]HackingTeam[

RCS 9

The hacking suite for governmental interception

Manuale dell'analista

Proprietà delle informazioni

NOTA: richieste di ulteriori copie di questo manuale o di informazioni tecniche sul prodotto, devono essere indirizzate a:

HT S.r.l.

via della Moscova, 13

20121 Milano (MI)

Italy

Tel.: + 39 02 29 060 603

Fax: + 39 02 63 118 946

e-mail: info@hackingteam.com

Sommario

Glossario dei termini

Di seguito i termini utilizzati in questo manuale e loro definizione.

A

Accounting
Sezione della console dedicata alla gestione degli accessi a RCS.

Agent elite
Agente installato su dispositivi sicuri. Permette di raccogliere tutti i tipi di evidence disponibili.

Agent scout
Sostituto dell'agent inviato sul dispositivo per verificarne il livello di sicurezza prima di installare gli agent veri e propri (elite o soldier).

Agent soldier
Agente installato su dispositivi non completamente sicuri. Permette di raccogliere solo alcuni tipi di evidence.

Agente
Sonde software installate sui dispositivi sotto monitoraggio. Progettate per raccogliere prove e comunicarle al Collector.

Alerting
Sezione della console dedicata alle segnalazioni di nuove prove.

Amministratore
Colui che abilita l'accesso al sistema agli utenti, crea i gruppi di lavoro e definisce le indagini in essere, gli obiettivi e il tipo di dati da raccogliere.

Amministratore di sistema
Colui che installa i server e le console, si occupa degli aggiornamenti software e del ripristino dei dati in caso di malfunzionamento.

Analista
Persona incaricata dell'analisi dei dati raccolti durante le indagini.

Anonymizer
(opzionale) Protegge il server da attacchi esterni e consente l'anonimato durante le operazioni di indagine. Trasferisce i dati degli agent ai Collector.

Audit
Sezione della console che riporta tutte le azioni degli utenti e del sistema. Utilizzata per controllare abusi di RCS.

avvisi da evidence
Avvisi, normalmente email, inviati agli analisti per avvisarli che una nuova evidence corrisponde alle regole impostate.

B

back end
Ambiente destinato alla decodifica e salvataggio delle informazioni raccolte. In architettura distribuita include il Master Node e i database Shard.

BRAS
(Broadband Remote Access Server) instrada il traffico da/a DSLAM verso la rete dell'ISP e fornisce l'autenticazione per gli iscritti dell'ISP.

BSSID
(Basic Service Set IDentifier) Identificativo dell'Access Point e dei suoi client.

C

Carrier
Servizio del Collector: invia i dati ricevuti dagli Anonymizer agli shard o al Master Node.

Collector
Servizio del Collector: riceve i dati inviati dagli agent, tramite la catena di Anonymizer.

console
Computer su cui è installato RCS Console. Accede direttamente a RCS Server o al Master Node.

D

Dashboard
Sezione della console dedicata all'Analista. Usata per avere una rapida panoramica dello stato delle investigazioni, dei target e degli agent più importanti.

DSLAM
(Digital Subscriber Line Access Multiplexer) apparato di rete, spesso collocato negli scambi telefonici dell'operatore telefonico. Connette più interfacce DSL a un canale di comunicazione digitale ad alta velocità usando le tecniche di multiplexing.

E

entità
Insieme di informazioni di intelligence associate al target e a persone e luoghi coinvolti nell'indagine.

ESSID
(Extended Service Set IDentifier) Conosciuto anche come SSID, identifica la rete WiFi.

evidence
Dati delle prove raccolti. Il formato dipende dal tipo di evidence (es.: immagine).

Exploit
Codice che, sfruttando un bug o una vulnerabilità, porta all'esecuzione di codice non previsto. Utilizzato per infettare i dispositivi dei target.

F

factory
Un modello per la configurazione e la compilazione di agent.

front end
Ambiente destinato a comunicare con gli agent per raccogliere informazioni e impostare la loro configurazione. In architettura distribuita include il Collector e il Network Controller.

G

Gruppo
Entità di intelligence che raggruppa più entità.

gruppo di alerting
Raggruppa gli utenti che devono ricevere notifiche via mail ogni volta che si genera un allarme di sistema (per esempio, il database ha superato il limite di spazio libero disponibile). Normalmente, questo gruppo è associato a nessuna operation.

M

Monitor
Sezione della console dedicata alle segnalazioni degli stati dei componenti e delle licenze.

N

Network Controller
Servizio del Collector: controlla lo stato dei Network Injector e degli Anonymizer, spedendo loro le nuove configurazioni o aggiornamenti software.

Network Injector
Componente hardware che controlla il traffico di rete del target e inietta un agent nelle risorse Web selezionate. Fornito in due versioni, Appliance o Tactical: Appliance è per installazioni presso ISP, mentre Tactical è utilizzato sul campo.

Network Injector Appliance
Versione rack di Network Injector, per l'installazione presso l'ISP. Cfr.: Tactical Network Injector.

O

operation
Investigazione verso uno o più target, i cui dispositivi saranno i destinatari degli agent.

P

Person
Entità di intelligence che rappresenta una persona coinvolta in un'indagine.

Position
Entità di intelligence che rappresenta un luogo coinvolto in un'indagine.

R

RCS
(Remote Control System) il prodotto oggetto di questo manuale.

RCS Console
Software dedicato all'interazione con RCS Server.

RCS Server
Una o più macchine, in base all'architettura di installazione, dove sono installati i componenti alla base di RCS: i database Shard, i Network Controller e Collector.

regole di alert
Regole che creano alert quando una nuova evidence viene salvata o quando l'agent sincronizza per la prima volta.

regole di injection
Impostazioni che definiscono come identificare traffico HTTP, quale risorsa da infettare e quale metodo usare per l'infezione.

S

sequenze di acquisizione
Insieme di eventi, azioni e moduli di acquisizione complessi che costituiscono la configurazione avanzata di un agent.

SSH
(Secure SHell) protocollo di rete per sessioni remote cifrate, servizi remoti o esecuzioni comandi.

System
Sezione della console dedicata alla gestione del sistema.

T

Tactical Network Injector
Versione portatile di Network Injector, per utilizzo tattico. Cfr.: Network Injector Appliance.

TAP
(Test Access Port) dispositivo hardware inserito in reti informatiche che permette il monitoraggio passivo del flusso dati in transito.

target
La persona fisica sotto investigazione. Nella sezione intelligence è rappresentata dall'entità Target.

Tecnico
Colui che su mandato dell'Amministratore crea e gestisce gli agent.

V

Virtual
Entità di intelligence che rappresenta un luogo virtuale (es. un sito web) coinvolto in un'indagine.

VPS
(Virtual Private Server) server remoto su cui installare l'Anonymizer. Normalmente disponibile a noleggio.

W

WPA
(WiFi Protected Access) Protezione per le reti WiFi.

WPA 2
(WiFi Protected Access) Protezione per le reti WiFi.

1

Introduzione a questa Guida

Presentazione

Obiettivi del manuale

Questo manuale guida l'*Analista* a utilizzare RCS Console per:

- tenere sotto controllo il target
- esplorare i dispositivi del target
- analizzare le evidence ed esportarle

Di seguito sono presentate le informazioni necessarie alla consultazione del manuale.

Contenuti

Questa sezione include i seguenti argomenti:

Novità della guida

Elenco note di rilascio e aggiornamenti di questa guida in linea.

Data rilascio	*Codice*	*Versione software*	*Descrizione*
19 Febbraio 2014	Manuale dell'analista 1.5 FEB-2014	9.2	Aggiunta gestione gruppi e nuovi filtri in Intelligence, *vedi "**Intelligence**" a pagina 55* . Aggiunta possibilità di trasformare una entità Person in una entità Target, *vedi "**Cose da sapere sulle entità**" a pagina 56* . Aggiunta evidence di tipo **Money**, *vedi "**Elenco dei tipi di evidence**" a pagina 49* . Aggiunta nuovo tipo di export di evidence verso un connector, *vedi "**Dati di esportazione delle evidence**" a pagina 48*
30 Settembre 2013	Manuale dell'analista 1.4 SET - 2013	9	Aggiornata documentazione della sezione Intelligence, *vedi "**Intelligence**" a pagina 55* . Aggiornate le procedure per l'analista, *vedi "**Procedure dell'Analista**" a pagina 16* . Aggiornata documentazione delle regole di alert, *vedi "**Alert**" a pagina 95* . Aggiornata documentazione per migliorie apportate all'interfaccia utenti. Migliorato sommario.
8 Luglio 2013	Manuale dell'analista -	8.4	Nessun aggiornamento alla documentazione.
15 Marzo 2013	Manuale dell'analista 1.3 MAR-2013	8.3	Aggiunta la sezione Intelligence *vedi "**Intelligence**" a pagina 55* . Aggiunta estrazione dei contenuti da tutti i formati di evidence tipo file. *Vedi "**Dettaglio di una evidence**" a pagina 45* Su licenza d'uso è possibile vedere i contenuti di una evidence nella propria lingua. *Vedi "**Analisi delle evidence (Evidence)**" a pagina 38* e *vedi "**Dettaglio di una evidence**" a pagina 45* .

Data rilascio	*Codice*	*Versione software*	*Descrizione*
15 Ottobre 2012	Manuale dell'analista 1.2 OTT-2012	8.2	Aggiunto salvataggio impostazione dei filtri su evidence e semplificata applicazione filtro **Info** sulle evidence. Aggiunta eliminazione evidence.*Vedi "**Analisi delle evidence (Evidence)**" a pagina 38 .* Se installato, possibilità di vedere i testi estratti da una evidence tipo screenshot. *Vedi "**Dettaglio di una evidence**" a pagina 45 .*
30 Giugno 2012	Manuale dell'analista 1.1 GIU 2012	8.1	Diverso recupero delle cartelle dal disco. *Vedi "**Recupero evidence da dispositivi (File System)** " a pagina 52 .*
16 Aprile 2012	Manuale dell'analista 1.0 APR-2012	8.0	Prima pubblicazione

Documentazione fornita

A corredo del software RCS sono forniti i seguenti manuali:

Manuale	*Destinatari*	*Codice*	*Formato di distribuzione*
Manuale dell'amministratore di sistema	Amministratore di sistema	*Manuale dell'amministratore di sistema 1.5 FEB-2014*	PDF
Manuale dell'amministratore	Amministratori	*Manuale dell'amministratore 1.5 FEB-2014*	PDF
Manuale del tecnico	Tecnici	*Manuale del tecnico 1.6 FEB-2014*	PDF
Manuale dell'analista (questo manuale)	Analisti	*Manuale dell'analista 1.5 FEB-2014*	PDF

Convenzioni tipografiche per le segnalazioni

Di seguito le segnalazioni previste in questo documento (Microsoft Manual of Style):

AVVERTENZA: indica una situazione rischiosa che se non evitata, può causare danni fisici all'utente o alle attrezzature.

PRUDENZA: indica una situazione rischiosa che se non evitata, può causare la perdita di dati.

IMPORTANTE: offre indicazioni essenziali al completamento del compito. Mentre le note possono essere trascurate e non inficiano il completamento del compito, le indicazioni importanti non devono essere trascurate.

NOTA: informazioni neutre e positive che enfatizzano o aggiungono informazioni a dei punti nel testo principale. Fornisce informazioni che possono essere applicate solo in casi speciali.

Suggerimento: consiglia l'utente nell'applicare le tecniche e le procedure descritte nel testo ai loro bisogni specifici. Può suggerire un metodo alternativo e non è fondamentale alla comprensione del testo.

Richiede assistenza: l'operazione può essere portata a termine solo su indicazioni dell'assistenza tecnica.

Convenzioni tipografiche per la formattazione

Di seguito la legenda di alcune convenzioni tipografiche:

Esempio	***Stile***	***Descrizione***
*Vedi "**Dati degli utenti**"*	*corsivo*	indica il titolo di un capitolo, una sezione, una sottosezione, un paragrafo, una tabella o una figura di questo manuale, o di un'altra pubblicazione di riferimento.
<ggmmaaaa>	<aaa>	indica un testo che dovrà essere specificato dall'utente secondo una certa sintassi. Nell'esempio <ggmmaaaa> è una data e può diventare "14072011".
Selezionare uno dei server elencati **[2]**.	**[x]**	indica l'oggetto citato nel testo e che compare nell'immagine adiacente.

Esempio	*Stile*	*Descrizione*
Fare clic su **Add**. Selezionare il menu **File, Save data.**	**grassetto**	indica una scritta sull'interfaccia operatore, sia di un elemento grafico (es.: tabella, scheda) sia di un pulsante a video.
Premere ENTER	MAIUSCOLO	indica il nome di tasti della tastiera.
Cfr.: Network Injector Appliance	-	suggerisce di confrontare la definizione di un termine in glossario o contenuto con altro termine o contenuto.

Destinatari del prodotto e di questa guida

Di seguito le figure professionali che interagiscono con RCS.

Destinatario	*Attività*	*Competenze*
Amministratore di sistema	Segue le indicazioni dell'assistenza HackingTeam fornite in fase contrattuale. Installa e aggiorna i server RCS, i Network Injector e le RCS Console. Programma e gestisce i backup. Ripristina i backup in caso di sostituzione dei server.  AVVERTENZA: l'amministratore di sistema deve avere tutte le competenze necessarie richieste. HackingTeam non si assume alcuna responsabilità di malfunzionamenti o danni alle attrezzature arrecati da una installazione non professionale.	*Tecnico di reti esperto*
Amministratore	Crea gli account e i gruppi autorizzati. Crea operation e target. Controlla lo stato del sistema e delle licenze.	*Responsabile dell'indagine*
Tecnico	Crea gli agent e li configura. Configura le regole di un Network Injector.	*Tecnico specializzato in intercettazioni*
Analista	Analizza le evidence e le esporta.	*Operativo*

Dati di identificazione dell'autore del software

HT S.r.l.
via della Moscova, 13
20121 Milano (MI)
Italy
Tel.: + 39 02 29 060 603

Fax: + 39 02 63 118 946
e-mail: info@hackingteam.com

2

RCS (Remote Control System)

Presentazione

Introduzione

RCS (Remote Control System) è una soluzione a supporto delle investigazioni che intercetta attivamente e passivamente dati e informazioni dai dispositivi dei bersagli di tali investigazioni. RCS infatti crea, configura e installa nell'assoluto anonimato degli agenti software che raccolgono dati e informazioni e inviano i risultati al database centrale per la decodifica e il salvataggio.

Contenuti

Questa sezione include i seguenti argomenti:

Differenze tra la versione RCS 8.0 e RCS 7.6

Di seguito le differenze rispetto alla versione RCS 7.6.

Glossario dei termini

RCS v. 7.6	*RCS 8.0 e successive*
Attività	Operation
Agente	Module
Anonymizer chain	Anonymizing chain
Backdoor	Agente
Backdoor Class	Factory
Collection Node (ASP)	Collector
Injection Proxy Appliance (IPA)	Network Injector Appliance
Log Repository (RCSDB)	Master Node e Shard aggiuntivi
Mobile Collection Node (RSSM)	Collector
RCSAnon	Anonymizer

3

RCS Console per l'Analista

Presentazione

Ruolo dell'Analista

Il ruolo dell'Analista è:

- selezionare e analizzare le evidence
- recuperare le prove di un dispositivo
- esportare evidence per l'autorità competente
- organizzare le prove dei dispositivi e le altre in suo possesso per formulare soluzioni per l'indagine

Funzioni abilitate per l'Analista

Per completare le attività che gli competono, l'Analista ha accesso alle seguenti funzioni:

- **Operation**
- **Intelligence**
- **Dashboard**
- **Alerting**

Contenuti

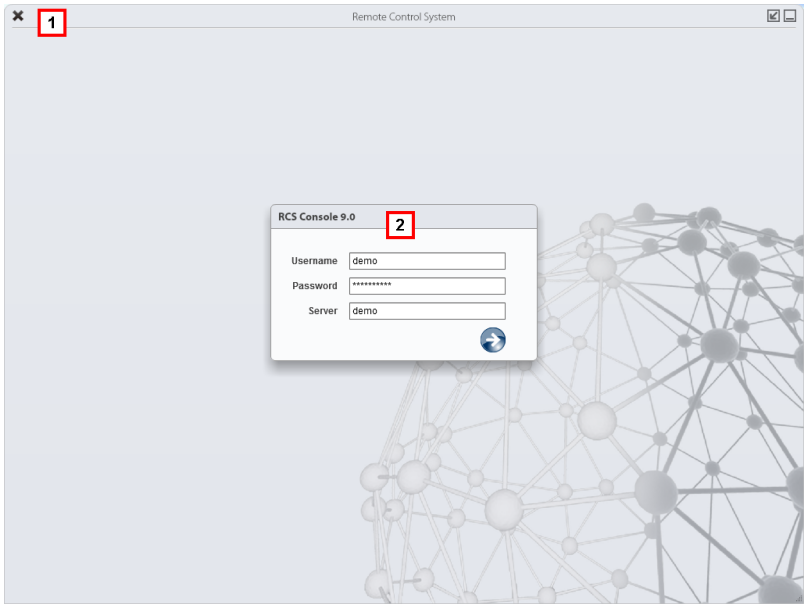
Questa sezione include i seguenti argomenti:

Avvio di RCS Console

All'avvio, RCS Console chiede di inserire le proprie credenziali precedentemente impostate dall'Amministratore.

Come si presenta la pagina di login

Ecco come viene visualizzata la pagina di login:



Area	*Descrizione*
1	Barra del titolo con pulsanti di comando: Chiusura di RCS Console. Pulsante di ingrandimento della finestra. Pulsante di riduzione a icona della finestra.
2	Finestra di dialogo per inserimento delle proprie credenziali.

