]HackingTeam[

RCS 9.5

La suite de hacking para intercepción gubernamental

Manual del analista

Propiedad de la información

las solicitudes de copias adicionales de este manual o de la información técnica del producto se deben enviar a:

HT S.r.l.

via della Moscova, 13

20121 Milan (MI)

Italia

Tel.: + 39 02 29 060 603

Fax: + 39 02 63 118 946

Correo electrónico: info@hackingteam.com

Contenido

Glosario

A continuación se detallan las definiciones utilizadas en este manual.

A

Accounting
Sección de la consola en la que se administra el acceso a RCS.

Administrador
Es la persona que permite el acceso al sistema, crea grupos de trabajo y define las operations, los targets y los tipos de datos que se recopilarán.

Administrador del sistema
Persona que instala los servidores y las consolas, actualiza el software y restaura los datos en caso de alguna falla.

Agent
Software de sondeo instalado en los dispositivos a monitorear. Está diseñado para reunir evidence y transmitirla al Collector.

Agent elite
Agent instalado en dispositivos seguros. Le permite recopilar todos los tipos de evidence disponibles.

Agent scout
Reemplaza al agent enviado al dispositivo para verificar el nivel de seguridad antes de instalar agents reales (elite o soldier).

Agent soldier
Agent instalado en dispositivos que no son completamente seguros. Solo le permite recopilar algunos tipos de evidence.

Alerting
Sección de la consola en la que se administran los alerts de nueva evidence.

alerts de evidence
Alertas, usualmente en forma de correos electrónicos, que se envían a los analistas cuando hay nueva evidence que coincide con las reglas establecidas.

Analista
Persona encargada de analizar los datos recopilados durante las operations.

Anonymizer
(opcional) Protege al servidor contra ataques externos y permite permanecer anónimo durante las investigaciones. Transfiere los datos del agent a los Collectors.

Audit
Sección de la consola que reporta las acciones de todos los usuarios y el sistema. Se utiliza para controlar el abuso de RCS.

B

back end
Entorno diseñado para desencriptar y guardar la información que se recopila. Incluye el Master Node y las bases de datos shard.

BRAS
(Broadband Remote Access Server) Dirige el tráfico hacia o desde el DSLAM a la red del ISP y administra la autentificación de los suscriptores del ISP.

BSSID
(Basic Service Set IDentifier) Punto de acceso y su identificador cliente.

C

Carrier
Servicio del Collector: envía los datos recibidos de los Anonymizers a las bases de datos shard o al Master Node.

Collector
Servicio de Collector: recibe los datos que envían los agents a través de la cadena de Anonymizers.

consola
Computadora en la que se instala RCS Console. Accede directamente a RCS Server o al Master Node.

D

Dashboard
Sección de la consola utilizada por el analista. Se usa para tener un resumen rápido del estado de las operations, targets y agents más importantes.

DSLAM
(Digital Subscriber Line Access Multiplexer) Dispositivo de red que usualmente se encuentra en la central telefónica de los operadores de telecomunicaciones. Conecta varias interfaces de líneas de abonados digitales (DSL) a un canal de comunicaciones de alta velocidad digital usando técnicas de multiplexión.

E

Emisor de RCS
Sistema RCS que recibe evidence de los agents y la transfiere a otros sistemas RCS (consultar) a través de las reglas de conexión. Es un sistema RCS completo.

entidad
Grupo de información de Intelligence vinculada con el target y con las personas y lugares involucrados en la investigación.

ESSID
(Extended Service Set IDentifier) También conocido como SSID. Permite identificar la red Wi-Fi.

evidence
Evidence de datos recopilados. El formato depende del tipo de evidence (p. ej.: imagen).

Exploit
Código que se aprovecha de un error o vulnerabilidad y ejecuta un código imprevisto. Se utiliza para infectar a los dispositivos de los targets.

F

factory
Una plantilla para la configuración y compilación de un agent.

front end
Entorno diseñado para comunicarse con los agents para recopilar información y establecer su configuración. Incluye Collectors.

G

Grupo
Entidad de Intelligence que agrupa a varias entidades.

grupo de alerting
Grupo de usuarios que reciben notificaciones por correo cuando se activa una alarma del sistema (por ejemplo, cuando la base de datos excede los límites de espacio disponible). Usualmente este grupo no está vinculado con ninguna operation.

M

Monitor
Sección de la consola en la que se monitorea el estado de los componentes y la licencia.

N

Network Controller
Servicio del Collector: verifica el estado del Network Injector y el Anonymizer y les envía nuevos parámetros de configuración y actualizaciones de software.

Network Injector
Componente de hardware que controla el tráfico de la red del target e inyecta un agent en los recursos web seleccionados. Viene en dos versiones, Appliance o Tactical: la primera es para la implementación en el ISP, la segunda se usa en el campo.

Network Injector Appliance
Versión apilable del Network Injector, para instalarlo en el ISP. Consulte: Tactical Network Injector.

O

operation
Investigación dirigida a uno o más targets, cuyos dispositivos tendrán agents.

P

Person
Entidad de Intelligence que representa a una persona involucrada en la investigación.

Position
Entidad de Intelligence que representa a un lugar involucrado en la investigación.

R

RCS
(Remote Control System). El producto que aquí se documenta.

RCS Console
Software diseñado para interactuar con RCS Server.

RCS Server
Una o más computadoras, según la arquitectura de instalación, donde se instalan los componentes esenciales de RCS: las bases de datos shard, los Network Controller y el Collector.

Receptor de RCS
Sistema RCS que recibe evidence de otros sistemas RCS emisores (consultar) pero nunca directamente de los agents. En comparación con un RCS completo, el receptor de RCS solo cuenta con las funciones de procesamiento de evidence.

reglas de alert
Reglas que crean alerts cuando se almacena nueva evidence o los agents se comunican por primera vez.

reglas de inyección
Opciones de configuración que definen cómo identificar el tráfico HTTP, qué recurso debe inyectarse y qué método se usará para la inyección.

S

secuencia de obtención
Grupo de eventos, acciones y módulos de obtención complejos, que forman parte de la configuración avanzada de agents.

SSH
(Secure SHell) Protocolo de red para la transmisión segura de datos, los servicios del intérprete de comandos remoto o la ejecución de comandos.

System
Sección de la consola en la que se administra el sistema.

T

Tactical Network Injector
Versión portátil del Network Injector, para uso táctico. Consulte: Network Injector Appliance.

TAP
(Test Access Port) Dispositivo de hardware que se instala en una red y que monitorea de forma pasiva el flujo de datos transmitido.

target
La persona física bajo investigación.Se representa por medio de la entidad Target en la sección Intelligence.

Técnico
Persona designada por el administrador para crear y administrar agents.

V

Virtual
Entidad de Intelligence que representa a una ubicación virtual (p. ej.: sitio web) involucrado en la investigación.

VPS
(Virtual Private Server) Servidor remoto en el que se instala el Anonymizer. Usualmente se alquila.

W

WPA

(Wi-Fi Protected Access) Protección de la red Wi-Fi.

WPA 2

(Wi-Fi Protected Access) Protección de la red Wi-Fi.

1

Introducción a esta guía

Presentación

Objetivos de este manual

Este manual sirve como guía para el *Analista* sobre cómo usar RCS Console para:

- monitorear el target
- explorar los dispositivos del target
- analizar evidence y exportarla

A continuación se muestra la información necesaria para consultar el manual.

Contenido

En esta sección se incluyen los siguientes temas:

Nuevas funciones de la guía

Lista de notas publicadas y actualizaciones a esta ayuda en línea.

Fecha de publicación	***Código***	***Versión de software.***	***Descripción***
24 de noviembre de 2014	Manual del analista 1.8 NOV-2014	9.5	Se agregaron filtros para el tipo de conexión, *consulte "**Administración de entidades: vista de enlaces**" en la página 67* .
20 de septiembre de 2014	Manual del analista 1.7 SEP-2014	9.4	Se agregaron notas para recuperar evidence del sistema de archivos, *consulte "**Qué debería saber acerca de la recuperación de evidence**" en la página 50* .
23 de junio de 2014	Manual del analista 1.6 JUN-2013	9.3	Se actualizó la sección de registro de sincronización de agents, *consulte "**Datos del registro de sincronización de un agent**" en la página 32* Se agregó la herramienta de exportación de evidence, *consulte "**Análisis de evidence (Evidence)**" en la página 37* .

Fecha de publicación	*Código*	*Versión de software.*	*Descripción*
19 de febrero de 2014	Manual del analista 1.5 FEB-2014	9.2	Se agregaron nuevos filtros y la opción de administración de grupos a Intelligence, *consulte "**Intelligence**" en la página 54* . Se agregó la posibilidad de transformar una entidad Person en una entidad Target, *consulte "**Qué debería saber acerca de las entidades**" en la página 55* . Se agregó la evidence de tipo **Money** *consulte "**Lista de tipos de evidence**" en la página 47* . Se agregó un nuevo tipo de exportación de evidence al conector, *consulte " **Datos de exportación de la evidence**" en la página 46*
30 de septiembre de 2013	Manual del analista 1.4 SEP - 2013	9	Se actualizó la documentación de la sección Intelligence, *consulte "**Intelligence**" en la página 54* . Se actualizaron los procedimientos del analista, *consulte "**Procedimientos del analista**" en la página 14* . Se actualizó la documentación de las reglas de alert, *consulte "**Alert**" en la página 94* . Se actualizó la documentación debido a las mejoras a la interfaz de usuario. Se mejoró el contenido.

Documentación incluida

Los siguientes manuales se incluyen con el software RCS:

Manual	*Destinatarios*	*Código*	*Formato de distribución*
Manual del administrador del sistema	Administrador del sistema	Manual del administrador del sistema 1.8 NOV-2014	PDF
Manual del administrador	Administradores	Manual del administrador 1.6 NOV-2014	PDF
Manual del técnico	Técnicos	Manual del técnico 1.9 NOV-2014	PDF
Manual del analista(este manual)	Analistas	Manual del analista 1.8 NOV-2014	PDF

Convenciones tipográficas de notas

Las notas previstas en este documento se detallan a continuación (Manual de estilo de Microsoft):

ADVERTENCIA: indica una situación de riesgo que, si no se evita, podría causar lesiones físicas en el usuario o daños en el equipo.

PRECAUCIÓN: indica una situación de riesgo que, si no se evita, puede causar la pérdida de datos.

IMPORTANTE: indica las acciones necesarias para realizar una tarea. Si bien pueden pasarse por alto algunas notas sin que esto afecte a la realización de la tarea, no se deberían omitir las indicaciones importantes.

NOTA: información neutral y positiva que enfatiza o complementa la información del texto principal. Proporciona información que puede aplicarse solo en casos especiales.

Sugerencia: recomendación para la aplicación de técnicas y procedimientos descritos en el texto de acuerdo a ciertas necesidades especiales. Puede sugerirse un método alternativo y no es esencial para la comprensión del texto.

Llamada al servicio: la operation solo puede completarse con la ayuda del servicio técnico.

Convenciones tipográficas de formato

A continuación se muestran las explicaciones de algunas convenciones tipográficas:

Ejemplo	*Estilo*	*Descripción*
Consulte "Datos del usuario"	*cursiva*	indica el título de un capítulo, una sección, una subsección, un párrafo, una tabla o una imagen de este manual u otra publicación a la que se hace referencia.
<ddmmaaaa>	<aaa>	indica un texto que el usuario debe ingresar de acuerdo a cierta sintaxis. En el ejemplo, <ddmmaaaa> es una fecha y un posible valor podría ser “14072011”.
Seleccione uno de los servidores de la lista **[2]**.	**[x]**	indica el objeto citado en el texto que aparece en la imagen adyacente.
Haga clic en **Agregar**. Seleccione el menú **Archivo, Guardar datos**.	**negrita**	indica el texto en la interfaz del operador, que puede ser un elemento gráfico (como una tabla o pestaña) o un botón en la pantalla (como mostrar).
Presione Entrar	primera letra mayúscula	indica el nombre de una tecla en el teclado.
Consulte: Network Injector Appliance.	-	sugiere que compare la definición de una palabra en el glosario o contenido con otra palabra o contenido.

Destinatarios del producto y de esta guía

A continuación se muestra una lista de los profesionales que interactúan con RCS.

Destinatario	*Actividad*	*Habilidades*
Administrador del sistema	Sigue las indicaciones de HackingTeam que se suministran durante la fase contractual. Instala y actualiza los RCS Servers, los Network Injectors y las RCS Cosoles. Programa y se encarga de realizar las copias de seguridad. Restaura las copias de seguridad si se reemplazan los servidores.  **ADVERTENCIA: el administrador del sistema debe tener las habilidades necesarias. HackingTeam no se hace responsable en caso de mal funcionamiento del equipo o de posibles daños ocasionados por la instalación por parte de una persona no profesional.**	Técnico de red experto
Administrador	Crea cuentas y grupos autorizados. Crea operations y targets. Monitorea el estado del sistema y de las licencias.	Administrador de investigación

Destinatario	*Actividad*	*Habilidades*
Técnico	Crea agents y los configura. Establece las reglas de Network Injector	Técnico especialista en intercepciones
Analista	Analiza la evidence y la exporta.	Operativo

Datos de identificación del autor del software

HT S.r.l.
via della Moscova, 13
20121 Milan (MI)
Italia
Tel.: + 39 02 29 060 603
Fax: + 39 02 63 118 946
Correo electrónico: info@hackingteam.com

2

RCS Console para el analista

Presentación

Introducción

RCS (Remote Control System) es una solución que soporta investigaciones por medio de la intercepción activa y pasiva de los datos y la información de los dispositivos bajo investigación. De hecho, RCS crea, configura e instala agents de software de forma anónima que recopilan datos e información y envían los resultados a la base de datos central para decodificarlos y guardarlos.

El rol del analista

El rol del analista es:

- seleccionar y analizar evidence
- recuperar evidence de un dispositivo
- exportar evidence para las autoridades
- organizar la evidence del dispositivo y otra evidence en su posesión para formular soluciones para la investigación

Funciones a las que el analista tiene acceso

Para realizar sus actividades, el analista tiene acceso a las siguientes funciones:

- **Operations**
- **Intelligence**
- **Dashboard**
- **Alerting**

Contenido

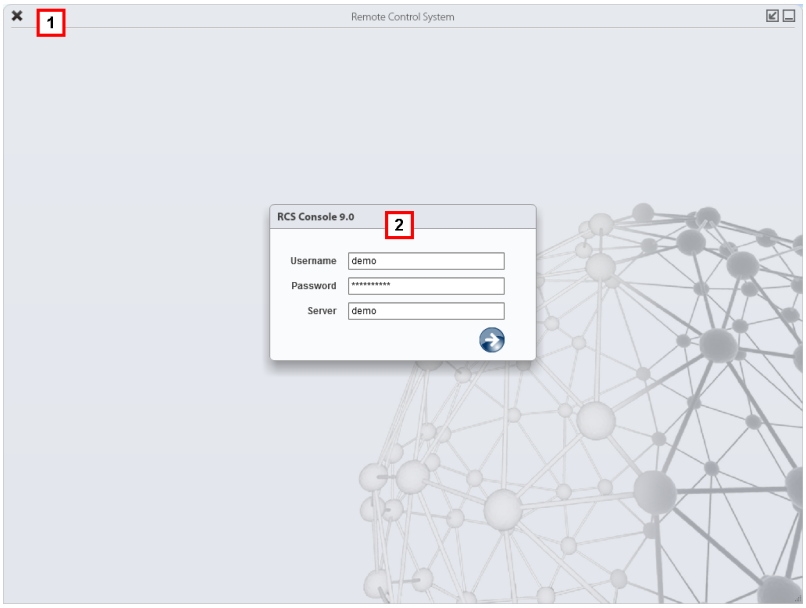
En esta sección se incluyen los siguientes temas:

Pantalla inicial de RCS Console

Cuando se abre RCS Console, se le pide que ingrese sus datos de inicio de sesión que estableció el administrador.

Cómo se ve la página de inicio de sesión

Así es como se ve la página de inicio de sesión:



Área	*Descripción*
1	Barra de título con botones de comando: Cierra RCS Console. Botón para ampliar la ventana. Botón para minimizar la ventana.
2	Ventana de diálogo para ingresar al sistema.

Acceso a RCS Console

Para acceder a las funciones de RCS Console:

Paso	*Acción*
1	En **Nombre de usuario** y **Contraseña,** ingrese sus datos de inicio de sesión asignados por el administrador.
2	En **Servidor,** ingrese el nombre del equipo o la dirección del servidor al que desea conectarse.
3	Haga clic en  : aparecerá la página principal con los menús activados según los privilegios de su cuenta. *Consulte "**Descripción de la página principal**" abajo* .

