Guida introduttiva

Sentinel 7.0.1

March 2012

Note legali

Per ulteriori informazioni, contattare NetIQ all'indirizzo:

1233 West Loop South, Houston, Texas 77027
Stati Uniti
www.netiq.com

Sommario

Informazioni sulla Guida

Questa guida funge da introduzione a Sentinel, un prodotto WorkloadIQ.

Destinatari

La presente guida è rivolta ai professionisti della sicurezza delle informazioni.

Feedback

È possibile inviare i propri commenti e suggerimenti relativi a questa guida e agli altri documenti forniti con questo prodotto. Per inserire i commenti, utilizzare l'apposita funzione disponibile in fondo a ogni pagina della documentazione online.

Aggiornamenti della documentazione

Per accedere alla versione più recente della *NetIQ Sentinel 7.0.1 Overview Guide (Guida introduttiva di NetIQ Sentinel 7.0.1*, visitare il sito Web della documentazione di Sentinel (http://www.novell.com/documentation/sentinel70).

Documentazione aggiuntiva

La documentazione tecnica di Sentinel è suddivisa in diversi volumi, ovvero:

- Guida rapida di Sentinel (http://www.novell.com/documentation/sentinel70/s70_quickstart/data/s70_quickstart.html)
- Guida all'installazione di Sentinel (http://www.novell.com/documentation/sentinel70/s70_install/data/bookinfo.html)
- Sentinel Administration Guide (Guida all'amministrazione di Sentinel) (http://www.novell.com/documentation/sentinel70/s70_admin/data/bookinfo.html)
- Guida dell'utente di Sentinel (http://www.novell.com/documentation/sentinel70/s70_user/data/bookinfo.html)
- Guida introduttiva di Collegamento Sentinel (http://www.novell.com/documentation/sentinel70/sentinel_link_overview/data/bookinfo.html)
- Eventi di revisione interni a Sentinel (http://www.novell.com/documentation/sentinel70/s70_auditevents/data/bookinfo.html)
- Sentinel SDK (http://www.novell.com/developer/develop_to_sentinel.html)

  Nel sito SDK di Sentinel vengono fornite informazioni relative alla creazione di plug-in specifici dei clienti.

Contattare Novell e NetIQ

Benché Sentinel adesso sia un prodotto NetIQ, Novell continua a gestire diverse funzioni di supporto.

- Sito Web di Novell (http://www.novell.com)
- Sito Web di NetIQ (http://www.netiq.com)
- Assistenza tecnica (http://support.novell.com/contact/getsupport.html?sourceidint=suplnav4_phonesup)
- Supporto in autonomia (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- Sito per il download delle patch (http://download.novell.com/index.jsp)
- Forum di supporto della comunità di Sentinel (http://forums.novell.com/novell-product-support-forums/sentinel/)
- TID di Sentinel (http://support.novell.com/products/sentinel)
- Sito Web dei plug-in di Sentinel (http://support.novell.com/products/sentinel/secure/sentinel61.html)
- **Elenco delle notifiche via e-mail:** iscrizione tramite il sito Web dei plug-in di Sentinel

Contattare l'assistenza alle vendite

Per informazioni relative ai prodotti, ai prezzi e alle funzionalità, rivolgersi al rivenditore locale. Nell'eventualità ciò non sia possibile, contattare il team di assistenza alle vendite.

Sedi globali: Uffici NetIQ (http://www.netiq.com/about_netiq/officelocations.asp)

Stati Uniti e Canada: 888-323-6768

E-mail: info@netiq.com

Sito Web: www.netiq.com

1 Panoramica di Sentinel

Sentinel è una soluzione SIEM (Security, Information and Event Management) e di monitoraggio della conformità che monitora automaticamente gli ambienti IT più complessi e garantisce la sicurezza necessaria per proteggerli.

1.1 Le ragioni che rendono importante la sicurezza

La sicurezza deve diventare una delle preoccupazioni prioritarie delle aziende moderne che mirano a ridurre i costi e a fidelizzare la clientela. Considerando che ogni record perduto ha un costo medio di 200 USD, una sola violazione e un paio di centinaia di record persi possono produrre un effetto significativo per l'azienda.

Se e quando la vostra azienda sarà oggetto di attacco, le possibili spese includono:

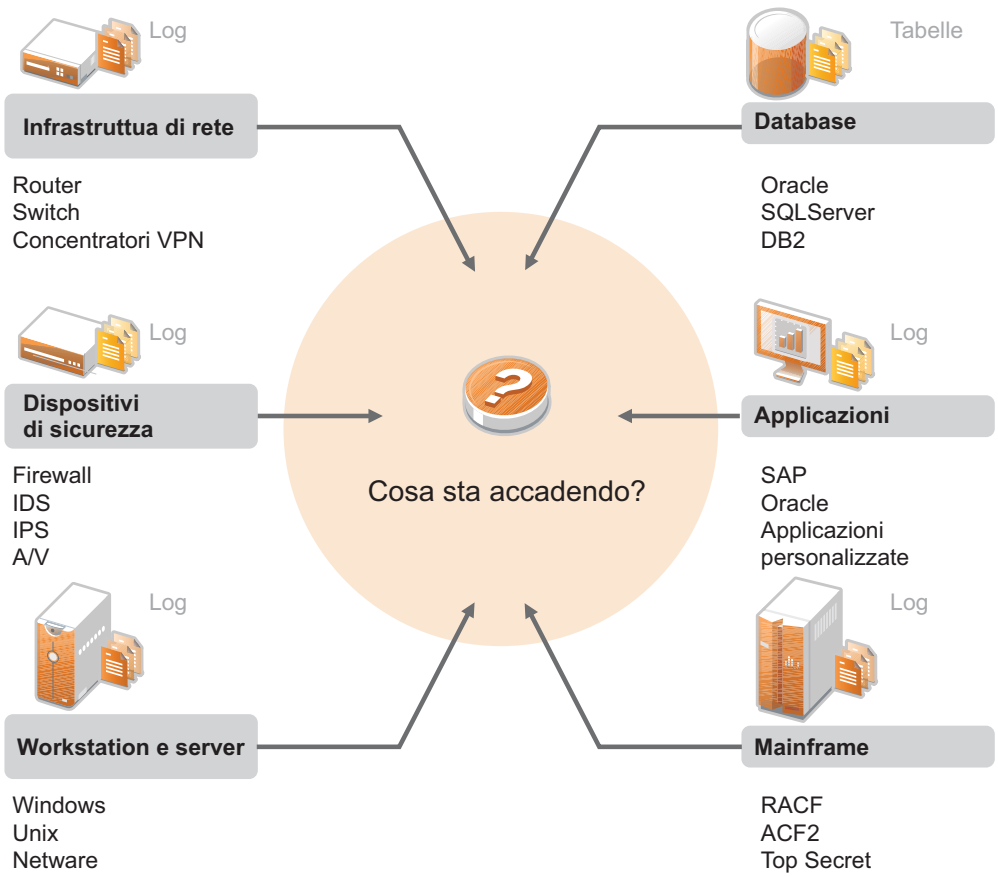
- Costi legali
- Costi d'indagine e forensi
- Aumento delle revisioni
- Multe e sanzioni
- Costo nascosto della perdita di credibilità con i clienti
- Cambiamento della clientela a causa della perdita di credibilità

