Übersichtshandbuch

Sentinel 7.0.1

March 2012

Rechtliche Hinweise

Weitere Informationen erhalten Sie von NetIQ unter folgender Anschrift:

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

Inhalt

Allgemeines zu diesem Handbuch

Dieses Handbuch bietet eine Übersicht über das WorkloadIQ-Produkt Sentinel.

Zielgruppe

Dieses Handbuch ist für Mitarbeiter des Bereichs Informationssicherheit vorgesehen.

Rückmeldungen

Wir freuen uns über Ihre Hinweise, Anregungen und Vorschläge zu diesem Handbuch und den anderen Teilen der Dokumentation zu diesem Produkt. Über die Funktion „Benutzerkommentare“ unten auf den einzelnen Seiten der Onlinedokumentation können Sie uns Ihre Kommentare mitteilen.

Aktualisierungen der Dokumentation

Die neueste Version des *NetIQ Sentinel 7.0.1-Übersichtshandbuchs* finden Sie auf der Sentinel-Dokumentationswebsite (http://www.novell.com/documentation/sentinel70).

Weitere Dokumentation

Die technische Dokumentation von Sentinel umfasst mehrere Bände. Dazu gehören:

- Sentinel Quick Start Guide (Kurzanleitung für Sentinel) (http://www.novell.com/documentation/sentinel70/s70_quickstart/data/s70_quickstart.html)
- Sentinel Installation Guide (Sentinel-Installationshandbuch) (http://www.novell.com/documentation/sentinel70/s70_install/data/bookinfo.html)
- Sentinel Administration Guide (Sentinel-Administrationshandbuch) (http://www.novell.com/documentation/sentinel70/s70_admin/data/bookinfo.html)
- Sentinel User Guide (Sentinel-Benutzerhandbuch) (http://www.novell.com/documentation/sentinel70/s70_user/data/bookinfo.html)
- Sentinel Link Overview Guide (Sentinel Link-Übersichtshandbuch) (http://www.novell.com/documentation/sentinel70/sentinel_link_overview/data/bookinfo.html)
- Sentinel Internal Audit Events (Sentinel-interne Auditereignisse) (http://www.novell.com/documentation/sentinel70/s70_auditevents/data/bookinfo.html)
- Sentinel SDK (http://www.novell.com/developer/develop_to_sentinel.html)

  Auf der Sentinel SDK-Website finden Sie Informationen zum Erstellen eigener Plugins.

Anfragen an Novell und NetIQ

Sentinel ist nun ein Produkt von NetIQ. Novell leistet jedoch noch viele der Supportfunktionen.

- Novell-Website (http://www.novell.com)

- NetIQ-Website (http://www.netiq.com)
- Technischer Support (http://support.novell.com/contact/getsupport.html?sourceidint=suplnav4_phonesup)
- Self-Support (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- Patch Download Site (http://download.novell.com/index.jsp)
- Sentinel Community Support Forum (http://forums.novell.com/novell-product-support-forums/sentinel/)
- Sentinel TIDS (http://support.novell.com/products/sentinel)
- Sentinel-Plugin-Website (http://support.novell.com/products/sentinel/secure/sentinel61.html)
- **EMail-Liste für Benachrichtigungen:** Registrieren Sie sich auf der Sentinel-Plugin-Website.

Anfragen an die Verkaufsunterstützung

Bei Fragen zu Produkten, Preisen und Funktionen wenden Sie sich an Ihren Händler vor Ort. Wenn dies nicht möglich ist, wenden Sie sich an unser Verkaufsunterstützungsteam.

Weltweit: NetIQ-Standorte (http://www.netiq.com/about_netiq/officelocations.asp)

Vereinigte Staaten und Kanada: 888-323-6768

EMail: info@netiq.com

Website: www.netiq.com

1 Produktübersicht zu Sentinel

Sentinel ist eine Lösung für das Sicherheitsinformations- und Ereignismanagement (SIEM) und die Compliance-Überwachung. Sentinel überwacht die komplexesten IT-Umgebungen automatisch und stellt die für den Schutz der IT-Umgebung erforderliche Sicherheit bereit.

1.1 Warum ist Sicherheit so wichtig?

Sicherheit sollte in heutigen Unternehmen von äußerstem Vorrang sein, denn dadurch lassen sich Kosten reduzieren und Kunden an das Unternehmen binden. Jeder durch ein Sicherheitsproblem verlorene Datensatz kostet durchschnittlich 200 Dollar. Eine einzige Sicherheitsverletzung mit mehreren Hunderttausend verlorenen Datensätzen kann bereits eine erhebliche Auswirkung auf das Geschäft haben.

Bei einem Angriff auf Ihr Unternehmen können unter anderem folgende Kosten entstehen:

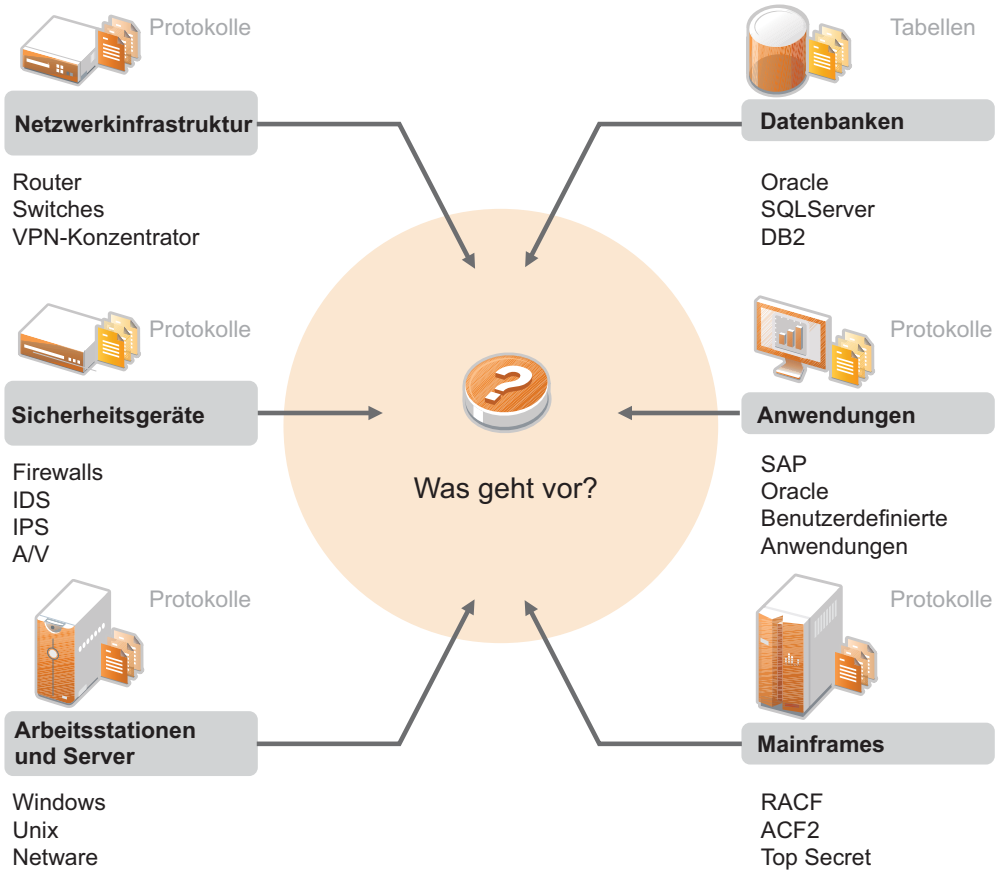
- Prozesskosten
- Ermittlungs- und Gerichtskosten
- Kosten für gesteigerte Audits
- Geld- und Vertragsstrafen
- Versteckte Kosten aus Verlust des Kundenvertrauens
- Verlorene Kunden durch Verlust des Kundenvertrauens