Descripción de la página principal

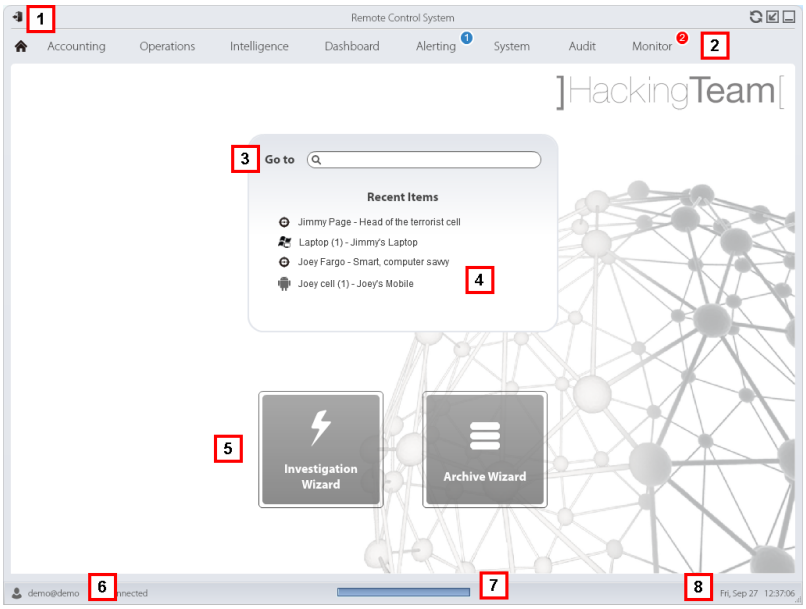
Para ver la página principal:	• haga clic en 

Introducción

Al abrir RCS Console se mostrará la página principal. Todos los usuarios verán la misma página. Los menús se verán activos según los privilegios asignados a la cuenta.

Cómo se ve

Así es como se ve la página principal, con elementos guardados que se abrieron recientemente. Detalle de los elementos y las acciones comunes:



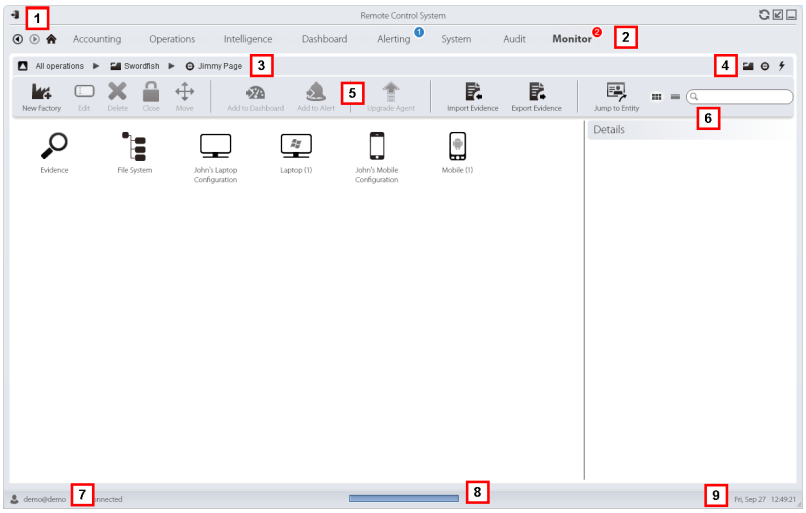
Área	*Descripción*
1	Barra de título con botones de comando.
2	Menú de RCS con las funciones activas para el usuario.
3	Cuadro de búsqueda para buscar operations, targets, agents y entidades, por nombre o descripción.
4	Enlaces a los cinco elementos abiertos (operation en la sección **Operations**, operation en la sección **Intelligence**, target, agent y entidad).
5	Botones del asistente.
6	Usuario conectado con opciones para cambiar el idioma y la contraseña.
7	Área de descarga con una barra de progreso durante la exportación o compilación.
8	Fecha y hora actuales con opciones para cambiar la zona horaria.

Elementos y acciones comunes de la interfaz

Cada página del programa usa elementos comunes y permite realizar acciones similares.
Para facilitar la comprensión del manual, en este capítulo se describirán los elementos y acciones compartidos por ciertas funciones.

Cómo se ve RCS Console

Así es como se ve usualmente la página de RCS Console. En este ejemplo se muestra la página de un target:



Área	*Descripción*
1	Barra de título con botones de comando:  Salir de RCS.  Botón para volver a cargar la página.  Botón para ampliar la ventana.  Botón para minimizar la ventana.
2	•  Botón Anterior del historial de navegación •  Botón Siguiente del historial de navegación •  Botón para regresar a la página principal • Menú de RCS con las funciones activas para el usuario.
3	Barra de navegación de la operation. A continuación se muestra la descripción de cada elemento:
4	Botones que permiten mostrar todos los elementos, independientemente del grupo al que pertenecen. A continuación se muestra la descripción de cada elemento:
5	Barra de herramientas de la ventana.

3

Ícono	*Descripción*
	Regresar al nivel superior.
	Muestra la página de la operation (sección **Operations**).
	Muestra la página del target.
	Muestra la página de la factory.
	Muestra la página del agent.
	Muestra la página de la operation (sección **Intelligence**).
	Muestra la página de la entidad.

4

Ícono	*Descripción*
	Muestra todas las operations.
	Muestra todos los targets.
	Muestra todos los agents.
	Muestra todas las entidades.

Área	*Descripción*
6	Botones y cuadro de búsqueda:

Objeto	*Descripción*
	Cuadro de búsqueda. Escriba parte del nombre para que aparezca una lista con los elementos que contienen esas letras.
	Muestra los elementos en una tabla.
	Muestra los elementos como íconos.

7	Usuario conectado con opciones para cambiar el idioma y la contraseña.
8	Área de descarga con una barra de progreso durante la exportación o compilación. Los archivos se descargan en el escritorio, en la carpeta Descarga de RCS. • Barra superior: porcentaje de generación en el servidor • Barra inferior: porcentaje de descarga desde el servidor a RCS Console.
9	Fecha y hora actuales con opciones para cambiar la zona horaria.

Acciones siempre disponibles en la interfaz

Cambiar el idioma de la interfaz o la contraseña

Para cambiar el idioma de la interfaz o la contraseña:

Paso	*Acción*
1	Haga clic en **[7]** para que aparezca una ventana de diálogo con los datos del usuario.
2	Cambie el idioma o la contraseña y haga clic en **Guardar** para confirmar y salir.

Cambiar la fecha y la hora de RCS Console a su zona horaria

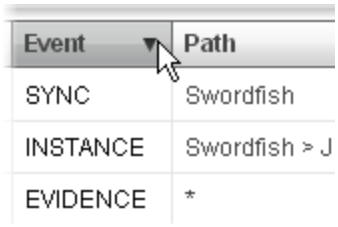
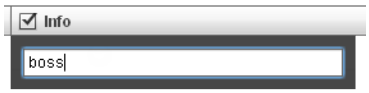
Para convertir todas las fechas y horas a su zona horaria:

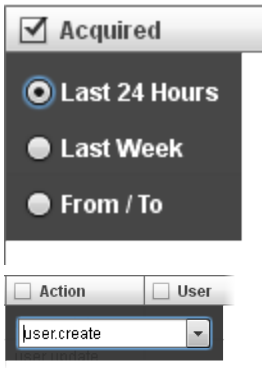
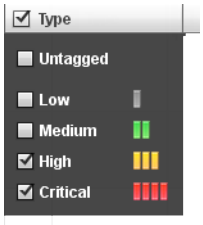
Paso	*Acción*
1	Haga clic en **[9]** para que aparezca una ventana de diálogo con la fecha y la hora actuales: **Hora UTC**: hora media de Greenwich (GMT) **Hora local**: fecha y hora donde se encuentra instalado el RCS Server **Hora de la consola**: fecha y hora de la consola que se está utilizando y que se puede cambiar.
2	Cambie la zona horaria y haga clic en **Guardar** para confirmar y salir: todas las fechas y horas se cambiarán según lo que haya indicado.

Acciones relacionadas con las tablas

RCS Console muestra varios datos en forma de tablas. Las tablas le permiten:

- ordenar los datos por columna en orden ascendente o descendente
- filtrar datos por columna

Acción	*Descripción*
Ordenar por columna	Haga clic en el encabezado de la columna para ordenarla de forma ascendente o descendente. 
Filtrar un texto	Escriba una parte del texto que desea buscar: se mostrarán solo los elementos que contengan esas letras.  Al escribir el mismo texto que en el ejemplo se mostrarán elementos con una descripción como: • "my**boss**" • "**boss**anova"

Acción	*Descripción*
Filtrar en base a una opción	Seleccione una opción: se mostrarán los elementos que coincidan con la opción seleccionada. 
Filtrar en base a varias opciones	Seleccione una o más opciones: se mostrarán los elementos que coincidan con las opciones seleccionadas. 
Cambiar el tamaño de la columna	Seleccione el borde de la columna y arrástrelo.

Procedimientos del analista

Introducción

La meta del analista es proporcionar evidencias válidas para la investigación en curso. La evidence:

- se recupera directamente desde el dispositivo por medio de un acceso físico
- se recupera por medio de un agent instalado

Para hacerlo, el analista puede realizar los siguientes procedimientos:

Procedimientos

Para recuperar evidence importante y recibir alertas

Para seleccionar y recuperar evidence importante:

Paso	Acción
1	En la sección **Sistema de archivos**, durante la intercepción remota, explore los discos duros del dispositivo en busca de archivos para descargar. *Consulte "**Recuperar evidence de los dispositivos (Sistema de archivos)**" en la página 51*
2	En la sección **Dashboard**, agregue la operation, los targets y los agents que se van a monitorear al Dashboard. *Consulte "**Monitoreo de evidence (Dashboard)**" en la página 91*
3	En la sección **Alerting**, defina las reglas para recibir alertas cuando llegue evidence de especial interés y para etiquetarla de acuerdo a su importancia. *Consulte "**Alert**" en la página 94* .

Análisis, selección y exportación de evidence

Para analizar, seleccionar y exportar evidence:

Paso	Acción
1	En la sección **Evidence**, analice la evidence y etiquétela de acuerdo a su nivel de importancia y a la necesidad de exportación. *Consulte "**Análisis de evidence (Evidence)**" en la página 37*
2	Para la evidence de especial interés, vea el análisis detallado. *Consulte "**Detalles de la evidence**" en la página 43*
3	En la sección **Evidence**, exporte la evidence útil. *Consulte "**Análisis de evidence (Evidence)**" en la página 37*
4	En la sección **Sistema de archivos**, exporte la estructura del disco duro *Consulte "**Recuperar evidence de los dispositivos (Sistema de archivos)**" en la página 51*

Procesar la información obtenida sobre las personas y lugares involucrados en la investigación

Para procesar la información obtenida sobre las personas y lugares involucrados en la investigación:

Paso	*Acción*
1	En la sección **Intelligence**, vea y administre las entidades de una operation. *Consulte "Administración de entidades: vistas de íconos y en tablas"* *"Administración de entidades: vista de enlaces" en la página 67* *"Administración de entidades: vista de posición" en la página 72* Administración de entidades: vista de posición*Consulte "Administración de entidades: vista de íconos y en tablas" en la página 65* .
2	Ver o editar los detalles de la entidad. *Consulte "Detalles de la entidad target" en la página 77* , *"Detalles de la entidad Person" en la página 82* *"Detalles de la entidad Position" en la página 85* *"Detalles de la entidad Virtual" en la página 87* *Consulte "Detalles de la evidence" en la página 43*
3	En la sección **Alerting**, cree reglas para recibir alertas cuando el sistema crea automáticamente nuevas entidades y nuevos enlaces y para etiquetar enlaces de acuerdo a su importancia. *Consulte "Alerting" en la página 96*

Operation y target

Presentación

Introducción

La administración de operations establece los targets que serán interceptados.

Contenido

En esta sección se incluyen los siguientes temas:

Qué debería saber acerca de las operations

Qué es una operation

Una operation es una investigación que se llevará a cabo. Una operation contiene uno o más targets, es decir, las personas físicas que se van a interceptar. El técnico asigna uno o más agents, de *escritorio* o *móviles,* al target. Por lo tanto, es posible instalar agents en una computadora o teléfono móvil.

Qué debería saber acerca de los targets

Qué es un target

Un target es una persona física que va a ser investigada. El técnico asigna uno o más agents, de escritorio o móviles, al target. Por lo tanto, es posible instalar agents en una computadora o teléfono móvil.

Administración de operations

Para administrar operations:	• Sección **Operations**

Propósito

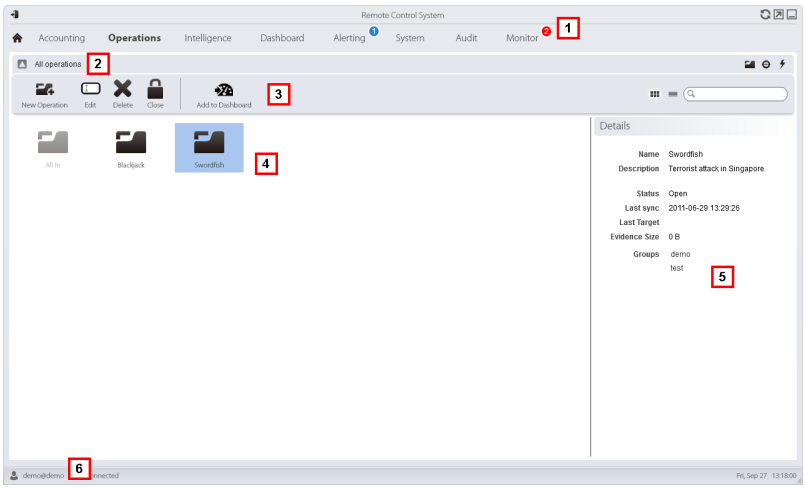
Esta función le permite:

- agregar la operation a los elementos que deberán monitorearse

NOTA: la función solo se activa si el usuario tiene autorización **Administración de operations**.

Cómo se ve la función

Así es como se ve la página:



Área	Descripción
1	Menú de RCS.
2	Barra de navegación
3	Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento:

Ícono	Descripción
	Agrega la operation al Dashboard.

4	Lista de operations creadas:  Operation abierta. Si se establecieron targets y se instalaron agents correctamente, se recibirá la evidence recopilada.  Operation cerrada. Todos los targets están cerrados y los agents desinstalados. Aún se pueden ver todos los targets y la evidence .
5	Datos de una operation seleccionada.
6	Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz *Consulte "**Elementos y acciones comunes de la interfaz**" en la página 10* .

Para ver una descripción de los datos en esta ventana *consulte "**Datos de la operation**" en la página siguiente* .

Para obtener más información sobre las operations *consulte "Qué debería saber acerca de las operations" en la página 18* .

Ver los targets de la operation

Para ver los targets de la operation:

Paso	*Acción*
1	Haga doble clic una operation: se abrirá la página de administración de targets. *Consulte "Página de la operation" abajo*

Datos de la operation

A continuación se describen los datos de la operation seleccionada:

Datos	*Descripción*
Nombre	Nombre de la operation.
Descripción	Descripción del usuario
Contacto	Los campos descriptivos se utilizan para definir, por ejemplo, el nombre de una persona de contacto (juez, abogado, etc.).
Estado	Estado de la operation y comando de cierre: **Abierta**: la operation está abierta. Si se establecieron targets y se instalaron agents correctamente, RCS recibe la evidence recopilada. **Cerrada**: la operation está cerrada y no podrá volver a abrirse. Los agents ya no enviarán más datos, pero todavía podrá consultar la evidence que ya se recibió.
Grupos	Grupos que pueden ver la operation.

Página de la operation

Para ver una operation:	• En la sección **Operations**, haga doble clic en una operation

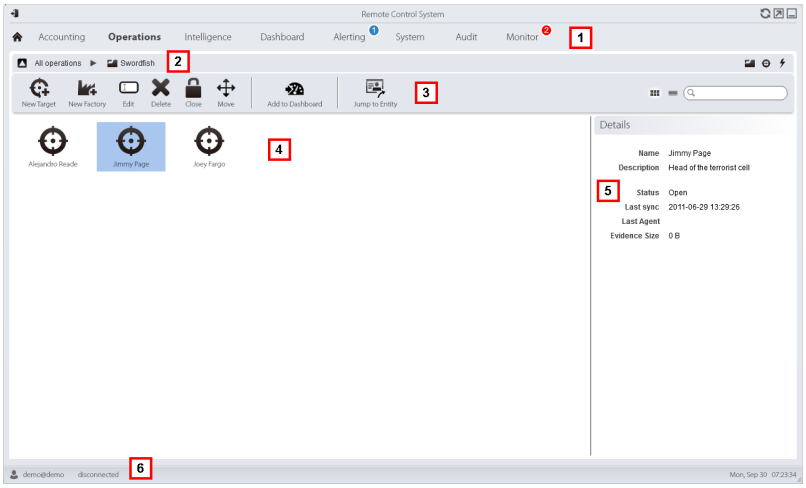
Propósito

Esta función le permite:

- agregar el target a los elementos que deberán monitorearse

Cómo se ve la función

Así es como se ve la página:



Área	*Descripción*
1	Menú de RCS.
2	Barra de navegación
3	Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento:

Ícono	*Función*
	Agrega el target al Dashboard.
	Abre la página de la entidad Target en Intelligence.

4	Lista de targets: target abierto target cerrado
5	Datos de un target seleccionado.
6	Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz *Consulte "**Elementos y acciones comunes de la interfaz**" en la página 10* .

Para obtener más información sobre las operations *consulte "**Qué debería saber acerca de las operations**" en la página 18* .

Para ver una descripción de los datos en esta ventana *consulte "**Datos de la página de la operation**" abajo* .

Datos de la página de la operation

A continuación se describen los datos del target seleccionado:

Datos	*Descripción*
Nombre	Nombre del target.
Descripción	Descripción del usuario
Estado	Define el estado del target:  Abierto. Si el técnico instala los agents correctamente, RCS recibirá la evidence recopilada.  Cerrado. Cerrado, ya no se podrá volver a abrir.

3

Targets

Presentación

Introducción

Un target es una persona física a quien se va a monitorear. Se pueden utilizar varios agents, uno por cada dispositivo de propiedad del target.