Accedere a RCS Console

Per accedere alle funzioni di RCS Console:

Passo	*Azione*
1	In **Username** e **Password** inserire le credenziali come assegnate dall'Amministratore.

Passo	*Azione*
2	In **Server** inserire il nome della macchina o l'indirizzo del server cui ci si vuole collegare.
3	Fare clic su  : si presenta l'homepage con i menu abilitati in base ai privilegi del proprio account. *Vedi "**Descrizione della homepage**" nel seguito .*

Descrizione della homepage

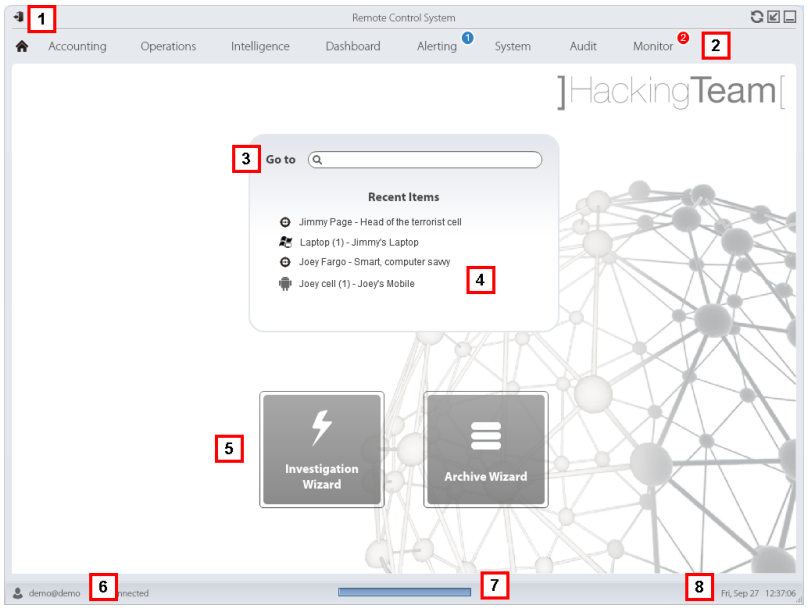
Per visualizzare l'homepage:	• fare clic su 

Introduzione

RCS Console presenta all'avvio questa homepage, unica per tutti gli utenti. I menu abilitati dipendono dai ruoli assegnati al proprio account.

Come si presenta

Ecco come viene visualizzata l'homepage con già presente una cronologia degli argomenti recenti. Per il dettaglio degli elementi e le azioni comuni:



Area	*Descrizione*
1	Barra del titolo con pulsanti di comando.

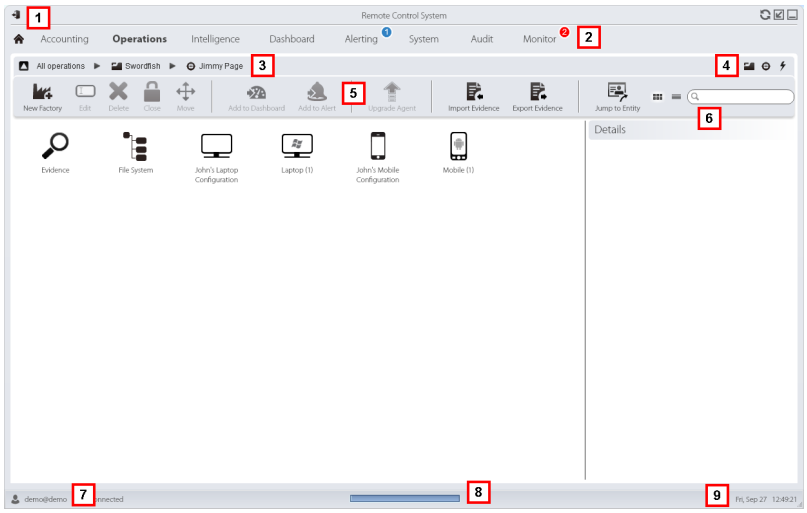
Area	*Descrizione*
2	Menu di RCS con le funzioni abilitate per l'utente
3	Casella di ricerca per cercare tra i nomi di operation, target, agent e entità, per nome o descrizione.
4	Collegamenti agli ultimi cinque elementi aperti (operation della sezione Operations, operation della sezione Intelligence, target,agent e entità).
5	Pulsanti per avvio dei Wizard.
6	Utente connesso con possibilità di cambiare la lingua e la password.
7	Area download con possibilità durante un'esportazione o una compilazione di vedere lo stato di avanzamento.
8	Data e ora attuale con possibilità di cambio fuso orario.

Elementi e azioni comuni dell'interfaccia

Ogni pagina del programma utilizza elementi comuni e permette azioni simili tra loro.
Per facilitare la consultazione di questo manuale, sono stati descritti in questo capitolo elementi e azioni comuni ad alcune le funzioni.

Come si presenta RCS Console

Ecco come viene visualizzata una pagina tipica di RCS Console. In questo esempio mostriamo la pagina di un target:



Area	*Descrizione*
1	Barra del titolo con pulsanti di comando: Logout da RCS. Pulsante di aggiornamento della pagina. Pulsante di ingrandimento della finestra. Pulsante di riduzione a icona della finestra.
2	• Pulsante per tornare alla homepage • Menu di RCS con le funzioni abilitate per l'utente
3	Barra di navigazione per l'operation. Di seguito la descrizione:

Icona	*Descrizione*
	Torna al livello superiore.
	Mostra la pagina dell'operation (sezione Operations).
	Mostra la pagina del target.
	Mostra la pagina della factory.
	Mostra la pagina dell'agent.
	Mostra la pagina dell'operation (sezione Intelligence).
	Mostra la pagina dell'entità.

4 Pulsanti per visualizzare tutti gli elementi indipendentemente dalla loro appartenenza. Di seguito la descrizione:

Icona	*Descrizione*
	Mostra tutte le operation.
	Mostra tutti i target.
	Mostra tutti gli agent.
	Mostra tutte le entità.

5 Barre con i pulsanti della finestra.

Area	*Descrizione*
6	Pulsanti e casella di ricerca:

Oggetto	*Descrizione*
	Casella di ricerca. Inserendo parte del nome compare l'elenco degli elementi che contengono le lettere inserite.
	Visualizza gli elementi in una tabella.
	Visualizza gli elementi come icone.

7	Utente connesso con possibilità di cambiare la lingua e la password.
8	Area download con possibilità durante un'esportazione o una compilazione di vedere lo stato di avanzamento. I file sono scaricati sul desktop nella cartella RCS Download. • barra superiore: percentuale generazione sul server. • barra inferiore: percentuale download dal server su RCS Console.
9	Data e ora attuale con possibilità di cambio fuso orario.

Azioni sempre disponibili sull'interfaccia

Cambiare la lingua dell'interfaccia o la propria password

Per cambiare la lingua dell'interfaccia o la propria password:

Passo	*Azione*
1	Fare clic su **[7]** compare una finestra di dialogo con i dati dell'utente.
2	Cambiare lingua o password e fare clic su **Save** per confermare e uscire.

Convertire le date-ora di RCS Console al proprio fuso orario

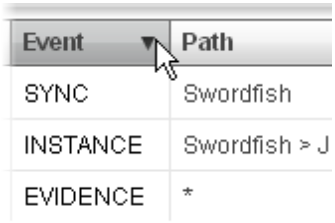
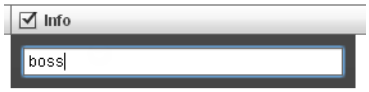
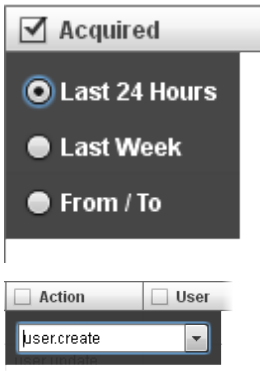
Per convertire tutte le date-ora al proprio fuso orario:

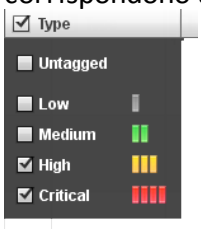
Passo	*Azione*
1	Fare clic su **[9]** compare una finestra di dialogo con la data-ora attuale: **UTC Time**: data-ora di Greenwitch (GMT) **Local Time**: data-ora dove è installato il server RCS **Console Time**: data-ora della console da cui si sta lavorando e che può essere convertita.
2	Cambiare il fuso orario e fare clic su **Save** per confermare e uscire: tutte le date-ora visualizzate sono convertite come richiesto.

Azioni sulle tabelle

RCS Console mostra diversi dati in forma di tabella. Le tabelle permettono di:

- ordinare i dati per colonna in ordine crescente/decrescente
- filtrare i dati per ogni colonna

Azione	*Descrizione*
Ordinare per colonna	Fare clic sull'intestazione per ottenere l'ordine per quella colonna, crescente o decrescente. 
Filtrare un testo	Inserire parte del testo che si sta cercando: compaiono solo gli elementi che contengono il testo digitato.  L'esempio mostrerà elementi con descrizioni tipo: • "my**boss**" • "**boss**anova"
Filtrare in base a un'opzione	Selezionare un'opzione: compaiono gli elementi che corrispondono all'opzione scelta. 

Azione	*Descrizione*
Filtrare in base a più opzioni	Selezionare una o più opzioni: compaiono gli elementi che corrispondono a tutte le opzioni scelte. 
Cambiare la dimensione delle colonne	Selezionare il bordo della colonna e trascinarlo.

Procedure dell'Analista

Introduzione

L'obiettivo dell'Analista è offrire delle prove valide per l'indagine in corso. Le prove sono:

- recuperate direttamente dal dispositivo tramite accesso fisico
- ricevute dall'agent installato

Per farlo può portare a termine le seguenti procedure:

Procedure

Per recuperare prove importanti ed essere avvisati

Per selezionare e recuperare prove importanti:

Passo	*Azione*
1	Nella sezione **File System**, se l'intercettazione è da remoto, esplorare l'hard disk dei dispositivi alla ricerca di file da scaricare. *Vedi "**Recupero evidence da dispositivi (File System)**" a pagina 52*
2	Nella sezione **Dashboard** aggiungere al pannello di controllo le operation, target e agent da controllare maggiormente. *Vedi "**Monitoraggio delle evidence (Dashboard)**" a pagina 92*
3	Nella sezione **Alerting** costruire le regole per essere avvisato quando arrivano prove di particolare interesse e per marcare delle evidence secondo la loro importanza. *Vedi "**Alert**" a pagina 95* .

Analizzare, selezionare ed esportare le evidence

Per analizzare, selezionare e esportare le evidence:

Passo	*Azione*
1	Nella sezione **Evidence** analizzare le evidence e marcarle in base all'importanza e alla necessità o meno di esportarle. *Vedi "**Analisi delle evidence (Evidence)**" a pagina 38 .*
2	Per le evidence di particolare interesse passare all'analisi dettagliata. *Vedi "**Dettaglio di una evidence**" a pagina 45*
3	Nella sezione **Evidence** esportare le evidence utili. *Vedi "**Analisi delle evidence (Evidence)**" a pagina 38 .*
4	Nella sezione **File System** esportare la struttura dell'hard disk. *Vedi "**Recupero evidence da dispositivi (File System)**" a pagina 52*

Per elaborare le informazioni ottenute sulle persone e i luoghi coinvolti nell'indagine

Per elaborare le informazioni ottenute sulle persone e il luoghi coinvolti nell'indagine:

Passo	*Azione*
1	Nella sezione **Intelligence** visualizzare e gestire le entità presenti in un'operation. *Vedi "**Gestione delle entità: vista a icone e vista tabellare**" a pagina 65 , "**Gestione delle entità: vista dei collegamenti**" a pagina 68 , "**Gestione delle entità: vista delle Position**" a pagina 73 .*
2	Visualizzare o modificare i dettagli di un'entità. *Vedi "**Dettaglio delle entità Target**" a pagina 77 ,* *"**Dettaglio delle entità Person**" a pagina 83 "**Dettaglio delle entità Position**" a pagina 85 "**Dettaglio delle entità Virtual**" a pagina 87 Vedi "**Dettaglio di una evidence**" a pagina 45*
3	Nella sezione **Alerting** costruire le regole per essere avvisato quando il sistema crea in automatico nuove entità e nuovi collegamenti e per marcare i collegamenti secondo la loro importanza.. *Vedi "**Alerting** " a pagina 97*

Operation e target

Presentazione

Introduzione

La gestione delle operation stabilisce i target da sottoporre a intercettazione.

Contenuti

Questa sezione include i seguenti argomenti:

Cose da sapere sulle operation

Cos'è un'operation

L'operation rappresenta l'indagine da eseguire. Un'operation contiene uno o più target, ovvero le persone fisiche da intercettare. Il Tecnico assegna al target uno o più agent di tipo *desktop* o *mobile*. Così l'agent può essere installato su un computer o su un dispositivo mobile.

Cose da sapere sui target

Cos'è un target

Il target rappresenta la persona fisica da investigare. Il Tecnico assegna al target uno o più agent di tipo desktop o mobile. Così l'agent può essere installato su un computer o su un dispositivo mobile.

Gestione delle operation

Per gestire le operation:	• sezione **Operations**

Scopo

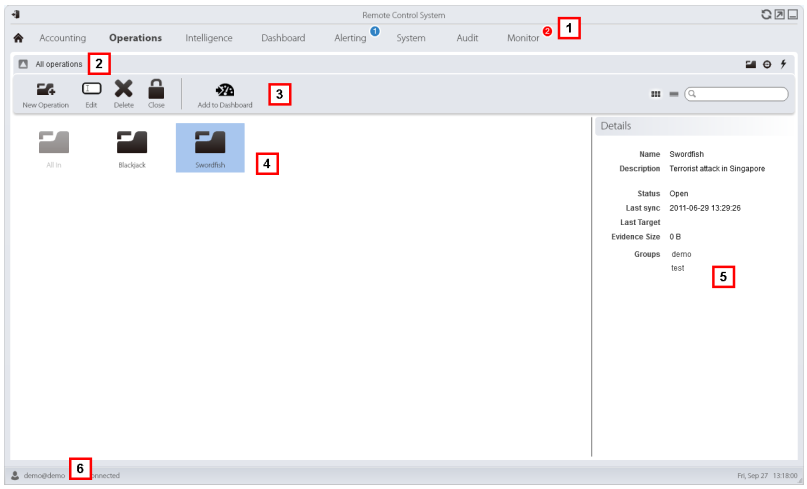
Questa funzione permette di:

- aggiungere l'operation agli elementi da tenere sotto controllo

NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Operation management**.

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area	*Descrizione*
1	Menu di RCS.
2	Barra di navigazione.
3	Barre con i pulsanti della finestra. Di seguito la descrizione: *Icona* *Descrizione* Aggiunge l'operation alla dashboard.
4	Elenco delle operation create: Operation aperta. Se sono stati definiti dei target e sono stati installati correttamente degli agent, si ricevono le evidence raccolte. Operation chiusa. Tutti i target sono chiusi e gli agent disinstallati. È comunque possibile vedere tutti i suoi target e tutte le sue evidence.
5	Dati dell'operation selezionata.
6	Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 12* .

Per la descrizione dei dati presenti sulla finestra *vedi "**Dati delle operation**" nella pagina di fronte* .

Per saperne di più sulle operation *vedi "**Cose da sapere sulle operation**" alla pagina precedente* .

Visualizzare i target di un'operation

Per visualizzare i target di un'operation:

Passo	*Azione*
1	Fare doppio clic su un'operation: si apre la pagina per la gestione dei target. *Vedi "**Pagina dell'operation**" nel seguito*

Dati delle operation

Di seguito la descrizione dei dati dell'operation selezionata:

Dato	*Descrizione*
Name	Nome dell'operation.
Description	Descrizione libera.
Contact	Campo descrittivo per definire, ad esempio, il nome di un referente (Giudice, Magistrato, e così via).
Status	Stato di un'operation e comando di chiusura: **OPEN**: l'operation è aperta. Se sono stati definiti dei target e sono stati installati correttamente degli agent, RCS riceve le evidence raccolte. **CLOSED**: l'operation è chiusa, senza più possibilità di riaprirla. Gli agent non inviano più i dati, ma è possibile consultare le evidence già ricevute.
Groups	Gruppi abilitati a visualizzare l'operation.

Pagina dell'operation

Per entrare in una operation:	• sezione **Operation**, doppio-clic su una operation

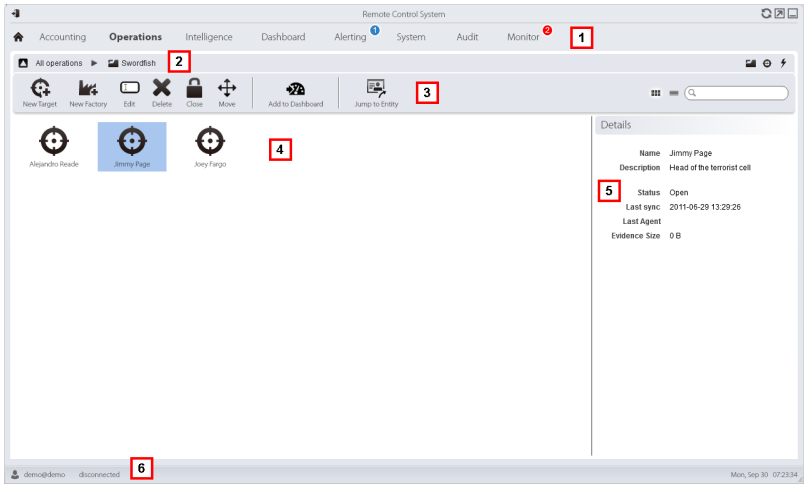
Scopo

Questa funzione permette di:

- aggiungere il target agli elementi da tenere sotto controllo

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area	*Descrizione*
1	Menu di RCS.
2	Barra di navigazione.
3	Barre con i pulsanti della finestra. Di seguito la descrizione:

Icona	*Funzione*
	Aggiunge il target alla dashboard.
	Apre la pagina dell'entità del target in intelligence.

