra fácilmente en cualquier entorno a través de scripts, complementos y herramientas de GUI para que los desarrolladores puedan ponerse en marcha de forma rápida y sencilla.
- Se puede probar y mantener la seguridad de las aplicaciones independientemente del lenguaje de desarrollo o de si está construido internamente, subcontratado, de terceros, de código abierto o móvil.
- Admite una amplia variedad de lenguajes, plataformas y frameworks para permitir revisiones de seguridad en entornos mixtos.
- Identifica vulnerabilidades en el código fuente, las prioriza por gravedad y ofrece orientación de corrección.
- Reúne a los equipos de desarrollo y seguridad para encontrar, revisar y solucionar problemas de seguridad para reducir el riesgo, el tiempo y los costos del software.
- Escalable con el creciente número de aplicaciones en las organizaciones.
- Gestión de forma proactiva de los requisitos de riesgo y compliance.
- Cuenta con el apoyo de Micro Focus Software Security Research Group, un equipo global reconocido como una de las principales organizaciones de seguridad para monitorear amenazas emergentes, y cuyo conocimiento se canaliza a Fortify Static Code Analyzer.

ScanCentral SAST

Cuando se dispone de múltiples máquinas capaces de realizar escaneo estático, y se pretende automatizar, se puede gestionar sus recursos de una mejor manera que solicitar cada análisis SAST en forma separada. Para eso, existe ScanCentral SAST que administra múltiples máquinas escaneadoras (sensores). De esa manera, se hace mucho más sencillo integrar múltiples instancias de Fortify Static Code Analyzer con otras soluciones que necesiten iniciar análisis estático.

Una instalación de ScanCentral SAST incluye los siguientes componentes:

- **ScanCentral Client:** Una máquina en la que Static Code Analyzer traduce el código, con múltiples parámetros posibles, y lo sube al ScanCentral Controller.

Esta interfaz se instala en los clientes que necesiten iniciar escaneos (como puede ser por ejemplo, una instancia de Jenkins).

- **ScanCentral Controller:** Servidor que recibe el código traducido desde los ScanCentral clientes, y lleva la información a los ScanCentral Sensors, además de subir opcionalmente los resultados a Software Security Center (SSC).
- **ScanCentral Sensors:** Red distribuida de máquinas que pueden realizar análisis estático, y que pueden recibir solicitudes de escaneo con código traducido. En el caso de tratarse de un lenguaje soportado, los sensores también pueden realizar la traducción del código fuente.

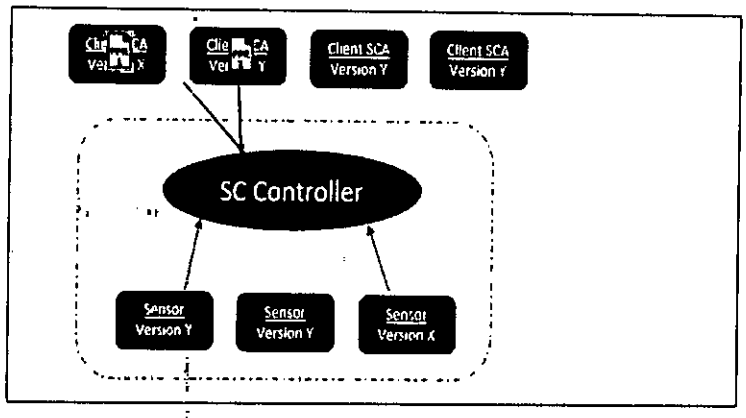
ALEJANDRO R. GARCIA ROMAN
KNOWLEDGE CONSULTING S.A.
CUIT: 30-71374700-5
PRESIDENTE

NANCY V. FERNANDEZ
SECRETARIA
Comisión de Preadjudicación
PODER JUDICIAL de la Nación

Folio 102

Lenguajes soportados para traducir en ScanCentral en la versión 22.1:
https://www.microfocus.com/documentation/fortify-software-security-center/2210/SC_SAST_Help_22.1.0/index.htm#Create_CS_Clients.htm?TocPath=About%2520Clients%257C_____1

A continuación, se muestra una arquitectura funcional de ejemplo con ScanCentral SAST, con el flujo explicado.



Dynamic Application Security Testing (DAST) y Interactive Application Security Testing (IAST)

Análisis Dinámico

El análisis dinámico de seguridad de aplicaciones (DAST) es el proceso de analizar una aplicación web a través del front-end para encontrar vulnerabilidades a través de ataques simulados. Este tipo de enfoque evalúa la aplicación desde "afuera hacia adentro" atacando una aplicación como lo haría un usuario malintencionado. Después de que un escáner DAST realiza estos ataques, busca resultados que no forman parte del conjunto de resultados esperado e identifica vulnerabilidades de seguridad.

DAST es importante porque los desarrolladores no tienen que depender únicamente de su propio conocimiento al crear aplicaciones. Al realizar DAST durante el SDLC, puede detectar vulnerabilidades en una aplicación antes de que se implemente al público. Si estas vulnerabilidades no se controlan y la aplicación se implementa como tal, esto podría provocar una violación de datos, lo que provocaría una gran pérdida financiera y daños a la reputación de su marca. El error humano inevitablemente desempeñará un papel en algún momento del ciclo de vida de desarrollo de software (SDLC), y cuanto antes se detecte una vulnerabilidad durante el SDLC, más barato será repararla. Cuando DAST se incluye como parte de la canalización de Integración continua/Desarrollo continuo (CI/CD), esto se denomina "DevOps seguro" o "DevSecOps".
Un escáner DAST busca vulnerabilidades en una aplicación en ejecución y luego envía alertas automáticas si encuentra fallas que permiten ataques como inyecciones SQL, Cross-Site Scripting (XSS) y más. Dado que las herramientas DAST están equipadas para funcionar en un entorno dinámico, pueden detectar fallas de tiempo de ejecución que las herramientas SAST no pueden identificar.

