

RCS 8.0

The hacking suite for governmental interception

Manuale dell'analista

Proprietà delle informazioni

© COPYRIGHT 2012, HT S.r.l.

Tutti i diritti riservati in tutti i paesi.

Nessuna parte di questo manuale può essere tradotta in altra lingua e/o adattata e/o riprodotta in altra forma e/o mezzo meccanico, elettronico, per fotocopie, registrazioni o altro, senza una precedente autorizzazione scritta da parte di HackingTeam .

Tutte le società e i nomi di prodotti possono essere marchi legali o marchi registrati delle rispettive società la cui proprietà viene qui riconosciuta, in particolare Internet Explorer™ è un marchio registrato dalla Microsoft Corporation.

L’elaborazione del testo e delle immagini è stata vagliata con la massima cura, nonostante ciò HackingTeam si riserva il diritto di modificare e/o aggiornare le informazioni qui contenute per correggere errori tipografi ci e/o imprecisioni, senza preavviso o alcun impegno da parte della stessa.

Qualsiasi riferimento a nomi, dati, e indirizzi di altre società non facenti parte di HackingTeam è casuale e, salvo diversa indicazione, è riportato a titolo puramente esemplificativo, allo scopo di meglio chiarire l’utilizzo del prodotto.

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 5](#_Toc321390637)

[Introduzione a questa Guida 8](#_Toc321390638)

[Novità della guida 8](#_Toc321390639)

[Documentazione fornita 8](#_Toc321390640)

[Convenzioni tipografiche per le segnalazioni 2](#_Toc321390641)

[Convenzioni tipografiche per la formattazione 2](#_Toc321390642)

[Destinatari del prodotto e di questa guida 3](#_Toc321390643)

[Dati di identificazione dell'autore del software 4](#_Toc321390644)

[RCS (Remote Control System) 4](#_Toc321390645)

[Differenze rispetto alle versioni precedenti 5](#_Toc321390646)

[RCS Console per l'Analista 5](#_Toc321390647)

[Ruolo dell'Analista 5](#_Toc321390648)

[Funzioni abilitate per l'Analista 5](#_Toc321390649)

[Avvio di RCS Console 6](#_Toc321390650)

[Come si presenta la pagina di login 6](#_Toc321390651)

[Accedere a RCS Console 6](#_Toc321390652)

[Descrizione della homepage 7](#_Toc321390653)

[Introduzione 7](#_Toc321390654)

[Come si presenta 7](#_Toc321390655)

[Elementi e azioni comuni dell'interfaccia 8](#_Toc321390656)

[Come si presenta RCS Console 8](#_Toc321390657)

[Azioni sempre disponibili sull'interfaccia 10](#_Toc321390658)

[Azioni sulle tabelle 11](#_Toc321390659)

[Procedure dell'Analista 13](#_Toc321390660)

[Introduzione 13](#_Toc321390661)

[Procedure 13](#_Toc321390662)

[Alert su nuove evidence 14](#_Toc321390663)

[Cose da sapere sugli alert dal target 14](#_Toc321390664)

[Cosa sono gli alert 14](#_Toc321390665)

[Utilità delle regole di alert 14](#_Toc321390666)

[Ambito di applicazione delle regole di alert 15](#_Toc321390667)

[Processo di alert 15](#_Toc321390668)

[Alert dal target (Alerting) 16](#_Toc321390669)

[Scopo 16](#_Toc321390670)

[Dati degli alert dal target (Alert) 19](#_Toc321390671)

[Dati delle regole di alert 19](#_Toc321390672)

[Dati delle registrazioni 21](#_Toc321390673)

[Tenere sotto controllo le attività dei target con la Dashboard 21](#_Toc321390674)

[Cose da sapere sulla Dashboard 21](#_Toc321390675)

[Componenti della Dashboard 21](#_Toc321390676)

[Processo di segnalazione delle evidence 22](#_Toc321390677)

[Monitoraggio delle evidence (Dashboard) 23](#_Toc321390678)

[Scopo 23](#_Toc321390679)

[Analisi delle evidence 25](#_Toc321390680)

[Cose da sapere sulle evidence 25](#_Toc321390681)

[Processo di analisi 25](#_Toc321390682)

[Filtrare le evidence 25](#_Toc321390683)

[Descrizione del file .tgz con le evidence esportate 26](#_Toc321390684)