4	Elenco dei target: target Aperto target Chiuso
5	Dati del target selezionato.
6	Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 12* .

Per saperne di più sulle operation *vedi "**Cose da sapere sulle operation**" a pagina 19* .

Per la descrizione dei dati presenti sulla finestra *vedi "**Dati della pagina di un'operation**" nel seguito* .

Dati della pagina di un'operation

Di seguito la descrizione dei dati del target selezionato:

Dato	*Descrizione*
Name	Nome del target.
Description	Descrizione libera.
Status	Definisce lo stato di un target:  Aperto. Se il Tecnico ha installato correttamente gli agent, RCS riceve le evidence raccolte.  Chiuso, senza più possibilità di riaprirlo.

4

I target

Presentazione

Introduzione

Un target è una persona fisica da sottoporre a monitoraggio. Possono essere utilizzati più agent, uno per ogni dispositivo posseduto dal target.

Contenuti

Questa sezione include i seguenti argomenti:

Pagina del target

Per entrare in un target	• sezione **Operations**, doppio-clic su una operation, doppio-clic su un target

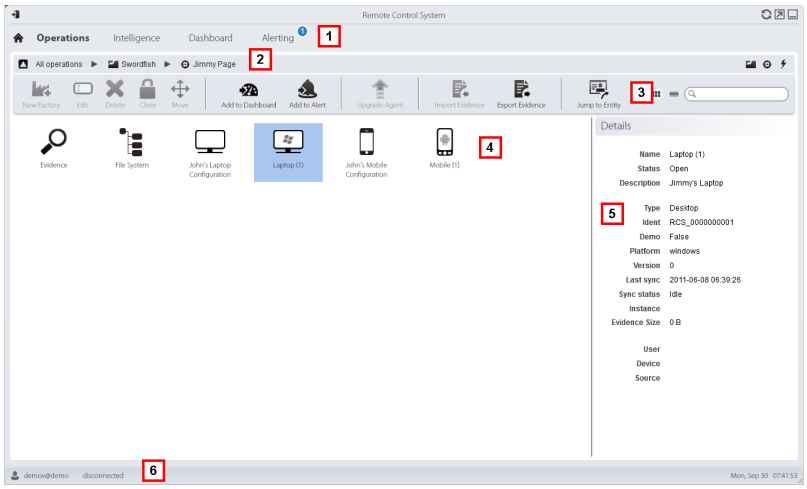
Scopo

Questa funzione permette di:

- esportare le evidence del target.
- entrare in un agent installato
- entrare nelle evidence dell'agent
- esplorare il dispositivo dell'agent

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area	*Descrizione*
1	Menu di RCS.
2	Barra di navigazione.

Area	*Descrizione*
3	Barre con i pulsanti della finestra. Di seguito la descrizione: NOTA: il pulsante visualizza gli elementi in elenco con i loro dati. *Icona* *Funzione* Aggiunge l'agent alla dashboard. Aggiunge l'agent agli alert: tutte le volte che avviene la sincronizzazione viene generato un alert. Esporta le evidence del target. NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Evidence export** . Apre la pagina dell'entità del target in intelligence.
4	Icone/elenco delle factory create e degli agent installati. : agent in modalità demo. : agent scout in attesa di verifica. : agent soldier installato. : agent elite installato.
5	Dati della factory o dell'agent selezionato.
6	Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 12* .

Per la descrizione dei dati presenti sulla finestra *vedi "**Dati della pagina target**" alla pagina successiva* .

Esportare le evidence del target

Per esportare le evidence :

Passo	*Azione*
1	Fare clic su **Export Evidence**: si apre la finestra di esportazione.
2	Fare clic su **Ok**: le evidence sono salvate nella cartella specificata.

Dati della pagina target

Per visualizzare i dati della pagina:	• sezione **Operations**, doppio-clic su una operation, doppio-clic su un target, fare clic su **Icon view** o **Table view**

Gli elementi della pagina possono essere visualizzati a icone o a tabella.

Visualizzazione a icone

Di seguito la descrizione delle icone:

Dato	*Descrizione*
	Esempio di agent scout per dispositivo desktop Windows, in stato Aperto.
	Esempio di agent soldier per dispositivo desktop Windows, in stato Aperto.
	Esempio di agent elite per dispositivo desktop Windows, in stato Aperto.

NOTA: agent in stato **CLOSED** hanno l'icona di colore grigio chiaro. Questa è l'icona di un agent mobile per Android in stato Chiuso:  .

Visualizzazione a tabella

Di seguito la descrizione dei dati:

Dato	*Descrizione*
Nome	Nome della factory o dell'agent.
Descrizione	Descrizione della factory o dell'agent.

Dato	*Descrizione*
Status	**Open**: l'agent è ancora attivo sul dispositivo e può continuare a inviare dati. **Closed**: l'agent non è più attivo. NOTA: un agent chiuso non può essere più aperto. I dati presenti in RCS sono ancora consultabili.
Type	Tipologia desktop o mobile.
Level	(solo agent) Livello dell'agent: scout, soldier, elite.
Platform	(solo agent) Sistema operativo su cui l'agent si è installato.
Version	(solo agent) Versione dell'agent. A ogni nuova configurazione viene creata una nuova versione.
Last sync	(solo agent) Data e ora dell'ultima sincronizzazione dell'agent.
Ident	(solo agent) Identificativo univoco di un agent.
Instance	(solo agent) Identificativo univoco del dispositivo su cui l'agent è installato.

5

Gli agent

Presentazione

Introduzione

Gli agent acquisiscono dati dal dispositivo su cui sono installati e li inviano ai Collector di RCS. La loro configurazione e il loro software possono essere aggiornati e possono essere trasferiti file in modo assolutamente invisibile dal/al target.

Contenuti

Questa sezione include i seguenti argomenti:

Pagina dell'agent

Per gestire gli agent:	• sezione **Operations**, doppio-clic su una operation, doppio-clic su un target, doppio-clic su un agent

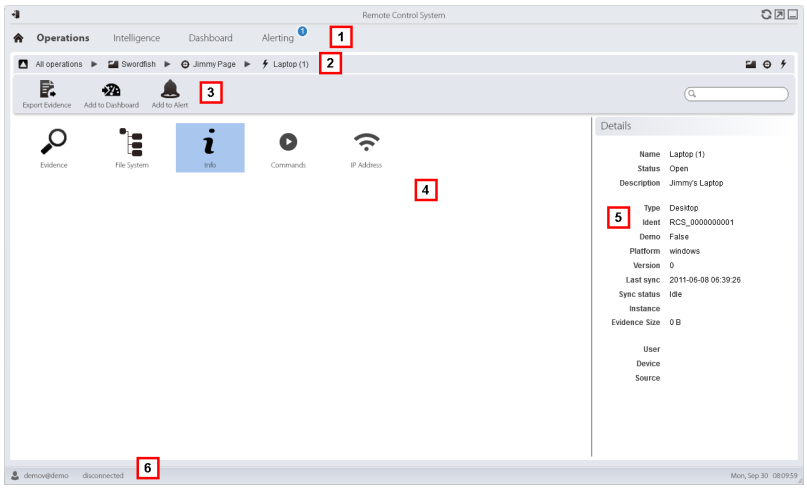
Scopo

Questa funzione permette di:

- verificare l'attività dell'agent tramite lo storico eventi.
- visualizzare le evidence raccolte dall'agent
- esplorare il file system e trasferire file dal dispositivo dove è installato l'agent

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area	*Descrizione*
1	Menu di RCS.
2	Barra di navigazione.

Area	*Descrizione*
3	Barre con i pulsanti della finestra.

Icona	*Descrizione*
	Esporta le evidence dell'agent.  NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Evidence export** .
	Aggiunge l'agent alla dashboard.
	Aggiunge l'agent agli alert: tutte le volte che avviene la sincronizzazione viene generato un alert.

4	Azioni possibili sull'agent. Di seguito la descrizione:

Icona	*Descrizione*
	Mostra l'elenco delle evidence raccolte dall'agent. *Vedi "**Analisi delle evidence (Evidence)**" a pagina 38* .
	Mostra il file system del dispositivo. *Vedi "**Recupero evidence da dispositivi (File System)**" a pagina 52* .
	Mostra lo storico degli eventi dell'agent (Info). *Vedi "**Dati dello storico eventi di un agent**" alla pagina successiva*
	Mostra il risultato dei comandi lanciati sul dispositivo tramite azioni **Execute** . *Vedi "**Pagina dei comandi**" alla pagina successiva* .
	Mostra lo storico sincronizzazioni dell'agent. *Vedi "**Dati dello storico sincronizzazioni dell'agent**" a pagina 34* .

5	Dettagli dell'agent.
6	Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "Elementi e azioni comuni dell'interfaccia" a pagina 12* .

Dati dello storico eventi di un agent

Di seguito la descrizione:

Campo	*Descrizione*
Acquired	Data-ora dell'evento acquisito sul dispositivo. È possibile filtrare. **Last 24 hours** è l'impostazione predefinita.
Received	Data-ora dell'evento registrato in RCS. È possibile filtrare. **Last 24 hours** è l'impostazione predefinita.
Content	Informazione di stato inviata dall'agent.

Pagina dei comandi

Per gestire i risultati dei comandi:	• sezione **Operations**, doppio-clic su una operation, doppio-clic su un target, doppio-clic su un agent, doppio-clic su **Commands**

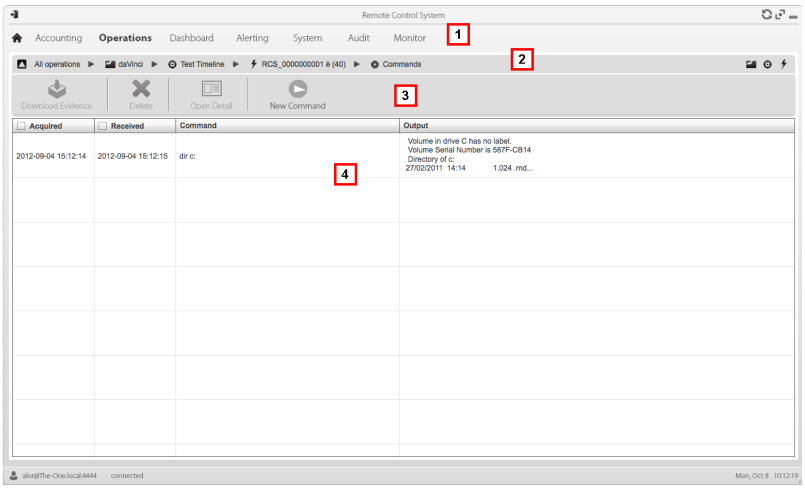
Scopo

Questa funzione permette di:

- verificare i risultati dei comandi eseguiti dall'azione **Execute** configurata sull'agent
- verificare i risultati del file eseguibile attivato durante il trasferimento di file da/a l'agent

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area	*Descrizione*
1	Menu di RCS.
2	Barra di navigazione.
3	Barre con i pulsanti della finestra. Di seguito la descrizione:

Icona	*Descrizione*
	Esporta in un file .txt il comando selezionato.
	Elimina i comandi selezionati.  NOTA: la funzione è sottoposta a licenza d'uso ed è abilitata solo se si è in possesso dell'autorizzazione **Evidence deletion.**
	Mostra il dettaglio del comando selezionato.

5	Elenco dei comandi in base ai filtri impostati.
6	Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 12 .*

Dati dello storico sincronizzazioni dell'agent

Di seguito la descrizione:

Campo	*Descrizione*
Acquired	Data-ora della sincronizzazione. È possibile filtrare. **Last 24 hours** è l'impostazione predefinita.
IP	Indirizzo IP da cui è stata fatta la sincronizzazione.
Address	Luogo da cui si è stabilita la connessione.

6

Analisi delle evidence

Presentazione

Introduzione

L'analisi delle evidence a livello di elenco o di dettaglio, seleziona le evidence per l'esportazione verso l'autorità competente.

Contenuti

Questa sezione include i seguenti argomenti:

Cose da sapere sulle evidence

Processo di analisi

Di seguito la descrizione del processo di analisi:

Fase	*Descrizione*
1	Mano a mano che il sistema raccoglie le evidence dall'agent le mostra e mantiene aggiornato il contatore totale.
2	L'Analista visualizza tutte le evidence e le marca per facilitare la consultazione della tabella e per successivamente esportarle.
3	L'Analista analizza le evidence entrando nel dettaglio.
4	Al termine dell'indagine o su richiesta, l'Analista esporta le evidence in un file consultabile tramite browser.

Accumulo delle evidence nel dispositivo

Le evidence vengono spedite dall'agent al Collector in ordine di creazione. Se un dispositivo sincronizza molto raramente o con una larghezza di banda molto ridotta è probabile che le evidence si accumulino sul dispositivo e sia necessario attendere molto tempo prima di ricevere i dati più recenti.

La stessa cosa può verificarsi se in coda è presente una evidence di grandi dimensioni: le evidence più recenti potranno essere spedite solo dopo aver completato la spedizione di questa evidence.

Per questo motivo si suggerisce di eliminare le evidence più vecchie e/o che superano una certa dimensione. La cancellazione avviene alla successiva sincronizzazione.

*Vedi "**Pagina dell'agent**" a pagina 30 .*

Filtrare le evidence

Per limitare la quantità di evidence visualizzate è possibile agire sui filtri nelle intestazioni di colonna.

*Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 12*

IMPORTANTE: se non ci sono evidence visualizzate controllare il contatore in basso a destra. Se mostra dei valori tipo "0/1270" significa che c'è un filtro impostato che impedisce la visualizzazione delle evidence.

I filtri selezionati possono essere salvati con una breve descrizione per essere successivamente recuperati.

IMPORTANTE: se vengono definiti filtri privati non potranno essere usati da altri utenti.

Tradurre le evidence

Su speciale licenza d'uso è disponibile il modulo RCS Translate che permette la traduzione delle evidence. Infatti comunica con un software terze parti di traduzione linguistica, che restituisce i testi tradotti nella lingua dell'interfaccia.

RCS Translate agisce sui seguenti tipi di evidence:

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

La traduzione è visibile sia nella pagina con l'elenco delle evidence, sia nella pagina di dettaglio della singola evidence.

Eliminare le evidence

La funzione serve per eliminare una o più evidence non più ritenute utili. Questa funzione dipende dal tipo di licenza installato.

La cancellazione delle evidence può avvenire anche in modo guidato tramite l'impostazione di un filtro che seleziona le evidence da cancellare (simile a quello che seleziona le evidence da esportare).

IMPORTANTE: il filtro compare solo se durante la pressione del pulsante Delete **si tiene premuto il tasto ALT.**

Descrizione del file .tgz con le evidence esportate

Il file .tgz esportato è un file compresso, apribile con la maggior parte dei programmi di compressione (es.: WinZip, WinRar). Una volta espanso si presenta come una cartella con file HTML.

Per vedere il file:

Passo	*Azione*
1	Aprire index.html con un browser: la home page mostra l'elenco delle giornate con la statistica per orario delle evidence raccolte.
2	Fare clic su una giornata: compare l'elenco delle evidence, simile a quello visualizzato nella funzione **Evidence**.
3	Su questo elenco sono possibili le seguenti azioni: • sulle immagini: fare clic per visualizzare l'immagine intera • sull'audio: fare clic per attivare il mini player • sui file scaricabili: fare clic su ↓↓ per scaricare il file

Suggerimento: nella cartella Style ci sono fogli di stile per eventuali personalizzazioni (es.: logo istituzionale). È possibile copiare questi fogli di stile sul server, in modo che abbiano impatto su tutti i report generati da RCS Console.

Analisi delle evidence (Evidence)

Per analizzare le evidence:	• sezione **Operations**, doppio-clic su una operation, doppio-clic su un target, fare clic su **Evidence** • sezione **Operations**, doppio-clic su una operation, doppio-clic su un target, doppio-clic su un agent, fare clic su **Evidence**

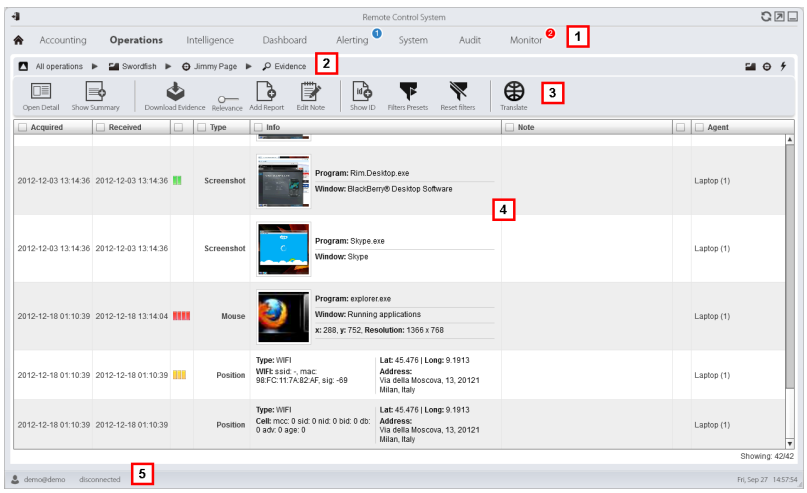
Scopo

Questa funzione permette di:

- preparare le evidence all'analisi, marcandole per grado di importanza, per destinarle a un report, o aggiungendo delle note personali
- visualizzare le evidence di interesse filtrando l'elenco
- tradurre contenuti di una evidence nella propria lingua (opzionale)
- analizzare superficialmente una evidence dall'elenco oppure entrare nel dettaglio per un'analisi più completa
- esportare le evidence

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area	*Descrizione*
1	Menu di RCS.
2	Barra di navigazione.

