

RCS 8.2

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 tipografici 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](#_Toc337471961)

[Introduzione a questa Guida 8](#_Toc337471962)

[Novità della guida 3](#_Toc337471963)

[Documentazione fornita 3](#_Toc337471964)

[Convenzioni tipografiche per le segnalazioni 4](#_Toc337471965)

[Convenzioni tipografiche per la formattazione 4](#_Toc337471966)

[Destinatari del prodotto e di questa guida 5](#_Toc337471967)

[Dati di identificazione dell'autore del software 5](#_Toc337471968)

[RCS (Remote Control System) 6](#_Toc337471969)

[Differenze rispetto alle versioni precedenti 7](#_Toc337471970)

[RCS Console per l'Analista 7](#_Toc337471971)

[Avvio di RCS Console 9](#_Toc337471972)

[Come si presenta la pagina di login 9](#_Toc337471973)

[Accedere a RCS Console 9](#_Toc337471974)

[Descrizione della homepage 10](#_Toc337471975)

[Introduzione 10](#_Toc337471976)

[Come si presenta 10](#_Toc337471977)

[Elementi e azioni comuni dell'interfaccia 11](#_Toc337471978)

[Come si presenta RCS Console 11](#_Toc337471979)

[Azioni sempre disponibili sull'interfaccia 14](#_Toc337471980)

**[Cambiare la lingua dell'interfaccia o la propria password](#_Toc337471981)** [14](#_Toc337471981)

**[Convertire le date-ora di RCS Console al proprio fuso orario](#_Toc337471982)** [14](#_Toc337471982)

[Azioni sulle tabelle 14](#_Toc337471983)

[Procedure dell'Analista 17](#_Toc337471984)

[Introduzione 17](#_Toc337471985)

[Procedure 17](#_Toc337471986)

**[Per recuperare prove importanti ed essere avvisati](#_Toc337471987)** [17](#_Toc337471987)

**[Analizzare, selezionare ed esportare le evidence](#_Toc337471988)** [17](#_Toc337471988)

[Alert su nuove evidence 18](#_Toc337471989)

[Cose da sapere sugli alert dal target 19](#_Toc337471990)

[Cosa sono gli alert 19](#_Toc337471991)

[Utilità delle regole di alert 19](#_Toc337471992)

[Ambito di applicazione delle regole di alert 19](#_Toc337471993)

[Processo di alert 19](#_Toc337471994)

[Alert dal target (Alerting) 21](#_Toc337471995)

[Scopo 21](#_Toc337471996)

**[Come si presenta la funzione](#_Toc337471997)** [21](#_Toc337471997)

[Per saperne di più 22](#_Toc337471998)

**[Aggiungere regola per essere allertati](#_Toc337471999)** [22](#_Toc337471999)

**[Modificare una regola di alert](#_Toc337472000)** [23](#_Toc337472000)

**[Aggiungere una regola per marcare automaticamente certe evidence](#_Toc337472001)** [23](#_Toc337472001)

**[Visualizzare le evidence corrispondenti all'alert registrata](#_Toc337472002)** [23](#_Toc337472002)

[Dati degli alert dal target (Alert) 24](#_Toc337472003)

[Dati delle regole di alert 24](#_Toc337472004)

[Dati delle registrazioni 25](#_Toc337472005)

[Monitoraggio delle attività dei target con la Dashboard 26](#_Toc337472006)

[Cose da sapere sulla Dashboard 27](#_Toc337472007)

[Componenti della Dashboard 27](#_Toc337472008)

[Processo di segnalazione delle evidence 27](#_Toc337472009)

[Monitoraggio delle evidence (Dashboard) 28](#_Toc337472010)

[Scopo 28](#_Toc337472011)

**[Come si presenta la funzione](#_Toc337472012)** [28](#_Toc337472012)

[Per saperne di più 29](#_Toc337472013)