All diese Punkte zeigen, wie wichtig der Schutz Ihrer IT-Umgebung ist. Durch das Internet und den wachsenden Anklang der Cloud-Technologie beginnt die Grenze zwischen Insidern und Außenstehenden zu verschwimmen.

1.2 Herausforderungen bei die Absicherung der IT-Umgebung

Aufgrund der Komplexität Ihrer IT-Umgebung ist deren Absicherung eine Herausforderung. Zahlreiche Anwendungen, Datenbanken, Mainframes, Arbeitsstationen und Server zeichnen Protokolle der in Ihrer IT-Umgebung stattfindenden Ereignisse auf. Zusätzlich haben Sie Sicherheits- und Netzwerkinfrastrukturgeräte, die ebenfalls Protokoll über die Ereignisse in Ihrer IT-Umgebung führen.

Abbildung 1-1 *Was geschieht in Ihrer Umgebung?*



Die Herausforderungen sind unter anderem durch folgende Gegebenheiten bedingt:

- Ihre IT-Umgebung besteht aus sehr vielen Geräten
- Die Protokolle haben verschiedene Formate
- Die Protokolle werden in Silos gespeichert
- In den Protokollen wird eine große Menge an Informationen generiert
- Ohne manuelle Analyse der Protokolle können Sie nicht feststellen, wer was getan hat

Einen wirklichen Nutzen aus diesen Informationen ziehen Sie nur, wenn Sie folgende Aufgaben ausführen können:

- Daten erfassen
- Daten konsolidieren
- Ungleichartige Daten als Ereignisse standardisieren, die einfach verglichen werden können
- Ereignisse Standardvorschriften zuordnen
- Daten analysieren
- Ereignisse aus mehreren Systemen vergleichen, um festzustellen, ob ein bestimmtes Muster auf ein Sicherheitsproblem hinweist
- Benachrichtigungen senden, sobald Daten außerhalb der Norm liegen

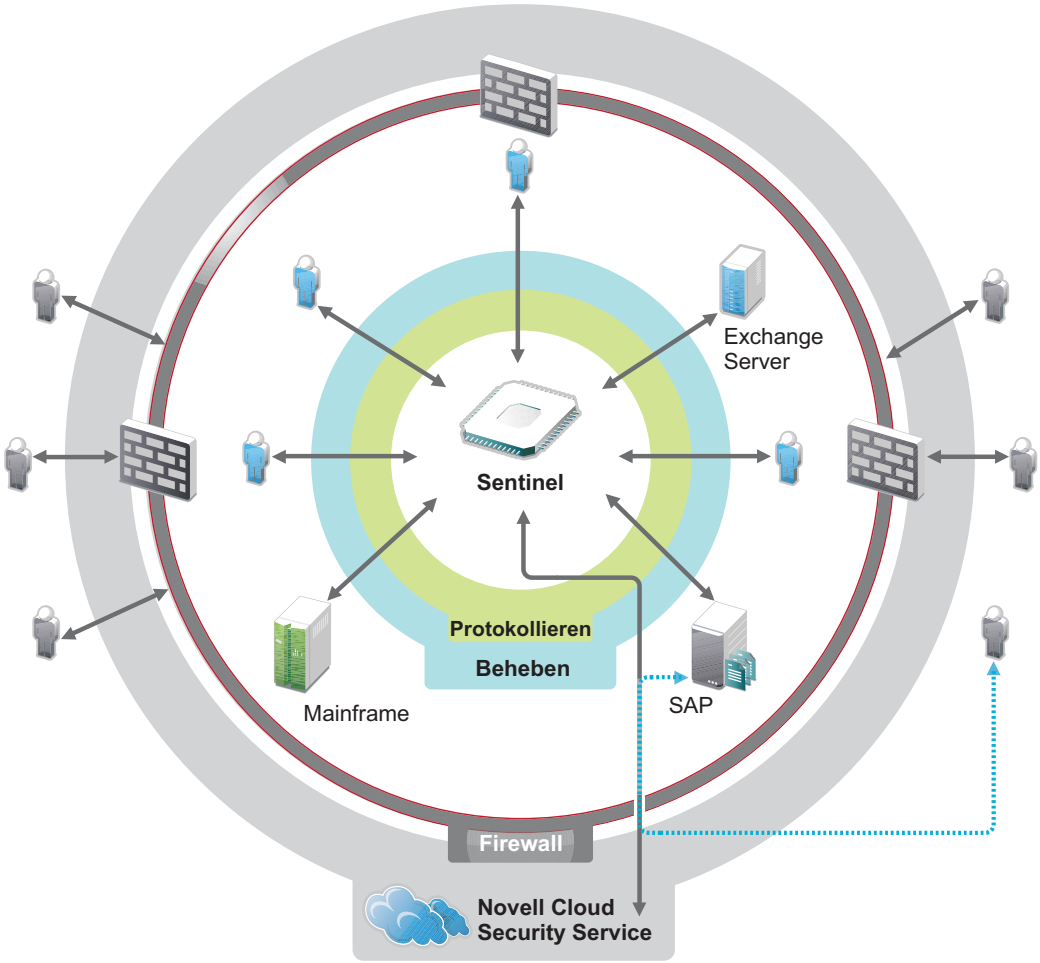
- Bei Benachrichtigungen entsprechende, mit den Geschäftsrichtlinien konforme Aktionen veranlassen
- Berichte zum Nachweis der Compliance generieren

Sie kennen nun die Herausforderungen, vor die Sie die Absicherung Ihrer IT-Umgebung stellt. Nun müssen Sie herausfinden, wie Sie Ihr Unternehmen für die Benutzer und vor den Benutzern schützen, ohne diese wie Kriminelle zu behandeln oder sie bis zu einem Punkt zu belasten, an dem Produktivität unmöglich wird. Sentinel stellt die Lösung bereit.