KCLATAM

ALEJANDRO R. GARCIA ROMAN
KNOWLEDGE CONSULTING S.A.
CUIT: 30-71374700-5
PRESIDENTE

NANCY V. FERNANDEZ
SECRETARIA
Comisión de Preadjudicación
PODER JUDICIAL de la

Folio 103

Para usar el ejemplo de un edificio, un escáner DAST puede considerarse como un guardia de seguridad. Sin embargo, en lugar de asegurarse de que las puertas y ventanas estén cerradas con llave, este guardia va un paso más allá al intentar entrar físicamente al edificio. El guardia podría intentar forzar las cerraduras de las puertas o romper las ventanas. Después de terminar este examen, el guardia podría informar al administrador del edificio y brindarle una explicación de cómo pudo ingresar al edificio. Se puede pensar en un escáner DAST de la misma manera: intenta activamente encontrar vulnerabilidades en un entorno en ejecución para que el equipo de DevOps sepa dónde y cómo solucionarlas.

Descripción de la solución

WebInspect es una solución DAST automatizada que proporciona una detección integral de vulnerabilidades y ayuda a los profesionales de seguridad y evaluadores de control de calidad a identificar vulnerabilidades de seguridad y problemas de configuración. Lo hace simulando ataques de seguridad externos del mundo real en una aplicación en ejecución para identificar problemas y priorizarlos para el análisis de causa raíz. WebInspect tiene numerosas API REST para beneficiar la integración y tiene la flexibilidad de administrarse a través de una interfaz de usuario intuitiva o ejecutarse completamente a través de la automatización.

Micro Focus Fortify WebInspect proporciona pruebas de seguridad de aplicaciones dinámicas automatizadas para que pueda escanear y corregir vulnerabilidades de aplicaciones web explotables.

Por lo general, DAST se realiza después de la producción, ya que emula ataques en una aplicación en ejecución; pero al tomar la decisión de "Desplazar DAST a la izquierda" (mover DAST antes en el proceso de desarrollo) puede detectar vulnerabilidades antes, lo que ahorra tiempo y dinero. Fortify WebInspect incluye políticas de análisis prediseñadas, lo que equilibra la necesidad de velocidad con los requisitos de las organizaciones.

Fortify WebInspect también incluye una función de análisis incremental, que permite evaluar rápidamente las vulnerabilidades solo en las áreas de la aplicación que han cambiado.

Fortify WebInspect permite:

- Asegurar DevOps con DAST automatizado
- Administrar el riesgo de AppSec a escala
- Lograr el cumplimiento de las principales normas de seguridad de datos
- Desplazar DAST a la izquierda (ShiftLeft)
- Rastrear frameworks y API modernos
- Crear una estrategia de AppSec más fuerte

Automatización con Integración

WebInspect se puede ejecutar como una solución totalmente automatizada para satisfacer las necesidades de escalado y DevOps, e integrarse con el SDLC sin agregar gastos adicionales.

Las API REST ayudan a lograr una integración más estrecha y ayudan a automatizar los análisis y comprobar si se han cumplido los requisitos de cumplimiento.

Integraciones preconstruidas para Micro Focus Application Lifecycle Management (ALM) y Quality Center, y otros sistemas de administración y pruebas de seguridad.

KCLATAM

ALEJANDRO R. GARCIA ROMAN
KNOWLEDGE CONSULTING S.A.
CUIT: 30-71374700-5
PRESIDENTE

NANCY V. FERNANDEZ
SECRETARIA
Comisión de Preadjudicio
PODER JUDICIAL de la

Folio 104

Las integraciones permiten a los equipos reutilizar scripts y herramientas existentes. WebInspect puede integrarse fácilmente con cualquier script de Selenium.

Escanear servicios web RESTful: admite formatos Swagger y OData a través de la herramienta de línea de comandos WISwag, lo que permite que WebInspect se adapte a cualquier canalización de DevOps.

Configuración básica: ScanCentral Admin puede preconfigurar una plantilla de escaneo y proporcionarla a los usuarios para escanear sus aplicaciones, sin necesidad de conocimientos de seguridad.

Hallazgo de vulnerabilidades

WebInspect se puede ajustar y optimizar para encontrar vulnerabilidades en el SDLC. Es posible utilizar también tecnología de agentes que amplía la cobertura de la superficie de ataque y detecta tipos adicionales de vulnerabilidades.

WebInspect Agent integra pruebas dinámicas y análisis de tiempo de ejecución para mejorar sus hallazgos y alcance. Identifica vulnerabilidades rastreando más de la aplicación, ampliando la cobertura de la superficie de ataque y exponiendo exploits mejor que las pruebas dinámicas por sí solas.