Ciò dimostra l'importanza della sicurezza per il vostro ambiente IT. Internet e il crescente utilizzo delle tecnologie cloud stanno rendendo sempre meno netto il confine che separa il personale interno da quello esterno.

1.2 Le sfide da affrontare per rendere sicuro l'ambiente IT

A causa della complessità che caratterizza gli ambienti IT, renderli sicuri è una vera e propria sfida. Esistono numerose applicazioni, database, mainframe, workstation e server di vario tipo, ognuno dei quali genera log specifici degli eventi che si verificano. A questi si aggiungono i dispositivi di sicurezza e quelli dell'infrastruttura di rete, ognuno dei quali fornisce log relativi a quanto avviene nell'ambiente IT.

Figura 1-1 *Eventi dell'ambiente IT*



Le sfide nascono dal fatto che:

- Nell'ambiente IT sono presenti numerosi dispositivi
- I log sono in formati diversi
- I log sono memorizzati in silos
- I log generano una grande quantità di informazioni
- Per individuare i responsabili dei vari eventi è necessario analizzare tutti i log manualmente

Affinché le informazioni siano utili è necessario essere in grado di:

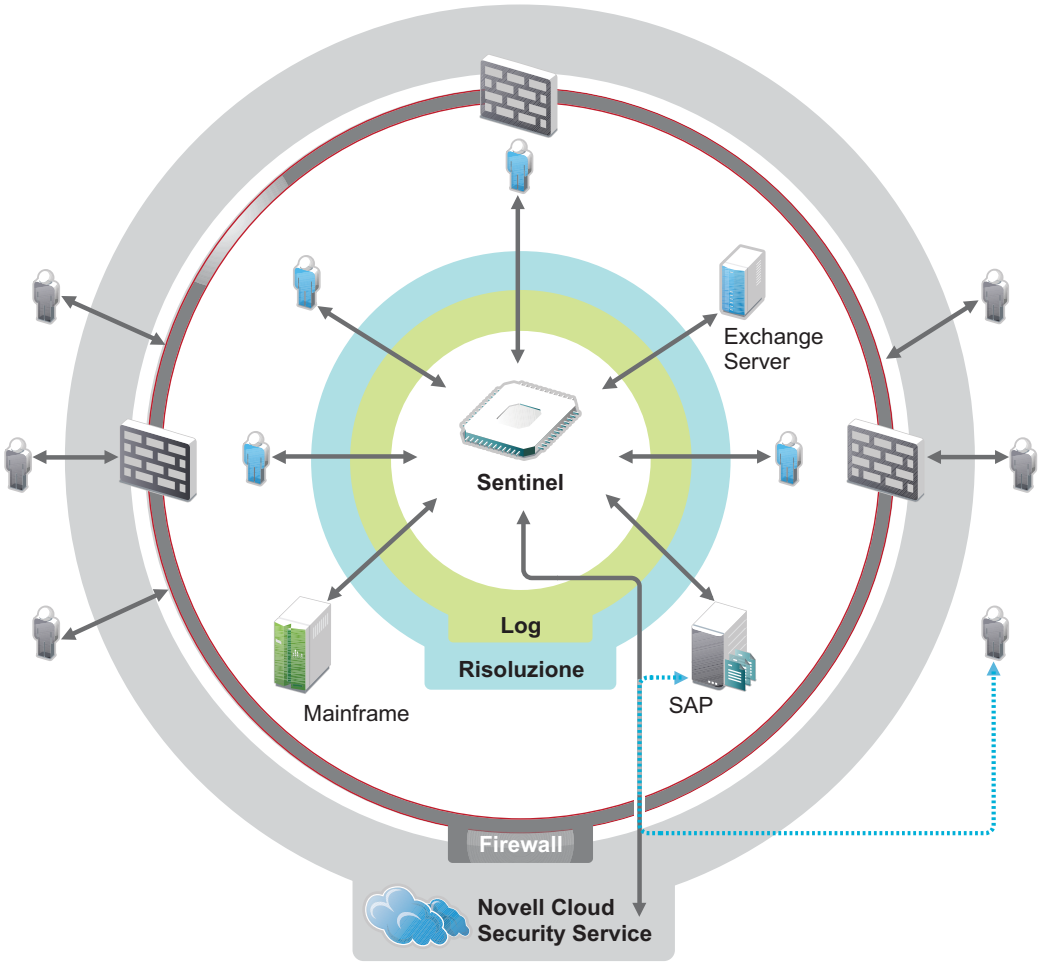
- Raccogliere i dati
- Consolidare i dati
- Normalizzare dati molto diversi in eventi che possono essere comparati facilmente
- Mappare gli eventi a normative standard
- Analizzare i dati
- Confrontare gli eventi di più sistemi per stabilire se sussistono problemi per la sicurezza
- Inviare notifiche quando i dati non sono conformi alle norme previste
- Avviare azioni a seguito delle notifiche, al fine di garantire la conformità alle policy aziendali
- Generare rapporti per dimostrare la conformità

Una volta comprese le sfide da affrontare per rendere sicuro il vostro ambiente IT, dovrete stabilire come rendere sicura l'azienda per gli utenti ma anche come proteggerla da essi senza trattarli come criminali o sovraccaricarli al punto da azzerarne la produttività. Sentinel vi offre la soluzione.