1.3 Die Lösung von Sentinel

Sentinel ist das zentrale Nervensystem der Unternehmenssicherheit. Es erfasst Daten aus Ihrer gesamten Infrastruktur – von Anwendungen, Datenbanken, Servern, Speichereinheiten und Sicherheitsgeräten. Es analysiert und korreliert die Daten und macht sie umsetzbar – entweder automatisch oder manuell.

Abbildung 1-2 *Die Lösung von Sentinel*



Sie wissen daher immer über wichtige Ereignisse in Ihrer IT-Umgebung Bescheid und können an Ressourcen vorgenommene Aktionen mit den Personen in Verbindung bringen, die diese Aktionen ausgeführt haben. Auf diese Weise lernen Sie das Verhalten der Benutzer kennen und können

erforderliche Kontrollen einführen. Unabhängig davon, ob die Personen Mitarbeiter des Unternehmens oder Außenstehende sind, können Sie deren Aktionen zusammenführen, sodass wirklich riskante Aktivitäten ersichtlich werden, bevor sie Schaden anrichten.

Dies ermöglicht Sentinel kostengünstig auf folgende Weise:

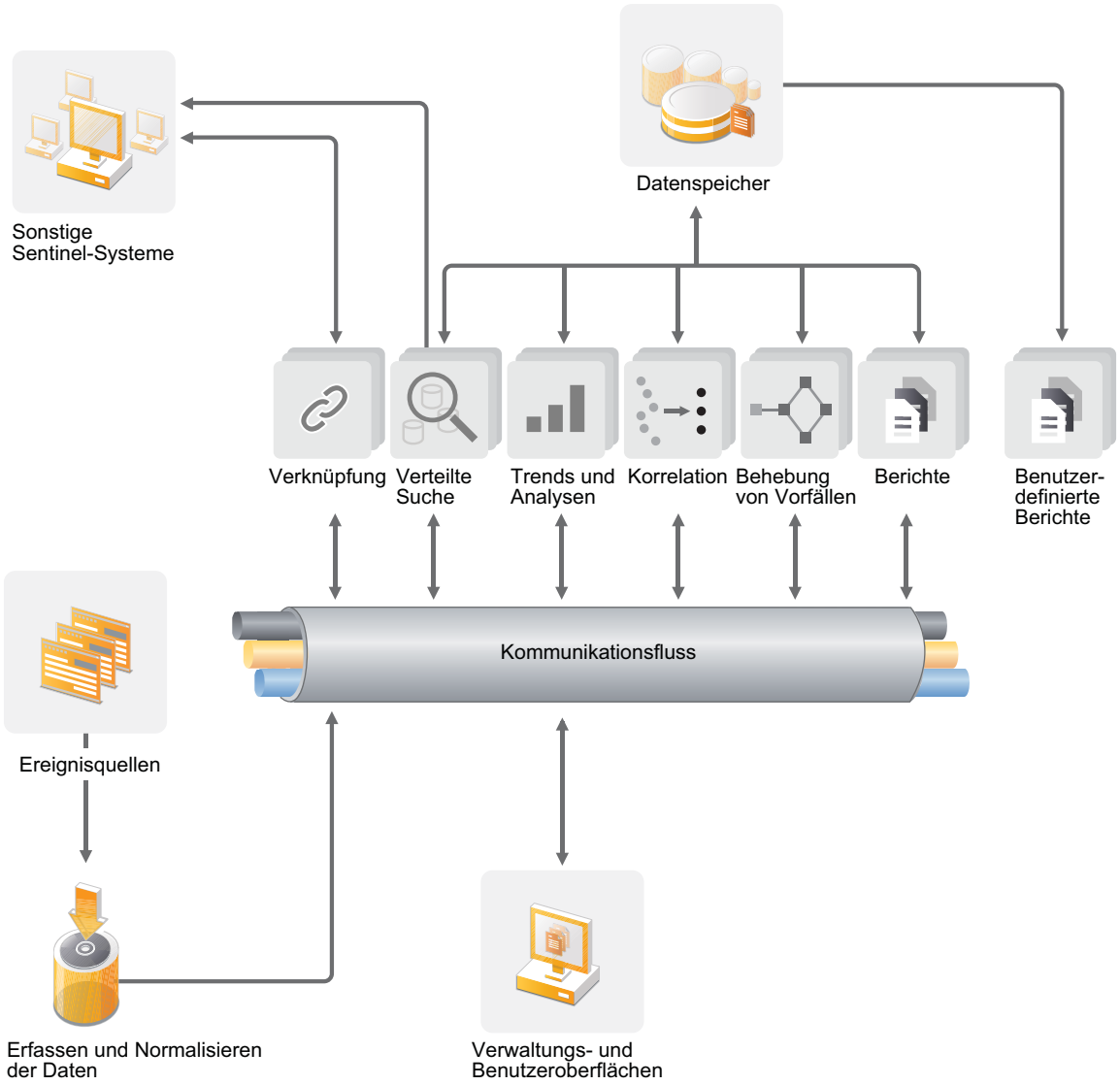
- Bereitstellen einer umfassenden Lösung für IT-Kontrollen zu mehreren Vorschriften gleichzeitig
- Keine Diskrepanzen zwischen dem, was eigentlich passieren sollte, und dem, was tatsächlich in Ihrer vernetzten Umgebung passiert
- Bereitstellen von Nachweisen für Auditoren und Prüfer, die belegen, dass Ihr Unternehmen Sicherheitskontrollen dokumentiert und überwacht sowie entsprechende Berichte erstellt
- Bereitstellen eines einsatzbereiten Programms für die Compliance-Überwachung und Berichterstellung
- Bereitstellen der Transparenz und Kontrolle, die Sie benötigen, um fortlaufend die Ergebnisse von Compliance- und Sicherheitsinitiativen Ihres Unternehmen zu bewerten

Sentinel automatisiert die Erfassung und Analyse von Protokolldaten sowie die anschließende Berichterstellung und gewährleistet so, dass die Bedrohungserkennung und die Audit-Anforderungen durch die implementierten IT-Kontrollen effektiv unterstützt werden. Sentinel bietet eine automatische Überwachung von Sicherheitsereignissen und Compliance-Ereignissen sowie IT-Steuerelemente, damit Sie im Fall einer Sicherheitsverletzung oder eines regelwidrigen Ereignisses sofort Maßnahmen ergreifen können. Mit Sentinel können Sie außerdem auf einfache Weise zusammenfassende Informationen über die Umgebung sammeln, damit sie wichtigen Stakeholdern den allgemeinen Sicherheitsstand bekanntmachen können.

2 Funktionsweise von Sentinel

Sentinel verwaltet kontinuierlich die Sicherheit betreffende Informationen und Ereignisse in Ihrer IT-Umgebung und bietet so eine vollständige Überwachungslösung. In der folgende Abbildung wird dargestellt, wie Sentinel funktioniert.