Contenido

En esta sección se incluyen los siguientes temas:

Página del target

Para abrir un target	• En la sección **Operations**, haga doble clic en una operation y en un target

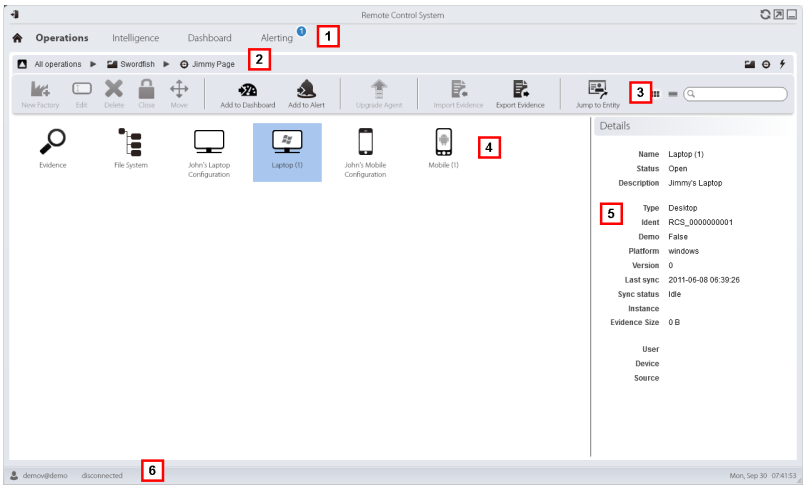
Propósito

Esta función le permite:

- exportar evidence del target
- abrir un agent instalado
- abrir la evidence del agent
- explorar el dispositivo del agent

Cómo se ve la función

Así es como se ve la página:



Área	*Descripción*
1	Menú de RCS.
2	Barra de navegación

Área	*Descripción*
3	Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento:

NOTA: el botón ☰ muestra los elementos en una lista con sus datos.

Ícono	*Función*
	Agrega el agent al Dashboard.
	Agrega el agent a los alerts: se genera un alert en cada sincronización.
	Exporta la evidence del target  NOTA: la función solo se activa si el usuario tiene autorización **Exportación de evidence**.
	Abre la página de la entidad Target en **Intelligence**.

4 Íconos/lista de factories creadas y agents instalados.

 : agent en modo de demostración.

 : agent scout esperando verificación.

 : agent soldier instalado.

 : agent elite instalado.

5 Datos de la factory o agent seleccionado.

6 Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz *Consulte "**Elementos y acciones comunes de la interfaz**" en la página 10* .

Para ver una descripción de los datos en esta ventana *consulte "**Datos de la página del target**" en la página siguiente* .

Exportar evidence del target

Para exportar evidence:

Paso	*Acción*
1	Haga clic en **Exportar evidence**: se abrirá la ventana de exportación.
2	Haga clic en **Exportar archivo**: la evidence se guardará en la carpeta especificada.

Datos de la página del target

Para ver los datos de la página:	• En la sección **Operations** , haga doble clic en una operation, luego en un target y luego haga clic en **Vista de íconos** o **Vista en tablas**

Los elementos de la página se pueden ver como íconos o como una tabla.

Vista de íconos

Los íconos se describen a continuación:

Datos	*Descripción*
	Ejemplo de agent scout instalado en un dispositivo de escritorio de Windows, en estado abierto.
	Ejemplo de agent soldier instalado en un dispositivo de escritorio con Windows, en estado abierto.
	Ejemplo de agent elite instalado en un dispositivo de escritorio con Windows, en estado abierto.

NOTA: los íconos de color gris claro corresponden a agents cerrados. Este es el ícono de un agent móvil para Android en estado cerrado:  .

Vista de Tabla

A continuación se describen los datos:

Datos	*Descripción*
Nombre	Nombre de la factory o agent.
Descripción	Descripción de la factory o agent
Estado	**Open**: el agent aún está activo en el dispositivo y puede continuar enviando datos. **Closed**: el agent ya no está activo.  NOTA: un agent cerrado no se puede volver a abrir. Los datos en RCS se podrán consultar más adelante.

Datos	*Descripción*
Tipo	De tipo escritorio o móvil.
Nivel	(solo para los agents) Nivel del agent: scout, soldier, elite.
Plataforma	(solo para los agents) Sistema operativo en la que se instala el agent.
Versión	(solo para los agents) Versión del agent. Se crea una nueva versión cada vez que se crea una nueva configuración.
Última sincronización	(solo para los agents) Fecha y hora de la última sincronización del agent.
Ident	(solo para los agents) Identificación unívoca de un agent.
Instancia	(solo para los agents) Identificación unívoca del dispositivo donde está instalado el agent.

4

Agents

Presentación

Introducción

Los agents obtienen datos del dispositivo en el que están instalados y los envían a los Collectors de RCS. Su configuración y software pueden actualizarse y transferir archivos que el target no notó.

Contenido

En esta sección se incluyen los siguientes temas:

Página del agent

Para administrar agents:	• En la sección **Operations**, haga doble clic en una operation, luego en un target y luego en un agent

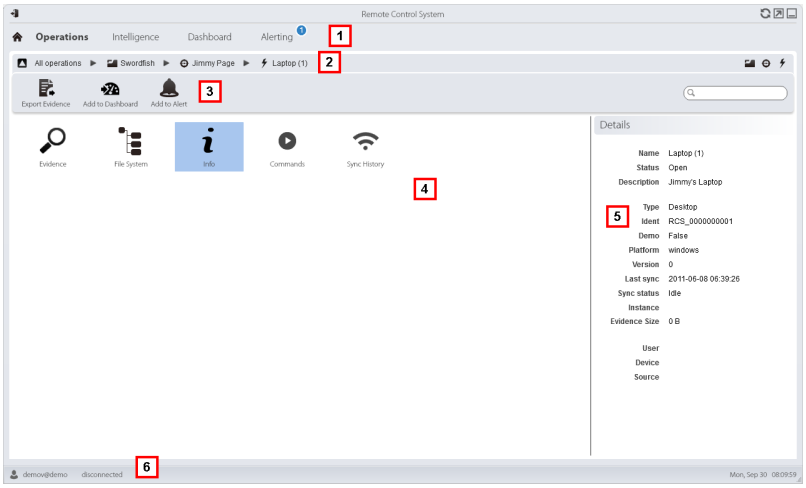
Propósito

Esta función le permite:

- verificar las actividades del agent a través del registro de eventos.
- ver la evidence recopilada por un agent
- explorar el sistema de archivos y transferir archivos desde el dispositivo en el que se encuentra instalado el agent

Cómo se ve la función

Así es como se ve la página:



Área	*Descripción*
1	Menú de RCS.
2	Barra de navegación

Área	*Descripción*
3	Barra de herramientas de la ventana.

Ícono	*Descripción*
	Permite exportar la evidence de un agent.  NOTA: la función solo se activa si el usuario tiene autorización **Exportación de evidence**.
	Agrega el agent al Dashboard.
	Agrega el agent a los alerts: se genera un alert en cada sincronización.

4 Posibles acciones en el agent. A continuación se muestra la descripción de cada elemento:

Ícono	*Descripción*
	Muestra la lista de evidence recopilada por el agent. *Consulte "**Análisis de evidence (Evidence)**" en la página 37* .
	Muestra el sistema de archivos del dispositivo. *Consulte "**Recuperar evidence de los dispositivos (Sistema de archivos)**" en la página 51* .
	Muestra el registro de eventos del agent (información). *Consulte "**Datos de registro de los eventos de un agent**" abajo* .
	Muestra los resultados de los comandos ejecutados en el dispositivo mediante las acciones **Execute**. *Consulte "**Página de comandos**" en la página siguiente* .
	Muestra el registro de sincronización del agent. *Consulte "**Datos del registro de sincronización de un agent**" en la página 32* .

5 Detalles del agent.

6 Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz *Consulte "**Elementos y acciones comunes de la interfaz**" en la página 10* .

Datos de registro de los eventos de un agent

A continuación se muestra la descripción de cada elemento:

Campo	*Descripción*
Obtención	Fecha y hora del evento obtenido en el dispositivo. Puede filtrarse. **Últimas 24 horas** es el valor predeterminado.
Recepción	Fecha y hora del evento registrado en RCS. Puede filtrarse. **Últimas 24 horas** es el valor predeterminado.
Contenido	Información de estado enviada por el agent.

Página de comandos

Para administrar resultados de comandos:	• En la sección **Operations**, haga doble clic en una operation, luego en un target, en un agent y en **Comandos**

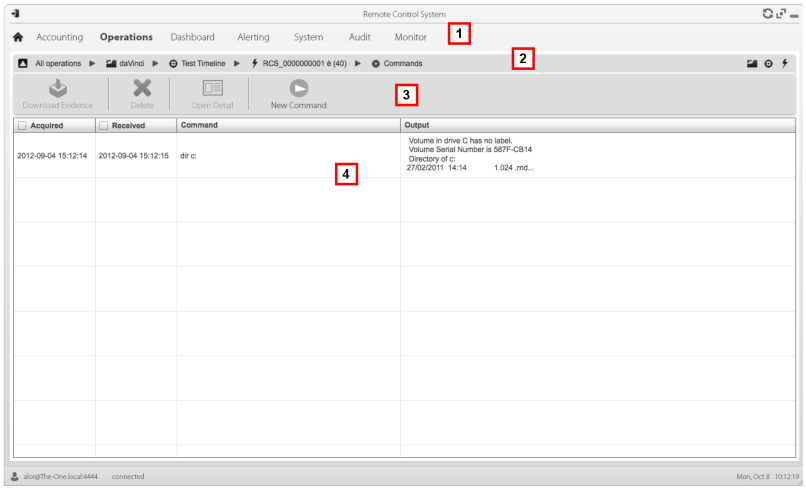
Propósito

Esta función le permite:

- verificar los resultados de los comandos ejecutados con la acción **Execute** establecida en el agent
- verificar los resultados del archivo ejecutable que se abre durante la transferencia de archivos hacia o desde el agent

Cómo se ve la función

Así es como se ve la página:



Área	*Descripción*
1	Menú de RCS.
2	Barra de navegación
3	Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento: *Ícono* *Descripción*  Permite exportar el comando seleccionado a un archivo .txt.  Elimina los comandos seleccionados.  NOTA: la función requiere una licencia de usuario y solo se activa si el usuario tiene **autorización Eliminación de evidence.**  Muestra los detalles de los comandos seleccionados.
5	Lista de comandos basada en los filtros establecidos.
6	Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz *Consulte "**Elementos y acciones comunes de la interfaz**" en la página 10* .

Datos del registro de sincronización de un agent

A continuación se muestra la descripción de cada elemento:

Campo	*Descripción*
Fin de sincronización	Fecha y hora en que terminó la sincronización. Puede filtrarse. **Últimas 24 horas** es el valor predeterminado.
Inicio de sincronización	Fecha y hora en que se inició la sincronización.
IP	Dirección IP usada para la sincronización.
Evidence	Número de piezas de evidence que se transfirieron realmente en esa sincronización de la cantidad total de piezas de evidence que se deben transferir.

Campo	*Descripción*
Tamaño	El tamaño total de la evidence transferida.
Velocidad	Velocidad de transferencia.
Expiró	Indica que la sincronización expiró.

5

Análisis de evidence

Presentación

Introducción

El análisis de la evidence a nivel de lista o detallado, permite seleccionar la evidence que se exportará a la autoridad competente.

Contenido

En esta sección se incluyen los siguientes temas:

Qué debería saber acerca de la evidence

Proceso de análisis

A continuación se describe el proceso de análisis:

Fase	*Descripción*
1	A medida que el sistema recopila evidence del agent, se muestra y actualiza el contador total.
2	El analista ve toda la evidence y la etiqueta para facilitar la consulta de la tabla y para exportarla posteriormente.
3	El analista analiza los detalles de la evidence entrante.
4	Al final de la investigación o a pedido, el analista exporta la evidence en un archivo que puede verse en un navegador.

Evidence acumulada en el dispositivo.

El agent envía la evidence al Collector en orden de creación. Si un dispositivo se sincroniza muy de vez en cuando o el ancho de banda es limitado, la evidence probablemente se acumulará en el dispositivo y tomará mucho tiempo recibir los datos más recientes.

Lo mismo puede ocurrir con la evidence de gran tamaño que está en la cola de espera: la evidence más recientes solo podrá enviarse después de haber enviado esta evidence.

Por este motivo, sugerimos que elimine la evidence más vieja y/o la evidence que exceda cierto tamaño. La evidence se elimina en la siguiente sincronización.

*Consulte "**Página del agent**" en la página 29 .*

Filtrar la evidence

Para limitar la cantidad de evidence que se desea ver, se pueden utilizar los filtros de los encabezados de las columnas.

*Consulte "**Elementos y acciones comunes de la interfaz**" en la página 10*

IMPORTANTE: si no se muestra ninguna evidence, revise el contado en la parte inferior derecha. Si el valor es parecido a "0/1270", esto significa que hay un filtro establecido que impide mostrar la evidence.

Los filtros seleccionados pueden guardarse con una descripción breve que puede consultarse más adelante.

IMPORTANTE: si se establecen filtros privados, no podrán ser utilizados por otros usuarios.

Traducir la evidence

El módulo RCS Translate está disponible con una licencia especial para la traducción de la evidence. De hecho, se comunica con un software de traducción de terceros que regresa el texto traducido a la interfaz de idioma.

RCS Translate traduce los siguientes tipos de evidence:

- clipboard
- chat
- file
- keylog
- message
- screenshot

Esta traducción se muestra en la página con la lista de evidence o en la página detallada de esa pieza de evidence particular.

Eliminar evidence

Esta función elimina una o más piezas de evidence que ya no se consideran útiles. Esta función depende del tipo de licencia instalada.

Para seleccionar la evidence que se va a eliminar se pueden utilizar los filtros (igual que cuando se selecciona evidence para su exportación).

IMPORTANTE: el filtro solo aparece cuando las teclas Suprimir **y Alt se presionan simultáneamente.**

Descripción del archivo .tgz con la evidence exportada

El archivo .tgz exportado es un archivo comprimido que puede abrirse con la mayoría de los programas de compresión (p. ej.: WinZip, WinRar). Una vez descomprimido, se ve como una carpeta con un archivo HTML.

Para ver el archivo:

Paso	*Acción*
1	Abra index.html con un navegador: la página principal muestra la lista de días con las estadísticas de la evidence recopilada por hora.
2	Haga clic en un día: aparecerá la lista de evidence, similar a la que se muestra la función **Evidence**.
3	Para esta lista, es posible realizar las siguientes acciones: • sobre las imágenes: haga clic para ver la imagen completa • sobre los archivos de audios: haga clic para ejecutar el mini reproductor • sobre los archivos descargables: haga clic en ↓↓ para descargar el archivo

Sugerencia: en la carpeta Estilo hay hojas de estilo para personalizar (p. ej.: logotipos, etc.). Estas hojas de estilo pueden copiarse al servidor que se usará en todos los informes generados por RCS Console.

Análisis de evidence (Evidence)

Para analizar evidence:	• En la sección **Operations**, haga doble clic en una operation y en un target, y luego haga clic en **Evidence** • En la sección **Operations**, haga doble clic en una operation, luego en un target, en un agent y por último haga clic en **Evidence**

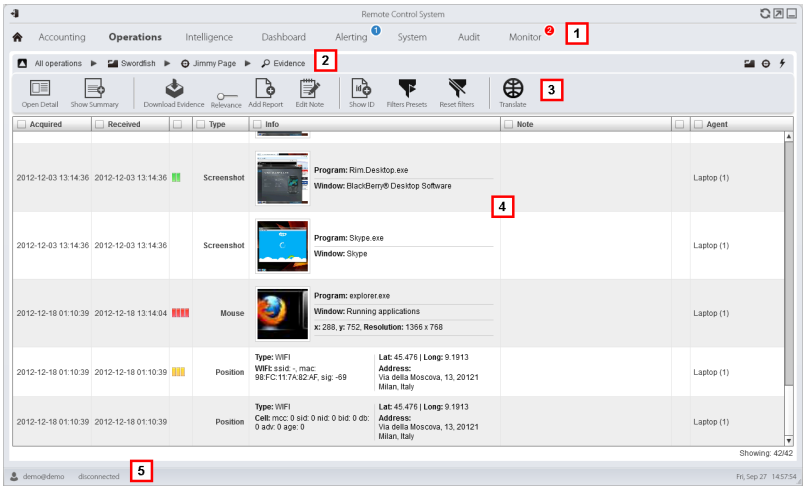
Propósito

Esta función le permite:

- preparar la evidence para analizarla, etiquetarla según el nivel de importancia, enviarla a un informe o agregar notas personales
- filtrar la lista para ver la evidence que le interesa
- traducir el contenido de la evidence al idioma de la interfaz (opcional)
- analizar superficialmente una evidence de la lista o ingresar a los detalles para hacer un análisis más profundo
- exportar evidence

Cómo se ve la función

Así es como se ve la página:



Área	*Descripción*
1	Menú de RCS.
2	Barra de navegación
3	Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento:

Ícono	*Descripción*
	Muestra los detalles de la evidence seleccionada. *Consulte "**Detalles de la evidence**" en la página 43*
	Muestra las cantidades totales por tipo de evidence.
	Exporta la evidence seleccionada en un archivo .tgz.  NOTA: la función solo se activa si el usuario tiene autorización **Exportación de evidence**.
	Elimina la evidence seleccionada.  NOTA: la función requiere una licencia de usuario y solo se activa si el usuario tiene autorización **Eliminación de evidence**.
	Aplica un nivel de importancia a la evidence seleccionada.
	Aplica una marca a la evidence seleccionada.
	Permite editar las notas de la evidence seleccionada.
	Muestra los códigos de ID de la evidence.
	Guarda los filtros seleccionados actualmente o carga la configuración de los filtros guardados previamente.
	Borra todos los filtros establecidos.
	Muestra el contenido en el idioma de la interfaz.  NOTA: esta función requiere una licencia de usuario.