Area	*Descrizione*
3	Barre con i pulsanti della finestra. Di seguito la descrizione:

Icona	*Descrizione*
	Mostra il dettaglio dell'evidence selezionata. *Vedi "**Dettaglio di una evidence**" a pagina 45*
	Mostra le quantità totali per tipo di evidence.
	Esporta le evidence selezionate in un file .tgz.  NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Evidence export** .
	Elimina le evidence selezionate.  Suggerimento: per eliminare più evidence secondo particolari criteri (es.: range di data) premere il tasto ALT e tenerlo premuto mentre si fa clic su questo pulsante: compare una finestra per l'impostazione dei criteri di eliminazione delle evidence. Per una descrizione dei campi *vedi "**Dati di esportazione delle evidence**" a pagina 48* , i campi sono simili.  NOTA: la funzione è sottoposta a licenza d'uso ed è abilitata solo se si è in possesso dell'autorizzazione **Evidence deletion**.
	Applica un grado di importanza alle evidence selezionate.
	Applica un segnalibro alle evidence selezionate.
	Modifica le note delle evidence selezionate.
	Mostra i codici identificativi delle evidence.
	Salva i filtri attualmente selezionati oppure carica una impostazione di filtri salvata precedentemente.
	Pulisce tutti i filtri impostati.
	Visualizza i contenuti nella lingua dell'interfaccia.  NOTA: questa funzione è sottoposta a licenza d'uso.

Area	*Descrizione*
4	Elenco delle evidence in base ai filtri impostati.
5	Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 12* .

Per la descrizione dei dati presenti sulla finestra *vedi "**Dati delle evidence**" a pagina 43*

Per la descrizione dei dati utili all'esportazione *vedi "**Dati di esportazione delle evidence**" a pagina 48* .

Per saperne di più sulle evidence*vedi "**Cose da sapere sulle evidence**" a pagina 36*

Per vedere l'elenco dei tipi di evidence *vedi "**Elenco dei tipi di evidence**" a pagina 49*

Preparare le evidence all'analisi e all'export marcandole per importanza

Per assegnare dei gradi di importanza alle evidence, utili per la visualizzazione e l'export:

Passo	*Azione*
1	Selezionare una o più evidence.
2	• Trascinare **Relevance** nella posizione desiderata oppure • Premere la combinazione di tasti corrispondente.
3	**Risultato**: le singole evidence riportano il simbolo corrispondente al grado di importanza. Sarà possibile filtrare per questo simbolo e includere/escludere le evidence in fase di export.

Preparare le evidence all'analisi e all'export marcandole per il report

Per includere/escludere evidence dal report e per filtrare la visualizzazione:

Passo	*Azione*
1	Selezionare una o più evidence.

Passo	*Azione*
2	• Fare clic su **Add Report** oppure • premere ALT+R
3	**Risultato**: le singole evidence riportano il segnalibro. Sarà possibile filtrare per questo simbolo e includere/escludere le evidence in fase di export.

Preparare le evidence all'analisi e all'export aggiungendo note personali

Per poter aggiungere note personali a una o più evidence:

Passo	*Azione*
1	Selezionare una o più evidence.
2	• Fare clic su **Edit Note** oppure • premere ALT+N
3	**Risultato**: il campo **Note** può essere modificato. Se sono selezionate più evidence, il testo scritto sarà copiato in tutti gli altri campi **Note**.

Analizzare una evidence

Per analizzare rapidamente o nel dettaglio una evidence:

Passo	*Azione*
1	Analizzare l'anteprima dell'evidence. Per esempio per i file audio è possibile eseguire un miniplayer per capire se la evidence è di interesse.
2	Fare doppio clic su una evidence: compare la finestra del dettaglio delle evidence. *Vedi "**Dettaglio di una evidence**" a pagina 45*

Visualizzare i contatori suddivisi per tipo

Per vedere le quantità di evidence totali suddivise per tipologia:

Passo	*Azione*
1	Fare clic su **Show Summary**: compaiono i simboli dei tipi di evidence ognuno con il proprio contatore.
2	Fare clic su **Hide Summary** per nascondere i contatori.

Esportare le evidence visualizzate

Per selezionare alcune evidence e esportarle:

Passo	*Azione*
1	Procedere prima alla marcatura delle evidence per grado di importanza e se devono essere considerate per il report (pulsante **Add report**).
2	Selezionare ulteriormente agendo sui filtri nelle intestazioni di colonna su gruppi omogenei di evidence (colonna **Included in report**).
3	Fare clic su **Export Evidence**: indicare quali evidence includere/escludere. Sono esportate le evidence che corrispondono ai criteri selezionati e hanno il campo **Included report** selezionato.*Vedi "Dati di esportazione delle evidence" a pagina 48* .
4	Fare clic su **Save**: viene creato il file .tgz e scaricato nella cartella RCS Download.

Dati delle evidence

Di seguito la descrizione dei dati delle evidence sia per l'agent, sia per il target:

Dato	*Descrizione*
Acquired	Data-ora di cattura della evidence. È possibile filtrare. **Last 24 hours** è l'impostazione predefinita.
Received	Data-ora di registrazione in RCS della evidence. È possibile filtrare. **Last 24 hours** è l'impostazione predefinita.  Suggerimento: questo dato è utile quando si ha il sospetto che il dispositivo del target non abbia la data-ora aggiornate e che quindi l'**Acquired** non sia valido.

Dato	*Descrizione*
Relevance	Gradi di importanza delle evidence, assegnato automaticamente da regole di alert o manualmente in questo elenco. Il grado di importanza viene impostato tramite: • comando **Relevance** da menu • tasti rapidi Elenco tasti rapidi. *Icona* / *Tasti rapidi* / *Descrizione*  ALT+4 — *Importanza massima*  ALT+3 — *Importanza intermedia*  ALT+2 — *Importanza normale*  ALT+1 — *Importanza minima* - ALT+0 — *Nessuna importanza*
Type	Tipo di evidence da selezionare. *Vedi "Elenco dei tipi di evidence" a pagina 49*
Info	Informazioni dell'evidence: testi, immagini, video, audio e così via. Ogni informazione è accompagnata da diversi campi (es.: campo **content**, **program**). Si può filtrare indicando semplicemente la parola intera da cercare oppure indicando il il nome intero del campo e la parola intera da cercare. Per esempio: • "boss" cerca la parola "boss" o "Boss" in tutti i campi • mentre "**content**:boss" cerca la parola "boss" o "Boss" solo nei campi di tipo **content**.
Note	Note inserite dall'Analista mediante: • menu **Edit Note** • tasto rapido ALT+N
Report	Segnalibro, che indica che l'evidence potrà essere inclusa/esclusa in fase di esportazione. Il segnalibro viene impostato mediante: • menu **Add Report** • tasto rapido ALT+R
Agente	(solo per evidence del target) Nome dell'agent che ha registrato l'evidence.

Dettaglio di una evidence

Per entrare nel dettaglio di una evidence:	• sezione **Operations**, doppio-clic su una operation, doppio-clic su un target, fare clic su **Evidence**, doppio clic su una evidence • sezione **Operations**, doppio-clic su una operation, doppio-clic su un target, doppio-clic su un agent, fare clic su **Evidence**, doppio clic su una evidence

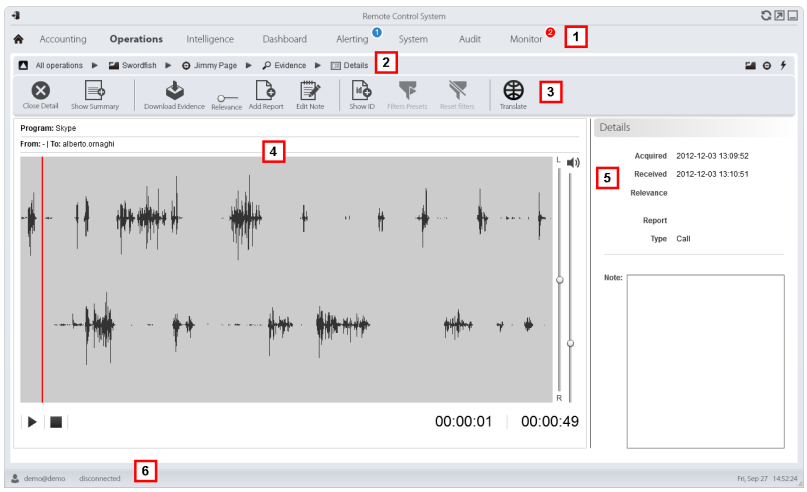
Scopo

Questa funzione permette di analizzare nel dettaglio una singola evidence. L'interfaccia cambia se l'evidence è di tipo testuale, audio, immagine o mappa.

NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Evidence editing**.

Come si presenta la funzione

Ecco come viene visualizzata il dettaglio di una evidence audio:



Area	*Descrizione*
1	Menu di RCS.
2	Barra di navigazione.

Area	*Descrizione*
3	Pulsanti per le azioni sulla evidence.

Icona	*Descrizione*
	Chiude il dettaglio e torna nell'elenco delle evidence. *Vedi "**Analisi delle evidence (Evidence)**" a pagina 38 .*
	Mostra le quantità totali per tipo di evidence.
	Esporta l'evidence in un file .tgz.
	Elimina l'evidence.  NOTA: la funzione è sottoposta a licenza d'uso ed è abilitata solo se si è in possesso dell'autorizzazione **Evidence deletion**.
	Applica un grado di importanza.
	Applica un segnalibro.
	Modifica le note.
	Mostra il codice identificativo.
	Salva i filtri attualmente selezionati oppure carica una impostazione di filtri salvata precedentemente.
	Pulisce tutti i filtri impostati.
	Visualizza i contenuti nella lingua dell'interfaccia.  NOTA: questa funzione è sottoposta a licenza d'uso.

4	Dettaglio dell'evidence. In base al tipo di evidence (audio, immagine, video) compaiono dei pulsanti di analisi.
5	Dati di dettaglio dell'evidence.
6	Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 12* .

Per saperne di più sulle evidence *vedi "**Cose da sapere sulle evidence**" a pagina 36* .

Per la descrizione dei dati presenti sulla finestra *vedi "**Dati delle evidence**" a pagina 43* .

Azioni su evidence di tipo immagine

Di seguito la descrizione delle azioni possibili sulle evidence che restituiscono un'immagine:

Icona	*Descrizione*
	(solo evidence tipo screenshot e file) Mostra il testo estratto. NOTA: se compare il messaggio "OCR non disponibile" significa che il documento è ancora in attesa di essere convertito e indicizzato. Se il pulsante non è presente significa che questa funzione non è stata installata. Rivolgersi al proprio Amministratore di sistema.
	(solo evidence tipo screenshot) Torna alla visualizzazione dell'immagine.
	Visualizza immagine a tutto schermo.
1:1	Visualizza immagine in dimensione reale.
	Ingrandisce e rimpicciolisce immagine.
	Ruota immagine.
Anti alias	Riduce effetto di scalettatura dell'immagine.
	L'immagine diventa l'immagine di default dell'entità di intelligence (se il modulo Intelligence è presente).

Azioni su evidence di tipo audio

Di seguito la descrizione delle azioni possibili sulle evidence che restituiscono un file audio:

Icona	*Descrizione*
	Regolazione volume.
	Avvia, mette in pausa e ferma audio.
	Bilancia suono su sorgente locale (target) e remota (interlocutore).

Dati di esportazione delle evidence

Dati di esportazione

Di seguito la descrizione dei dati necessari per l'esportazione delle evidence.

IMPORTANTE: le evidence esportate saranno tutte e soltanto quelle che rispettano tutti i criteri specificati!

Dato	*Descrizione*
Da **A**	Intervallo di tempo delle evidence da esportare.
Acquisizione	Considera la data come data di acquisizione della prova sul dispositivo del target.
Ricezione	Considera la data come data di ricezione della prova.
Rilevanza	Gradi di importanza delle evidence da esportare.
Tipo	Tipi di evidence da esportare. NOTA: quando nessun tipo di evidence è selezionato, RCS esporta automaticamente tutti i tipi.
Report	Se selezionato, sono esportate solo le evidence con campo **Report** selezionato. È possibile includere o escludere l'esportazione delle note.

Dato	*Descrizione*	
Nome report	Nome del file di esportazione. Per impostazione predefinita, RCS nomina il file con la seguente nomenclatura:	
	Esportazione evidence dalla pagina	***Nome file***
	Target	*nome target* - *nome agent* - Evidence Export.tgz
	Agente	*nome agent* - Evidence Export.tgz
Export file	Avvia esportazione del file.	
Export to connector	Avvia esportazione delle evidence verso il connector.	

Comandi di esportazione

Di seguito la descrizione dei comandi per l'esportazione delle evidence.

Comando	*Descrizione*
Export to file	Avvia esportazione del file.
Export to connector	Avvia esportazione delle evidence verso il connector. NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Connectors management.**

Elenco dei tipi di evidence

Di seguito la descrizione dei tipi di evidence disponibili:

Modulo	*Tipo file*	*Registrazione di...*
Accessed files	testo	*(solo desktop) documenti o immagini aperti dal target.*
Addressbook	testo	*contatti.*
Application	testo	*applicazioni utilizzate.*
Calendar	testo	*calendario.*
Call	audio	*chiamate (es.: GSM e VoIP).*
Camera	immagine	*immagini della webcam.*
Chat	testo	*chat.*
Clipboard	testo	*informazioni copiate nella clipboard.*

Modulo	*Tipo file*	*Registrazione di...*
Dispositivo	testo	*informazioni del sistema.*
File	testo	*file aperti dal target.*
File System	testo	*struttura dell'hard disk esplorabile nella funzione File System.* *Vedi "**Recupero evidence da dispositivi (File System)**" a pagina 52*
Info	testo	*informazioni fornite dall'agent e definite nella configurazione.*
Keylog	testo	*tasti premuti sulla tastiera.*
Messages	testo	*e-mail.*
Money	testo	*informazioni del portafoglio digitale di cryptocurrency (es.: Bitcoin).*
Mic	audio	*audio.*
Mouse	immagine	*clic del mouse.*
Password	testo	*password.*
Position	immagine	*posizione geografica del target.*
Print	immagine	*pagine stampate.*
Screenshots	immagine	*immagini attive sul display del target.*
URL	testo	*pagine web visitate.*

7

Esplorazione e recupero prove da dispositivi online

Presentazione

Introduzione

L'esplorazione graduale di un dispositivo permette di trovare prove di interesse e scaricarle.

Contenuti

Questa sezione include i seguenti argomenti:

Cose da sapere sul recupero prove

Descrizione

La funzione mostra l'alberatura del FileSystem del dispositivo su cui è presente l'agent (o di più dispositivi se si sta esplorando il FileSystem di un target).

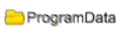
È possibile esplorare gradualmente l'alberatura del FileSystem, richiedendo prima la lettura della struttura di primo livello (comando **Retrieve default**) ed esplorando successivamente le cartelle e richiedendo poi la lettura o rilettura della cartella selezionata (comando **Retrieve subtree**).

Una volta che si identifica un file di interesse, lo si può scaricare e salvare come evidence di tipo file (comando **Download**)

NOTA: la lettura delle cartella o il download di un file avviene a seguito di una sincronizzazione.

Componenti del File System

La struttura di ogni dispositivo mostra le cartelle da esplorare e quelle esplorate:

Esempio	*Descrizione*
	Root del dispositivo.
	Cartella non ancora esplorata.
	Cartella esplorata.

Recupero evidence da dispositivi (File System)

Per gestire il File System del dispositivo:	• sezione **Operations**, doppio-clic su una operation, doppio-clic su un target, fare clic su **File System** • sezione **Operations**, doppio-clic su una operation, doppio-clic su un target, doppio-clic su un agent, fare clic su **File System**

Scopo

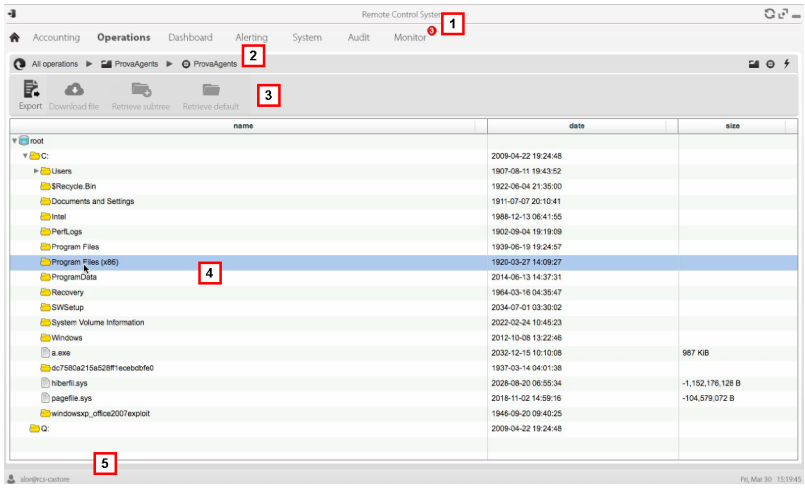
Questa funzione permette di:

- esplorare l'alberatura del FileSystem del dispositivo su cui è presente l'agent (o di più dispositivi se si sta esplorando il FileSystem di un target).
- Selezionare il file da inserire nella coda di download dell'agent
- esportare la struttura (file system) esplorata

NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **File system browsing on agent**.