Abbildung 2-1 *Funktionsweise von Sentinel*



Sentinel führt folgende Aufgaben aus:

- Erfassen von Protokoll-, Ereignis- und Sicherheitsinformationen aus allen Ereignisquellen Ihrer IT-Umgebung
- Konvertieren der erfassten Protokoll-, Ereignis- und Sicherheitsinformationen in ein Standardformat
- Hinzufügen der standardisierten Informationen zu einem Nachrichtenbus, der Tausende Nachrichtenpakete pro Sekunde übermitteln kann
- Kommunizieren mit allen Sentinel-Komponenten über den Nachrichtenbus (optimale Skalierbarkeit)

An diesem Punkt greifen die verschiedenen Sentinel-Komponenten auf den Nachrichtenbus zu. Sentinel übernimmt dabei folgende Aufgaben bzw. bietet folgende Möglichkeiten:

- Speichern der Ereignisse in einem dateibasierten Datenspeicher mit flexiblen, benutzerdefinierbaren Datenbeibehaltungsrichtlinien
- Hierarchische Verknüpfung mehrerer Sentinel-Systeme wie Sentinel Log Manager, Sentinel und Sentinel Rapid Deployment
- Suche nach Ereignissen nicht nur auf dem lokalen, sondern auch auf weltweit verteilten Sentinel-Servern
- Durchführen statistischer Analysen zur Definition einer Baseline und Vergleich mit den aktuell einlaufenden Informationen, um verdeckte Probleme zu erkennen
- Korrelieren einer Gruppe ähnlicher oder vergleichbarer Ereignisse, die innerhalb eines bestimmten Zeitraums stattgefunden haben, um ein Muster zu erkennen
- Einteilen von Ereignissen in Vorfälle, wodurch sich Response Management und Nachverfolgung effizienter gestalten
- Berichterstellung auf Basis aktueller und alter Ereignisse

In den folgenden Abschnitten werden die Komponenten von Sentinel beschrieben.

- Abschnitt 2.1, „Ereignisquellen“, auf Seite 13
- Abschnitt 2.2, „Sentinel-Ereignis“, auf Seite 14
- Abschnitt 2.3, „Connectors“, auf Seite 16
- Abschnitt 2.4, „Collectors“, auf Seite 16
- Abschnitt 2.5, „Collector-Manager“, auf Seite 17
- Abschnitt 2.6, „Kommunikationsbus“, auf Seite 17
- Abschnitt 2.7, „Sentinel-Datenspeicher“, auf Seite 19
- Abschnitt 2.8, „Filter“, auf Seite 19
- Abschnitt 2.9, „Korrelation“, auf Seite 20
- Abschnitt 2.10, „Sicherheitsintelligenz“, auf Seite 20
- Abschnitt 2.11, „iTrac“, auf Seite 20
- Abschnitt 2.12, „Berichte“, auf Seite 21
- Abschnitt 2.13, „Ereignisanalyse“, auf Seite 21

2.1 Ereignisquellen

Sentinel erfasst Sicherheitsinformationen und Ereignisse aus zahlreichen unterschiedlichen Quellen Ihrer IT-Umgebung. Diese Quellen werden als Ereignisquellen bezeichnet. Bei diesen Ereignisquellen kann es sich um zahlreiche verschiedene Komponenten in Ihrem Netzwerk handeln.

Die nachfolgende Abbildung zeigt einige Ereignisquellen, von denen Sentinel Informationen abrufen kann.

Sicherheitsbereich: Geräte und Software, die den Sicherheitsbereich Ihrer Umgebung bilden.

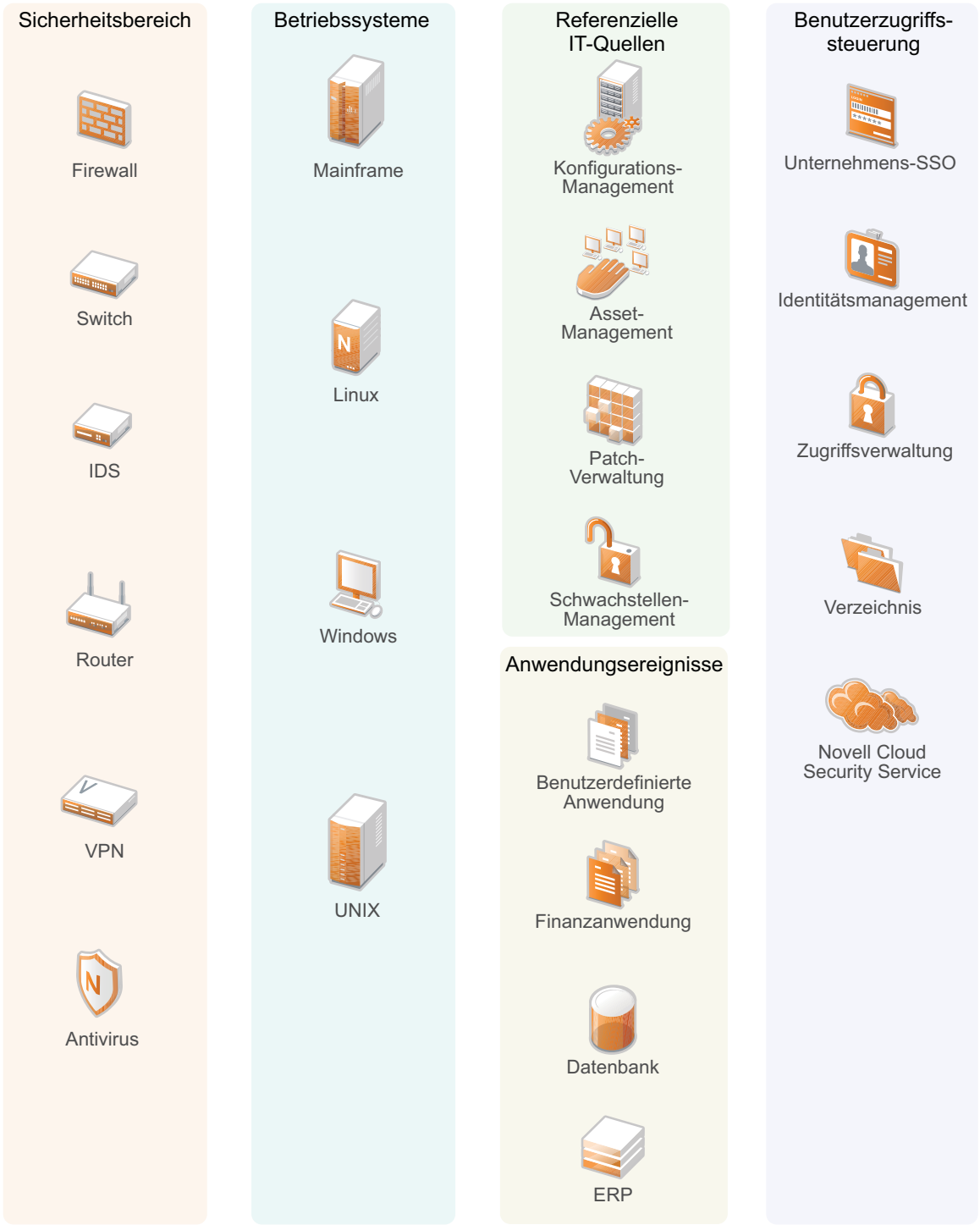
Betriebssysteme: Ereignisse aus den verschiedenen Betriebssystemen, die im Netzwerk ausgeführt werden.