[Analisi delle evidence (Evidence) 26](#_Toc321390685)

[Scopo 26](#_Toc321390686)

[Dati delle evidence 30](#_Toc321390687)

[Dettaglio di una evidence 31](#_Toc321390688)

[Scopo 32](#_Toc321390689)

[Dati di esportazione delle evidence 34](#_Toc321390690)

[Elenco dei tipi di evidence 35](#_Toc321390691)

[Esplorazione e recupero prove da dispositivi online 36](#_Toc321390692)

[Cose da sapere sul recupero prove 36](#_Toc321390693)

[Descrizione 36](#_Toc321390694)

[Componenti del File System 36](#_Toc321390695)

[Recupero evidence da dispositivi (File System) 37](#_Toc321390696)

[Scopo 37](#_Toc321390697)

[I target 38](#_Toc321390698)

[Pagina del target 39](#_Toc321390699)

[Scopo 39](#_Toc321390700)

[Dati della pagina target 41](#_Toc321390701)

[Visualizzazione a icone 41](#_Toc321390702)

[Visualizzazione a tabella 41](#_Toc321390703)

[Gli agent 42](#_Toc321390704)

[Pagina dell'agent 43](#_Toc321390705)

[Scopo 43](#_Toc321390706)

[Dati dello storico di un agent 45](#_Toc321390707)

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 |
| --- | --- | --- | --- |
| 16 Aprile 2012 | Manuale dell'analista  1.0 FEB/2012  Analyst's Guide  1.0 FEB/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 - 1.0 FEB/2012 | PDF |
| Manuale dell'amministratore | Amministratori | Manuale dell'amministratore - 1.0 FEB/2012 | PDF |
| Manuale del tecnico | Tecnici | Manuale del tecnico - 1.0 FEB/2012 | PDF |
| Manuale dell'analista (questo manuale) | Analisti | Manuale dell'analista - 1.0 FEB/2012 | PDF |

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

Funzioni abilitate per l'Analista

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

* Operation
* Dashboard
* Alerting

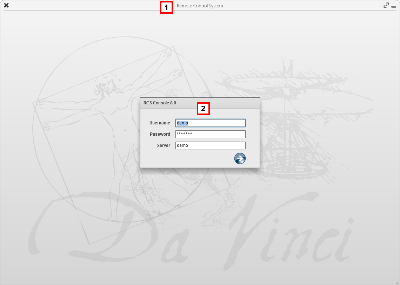
Questa sezione include i seguenti argomenti:

Avvio di RCS Console

RCS Console all'avvio 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. |
| 2 | In Server inserire il nome macchina o l’indirizzo del server a 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". |

Descrizione della homepage

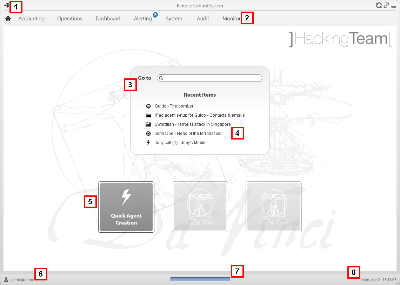
|  |  |
| --- | --- |
| Per visualizzare l'homepage: | * fare clic su |

Introduzione

RCS Console presenta all'avvio questa homepage. L'homepage è identica per tutti gli utenti. Solo i menu abilitati dipendono dai ruoli assegnati al proprio account.

Come si presenta

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



| Area | Descrizione |
| --- | --- |
| 1 | Barra del titolo con pulsanti di comando. |
| 2 | Menu di RCS con le funzioni abilitate per l'utente. |
| 3 | Casella di ricerca per cercare tra i nomi di operation, target, agent. |
| 4 | Collegamenti agli ultimi cinque elementi aperti (operation, target e agent). |
| 5 | Pulsanti per avvio del Wizard. |
| 6 | Utente connesso con possibilità di cambiare la lingua e la password. |
| 7 | Area download con possibilità durante l'esportazione o una compilazione di vedere lo stato di avanzamento. |
| 8 | Data e ora attuale con possibilità di cambio fuso orario. |

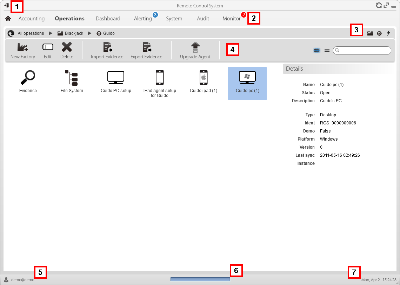
Elementi e azioni comuni dell'interfaccia

