Request Tracker for Incident Respond v. 2.0

XVIII Grupos de Trabajo

Universidad Autónoma de Madrid

Madrid, 1 de Junio de 2006

Carlos Fuentes Bermejo <carlos.fuentes@rediris.es>

Indice

- RTIR Working Group
  - Objetivos
  - Futuro
- Proyecto
  - Requerimientos
  - Estado

RTIR Working Group

- RTIR creado por JANET-CERT y ampliamente utilizado en los CSIRTs académicos
- Creado en el 11th TF-CSIRT (Enero de 2004)
- Constituido por 9 CERTs Europeos:
  - JANET-CERT (Chairman)
  - IRIS-CERT (Co-Chairman)
  - ACONet-CERT
  - CERT-Polska
  - CERT.PT
  - LITNet-CERT
  - …

RTIR Working Group - Objetivos

- Primera fase
  - Crear un foro de interés en la herramienta
  - Describir nuevas funcionalidades
  - Crear un consorcio para la ampliación de la herramienta
  - Cursos
- Segunda fase
  - Escribir los requerimientos para versión 2
  - Buscar fondos para poder llevar a cabo el proyecto
- Tercera fase
  - Dirección del proyecto de desarrollo
  - Divulgación y promoción de la nueva versión

RTIR Working Group - Futuro

- Incorporación de nuevos equipos
- Creación de un sitio web de referencia
  - Documentación de la herramienta
  - Soporte de la misma

Proyecto

- Administrado por TERENA y dirigido por RTIR-WG
- Desarrollado por BestPractical
- TERENA y BestPractical firmaron el contrato el 6 de Septiembre de 2005
  - Oficialmente los trabajos empezaron el 6 de Octubre
  - La duración es de 1 año y medio
- Tiene un coste de $95350
- Dividido en 3 fases
  - 6 meses de duración cada una
  - Incluyen 15 días para verificación
    - Workflow, Funcionalidad y requerimientos especificos
- IRIS-CERT es el punto de contacto técnico con BP
- Incluye un año de soporte gratis
  - Descuentos para futuros años

Proyecto - Requerimientos

- Integración de contactos de seguridad en los Incidentes
- Integración con RTFM
- Interacción con RT
- Sanitizacion de la BBDD
- PGP/GPG
- Múltiples ámbitos de actuación
- Uso simultaneo
- Recuperación del sistema
- Creación de Informes

Proyecto - Estado y Futuro

- Estado
  - Finalizada la primera fase - 24 de Mayo
  - Dos periodos de pruebas
    - El primero fue rechazado.
      - Demasiados bugs en el sofware
      - Modificaciones en el workflow
    - El segundo consiguió la aceptación
      - Todavía quedan bugs por resolver
- Futuro
  - Se publicará la primera versión oficial RTIR v.2
    - Disponible en unas 2 o 3 semanas
  - Se comenzarán los trabajos de la 2ª Fase

Preguntas