WebInspect realiza la Priorización con tecnologías avanzadas:

- Políticas personalizadas que se ajustan a alta velocidad con el administrador de políticas
- Crawling y auditoría simultáneos
- Deduplicación: Reducción del número de ataques enviados, al evitar escanear la misma clase/función en una parte diferente de la aplicación.
- Evasión de verificación: reducción del número de ataques enviados evitando enviar múltiples ataques a un tipo de verificación específico si el agente determina que la aplicación puede manejar el ataque. La información se carga en Fortify Software Security Center (SSC) y se usa con los resultados del análisis de Fortify Static Code Analyzer donde se correlacionan los problemas.
- La detección de páginas redundantes permite tiempos de escaneo reducidos.

Crawling de frameworks y tecnologías web modernas

La evaluación de la aplicación en ejecución en un entorno de control de calidad, prueba o ensayo.

WebInspect realiza crawling de frameworks y tecnologías web modernas con una auditoría integral de todas las clases de vulnerabilidad.

Compatibilidad con las últimas tecnologías web, incluidas HTML5, JSON, AJAX, JavaScript, HTTP2 y más.

Una nueva clase de vulnerabilidades denominadas "Fuera de banda" o vulnerabilidades OAST. Con el servidor OAST de Fortify público, WebInspect puede detectar vulnerabilidades de OAST como Log4Shell.

Detección de aplicaciones Single Page (SPA) compatible con estos frameworks comunes: Angular, AngularJS, React, GWT, Vue, Dojo y Backbone.

Análisis de sitios web optimizados para dispositivos móviles, así como llamadas de servicios web nativos.

KCLATAM

ALEJANDRO R. GARCIA ROMAN
KNOWLEDGE CONSULTING S.A.
CUIT: 30-71374700-5
PRESIDENTE

NANCY V. FERNANDEZ
SECRETARIA
Comisión de Preadjudic
Folio 105

WebInspect proporciona características como la generación automática de macros, la validación de macros y la validación de correcciones, para permitir que los equipos pequeños detecten y reparen las vulnerabilidades a escala.

Una solución para los problemas de bloqueo de SCHANNEL, OpenSSL Preview proporciona una solución simple para entornos donde SSL está restringido por el registro o la política de grupo.

Software Security Center

Fortify Software Security Center ayuda a los profesionales de la seguridad, los especialistas en control de calidad (QA) y los desarrolladores a facilitar la seguridad de las aplicaciones web en toda la organización. Con Software Security Center, se puede reducir el riesgo general de las aplicaciones nuevas y operativas al tiempo que ahorra tiempo y dinero al abordar las vulnerabilidades a lo largo de todo el ciclo de vida de la aplicación.

Se puede clasificar y corregir rápidamente las vulnerabilidades mediante el uso de los analizadores estáticos y dinámicos de Fortify Software Security Center Server. Los equipos de seguridad y desarrollo obtienen un espacio de trabajo y un repositorio colaborativos basados en la web para trabajar juntos utilizando interfaces específicas de cada rol. Los desarrolladores obtienen información de referencia detallada, describiendo problemas y dando instrucciones detalladas para solucionarlos, en el lenguaje de programación del código en cuestión, lo que les ayuda a aprender sobre las prácticas de codificación segura.

Fortify Software Security Center permite a cualquier organización de cualquier tamaño automatizar cualquiera o todos los aspectos de un programa SSA exitoso. Fortify Software Security Center puede ayudar principalmente en los siguientes elementos:

- Solucionar los problemas de seguridad inmediatos en el software que ya ha implementado.
- Reducir el riesgo sistémico en el software que se está desarrollando o adquiriendo de los proveedores.
- Cumplir con los objetivos de compliance de los mandatos de seguridad internos y externos.

Características Principales

- Proporciona una imagen precisa del riesgo de software en toda la organización.
- Repositorio central que proporciona visibilidad de todo el programa de pruebas de seguridad de aplicaciones.
- Plataforma para clasificar, auditar, priorizar y remediar los resultados.
- Revisa, gestiona y realiza un seguimiento de las actividades de pruebas de seguridad en toda la organización.
- Ofrece actualizaciones sobre el estado de seguridad, las tendencias, el cumplimiento y la generación de informes.
- Permite que los equipos de seguridad y desarrollo colaboren para resolver problemas de seguridad.
- Reduce el tiempo para encontrar y solucionar problemas de vulnerabilidad en el software.
- Reduce los costos asociados con el desarrollo, la remediación y el cumplimiento.
- Aumenta la productividad mediante la automatización de los procedimientos de seguridad de las aplicaciones.
- Acelera el tiempo de comercialización al garantizar menos retrasos relacionados con la seguridad.

KCLATAM

ALEJANDRO R. GARCIA ROMAN
KNOWLEDGE CONSULTING S.A.
CUIT: 30-71374700-5
PRESIDENTE

NANCY V. FERNANDEZ
SECRETARIA
Comisión de Preadjudicación
PODER JUDICIAL de la Nación

Folio 106

Con Fortify Software Security Center proporciona capacidades inigualables en dos áreas principales, diseñadas para ayudar a alcanzar los objetivos de seguridad de software más esenciales:

- **Pruebas de seguridad**: identificar vulnerabilidades explctables en menos tiempo y con menos esfuerzo, sin importar cómo o dónde se origine su software.
- **Ciclo de vida de desarrollo seguro**: trabajar con desarrollo y los proveedores para solucionar los problemas de seguridad rápidamente en el software implementado y garantizar que la seguridad esté integrada en todo el software futuro desde el principio.