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 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 | |  | Mostra la pagina del target | |  | Mostra la pagina della factory | |  | Mostra la pagina dell'agent | |
| 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 | |
| 5 | Barra con i pulsanti della finestra. |
| 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 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 [6] compare una finestra di dialogo con i dati dell'utente. |
| 2 | Cambiare lingua o password e fare clic su 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 [8] compare una finestra di dialogo con la data-ora attuale:  Ora UTC: data-ora di Greenwitch (GMT)  Ora Locale: data-ora dove è installato il server RCS  Ora Console: data-ora della console da cui si sta lavorando e che può essere convertita. |
| 2 | Cambiare il fuso orario e fare clic su 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

Per ordinare una tabella: fare clic sull'intestazione della tabella.

Per cambiare dimensione delle colonne di una tabella: Selezionare il bordo della colonna e trascinarlo.

| 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" * "bossanova" |
| Filtrare in base a un'opzione | Selezionare un'opzione: compaiono gli elementi che corrispondono all'opzione scelta. |
| Filtrare in base a più opzioni | Selezionare una o più opzioni: compaiono gli elementi che corrispondono a tutte le opzioni scelte. |



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)" |
| 2 | Nella sezione Dashboard aggiungere al pannello di controllo le operation, target e agent da controllare maggiormente.  Vedi "Monitoraggio delle evidence (Dashboard)" |
| 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 dal target (Alerting)" |

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)". |
| 2 | Per le evidence di particolare interesse passare all'analisi dettagliata.  Vedi "Dettaglio di una evidence" |
| 3 | Nella sezione Evidence esportare le evidence utili.  Vedi "Analisi delle evidence (Evidence)". |
| 4 | Nella sezione File System esportare la struttura dell'hard disk.  Vedi "Recupero evidence da dispositivi (File System)" |

Alert su nuove evidence

Presentazione

Introduzione

Gli alert segnalano la ricezione di prove e marcano automaticamente le evidence (per l'analisi e l'export) al momento della ricezione.

Contenuti

Questa sezione include i seguenti argomenti:

Cose da sapere sugli alert dal target

Cosa sono gli alert

In fase investigativa sono diverse le prove raccolte dal dispositivo del target. Oltre a raccogliere le prove per analizzarle, può essere utile venire "allertati" in tempo reale tramite email o tramite una notifica in RCS Console, di avvenimenti particolari che riguardano il target.

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 email e registri un log ad 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.

Utilità delle regole di alert

Le regole di alert indicano al sistema per quali evidenceo sincronizzazioni essere avvisati. Inoltre possono essere usate per assegnare automaticamente a certe evidence dei gradi di importanza, utilizzabili in fase di analisi per una selezione delle evidence.

Ambito di applicazione delle regole di alert

È possibile creare regole che avvisano dell'arrivo di una evidence nel sistema 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

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 email è opzionale.

| Fase | Descrizione |
| --- | --- |
| 1 | L'Analista crea delle regole per essere avvisato dell'arrivo di evidence particolari, o di sincronizzazioni del dispositivo del target. Le regole registrano gli alert, le notificano all’interno di RCS Console e le inviano via email (opzionale). |
| 2 | Il sistema intercetta le evidence in arrivo e le confronta con le regole di alert.   | Se la prova... | Allora... | | --- | --- | | corrisponde a una regola di alert | il sistema registra la prova come evidence e genera un alert che applica automaticamente il grado di importanza scelto. Opzionalmente viene inviata dal sistema un’email di notifica. | | non corrisponde a una regola di alert | il sistema registra la prova come evidence senza generare alert. | |
| 3 | L'Analista riceve una email 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. |
| 4 | Terminato il controllo, l'Analista elimina le registrazioni di alert. |

Alert dal target (Alerting)

|  |  |
| --- | --- |
| Per ricevere alert dal target: | * sezione Alerting |

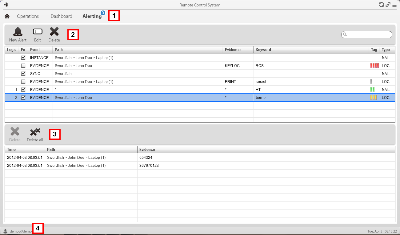
Scopo

Questa funzione permette di:

* ricevere alert quando un certo tipo di evidence sono intercettate o quando il dispositivo del target si sincronizza con RCS.
* marcare automaticamente le evidence per importanza per facilitare l'analisi successiva.
* controllare tutte gli alert registrate e navigare direttamente nelle evidence che le hanno generate.