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area	*Descrizione*
1	Menu di RCS.
2	Barra di navigazione.
3	Barre con i pulsanti della finestra. Di seguito la descrizione:

Icona	*Descrizione*
	Esporta la struttura completa in un file .tgz.
	Scarica il file selezionato nelle evidence di tipo **File**.
	Esplora il contenuto della cartella selezionata.
	Richiede la struttura di primo livello del disco.
	Visualizza elenco delle richieste al Filesystem attualmente in sospeso in attesa della successiva sincronizzazione.

Area	*Descrizione*
4	Struttura dell'hard disk del dispositivo.
5	Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 12* .

Per saperne di più sull'esplorazione del file-system *vedi "**Cose da sapere sul recupero prove**" a pagina 52*

Esplorare il contenuto del file system e scaricare file

Per esplorare il contenuto e scaricare contenuti interessanti:

Passo	*Azione*
1	Selezionare una cartella.
2	• Fare clic su **Retrieve** e impostare il livello di profondità delle sottocartelle • Fare clic su **Save**: alla successiva sincronizzazione è restituita la struttura delle sottocartelle fino al livello richiesto.  Suggerimento: chiedere pochi livelli per volta, procedere gradualmente.
3	Ripetere il passo 1-2 sulle sottocartelle che si vogliono esplorare.
4	Dopo aver identificato il file di interesse, selezionarlo e fare clic su **Download**: alla successiva sincronizzazione il file viene scaricato come evidence di tipo **File** .

Intelligence

Presentazione

Introduzione

La sezione permette di rappresentare ad alto livello le interazioni tra i target, correlando le evidence ricevute dagli agent con altre informazioni in proprio possesso.

Contenuti

Questa sezione include i seguenti argomenti:

Cose da sapere sull'intelligence

Presentazione

Introduzione

Nella sezione Intelligence l'Analista elabora le informazioni dell'indagine in suo possesso .

Le persone soggette ad investigazione, le altre persone e i luoghi coinvolti nelle indagini sono rappresentati da *entità*. Le relazioni tra persone e tra persone e luoghi sono rappresentate come *collegamenti* tra entità.

Sulla base delle evidence ricevute dai dispositivi dei target, il sistema crea nuove entità e nuovi collegamenti tra le entità. L'Analista interpreta e organizza queste informazioni aggiungendo, modificando ed eliminando entità o collegamenti secondo l'evoluzione delle indagini.

La licenza per la sezione Intelligence

Le funzioni dell'intelligence sono sottoposte a licenza d'uso.

In assenza di licenza d'uso l'Analista può utilizzare la sezione Intelligence solo per visualizzare e aggiungere i dettagli dei target presenti nell'operation; non vengono fornite le elaborazioni del sistema sulla base delle evidence raccolte. Le uniche entità presenti sono quelle Target e possono essere gestite solo con la vista a icone o vista tabellare, *vedi "**Gestione delle entità: vista a icone e vista tabellare**" a pagina 65* .

Per saperne di più

*Vedi "**Cose da sapere sulle entità**" nel seguito* .

*Vedi "**Cose da sapere sui collegamenti**" a pagina 58* .

*Vedi "**Cose da sapere sulle entità Gruppo**" a pagina 60*

*Vedi "**Cose da sapere su come lavora l'intelligence** " a pagina 61* .

Cose da sapere sulle entità

Introduzione

L'entità rappresenta una persona o un luogo coinvolti in un'indagine.

Ogni entità è definita tramite delle informazioni di dettaglio che permettono al sistema di individuare relazioni tra le entità.

Le persone coinvolte nell'indagine: entità Target e entità Person

Il sistema definisce due tipi di entità per rappresentare le persone coinvolte in un'indagine:

-  : tipo Target, per le persona soggette ad intercettazione
-  : tipo Person, per le persone non soggette ad intercettazione

I luoghi coinvolti nell'indagine: entità Position e entità Virtual

Il sistema definisce due tipi di entità per rappresentare i luoghi coinvolti in un'indagine:

-  : tipo Position, per i luoghi fisici
-  : tipo Virtual, per i luoghi virtuali come le pagine web

Gestire le entità

L'Analista gestisce le entità affinché rappresentino l'evoluzione dell'indagine, quindi:

- aggiunge nuove entità per monitorare altre persone e luoghi che si rivelano interessanti
- aggiunge dettagli alle entità per fornire nuovi dati al sistema per individuare relazioni tra le entità
- elimina entità quando ritiene che rappresentano persone o luoghi non interessanti per l'indagine
- forma entità Gruppo per facilitare la visualizzazione e l'analisi delle informazioni, *vedi "**Cose da sapere sulle entità Gruppo**" a pagina 60*

Entità Target

L'entità Target viene creata automaticamente alla creazione del target nella sezione Operations. Nome e descrizione sono gli stessi assegnati nella sezione Operations.

NOTA: non è possibile eliminare l'entità Target dalla sezione Intelligence. Per eliminarla è necessario eliminare il target nella sezione Operations.

NOTA: è possibile modificare il nome e la descrizione del Target senza che questa modifica abbia impatto sulla sezione Operations.

Il sistema aggiunge dettagli dell'entità Target con le informazioni raccolte nelle evidence (es.: foto, persone più contattate). L'Analista può aggiungere altre informazioni in suo possesso. *Vedi "**Dettaglio delle entità Target**" a pagina 77*

Entità Person

L'entità Person può essere creata manualmente dall'Analista o automaticamente dal sistema.

L'entità Person è definita tramite gli identificativi che utilizza per comunicare, via telefono o via internet (es.: numero di telefono, contatto Skype).

NOTA: più la scheda di dettaglio dell'entità è ricca di informazioni maggiore è la probabilità che il sistema individui collegamenti tra quella entità e le altre entità.

Se una entità Person diventa oggetto di intercettazione è possibile trasformarla/modificarla in entità Target. In questo modo il sistema crea nella corrispondente Operation un nuovo target.

NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Target management.**

*Vedi "**Dettaglio delle entità Person**" a pagina 83*

Entità Position

L'entità Position può essere creata manualmente dall'Analista o automaticamente dal sistema.

L'entità Position è definita dalle coordinate geografiche (latitudine e longitudine) o dall'indirizzo del luogo che rappresenta e da un raggio di accuratezza.

NOTA: il raggio di accuratezza deve essere adeguato al tipo di luogo (es.: 50-100m per un edificio, molto di più nel caso di un parco).

*Vedi "**Dettaglio delle entità Position**" a pagina 85*

Entità Virtual

L'entità Virtual deve essere creata manualmente dall'Analista.

L'entità Virtual è definita tramite uno o più indirizzi URL della pagina web che rappresentano.

*Vedi "**Dettaglio delle entità Virtual**" a pagina 87*

Cose da sapere sui collegamenti

Introduzione

Un collegamento rappresenta una relazione tra le entità. Tra due entità può esistere un solo collegamento.

Esistono tre tipi di collegamenti:

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

I collegamenti Know

I collegamenti Know rappresentano una relazione di tipo *conoscenza*. Due entità hanno un collegamento Know quando almeno una delle due ha nella propria rubrica il contatto dell'altra.

Un collegamento Know può essere direzionale o bidirezionale.

I collegamenti Peer

I collegamenti Peer indicano che tra le entità c'è stato un *contatto*.

Due entità che rappresentano persone hanno un collegamento Peer quando c'è stata una comunicazione diretta tra le due entità (es.: telefonata, chat). La relazione può essere sia direzionale che bidirezionale.

Un'entità che rappresenta una persona e una che rappresenta un luogo hanno un collegamento Peer quando la persona è stata in quel luogo (fisico o nel web). La relazione è solamente direzionale: dall'entità che rappresenta una persona a quella che rappresenta un luogo.

I collegamenti Peer rappresentano una relazione più forte dei collegamenti Know, quindi sostituiscono un eventuale collegamento Know già presente tra le entità.

Gestire i collegamenti Peer e Know

L'Analista gestisce i collegamenti affinché rappresentino l'evoluzione dell'indagine, quindi:

- aggiunge o modifica collegamenti tra due entità quando è in possesso di informazioni che provano una relazione tra le due
- attribuisce un grado di importanza ai collegamenti per rappresentare la rilevanza della relazione nell'indagine
- elimina i collegamenti quando è in possesso di informazioni che provano l'assenza di relazione o che la relazione non è rilevante per l'indagine.

I collegamenti Identity

I collegamenti Identity rappresentano un suggerimento di relazione di *identità* tra due entità che rappresentano persone. Questo tipo di collegamento è creato automaticamente dal sistema quando le due entità condividono almeno un identificativo (es.: numero di telefono).

I collegamenti Identity non hanno direzionalità.

Gestire i collegamenti Identity

I collegamenti identity richiedono all'Analista di decidere quale sia la ragione della loro presenza e di agire di conseguenza:

- se sono la stessa persona, le due entità devono essere unite;
- se sono due persone diverse che hanno utilizzato lo stesso identificativo, si deve eliminare da una delle entità l'identificativo comune e eliminare il collegamento.

Valore temporale dei collegamenti

I collegamenti sono il risultato di un'elaborazione automatica o manuale avvenuta in un certo momento, tuttavia solo per i collegamenti Peer creati automaticamente dal sistema viene registrato l'istante di creazione del collegamento, ovvero quando c'è stata la prima relazione tra le entità.

In questo modo è possibile selezionare un periodo di analisi per vedere quando si sono create certe relazioni.

Per gli altri collegamenti, una volta che sono stati creati (automaticamente o manualmente) per il sistema risultano come presenti da sempre.

Cose da sapere sulle entità Gruppo

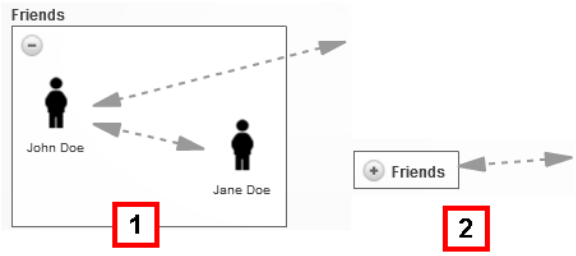
Introduzione

L'entità Gruppo raggruppa altre entità e può essere creata in automatico dal sistema o manualmente dall'Analista.

Il Gruppo ha due stati di visualizzazione:

- espanso, per visualizzare tutte le entità che rappresenta e i loro collegamenti.
- ridotto, per occupare meno spazio e facilitare la visualizzazione delle altre entità. Vengono visualizzati i collegamenti da e verso il gruppo ma non i collegamenti interni al gruppo.

Esempio di Gruppo espanso **[1]** ed di Gruppo ridotto **[2].**



I Gruppi sono visualizzati solo nella vista dei collegamenti, *vedi "Gestione delle entità: vista dei collegamenti" a pagina 68* .

Entità Gruppo create dal sistema

Il sistema crea automaticamente un Gruppo solo quando rileva collegamenti tra entità Person o Target appartenenti a due operation diverse. In ognuna delle due operation crea un Gruppo assegnandogli il nome dell'altra operation.

Il Gruppo creato rappresenta la/le entità di tipo Person o Target di quell'operation che hanno un collegamento con le entità dell'operation che si sta analizzando.

Il Gruppo può essere espanso solo se si hanno i permessi per gestire anche l'operation cui le entità che rappresenta appartengono. Altrimenti, l'unico stato di visualizzazione possibile è quello ridotto.

Entità Gruppo create manualmente

L'Analista può raggruppare in un Gruppo qualsiasi tipo di entità, ma un'entità può appartenere a un solo Gruppo.

La creazione di un Gruppo può aiutare nell'elaborazione dei dati. Per esempio, si può decidere di creare un'entità Gruppo con nome "Famiglia Rossi" con le entità che rappresentano persone e luoghi associati alla Famiglia Rossi.

Cose da sapere su come lavora l'intelligence

Introduzione

L'intelligence supporta l'Analista nell'elaborazione delle evidence e dei dati dell'indagine.

Processo di intelligence

Fase	*Descrizione*
1	Il sistema crea un'operation nella sezione Intelligence quando viene aperta un'operation nella sezione Operations.
2	Il sistema crea un'entità Target quando viene creato un target nella sezione Operations.
3	Il sistema, sulla base delle evidence raccolte dai dispositivi dei target, crea collegamenti con le entità Target e crea nuove entità e collegamenti. NOTA: il sistema elabora le informazioni provenienti dai target di tutte le operation aperte.
4	L'Analista aggiunge entità per rappresentare persone, luoghi e pagine web che sospetta possano essere interessanti per l'indagine e inserisce dettagli.
5	Il sistema continua ad aggiornare le entità e i loro collegamenti sulla base di nuove evidence e delle informazioni inserite dall'Analista.
6	L'Analista interpreta e gestisce le entità e i loro collegamenti per proporre soluzioni per l'indagine. NOTA: l'Analista può impostare una regola di alerting per essere avvisato ogni volta che il sistema crea un'entità o un collegamento. *Vedi "Alert" a pagina 95* .

Criteri per la creazione automatica di collegamenti Know

Se le evidence indicano che...	Il sistema crea...
i target John e Paul hanno nella rubrica l'identificativo 003214567	• un'entità Person con l'identificativo 003214567 • un collegamento Know direzionale da John all'entità Person • un collegamento Know direzionale da Paul all'entità Person
il target John ha nella rubrica l'identificativo 003214567 del entità Target/Person Paul	un collegamento Know direzionale da John verso Paul

Criteri per la creazione automatica di collegamenti Peer con entità Target e Person

Se le evidence indicano che...	Il sistema crea...
i target John e Paul hanno comunicato con l'identificativo 003214567	• un'entità Person con l'identificativo 003214567 • un collegamento Peer direzionale da John all'entità Person • un collegamento Peer direzionale da Paul all'entità Person
il target John ha comunicato con l'entità Target/Person Paul	un collegamento Peer direzionale da John a Paul
il target John comunica spesso con l'identificativo 003214567	• un'entità Person con l'identificativo 003214567 • un collegamento Peer direzionale da John all'entità Person

Criteri per la creazione automatica di collegamenti Peer con entità Position

Se le evidence indicano che...	Il sistema crea...
i target John e Paul sono stati nello stesso momento in Times Square	• un'entità Position con le coordinate geografiche di Times Square • un collegamento Peer direzionale da John all'entità Position • un collegamento Peer direzionale da Paul all'entità Position
il target John è stato nel luogo associato all'entità Position Ufficio di John	un collegamento Peer direzionale da John all'entità Ufficio di John
il target John è spesso in Times Square	• un'entità Position con le coordinate geografiche di Times Square • un collegamento Peer direzionale da John all'entità Position

NOTA: per il sistema un target ha visitato un luogo se vi è rimasto almeno 15 minuti. Due target hanno visitato lo stesso luogo nello stesso momento se sono rimasti in quel luogo contemporaneamente per almeno 15 minuti.

Criteri per la creazione automatica di collegamenti Peer con entità Virtual

Se le evidence indicano che...	Il sistema crea...

il target John ha visitato l'URL www.secretplaces.com associata all'entità Virtual Secret places website	un collegamento Peer direzionale da John a Secret places website

Criteri per la creazione automatica di collegamenti Identity tra entità Target e Person

Se il sistema rileva che...	Il sistema crea...
l'entità Target/Person John ha tra i suoi identificativi 003214567 e anche l'entità Target/Person Paul ha tra i suoi identificativi 003214567	un collegamento Identity tra John e Paul

Criteri per la creazione automatica di collegamenti tra entità Target/Person di operation diverse

Se il sistema rileva che...	Il sistema crea...
sussistono le condizioni per creare un collegamento tra l'entità Target/Person John dell'operation Traffico di droga e l'entità Target/Person Paul dell'operation Traffico di armi	nell'operation Traffico di droga, • l'entità Gruppo Traffico di armi • un collegamento tra John e il Gruppo Traffico di armi nell'operation Traffico di armi, • l'entità gruppo Traffico di droga • un collegamento tra Paul e il Gruppo Traffico di droga

NOTA: i criteri per la creazione di un collegamento tra operation sono uguali a quelli per un collegamento all'interno dell'operation.

NOTA: se l'entità Gruppo è già stata creata a causa di una precedente relazione, viene creato solo il collegamento.

NOTA: il tipo e la direzionalità del collegamento creato sono determinati dalle stesse regole dei collegamenti tra entità della stessa operation.