Las pruebas de seguridad con Fortify Software Security Center ayudan a obtener rápidamente una imagen precisa del riesgo en las aplicaciones, independientemente de si se desarrollan internamente o por proveedores. Proporciona el conjunto más amplio de capacidades de pruebas de seguridad disponibles, tales como:

- Análisis estático, también conocido como Static Application Security Testing (SAST), disponible a través de Fortify Static Code Analyzer (SCA):
  - Detecta más tipos de vulnerabilidades potenciales que cualquier otro método de detección
  - Identifica la causa raíz de las vulnerabilidades con detalles de línea de código
  - Ayuda a identificar problemas críticos durante el desarrollo cuando son más fáciles y menos costosos de solucionar
- Análisis dinámico, también conocido como pruebas dinámicas de seguridad de aplicaciones (DAST), disponible a través de WebInspect
  - Detecta vulnerabilidades en la ejecución de aplicaciones web y servicios web mediante la simulación de escenarios de ataque completos
  - Valida si una vulnerabilidad en particular es de hecho realmente explotable
  - Acelera la corrección al permitir saber con certeza qué problemas abordar primero y por qué

Manejo del riesgo de software en toda la organización

Con capacidades versátiles como las que se ofrecen en el servidor de Fortify Software Security Center, los componentes seguros del ciclo de vida del desarrollo proporcionan todo lo necesario para garantizar que los equipos de desarrollo y los proveedores externos puedan eliminar de manera eficiente el riesgo de todas las aplicaciones, ya sea que se implementen actualmente, en desarrollo o en planificación.

Gestión de la corrección

Con Fortify Software Security Center, diversos equipos de seguridad y desarrollo pueden trabajar juntos como uno solo para clasificar, corregir, rastrear, validar y administrar rápidamente los problemas de vulnerabilidad en el software implementado. Los entornos de colaboración compartidos y los conjuntos de herramientas de auditoría permiten al personal clave aplicar procesos repetibles y automatizados para abordar los problemas de manera más rápida y rentable. Además, aceleran aún más la corrección porque se integran con entornos de desarrollo integrado (IDE) estándar de la industria, herramientas de garantía de calidad (QA) y sistemas de seguimiento de errores.

LATAM

ALEJANDRO R. GARCIA ROMAN
KNOWLEDGE CONSULTING S.A.
CUIT: 30-71374700-5
PRESIDENTE

NANCY V. FERNANDEZ
SECRETARIA
Comisión de Preadjudicación
PODER JUDICIAL de la Nación

Folio 107

Gestión proactiva de la seguridad del software

La suite de Fortify Software Security Center permite incorporar la seguridad del software en todos los procesos relacionados con el software. Sus herramientas centralizadas y plantillas predefinidas ayudan a automatizar y orquestar las muchas actividades necesarias para aplicar las políticas y las mejores prácticas de Software Security Assurance desde el principio en el desarrollo de nuevo software y en cada etapa del ciclo de vida de la aplicación. Además, sirve como un sistema de registro para todas las actividades de seguridad de software, al tiempo que lo ayuda a fomentar una cultura de conciencia de seguridad de aplicaciones en toda su organización.

KCLATAM

ALEJANDRO R. GARCIA ROMAN
KNOWLEDGE CONSULTING S.A.
CUIT: 30-71374700-5
PRESIDENTE

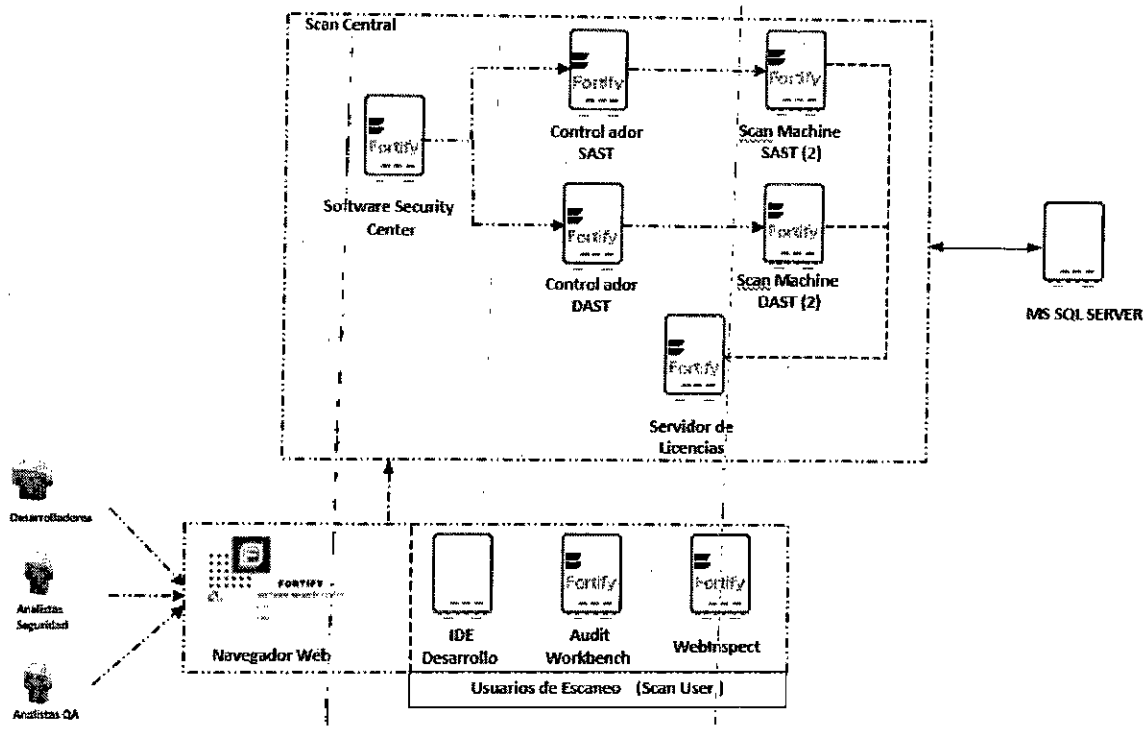
NANCY V. FERNANDEZ
SECRETARIA
Comisión de Preadjudicación
PODER JUDICIAL de la C.A.B.A.