1.3 La soluzione Sentinel

Sentinel funge da sistema nervoso centrale della sicurezza aziendale. Raccoglie i dati provenienti da tutta l'infrastruttura, vale a dire da applicazioni, database, server e dispositivi di memorizzazione e sicurezza, Consente di analizzare e mettere in correlazione i dati, automaticamente o manualmente, rendendoli più pratici.

Figura 1-2 *La soluzione Sentinel*



Grazie a Sentinel potete essere informati sugli eventi importanti che si verificano nel vostro ambiente IT in un preciso momento e avere la possibilità di collegare le azioni intraprese sulle risorse alle persone che le intraprendono. In questo modo potrete conoscere i comportamenti degli utenti e monitorare efficacemente il controllo. A prescindere dal fatto che l'utente sia un interno o un esterno, potrete raggruppare tutte le azioni che svolge e quindi individuare le attività rischiose prima che arrechino danni.

Sentinel svolge queste funzioni senza gravare eccessivamente sui costi poiché:

- Offre un'unica soluzione per gestire i controlli IT in funzione di normative diverse.

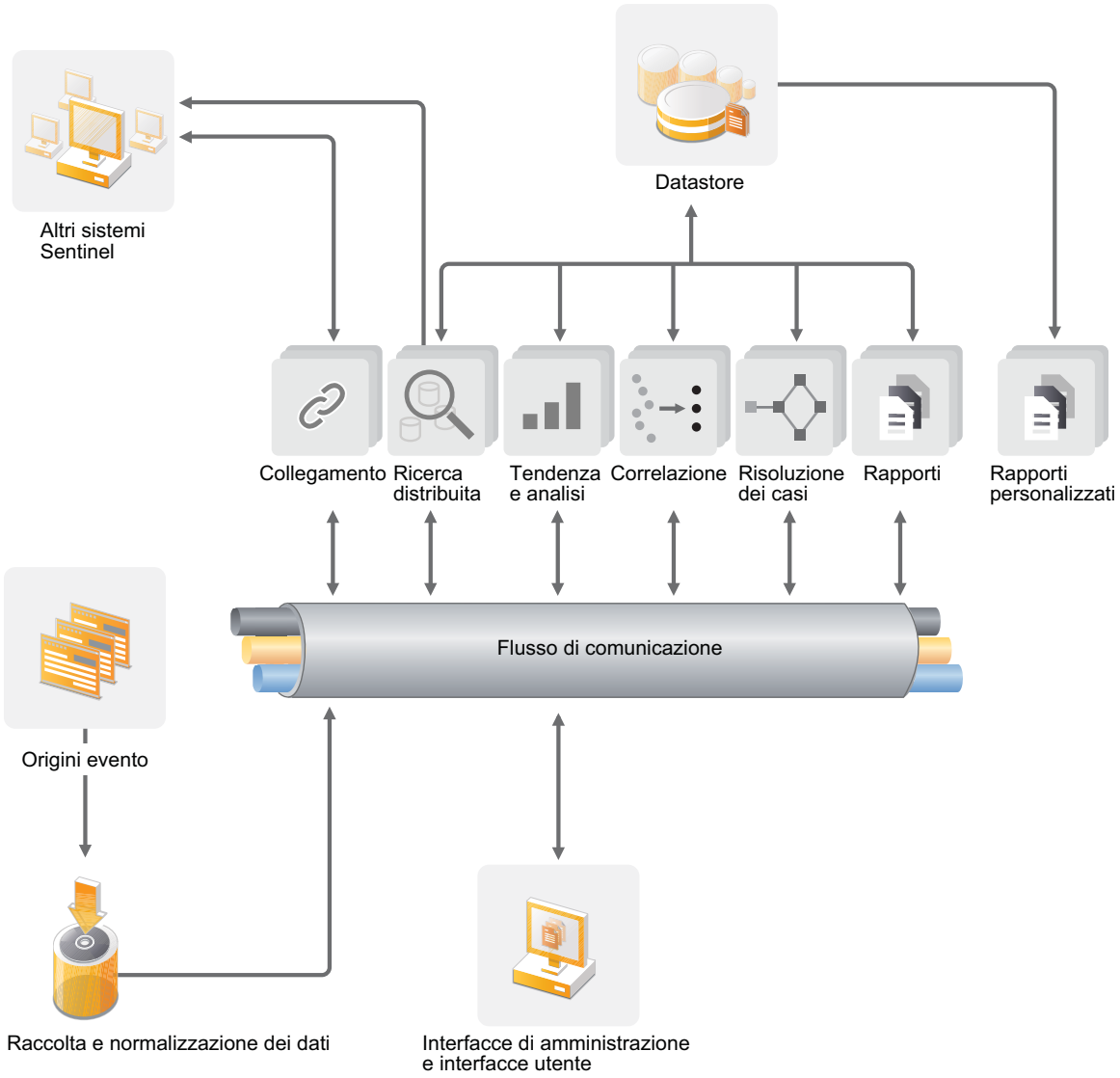
- Colma il gap cognitivo fra ciò che le norme prevedono e quello che effettivamente avviene nell'ambiente di rete.
- Dimostra ai revisori e ai funzionari che la vostra organizzazione documenta, monitora e genera rapporti sui controlli di sicurezza.
- Include programmi di monitoraggio della conformità e di reportistica pronti all'uso.
- Consente di acquisire la visibilità e il controllo necessari per verificare costantemente la conformità della vostra organizzazione e i programmi di sicurezza.

Sentinel automatizza i processi di raccolta dei log, analisi e generazione dei rapporti affinché i controlli IT soddisfino efficacemente le esigenze di rilevamento delle minacce e revisione. Sentinel fornisce un monitoraggio automatizzato degli eventi di sicurezza, degli eventi di conformità e dei controlli IT, consentendo di intervenire tempestivamente qualora si produca una violazione alla sicurezza o un evento di non conformità. Inoltre, Sentinel permette di raccogliere facilmente le informazioni di riepilogo relative all'ambiente, affinché sia possibile comunicare alle principali parti interessate la condizione generale rispetto alla sicurezza.