Come si presenta la funzione

Ecco come viene visualizzata la pagina già popolata:



| Area | Descrizione |
| --- | --- |
| 1 | Menu di RCS.Vedi "Elementi e azioni comuni dell'interfaccia"  : indica la quantità di alert ricevuti . Il contatore viene azzerato automaticamente dopo due settimane, oppure quando si eliminano le notifiche. |
| 2 | Barra con i pulsanti dedicati alle regole di alert. Di seguito la descrizione:   | Icona | Descrizione | | --- | --- | |  | Crea una nuova regola di alert. | |  | 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. Vedi "Elementi e azioni comuni dell'interfaccia". |

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. Vedi "Dati degli alert dal target (Alert)". |
| 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 intercetta le evidence che corrispondono 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. Vedi "Dati degli alert dal target (Alert)". |
| 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 intercetta le evidence che corrispondono alla regola, invia l'alert. |

Aggiungere una regola per marcare automaticamente certe evidence

Per marcare automaticamente certe evidence senza registrare alert né inviarle:

| Passo | Azione |
| --- | --- |
| 1 | Fare clic su New Alert: compaiono i dati da compilare. Vedi "Dati degli alert dal target (Alert)". |
| 2 | * Impostare i criteri per selezionare le evidence * In Type selezionare None. * In Tag impostare il marcatore 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 le evidence corrispondenti all'alert registrata

Per visualizzare le evidence corrispondenti a un alert:

| Passo | Azione |
| --- | --- |
| 1 | Selezionare la regola di alert che presenta almeno una registrazione (colonna Logs): nell'elenco delle registrazioni compaiono tutte gli alert registrate. |
| 2 | Dall'elenco degli alert registrate, fare doppio clic nella colonna Evidence: si apre direttamente l'elenco delle evidence che hanno fatto scattare l'alert. |

Dati degli alert dal target (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. |
| Enabled | Abilita o disabilita la regola di alert. |
| Event | 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. |
| Path | operation, target, agent e factory le cui evidence e sincronizzazioni sono da tenere sotto controllo. Indica quindi l'ambito di applicazione della regola.  Per esempio, 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. |
| 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" |
| 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) Marca l'evidence automaticamente con diversi gradi di importanza, per facilitare la ricerca delle evidence più importanti in fase di analisi:   |  |  | | --- | --- | | Icona | **Descrizione** | |  | Importanza massima | |  | Importanza intermedia | |  | Importanza normale | |  | Importanza minima | | - | Nessuna importanza | |
| Type | Tipo di alert da ricevere a fronte di una evidence:   * Log: alert registrata e notificata in RCS Console. * Mail: email e alert registrata * None: nessun alert né registrata, né via email. Utile per marcare automaticamente le evidence per importanza (Tag) |
| Suppression Time | (solo alert tipo Mail) Tempo di latenza per l'invio di email di alert identiche. Serve a evitare email identiche successive alla prima. Per esempio, se il target non comunica da tempo le sue prove e si è scelto di essere avvisati via email, può accadere che all'arrivo delle prime evidence si sia subissati dalla ricezione di email. Mettendo un Suppression time di 30 minuti, si riceverà una mail ogni 30 minuti.  NOTA: questo parametro limita solo l'invio di email, le registrazioni sono sempre attive. |

Dati delle registrazioni

Di seguito la descrizione delle registrazioni degli alert:

| Dato | Descrizione |
| --- | --- |
| Time | 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. |
| Evidence | Quantità di evidence che hanno generato l'alert. |

Tenere sotto controllo le 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 ad 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".