4	Lista de evidence basada en los filtros establecidos.
5	Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz *Consulte "**Elementos y acciones comunes de la interfaz**" en la página 10* .

Para ver una descripción de los datos en esta ventana, *consulte "**Datos de la evidence**" en la página 41* .

Para ver una descripción de los datos que pueden exportarse, *consulte "**Datos de exportación de la evidence**" en la página 46* .

Para obtener más información sobre la evidence,,*consulte "**Qué debería saber acerca de la evidence**" en la página 35* .

Para ver una lista con los tipos de evidence *consulte "**Lista de tipos de evidence**" en la página 47*

Preparar la evidence para el análisis y la exportación, por medio de la asignación de etiquetas por importancia

Para asignar niveles de importancia a la evidence, lo cual es útil para la visualización y exportación:

Paso	*Acción*
1	Seleccione una o más piezas de evidence.
2	• Arrastre **Importancia** a la posición requerida o • Presione la combinación de teclas correspondiente.
3	**Resultado**: las piezas de evidence particulares se etiquetan con un símbolo de acuerdo a su nivel de importancia. Es posible filtrar la evidence por este símbolo así como incluirla o excluirla de la exportación.

Preparar la evidence para el análisis y la exportación, por medio de la asignación de etiquetas para el informe

Para incluir o excluir evidence en un informe y filtrar para su visualización:

Paso	*Acción*
1	Seleccione una o más piezas de evidence.
2	• Haga clic en **Agregar informe** o • presione Alt + R
3	**Resultado**: se marcan ciertas piezas de evidence particulares. Es posible filtrar la evidence por este símbolo así como incluirla o excluirla de la exportación.

Preparar la evidence para el análisis y la exportación, agregando notas personales

Para agregar notas personales a una o más piezas de evidence:

Paso	*Acción*
1	Seleccione una o más piezas de evidence.
2	• Haga clic en **Editar nota** o • presione Alt + N
3	**Resultado**: se puede editar el campo **Notas**. Si se seleccionan varias piezas de evidence, el texto ingresado se copiará a todos los demás campos **Nota**.

Análisis de evidence

Para analizar la evidence rápidamente o de forma profunda:

Paso	*Acción*
1	Analice la vista previa de la evidence. Por ejemplo, se puede ejecutar un mini reproductor para los archivos de audio, para saber si la evidence es importante o no.
2	Haga doble clic en la evidence: aparecerán los detalles de la evidence. *Consulte "Detalles de la evidence" en la página 43*

Ver los contadores separados por tipo

Para ver la cantidad total de evidence separada por tipo:

Paso	*Acción*
1	Haga clic en **Mostrar resumen**: aparecerán los símbolos de cada tipo de evidence, cada uno con su propio contador.
2	Haga clic en **Ocultar resumen** para ocultar los contadores.

Exportar la evidence que se muestra

Para seleccionar algunas piezas de evidence y exportarlas:

Paso	*Acción*
1	Primero etiquete la evidence según el nivel de importancia y en base a si debe considerarse en el informe o no (botón **Agregar informe**).
2	Seleccione por medio de los filtros de los encabezados de las columnas en grupos de evidence homogéneos (columna **Incluir en el informe**).
3	Haga clic en **Exportar evidence**: indica la evidence que se incluirá o excluirá. Se exportará la evidence que cumple con los criterios seleccionados y tiene marcado el campo **Incluir en el informe**.*Consulte "Datos de exportación de la evidence" en la página 46* .
4	Haga clic en **Guardar**: se crea y descarga un archivo .tgz file en la carpeta Descarga de RCS.

NOTA: la evidence también se puede exportar con el intérprete de comandos de Windows que se encuentra en la carpeta C:\RCS\DB\bin. El comando es: `rcs-db-export`. Ingrese `rcs-db-export --help` para ver la sintaxis correcta y la descripción de todas las opciones de comandos.

Eliminación de evidence en base a criterios especiales

Para eliminar varias piezas de evidence en base a criterios especiales (p. ej.: rango de fechas):

Paso	*Acción*
1	Mantenga presionada la tecla Alt y haga clic en  : aparecerá una ventana donde podrá establecer los criterios de eliminación de evidence. Para ver las descripciones de los campos *consulte "Datos de exportación de la evidence" en la página 46* , los campos son similares.

Datos de la evidence

Los datos de la evidence se describen a continuación tanto para el agent como para el target:

Datos	*Descripción*
Obtención	Fecha y hora en que se obtuvo la evidence. Puede filtrarse. **Últimas 24 horas** es el valor predeterminado.
Recepción	Fecha y hora en que se registró la evidence en RCS. Puede filtrarse. **Últimas 24 horas** es el valor predeterminado. Sugerencia: estos datos son útiles cuando sospecha que la fecha y la hora del dispositivo del target no está actualizada y la **Obtención** no es válida.

Datos	*Descripción*
Relevancia	Nivel de importancia de la evidence: las reglas de alert lo asignan automáticamente o se puede asignar manualmente en esta lista. El nivel de importancia se asigna utilizando: • el comando del menú **Relevancia** • teclas de acceso directo Lista de teclas de acceso directo.

Ícono	*Teclas de acceso directo*	*Descripción*
	Alt + 4	*Importancia máxima*
	Alt + +3	*Importancia intermedia*
	Alt + +2	*Importancia normal*
	Alt + +1	*Importancia mínima*
-	Alt + +0	*Sin importancia*

Tipo	Tipo de evidence a seleccionar. *Consulte "**Lista de tipos de evidence**" en la página 47*
Info	Información de la evidence: texto, imágenes, videos, audio, etc. Toda la información está acompañada de diferentes campos (p. ej.: los campos **contenido**, **programa**). Para filtrarlos indique las palabras que desea buscar o el nombre del campo y la palabra que desea buscar. Por ejemplo: • al escribir "jefe" se busca la palabra "jefe" o "Jefe" en todos los campos • mientras que si se escribe "**contenido**:jefe" se busca la palabra "jefe" o "Jefe" solo en los campos **contenido**.
Notas	Notas ingresadas por el analista mediante: • Menú **Editar nota** • tecla de acceso directo Alt + N
Reporte	Marca que permite indicar si la evidence puede incluirse o excluirse durante la exportación. La marca se asigna por medio de: • Menú **Agregar informe** • tecla de acceso directo Alt + R
Agent	(solo para la evidence del target) Nombre del agent que registró la evidence.

Detalles de la evidence

Para ver los detalles de la evidence:	• En la sección **Operations**, haga doble clic en una operation y luego en un target; haga clic en **Evidence** y luego doble clic en una pieza de evidence • En la sección **Operations**, haga doble clic en una operation, luego en un target y luego en un agent; haga clic en **Evidence** y doble clic en una pieza de evidence

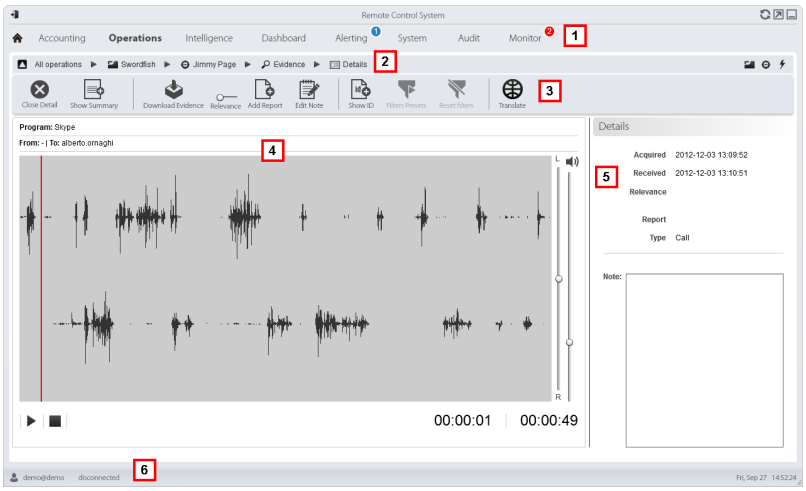
Propósito

Esta función le permite analizar los detalles de una evidence específica. La interfaz cambia de acuerdo con el tipo de evidence: texto, audio, imagen o mapa.

NOTA: la función solo se activa si el usuario tiene autorización **Editar evidence**.

Cómo se ve la función

Así es como se ven los detalles de la evidence de audio:



Área	*Descripción*
1	Menú de RCS.
2	Barra de navegación

Área	*Descripción*
3	Botones de acción de la evidence.

Ícono	*Descripción*
	Cierre los detalles y regrsee a la lista de evidence. *Consulte "**Análisis de evidence (Evidence)**" en la página 37* .
	Muestra las cantidades totales por tipo de evidence.
	Exporta la evidence en un archivo .tgz.
	Elimina la evidence.  NOTA: la función requiere una licencia de usuario y solo se activa si el usuario tiene autorización **Eliminación de evidence**.
	Aplica un nivel de importancia.
	Aplica una marca.
	Permite editar las notas.
	Muestra el código de ID.
	Guarda los filtros seleccionados actualmente o carga la configuración de los filtros guardados previamente.
	Borra todos los filtros establecidos.
	Muestra el contenido en el idioma de la interfaz.  NOTA: esta función requiere una licencia de usuario.

4 Detalles de la evidence. Los botones de análisis se muestran en base al tipo de evidence (audio, imagen, video).

5 Datos de detalles de la evidence.

6 Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz *Consulte "**Elementos y acciones comunes de la interfaz**" en la página 10* .

Para obtener más información sobre la evidence *consulte "**Qué debería saber acerca de la evidence**" en la página 35* .

Para ver una descripción de los datos en esta ventana, *consulte "**Datos de la evidence**" en la página 41* .

Acciones de la evidence del tipo imagen

A continuación se describen las acciones que pueden ejecutarse para la evidence de imagen:

Ícono	*Descripción*
	(solo para evidence de tipo screenshot y archivo) Muestra el texto extraído.  NOTA: si aparece el mensaje "OCR no disponible", esto significa que el documento aún no fue convertido e indexado. Si no se muestra el botón, esto significa que no se instaló la función. Póngase en contacto con el administrador del sistema.
	(solo para la evidence de tipo screenshot) Regresa a la vista de la imagen.
	Vista de pantalla completa.
1:1	Vista de la imagen en tamaño real.
	Amplía y reduce la imagen.
	Gira la imagen.
Antialias	Reduce el efecto del cambio de tamaño de la imagen.
	La imagen se convierte en la imagen predeterminada de la entidad Intelligence (si se instala el módulo **Intelligence**).

Acciones de la evidence del tipo audio

A continuación se describen las acciones que pueden ejecutarse para la evidence de audio:

Ícono	*Descripción*
	Ajustar volumen.
	Iniciar, pausar y detener el audio.
	Balance de volumen en una fuente local (target) y remota (interlocutor).

Datos de exportación de la evidence

Datos de exportación

A continuación se detallan los datos necesarios para exportar la evidence.

IMPORTANTE: solo se exportará la evidence que cumpla con ciertos criterios específicos.

Datos	*Descripción*
Desde **Hasta**	Rango de tiempo de la evidence a exportar.
Obtención	Considera la fecha como la fecha de obtención de la evidence en el dispositivo del target.
Recepción	Considera la fecha como la fecha de recepción de la evidence.
Relevancia	Nivel de importancia de la evidence a exportar.
Tipo	Tipos de evidence a exportar. NOTA: cuando no se selecciona ningún tipo de evidence, RCS exporta automáticamente todos los tipos.

Datos	*Descripción*
Reporte	Si se selecciona, solo se exportará la evidence con el campo **Informe** seleccionado. Es posible incluir o excluir la exportación de las notas.
Nombre del informe	Nombre del archivo exportado. De manera predeterminada, RCS asigna el nombre del archivo de la siguiente manera:

Evidence exportada de la página	*Nombre de archivo*
Target	*nombre del target* - *nombre del agent* - Evidence Export.tgz
Agent	*nombre del agent* - Evidence Export.tgz

Exportar Comandos

A continuación se describen los comandos de exportación de evidence.

Comando	*Descripción*
Exportar archivo	Inicia la exportación del archivo.
Exportar al conector	Inicia la exportación de la evidence al conector. NOTA: la función solo se activa si el usuario tiene autorización **Administración de conectores**.

Lista de tipos de evidence

A continuación se describen los tipos de evidence disponibles:

Módulo	*Tipo de archivo*	*Registro...*
Accessed files	texto	(solo para computadoras de escritorio) Registra los documentos o imágenes que abrió el target.
Addressbook	texto	contactos.
Application	texto	aplicaciones usadas.
Calendar	texto	calendario.
Call	audio	llamadas (p. ej.: GSM y VoIP).
Camera	image	Imágenes de la cámara web.
Chat	texto	chat.

Módulo	*Tipo de archivo*	*Registro...*
Clipboard	texto	información copiada en el portapapeles.
Dispositivo	texto	información del sistema.
File	texto	archivos abiertos por el target.
File System	texto	estructura del disco duro que puede explorarse con la función Sistema de archivos. *Consulte "**Recuperar evidence de los dispositivos (Sistema de archivos)**" en la página 51*
Info	texto	información proporcionada por el agent y definida en la configuración.
Keylog	texto	teclas presionadas en el teclado.
Messages	texto	correo electrónico.
Money	texto	Información sobre el monedero digital de criptodivisas (p. ej.: Bitcoin).
Mic	audio	audio.
Mouse	image	clics del mouse.
Contraseña	texto	password.
Position	image	posición geográfica del target.
Print	image	páginas impresas.
Screenshots	image	imágenes en la pantalla del target.
URL	texto	visited websites.

6

Exploración y recuperación de evidence de dispositivos en línea

Presentación

Introducción

La exploración gradual del dispositivo le permite encontrar y descargar evidence de su interés.

Contenido

En esta sección se incluyen los siguientes temas:

Qué debería saber acerca de la recuperación de evidence

Descripción

La función muestra la estructura del árbol del sistema de archivos del dispositivo donde se instala el agent (o de varios dispositivos, si se explora un sistema de archivos del target).

Operations

Es posible explorar la estructura en árbol del sistema de archivos de forma gradual. Primero se lee la estructura de primer nivel (comando **Recuperación predeterminada**), luego se exploran las carpetas, y a continuación se leen o se vuelven a leer las carpetas seleccionadas (comando **Descargar subárbol**).

Leer una carpeta o descargar un archivo después de la sincronización. Cuando se solicita leer una carpeta que ya se exploró (p. ej.: para ver los cambios), las diferencias se mostrarán al recibir los datos después de la siguiente sincronización. La carpeta que se desea explorar quedará resaltada en rojo y cambiará a verde cuando lleguen datos relevantes.

Interacción entre el sistema de archivos y la evidence de tipo de archivo

Una vez que se encuentra el archivo deseado, se puede descargar y guardar como evidence de tipo **Archivo** (comando **Descargar archivo**)

NOTA: la estructura de árbol del sistema de archivos de RCS Console se integra automáticamente con los datos recibidos de la evidence de tipo **Archivo**.

Componentes del sistema de archivos

La estructura de cada dispositivo muestra las carpetas que se van a explorar y aquellas que ya se exploraron:

Ejemplo	*Descripción*
Agents	Raíz del dispositivo.
ProgramData	Carpeta que aún no se exploró.
Users	Carpeta explorada.

Recuperar evidence de los dispositivos (Sistema de archivos)

Para administrar el sistema de archivos del dispositivo.	• En la sección **Operations**, haga doble clic en una operation y en un target, y luego haga clic en **Sistema de archivos** • En la sección **Operations**, haga doble clic en una operation, en un target, en un agent y haga clic en **Sistema de archivos**

Propósito

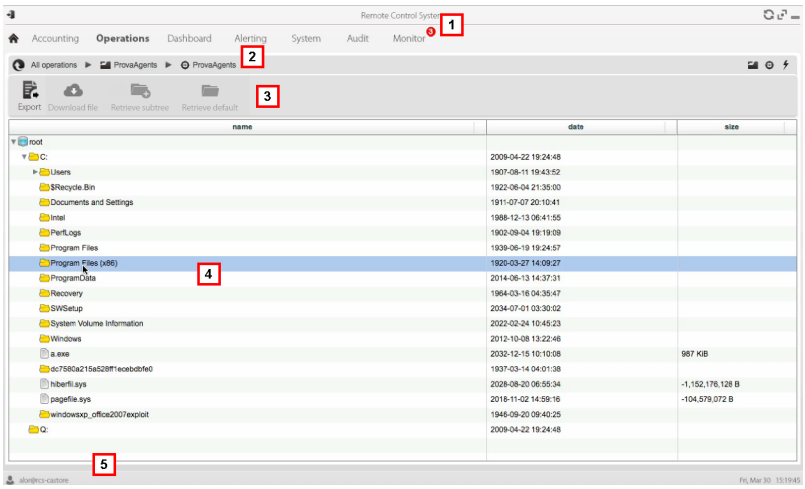
Esta función le permite:

- explorar la estructura en árbol del sistema de archivos del dispositivo donde se instala el agent (o de varios dispositivos, si se explora un sistema de archivos del target).
- seleccione el archivo que desea agregar a la cola de descarga del agent
- exportar la estructura explorada (sistema de archivos)

NOTA: la función solo se activa si el usuario tiene autorización **Explorar el sistema de archivos con un agent**.