2 Le funzioni di Sentinel

Sentinel gestisce costantemente le informazioni e gli eventi relativi alla sicurezza sfruttando l'ambiente IT dell'utente per fornire una soluzione di monitoraggio completa. La figura seguente illustra in che modo Sentinel svolge queste funzioni.

Figura 2-1 *Le funzioni di Sentinel*



Le funzioni svolte da Sentinel sono:

- Raccolta di log, eventi e informazioni sulla sicurezza da tutte le diverse origini degli eventi presenti nell'ambiente IT.
- Standardizzazione in un unico formato, di log, eventi e informazioni sulla sicurezza.
- Inserimento delle informazioni standardizzate in un bus dei messaggi, capace di trasmettere migliaia di pacchetti di messaggi al secondo.
- Comunicazione con tutti i componenti di Sentinel mediante il bus dei messaggi ai fini della scalabilità.

I vari componenti di Sentinel accedono quindi al bus dei messaggi e Sentinel esegue o permette di eseguire le operazioni seguenti:

- Memorizzazione degli eventi in un datastore basato su file, con policy di permanenza dei dati flessibili e personalizzabili.
- Collegamento gerarchico di più sistemi Sentinel, inclusi Sentinel Log Manager, Sentinel e Sentinel Rapid Deployment.
- Ricerca di eventi non solo nel server Sentinel locale, ma anche in altri server Sentinel situati in altre parti del mondo.
- Analisi statistica per definire una linea di base da mettere a confronto con quanto sta avvenendo allo scopo di stabilire se esistono problemi che non sono stati rilevati.
- Correlazione di un gruppo di eventi simili o confrontabili in un determinato periodo al fine di stabilire uno schema.
- Organizzazione degli eventi in incidenti ai fini della gestione delle risposte e del controllo.
- Rapporti sulle capacità in base agli eventi in tempo reale e a quelli presenti nella cronologia.

Nelle sezioni seguenti si illustrano nel dettaglio i componenti di Sentinel.

2.1 Origini evento

Sentinel raccoglie informazioni ed eventi relativi alla sicurezza da diverse origini all'interno del vostro ambiente IT. Tali origini sono denominate origini degli eventi e possono essere numerosi elementi diversi presenti sulla rete.

Nella figura seguente sono rappresentate alcune delle origini degli eventi da cui Sentinel può raccogliere informazioni:

Perimetro di sicurezza: Dispositivi e software utilizzati per creare un parametro di sicurezza per l'ambiente dell'utente.

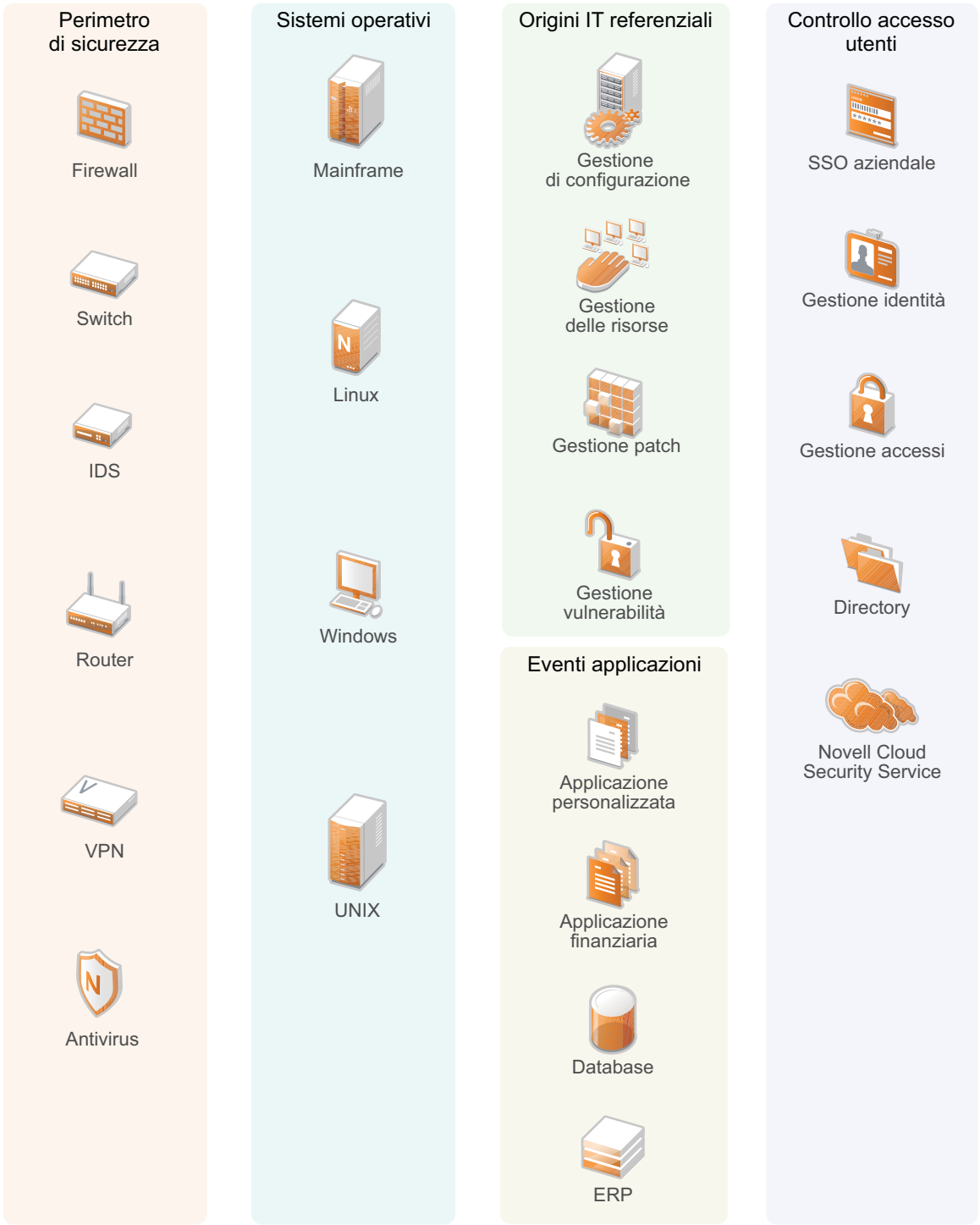
Sistemi operativi: eventi di diversi sistemi operativi utilizzati nella rete.