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)

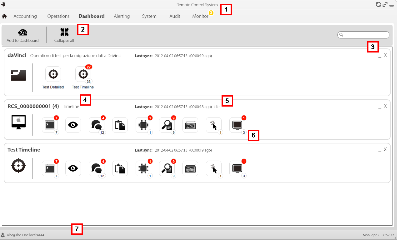
|  |  |
| --- | --- |
| Per controllare la ricezione delle evidence: | * sezione Dashboard |

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 già popolata:



| Area | Descrizione |
| --- | --- |
| 1 | Menu di RCS. Vedi "Elementi e azioni comuni dell'interfaccia". |
| 2 | Barra 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.  Vedi "Elementi e azioni comuni dell'interfaccia" |

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. |
| 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".   Per l'elemento target:   * fare doppio clic sull'agent: si apre la pagina dell'agent. Vedi "Pagina dell'agent".   Per l'elemento agent:   * fare doppio clic sul tipo di evidence: si apre la pagina delle evidence. Vedi "Analisi delle evidence (Evidence)" |

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. |

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"

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.

Descrizione del file .tgz con le evidence esportate

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

Per navigare nel 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, entrare in una operation, entrare in un target, fare clic su Evidence * sezione Operations, entrare in una operation, entrare in un target, entrare in un agent, fare clic su Evidence |

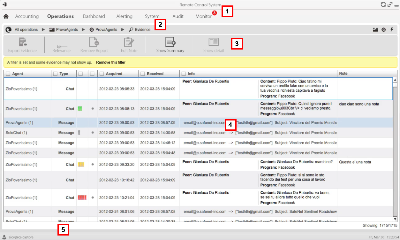
Scopo

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
* 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 già popolata:



| Area | Descrizione |
| --- | --- |
| 1 | Menu di RCS. Vedi "Elementi e azioni comuni dell'interfaccia". |
| 2 | Barra di navigazione. Vedi "Elementi e azioni comuni dell'interfaccia". |
| 3 | Barra con i pulsanti della finestra. Di seguito la descrizione:   | Icona | Descrizione | | --- | --- | |  | Esporta le evidence visualizzate in un file .tgz | |  | Applica un grado di importanza alle evidence selezionate. | |  | Applica un segnalibro alle evidence selezionate. | |  | Modifica le note delle evidence selezionate. | |  | Mostra le quantità totali per tipo di evidence | |  | Mostra il dettaglio dell'evidence selezionata. Vedi "Dettaglio di una evidence" | |
| 4 | Elenco delle evidence in base ai filtri impostati. |
| 5 | Barra di stato di RCS.  Vedi "Elementi e azioni comuni dell'interfaccia" |

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 Vedi "Dati delle evidence" |
| 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 poter escludere/includere evidence dal report e per filtrare la visualizzazione:

| Passo | Azione |
| --- | --- |
| 1 | Selezionare una o più evidence |
| 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" |

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. Se si è scelto di considerare il campo Included in report per esportare solo le evidence che corrispondono al criterio selezionato e che hanno il campo Included report attivato, selezionare l'opzione relativa. Vedi "Dati di esportazione delle evidence". |
| 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. |
| 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" |
| Info | Informazioni dell'evidence: testi, immagini, video, audio e così via  Si può filtrare indicando il nome intero del campo e parte del testo da cercare.  Per esempio:   * "content:boss" * "program:word" * e così via |
| 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 |
| Agent | (solo per evidence del target) Nome dell'agent che ha registrato l'evidence. |

Dettaglio di una evidence

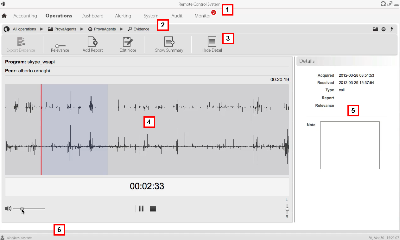
|  |  |
| --- | --- |
| Per entrare nel dettaglio di una evidence: | * sezione Operations, entrare in una operation, entrare in un target, fare clic su Evidence, doppio clic su una evidence * sezione Operations, entrare in una operation, entrare in un target, entrare in un agent, fare clic su Evidence,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

Come si presenta la funzione

Ecco come viene visualizzata il dettaglio di una evidence audio:



| Area | Descrizione |
| --- | --- |
| 1 | Menu di RCS. Vedi "Elementi e azioni comuni dell'interfaccia". |
| 2 | Barra di navigazione. Vedi "Elementi e azioni comuni dell'interfaccia". |
| 3 | Pulsanti per le azioni sulle evidence.   | Icona | Descrizione | | --- | --- | |  | Applica un grado di importanza alle evidence selezionate. | |  | Applica un segnalibro alle evidence selezionate. | |  | Modifica le note delle evidence selezionate. | |  | Mostra le quantità totali per tipo di prove. | |  | Nasconde il dettaglio dell'evidence selezionata. | |
| 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.  Vedi "Elementi e azioni comuni dell'interfaccia" |