**[Aggiungere un elemento alla Dashboard](#_Toc337472014)** [29](#_Toc337472014)

**[Visualizzare una evidence segnalata nella Dashboard](#_Toc337472015)** [30](#_Toc337472015)

[Analisi delle evidence 30](#_Toc337472016)

[Cose da sapere sulle evidence 32](#_Toc337472017)

[Processo di analisi 32](#_Toc337472018)

[Accumulo delle evidence nel dispositivo 32](#_Toc337472019)

[Filtrare le evidence 32](#_Toc337472020)

[Eliminare le evidence 32](#_Toc337472021)

[Descrizione del file .tgz con le evidence esportate 33](#_Toc337472022)

[Analisi delle evidence (Evidence) 33](#_Toc337472023)

[Scopo 33](#_Toc337472024)

**[Come si presenta la funzione](#_Toc337472025)** [34](#_Toc337472025)

[Per saperne di più 35](#_Toc337472026)

**[Preparare le evidence all'analisi e all'export marcandole per importanza](#_Toc337472027)** [35](#_Toc337472027)

**[Preparare le evidence all'analisi e all'export marcandole per il report](#_Toc337472028)** [36](#_Toc337472028)

**[Preparare le evidence all'analisi e all'export aggiungendo note personali](#_Toc337472029)** [36](#_Toc337472029)

**[Analizzare una evidence](#_Toc337472030)** [37](#_Toc337472030)

**[Visualizzare i contatori suddivisi per tipo](#_Toc337472031)** [37](#_Toc337472031)

**[Esportare le evidence visualizzate](#_Toc337472032)** [37](#_Toc337472032)

[Dati delle evidence 38](#_Toc337472033)

[Dettaglio di una evidence 39](#_Toc337472034)

[Scopo 40](#_Toc337472035)

**[Come si presenta la funzione](#_Toc337472036)** [40](#_Toc337472036)

[Per saperne di più 41](#_Toc337472037)

**[Azioni su evidence di tipo immagine](#_Toc337472038)** [41](#_Toc337472038)

**[Azioni su evidence di tipo audio](#_Toc337472039)** [42](#_Toc337472039)

[Dati di esportazione delle evidence 42](#_Toc337472040)

[Elenco dei tipi di evidence 43](#_Toc337472041)

[Pagina dei comandi 44](#_Toc337472042)

[Scopo 44](#_Toc337472043)

**[Come si presenta la funzione](#_Toc337472044)** [45](#_Toc337472044)

[Per saperne di più 46](#_Toc337472045)

[Esplorazione e recupero prove da dispositivi online 46](#_Toc337472046)

[Cose da sapere sul recupero prove 47](#_Toc337472047)

[Descrizione 47](#_Toc337472048)

[Componenti del File System 47](#_Toc337472049)

[Recupero evidence da dispositivi (File System) 47](#_Toc337472050)

[Scopo 47](#_Toc337472051)

**[Come si presenta la funzione](#_Toc337472052)** [47](#_Toc337472052)

[Per saperne di più 48](#_Toc337472053)

**[Esplorare il contenuto del file system e scaricare file](#_Toc337472054)** [49](#_Toc337472054)

[I target 49](#_Toc337472055)

[Pagina del target 50](#_Toc337472056)

[Scopo 50](#_Toc337472057)

**[Come si presenta la funzione](#_Toc337472058)** [50](#_Toc337472058)

[Per saperne di più 51](#_Toc337472059)

**[Esportare le evidence del target](#_Toc337472060)** [51](#_Toc337472060)

[Dati della pagina target 52](#_Toc337472061)

[Visualizzazione a icone 52](#_Toc337472062)

[Visualizzazione a tabella 52](#_Toc337472063)

[Gli agent 53](#_Toc337472064)

[Pagina dell'agent 54](#_Toc337472065)

[Scopo 54](#_Toc337472066)

**[Come si presenta la funzione](#_Toc337472067)** [54](#_Toc337472067)

[Per saperne di più 55](#_Toc337472068)

[Dati dello storico eventi di un agent 56](#_Toc337472069)

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.