Origini IT referenziali: software utilizzato per eseguire manutenzione e controllo di risorse, patch, configurazione e vulnerabilità.

Eventi delle applicazioni: eventi generati dalle applicazioni installate nella rete.

Controllo degli accessi degli utenti: eventi generati da applicazioni o dispositivi che consentono agli utenti di accedere alle risorse aziendali.

Figura 2-2 *Origini evento*



2.2 Evento Sentinel

Sentinel riceve le informazioni dai dispositivi, le normalizza in una struttura denominata evento che, successivamente, categorizza e invia per l'elaborazione. Grazie all'aggiunta di informazioni categorizzate (tassonomia) agli eventi, questi possono essere comparati più semplicemente tra i

sistemi che li segnalano secondo modalità distinte. Ad esempio, gli errori relativi all'autenticazione. Gli eventi vengono elaborati dal motore di correlazione con visualizzazione in tempo reale, dai dashboard e dal server di back end.

Un evento contiene oltre 200 campi. I campi di un evento sono di vario tipo e vengono utilizzati per diversi scopi. Esistono alcuni campi predefiniti come, ad esempio, quelli che fanno riferimento alla gravità, la criticità, l'IP di destinazione e la porta di destinazione. Sono presenti due set di campi configurabili: i campi riservati, solo per uso interno di Sentinel, consentono espansioni future, mentre i campi personalizzati sono concepiti per permettere le estensioni dei clienti.

Lo scopo dei campi può comunque essere modificato mediante la loro ridenominazione. L'origine di un campo può essere esterna, vale a dire configurata esplicitamente dal dispositivo o dal servizio di raccolta corrispondente, oppure può essere referenziale. Il valore di un campo referenziale viene calcolato come una funzione di uno o più campi diversi mediante il servizio di mappatura. Ad esempio, un campo può essere definito come il codice di costruzione della struttura contenente la risorsa menzionata come l'IP di destinazione di un evento. Ad esempio, un campo può essere calcolato dal servizio di mappatura mediante una mappatura definita dal cliente che utilizza l'IP di destinazione dell'evento.

- Sezione 2.2.1, “Servizio di mappatura”, a pagina 15
- Sezione 2.2.2, “Streaming delle mappe”, a pagina 15
- Sezione 2.2.3, “Rilevamento degli exploit (Servizio di mappatura)”, a pagina 16

2.2.1 Servizio di mappatura

Il servizio di mappatura consente di elaborare un meccanismo complesso per propagare i dati aziendali rilevanti in tutto il sistema. Tali dati possono arricchire gli eventi con informazioni referenziali, fornendo il contesto necessario affinché gli analisti siano in grado di adottare le decisioni in modo più efficace, redattare rapporti più utili e scrivere regole di correlazioni più razionali.

L'utente può integrare i dati evento utilizzando le mappature per aggiungere ulteriori informazioni, quali i dettagli relativi a host e identità, agli eventi che vengono recuperati dai dispositivi di origine. Tali informazioni aggiuntive possono essere utilizzate per eseguire correlazioni o generare rapporti avanzati. Oltre a quelle personalizzate definite dall'utente, il sistema supporta diverse mappature incorporate.

Le mappature definite in Sentinel vengono memorizzate in due modi:

- Le mappature incorporate sono memorizzate nel database, vengono aggiornate mediante le API nel codice del servizio di raccolta ed esportate automaticamente nel servizio di mappatura.
- Le mappature personalizzate vengono memorizzate come file CSV e possono essere aggiornate sul file system o mediante la Map Data Configuration UI (interfaccia utente di configurazione dei dati di mappatura), per essere quindi caricate dal servizio di mappatura.

In entrambi i casi, i file CSV vengono conservati nel server Sentinel centrale ma le modifiche alle mappature sono distribuite a ciascuna Gestione servizi di raccolta e applicate localmente. Questa elaborazione distribuita assicura che l'attività di mappatura non sovraccarichi il server principale.

2.2.2 Streaming delle mappe

Il servizio di mappatura utilizza un modello di aggiornamento dinamico ed esegue lo streaming delle mappe da un punto all’altro, evitando la creazione di mappe statiche di grandi dimensioni nella memoria dinamica. L’importanza della capacità di streaming è particolarmente rilevante in un

sistema in tempo reale mission-critical, ad esempio quello di Sentinel dove è necessario un movimento costante, prevedibile e veloce dell'indipendenza dei dati di qualsiasi carico transitorio sul sistema.

2.2.3 Rilevamento degli exploit (Servizio di mappatura)

Sentinel consente di creare riferimenti incrociati tra le firme dei dati relativi agli eventi e i dati della scansione delle vulnerabilità. Ciò consente di inviare una notifica immediata e automatica agli utenti quando un attacco cerca di penetrare in un sistema vulnerabile. Tale funzionalità è garantita da:

- feed di dati di Advisor
- rilevamento delle intrusioni
- scansione delle vulnerabilità
- Firewall

In Advisor è incluso un riferimento incrociato tra le firme dei dati relativi agli eventi e i dati relativi alla scansione delle vulnerabilità. Il feed di dati Advisor contiene informazioni relative alle vulnerabilità e alle minacce oltre che una normalizzazione delle firme eventi e dei plug-in di vulnerabilità. Per ulteriori informazioni relative a Advisor, vedere "Configuring Advisor (Configurazione di Advisor)" in *NetIQ Sentinel 7.0.1 Administration Guide (Guida all'amministrazione di NetIQ Sentinel 7.0)*.