Cómo se ve la función

Así es como se ve la página:



Área	*Descripción*
1	Menú de RCS.
2	Barra de navegación

Área	*Descripción*
3	Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento:

Ícono	*Descripción*
	Exporta la estructura completa a un archivo .tgz.
	Descarga el archivo seleccionado a una evidence de tipo **Archivo**.
	Explora el contenido de la carpeta seleccionada.
	Solicita la estructura de primer nivel del disco.
	Muestra la lista de solicitudes al sistema de archivos actualmente suspendidas que esperan a la siguiente sincronización.

4	Estructura del disco duro del dispositivo.
5	Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz *Consulte "**Elementos y acciones comunes de la interfaz**" en la página 10* .

Para obtener más información sobre la exploración del sistema de archivos, *consulte "**Qué debería saber acerca de la recuperación de evidence**" en la página 50*

Exploración del contenido del sistema de archivos y descarga de archivos

Para explorar el contenido y descargar el contenido que sea de su interés:

Paso	*Acción*
1	Seleccione una carpeta.
2	• Haga clic en **Descargar subárbol** y establezca el nivel de profundidad de las subcarpetas • Haga clic en **Guardar**: las carpetas que tengan algún cambio quedarán resaltadas en la siguiente sincronización.

Sugerencia: indique unos pocos niveles por vez, proceda gradualmente.

Paso	*Acción*
3	Repita los pasos 1-2 en las subcarpetas a explorar.
4	Después de identificar el archivo que le interesa, selecciónelo y haga clic en **Descargar archivo**: en la siguiente sincronización se descargará el archivo como una evidence de tipo **Archivo**.

Intelligence

Presentación

Introducción

La sección le permite representar las interacciones entre targets a un nivel alto, relacionando la evidence recibida de los agents con otra información con la que ya se cuenta.

Contenido

En esta sección se incluyen los siguientes temas:

Qué debería saber acerca de Intelligence

Presentación

Introducción

El analista procesa la información de la investigación en su posesión en la sección Intelligence.

Tanto las personas bajo investigación como otras personas y lugares involucrados en la investigación son representados por medio de *entidades*. Tanto las relaciones entre las personas como las relaciones entre personas y lugares, se representan por medio de *enlaces* entre entidades.

El sistema crea nuevas entidades y nuevos enlaces entre entidades en base a la evidence recibida desde los dispositivos del target. El analista interpreta y organiza esta información, agrega, edita o elimina entidades o enlaces, de acuerdo con la evolución de la investigación.

Licencia para la sección Intelligence

Las funciones de Intelligence solo están disponibles por medio de una licencia.

Sin una licencia de usuario, el analista solo puede usar la sección Intelligence para ver y agregar datos en los targets de la operation; el sistema no procesará información en base a la evidence recopilada. Las únicas entidades incluidas son los Targets y solo pueden verse como íconos o en tablas,*consulte "**Administración de entidades: vista de íconos y en tablas**" en la página 65 .*

Para obtener más información

*Consulte "**Qué debería saber acerca de las entidades**" abajo .*
*Consulte "**Qué debería saber acerca de los enlaces**" en la página 57 .*
*Consulte "**Qué debería saber acerca de las entidades Grupo**" en la página 59*
*Consulte "**Qué debería saber acerca de cómo funciona Intelligence**" en la página 60*

Qué debería saber acerca de las entidades

Introducción

La entidad representa a una persona o lugar involucrado en una investigación.

Cada entidad se define por medio de la información detallada que le permite al sistema identificar las relaciones entre las entidades.

Las personas involucradas en la investigación: las entidades Target y las entidades Person

El sistema define dos tipos de entidades para representar a las personas involucradas en una investigación:

-  :tipo Target, para las personas sujetas a intercepciones
-  :tipo Person, para las personas no sujetas a intercepciones

Los lugares involucrados en una investigación: entidad Position y entidad Virtual

El sistema define dos tipos de entidades para representar a los lugares involucrados en una investigación:

-  : tipo Posición, sitios físicos
-  : tipo Virtual, sitios virtuales como páginas web

Administración de entidades

El analista administra las entidades para que representen la evolución de la investigación, por lo tanto, se encarga de:

- agregar entidades para monitorear a otras personas y lugares que se consideran de interés
- agregar detalles a las entidades para proporcionar nuevos datos al sistema e identificar relaciones entre las entidades
- eliminar entidades cuando las personas o los lugares se consideran insignificantes para la investigación
- formar la entidad Grupo para mostrar y analizar la información más fácilmente, *consulte "**Qué debería saber acerca de las entidades Grupo**" en la página 59*

Entidad Target

La entidad Target se crea automáticamente al crear un target en la sección Operations. El nombre y la descripción son los mismos que se asignaron en la sección Operations.

NOTA: Las entidades Target no pueden eliminarse desde la sección Intelligence. Para eliminarlas, se deben eliminar los targets desde la sección Operations.

NOTA: es posible cambiar el nombre y la descripción del target sin que esto afecte a la sección Operations.

El sistema agrega detalles de la entidad Target con la información recopilada de la evidence (por ejemplo: fotos, personas más contactadas). El analista puede actualizar otra información que tenga en su poder. *Consulte "**Detalles de la entidad target**" en la página 77*

Entidad Person

El analista puede crear una entidad Person de forma manual o el sistema puede crearla automáticamente.

La entidad Person se define como los ID que usa para comunicarse, por teléfono o Internet (por ejemplo: número de teléfono, contacto de Skype).

NOTA: mientras más información se incluya en la hoja de datos, mayor será la probabilidad de que el sistema identifique enlaces entre esa entidad y otras.

Si una entidad Person se convierte en el objeto de una intercepción, puede transformarse o cambiar a una entidad Target. De esta forma, el sistema crea un nuevo target en la operation correspondiente.

NOTA: la función solo se activa si el usuario tiene autorización **Administración de targets**.

Consulte "Detalles de la entidad Person" en la página 82

Entidad Position

El analista puede crear una entidad Position de forma manual o el sistema puede crearla automáticamente.
La entidad Position se define como las coordenadas geográficas (latitud y longitud) o la dirección del sitio a la que representa y un rango de precisión.

NOTA: el rango de precisión debe ser adecuado para el tipo de lugar (p. ej.: 50-100 m para un edificio, mucho más para un parque).

Consulte "Detalles de la entidad Position" en la página 85

Entidad Virtual

El analista debe crear la entidad Virtual manualmente.
La entidad Virtual se define como una o más direcciones URL de la página web a la que representan.
Consulte "Detalles de la entidad Virtual" en la página 87

Qué debería saber acerca de los enlaces

Introducción

Un enlace es una relación entre entidades. Solo puede haber un enlace entre dos entidades.
Existen tres tipos de enlaces:

- ····· Know
- —— Peer
- ---- Identity

Enlaces Know

Los enlaces Know representan relaciones de tipo *conocimiento*. Dos entidades tienen un enlace Know cuando al menos una de las dos tiene a la otra en su agenda.

Un enlace Know puede ser unidireccional o bidireccional.

Enlaces Peer

Un enlace Peer significa que hubo algún *contacto* entre las dos entidades.

Dos entidades que representan a personas tienen un enlace Peer cuando hubo una comunicación directa entre las dos entidades (p. ej.: llamada telefónica, chat). La relación puede ser unidireccional y bidireccional.

Una entidad que representa a una persona y una que representa a un lugar tienen un enlace Peer cuando la persona estuvo en ese lugar (de forma física o a través de Internet). La relación es solo unidireccional: de la entidad que representa a una persona a la que representa un lugar.

Los enlaces Peer representan una relación más fuerte que los enlaces Know, por lo que reemplazan a cualquier enlace Know entre las entidades.

manejo de los enlaces Peer y Know

El analista administra los enlaces para que representen la evolución de la investigación, por lo tanto, se encarga de:

- agregar o editar enlaces entre dos entidades cuando tiene en su posesión información que demuestra una relación entre ambas
- asignar un nivel de importancia a los enlaces para representar la importancia de la relación en la investigación
- eliminar enlaces cuando cuenta con información que demuestra una falta de relación o si la relación es insignificante para la investigación.

Enlaces Identity

Los enlaces Identity representan una sugerencia de una relación de *identidad* entre dos entidades que representan a personas. El sistema crea este tipo de enlaces automáticamente cuando las dos entidades comparten cuando menos una identificación (p. ej.: número de teléfono).

Los enlaces Identity no tienen direcciones.

Administración de los enlaces Identity

El analista debe decidir el motivo de los enlaces Identity y cómo actuar según el caso:

- si son la misma persona, ambas entidades deben combinarse
- si son dos personas diferentes que usaron la misma identificación, la identificación compartida debe ser eliminada de una de las entidades y también se debe eliminar el enlace

Valor temporal del enlace

Los enlaces son el resultado de un proceso manual o automático en un determinado momento. Sin embargo, el momento en que se creó un enlace, es decir, cuando se formó la primera relación entre las entidades, solo se registra para los enlaces creados automáticamente por el sistema.

De esta forma, se puede seleccionar un análisis periódico para ver cuándo se crearon ciertas relaciones.

Para los demás enlaces, una vez que se crearon (automática o manualmente) se considera que el sistema los creó en un comienzo.

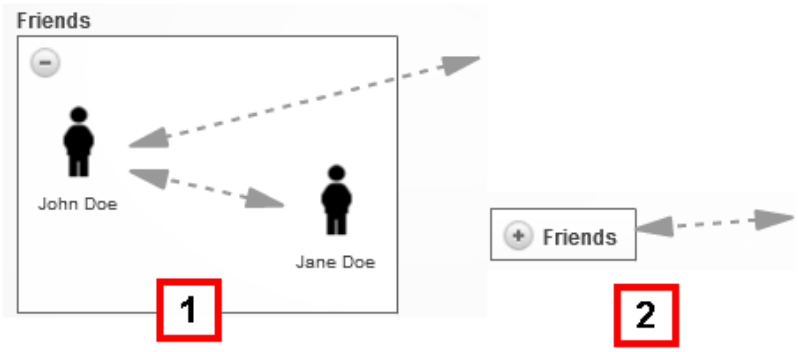
Qué debería saber acerca de las entidades Grupo

Introducción

Las entidades Grupo agrupan a otras entidades. El sistema puede crearlas automáticamente y el analista puede crearlas manualmente.
El grupo tiene dos formas de visualización:

- expandida, que permite ver todas las entidades que representa y sus enlaces
- reducida, que ocupa menos espacio y facilita la visualización de las entidades. Se muestran las conexiones hacia y desde el grupo, pero sin los enlaces dentro del grupo.

Ejemplo de un grupo expandido **[1]** y un grupo reducido **[2].**



Los grupos solo se muestran en la vista de enlaces, *consulte "**Administración de entidades: vista de enlaces**" en la página 67 .*

Entidades Grupo creadas por el sistema

El sistema crea un grupo automáticamente solo cuando encuentra una relación entre una entidad Person y una entidad Target que pertenecen a dos operations diferentes. Crea un Grupo en ambas operations y asigna a cada uno el nombre de la otra operation.
El Grupo creado representa a la entidad de tipo Person o Target en la operation relacionada con las entidades de la operation que se está analizando.
El Grupo solo puede expandirse si tiene permiso de administrar la operation a la que pertenecen las entidades a las que representa. De lo contrario, la única forma de visualización es la reducida.

Entidad Grupo creada manualmente.

El analista puede agrupar cualquier tipo de entidad en un Grupo, pero una entidad solo puede pertenecer a un grupo.

La creación de un Grupo puede ayudar con el procesamiento de datos. Por ejemplo, puede decidir crear una entidad Grupo llamada "Familia Rossi" con entidades que representen a las personas y lugares asociados con la familia Rossi.

Qué debería saber acerca de cómo funciona Intelligence

Introducción

Intelligence permite que el analista procese la evidence y los datos de la investigación.

Proceso de Intelligence

Fase	*Descripción*
1	Cuando se abre una operation en la sección Operations, el sistema crea una operation en la sección Intelligence.
2	Cuando se crea un target en las sección Operations, el sistema crea una entidad Target.
3	El sistema, en base a la evidence recopilada desde los dispositivos del target, crea enlaces con las entidades Target, así como nuevas entidades y enlaces. NOTA: el sistema procesa información desde los targets en todas las operations abiertas.
4	El analista agrega entidades para representar a las personas, lugares y páginas web que considera de interés para la investigación y agrega detalles.
5	El sistema continúa actualizando entidades y sus enlaces en base a la nueva evidence e información agregada por el analista.
6	El analista interpreta y administra entidades y sus enlaces para proponer soluciones para la investigación. NOTA: el analista puede establecer una regla de alert para recibir una alerta cuando el sistema crea una entidad o enlace. *Consulte "**Alert**" en la página 94* .

Criterios para la creación automática de enlaces Know

Si la evidence indica que...	*El sistema crea...*
los targets John y Paul tienen la identificación 003214567 en sus agendas	• una entidad Person con identificación 003214567 • un enlace unidireccional Know de John a la entidad Person • un enlace unidireccional Know de John a la entidad Person
el target John tiene una identificación 003214567 en su agenda para la entidad Target/Person Paul	un enlace unidireccional Know de John a Paul

Criterio de creación automática de enlaces Peer con entidades Target y Person

Si la evidence indica que...	*El sistema crea...*
los targets John y Paul se comunicaron con la identificación 003214567	• una entidad Person con identificación 003214567 • un enlace unidireccional Peer de John a la entidad Person • un enlace unidireccional Peer de Paul a la entidad Person
el target John se comunicó con la entidad Target/Person Paul	un enlace unidireccional Peer de John a Paul
el target John se comunica frecuentemente con la identificación 003214567	• una entidad Person con identificación 003214567 • un enlace unidireccional Peer de John a la entidad Person

Criterio de creación automática de enlaces Peer con entidades Position

Si la evidence indica que...	*El sistema crea...*
los targets John y Paul estuvieron en Times Square al mismo tiempo	• una entidad Position con las coordenadas geográficas de Times Square • un enlace unidireccional Peer de John a la entidad Position • un enlace unidireccional Peer de Paul a la entidad Position
el target John estuvo en el lugar asociado con la entidad Position de la oficina de John	un enlace unidireccional Peer de John a la entidad oficina de John

Si la evidence indica que...	*El sistema crea...*
el target John con frecuencia está en Times Square	• una entidad Position con las coordenadas geográficas de Times Square • un enlace unidireccional Peer de John a la entidad Position

NOTA: para el sistema, un target visitó un lugar si estuvo allí por un tiempo mínimo de 15 minutos. Dos targets visitaron el mismo lugar al mismo tiempo si estuvieron allí al mismo tiempo por 15 minutos como mínimo.

Criterio de creación automática de enlaces Peer con entidades Virtuales

Si la evidence indica que...	*El sistema crea...*
el target John visitó la dirección URL www.lugaressecretos.com asociada con la entidad Virtual del sitio web Lugares secretos	un enlace unidireccional Peer de John al sitio web Lugares secretos

Criterio de creación automática de enlaces Identity con entidades Target y Person

Si el sistema detecta que...	*El sistema crea...*
La entidad Target/Person John tiene el número 003214567 en sus datos de identificación y la entidad Target/Person Paul tiene el número 003214567 en sus datos de identificación	un enlace Identity entre John y Paul

El criterio de creación automática de enlaces entre las entidades Target/Person en diferentes operations

Si el sistema detecta que...	*El sistema crea...*
se cumplen las condiciones para crear un enlace entre la entidad Target/Person de tráfico de drogas John y la entidad Target/Person de tráfico de armas Paul NOTA: el criterio de creación de enlace entre operations es el mismo que los de un enlace dentro de la operation.	en la operation de tráfico de drogas, • la entidad Grupo de tráfico de armas • un enlace entre John y el Grupo de tráfico de armas en la operation de tráfico de armas • la entidad Grupo de tráfico de drogas • un enlace entre Paul y el Grupo de tráfico de drogas NOTA: si la entidad de grupo se creó debido a una relación previa, solo se crea el enlace. NOTA: el tipo y la dirección del enlace creado está determinado por las mismas reglas de enlace entre las entidades de la misma operation.

Administración de la operation Intelligence

Para administrar operations sujetas a inteligencia:	• Sección **Intelligence**

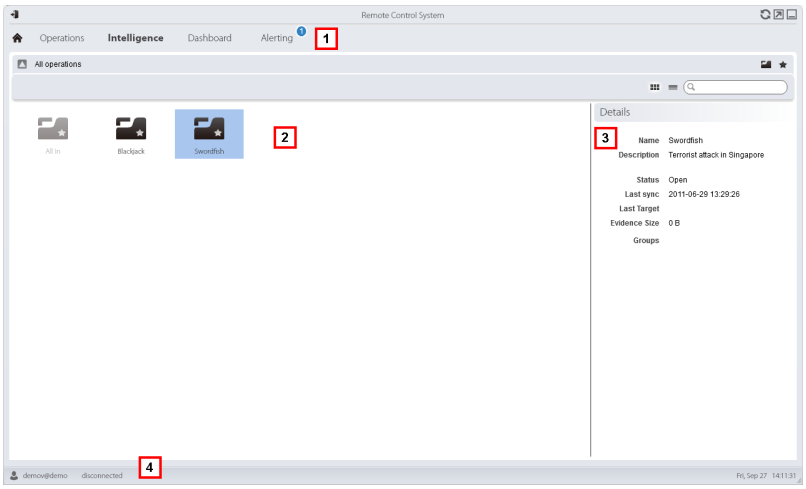
Propósito

Esta función le permite:

- ver operations Intelligence

Cómo se ve la función

Así es como se ve la página:



Área	*Descripción*
1	Menú de RCS.
2	Lista de operations:  Operation abierta.  Todas las operations. Muestra las entidades en todas las operations.
3	Datos de una operation seleccionada.
4	Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz *Consulte "**Elementos y acciones comunes de la interfaz**" en la página 10* .