Gestione delle operation sottoposte a intelligence

Per gestire le operation sottoposte a intelligence:	• sezione **Intelligence**

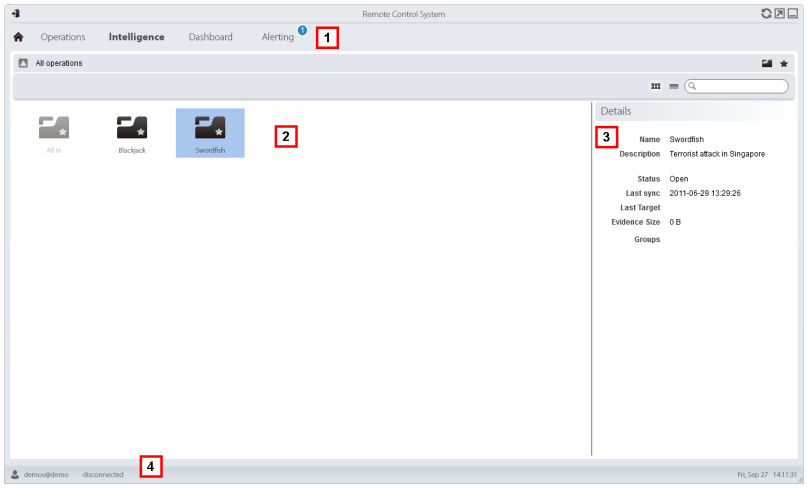
Scopo

Questa funzione permette di:

- visualizzare le operation sottoposte a intelligence

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area	*Descrizione*
1	Menu di RCS.
2	Elenco delle operation:  Operation aperta.  Tutte le operation. Mostra le entità di tutte le operation.
3	Dati dell'operation selezionata.
4	Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 12 .*

Visualizzare le entità di un'operation

Per visualizzare le entità di un'operation:

Passo	*Azione*
1	Fare doppio clic su un'operation: si apre la pagina per la gestione delle entità. *Vedi "Gestione delle entità: vista dei collegamenti" a pagina 68*

Gestione delle entità: vista a icone e vista tabellare

Per gestire le entità:	• sezione **Inteligence**, doppio-clic su una operation, fare clic su **Icon view** o **Table view**

Scopo

Questa funzione permette di:

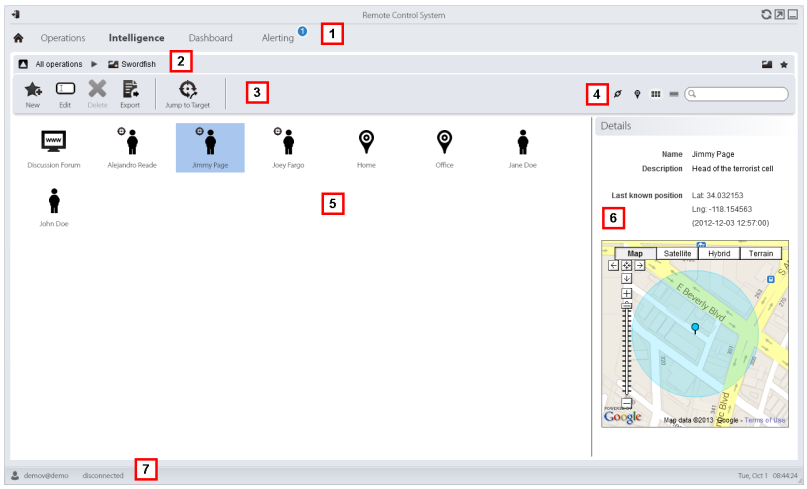
- visualizzare le entità di una operation
- gestire le entità di una operation
- aprire la pagina del target associato all'entità Target

NOTA: in assenza di licenza d'uso le uniche entità visualizzate e gestite sono le entità Target.

NOTA: La funzione è abilitata solo se si è in possesso dell'autorizzazione **Entity management**.

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area	*Descrizione*
1	Menu di RCS.
2	Barra di navigazione.
3	Barre con i pulsanti della finestra. Di seguito la descrizione:

Icona	*Funzione*
	Crea una nuova entità
	Modifica un'entità
	Elimina un'entità
	Esporta i dati dell'entità in formato `.html`
	Apre la pagina del target associato all'entità. *Vedi "**Pagina del target**" a pagina 25* .

Area	Descrizione
4	Pulsanti delle viste e casella di ricerca:

Oggetto	Descrizione
	Casella di ricerca. Inserendo parte del nome o della descrizione compare l'elenco delle entità che contengono le lettere inserite.
	Visualizza le entità in una tabella.
	Visualizza le entità come icone.
	Visualizza le entità Target e Position e i collegamenti tra loro su una mappa. *Vedi "**Gestione delle entità: vista delle Position**" a pagina 73*
	Visualizza le entità e i collegamenti tra loro in un grafico. *Vedi "**Gestione delle entità: vista dei collegamenti**" alla pagina successiva*

5	Elenco delle entità
6	Dati dell'entità selezionata.
7	Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 12* .

Per saperne di più su intelligence *vedi "**Cose da sapere sull'intelligence**" a pagina 56 vedi "**Cose da sapere sulle entità**" a pagina 56*

Visualizzare il dettaglio di una entità

Per visualizzare il dettaglio dell'entità:

Passo	Azione
1	Fare doppio clic su una entità: si apre la pagina del dettaglio: • *"**Dettaglio delle entità Target**" a pagina 77* . • *"**Dettaglio delle entità Person**" a pagina 83* . • *"**Dettaglio delle entità Position**" a pagina 85* . • *"**Dettaglio delle entità Virtual**" a pagina 87* .

Gestione delle entità: vista dei collegamenti

Per gestire le entità sottoposte a intelligence:	• sezione **Inteligence**, doppio-clic su una operation, fare clic su **Link View**

Scopo

Questa funzione permette di:

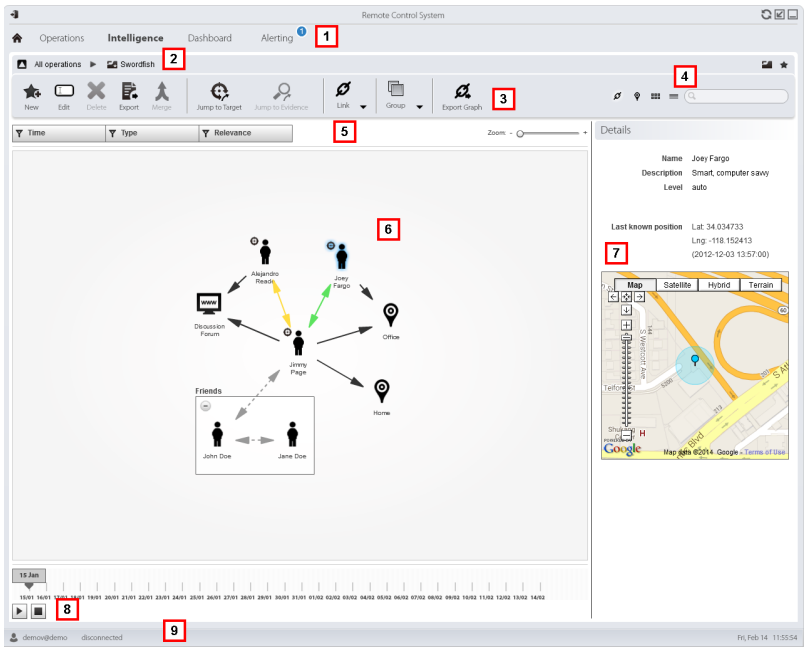
- visualizzare in un grafico le entità di un'operation e i loro collegamenti all'interno dell'operation o con altre operation
- gestire le entità
- gestire i collegamenti tra entità
- aprire la pagina del target associato all'entità Target
- aprire le evidence corrispondenti a un collegamento
- visualizzare in modo dinamico le evidence corrispondenti ai collegamenti tra le entità

NOTA: questa funzione è sottoposta a licenza d'uso. In assenza di licenza, la vista di default delle entità di una operation è la vista a icone, *vedi "**Gestione delle entità: vista a icone e vista tabellare**" a pagina 65* .

NOTA: questa funzione è abilitata solo se si è in possesso dell'autorizzazione **Entity management**.

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area	*Descrizione*
1	Menu di RCS.
2	Barra di navigazione.

Area	*Descrizione*
3	Barre con i pulsanti della finestra. Di seguito la descrizione:

Icona	*Funzione*
	Crea una nuova entità
	Modifica una entità
	Elimina un'entità
	Esporta i dati dell'entità in formato `.html`
	Unisce due entità
	Apre la pagina del target associato all'entità. *Vedi "**Pagina del target**" a pagina 25* .
	Apre le evidence corrispondenti al collegamento selezionato. *Vedi "**Analisi delle evidence (Evidence)**" a pagina 38*
	 : crea un collegamento  : modifica un collegamento  : elimina un collegamento : applica un grado di importanza al collegamento
	 : crea un'entità Gruppo  : elimina un'entità Gruppo
	Esporta il grafico dell'entità in formato `.graphml`

Area	*Descrizione*
4	Pulsanti delle viste e casella di ricerca:

Oggetto	*Descrizione*
	Casella di ricerca. Inserendo parte del nome o della descrizione compare l'elenco delle entità che contengono le lettere inserite.
	Visualizza le entità in una tabella. *Vedi "**Gestione delle entità: vista a icone e vista tabellare**" a pagina 65*
	Visualizza le entità come icone. *Vedi "**Gestione delle entità: vista a icone e vista tabellare**" a pagina 65*
	Visualizza le entità Target e Position e i collegamenti tra loro su una mappa. *Vedi "**Gestione delle entità: vista delle Position**" a pagina 73*
	Visualizza le entità e i collegamenti tra loro in un grafico.

5 Area dei filtri

6 Grafico delle entità e dei collegamenti in base ai filtri impostati

NOTA: il collegamenti Know, Identity e i collegamenti creati manualmente sono sempre visualizzati a prescindere dal periodo selezionato.

NOTA: al centro del grafico viene posizionata l'entità con più collegamenti.

7 Dati dell'entità selezionata.

8 Comando per visualizzare dinamicamente la quantità, la direzione e la frequenza delle evidence che definiscono i collegamenti tra le entità visualizzate nel grafico in base ai filtri impostati.

9 Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 12* .

Per saperne di più su intelligence *vedi "**Cose da sapere sull'intelligence**" a pagina 56 vedi "**Cose da sapere sulle entità**" a pagina 56*

Visualizzare il dettaglio di una entità

Per visualizzare il dettaglio dell'entità:

Passo	*Azione*
1	Fare doppio clic su una entità: si apre la pagina del dettaglio. • *"**Dettaglio delle entità Target**" a pagina 77 .* • *"**Dettaglio delle entità Person**" a pagina 83 .* • *"**Dettaglio delle entità Position**" a pagina 85 .* • *"**Dettaglio delle entità Virtual**" a pagina 87 .*

Unire due entità in una entità

Per unire due entità in una entità:

Passo	*Azione*
1	Selezionare le due entità tenendo premuto il tasto **Ctrl** della tastiera. NOTA: possono essere unite solo un'entità Target con un'entità Person o due entità Person.
2	Fare clic su **Merge** **Risultato:** nel grafico è visualizzata un'entità con nome e descrizione della prima entità selezionata e i dettagli di entrambe. NOTA: se si unisce un'entità Target e un'entità Person, rimane l'entità Target con anche i dettagli dell'entità Person.

Creare un collegamento tra due entità

Per creare un collegamento tra due entità:

Passo	*Azione*
1	Selezionare le due entità tenendo premuto il tasto **Ctrl** della tastiera.
2	Selezionare la direzione, il tipo e il grado di importanza del collegamento e fare clic su **Save.** **Risultato**: il collegamento viene visualizzato nel grafico

Creare un Gruppo

Per creare un Gruppo:

Passo	*Azione*
1	Selezionare le entità che si vogliono raggruppare tenendo premuto il tasto **Ctrl** della tastiera.
2	Fare clic su **Gruppo, Gruppo.** **Risultato**: il Gruppo viene visualizzato nel grafico.

Visualizzare dinamicamente le evidence dei collegamenti tra le entità

Per visualizzare dinamicamente le evidence dei collegamenti tra le entità:

Passo	*Azione*
1	Controllare che sulla mappa le entità visualizzate e il periodo selezionato siano quelli desiderati. Utilizzare i filtri per impostare quanto desiderato.
2	Fare clic su **Play** per attivare la visualizzazione. **Risultato**: sui collegamenti scorrono sotto forma di pallini rossi le evidence raccolte. NOTA: la direzione di scorrimento del pallino indica la direzione dell'evidence (es.: il pallino rosso va dall'entità John all'entità Paul se John ha scritto una e-mail a Paul). NOTA: il numero di pallini indica la quantità di evidence: un pallino indica che sono state raccolte meno di 10 evidence, due pallini tra 10 e 50 evidence, tre pallini se sono state raccolte più di 50 evidence. NOTA: se quel giorno il collegamento è stato creato, viene visualizzato sulla mappa in corrispondenza di quel giorno.
3	Fare clic su **Stop** per interrompere la visualizzazione.

Gestione delle entità: vista delle Position

Per gestire le entità sottoposte a intelligence:	• sezione **Inteligence**, doppio-clic su una operation, fare clic su **Position view**

Scopo

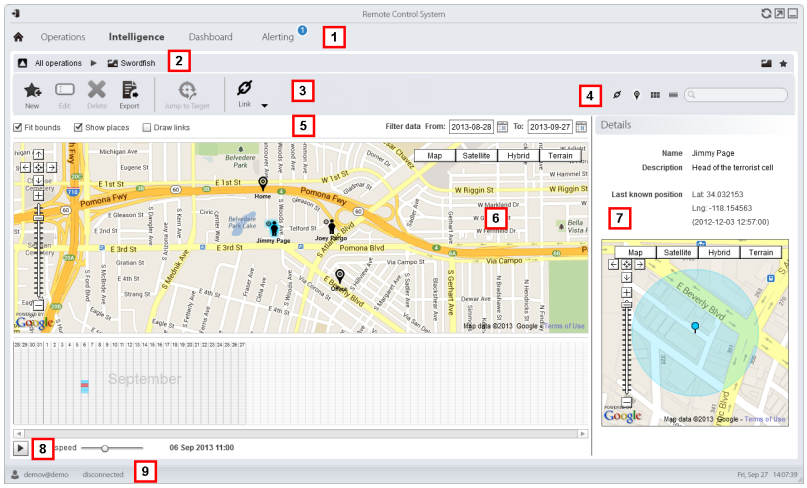
Questa funzione permette di:

- visualizzare su una mappa le entità Target e le entità Position di una operation e i loro collegamenti
- gestire le entità Target e Position
- gestire i collegamenti tra entità Target e Position
- aprire la pagina del target associato all'entità Target
- aprire le evidence corrispondenti a un collegamento
- visualizzare in modo dinamico gli spostamenti delle entità Target

NOTA: questa funzione è sottoposta a licenza d'uso e è abilitata solo se si è in possesso dell'autorizzazione **Entity management**.

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area	*Descrizione*
1	Menu di RCS.
2	Barra di navigazione.

Area	*Descrizione*

3 Barre con i pulsanti della finestra. Di seguito la descrizione:

Icona	*Funzione*
	Crea una nuova entità
	Modifica una entità
	Elimina un'entità
	Esporta i dati dell'entità in formato `.html`
	Apre la pagina del target associato all'entità. *Vedi "**Pagina del target**" a pagina 25* .
	Apre le evidence corrispondenti al collegamento selezionato. *Vedi "**Analisi delle evidence (Evidence)**" a pagina 38*
	 : crea un collegamento  : modifica un collegamento  : elimina un collegamento : applica un grado di importanza al collegamento

4 Pulsanti delle viste e casella di ricerca:

Oggetto	*Descrizione*
	Casella di ricerca. Inserendo parte del nome o della descrizione compare l'elenco delle entità che contengono le lettere inserite.
	Visualizza le entità in una tabella. *Vedi "**Gestione delle entità: vista a icone e vista tabellare**" a pagina 65* .
	Visualizza le entità come icone. *Vedi "**Gestione delle entità: vista a icone e vista tabellare**" a pagina 65* .
	Visualizza le entità Target e Position e i collegamenti tra loro su una mappa.
	Visualizza le entità e i collegamenti tra loro in un grafico. *Vedi "**Gestione delle entità: vista dei collegamenti**" a pagina 68* .

Area	*Descrizione*
5	Area dei filtri
6	Mappa delle entità e dei collegamenti in base ai filtri impostati. NOTA: l'entità Target è posizionata nell'ultima posizione acquisita nel periodo selezionato. NOTA: i collegamenti creati manualmente sono sempre visualizzati a prescindere dal periodo selezionato.
7	Dati dell'entità selezionata.
8	Comando per visualizzare gli spostamenti delle entità Target in base ai filtri impostati.
9	Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 12* .

Per saperne di più su intelligence *vedi "**Cose da sapere sull'intelligence**" a pagina 56 vedi "**Cose da sapere sulle entità**" a pagina 56*

Visualizzare il dettaglio di una entità

Per visualizzare il dettaglio dell'entità:

Passo	*Azione*
1	Fare doppio clic su una entità: si apre la pagina del dettaglio. • *"**Dettaglio delle entità Target**" nella pagina di fronte* . • *"**Dettaglio delle entità Person**" a pagina 83* . • *"**Dettaglio delle entità Position**" a pagina 85* .

Creare un collegamento tra due entità

Per creare un collegamento tra due entità:

Passo	*Azione*
1	Selezionare un'entità Target e un'entità Position tenendo premuto il tasto **Ctrl** della tastiera.

Passo	*Azione*
2	Selezionare il grado di importanza e fare clic su **Save.** **Risultato**: il collegamento viene visualizzato nel grafico.

Visualizzare dinamicamente gli spostamenti dei target

Per gestire la visualizzazione dinamica degli spostamenti dei target:

Passo	*Azione*
1	Controllare che sulla mappa le entità visualizzate e il periodo selezionato siano quelli desiderati. Utilizzare i filtri per impostare quanto desiderato.
2	Fare clic su **Play** per attivare la visualizzazione. **Risultato**: le entità Target visualizzate sulla mappa si muovono ripercorrendo gli spostamenti registrati nelle evidence. NOTA: se nel periodo selezionato non esistono evidence relative alla posizione del target, l'entità Target rimane posizionata nell'ultima posizione acquisita ma la sua icona sbiadisce piano piano fino a scomparire o a comparire nella successiva posizione registrata.
3	Fare clic su **Stop** per interrompere la visualizzazione.