2.3 Connettori

I connettori hanno la funzione di stabilire le connessioni fra le origini degli eventi e il sistema Sentinel. Utilizzando i protocolli standard del settore per recuperare eventi quali syslog, JDBC da leggere mediante le tabelle del database, WMI da leggere mediante i log degli eventi di Windows e così via, i connettori forniscono:

- Trasporto dei dati evento non elaborati dalle origini evento al servizio di raccolta.
- Connessione per il filtraggio specifico.
- Connessione per la gestione degli errori.

2.4 Servizi di raccolta

I servizi di raccolta raccolgono e standardizzano le informazioni provenienti dai connettori. I servizi di raccolta sono scritti in Javascript e definiscono la logica per:

- Ricezione dei dati non elaborati dai servizi di raccolta.
- Analisi sintattica e normalizzazione dei dati.
- Applicazione della logica di ripetibilità ai dati.
- Conversione dei dati specifici del dispositivo in dati specifici di Sentinel.
- Formattazione degli eventi.
- Passaggio dei dati normalizzati, analizzati sintatticamente e formattati a Gestione servizi di raccolta.

2.5 Gestione servizi di raccolta

Gestione servizi di raccolta gestisce la raccolta dei dati, monitora i messaggi di stato del sistema e applica i filtri agli eventi in base secondo necessità. Le funzioni principali di Gestione servizi di raccolta sono:

- Trasformazione degli eventi..
- Aggiunta di pertinenza aziendale agli eventi mediante il servizio di mappatura.
- Filtraggio globale degli eventi.
- Instradamento degli eventi.
- Distinzione fra dati in tempo reale, vulnerabilità, risorse e dati non in tempo reale.
- Invio di un messaggio di stato al server Sentinel.

2.6 Bus di comunicazione

Il bus di comunicazione utilizza un'architettura basata su standard e orientata ai servizi (SOA) che associa i vantaggi dell'elaborazione in memoria a quelli dell'elaborazione distribuita. Questo bus è denominato iSCALE ed è un bus dei messaggi speciale, in grado di gestire volumi elevati di dati.

- Sezione 2.6.1, "Bus messaggi", a pagina 17
- Sezione 2.6.2, "Canali", a pagina 18

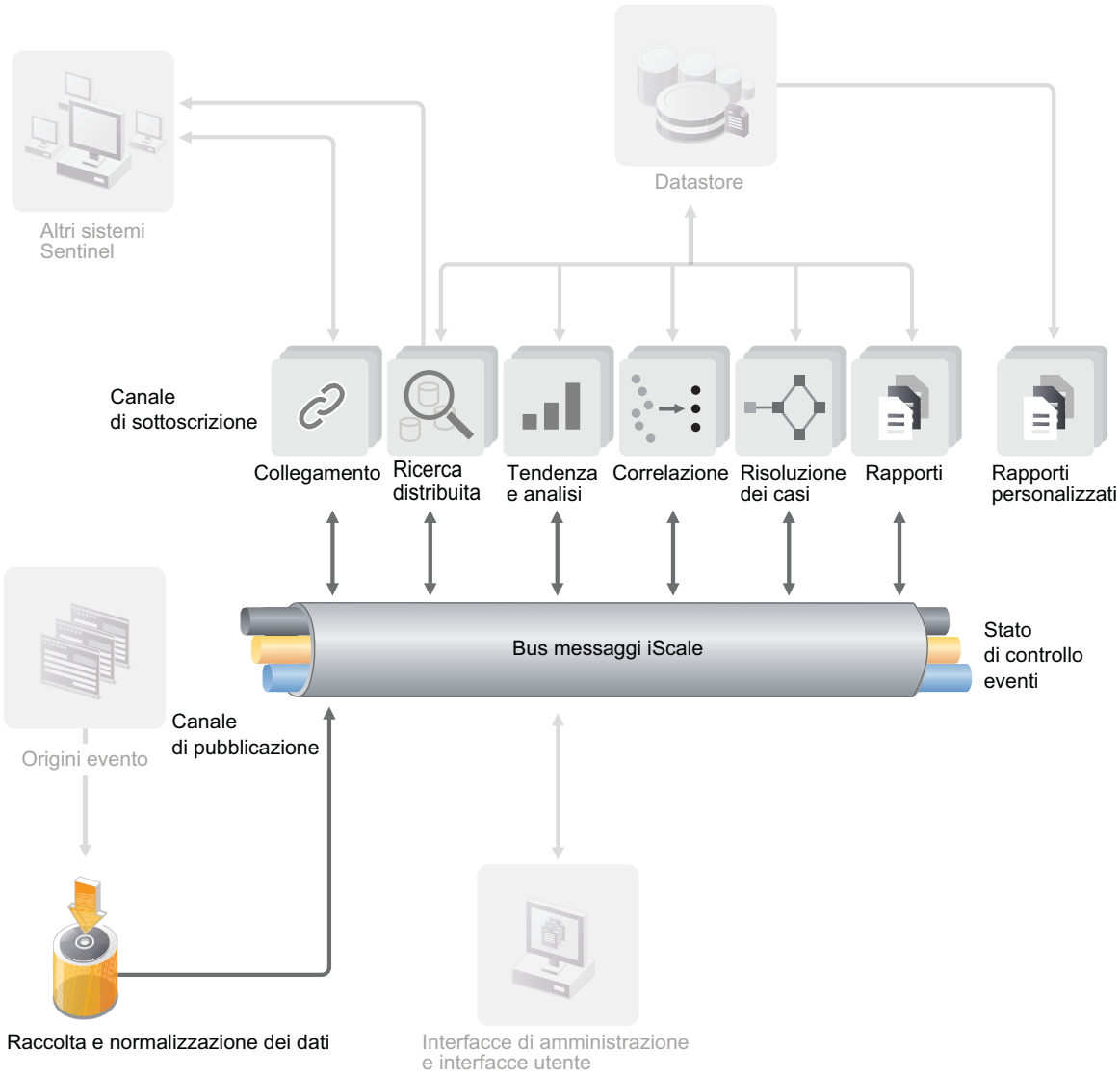
2.6.1 Bus messaggi

Il bus messaggi iSCALE consente di scalare in modo indipendente i singoli componenti e allo stesso tempo di eseguire un'integrazione basata sugli standard con le applicazioni esterne. La chiave della scalabilità risiede nel fatto che, diversamente da altro software distribuito, due componenti peer non comunicano mai tra di loro in modo diretto. Tutti i componenti comunicano attraverso il bus dei messaggi, il quale è in grado di spostare migliaia di pacchetti di messaggi al secondo.