IT-Referenzquellen: Software für die Verwaltung und Nachverfolgung von Inventar, Patches, Konfigurationen und Anfälligkeiten.

Anwendungsereignisse: Ereignisse, die von den im Netzwerk installierten Anwendungen generiert werden.

Benutzerzugriffssteuerung: Ereignisse, die von Anwendungen oder Geräten generiert werden, über die Benutzer Zugriff auf Unternehmensressourcen erhalten.

Abbildung 2-2 *Ereignisquellen*



2.2 Sentinel-Ereignis

Sentinel empfängt Informationen von Geräten, standardisiert diese Informationen in einer als Ereignis bezeichneten Struktur, klassifiziert das Ereignis und sendet es zur Verarbeitung. Durch Hinzufügen von Kategorieinformationen (Taxonomie) zu den Ereignissen können die Ereignisse

leichter über verschiedene Systeme hinweg verglichen werden, die Ereignisse auf unterschiedliche Weise berichten. Ein Beispiel hierfür sind Authentifizierungsfehler. Ereignisse werden in der Echtzeitanzeige, von der Correlation Engine, von Dashboards sowie vom Back-End-Server verarbeitet.

Ein Ereignis umfasst über 200 Felder. Ereignisfelder weisen unterschiedliche Typen auf und dienen unterschiedlichen Zwecken. Es gibt einige vordefinierte Felder, beispielsweise zur Angabe des Schweregrads (severity), der Gefährlichkeit (criticality), der Ziel-IP (destination IP) und des Ziel-Ports (destination port). Konfigurierbare Felder teilen sich in zwei Gruppen ein: Reservierte Felder sind für die interne Verwendung durch Sentinel vorgesehen (für künftige Erweiterungen), Kundenfelder sind für vom Kunden entwickelte Erweiterungen bestimmt.

Felder können durch Umbenennung einen neuen Zweck erfüllen. Die Quelle eines Felds kann entweder extern (die Festlegung erfolgt also explizit durch das Gerät oder den entsprechenden Collector) oder referenziell sein. Der Wert eines referenziellen Felds wird unter Verwendung des Zuordnungsservice als Funktion eines oder mehrerer weiterer Felder berechnet. Ein Feld kann beispielsweise der Gebäudecode des Gebäudes sein, in dem sich das Inventar befindet (die Angabe erfolgt als Ziel-IP eines Ereignisses). Ein Feld kann beispielsweise vom Zuordnungsservice als kundendefinierte Zuordnung berechnet werden (unter Verwendung der Ziel-IP aus dem Ereignis).

- Abschnitt 2.2.1, „Zuordnungsservice“, auf Seite 15
- Abschnitt 2.2.2, „Streaming von Zuordnungen“, auf Seite 16
- Abschnitt 2.2.3, „Exploit-Erkennung (Zuordnungsservice)“, auf Seite 16

2.2.1 Zuordnungsservice

Der Zuordnungsservice stellt einen fortschrittlichen Mechanismus zur Weiterleitung relevanter Geschäftsdaten im gesamten System bereit. Diese Daten können Ereignisse um referenzielle Informationen erweitern, die Kontextinformationen zur Verfügung stellen, die Analysten bei der Entscheidungsbildung und beim Erstellen nützlicher Berichte und gut durchdachter Korrelationsregeln unterstützen.

Sie können die Ereignisdaten bereichern, indem Sie über Zuordnungen zusätzliche Informationen wie Host und Identitätsdetails zu den von den Ursprungsgeräten eingehenden Ereignissen hinzufügen. Diese zusätzlichen Informationen können für erweiterte Korrelationen und zur Berichterstellung genutzt werden. Das System unterstützt neben mehreren integrierten Zuordnungen auch benutzerdefinierte Zuordnungen.

In Sentinel definierte Zuordnungen werden auf zwei verschiedene Weisen gespeichert:

- Integrierte Zuordnungen werden in der Datenbank gespeichert, über APIs im Collector-Code aktualisiert und automatisch zum Zuordnungsservice exportiert.
- Benutzerdefinierte Zuordnungen werden als CSV-Dateien gespeichert und können im Dateisystem oder über die Benutzeroberfläche für die Zuordnungsdatenkonfiguration aktualisiert werden. Anschließend werden Sie vom Zuordnungsservice geladen.

In beiden Fällen werden die CSV-Dateien auf dem zentralen Sentinel-Server bewahrt. Änderungen an den Zuordnungen werden jedoch an die einzelnen Collector-Managers verteilt und lokal angewendet. Diese verteilte Verarbeitung gewährleistet, dass die Zuordnungsaktivität den Hauptserver nicht überlastet.

2.2.2 Streaming von Zuordnungen

Der Zuordnungsservice setzt ein Modell zur dynamischen Aktualisierung ein, wobei die Zuordnungen per Streaming von einem Punkt an den nächsten übertragen werden. Auf diese Weise wird verhindert, dass sich große Datenmengen an statischen Zuordnungen im dynamischen Speicher ansammeln. Der Wert dieser Streaming-Funktion erweist sich insbesondere in einem für das Unternehmen essenziellen Echtzeitsystem wie Sentinel, in dem Datenbewegungen unabhängig von einer möglichen temporären Systemauslastung zuverlässig, prädiktiv und flexibel erfolgen müssen.

2.2.3 Exploit-Erkennung (Zuordnungsservice)

In Sentinel können Querverweise zwischen den Signaturen von Ereignisdaten und den Daten von Anfälligkeitsabsuchen erstellt werden. Benutzer werden automatisch und umgehend benachrichtigt, wenn ein anfälliges System durch einen Angriff ausgenutzt zu werden droht. Hier kommt Folgendes zum Einsatz:

- Advisor-Feed
- Intrusion Detection
- Anfälligkeitsabsuchen
- Firewalls

Advisor stellt Querverweise zwischen den Signaturen von Ereignisdaten und den Daten von Anfälligkeitsabsuchen her. Advisor-Feed enthält Informationen zu Schwachstellen und Bedrohungen sowie eine Standardisierung von Ereignissignaturen und Schwachstellen-Plugins. Weitere Informationen zu Advisor finden Sie im Abschnitt "Configuring Advisor" (Advisor konfigurieren) im *NetIQ Sentinel 7.0.1 Administration Guide* (NetIQ Sentinel 7.0-Administrationshandbuch).