Ver las entidades de la operation

Para ver las entidades de la operation:

Paso	*Acción*
1	Haga doble clic en una operation: se abrirá la página de administración de entidades. *Consulte "**Administración de entidades: vista de enlaces**" en la página 67*

Administración de entidades: vista de íconos y en tablas

Para administrar entidades:	• En la sección **Intelligence**, haga doble clic en una operation y luego haga clic en **Vista de íconos** o **Vista en tablas**

Propósito

Esta función le permite:

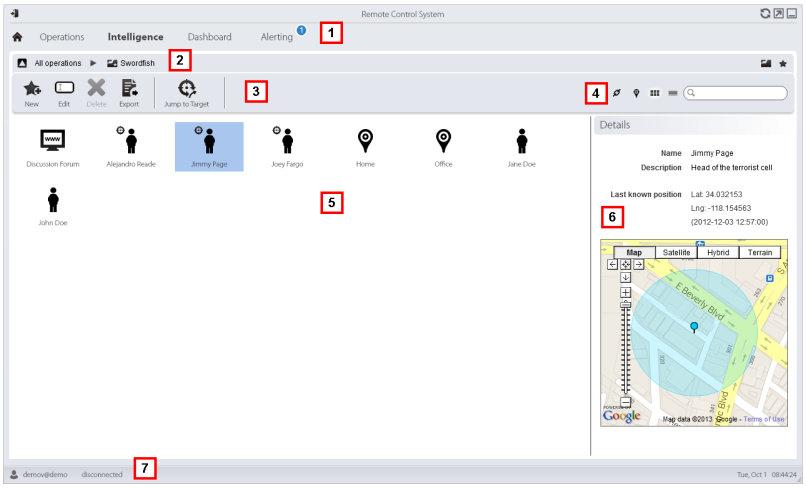
- ver las entidades de la operation
- administrar las entidades de la operation
- abrir la página del target vinculada con la entidad Target

NOTA: las únicas entidades que se pueden ver y administrar sin una licencia de usuario son las entidades Target.

NOTA: la función solo se activa si el usuario tiene autorización **Administración de entidades**.

Cómo se ve la función

Así es como se ve la página:



Área	*Descripción*
1	Menú de RCS.
2	Barra de navegación

Área	*Descripción*
3	Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento:

Ícono	*Función*
	Permite crear una nueva entidad
	Permite editar una entidad
	Elimina una entidad
	Exporta los datos de una entidad en formato `.html`
	Abre la página del target asociada con la entidad.*Consulte "**Página del target**" en la página 24* .

4	Botones de vista y del cuadro de búsqueda:

Objeto	*Descripción*
	Cuadro de búsqueda. Al escribir parte del nombre o la descripción se mostrará una lista con las entidades que contienen esas letras.
	Muestra las entidades en una tabla.
	Muestra las entidades como íconos
	Muestra las entidades Target y Position y sus enlaces en un mapa. *Consulte "**Administración de entidades: vista de posición**" en la página 72*
	Muestra las entidades y sus enlaces en un gráfico. *Consulte "**Administración de entidades: vista de enlaces**" en la página opuesta*

5	Lista de entidades
6	Datos de una entidad seleccionada.
7	Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz *Consulte "**Elementos y acciones comunes de la interfaz**" en la página 10* .

Para obtener más información sobre Intelligence *consulte "Qué debería saber acerca de Intelligence" en la página 55 consulte "Qué debería saber acerca de las entidades" en la página 55*

Ver los detalles de una entidad

Para ver los detalles de una entidad:

Paso	*Acción*
1	Haga doble clic en una entidad: se abrirá la página de detalles. • *"Detalles de la entidad target" en la página 77 .* • *"Detalles de la entidad Person" en la página 82 .* • *"Detalles de la entidad Position" en la página 85 .* • *"Detalles de la entidad Virtual" en la página 87 .*

Administración de entidades: vista de enlaces

Para administrar entidades sujetas a inteligencia:	• En la sección **Intelligence**, haga doble clic en una operation y luego haga clic en **Mapa de enlaces**

Propósito

Esta función le permite:

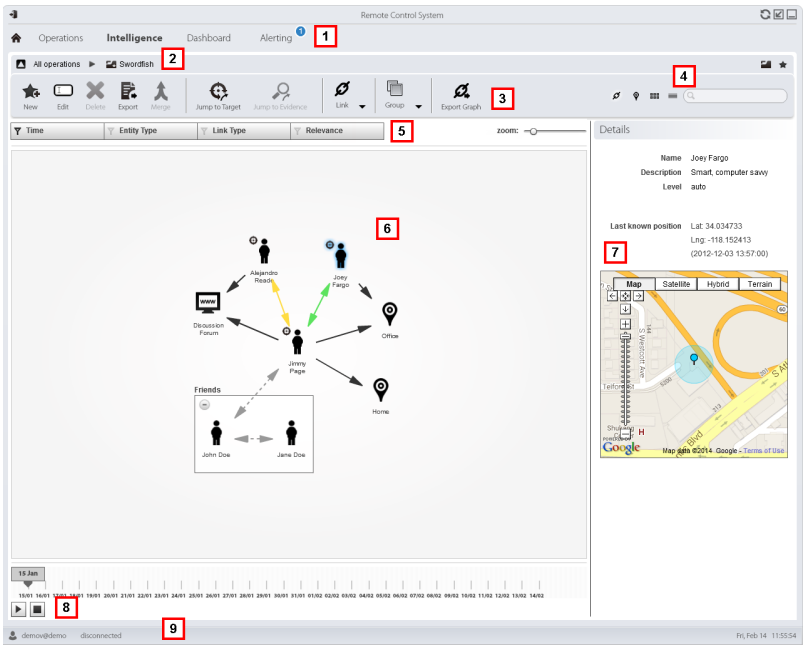
- ver las entidades de la operation y sus enlaces en la operation o en otras operations en un gráfico
- administrar entidades
- administrar enlaces de entidades
- abrir la página del target vinculada con la entidad Target
- abrir la evidence asociada con un enlace
- ver dinámicamente la evidence asociada con los enlaces de entidades

NOTA: esta función requiere una licencia de usuario. Sin la licencia, la vista predeterminada de entidades de la operation es la de íconos, *consulte "Administración de entidades: vista de íconos y en tablas" en la página 65 .*

NOTA: la función solo se activa si el usuario tiene autorización **Administración de entidades**.

Cómo se ve la función

Así es como se ve la página:



Área	*Descripción*
1	Menú de RCS.
2	Barra de navegación

Área	*Descripción*
3	Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento:

Ícono	*Función*
	Permite crear una nueva entidad
	Permite editar una entidad
	Elimina una entidad
	Exporta los datos de una entidad en formato `.html`
	Combina dos entidades
	Abre la página del target asociada con la entidad.*Consulte "**Página del target**" en la página 24* .
	Abre la evidence que contribuyó a generar ese enlace. Se establecieron filtros de tipo de enlace en el gráfico. La evidence que se muestra se filtrará según el caso (p. ej., solo Whatsapp y Facebook). *Consulte "**Análisis de evidence (Evidence)**" en la página 37*
	 : crea un enlace  : permite editar un enlace  : elimina un enlace : aplica un nivel de importancia al enlace
	 : crea una entidad Grupo  : elimina una entidad Grupo  : expande todos los grupos  : contrae todos los grupos
	Exporta el gráfico de entidades en formato `.graphml`.

Área	*Descripción*
4	Botones de vista y del cuadro de búsqueda:

Objeto	*Descripción*
	Cuadro de búsqueda. Al escribir parte del nombre o la descripción se mostrará una lista con las entidades que contienen esas letras.
	Muestra las entidades en una tabla. *Consulte "**Administración de entidades: vista de íconos y en tablas**" en la página 65*
	Muestra entidades como íconos *Consulte "**Administración de entidades: vista de íconos y en tablas**" en la página 65*
	Muestra las entidades Target y Position y sus enlaces en un mapa. *Consulte "**Administración de entidades: vista de posición**" en la página 72*
	Muestra las entidades y sus enlaces en un gráfico.

5 Área de filtros

6 Gráfico de entidades y enlaces basado en los filtros establecidos

NOTA: los enlaces Know e Identity creados manualmente siempre se muestran, independientemente del período que se seleccione.

NOTA: la entidad con más enlaces se coloca en la parte central del gráfico.

7 Datos de una entidad seleccionada.

8 Comando que muestra dinámicamente la cantidad, la dirección y la frecuencia de la evidence que define los enlaces entre las entidades que se muestran en el gráfico en base a los filtros establecidos.

9 Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz *Consulte "**Elementos y acciones comunes de la interfaz**" en la página 10* .

Para obtener más información acerca de Intelligence *consulte "**Qué debería saber acerca de Intelligence**" en la página 55 consulte "**Qué debería saber acerca de las entidades**" en la página 55*

Ver los detalles de una entidad

Para ver los detalles de una entidad:

Paso	*Acción*
1	Haga doble clic en una entidad: se abrirá la página de detalles. • *"**Detalles de la entidad target**" en la página 77 .* • *"**Detalles de la entidad Person**" en la página 82 .* • *"**Detalles de la entidad Position**" en la página 85 .* • *"**Detalles de la entidad Virtual**" en la página 87 .*

Combinar dos entidades en una

Para combinar dos entidades en una:

Paso	*Acción*
1	Manteniendo presionada la tecla Ctrl en el teclado, seleccione dos entidades. NOTA: solo se pueden combinar una entidad Person con una entidad Target o dos entidades Person.
2	Haga clic en **Combinar** **Resultado:** en el gráfico se mostrará una entidad con el nombre y la descripción de la primera entidad con los detalles de ambas. NOTA: si una entidad Target se combina con una entidad Person, la entidad Target mantiene los detalles de la entidad Person.

Crear un enlace entre dos entidades

Para crear un enlace entre dos entidades:

Paso	*Acción*
1	Manteniendo presionada la tecla Ctrl en el teclado, seleccione dos entidades.
2	Haga clic en **Enlaces, Agregar**
3	Seleccione la dirección, el tipo y el nivel de importancia del enlace y haga clic en **Guardar.** **Resultado**: el enlace se mostrará en el gráfico

Crear un grupo

Para crear un grupo:

Paso	*Acción*
1	Manteniendo presionada la tecla Ctrl en el teclado, seleccione las entidades que desea agrupar.
2	Haga clic en **Grupo, Grupo.** **Resultado**: el grupo se mostrará en el gráfico.

Ver de forma dinámica la evidence de los enlaces entre las entidades

Para ver de forma dinámica la evidence de los enlaces entre las entidades:

Paso	*Acción*
1	Asegúrese de que las entidades que se muestran en el gráfico y el período de tiempo seleccionado sean los que desee ver. Use los filtros para establecer sus preferencias.
2	Haga clic en **Reproducir** para mostrar. **Resultado**: se deslizarán puntos rojos a lo largo de los enlaces para representar la evidence recopilada.  NOTA: la dirección en la cual se deslizan los puntos indica la dirección de la evidence (p. ej.: el punto rojo se desliza desde la entidad John a la entidad Paul si John le envió un correo electrónico a Paul).  NOTA: la cantidad de puntos indica la cantidad de evidence: un punto indica que al menos se recopilaron 10 piezas de evidence; dos puntos, entre 10 y 50 piezas; tres puntos, se recopilaron más de 50 piezas de evidence.  NOTA: si el enlace se creó ese día, se mostrará en el mapa ese mismo día.
3	Haga clic en **Detener** para dejar de mostrarlo.

Administración de entidades: vista de posición

Para administrar entidades sujetas a inteligencia:	• En la sección **Intelligence**, haga doble clic en una operation y luego haga clic en **Mapa de posición**

Propósito

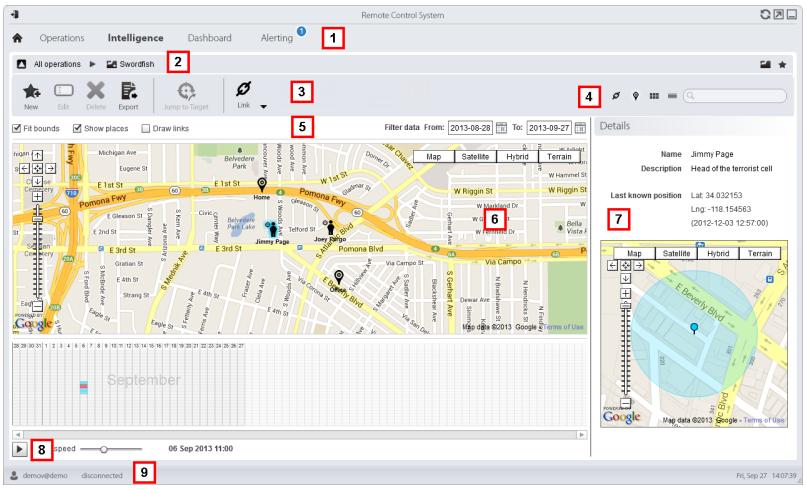
Esta función le permite:

- mostrar las entidades Target y Position para una operation y sus enlaces en un mapa.
- administrar las entidades Target y Position
- administrar los enlaces entre las entidades Target y Position
- abrir la página del target vinculada con la entidad Target
- abrir la evidence asociada con un enlace
- mostrar dinámicamente los movimientos entre entidades Target

NOTA: la función requiere una licencia de usuario y solo se activa si el usuario tiene autorización **Administración de entidades**.

Cómo se ve la función

Así es como se ve la página:



Área	*Descripción*
1	Menú de RCS.
2	Barra de navegación

Área	*Descripción*
3	Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento:

Ícono	*Función*
	Permite crear una nueva entidad
	Permite editar una entidad
	Elimina una entidad
	Exporta los datos de una entidad en formato `.html`
	Abre la página del target asociada con la entidad.*Consulte "**Página del target**" en la página 24* .
	Abre la evidence asociada con el enlace seleccionado. *Consulte "**Análisis de evidence (Evidence)**" en la página 37*
	 : crea un enlace  : permite editar un enlace  : elimina un enlace : aplica un nivel de importancia al enlace

Área	*Descripción*
4	Botones de vista y del cuadro de búsqueda:

Objeto	*Descripción*
	Cuadro de búsqueda. Al escribir parte del nombre o la descripción se mostrará una lista con las entidades que contienen esas letras.
	Muestra las entidades en una tabla. *Consulte "**Administración de entidades: vista de íconos y en tablas**" en la página 65* .
	Muestra entidades como íconos *Consulte "**Administración de entidades: vista de íconos y en tablas**" en la página 65* .
	Muestra las entidades Target y Position y sus enlaces en un mapa.
	Muestra las entidades y sus enlaces en un gráfico. *Consulte "**Administración de entidades: vista de enlaces**" en la página 67* .

5 Área de filtros

6 Mapa de entidades y enlaces basado en los filtros establecidos

NOTA: la entidad Target se coloca en la última posición obtenida en el período seleccionado.

NOTA: los enlaces creados manualmente siempre se muestran, independientemente del período que se seleccione.

7 Datos de una entidad seleccionada.

8 Comando para mostrar los movimientos de la entidad Target en base a los filtros establecidos.

9 Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz *Consulte "**Elementos y acciones comunes de la interfaz**" en la página 10* .

Para obtener más información sobre Intelligence *consulte "**Qué debería saber acerca de Intelligence**" en la página 55 consulte "**Qué debería saber acerca de las entidades**" en la página 55*

Ver los detalles de una entidad

Para ver los detalles de una entidad:

Paso	*Acción*
1	Haga doble clic en una entidad: se abrirá la página de detalles. • *"**Detalles de la entidad target**" en la página opuesta .* • *"**Detalles de la entidad Person**" en la página 82 .* • *"**Detalles de la entidad Position**" en la página 85 .*

Crear un enlace entre dos entidades

Para crear un enlace entre dos entidades:

Paso	*Acción*
1	Manteniendo presionada la tecla Ctrl en el teclado, seleccione una entidad Target y una entidad Position.
2	Seleccione el nivel de importancia y haga clic en **Guardar.** **Resultado**: el enlace se mostrará en el gráfico

Ver dinámicamente los movimientos de los targets

Para administrar la vista dinámica de los movimientos de los targets:

Paso	*Acción*
1	Asegúrese de que las entidades que se muestran en el gráfico y el período de tiempo seleccionado sean los que desee ver. Use los filtros para establecer sus preferencias.
2	Haga clic en **Reproducir** para mostrar. **Resultado**: las entidades Target que se muestran en el mapa se desplazan de acuerdo con los movimientos registrados en la evidence.  NOTA: si no hay ninguna evidence en la posición del target en el período seleccionado, la entidad Target permanece en la última posición obtenida pero su ícono se desvanece lentamente hasta que desaparece o aparece en la siguiente posición registrada.
3	Haga clic en **Detener** para dejar de mostrarlo.