Folio 108

Arquitectura referencial

La arquitectura y dimensionamiento mostrados son referenciales, y la versión final será confirmada con servicios profesionales en la etapa de Análisis y Diseño

- Fortify ScanCentral con 2 Scan Machine y 10 Scan Users
- Se considera el despliegue en máquinas virtuales



Alcance de los servicios profesionales propuestos

Los servicios profesionales propuestos de la solución de seguridad de Micro Focus descritos en este capítulo, se relacionan a la implementación de la solución de seguridad propuesta de Micro Focus Fortify en su versión On-Premise, en infraestructura del cliente para aquellos componentes identificados bajo esta modalidad, de acuerdo con la arquitectura lógica descrita a continuación.

Estos servicios serán entregados por el personal de KCLATAM y Micro Focus, en idioma español con la dedicación del tiempo para cada etapa.

Las siguientes tablas describen las características y alcances de los servicios profesionales propuestos.

KCLATAM

ALEJANDRO R. GARCIA ROMAN
KNOWLEDGE CONSULTING S.A.
CUIT: 30-71374700-5
PRESIDENTE

NANCY V. FERNANDEZ
SECRETARIA
Comisión de Preadjudicación
PODER JUDICIAL de la Folio 109

Implementación de la solución propuesta de Micro Focus Fortify

En esta etapa, equipo de Servicios Profesionales de KCLATAM y Micro Focus estará encargado de la implementación base de la solución de Micro Focus Fortify, de acuerdo con la arquitectura lógica que se muestra a continuación.

Los siguientes puntos describen las consideraciones asociadas a la arquitectura lógica propuesta:

- La arquitectura y dimensionamiento mostrados son referenciales y se detallará al inicio de la entrega de los servicios profesionales propuestos.
- Se considera Static Code Analyzer (software), en modalidad de ScanCentral SAST para realizar análisis estático.
- Se considera ScanCentral DAST (software), para realizar análisis dinámico.
- Se considera despliegue en los ambientes del PJN..
- La base de datos y la infraestructura de hardware/vms debe ser provista por el cliente.
- Se considera el despliegue en máquinas virtuales.
- La presente arquitectura es meramente referencial y deberá ser revisada con los detalles propios del proyecto una vez completada la fase de relevamiento y análisis

Las siguientes tablas resumen los requerimientos mínimos de Hardware y Software para implementar esta arquitectura y que el Cliente deberá proveer.

Componentes:

Componente	Capacidades de Hardware	Cantidad	Sistema Operativo Soportado
Software Security Center	• RAM = 16 GB. • CPU = 8vCPU • Storage = 150 GB	• 1	• Windows Server 2012 R2, Server 2016, Server 2019+ • Red Hat Enterprise Linux 6 update 5 and later, Red Hat Enterprise Linux 7.x, 8 • SUSE Linux Enterprise Server 12, 15 • Docker
Controlador DAST	• CPU = 8 vCPU • RAM = 16 GB • Storage = 150 GB	• 1	• Windows 10 Pro, Windows Server 2019 • Docker
Controlador SAST	• CPU = 8 vCPU • RAM = 16 GB • Storage = 150 GB	• 1	• Windows Server 2012 R2, 2016, 2019 • Red Hat Enterprise Linux 6 update 5 and later, Red Hat Enterprise Linux 7.x, 8, SUSE Linux Enterprise Server 12, 15 • Docker

KCLATAM

ALEJANDRO R. GARCIA ROMAN
KNOWLEDGE CONSULTING S.A.
CUIT: 30-71374700-5
PRESIDENTE

NANCY V. FERNANDEZ
SECRETARIA
Comisión de Preadjudicación
PODER JUDICIAL de la Nación
Folio 110

Componente	Capacidades de Hardware		Sistema Operativo Soportado
 Servidor de Licencias	• RAM = 4 GB • CPU = 4 vCPU • Storage = 150 GB	• 1	• Windows 10 Pro, Windows Server 2019 • Docker
 Scan Machine	• CPU = 8 vCPU • RAM = 32 GB • Storage = 200 GB	• 4	• Windows 10, Windows 8.1, Windows Server 2016, Windows Server 2019

Componente	Capacidades de Hardware	Sistema Operativo Soportado
 MS SQL SERVER	• 64GB RAM Recomendado • 16 CPU Cores	

Para más información, se podrán consultar los siguientes enlaces:

- Para requerimientos de Hardware y Software

https://www.microfocus.com/documentation/fortify-static-code-analyzer-and-tools/2210/Fortify_Sys_Reqs_22.1.0/index.htm#Resources/HTMLelements/Support.htm?TocPath=_____2

El alcance asociado a esta etapa se describe a continuación:

Etapa	Alcance
Análisis y Diseño	• Análisis y diseño de los componentes que integran la solución propuesta de seguridad de Micro Focus Fortify, de acuerdo con la arquitectura lógica mostrada. • La arquitectura propuesta será escalable para la inclusión de nuevos componentes o robustecimiento de la infraestructura de seguridad, para etapas futuras.
Instalación y configuración base	• Instalación, configuración y puesta a punto de los siguientes componentes: o Micro Focus ScanCentral DAST, en un servidor de un ambiente o Micro Focus ScanCentral SAST, en un servidor de un ambiente o Micfro Focus Software Security Center, en un servidor de un ambiente

KCLATAM

ALEJANDRO R. GARCIA ROMAN
KNOWLEDGE CONSULTING S.A.
CUIT: 30-71374700-5
PRESIDENTE

NANCY V. FERNANDEZ
SECRETARIA
Comisión de Preadjudicación
PODER JUDICIAL DE T...

Folio 111

Etapa	Alcance
Configuración	• Configuración y conectividad LDAP, para la gestión de usuarios, perfiles y notificaciones vía SMTP. • Integración entre los componentes que conforman la arquitectura de Micro Focus Fortify: • Integración de SCA a SSC y Scan Central SAST • Integración de Jenkins • Creación de perfiles.
Configuración y escaneo de aplicaciones	• Escaneo de aplicaciones (1 para DAST y 1 para SAST) o Interpretación de resultados o Entrega de reporte o Publicación de resultados en SSC o Explicación de resultados
Integraciones	• Integración de JenKins, considerando hasta 1 pipeline.
Despliegue	• Pruebas de funcionalidad de los componentes instalados y configurados en el ambiente propio del PJN. • Generación de la memoria técnica del proyecto. • Transferencia de conocimientos sobre la implementación realizada y sobre los componentes implementados en la infraestructura del Cliente. • Acompañamiento post Producción (5 días)

Plan de trabajo

El cronograma establecido, así como las semanas planteadas figuran a modo de referencia considerando que el trabajo se realice en semanas consecutivas y mostrando tiempos efectivos. Asimismo, el cronograma será revisado, detallado y acordado con el cliente al inicio del proyecto para realizar los ajustes que fueran necesarios en base a los hallazgos y necesidades puntuales que pudieran detectarse.

Como se puede observar, el proyecto de implementación y puesta a punto de la solución de Micro Focus Fortify en los ambientes del Cliente tiene una duración aproximada de 6 semanas más la etapa de capacitación formal (descrita más adelante); realizando los alcances detallados en los párrafos anteriores. Cabe destacar que la fecha de comienzo del proyecto deberá coordinarse con El Cliente una vez aceptada esta propuesta, de acuerdo con la disponibilidad de recursos.

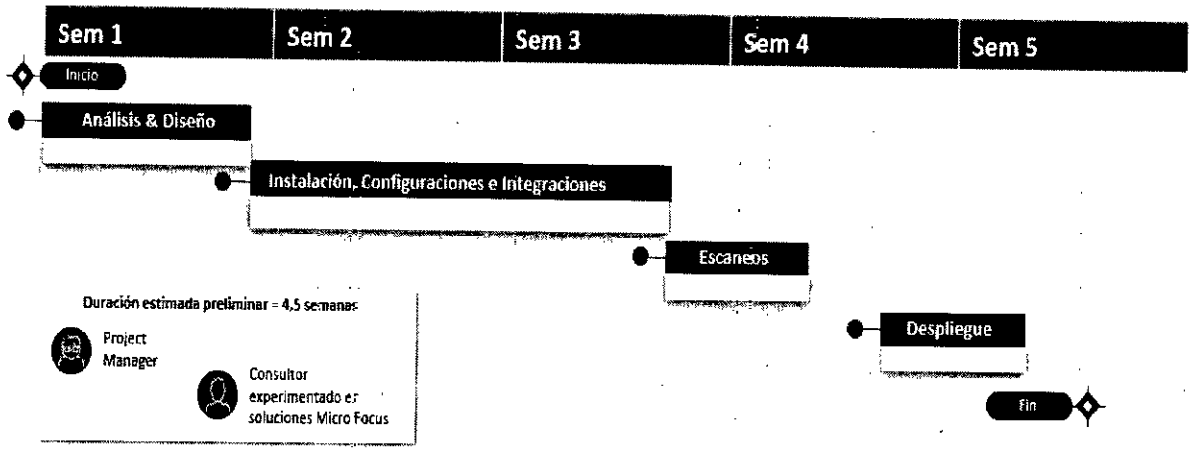
Al igual que se mencionó en la sección de alcance del proyecto, Micro Focus puede asumir un compromiso en relación con los tiempos de desarrollo en el proyecto, pero los tiempos totales del proyecto dependen en mayor medida del Cliente. Esto se debe a que es el actor principal de las etapas previas (análisis, diseño) y pruebas y validación. Si el Cliente se extiende por encima de los tiempos definidos en esta propuesta, Micro Focus podrá disponer del equipo de trabajo para asignarlos a otros proyectos, debiendo validar con al menos 5 semanas de anticipación la fecha en que se retome la actividad.

KCLATAM

ALEJANDRO R. GARCIA ROMAN
KNOWLEDGE CONSULTING S.A.
CUIT: 30-71374700-5
PRESIDENTE

Folio 112

NANCY V. FERNANDEZ
SECRETARIA
Comisión de Preadjudicar
PODER JUDICIAL de la



Plazo de entrega de las licencias

Las licencias incluidas en la presente oferta, serán entregadas dentro de los 10 días de recibida la orden de compra por parte del PJN.

