ITAC end-to-end testing®

Detección y prevención de problemas de seguridad a nivel de aplicaciones.

El servicio de validación de desarrollo seguro **ITAC end-to-end testing®** permite identificar vulnerabilidades de seguridad a nivel de aplicaciones y generar recomendaciones para solucionarlas; usando técnicas avanzadas de revisión de análisis estático del código fuente y análisis dinámico de las aplicaciones, combinado con la experiencia de consultores altamente calificados, quienes están certificados en codificación segura, estandarización de los procesos de desarrollo como ISO y CMMI, y soporte usando herramientas especializadas.

Es recomendable que cualquier organización que realice desarrollo de software internamente o a través de proveedores externos, adopte como necesidad estratégica para su negocio, mecanismos que permitan la identificación temprana de vulnerabilidades de seguridad a nivel de aplicaciones e implemente las mejores prácticas para su protección.

Características del servicio:

- Evaluación en el cumplimiento de PCI DSS Sección 6: "Desarrollar y mantener sistemas y aplicaciones seguras" mediante la revisión del código fuente.
- Verificación del código fuente, con el fin de verificar si es vulnerable a cualquiera de las 10 vulnerabilidades más críticas para las aplicaciones web, de acuerdo a OWASP (http://www.owasp.org).
- Revisión completa, con el fin de verificar que el código fuente no tenga ninguno de los 25 errores de software más peligrosos; categoría creada por SANS (http://www.sans.org/top25-software-errors/).
- Identificación de debilidades (acorde a) SAMATE. Anexo A, en el código de alta complejidad. (http://samate.nist.gov).
- Las vulnerabilidades identificadas abarcan las siguientes categorías, entre otras:
  - Ataques basados en parámetros de entrada.
  - Vulnerabilidades de puerta trasera.
  - Configuración de ambientes inseguros.
  - Controles débiles de seguridad.
  - Abrazos mortales (deadlocks) y condiciones de competencia.
  - Comportamiento de aplicación no determinístico.
  - Manejo inseguro de errores y auditoría.
  - Exposición de información sensible.
- Validación de las normas de seguridad específicas del negocio:
  - Verificación de patrones de los números de producto, cuentas, etc.
  - Normas específicas de negocio parametrizadas.
- Lenguajes soportados
  - Java, JSP, C, C++, ASP, .NET (C#, VB.NET, ASP.NET, Managed C++), PL/SQL

BENEFICIOS:

- ✓ Prevención de defectos que tengan impacto en la seguridad de las aplicaciones web y SOA (servicios web).
- ✓ Apoyo en la adherencia a estándares y estándares seguros como OWASP, HIPAA, CWE/SANS.
- ✓ Reducción de costos debido a la adquisición y mantenimiento de herramientas, así como una mayor capacidad de trabajo para los controles de seguridad de las aplicaciones.
- ✓ Ahorro en contratación, formación y administración de recursos humanos especializados en conceptos de seguridad, en los niveles de desarrollo y herramientas especializadas.
- ✓ Obtención de resultados tangibles antes de la implementación a gran escala.

www.itac.co/endtoendtesting - endtoendtesting@itac.co

ITAC » www.itac.co
Phone: +571 744- 4822
info@itac.co
Bogotá - Colombia

Distributors and resellers:

ASYSTEC
Phone: +011 (809) 3 34 61 54
fdelacruz@asystec.com.do
Caribbean Region

DIGIWARE Seguridad de la Información
North America - Phone: +1 (305) 913-8569 (USA)
info_us@digiware.net
Latin America - Phone: +571 508 2220 (COL)
info@digiware.net