Dettaglio delle entità Target

Per vedere il dettaglio di un'entità:	• sezione **Intelligence,** doppio-clic su una operation, doppio-clic su una entità **Target**

Scopo

Questa funzione permette di:

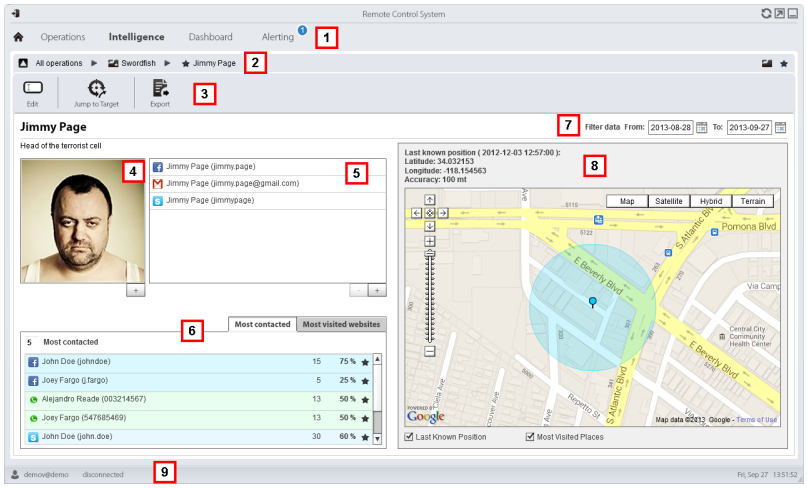
- visualizzare le informazioni di dettaglio dell'entità Target elaborate dal sistema
- aggiungere informazioni di dettaglio dell'entità Target
- creare nuove entità in collegamento con l'entità Target

NOTA: alcune informazioni di dettaglio e alcune azioni sono abilitate solo con licenza d'uso.

NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Entity management**.

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area	*Descrizione*
1	Menu di RCS.
2	Barra di navigazione.
3	Barre con i pulsanti della finestra. Di seguito la descrizione:

Icona	*Funzione*
	Modifica i dati dell'entità.
	Esporta i dati dell'entità in formato `.html`
	Apre la pagina del target associato all'entità. *Vedi "**Pagina del target**" a pagina 25 .*

4	Foto del target associato all'entità. Di default è la prima immagine catturata dalla webcam.
5	Elenco identificativi del target individuati dalle evidence o aggiunti manualmente.

Area	*Descrizione*
6	Tabelle con le persone più contattate e i siti web più visitati in base al periodo selezionato. Con doppio clic si apre la pagina delle evidence corrispondenti a quel dato.
7	Periodo di interesse per la ricerca.
8	Mappa con indicati: • ultima posizione acquisita del target, • luoghi più visitati nel periodo selezionato, • luoghi visitati dal target inseriti manualmente.
9	Barra di stato RCS

Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 12* .

Per saperne di più su intelligence *vedi "**Cose da sapere sull'intelligence**" a pagina 56 vedi "**Cose da sapere sulle entità**" a pagina 56*

Aggiungere la foto del target

Per aggiungere la foto:

Passo	*Azione*
1	• Fare clic su **+** e selezionare una foto oppure • dalla pagina delle **Evidence** entrare nel dettaglio di una evidence webcam e selezionare l'immagine **Risultato**: l'immagine selezionata diventa l'immagine di default.

Aggiungere identificativi del target

Per aggiungere identificativi:

Passo	*Azione*
1	Fare clic su **+** e inserire i dati.  NOTA: il campo **Account** corrisponde al vero e proprio identificativo del target (es.: john.john@email.com); il campo **Nome** a un nominativo facoltativo da associare all'identificativo (es.: John). **Risultato:** viene aggiunto l'identificativo all'elenco.

Visualizzare le persone contattate frequentemente

Per visualizzare le persone contattate frequentemente:

Passo	*Azione*
1	Selezionare il periodo di interesse.
2	Nella casella di testo accanto a **Most contacted** inserire la quantità di persone per tipo di mezzo di comunicazione che si vogliono visualizzare.
3	Premere **Invio** sulla tastiera. **Risultato**: nella tabella vengono riportate le informazioni relative alle persone più contattate nel periodo selezionato, *vedi "Dati del dettaglio delle entità Target" a pagina 82*

Visualizzare i siti web visitati frequentemente

Per visualizzare i siti web visitati frequentemente:

Passo	*Azione*
1	Selezionare il periodo di interesse.
2	Nella casella di testo accanto a **Most visited websites** inserire il numero di siti web che si vogliono visualizzare.
3	Premere **Invio** sulla tastiera. **Risultato**: nella tabella vengono riportate le informazioni relative ai siti web più visitati nel periodo selezionato, *vedi "Dati del dettaglio delle entità Target" a pagina 82*

Collegare l'entità Target a una persona contattata frequentemente

Per collegare l'entità Target a una persona contattata frequentemente:

Passo	*Azione*
1	Nella tabella **Most Contacted** fare clic su **Add as Entity** della riga desiderata e inserire i dati. **Risultato** : viene aggiunta all'elenco delle entità dell'operation un'entità Person con l'identificativo selezionato e con un collegamento Peer con l'entità Target. NOTA: il risultato è lo stesso se si crea manualmente un'entità Person con l'identificativo della tabella e si aggiunge un collegamento Peer tra l'entità Target e l'entità creata.

Collegare il target a un sito web visitato frequentemente

Per collegare il target a un sito web visitato frequentemente:

Passo	*Azione*
1	Nella tabella **Most visited websites** fare clic su **Add as Entity** della riga desiderata e inserire i dati. **Risultato** : viene aggiunta all'elenco delle entità dell'operation un'entità Virtual con l'URL selezionato e con un collegamento Peer con l'entità Target. NOTA: il risultato è lo stesso se si crea manualmente un'entità Virtual con l'indirizzo URL della tabella e si aggiunge un collegamento Peer tra l'entità Target e l'entità creata.

Visualizzare l'ultima posizione acquisita

Per visualizzare sulla mappa l'ultima posizione del target:

Passo	*Azione*
1	Selezionare la casella di controllo **Last position.** **Risultato**: un segnalino blu indica la posizione corrispondente.

Visualizzare i luoghi più visitati

Per visualizzare sulla mappa i luoghi più visitati:

Passo	*Azione*
1	Selezionare la casella di controllo **Most visited places.** **Risultato**: le posizioni più visitate vengono visualizzate sulla mappa con segnalini rossi.

Aggiungere un'entità Position visitata dal target

Per aggiungere manualmente un'entità Position visitata dal target:

Passo	*Azione*
1	Nella mappa, fare clic su **+** e inserire i dati. Suggerimento: inserire un **Nome** e una **Descrizione** significative che aiutino a ricordare la relazione tra il target e il luogo. **Risultato:** viene aggiunta all'elenco delle entità dell'operation un'entità Position con un collegamento Peer con l'entità Target. NOTA: il risultato è lo stesso se si crea manualmente un'entità Position e si aggiunge un collegamento Peer tra l'entità Target e l'entità creata.

Dati del dettaglio delle entità Target

Tabella delle persone più contattate

Di seguito la descrizione dei dati riportati nella tabella delle persone più contattate dal target:

Dato	*Descrizione*
prima colonna	icona del mezzo di comunicazione utilizzato e identificativo della persona.
seconda colonna	quantità di contatti del target con la persona nel periodo selezionato.
terza colonna	percentuale di comunicazione del target con la persona nel periodo selezionato. NOTA: il calcolo viene fatto per mezzo di comunicazione e considerando i contatti visualizzati.
★	pulsante per creare un'entità Person con quell'identificativo e creare un collegamento Peer con l'entità Target.

Tabella dei siti web più visitati

Di seguito la descrizione dei dati riportati nella tabella dei siti web più visitati:

Dato	*Descrizione*
prima colonna	indirizzo URL del sito web visitato.
seconda colonna	quantità di visite del target al sito web nel periodo selezionato.
terza colonna	percentuale di visita del target al sito web nel periodo selezionato. NOTA: il calcolo viene fatto considerando i siti web visualizzati.
	pulsante per creare un'entità Virtual con quell'indirizzo URL e creare un collegamento Peer con l'entità Target.

Dettaglio delle entità Person

Per vedere il dettaglio di un'entità:	• sezione **Intelligence,** doppio-clic su una operation, doppio-clic su una entità **Person**

Scopo

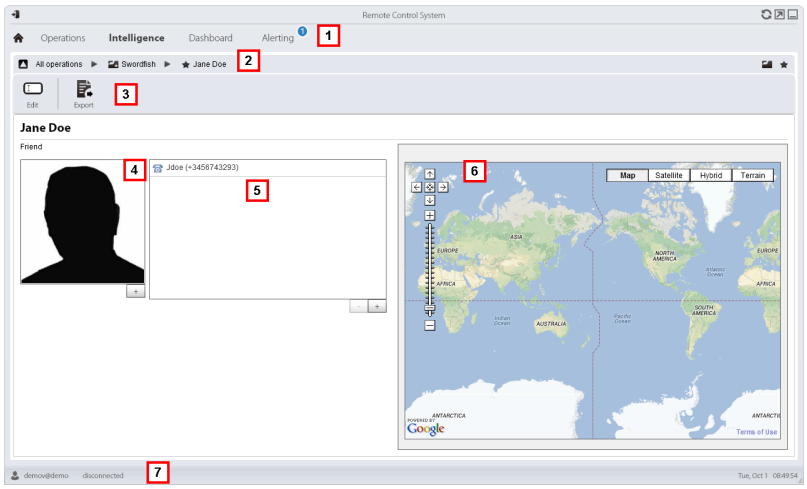
Questa funzione permette di:

- visualizzare le informazioni di dettaglio dell'entità Person
- aggiungere informazioni di dettaglio dell'entità Person
- creare entità Position in collegamento con l'entità Person

NOTA: questa funzione è sottoposta a licenza d'uso e è abilitata solo se si è in possesso dell'autorizzazione **Entity management**.

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area	*Descrizione*
1	Menu di RCS.
2	Barra di navigazione.
3	Barre con i pulsanti della finestra. Di seguito la descrizione:

Icona	*Funzione*
	Modifica i dati dell'entità.
	Esporta i dati dell'entità in formato `.html`

4	Foto della persona associata all'entità.
5	Elenco identificativi della persona associata all'entità.
6	Mappa con indicate le posizioni collegate all'entità.
7	Barra di stato RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 12 .*

Per saperne di più su intelligence *vedi "**Cose da sapere sull'intelligence**" a pagina 56 vedi "**Cose da sapere sulle entità**" a pagina 56*

Aggiungere un'immagine della persona

Per aggiungere un'immagine:

Passo	*Azione*
1	Fare clic su **+** e selezionare una immagine. **Risultato:** l'immagine selezionata diventa l'immagine di default.

Aggiungere degli identificativi della persona

Per aggiungere identificativi:

Passo	*Azione*
1	Fare clic su **+** e inserire i dati. NOTA: il campo **Account** corrisponde al vero e proprio identificativo della persona (es. john.john@email.com); il campo **Nome** a un nominativo facoltativo da associare all'identificativo (es. John). **Risultato:** viene aggiunto l'identificativo all'elenco.

Aggiungere un'entità Position visitata dall'entità

Per aggiungere manualmente un'entità Position visitata dall'entità:

Passo	*Azione*
1	Nella mappa, fare clic su **+** e inserire i dati. Suggerimento: inserire un **Nome** e una **Descrizione** significative che aiutino a ricordare la relazione tra la persona e il luogo. **Risultato:** viene aggiunta all'elenco delle entità dell'operation un'entità Position con un collegamento Peer con l'entità Person. NOTA: il risultato è lo stesso se si crea manualmente un'entità Position e si aggiunge un collegamento Peer tra l'entità Person e l'entità creata.

Dettaglio delle entità Position

Per vedere il dettaglio di un'entità:	• sezione **Intelligence,** doppio-clic su una operation, doppio-clic su una entità **Position**

Scopo

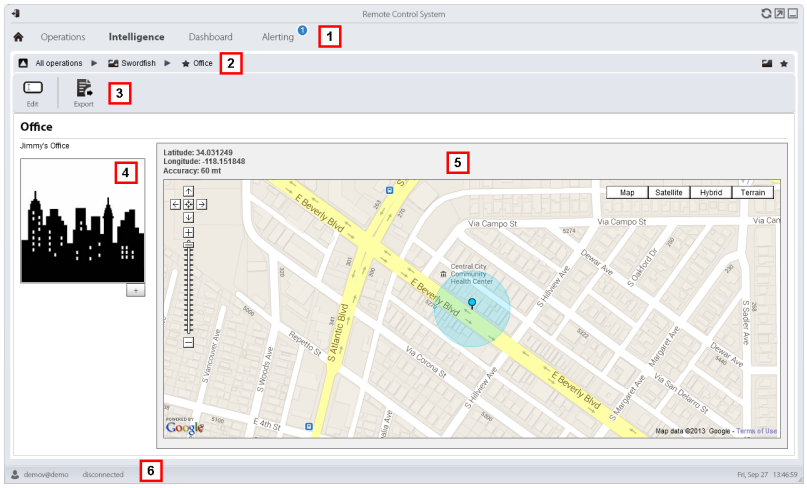
Questa funzione permette di:

- visualizzare le informazioni di dettaglio dell'entità Position
- aggiungere una foto del luogo associato all'entità

NOTA: questa funzione è sottoposta a licenza d'uso e è abilitata solo se si è in possesso dell'autorizzazione **Entity management**.

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area	*Descrizione*
1	Menu di RCS.
2	Barra di navigazione.
3	Barre con i pulsanti della finestra. Di seguito la descrizione:

Icona	*Funzione*
	Modifica i dati dell'entità.
	Esporta i dati dell'entità in formato `.html`

4	Foto del luogo associato all'entità.

Area	*Descrizione*
5	Mappa con indicato il luogo associato all'entità.
6	Barra di stato RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 12 .*
Per saperne di più su intelligence *vedi "**Cose da sapere sull'intelligence**" a pagina 56 .*

Aggiungere un'immagine del luogo

Per aggiungere un'immagine:

Passo	*Azione*
1	Fare clic su **+** e selezionare un'immagine. **Risultato:** l'immagine selezionata diventa l'immagine di default.

Dettaglio delle entità Virtual

Per vedere il dettaglio di un'entità:	• sezione **Intelligence,** doppio-clic su una operation, doppio-clic su una entità **Virtual**

Scopo

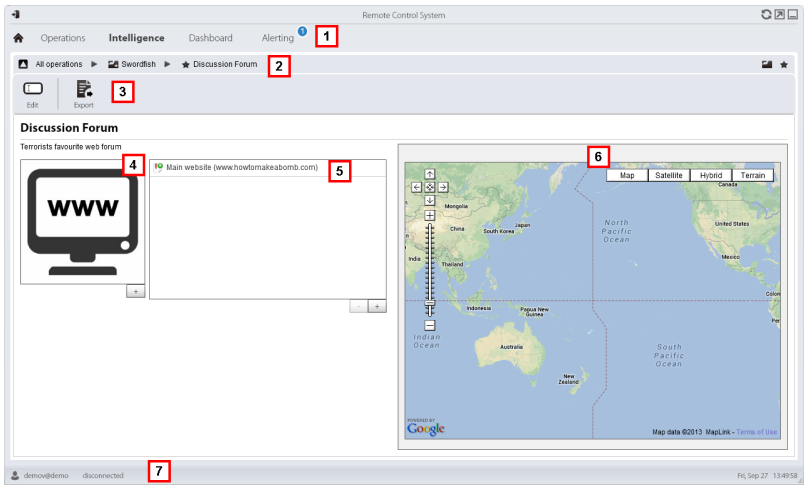
Questa funzione permette di:

- visualizzare le informazioni di dettaglio dell'entità Virtual
- aggiungere informazioni di dettaglio dell'entità Virtual

NOTA: questa funzione è sottoposta a licenza d'uso e è abilitata solo se si è in possesso dell'autorizzazione **Entity management**.

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area	*Descrizione*
1	Menu di RCS.
2	Barra di navigazione.
3	Barre con i pulsanti della finestra. Di seguito la descrizione:

Icona	*Funzione*
	Modifica i dati dell'entità.
	Esporta i dati dell'entità in formato `.html`

4	Immagine del contenuto dell'indirizzo associato all'entità.
5	Elenco indirizzi web associati all'entità.
6	Mappa con indicata la posizione corrispondente all'indirizzo web individuata automaticamente dal sistema tramite l'indirizzo IP.
7	Barra di stato RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 12* .

Per saperne di più su intelligence *vedi "**Cose da sapere sull'intelligence**" a pagina 56 vedi "**Cose da sapere sulle entità**" a pagina 56*

Aggiungere un'immagine dell'indirizzo web

Per aggiungere immagini:

Passo	*Azione*
1	Fare clic su **+** e selezionare un'immagine. **Risultato**: l'immagine selezionata diventa l'immagine di default.

Aggiungere indirizzi web all'entità

Per aggiungere indirizzi web all'entità:

Passo	*Azione*
1	Fare clic su **+** e inserire i dati. **Risultato:** viene aggiunto l'indirizzo all'elenco.

8

Monitoraggio delle attività dei target con la Dashboard

Presentazione

Introduzione

La Dashboard facilita il controllo delle attività degli agent connessi e del flusso di prove in arrivo.