Sfruttando le incredibili capacità del bus messaggi, il canale di comunicazione a elevata capacità di trasmissione riesce a ridurre al minimo e a sostenere una elevata frequenza di trasmissione dei dati lungo i componenti indipendenti del sistema. Gli eventi sono compressi e cifrati via cavo per garantire una consegna sicura ed efficiente dal limite della rete o dai punti di raccolta all'hub del sistema, dove vengono eseguite le analisi in tempo reale.

Il bus messaggi iSCALE utilizza una serie di servizi per inviare i messaggi in coda che migliorano l'affidabilità delle comunicazioni al di la degli aspetti di sicurezza e delle prestazioni della piattaforma. Mediante una serie di code transitorie e durature, il sistema garantisce un'affidabilità e una tolleranza agli errori senza paragoni. Ad esempio, i messaggi importanti in transito sono salvati (inserendoli in coda) in caso di errore nel percorso di comunicazione. Una volta che il sistema ha risolto gli errori che si sono verificati e ha eseguito il ripristino, il messaggio in coda viene inviato a destinazione.

Figura 2-3 *Bus dei messaggi iSCALE*



2.6.2 Canali

La piattaforma iSCALE utilizza un modello basato sui dati o sugli eventi che consente di scalare in modo indipendente i componenti dell'intero sistema in base al carico di lavoro. Si ottiene così una distribuzione flessibile che si adatta all'ambiente specifico del cliente, in quanto un sito può avere una grande quantità di dispositivi con volumi contenuti di eventi, mentre un altro può avere un numero inferiore di dispositivi ma volumi elevati di eventi. In questi casi, le densità degli eventi, ovvero l'aggregazione e lo schema multiplex degli eventi sul cavo dai punti di raccolta, sono diverse e il bus dei messaggi consente di scalare in modo coerente carichi di lavoro molto diversi.

iSCALE sfrutta un ambiente indipendente con canali multipli che elimina qualsiasi contenzioso e incoraggia l'elaborazione parallela degli eventi. Questi canali e sottocanali non lavorano solo per il trasporto dei dati relativi agli eventi ma offrono inoltre un controllo accurato dei processi per scalare e bilanciare il carico del sistema in varie condizioni di carico. L'utilizzo di canali di servizio indipendenti, ad esempio canali di controllo e di stato, in aggiunta al principale canale degli eventi, consente di scalare in modo sofisticato ed efficace in termini di costo l'architettura basata sugli eventi.

2.7 Memorizzazione dei dati

Sentinel offre varie opzioni per la memorizzazione dei dati raccolti. Per default, riceve da Gestioni servizi di raccolta due flussi di dati separati ma simili: i dati degli eventi e i dati non elaborati, che vengono memorizzati nel file system locale del server Sentinel.

È possibile configurare Sentinel affinché memorizzi i dati in un'ubicazione sulla rete. Sentinel può essere configurato anche in modo che gli eventi vengano memorizzati in un database esterno, in base a policy di sincronizzazione dei dati. Per ulteriori informazioni, vedere "Configurazione della memorizzazione dei dati" nella *NetIQ Sentinel 7.0.1 Administration Guide (Guida all'amministrazione di NetIQ Sentinel 7.0.1)*.

2.8 Filtri

I filtri di Sentinel consentono di personalizzare la ricerca degli eventi ed evitare il sovraccarico di dati. Questa funzione rende disponibile un Generatore filtro utile per creare interrogazioni di ricerca semplici e complesse. Le interrogazioni di ricerca possono essere salvate come filtro e riutilizzate secondo necessità, effettuando così la ricerca semplicemente selezionando il filtro invece di specificarla manualmente tutte le volte.

Potete riutilizzare i filtri quando usate o configurate funzioni di Sentinel quali:

- Creazione dei dashboard di Security Intelligence.

  Per ulteriori informazioni, vedere "Creating a Dashboard (Creazione di un dashboard)" nella *NetIQ Sentinel 7.0.1 User Guide (Guida dell'utente di NetIQ Sentinel 7.0.1)*.

- Visualizzazione di eventi in tempo reale in Active Views.

  Per ulteriori informazioni, vedere "Viewing Events (Visualizzazione degli eventi)" in *NetIQ Sentinel 7.0.1 User Guide (Guida dell'utente di NetIQ Sentinel 7.0.1)*.

- Configurazione delle policy di permanenza dei dati.

  Per ulteriori informazioni, vedere "Configuring Data Retention Policies (Configurazione delle policy di permanenza dei dati)" in *NetIQ Sentinel 7.0.1 Administration Guide (Guida all'amministrazione di NetIQ Sentinel 7.0.1)*.

- Configurazione della sincronizzazione dei dati.

  Per ulteriori informazioni, vedere "Configurazione della sincronizzazione dei dati" nella *NetIQ Sentinel 7.0.1 Administration Guide (Guida all'amministrazione di NetIQ Sentinel 7.0.1)*.

- Test di una regola di correlazione.

  Per ulteriori informazioni, vedere, "Correlating Event Data (Correlazione dei dati evento)" nella *NetIQ Sentinel 7.0.1 User Guide (Guida per l'utente di NetIQ Sentinel 7.0.1)*.

Sentinel fornisce per default un elenco di filtri, oltre a consentire la creazione di filtri personalizzati. Per ulteriori informazioni, vedere "Configuring Filters (Configurazione dei filtri)" nella *NetIQ Sentinel 7.0.1 User Guide (Guida per l'utente di NetIQ Sentinel 7.0.1)*.

2.9 Correlazione

Anche se un solo evento può sembrare irrilevante, in combinazione con altri eventi potrebbe informare sulla presenza di un problema potenziale. Sentinel consente di eseguire la correlazione di tali eventi nel Motore di correlazione grazie alle regole create e distribuite dall'utente, permettendo di intervenire nel modo più appropriato e attenuare tali problemi.