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.

C

Collector

Riceve i dati inviati dagli agent, direttamente o 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

evidence

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

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 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

Componente che 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 in ambienti WiFi.

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.

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.

Tecnico

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

V

VPS

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

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 |
| --- | --- | --- | --- |
| 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 33.  Se installato, possibilità di vedere i testi estratti da una evidence tipo screenshot. Vedi "Dettaglio di una evidence" a pagina 39. |
| 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)" . |
| 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  1.2 OTT-2012 | PDF |
| Manuale dell'amministratore | Amministratori | Manuale dell'amministratore  1.2 OTT-2012 | PDF |
| Manuale del tecnico | Tecnici | Manuale del tecnico  1.2 OTT-2012 | PDF |
| Manuale dell'analista (questo manuale) | Analisti | Manuale dell'analista  1.2 OTT-2012 | 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. |
| 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

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 rispetto alle versioni precedenti

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 |

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

Contenuti

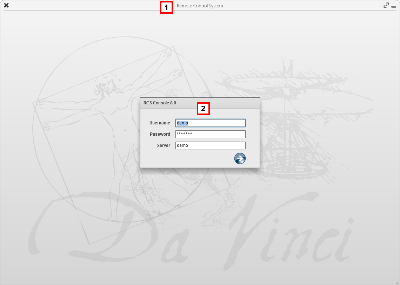
Questa sezione include i seguenti argomenti:

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. |
| 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" . |

Descrizione della homepage

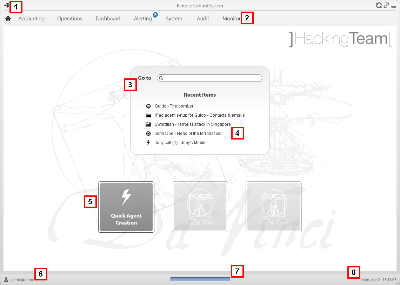
|  |  |
| --- | --- |
| Per visualizzare l'homepage: | * fare clic su |

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. |
| 2 | Menu di RCS con le funzioni abilitate per l'utente |
| 3 | Casella di ricerca per cercare tra i nomi di operation, target e agent, per nome o descrizione. |
| 4 | Collegamenti agli ultimi cinque elementi aperti (operation, target e agent). |
| 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. |

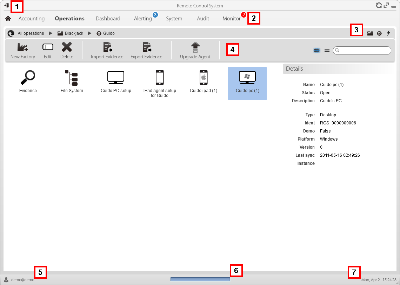
Elementi e azioni comuni dell'interfaccia

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. | |  | 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 | Barre 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 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 [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

| 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:   * "myboss" * "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. |
| 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)" |
| 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 e-mail 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 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.

Utilità delle regole di alert

Le regole di alert indicano al sistema per quali evidence o 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 e-mail 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 e-mail (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’e-mail di notifica. | | non corrisponde a una regola di alert | il sistema registra la prova come evidence 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. |
| 4 | Terminato il controllo, l'Analista elimina le registrazioni di alert. |

Alert dal target (Alerting)

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

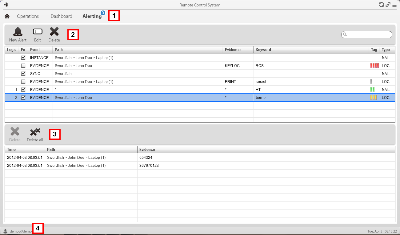
Scopo

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 tutti gli alert registrati e navigare direttamente nelle evidence 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. |
| 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. |

Per saperne di più

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

Per la descrizione dei dati presenti sulla finestra vedi "Dati degli alert dal target (Alert)"

Per saperne di più sugli alertvedi "Cose da sapere sugli alert dal target" .