Contenuti

Questa sezione include i seguenti argomenti:

Cose da sapere sulla Dashboard

Componenti della Dashboard

La Dashboard è composta da uno o più elementi scelti a discrezione dell'utente tra:

- operation
- target
- agent

Ogni elemento mostra il totale delle evidence raccolte. I valori sono aggiornati a ogni sincronizzazione:

- **Numero rosso**: quantità di evidence ricevute all'ultima sincronizzazione.
- **Numero nero**: quantità di evidence ricevute a partire dal momento del login.

Esempio	*Descrizione*
Evidence dell'operation: 	Compaiono i target dell'operation e la quantità di evidence per target.
Evidence del target: 	Compaiono le evidence del target e la quantità di evidence per ogni tipo.
Evidence dell'agent: 	Compaiono le evidence dell'agent e la quantità di evidence per ogni tipo.

NOTA: l'assenza dei numeri, indica che, dal momento della login, non sono ancora arrivate evidence.

Per vedere l'elenco completo dei tipi di evidence *vedi "Elenco dei tipi di evidence" a pagina 49* .

Processo di segnalazione delle evidence

Di seguito la descrizione del processo di segnalazione delle evidence:

Fase	*Descrizione*
1	L'Analista aggiunge alla propria Dashboard gli elementi operation, target o agent di cui vuole controllare le evidence.
2	Alla successiva sincronizzazione di ogni agent, il sistema aggiorna i contatori se riceve evidence.
3	L'Analista controlla le evidence più recenti quelle indicate dal numero rosso. Se ne vuole vedere il dettaglio fa clic sopra l'icona corrispondente.
4	All'uscita della sessione corrente il sistema azzera i numeri.

Monitoraggio delle evidence (Dashboard)

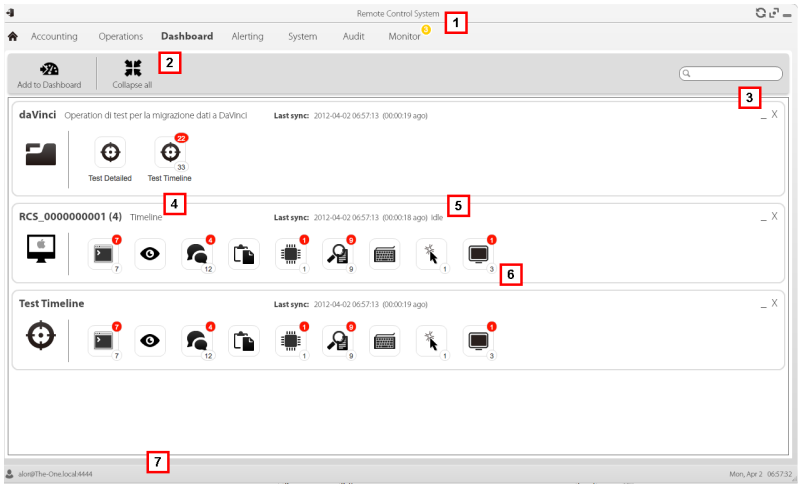
Per controllare la ricezione delle evidence:	• sezione **Dashboard**

Scopo

La Dashboard permette di tenere sotto controllo certe operation, target o agent e vedere le evidence che arrivano. È completamente configurabile. Per esempio è possibile costruire una Dashboard per controllare solo alcuni dispositivi del target.

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area	*Descrizione*
1	Menu di RCS.
2	Barre con i pulsanti della finestra. Di seguito la descrizione:

Icona	*Descrizione*
	Aggiunge un nuovo elemento da controllare.
	Comprime o espande i riquadri di tutti gli elementi della Dashboard.
	

3	Pulsanti per minimizzare o eliminare l'elemento dalla dashboard.
4	Nome e descrizione di un elemento della Dashboard.
5	Data dell'ultima sincronizzazione dell'elemento. **In progress**: sincronizzazione in corso. **Idle**: sincronizzazione non in corso
6	Evidence recentemente acquisite in una operation, target o agent.
7	Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 12* .

Per saperne di più sulla Dashboard *vedi "**Cose da sapere sulla Dashboard**" a pagina 91* .

Aggiungere un elemento alla Dashboard

Per aggiungere un nuovo elemento alla Dashboard:

Passo	*Azione*
1	Fare clic su **Add to Dashboard**: si apre la finestra per la ricerca degli elementi da aggiungere.
2	Digitare parte del nome o descrizione dell'elemento da aggiungere: compare l'elenco degli elementi corrispondenti alla ricerca.

Passo	*Azione*
3	• Selezionare l'elemento dall'elenco: l'elemento è automaticamente aggiunto alla Dashboard e la finestra di ricerca rimane aperta per una nuova ricerca. • Ripetere i passi 2 e 3 fino a quando sono stati inseriti tutti gli elementi desiderati.
5	Una volta terminato l'inserimento degli elementi, fare clic su ✖ per chiudere la finestra di ricerca e tornare alla Dashboard.

Visualizzare una evidence segnalata nella Dashboard

Per visualizzare una evidence della Dashboard

NOTA: facendo clic su un target o un'operation si apre l'area di lavoro dell'oggetto selezionato, da dove l'Analista può aprire gli agent desiderati.

Passo	*Azione*
1	Per l'elemento operation: • fare doppio clic sul target: si apre la pagina del target. *Vedi "**Pagina del target**" a pagina 25* . Per l'elemento target: • fare doppio clic sull'agent: si apre la pagina dell'agent. *Vedi "**Pagina dell'agent**" a pagina 30* . Per l'elemento agent: • fare doppio clic sul tipo di evidence: si apre la pagina delle evidence. *Vedi "**Analisi delle evidence (Evidence)**" a pagina 38*

9

Alert

Presentazione

Introduzione

Gli alert segnalano la ricezione di evidence, la sincronizzazione di agent o la creazione automatica da parte del sistema di entità e collegamenti tra entità. Inoltre, permettono di marcare automaticamente le evidence e i collegamenti per l'analisi e l'export.

Contenuti

Questa sezione include i seguenti argomenti:

Cose da sapere sugli alert

Cosa sono gli alert

In fase investigativa può essere utile venire "allertati" in tempo reale tramite e-mail o tramite una notifica in RCS Console, di avvenimenti particolari che riguardano il target.

È possibile essere allertati quando:

- arrivano nuove evidence
- avvengono sincronizzazioni con l'agent
- vengono create automaticamente entità e collegamenti tra entità (intelligence)

Per esempio, se da tempo si sta attendendo l'arrivo di prove da un target, si può creare una regola di alert che invii una e-mail e registri un log a ogni prova ricevuta. In questo modo si viene notificati immediatamente quando il target riprende le proprie attività. Successivamente si può disabilitare la regola e semplicemente consultare le evidence mano a mano che arrivano.

Oppure, se si usa l'intelligence, può essere utile venire "allertati" quando viene creato un collegamento a una particolare entità o una nuova entità nell'operation.

Le regole di alert

Le regole di alert definiscono quindi per quali eventi essere allertati. Possono essere usate anche per assegnare automaticamente a evidence o a collegamenti di intelligence dei gradi di importanza, utilizzabili in fase di analisi.

Ambito di applicazione delle regole di alert

Le regole che avvisano dell'arrivo di una evidence possono essere create a livello di:

- **Operation**: tutte le evidence di tutti i target dell'operation
- **Target**: tutte le evidence di tutti gli agent del target
- **Agent**: tutte le evidence dell'agent

Le regole che avvisano della creazione automatica di un'entità di intelligence possono essere create a livello di:

- **Operation**: avvisa se è creata un'entità per quell'operation

Le regole che avvisano della creazione automatica di un collegamento di intelligence possono essere create a livello di:

- **Operation**: avvisa se è creato un collegamento per qualsiasi delle entità dell'operation
- **Entità**: avvisa se è creato un collegamento per quell'entità

NOTA: ogni utente sarà avvisato in base alle proprie regole impostate.

Processo di alert

Di seguito la descrizione del processo di alert:

NOTA: l'invio di e-mail è opzionale.

Fase	*Descrizione*
1	L'Analista crea delle regole per essere avvisato dell'arrivo di evidence particolari, di sincronizzazioni dell'agent o di creazioni automatiche di entità o collegamenti di intelligence. Le regole registrano gli alert, le notificano all'interno di RCS Console e le inviano via e-mail (opzionale).
2	Il sistema intercetta le evidence in arrivo o analizza l'elemento che sta creando e li confronta con le regole di alert.

Se la prova...	*Allora...*
corrisponde a una regola di alert	il sistema registra la prova come *evidence* o aggiunge l'entità o il collegamento all'operation e genera un alert che applica automaticamente il grado di importanza scelto. Opzionalmente viene inviata dal sistema un'e-mail di notifica.
non corrisponde a una regola di alert	il sistema registra la prova come *evidence* o aggiunge l'entità o il collegamento all'operation senza generare alert.

3	L'Analista riceve una e-mail di alert (se la regola di alert lo prevede) e controlla le registrazioni degli alert. Da un alert naviga direttamente nelle evidence che l'hanno generata o all'entità creata o alla vista dei collegamenti.
4	Terminato il controllo, l'Analista elimina le registrazioni di alert.

Alerting

Per ricevere alert dal target:	• sezione **Alerting**

Scopo

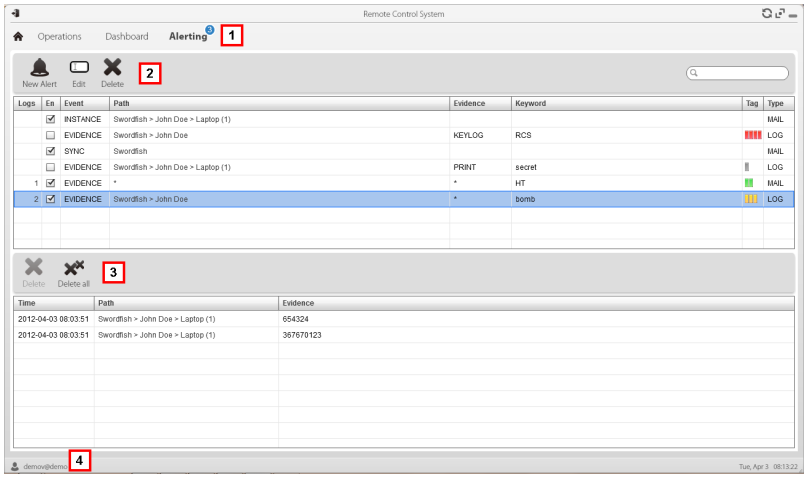
Questa funzione permette di:

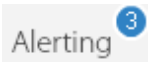
- ricevere alert quando un certo tipo di evidence sono intercettate, quando il dispositivo del target si sincronizza con RCS o quando l'intelligence crea automaticamente entità o collegamenti tra entità.

- marcare automaticamente le evidence o i collegamenti dell'intelligence per importanza, per facilitare l'analisi successiva.
- controllare tutti gli alert registrati e navigare direttamente all'evento che li hanno generati.

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area	*Descrizione*
1	Menu di RCS.  : indica la quantità di alert ricevuti . Il contatore viene azzerato automaticamente dopo due settimane, oppure quando si eliminano le notifiche.

Area	*Descrizione*
2	Barra con i pulsanti dedicati alle regole di alert. Di seguito la descrizione:

Icona	*Descrizione*
	Crea una nuova regola di alert.  NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Alerts creation**.
	Modifica la regola di alert selezionata.
	Elimina la regola di alert selezionata.  ***PRUDENZA: tutte le notifiche generate sono rimosse.***

3	Barra con i pulsanti dedicati alle registrazioni degli alert. Di seguito la descrizione:

Icona	*Descrizione*
	Elimina la registrazione di alert selezionata.
	Elimina tutte le registrazioni di alert.

4	Menu di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 12* .

Per la descrizione dei dati presenti sulla finestra *vedi "**Dati degli alert** " a pagina 101*

Per saperne di più sugli alert*vedi "**Cose da sapere sugli alert**" a pagina 96* .

Aggiungere regola per essere allertati

Per essere allertati occorre impostare una regola:

Passo	*Azione*
1	Fare clic su **New Alert**: compaiono i dati da compilare.

Passo	*Azione*
2	• Compilare i dati richiesti indicando in **Type** la modalità con cui si vuole essere allertati. • Selezionare la casella **Enabled** se si desidera che la regola sia già attiva.
3	Fare clic su **Save**: nell'area di lavoro principale compare la nuova regola di alert. Non appena il sistema registra un evento che corrisponde alla regola, invia l'alert.

Modificare una regola di alert

Per modificare una regola di alert:

Passo	*Azione*
1	Selezionare la regola di alert da modificare Fare clic su **Edit**: compaiono i dati da modificare.
2	• Modificare i dati. • Selezionare la casella **Enabled** se si desidera che la regola sia attiva da subito.
3	Fare clic su **Save**: nell'area di lavoro principale compare la nuova regola di alert. Non appena il sistema registra un evento che corrisponde alla regola, invia l'alert.

Aggiungere una regola per marcare automaticamente certe evidence o certi collegamenti di intelligence tra entità

Per marcare automaticamente certe evidence o certi collegamenti senza registrare alert né inviarle:

Passo	*Azione*
1	Fare clic su **New Alert**: compaiono i dati da compilare.
2	• Impostare i criteri per selezionare le evidence o i collegamenti • In **Type** selezionare **None.** • In **Relevance** impostare il grado di importanza • Selezionare la casella **Enabled** se si desidera che la regola sia già attiva.
3	Fare clic su **Save**: nell'area di lavoro principale compare la nuova regola di alert. Non appena il sistema riceve una prova corrispondente a questa regola, la marca.

Visualizzare gli eventi corrispondenti all'alert registrato

Per visualizzare gli eventi corrispondenti a un alert:

Passo	*Azione*
1	Selezionare la regola di alert che presenta almeno una registrazione (colonna **Logs**): compare l'elenco delle registrazioni tutti gli alert registrati.
2	Dall'elenco degli alert registrati, fare doppio clic sulla riga corrispondente. **Risultato**: si apre direttamente: • l'elenco delle evidence che hanno fatto scattare l'alert (evento **Evidence**) • il dettaglio dell'entità (evento **Entity**) • la vista dei collegamenti (evento **Link**)

Dati degli alert

Dati delle regole di alert

Di seguito la descrizione dei dati delle regole di alert:

Dato	*Descrizione*
Logs	(solo in tabella) Quantità di notifiche ricevute corrispondenti alla regola.
Abilitato	Abilita o disabilita la regola di alert.
Evento	Tipo di evento che scatena l'alert: • **Evidence**: attiva la regola quando arriva una evidence che soddisfa i criteri di seguito indicati. • **Sync**: attiva la regola quando l'agent di seguito indicato effettua la sincronizzazione. • **Instance**: attiva la regola quando l'agent creato (istanziato) dalla factory di seguito indicata esegue la prima sincronizzazione. • **Entity**: attiva la regola quando il sistema crea in automatico una nuova entità di intelligence all'interno dell'operation indicata. • **Link**: attiva la regola quando il sistema crea in automatico un collegamento tra entità di intelligence all'interno dell'operation indicata o con l'entità indicata.
Path	operation, target, entità, agent e factory da tenere sotto controllo. Indica quindi l'ambito di applicazione della regola. Per esempio, per l'evento **Evidence**, se si sceglie un'operation si controllano le evidence di tutta l'operation. Se si sceglie un agent, si controllano le evidence di quell'agent.

Dato	*Descrizione*
Evidence	(solo eventi tipo **Evidence**) Tipo di evidence per cui si desidera essere avvisati.  Suggerimento: '*****' indica tutti i tipi di evidence. Per la descrizione di tutti i tipi *vedi "Elenco dei tipi di evidence" a pagina 49*
Keyword	(solo eventi tipo **Evidence**) Parole chiave che l'evidence deve contenere per attivare l'alert. Per esempio, la chiave "password" crea un alert quando l'evidence (audio, documento) contiene la parola "password".
Tag	(solo eventi tipo **Evidence** o **Link**) Marca l'evidence o il collegamento automaticamente con diversi gradi di importanza, per facilitare la fase di analisi: **Icona** **Descrizione**  Importanza massima.  Importanza intermedia.  Importanza normale.  Importanza minima. - Nessuna importanza.
Type	Tipo di alert da ricevere a fronte di un evento: • **Log**: alert registrata e notificata in RCS Console. • **Mail**: e-mail e alert registrata • **None**: nessun alert né registrata, né via e-mail. Utile per marcare automaticamente le evidence o i collegamenti per importanza (**Tag**)
Suppression Time	(solo alert tipo **Mail**) Tempo di latenza per l'invio di e-mail di alert identiche. Serve a evitare e-mail identiche successive alla prima. Per esempio, se il target non comunica da tempo le sue prove e si è scelto di essere avvisati via e-mail, può accadere che all'arrivo delle prime evidence si sia subissati dalla ricezione di e-mail. Mettendo un **Suppression time** di 30 minuti, si riceverà una mail ogni 30 minuti.  NOTA: questo parametro limita solo l'invio di e-mail. Gli eventi vengono sempre registrati.

Dati delle registrazioni

Di seguito la descrizione delle registrazioni degli alert:

Dato	*Descrizione*
Date	ora-data dell'alert.
Path	Raggio di azione da cui è stata generata l'alert. Per esempio, se nella regola in **Path**, è stato scelto un target, qui comparirà il nome del target e il nome dell'operation cui appartiene.
Info	Quantità e tipo di eventi che hanno generato l'alert.

]HackingTeam[

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

RCS 9 Manuale dell'analista
Manuale dell'analista 1.5 FEB-2014

info@hackingteam.com