2.3 Connectors

Connectors stellen die Verbindungen zwischen den Ereignisquellen und dem Sentinel-System her. Connectors verwenden branchenübliche Protokolle zum Erfassen von Ereignissen, wie Syslog, JDBC zum Lesen von Datenbanktabellen, WMI zum Lesen aus Windows-Ereignisprotokollen usw. und stellen so Folgendes zur Verfügung:

- Transport der Ereignisrohdaten von den Ereignisquellen zum Collector
- Verbindungsspezifische Filter
- Fehlerbehandlung im Rahmen der Verbindungen

2.4 Collectors

Collectors standardisieren und erfassen die Informationen von den Connectors. Collectors werden in JavaScript erstellt und definieren die Logik für Folgendes:

- Empfangen der Rohdaten von den Connectors
- Analysieren und Standardisieren der Daten
- Anwenden wiederholbarer Logik auf die Daten
- Konvertieren gerätespezifischer Daten in Sentinel-spezifische Daten

- Formatieren der Ereignisse
- Weiterleiten der standardisierten, analysierten und formatierten Daten an den Collector-Manager

2.5 Collector-Manager

Der Collector-Manager verwaltet die Datenerfassung, überwacht Meldungen zum Systemstatus und führt bei Bedarf eine Ereignisfilterung durch. Zu den Hauptaufgaben des Collector-Manager zählen die folgenden Funktionen:

- Umwandeln von Ereignissen
- Hinzufügen einer Geschäftsrelevanz zu Ereignissen durch den Zuordnungsservice
- Globale Filterung der Ereignisse
- Weiterleiten der Ereignisse
- Ermitteln von Echtzeit- und Nicht-Echtzeit-Daten sowie von Anfälligkeits- und Inventardaten
- Senden von Statusmeldungen an den Sentinel-Server

2.6 Kommunikationsbus

Die Kommunikationsbus-Architektur setzt auf einer standardbasierten, serviceorientierten Architektur (Service Oriented Architecture, SOA) auf, die die Vorteile der speicherinternen Verarbeitung und des verteilten Computing vereint. Bei dem verwendeten iSCALE-Kommunikationsbus handelt es sich um einen spezialisierten Nachrichtenbus, der große Datenmengen verarbeiten kann.

- Abschnitt 2.6.1, „Nachrichtenbus“, auf Seite 17
- Abschnitt 2.6.2, „Kanäle“, auf Seite 18

2.6.1 Nachrichtenbus

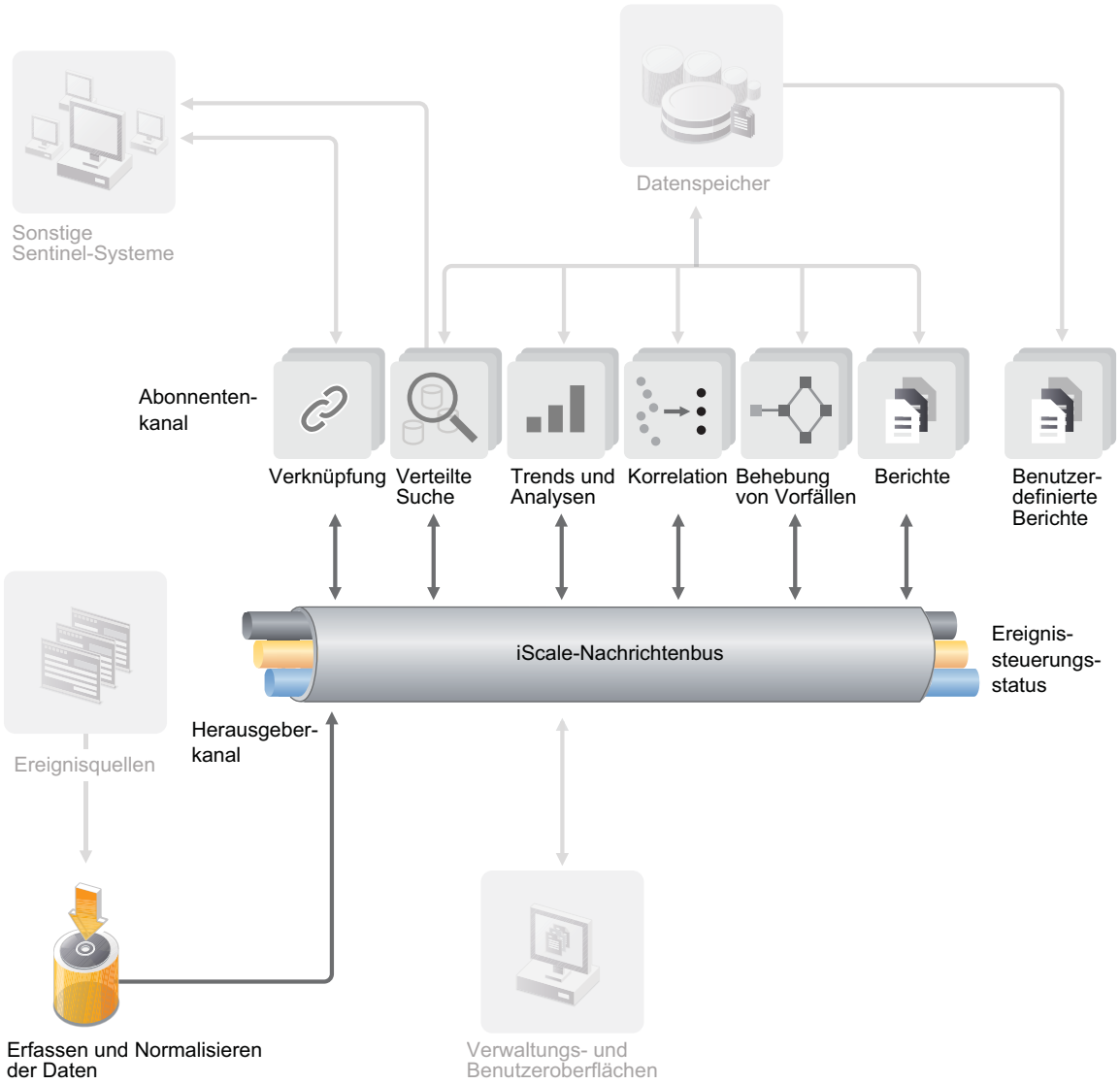
Der iSCALE-Nachrichtenbus ermöglicht die unabhängige Skalierung einzelner Komponenten sowie die standardbasierte Integration in externe Anwendungen. Der Schlüssel zur Skalierbarkeit liegt darin, dass – im Gegensatz zu anderer verteilter Software – keine zwei Peer-Komponenten direkt miteinander kommunizieren. Sämtliche Komponenten kommunizieren über den Nachrichtenbus, der Tausende Nachrichtenpakete pro Sekunde übermitteln kann.