Capacitación Oficial

De acuerdo con los requerimientos expresados por parte del Cliente final, se proponen grupos y perfiles de usuarios para capacitarse.

En este apartado se describe la capacitación propuesta para los componentes de Micro Focus Fortify

Nombre del Curso	Duración	Descripción
Fortify-DAST-22.1-WebInspect Dynamic Application Security Testing (DAST) con WebInspect + Incluye examen de Certificación profesional	32 horas	Hasta cinco (5) participantes en modo privado en español.

Nombre del Curso	Duración	Descripción
Fortify-SAST-22.1-Fortify SCA and SSC + Incluye examen de Certificación profesional	32 horas	Hasta cinco (5) participantes en modo privado en español.

Capacitación para usuarios administradores/responsables de la estrategia de DevSecOps

Los asistentes que el Cliente seleccione para tomar esta fase de entrenamiento se recomiendan que sean aquellos usuarios internos que tengan el rol de administradores y/o responsables de la implementación y cumplimiento de la estrategia de desarrollo seguro de aplicaciones (DevSecOps) y que, a partir de estas figuras, transfieran las actividades y conocimientos que proveen las soluciones de Micro Focus propuestas para el cumplimiento de los objetivos del proyecto.

KCLATAM

ALEJANDRO R. GARCIA ROMAN
KNOWLEDGE CONSULTING S.A.
CUIT: 30-71374700-5
PRESIDENTE

NANCY F. FERNANDEZ
SECRETARIA
Comisión de Preadjudicación
PODER JUDICIAL de la Nación

Folio 7/13

La estrategia que se persigue con esta propuesta de entrenamiento es que sean cursos dictados al personal clave del Cliente y en etapas posteriores, puedan trasmitir los conocimientos adquiridos al resto del personal involucrado en estas soluciones, para unificar los conocimientos al resto del equipo del Cliente.

La capacitación formal de las soluciones de Micro Focus Fortify se definen la modalidad de entrega en grupo cerrado, privado y virtual.

Para esta modalidad y alcance, las características de estos entrenamientos se describen en los siguientes puntos:

- El entrenamiento es para 5 personas, en grupo Cerrado específico para el personal del Cliente. Clase privada, en idioma español.
- El entrenamiento será formal Oficial del Fabricante de la solución de Micro Focus Fortify en la modalidad de clase privada, en idioma español con un instructor oficial certificado.
- El curso se dictará en idioma español y constará de una parte teórica y otra práctica sobre el proyecto del cliente.
- La capacitación formal tendrá de duración 32 horas de currículo cada curso.

Criterios para el dictado de los entrenamientos

Los siguientes apartados describen los criterios para la impartición del entrenamiento descritos en esta propuesta.

- Todos los estudiantes deben participar a la clase en la misma fecha.
- Normalmente, las clases son en días continuos en jornadas de 6 horas lunes a viernes (si aplica) y en un horario propuesto de 9:00 hrs a 18:00 hrs. (Días hábiles), con 1 hora de comida, pero el horario final se acodardá finalmente con el Cliente.
- La fecha de dictado de la clase privada en español será definida oportunamente y de común acuerdo con el cliente.

Los entrenamientos incluyen:

- Certificado de participación para cada estudiante en clase formal del fabricante.
- Instructor certificado

Características de los entrenamientos por entregarse:

- Se entrega un certificado de participación para cada estudiante en clase formal de fabricante.
- Instructor certificado.

Las siguientes tablas muestran el detalle del entrenamiento propuestos para esta modalidad de entrega:

Fortify-DAST-22.1 - Testeo de Dinámico de Aplicaciones (DAST) con WebInspect

ALEJANDRO R. GARCIA ROMAN
KNOWLEDGE CONSULTING S.A.
CUIT 30-71374700-5
PRESIDENTE

NANCY V. FERNANDEZ
SECRETARIA
Comisión de Preadjudica...
PODER JUDICIAL de la ...

Folio 114

Módulos	Objetivos
Módulo 1: **Seguridad de Aplicaciones y OWASP Top 10**	• Reconocer el punto de vista de los atacantes y las vulnerabilidades. • Definir el OWASP Top 10. • Identificar el ciclo de vida del desarrollo de software (SDLC).
Módulo 2: **Componentes y Conceptos de WebInspect**	• Definir componentes y características de WebInspect. • Entender SAST y sus desafíos. • Reconocer la importancia del agente WebInspect.
Módulo 3: **Escaneos y Macros**	• Crear escaneos autenticados y no autenticados. • Producir macros de login y workflow. • Como utilizar herramientas de pre-escaneos de seguridad. • Revisión de escaneos (errores y performance).
Módulo 4: **Escaneos para móviles**	• Definir el OWASP Top 10 para móviles. • Aprender el escaneo de API para móviles.
Módulo 5: **HTTP Testers de Seguridad**	• Identificar las características operativas y sintácticas de HTTP. • Distinguir los 4 tipos de datos HTTP y entender cada método de prueba.
Módulo 6: **Resultados de Escaneos**	• Reconocer los elementos de la página de resultados del análisis. • Navegar por la página de resultados del análisis. • Corrección de vulnerabilidades. • Recuperar archivos de registro.
Módulo 7: **Gestión de Políticas de Escaneo**	• Comprender el Cumplimiento y Políticas. • Utilizar las directivas de análisis predeterminadas y personalizadas.
Módulo 8: **Reportes**	• Interpretar los informes predeterminados de WebInspect. • Creación de informes personalizados.
Módulo 9: **Escaneo de Web Services y REST API**	• Crear un análisis de servicios web. • Crear un análisis de la API de REST.
Módulo 10: **Configuración de Escaneos predeterminados de aplicaciones**	• Reconocer las diferentes configuraciones de WebInspect y WebInspect Scans.
Módulo 11: **Kit de herramientas de seguridad**	• Identificar las herramientas estándar y restringidas de WebInspect.