Azioni su evidence di tipo immagine

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

| Icona | Descrizione |
| --- | --- |
| [ICO] | Visualizza immagine a tutto schermo |
| [ICO] | Visualizza immagine in dimensione reale |
| [ICO] | Ingrandisce e rimpicciolisce immagine |
| [ICO] | Ruota immagine |
| Anti alias | Riduce effetto di scalettatura dell'immagine. |

Azioni su evidence di tipo audio

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

| Icona | Descrizione |
| --- | --- |
| [ICO] | Zoom della porzione di segnale audio selezionata con il cursore |
| [ICO] | Avvia, mette in pausa e ferma audio |
| [ICO] | Bilancia suono su altoparlanti sinistra e destra |

Tutte le azioni

Di seguito la descrizione delle azioni possibili in questa finestra:

Dati di esportazione delle evidence

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 |
| --- | --- |
| From  To | Intervallo di tempo delle evidence da esportare. |
| Relevance | Gradi di importanza delle evidence da esportare. |
| Type | 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 |
| Report Name | 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 | | Agent | <nome agent> - Evidence Export.tgz | |

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 (telefono, Skype, MSN) |
| Camera | immagine | immagini della webcam |
| Chat | testo | chat |
| Clipboard | testo | informazioni copiate nella clipboard |
| Device | 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)*"* |
| Info | testo | informazioni fornite dall’agente e definite nella configurazione |
| Keylog | testo | tasti premuti sulla tastiera |
| Messages | testo | email |
| 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 |

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 device se si sta esplorando il FileSystem di un target).

All’apertura, l’alberatura conterrà solo una parte dei file e delle directory contenute nel sistema; nello specifico:

* tutte le root locali (es.: "c:\", "d:\")
* la cartella Documenti dell'utente connesso in quel momento

Il comando Retrieve permette di richiedere esplicitamente la lettura (o la rilettura) del contenuto di una data cartella.

Il comando Download scarica un file e lo salva come evidence di tipo File.

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, entrare in una operation, entrare in un target, fare clic su File System * sezione Operations, entrare in una operation, entrare in un target, entrare in un agent, fare clic su File System |

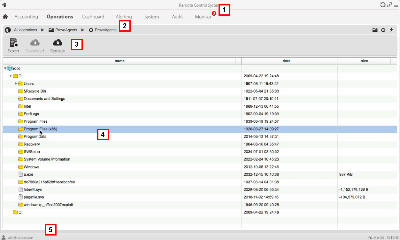
Scopo

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

Come si presenta la funzione

Ecco come viene visualizzata la pagina già popolata:



| Area | Descrizione |
| --- | --- |
| 1 | Menu di RCS.Vedi "Elementi e azioni comuni dell'interfaccia".Fare riferimento a "Elementi e azioni comuni dell'interfaccia" |
| 2 | Barra di navigazione. Vedi "Elementi e azioni comuni dell'interfaccia". |
| 3 | Barra con i pulsanti della finestra. Di seguito la descrizione:   | Icona | Descrizione | | --- | --- | |  | Esporta la strutta completa in un file .tgz | |  | Download: scarica il file selezionato nelle evidence di tipo File. | |  | Retrieve: richiede di esplorare il contenuto della cartella selezionata | |
| 4 | Struttura dell'hard disk del dispositivo |
| 5 | Barra di stato di RCS. Vedi "Elementi e azioni comuni dell'interfaccia". |

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. |

I target

Presentazione

Introduzione

Un target è una persona fisica da sottoporre a monitoraggio. A questo scopo possono essere utilizzati più agent, uno per ogni device posseduto dal target.