Durch optimale Nutzung der einzigartigen Funktionen des Nachrichtenbusses kann der High-Throughput-Kommunikationskanal eine hohe Datendurchsatzrate über unabhängige Komponenten des Systems hinweg erzielen und aufrechterhalten. Ereignisse werden beim Transport komprimiert und verschlüsselt, um die sichere und effiziente Zustellung vom Rand des Netzwerks bzw. von Sammelpunkten zum Hub des Systems zu gewährleisten, wo Echtzeitanalysen vorgenommen werden.

Beim iSCALE-Nachrichtenbus kommen eine Reihe von Warteschlangenservices zum Einsatz, die die Zuverlässigkeit der Kommunikation über die Sicherheits- und Leistungsaspekte der Plattform hinaus erhöhen. Durch eine Vielzahl temporärer und permanenter Warteschlangen bietet das System unübertroffene Zuverlässigkeit und Fehlertoleranz. So werden beispielsweise wichtige Meldungen/

Nachrichten, die sich im Transit befinden, für den Fall gespeichert (in eine Warteschlange gestellt), dass es zu einem Ausfall im Kommunikationspfad kommt. Die in die Warteschlange gestellten Nachrichten gelangen an ihr Ziel, nachdem das System nach dem Ausfall wiederhergestellt wurde.

Abbildung 2-3 *iSCALE-Nachrichtenbus*



2.6.2 Kanäle

Die iSCALE-Plattform umfasst ein datengesteuertes und ein ereignisgesteuertes Modell, das abhängig von der Arbeitsauslastung die unabhängige Skalierung von Komponenten für das gesamte System ermöglicht. Hieraus ergibt sich ein flexibles Bereitstellungsmodell für die unterschiedlichen Systemumgebungen beim Kunden: An einem Standort sind möglicherweise zahlreiche Geräte mit geringem Ereignisvolumen vorhanden, an einem anderen weniger Geräte mit ausgesprochen hohem

Ereignisvolumen. Die Ereignisdichte, also die Ereignisaggregation und das Ereignis-Multiplexing-Muster beim Transport von den Sammelpunkten, ist in diesen Fällen unterschiedlich, wobei der Nachrichtenbus die konsistente Skalierung bei ungleich ausfallender Arbeitsauslastung ermöglicht.

iSCALE nutzt die Vorteile einer unabhängigen Umgebung mit mehreren Kanälen. Auf diese Weise werden Konflikte nahezu ausgeschlossen und die Parallelverarbeitung von Ereignissen wird gefördert. Diese Kanäle und Teilkanäle können nicht nur für den Ereignisdatentransport verwendet werden, sie ermöglichen auch die präzise Vorgangssteuerung für Skalierung und Lastenausgleich bei unterschiedlichen Auslastungen. Durch unabhängige Servicekanäle, beispielsweise Steuerkanäle und Statuskanäle, die neben dem Hauptereigniskanal zum Einsatz kommen, kann die ereignisgesteuerte Architektur auf hohem Niveau und kosteneffizient skaliert werden.

2.7 Sentinel-Datenspeicher

Zum Speichern der erfassten Daten bietet Sentinel verschiedene Optionen. Standardmäßig erhält Sentinel von den Collector-Managern zwei getrennte, aber ähnliche Datenströme: die Ereignisdaten und die Rohdaten. Diese Daten werden im lokalen Dateisystem auf dem Sentinel-Server gespeichert.

Sentinel kann aber auch so konfiguriert werden, dass die Daten in einem Netzwerkspeicher gespeichert werden. Außerdem können Sie Sentinel mithilfe von Datensynchronisierungsrichtlinien so konfigurieren, dass die Ereignisdaten in einer externen Datenbank gespeichert werden. Weitere Informationen finden Sie unter "Configuring Data Storage (Konfigurieren der Datenspeicherung)" im *NetIQ Sentinel 7.0.1 Administration Guide (NetIQ Sentinel 7.0.1-Administrationshandbuch)*.

2.8 Filter

Filter haben in Sentinel die Aufgabe, die Ereignissuche anzupassen und zu verhindern, dass zu viele Daten zurückgegeben werden. Diese Funktion enthält einen Filtereditor, mit dem Sie einfache wie komplexe Suchabfragen erstellen können. Suchabfragen können Sie als Filter speichern und nach Bedarf wiederverwenden. Sie können die gleiche Suche also durch Auswahl eines Filters durchführen, statt die Abfrage jedes Mal erneut einzugeben.

Filter können bei der Verwendung oder Konfiguration von Sentinel-Funktionen wie den Folgenden eingesetzt werden:

- Erstellen von Sicherheitsintelligenz-Dashboards

  Weitere Informationen finden Sie im Abschnitt "Creating a Dashboard" (Erstellen eines Dashboards) im *NetIQ Sentinel 7.0.1 User Guide* (NetIQ Sentinel 7.0.1-Benutzerhandbuch).

- Anzeigen von Echtzeitereignissen in Active Views

  Weitere Informationen finden Sie im Abschnitt "Viewing Events" (Ereignisse anzeigen) im *NetIQ Sentinel 7.0.1 User Guide* (NetIQ Sentinel 7.0.1-Benutzerhandbuch).

- Konfigurieren einer Datenaufbewahrungsrichtlinie

  Weitere Informationen finden Sie im Abschnitt "Configuring Data Retention Policies" (Datenaufbewahrungsrichtlinien konfigurieren) im *NetIQ Sentinel 7.0.1 Administration Guide* (NetIQ Sentinel 7.0.1-Administrationshandbuch).

- Konfigurieren der Datensynchronisierung

  Weitere Informationen finden Sie unter "Configuring Data Synchronization (Konfigurieren der Datensynchronisierung)" im *NetIQ Sentinel 7.0.1 Administration Guide (NetIQ Sentinel 7.0.1-Administrationshandbuch)*.

- Testen einer Korrelationsregel

  Weitere Informationen finden Sie unter "Correlating Event Data (Korrelation von Ereignisdaten) " im *NetIQ Sentinel 7.0.1 User Guide (NetIQ Sentinel 7.0.1-Benutzerhandbuch)*.

Sentinel stellt eine vordefinierte Liste mit Filtern bereit. Darüber hinaus können Sie auch eigene Filter erstellen. Weitere Informationen finden Sie unter "Configuring Filters (Konfigurieren von Filtern)" im *NetIQ Sentinel 7.0.1 User Guide (NetIQ Sentinel 7.0.1-Benutzerhandbuch)*.

2.9 Korrelation

Ein einzelnes Ereignis mag unbedeutend erscheinen. In Verbindung mit anderen Ereignissen kann es jedoch vor potenziellen Problemen warnen. Sentinel unterstützt Sie bei der Ereigniskorrelation, indem es die Regeln anwendet, die Sie in der Correlation Engine erstellen und bereitstellen, und geeignete Maßnahmen zum Abschwächen des Problems ergreift.