Grazie alla correlazione sono disponibili nuove funzioni di gestione degli eventi di sicurezza, le quali consentono di automatizzare l'analisi del flusso di eventi in ingresso per individuare eventuali schemi di interesse. La correlazione consente di definire regole per l'identificazione di minacce critiche e modelli di attacco complessi, al fine di poter stabilire una priorità per gli eventi, nonché reagire e gestire i casi in modo efficace. Per ulteriori informazioni, vedere, "Correlating Event Data (Correlazione dei dati evento)" nella *NetIQ Sentinel 7.0.1 User Guide (Guida per l'utente di NetIQ Sentinel 7.0.1)*.

2.10 Security Intelligence

La funzione di correlazione di Sentinel consente di conoscere i modelli di attività, sia per motivi di sicurezza, conformità o altro. La funzione Security Intelligence ricerca l'attività anomala e potenzialmente pericolosa, ma non confronta alcun modello noto.

La funzione Security Intelligence di Sentinel si concentra sull'analisi statistica dei dati relativi alle serie di tempi, al fine di consentire agli analisti d'individuare e analizzare le deviazioni (anomalie) sia tramite un motore statistico automatico che mediante la rappresentazione visiva dei dati statistici per l'interpretazione manuale. Per ulteriori informazioni, vedere "Analisi di tendenze nei dati" nella *NetIQ Sentinel 7.0.1 User Guide (Guida per l'utente di NetIQ Sentinel 7.0.1)*.

2.11 iTRAC

I workflow iTRAC sono stati concepiti al fine di offrire una soluzione semplice e flessibile per l'automatizzazione e il controllo dei processi aziendali di risposta agli incidenti. iTRAC sfrutta il sistema degli incidenti di Sentinel per controllare la sicurezza o i problemi del sistema dall'identificazione (mediante regole di correzione o identificazione manuale) fino alla risoluzione.

I workflow possono essere creati utilizzando procedure manuali o automatiche. Sono supportate funzioni avanzate quali diramazione, riassegnazione in base al tempo e variabili locali. L'integrazione con script e plug-in esterni consente l'interazione flessibile con sistemi di terze parti. I rapporti completi permettono agli amministratori di comprendere e ottimizzare i processi di risposta agli incidenti. Per ulteriori informazioni, vedere "Configuring iTRAC Workflows (Configurazione dei workflow di iTRAC)" in *NetIQ Sentinel 7.0.1 User Guide (Guida dell'utente di NetIQ Sentinel 7.0.1)*.

2.12 Rapporti

Sentinel vi consente di creare rapporti sui dati raccolti. Sentinel viene offerto con una varietà di rapporti personalizzabili, alcuni dei quali sono di carattere generale mentre altri sono specifici del dispositivo (ad esempio, SUSE Linux). Alcuni rapporti sono flessibili e consentono agli utenti di specificare le colonne da visualizzare nei risultati.

Gli utenti possono eseguire, programmare e inviare tramite e-mail i rapporti in formato PDF. Possono inoltre eseguire qualsiasi rapporto come una ricerca e quindi interagire con i risultati proprio come una qualsiasi ricerca, cioè perfezionandoli o eseguendo un'azione sui risultati. I rapporti possono

anche essere eseguiti sui server Sentinel distribuiti in diverse ubicazioni geografiche. Per ulteriori informazioni, vedere "Reporting (Generazione di rapporti)" in *NetIQ Sentinel 7.0.1 User Guide (Guida dell'utente di NetIQ Sentinel 7.0.1)*.

2.13 Analisi evento

Sentinel offre un potente set di strumenti che facilitano il reperimento e l'analisi di dati evento critici. Il sistema è configurato e ottimizzato affinché possa offrire la massima efficienza per ogni tipo specifico di analisi. È dotato, inoltre, di metodi che consentono la transizione semplificata e lineare tra i vari tipi di analisi.

L'esame degli eventi in Sentinel spesso inizia con la visualizzazione in tempo reale di Active Views. Sebbene siano disponibili molti altri strumenti avanzati, Active Views visualizza i flussi evento filtrati insieme a grafici di riepilogo che possono essere utilizzati per un'analisi semplice e approssimativa delle tendenze dei dati, dei dati evento e dell'identificazione di eventi specifici. Familiarizzando con il prodotto, l'utente sarà in grado di creare filtri configurati per classi specifici di dati, come gli output provenienti dalla correlazione. Active Views può essere utilizzato come un dashboard in cui viene visualizzata un'attitudine relativa alla sicurezza e operatività generica.

Successivamente, è possibile utilizzare la ricerca interattiva per elaborare analisi degli eventi più dettagliate. In questo modo, è possibile eseguire ricerche più rapide e semplici e trovare i dati relativi a determinate interrogazioni, come attività in base a un utente o su un sistema particolare. Selezionando i dati evento o utilizzando il riquadro di ottimizzazione a sinistra, è possibile concentrarsi rapidamente su eventi particolarmente interessanti.

Durante l'analisi di centinaia di eventi, le funzioni di generazione dei rapporti offerte da Sentinel forniscono un controllo personalizzato del layout degli eventi, consentendo la visualizzazione di ampi volumi di dati. Sentinel rende la transizione più semplice in quanto consente di trasferire le ricerche interattive create nell'interfaccia di ricerca, in un modello di generazione dei rapporti in grado di creare all'istante un rapporto, in cui vengono visualizzati gli stessi dati, ma in un formato organizzato meglio e concepito per numero di eventi elevato.

A tale scopo, Sentinel include numerosi modelli. Alcuni sono configurati per consentire la visualizzazione di particolari tipi di informazioni, come i dati di autenticazione o la creazione di utenti, mentre altri sono di tipo più generico e consentono di personalizzare i gruppi e le colonne del rapporto in modo interattivo.

Familiarizzando con il prodotto, l'utente sarà in grado di sviluppare i filtri e i rapporti più comuni semplificando notevolmente i workflow. Sentinel supporta totalmente la memorizzazione di queste informazioni e le distribuisce a tutto il personale dell'azienda. Per ulteriori informazioni, vedere (Generazione di rapporti) *NetIQ Sentinel 7.0.1 User Guide (Guida dell'utente di NetIQ Sentinel 7.0.1)*.