Contenuti

Questa sezione include i seguenti argomenti:

Pagina del target

|  |  |
| --- | --- |
| Per entrare in un target | * **sezione Operations, entrare in una operation, entrare in un target** |

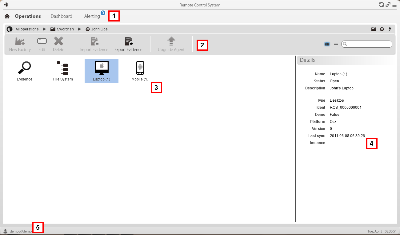
Scopo

Questa funzione permette di:

* esportare le evidence del target.
* entrare in un agent installato (Vedi "Pagina dell'agent").
* entrare nelle evidence dell'agent
* esplorare il dispositivo dell'agent

Come si presenta la funzione

Ecco come viene visualizzata la pagina già popolata:



| Area | Descrizione |
| --- | --- |
| 1 | Menu di RCS. Vedi "Elementi e azioni comuni dell'interfaccia". |
| 2 | Barra di navigazione. Vedi "Elementi e azioni comuni dell'interfaccia". |
| 3 | Barra con i pulsanti della finestra. Di seguito la descrizione:  NOTA: il pulsante visualizza gli elementi in elenco con i loro dati.Vedi "Dati della pagina target"   | Icona | Descrizione | | | | --- | --- | --- | --- | |  | Esporta le evidence del target in formato .tgz. | | | |
| 4 | Icone/elenco delle factory create e degli agent installati.  : agent in modalità demo  Per la descrizione delle icone e dei dati della tabella vedi "Dati della pagina target". |
| 5 | Dati della factory o dell'agent selezionato. |
| 6 | Barra di stato di RCS. Vedi "Elementi e azioni comuni dell'interfaccia". |



Dati della pagina target

|  |  |
| --- | --- |
| Per visualizzare i dati della pagina: | * sezione Operations, entrare in una operation, entrare in 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 |
| --- | --- |
|  | Agent di tipo desktop, in stato Aperto, per i sistemi operativi:   * OSX * Windows |
|  | Agent di tipo mobile, in stato Aperto, per sistemi operativi:   * Android, * BlackBerry, * iOS, * Symbian * Windows Mobile |

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 |
| --- | --- |
| Name | Nome della factory o dell'agent. |
| Description | Descrizione della factory o dell'agent. |
| Status | Open: l’agent è ancora attivo sul device e può continuare a inviare dati.  Closed**: l’agente 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. |
| Platform | (solo agent) Sistema operativo su cui l'agent si è installato. |
| Version | (solo agent) Versione dell'agent. Ad ogni riconfigurazione 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. |

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 al target.

Contenuti

Questa sezione include i seguenti argomenti:

Pagina dell'agent

|  |  |
| --- | --- |
| Per gestire  gli agent: | * sezione Operations, entrare in una operation, entrare in un target, entrare in un agent |

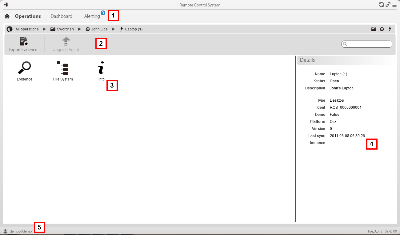
Scopo

Questa funzione permette di:

* verificare l'attività dell'agent tramite lo storico.
* esportare le evidence dell'agent
* 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 già popolata:



| Area | Descrizione |
| --- | --- |
| 1 | Menu di RCS. Vedi "Elementi e azioni comuni dell'interfaccia". |
| 2 | Barra di navigazione. Vedi "Elementi e azioni comuni dell'interfaccia". |
| 3 | Barra con i pulsanti della finestra. |
| 4 | Azioni possibili sull'agent. Di seguito la descrizione:   | Icona | Descrizione | | --- | --- | |  | Mostra l'elenco delle evidence raccolte dall'agent. Vedi "Analisi delle evidence (Evidence)". | |  | Mostra il file system del dispositivo. Vedi "Recupero evidence da dispositivi (File System)". | |  | Mostra lo storico delle attività dell'agent. Vedi "Dati dello storico di un agent". | |
| 5 | Dettagli dell'agent. |
| 6 | Barra di stato di RCS. Vedi "Elementi e azioni comuni dell'interfaccia". |

Dati dello storico 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. |



|  |  |
| --- | --- |
| RCS8.0Manuale dell'amministratore di sistema  Manuale dell'amministratore di sistema 1.0 FEB/2012  © COPYRIGHT 2012  info@hackingteam.com | **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 |
| RCS8.0Manuale dell'utente  Manuale dell'utente 1.0 FEB/2012  © COPYRIGHT 2012  info@hackingteam.com | **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 |