Die Korrelation bietet zusätzliche Intelligenz bei der Verwaltung von Sicherheitsereignissen, indem sie die Analyse des eingehenden Ereignisstroms automatisiert und auf diese Weise sicherheitsrelevante Muster erkennt. Durch Korrelation lassen sich Regeln definieren, durch die kritische Bedrohungen und komplexe Angriffsmuster identifiziert werden. Dies ermöglicht die vorrangige Behandlung bestimmter Ereignisse, wodurch die Vorfallsverwaltung und -behandlung an Effizienz gewinnt. Weitere Informationen finden Sie unter "Correlating Event Data (Korrelation von Ereignisdaten) " im *NetIQ Sentinel 7.0.1 User Guide (NetIQ Sentinel 7.0.1-Benutzerhandbuch)*.

2.10 Sicherheitsintelligenz

Die Korrelationsfunktion in Sentinel bietet die Möglichkeit, nach bekannten Aktivitätsmustern zu suchen, ob für Sicherheits-, Compliance- oder andere Gründe. Die Sicherheitsintelligenzfunktion sucht nach Aktivitäten, die ungewöhnlich und möglicherweise schädlich sind, aber mit keinem bekannten Muster übereinstimmen.

Die Sentinel-Funktion der Sicherheitsintelligenz setzt in erster Linie auf die statistische Analyse von Zeitreihendaten. Die Funktion ermöglicht Analysten die Erkennung und Analyse von Abweichungen (Anomalien) mithilfe einer automatisierten Statistik-Engine bzw. durch manuelle Interpretation grafischer Statistiken. Weitere Informationen finden Sie im Abschnitt "Analyzing Trends in Data" (Datentrends analysieren) im *NetIQ Sentinel 7.0.1 User Guide* (NetIQ Sentinel 7.0.1-Benutzerhandbuch).

2.11 iTrac

iTRAC-Workflows bieten eine einfache, flexible Lösung für die Automatisierung und Nachverfolgung der Vorfallsbehandlungsprozesse in einem Unternehmen. iTRAC nutzt das interne Vorfallsystem von Sentinel zur Verfolgung von Sicherheits- und Systemproblemen von deren Identifizierung (mithilfe von Korrelationsregeln oder durch manuelle Erkennung) bis hin zu deren Behebung.

Workflows können aus manuellen und automatischen Schritten bestehen. Auch erweiterte Funktionen wie Verzweigungen, zeitgesteuerte Eskalation und lokale Variablen werden unterstützt. Die Möglichkeit der Integration externer Skripts und Plugins bietet Raum für die flexible Interaktion mit Systemen von Drittanbietern. Dank umfassender Berichtsfunktionen können Administratoren

den Vorfallsbehandlungsprozess besser verstehen und anpassen. Weitere Informationen finden Sie im Abschnitt "Configuring iTRAC Workflows" (iTRAC-Workflows konfigurieren) im *NetIQ Sentinel 7.0.1 User Guide* (NetIQ Sentinel 7.0.1-Benutzerhandbuch).

2.12 Berichte

Zu den in Sentinel erfassten Daten können Berichte erstellt werden. Sentinel stellt die verschiedensten Arten von benutzerdefinierbaren Berichten bereit, von denen einige eher allgemein, andere hingegen für bestimmte Geräte vorgesehen sind (z. B. SUSE Linux). In einigen Berichten können die im Ergebnis angezeigten Spalten vom Benutzer ausgewählt werden.

Die Benutzer können PDF-Berichte ausführen, planen und per E-Mail versenden. Sie können jeden Bericht als Suche ausführen und das Ergebnis wie bei jeder Suche beeinflussen, indem sie die Suche präzisieren oder bestimmte Aktionen am Ergebnis ausführen. Die Berichte können auch auf geografisch verteilten Sentinel-Servern ausgeführt werden. Weitere Informationen finden Sie unter "Reporting (Berichterstellung)" im *NetIQ Sentinel 7.0.1 User Guide (NetIQ Sentinel 7.0.1-Benutzerhandbuch)*.

2.13 Ereignisanalyse

Sentinel stellt leistungsfähige Tools zur Verfügung, um Sie beim Erkennen und Analysieren kritischer Ereignisdaten zu unterstützen. Das System ist auf höchste Effizienz für beliebige Analysetypen abgestimmt und optimiert und stellt Methoden zur Verfügung, die den nahtlosen Übergang von einer Analyseart zur anderen ermöglichen.

Das Untersuchen von Ereignissen in Sentinel beginnt meist mit den Active Views, die Daten in nahezu Echtzeit darstellen. Ergänzend zu ausgefeilteren Tools zeigen Active Views gefilterte Ereignisströme mit zusammenfassenden Diagrammen an, die zur einfachen, groben Analyse von Ereignistrends und Ereignisdaten sowie zur Identifizierung bestimmter Ereignisse verwendet werden können. Mit der Zeit erstellen Sie abgestimmte Filter für bestimmte Datenklassen, zum Beispiel für die Ausgabe von Korrelationen. Sie können Active Views als Dashboard verwenden, das den allgemeinen Betriebs- und Sicherheitsstand darstellt.

Mit der interaktiven Suche können Sie die Ereignisse dann detaillierter analysieren. So können Sie schnell und einfach Daten in Bezug auf eine bestimmte Abfrage finden, zum Beispiel zur Aktivität eines bestimmten Benutzers oder auf einem bestimmten System. Durch Klicken auf die Ereignisdaten oder über den Verfeinerungsbereich auf der linken Seite können Sie schnell bestimmte Ereignisse herausgreifen.

Wenn Sie Hunderte von Ereignissen analysieren, bieten die Berichtfunktionen von Sentinel eine benutzerdefinierte Steuerung des Ereignislayouts und die Möglichkeit zur Anzeige größerer Datenmengen. Sentinel erleichtert diesen Übergang durch die Möglichkeit, interaktive Suchen aus der Suchoberfläche in eine Berichtvorlage zu übertragen. Hier wird sofort ein Bericht erstellt, der die gleichen Daten anzeigt, jedoch in einem Format, das für eine große Anzahl an Ereignissen besser geeignet ist.

Für diesen Zweck enthält Sentinel viele verschiedene Vorlagen. Einige Vorlagen sind auf die Anzeige bestimmter Informationstypen abgestimmt, beispielsweise Authentifizierungsdaten oder Daten zur Benutzererstellung, andere sind Allzweckvorlagen, in denen Sie Gruppen und Spalten im Bericht interaktiv anpassen können.

Mit der Zeit werden Sie häufig gebrauchte Filter und Berichte entwickeln, die Ihre Arbeitsabläufe erleichtern. Sentinel unterstützt das Speichern und Verteilen dieser Informationen an die Mitglieder in Ihrer Organisation. Weitere Informationen finden Sie im *NetIQ Sentinel 7.0.1 User Guide* (NetIQ Sentinel 7.0.1-Benutzerhandbuch).