Detalles de la entidad target

Para ver los detalles de una entidad:	• En la sección **Intelligence**, haga doble clic en una operation, y luego en una entidad **Target**

Propósito

Esta función le permite:

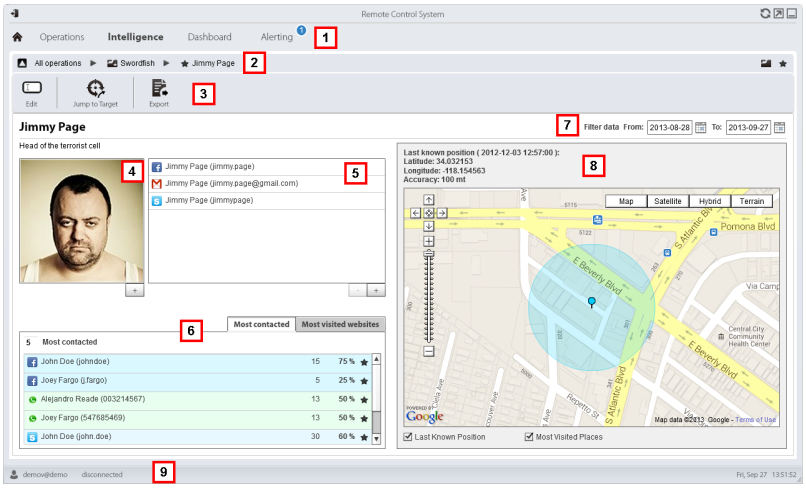
- ver información detallada de la entidad Target procesada por el sistema
- agregar información detallada sobre la entidad Target
- crear nuevas entidades asociadas con la entidad Target

NOTA: para activar algunos detalles y acciones se requiere una licencia de usuario.

NOTA: la función solo se activa si el usuario tiene autorización **Administración de entidades**.

Cómo se ve la función

Así es como se ve la página:



Área	*Descripción*
1	Menú de RCS.
2	Barra de navegación

Área	*Descripción*
3	Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento:

Ícono	*Función*
	Permite editar los datos de una entidad.
	Exporta los datos de una entidad en formato `.html`
	Abre la página del target asociada con la entidad.*Consulte "**Página del target**" en la página 24* .

4	Foto del target vinculado con la entidad. Es la primera imagen capturada por la cámara web de forma predeterminada.
5	Lista de datos de identificación de los targets identificados por medio de la evidence o agregados manualmente.
6	Tabla de las personas con las que más se contactó y de los sitios web que más visitó en el período seleccionado. Haga doble clic para abrir la página de evidence para ese dato.
7	Período de búsqueda.
8	Mapa que indica: • última posición del target • lugares más visitados en el período seleccionado • lugares que visitó el target ingresados manualmente
9	Barra de estado de RCS

Para obtener más información

Para ver las descripciones de los elementos de la interfaz *Consulte "**Elementos y acciones comunes de la interfaz**" en la página 10* .

Para obtener más información sobre Intelligence *consulte "**Qué debería saber acerca de Intelligence**" en la página 55 consulte "**Qué debería saber acerca de las entidades**" en la página 55*

Agregar la foto del target

Para agregar una foto:

Paso	*Acción*
1	• Haga clic en **+** y seleccione una foto o • en la página **Evidence**, abra los detalles de la evidence de tipo cámara web y seleccione una imagen **Resultado**: la imagen seleccionada se convierte en la imagen predeterminada.

Agregar los datos de identificación de un target

Para agregar los datos de identificación:

Paso	*Acción*
1	Haga clic en **+** e ingrese los datos. NOTA: el campo **Cuenta** es la identidad real del target (p. ej.: john.john@email.com); el campo **Nombre** es un nombre opcional que se asocia a los datos de identificación (p. ej.: John). **Resultado:** los datos de identificación se agregan a la lista.

Ver las personas con las que más se contacta

Para ver personas con las que más se contacta:

Paso	*Acción*
1	Seleccione el período deseado
2	En el cuadro de texto junto a **Más contactados,** ingrese la cantidad de personas que desea ver por tipo de medio de comunicación.
3	Presione **Entrar** en el teclado. **Resultado**: la información sobre las personas con las que más se contacta en el período seleccionado aparecerá en la tabla, *consulte "**Detalles de la entidad target**" en la página 81*

Ver los sitios web más visitados

Para ver los sitios web más visitados:

Paso	*Acción*
1	Seleccione el período deseado
2	En el cuadro de texto junto a **Sitios web más visitados,** ingrese la cantidad de sitios web que desea ver.
3	Presione **Entrar** en el teclado. **Resultado**: la información sobre los sitios web más visitados en el período seleccionado aparecerá en la tabla, *consulte "**Detalles de la entidad target**" en la página opuesta*

Relacionar la entidad Target con una persona con la que se contacta con frecuencia

Para relacionar la entidad Target con una persona con la que se contacta con frecuencia:

Paso	*Acción*
1	En la tabla **Más contactados**, haga clic en **Agregar como entidad** en la fila que desee. **Resultado** : una entidad Person con los datos de identificación seleccionados se agrega a la lista de entidades de operation junto con el enlace Peer con la entidad Target. NOTA: se obtendrá el mismo resultado si se crea una entidad Person manualmente con los datos de identificación de la tabla y se agrega un enlace Peer entre la entidad Person y la entidad creada.

Relacionar al target con un sitio web visitado con frecuencia

Para relacionar al target con un sitio web visitado con frecuencia:

Paso	*Acción*
1	En la tabla **Sitios web más visitados**, haga clic en **Agregar como entidad** en la fila que desee. **Resultado** : una entidad Virtual con la dirección URL seleccionada se agrega a la lista de entidades de operation junto con el enlace Peer con la entidad Target. NOTA: se obtendrá el mismo resultado si se crea una entidad Virtual manualmente con las direcciones URL de la tabla y se agrega un enlace Peer entre la entidad Person y la entidad creada.

Ver la última posición obtenida

Para ver la última posición del target en el mapa:

Paso	*Acción*
1	Marque el cuadro de verificación **Última posición conocida**. **Resultado:** una bandera azul indica la posición correspondiente.

Ver lugares visitados con frecuencia

Para ver los lugares visitados con frecuencia en el mapa:

Paso	*Acción*
1	Marque el cuadro de verificación **Sitios web más visitados**. **Resultado**: las posiciones más visitadas se muestran en el mapa con banderas rojas.

Agregar una entidad Position visitada por el target

Para agregar manualmente una entidad Position visitada por el target:

Paso	*Acción*
1	En el mapa, haga clic en **+** y escriba los datos.  Sugerencia: agregue un **Nombre** y una **Descripción** significativos que ayuden a identificar la relación entre el target y el lugar. **Resultado:** un enlace Peer entre una entidad Position y la entidad Target se agrega a la lista de entidades de la operation.  NOTA: se obtendrá el mismo resultado si se crea una entidad Position manualmente y se agrega un enlace Peer entre el target y la entidad creada.

Detalles de la entidad target

Tabla de personas más contactadas

A continuación hay una descripción de los datos que se indican en la tabla de personas más contactadas por el target:

Datos	*Descripción*
primera columna	ícono de la forma de comunicación y los datos de identificación de la persona.
segunda columna	cantidad de veces en que el target se contactó con la persona en el período seleccionado.
tercera columna	porcentaje de comunicaciones del target con la persona en el período seleccionado.  NOTA: los cálculos se basan en los medios de comunicación considerando los contactos que se muestran.
	botón para crear una entidad Person con los datos de identificación y para crear un enlace Peer con la entidad Target.

Tabla de sitios web más visitados

A continuación se muestra una descripción de los datos indicados en la tala de sitios web más visitados:

Datos	*Descripción*
primera columna	dirección URL de los sitios web visitados.
segunda columna	cantidad de visitas del target al sitio web en el período seleccionado.
tercera columna	porcentaje de visitas del target al sitio web en el período seleccionado.  NOTA: los cálculos se basan en los sitios web mostrados.
	botón para crear una entidad Virtual con esa dirección URL y para crear un enlace Peer con la entidad Target.

Detalles de la entidad Person

Para ver los detalles de una entidad:	• En la sección **Intelligence**, haga doble clic en una operation, y luego en una entidad **Persona**

Propósito

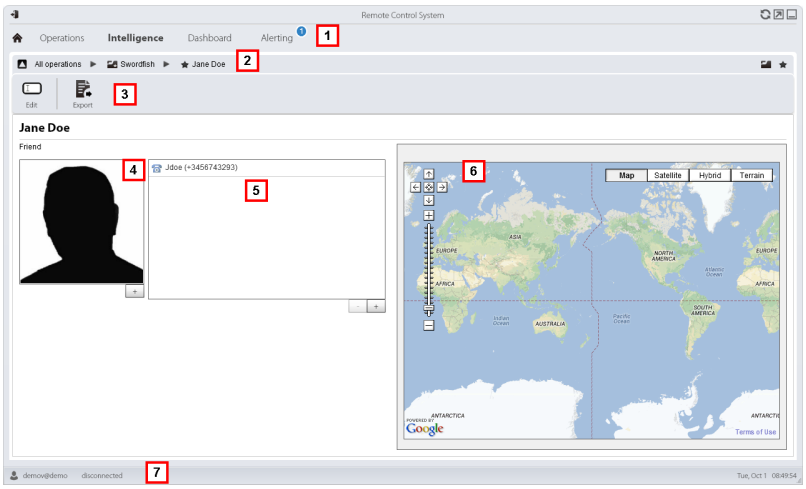
Esta función le permite:

- ver información detallada sobre la entidad Person
- agregar información detallada sobre la entidad Person
- crear entidades Position conectadas con la entidad Person

NOTA: la función requiere una licencia de usuario y solo se activa si el usuario tiene autorización **Administración de entidades**.

Cómo se ve la función

Así es como se ve la página:



Área	*Descripción*
1	Menú de RCS.
2	Barra de navegación
3	Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento:

Ícono	*Función*
	Permite editar los datos de una entidad.
	Exporta los datos de una entidad en formato `.html`

4	Foto de la persona asociada con la entidad.
5	Lista de los datos de identificación de la persona asociada con la entidad.

Área	*Descripción*
6	Mapa que indica las posiciones asociadas con la entidad.
7	Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz *Consulte "**Elementos y acciones comunes de la interfaz**" en la página 10* .

Para obtener más información sobre Intelligence *consulte "**Qué debería saber acerca de Intelligence**" en la página 55 consulte "**Qué debería saber acerca de las entidades**" en la página 55*

Agregar la foto de una persona

Para agregar una imagen:

Paso	*Acción*
1	Haga clic en **+** y seleccione una foto **Resultado**: la imagen seleccionada se convierte en la imagen predeterminada.

Agregar los datos de identificación de una persona

Para agregar los datos de identificación:

Paso	*Acción*
1	Haga clic en **+** e ingrese los datos.  NOTA: el campo **Cuenta** es la identidad real de la persona (p. ej.: john.john@email.com); el campo **Nombre** es un nombre opcional que se asocia a los datos de identificación (p. ej.: John). **Resultado:** los datos de identificación se agregan a la lista.

Agregar una entidad Position visitada por la entidad

Para agregar manualmente una entidad Position visitada por la entidad

Paso	*Acción*
1	En el mapa, haga clic en **+** y escriba los datos.  Sugerencia: agregue un **Nombre** y una **Descripción** significativos que ayuden a identificar la relación entre la persona y el lugar. **Resultado:** un enlace Peer entre una entidad Position y la entidad Person se agrega a la lista de entidades de la operation.  NOTA: se obtendrá el mismo resultado si se crea una entidad Position manualmente y se agrega un enlace Peer entre la entidad Person y la entidad creada.

Detalles de la entidad Position

Para ver los detalles de una entidad:	• En la sección **Intelligence**, haga doble clic en una operation, y luego en una entidad **Posición**

Propósito

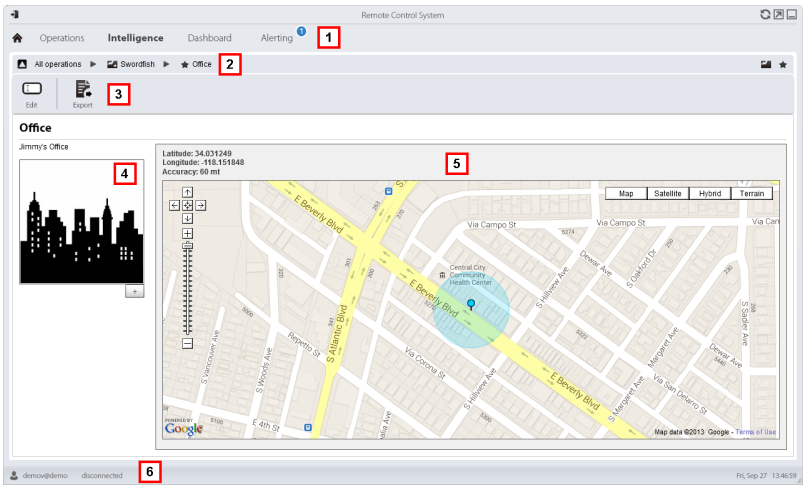
Esta función le permite:

- ver información detallada sobre la entidad Position
- agregar una foto del lugar vinculado con la entidad


NOTA: la función requiere una licencia de usuario y solo se activa si el usuario tiene autorización **Administración de entidades**.

Cómo se ve la función

Así es como se ve la página:



Área	*Descripción*
1	Menú de RCS.
2	Barra de navegación
3	Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento:

Ícono	*Función*
	Permite editar los datos de una entidad.
	Exporta los datos de una entidad en formato `.html`

4	Foto del lugar vinculado con la entidad.
5	Mapa del lugar vinculado con la entidad.
6	Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz *Consulte "**Elementos y acciones comunes de la interfaz**" en la página 10* .

Para obtener más información sobre Intelligence *consulte "**Qué debería saber acerca de Intelligence**" en la página 55* .

Agregar una imagen del sitio

Para agregar una imagen:

Paso	*Acción*
1	Haga clic en **+** y seleccione una imagen. **Resultado**: la imagen seleccionada se convierte en la imagen predeterminada.

Detalles de la entidad Virtual

Para ver los detalles de una entidad:	• En la sección **Intelligence**, haga doble clic en una operation, y luego en una entidad **Virtual**

Propósito

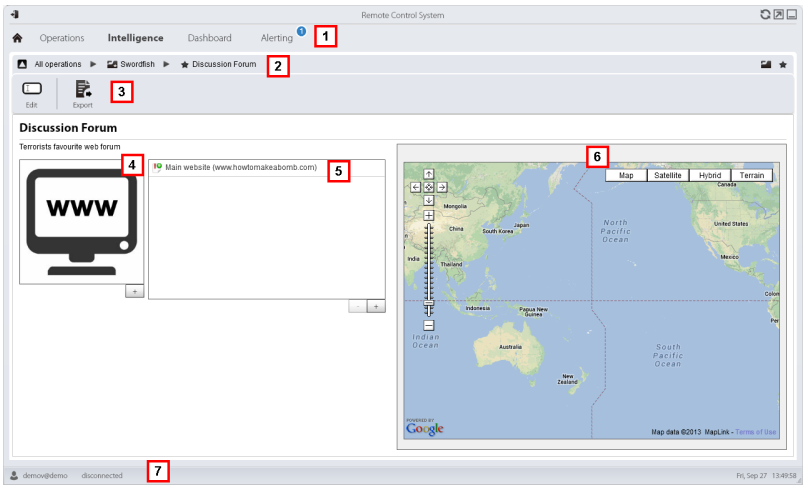
Esta función le permite:

- ver información detallada sobre la entidad virtual
- agregar información detallada sobre la entidad virtual

NOTA: la función requiere una licencia de usuario y solo se activa si el usuario tiene autorización **Administración de entidades**.

Cómo se ve la función

Así es como se ve la página:



Área	*Descripción*
1	Menú de RCS.
2	Barra de navegación

Área	*Descripción*
3	Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento:

Ícono	*Función*
	Permite editar los datos de una entidad.
	Exporta los datos de una entidad en formato `.html`

4	Imagen del contenido de la dirección asociada con la entidad.
5	Lista de direcciones web asociadas con la entidad.
6	Mapa donde se indica la posición de la dirección web identificada automáticamente por el sistema por medio de la dirección IP.
7	Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz *Consulte "**Elementos y acciones comunes de la interfaz**" en la página 10* .

Para obtener más información sobre Intelligence *consulte "**Qué debería saber acerca de Intelligence**" en la página 55 consulte "**Qué debería saber acerca de las entidades**" en la página 55*

Agregar una imagen de la dirección web

Para agregar imágenes:

Paso	*Acción*
1	Haga clic en **+** y seleccione una imagen. **Resultado**: la imagen seleccionada se convierte en la imagen predeterminada.

Agregar direcciones web a la entidad

Para agregar direcciones web a la entidad:

Paso	*Acción*
1	Haga clic en **+** e ingrese los datos. **Resultado:** la dirección se agrega a la lista.

7

Monitoreo de las actividades del target desde el Dashboard

Presentación

Introducción

El Dashboard le ayuda a monitorear las actividades de los agents conectados y el flujo de evidence entrante.