KC LATAM

ALEJANDRO R. GARCIA ROMAN
KNOWLEDGE CONSULTING S.A.
CUIT: 30-71374700-5
PRESIDENTE

NANCY V. FERNANDEZ
SECRETARIA
Comisión de Preadjudicación
PODER JUDICIAL de la Nación

FOLIO 115

Fortify-SAST-22.1 - Fortify SCA y SSC

Módulos	Objetivos
Módulo 1: **Arquitectura Fortify y Vision General de Seguridad de Aplicaciones**	• Identificar la arquitectura y el flujo de trabajo de Fortify. • Reconocer la importancia de la Seguridad de aplicaciones en el ciclo de vida de desarrollo de software (SDLC).
Módulo 2: **Fortify SSC Ajustes**	• Reconocer la versión de la aplicación y las opciones de administración. • Crear de una versión de la aplicación y actualización de los paquetes de reglas de SSC. • Integrar los resultados del análisis de Audit Workbench con las versiones de la aplicación SSC.
Módulo 3: **Fortify SCA Análisis de Métricas**	• Describir el proceso de escaneo automatizado. • Explicar la función de cada analizador. • Reconocer cómo se colocan los hallazgos dentro de cada carpeta de riesgo.
Módulo 4: **Escaneo Estático**	• Definir las características y el uso de las opciones de escaneo de Fortify=. • Reconozca los diferentes complementos IDE que se integran con Fortify SCA Analysis. • Ejecute correctamente los análisis de Fortify de varias maneras, utilizando: o Audit Workbench o Scan Wizard o Command Line o Eclipse o Visual Studio
Módulo 5: **Auditoría de los resultados de análisis de Fortify**	• Verificar los resultados del análisis en Audit Workbench. • Identificar los hallazgos en la carpeta Critical. • Utilizar Smart View para obtener una representación visual de los problemas de flujo de datos en el código. • Reconocer categorías de hallazgos en la carpeta Critical. • Aplicar el método de validación adecuado para corregir una vulnerabilidad determinada. • Filtre, audite y suprima problemas para reducir el ruido.

KCLATAM

ALEJANDRO R. GARCIA ROMAN
KNOWLEDGE CONSULTING S.A.
CUIT: 30-71374700-5
PRESIDENTE

NANCY V. FERNANDEZ
SECRETARIA
Comisión de Preadjudicación
PODER JUDICIAL

Folio 116

OF 1

	• Encontar información, es decir, detalles y recomendaciones, para solucionar problemas de seguridad.
Módulo 6: **Data Validation**	• Implementar de forma segura la validación de datos. • Seleccionar la validación de datos adecuada para una situación concreta. • Amplíe las bibliotecas de validación de datos.
Módulo 7: **Análisis, Rastreo y Corrección de Vulnerabilidades**	• Leer correctamente el seguimiento del análisis • Audite las vulnerabilidades para: o SQL Injection o XSS o Log Forging o Cross-Site Request Forger (CSRF)
Módulo 8: **Reglas Personalizadas**	• Reconocer cómo usar reglas de limpieza de flujo de datos para integrar la validación de datos en Fortify. • Crear regla de validación de datos.
Módulo 9: **Utilización de Fortify SSC (Software Security Center), Auditoría y Reportes**	• Navegue de manera efectiva por Fortify SSC (Centro de seguridad de software). • Revise los resultados del análisis, cargue y audite los problemas mediante las capacidades de SSC. • Generate reports to show outstanding issues, progress on security goals and a summary of the vulnerabilities detected during a scan.
Módulo 10: **Seguimiento de Errores**	• Utilizar la herramienta de seguimiento de errores a través de SSC y AWB.
Módulo 11: **Utilizar Asistente de Auditoría en SSC**	• Reconocer el valor de utilizar Audit Assistant. • Definir las políticas de predicción de inquilinos de Fortify Scan Analytics. • Configure su SSC para utilizar Audit Assistant. • Enviar datos de capacitación, problemas y revisar los resultados de AA.

Adicionalmente, como valor agregado, se podrán consultar y participar en los entrenamientos en formato eLearning que se describen en el siguiente enlace y que complementa a los descritos en esta sección de la propuesta de entrenamiento y que aplicarán para algunas de los productos propuestos y descritos en este documento:

https://community.microfocus.com/cyberres/fortify/fortify-education-after-hours/f/forum/509597/direct-one-click-quick-access-to-our-free-fortify-digital-learning-offerings

KCLATAM

ALEJANDRO R. GARCIA ROMAN
KNOWLEDGE CONSULTING S.A.
CUIT: 30-71374700-5
PRESIDENTE

NANCY V. FERNANDEZ
SECRETARIA
Comisión de Preadjudicación

Folio 117