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. |
| 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 riceve 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. |
| 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 riceve 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. |
| 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. |
| 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. |
| 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: e-mail e alert registrata * None: nessun alert né registrata, né via e-mail. Utile per marcare automaticamente le evidence 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. Le evidence vengono sempre registrate. |

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. |

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" .

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)

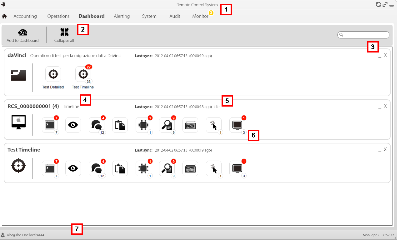
|  |  |
| --- | --- |
| Per controllare la ricezione delle evidence: | * sezione Dashboard |

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" .

Per saperne di più sulla Dashboard vedi "Cose da sapere sulla Dashboard" .

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. |

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" .

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.

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.

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 |

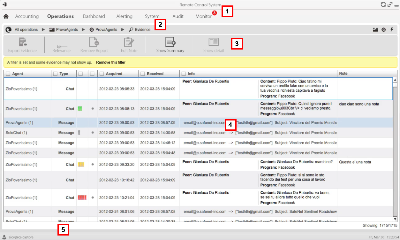
Scopo

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
* 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. |
| 3 | Barre con i pulsanti della finestra. Di seguito la descrizione:   | Icona | Descrizione | | --- | --- | |  | Esporta le evidence selezionate in un file .tgz. | |  | 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 preme 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 42, i campi sono simili. | |  | 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. | |  | Mostra le quantità totali per tipo di evidence. | |  | Mostra il dettaglio dell'evidence selezionata. Vedi "Dettaglio di una evidence" | |  | Salva i filtri attualmente selezionati oppure carica una impostazione di filtri salvata precedentemente. | |  | Pulisce tutti i filtri impostati. | |
| 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" .

Per la descrizione dei dati presenti sulla finestra vedi "Dati delle evidence"

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

Per saperne di più sulle evidencevedi "Cose da sapere sulle evidence"

Per vedere l'elenco dei tipi di evidence vedi "Elenco dei tipi di evidence"

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. |
| 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. Sono esportate le evidence che corrispondono ai criteri selezionati e hanno il campo Included report selezionato.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. Ogni informazione è accompagnata da diversi capi (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

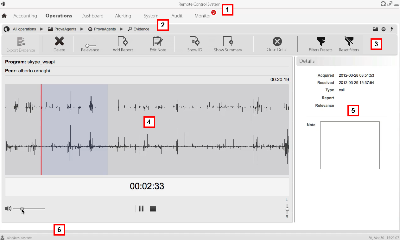
|  |  |
| --- | --- |
| Per entrare nel dettaglio di una evidence: | * sezione Operations, doppio-clic su una operation, doppio-clic su un target, fare clic su Evidence, doppio clic su una evidence * sezione Operations, doppio-clic su una operation, doppio-clic su un target, doppio-clic su un agent,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

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. |
| 3 | Pulsanti per le azioni sulla evidence.   | Icona | Descrizione | | --- | --- | |  | Esporta l'evidence in un file .tgz. | |  | Elimina l'evidence. | |  | Applica un grado di importanza. | |  | Applica un segnalibro. | |  | Modifica le note. | |  | Mostra il codice identificativo. | |  | Mostra le quantità totali per tipo di evidence. | |  | Chiude il dettaglio e torna nell'elenco delle evidence. Vedi "Analisi delle evidence (Evidence)" a pagina 33. | |  | Salva i filtri attualmente selezionati oppure carica una impostazione di filtri salvata precedentemente. | |  | Pulisce tutti i filtri impostati. | |
| 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" .

Per saperne di più sulle evidence vedi "Cose da sapere sulle evidence" .

Per la descrizione dei dati presenti sulla finestra vedi "Dati delle evidence" .