Contenido

En esta sección se incluyen los siguientes temas:

Qué debería saber acerca del Dashboard

Componentes del Dashboard

El Dashboard consta de uno o más elementos que el usuario elige entre:

- operation
- target
- agent

Cada elemento muestra la cantidad total de evidence recopilada. Los valores se actualizan en cada sincronización:

- **Número rojo**: cantidad de evidence recibida en la última sincronización.
- **Número negro**: cantidad de evidence recibida desde que inició sesión.

Ejemplo	*Descripción*
Evidence de la operation: 	Aparecerán los targets de la operation y la cantidad de evidence por target.
Evidence del target: 	Aparecerá la evidence del target y la cantidad de evidence por tipo.
Evidence de agent: 	Aparecerá la evidence del agent y la cantidad de evidence por tipo.

NOTA: si falta algún número es porque aún no ha llegado evidence desde que inició sesión.

Para ver la lista completa de los tipos de evidence *consulte "Lista de tipos de evidence" en la página 47* .

Proceso de alert de evidence

A continuación se describe el proceso de alert de evidence:

Fase	*Descripción*
1	El analista agrega los elementos operation, target o agent cuya evidence va a ser monitoreada en el Dashboard.
2	Si se recibe evidence, el sistema actualizará los contadores la próxima vez que los agents se sincronicen.
3	El analista revisa la evidence más reciente, aquella indicada con el número azul. Para ver los detalles, haga clic en el ícono correspondiente.
4	El sistema reinicia los números cuando el usuario cierra la sesión actual.

Monitoreo de evidence (Dashboard)

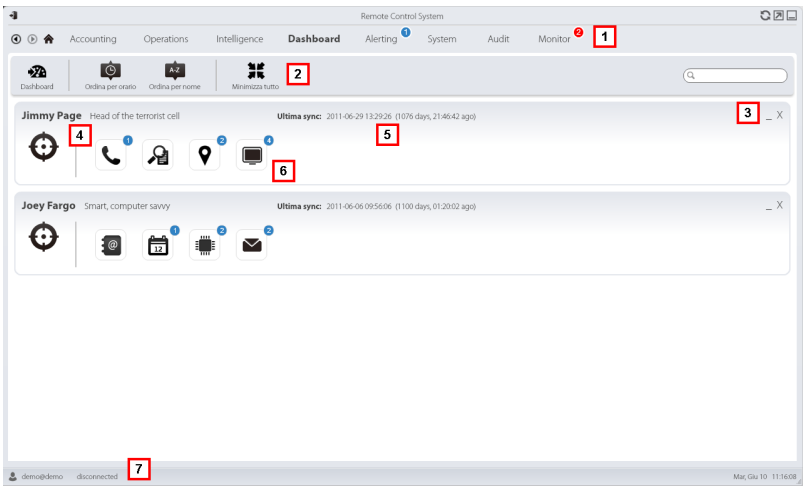
Para monitorear la evidence recibida:	• Sección **Dashboard**

Propósito

El Dashboard le permite monitorear ciertas operations, targets y agents así como ver la evidence entrante. Las opciones pueden personalizarse completamente. Por ejemplo, el Dashboard puede configurarse para monitorear únicamente algunos dispositivos del target.

Cómo se ve la función

Así es como se ve la página:



Área	*Descripción*
1	Menú de RCS.
2	Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento:

Ícono	*Descripción*
	Permite agregar un nuevo elemento a monitorear.
	Ordena elementos desde el que tiene la fecha de sincronización más reciente hasta el que tiene la fecha más antigua.
	Ordena elementos por nombre en orden alfabético.
	Contrae o expande todas las ventanas de elementos del Dashboard.

3	Teclas usadas para contraer o eliminar elementos en el Dashboard.
4	Nombre y descripción de los elementos del Dashboard.
5	Fecha de la última sincronización de elementos. **En curso**: sincronización en curso. **Inactiva**: sincronización detenida
6	Evidence obtenida recientemente en una operation, target o agent.
7	Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz *Consulte "**Elementos y acciones comunes de la interfaz**" en la página 10* .

Para obtener más información acerca del Dashboard, *consulte "**Qué debería saber acerca del Dashboard**" en la página 90* .

Agregar un elemento al Dashboard

Para agregar un nuevo elemento al Dashboard:

Paso	*Acción*
1	Haga clic en **Dashboard**: se abrirá una ventana que permite buscar los elementos que desea agregar.
2	Escriba parte del nombre o la descripción del elemento que desea agregar: aparecerá una lista con los elementos que coinciden con la búsqueda.
3	• Seleccione el elemento de la lista: el elemento se agregará automáticamente al Dashboard y la ventana de búsqueda quedará abierta para realizar una nueva búsqueda. • Repita los pasos 2 y 3 hasta que haya agregado todos los elementos deseados.
5	Después de agregar los elementos, haga clic en ✖ o **Listo** para cerrar la ventana de búsqueda y regresar al Dashboard.

Ver la evidence indicada en el Dashboard

Para ver la evidence en el Dashboard

NOTA: haga clic en un target u operation para abrir el área de trabajo del objeto seleccionado donde el analista pueda ver los agents que desee.

Paso	*Acción*
1	Para el elemento operation: • haga doble clic en el target para abrir la página del target. *Consulte "**Página del target**" en la página 24 .* Para el elemento target: • haga doble clic en el agent: se abrirá la página del agent. *Consulte "**Página del agent**" en la página 29 .* Para el elemento agent: • haga doble clic en el tipo de evidence: aparecerá la página de evidence. *Consulte "**Análisis de evidence (Evidence)**" en la página 37*

8

Alert

Presentación

Introducción

Los alerts se activan con la recepción de evidence, la sincronización de agents, la creación automática de entidades o la conexión ente entidades. Además, le permite etiquetar evidence automáticamente y vincularla para análisis y exportación.

Contenido

En esta sección se incluyen los siguientes temas:

Qué debería saber acerca de alerts

Qué son los alerts

Durante la fase de investigación, puede ser útil recibir alertas en tiempo real sobre eventos especiales que se relacionan con el target, ya sea por correo electrónico o por medio de notificaciones en RCS Console.

Es posible recibir alerts cuando:

- llega nueva evidence
- el agent se sincroniza
- se crean entidades automáticamente y se conectan entre sí (Intelligence)

Por ejemplo, si hace tiempo que se espera la llegada de evidence de un target, se puede crear una regla de alert para que se envíe un correo electrónico y se actualice un registro cada vez que se reciba información. De esta forma, los usuarios reciben una notificación inmediata cuando el target reanuda las actividades. Más adelante se puede desactivar la regla y consultar la evidence a medida que va llegando.

O, si se usa Intelligence, puede ser útil recibir una alerta cuando se crea un enlace a una entidad determinada o se crea una nueva entidad en la operation.

Reglas de alert

En las reglas de alert se establece qué eventos generan alerts. Se pueden utilizar para asignar niveles de importancia a la evidence o a las relaciones de Intelligence de forma automática, que son útiles en la fase de análisis.

Ámbito de aplicación de las reglas de alert

Las reglas para notificar cuando llega evidence se pueden crear en los siguientes niveles:

- **Operation**: toda la evidence de todos los targets de la operation
- **Target**: toda la evidence de todos los agents del target
- **Agent**: toda la evidence del agent

Las reglas para notificar la creación automática de una entidad Intelligence se pueden crear en los siguientes niveles:

- **Operation**: notifica cuando se crea una entidad en esa operation

Las reglas para notificar la creación automática de un enlace de Intelligence se pueden crear en los siguientes niveles:

- **Operation**: notifica cuando se crea un enlace para cualquier entidad de la operation
- **Entidad**: notifica cuando se crea un enlace para esa entidad

NOTA: cada usuario recibirá alertas según las reglas establecidas.

Proceso de alert

A continuación se describe el proceso de alert:

NOTA: el envío de un correo electrónico es opcional.

Fase	*Descripción*
1	El analista crea reglas para recibir alertas ante la llegada de cierta evidence, la sincronización de agents o la creación automática de entidades o enlaces de Intelligence. Las reglas registran los alerts, los notifican a RCS Console y los envían por correo electrónico (opcional).
2	El sistema intercepta la evidence entrante o analiza el elemento que se está creando y lo compara con las reglas de alert.

Si la evidence...	*Entonces...*
corresponde a una regla de alert	El sistema guarda la prueba como *evidence* o agrega la entidad o enlace a la operation, generando un alert que aplica automáticamente el nivel de importancia seleccionado. Opcionalmente, el sistema puede enviar una notificación por correo electrónico.
no corresponde a una regla de alert	El sistema guarda la prueba como *evidence* o agrega lo entidad o enlace a la operation sin generar ningun alert.

3	El analista recibe un correo electrónico de alert (si se establece en la regla de alert) y revisa el registro de alert. Desde un alert, abre directamente la evidence que la generó o la entidad creada o la vista de enlaces.
4	Después de revisarlo, el analista elimina los registros de alert.

Alerting

Para recibir alert del target:	• Sección **Alerting**

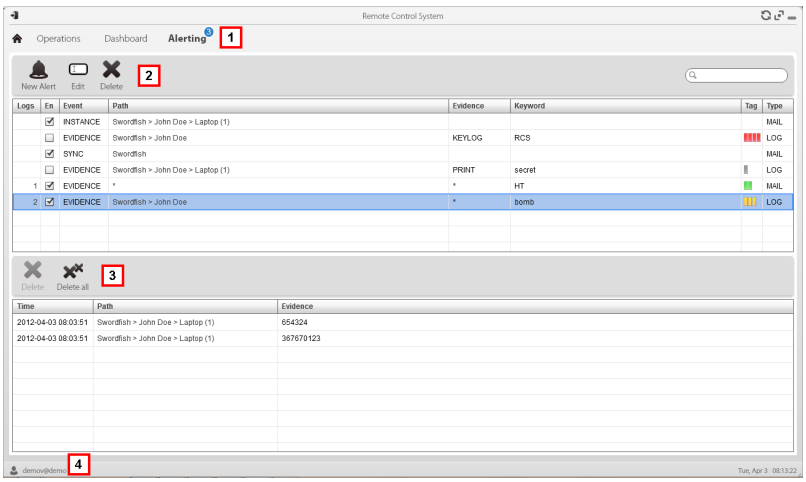
Propósito

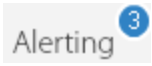
Esta función le permite:

- recibir alert cuando se intercepta cierto tipo de evidence, cuando el dispositivo del target se sincroniza con RCS o cuando Intelligence crea automáticamente entidades o enlaces entre entidades.
- etiquetar automáticamente la evidence o los enlaces de Intelligence por nivel de importancia, para facilitar el análisis posterior.
- monitorear todos los alerts registrados y abrir la evidence que los generó directamente.

Cómo se ve la función

Así es como se ve la página:



Área	*Descripción*
1	Menú de RCS.  : indica la cantidad de alerts recibidas. El contador se reinicia automáticamente después de dos semanas o cuando se eliminan las notificaciones.
2	Barra de herramientas de la regla de alert. A continuación se muestra la descripción de cada elemento:

Ícono	*Descripción*
	Permite crear una nueva regla de alert.  NOTA: la función solo se activa si el usuario tiene autorización **Creación de alerts**.
	Permite editar la regla de alert seleccionada.
	Elimina la regla de alert seleccionada.  ***PRECAUCIÓN: se eliminarán todas las notificaciones generadas.***

3	Barra de herramientas del registro de alert. A continuación se muestra la descripción de cada elemento:

Ícono	*Descripción*
	Elimina el registro de alerts seleccionado.
	Elimina todos los registros de alerts.

4	Menú de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz *Consulte "**Elementos y acciones comunes de la interfaz**" en la página 10* .

Para ver una descripción de los datos en esta ventana *consulte "**Datos de alert**" en la página 100* .

Para obtener más información sobre alerts*consulte "**Qué debería saber acerca de alerts**" en la página 95* .

Agregar una regla para recibir alertas

Para recibir alertas se debe establecer una regla:

Paso	*Acción*
1	Haga clic en **Nuevo alert**: aparecerán los campos para ingresar datos.
2	• Ingrese los datos solicitados. Indique el método de alert en **Tipo**. • Seleccione el cuadro de verificación **Activado** para aplicar la regla.
3	Haga clic en **Guardar**: aparecerá la nueva regla de alert en el área de trabajo principal. Cuando el sistema registra un evento que coincide con la regla se envía un alert.

Editar de una regla de alert

Para editar una regla de alert

Paso	*Acción*
1	Seleccione la regla de alert que desea editar Haga clic en **Editar**: aparecerán los datos a editar.
2	• Edite los datos. • Seleccione el cuadro de verificación **Activado** para aplicar la regla inmediatamente.
3	Haga clic en **Guardar**: aparecerá la nueva regla de alert en el área de trabajo principal. Cuando el sistema registra un evento que coincide con la regla se envía un alert.

Agregar una regla para etiquetar automáticamente cierta evidence o ciertos enlaces de Intelligence entre entidades

Para etiquetar automáticamente cierta evidence o enlaces sin registrar o enviar alerts:

Paso	*Acción*
1	Haga clic en **Nuevo alert**: aparecerán los campos para ingresar datos.
2	• Establezca los criterios para seleccionar la evidence o los enlaces • En **Tipo**, seleccione **Ninguno.** • En **Importancia**, establezca el nivel de importancia • Seleccione el cuadro de verificación **Activado** para aplicar la regla.
3	Haga clic en **Guardar**: aparecerá la nueva regla de alert en el área de trabajo principal. Cuando el sistema reciba evidence que coincida con esta regla, se etiquetará la evidence.

Ver de eventos que coinciden con el alert registrado

Para ver la evidence que coincide con un alert:

Paso	*Acción*
1	Seleccione la regla de alert que tenga cuando menos un registro (columna **Registros**): todos los alerts registrados aparecen en la lista.
2	Haga doble clic en la fila correspondiente en la lista de alerts registrados. **Resultado**: se abre directamente: • la lista de evidence que generó el alert (Evento **Evidence**). • los detalles de la entidad (evento **Entity**) • la vista de enlaces (evento **Link**)

Datos de alert

Datos de la regla de alert

A continuación se muestran los datos de la regla de alert:

Datos	*Descripción*
Registros	(solo en una tabla) Cantidad de notificaciones recibidas que coinciden con la regla.
Activado	Activa o desactiva la regla de alert.
Evento	Tipo de evento que activa el alert: • **Evidence**: activa la regla cuando llega evidence que cumple con los criterios descritos más abajo. • **Sync**: activa la regla cuando el agent indicado abajo ejecuta una sincronización. • **Instance**: activa la regla cuando el agent creado (de la instancia) por la factory que se indica más abajo ejecuta la primera sincronización. • **Entity**: activa la regla cuando el sistema crea una nueva entidad Intelligence en la operation indicada. • **Link**: activa la regla cuando el sistema crea automáticamente un nuevo enlace entre las entidades Intelligence en una operation o con la entidad indicada.
Ruta de acceso	operation, target, entidad, agent y factory a monitorear. Indica el campo de aplicación de la regla. Por ejemplo, para el evento **Evidence**, si se selecciona una operation, se monitorea toda la evidence de la operation. Si se selecciona un agent, se monitorea la evidence de ese agent.

Datos	*Descripción*
Evidence	(solo los eventos de tipo **Evidence**) Tipo de evidence que genera alerts.  Sugerencia: '*****' indica todos los tipos de evidence. Para ver una descripción de todos los tipos *consulte "**Lista de tipos de evidence**" en la página 47*
Llave	(solo los eventos del tipo **Evidence**) Palabras clave que la evidence debe contener para activar el alert. Por ejemplo, la palabra clave "contraseña" crea un alert cuando la evidence (archivo de audio, documento) contiene la palabra "contraseña".
Relevancia	(solo los eventos de tipo **Evidence** o **Link**) Etiqueta automáticamente la evidence o el enlace con diferentes niveles de importancia para facilitar el análisis: **Ícono** **Descripción** Importancia máxima.  Importancia intermedia.  Importancia normal.  Importancia mínima. - Sin importancia.
Tipo	Tipo de alert que se recibirá cuando llegue la evidence: • **Log**: alert registrado y notificado en RCS Console. • **Mail**: correo electrónico y alert registrado • **None**: alert no registrado ni enviado por correo electrónico. Útil para etiquetar la evidence o los enlaces automáticamente por nivel de importancia (**Relevance**)
Tipo de supresión	(solo los alerts de tipo **Mail**) Tiempo de latencia para enviar correos electrónicos de alert idénticos. Se usa para evitar los correos electrónicos idénticos después de recibir el primero. Por ejemplo, si el target no comunicó su evidence por un tiempo y se seleccionó el alert por correo electrónico, es posible que sea "bombardeado" con correos electrónicos cuando llegue la primera evidence. Cuando **Suppression time** tiene el valor 30 minutos, se recibirá un correo electrónico cada 30 minutos.  NOTA: esta opción solo limita el envío de correos electrónicos. Los eventos siempre se registran.

Datos del registro

A continuación se describen los registros de alert:

Datos	*Descripción*
Fecha	Fecha y hora del alert.
Ruta de acceso	Rango de acción desde el cual se generó el alert. Por ejemplo, si se selecciona un target en la regla **Ruta**, aquí aparecerán el nombre del target y el nombre de la operation a la que pertenece.
Info	Cantidad y tipo de eventos que generaron el alert.

]HackingTeam[

HT S.r.l.
via della Moscova, 13
20121 Milan (MI)
Italia
tel.: + 39 02 29 060 603
fax:+ 39 02 63 118 946
www.hackingteam.com
e-mail:info@hackingteam.com

RCS 9.5 Manual del analista
Manual del analista 1.8 NOV-2014

info@hackingteam.com