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) Mostra il testo convertito dall'immagine.  NOTA: se compare il messaggio "OCR non disponibile" significa che l'immagine è ancora in attesa di essere convertita in testo. 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. |
|  | Visualizza immagine in dimensione reale. |
|  | Ingrandisce e rimpicciolisce immagine. |
|  | 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 |
| --- | --- |
|  | Regolazione volume. |
|  | Avvia, mette in pausa e ferma audio. |
|  | Bilancia suono su altoparlanti sinistra e destra. |

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. |
| Acquired | Considera la data come data di acquisizione della prova sul dispositivo del target. |
| Received | **Considera la data come data di ricezione della prova.** |
| 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. È possibile includere o escludere l'esportazione delle note. |
| 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 | | Agente | <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. |
| 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)*"* |
| Info | testo | informazioni fornite dall’agent e definite nella configurazione. |
| Keylog | testo | tasti premuti sulla tastiera. |
| Messages | testo | e-mail. |
| 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. |

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 |

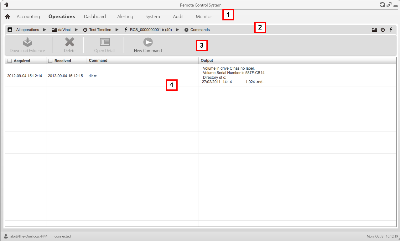
Scopo

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. | |  | 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 11.

Per la descrizione dei dati presenti sulla finestra vedi "Dati delle evidence" a pagina 38

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 |

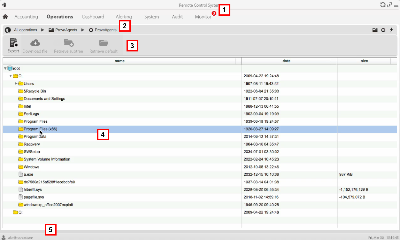
Scopo

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

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. | |  | Download: scarica il file selezionato nelle evidence di tipo File. | |  | Retrieve subtree: esplora il contenuto della cartella selezionata. | |  | Retrieve default: richiede la struttura di primo livello del disco. | |
| 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" .

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

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. 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 |

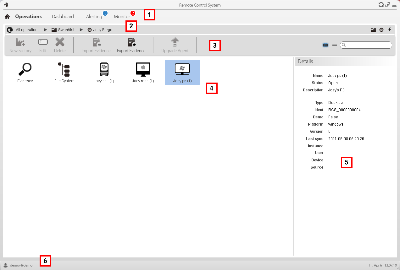
Scopo

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. |
| 3 | Barre con i pulsanti della finestra. Di seguito la descrizione:  NOTA: il pulsante visualizza gli elementi in elenco con i loro dati.   | Icona | Descrizione | | --- | --- | |  | Esporta le evidence del target in formato .tgz. | |
| 4 | Icone/elenco delle factory create e degli agent installati.  : agent in modalità demo.  : scout agent in attesa di verifica. |
| 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" .

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

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 |
| --- | --- |
|  | Agent di tipo desktop, in stato Aperto, per i sistemi operativi:   * OS X * Windows |
|  | Agent di tipo mobile, in stato Aperto, per i 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:.



NOTA: lo scout agent mostra una bussola accanto all'icona del dispositivo. Questa è l'icona di uno scout agent desktop Windows .



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. |
| 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. |
| 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. |

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 |

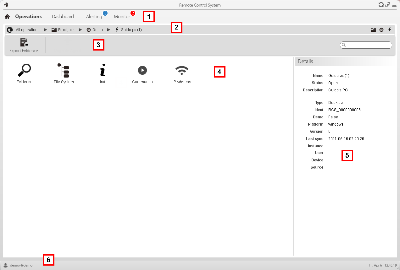
Scopo

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. |
| 3 | Barre 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 degli eventi dell'agent (Info). Vedi "Dati dello storico eventi di un agent" | |
| 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" .

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. |

|  |  |
| --- | --- |
| RCS 8.2 Manuale dell'analista  Manuale dell'analista 1.2 OTT-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 |