RSA NetWitness® Orchestrator

Hauptmerkmale

- Integration in die RSA NetWitness Platform
- Von Threat Intelligence gesteuertes Incident-Management
- Relevanzbestimmung durch Kompromittierungsindikatoren (IOCs)
- Verbesserte Playbook-Steuerung für bessere Quality of Service
- Ausführung in Echtzeit
- Optimierte Zusammenarbeit von Teams und Tools
- Automatische Dokumentation
- Skalierbare und sichere multi-mandantenfähige Plattform
- Erweiterbares Integrationsframework
- Flexible Vor-Ort- und Cloud-Bereitstellung

Hauptvorteile

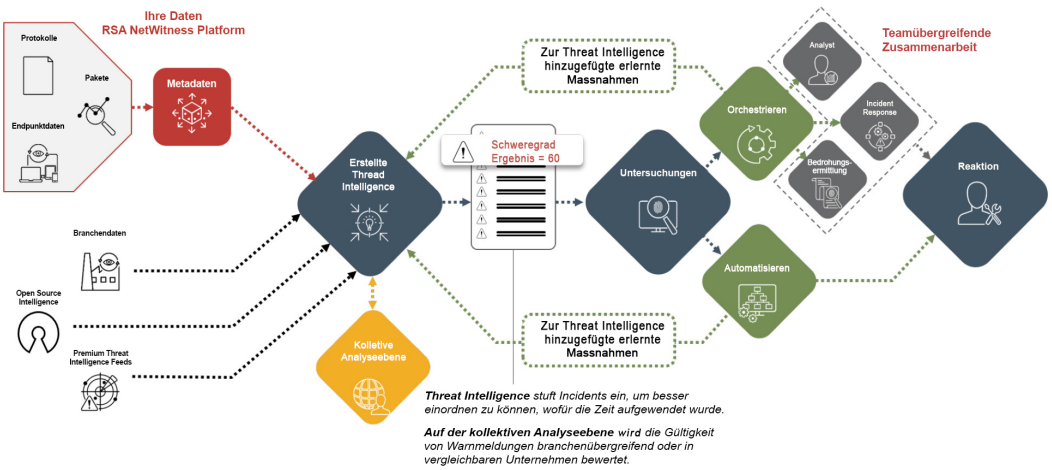
- Automatisierung: Unterstützung der Software zur Erledigung aufgabenorientierter „menschlicher Arbeit“ und Automatisierung der Bedrohungssuche
- Orchestrierung: Automatisierung oder Systematisierung der Entscheidungsfindung
- Dashboard und Reporting: Visualisierung der auf Threat Intelligence basierenden Metriken
- Incident-Management und Zusammenarbeit: Bereitstellung von End-to-End-Incident-Management
- Reaktionszeit: Schnellere Reaktionszeiten und weniger Fehler, höhere Produktivität der Analysten und Minimierung der durchschnittlichen Problembehebungszeit (Mean Time To Remediation, MTTR)

Fokus auf wichtigste Bedrohungen

In einer Ära ständig wachsender Angriffsflächen ist der Schutz vor Bedrohungsakteuren – von Commodity-Malware über Insiderbedrohungen und Crimeware bis hin zu staatlich tolerierten Angriffen, Hacktivisten und Terroristen – zu einer immer komplexeren und zeitaufwendigeren Aktivität geworden. Nicht alle Bedrohungen werden auf die gleiche Weise erstellt und nicht alle erfordern Ihre Aufmerksamkeit. Die getrennten Silos von Präventions-, Monitoring- und Ermittlungstechnologien verhindern die Erkennung falsch positiver Ergebnisse, die Eliminierung manueller wiederkehrender Aktionen sowie konzentrierte Reaktionen. Sicherheitsteams benötigen eine umfassende Lösung, mit denen Security Operations Center (SOC) Prozesse effektiv automatisieren und die wichtigsten Bedrohungen erkennen und auf diese reagieren können.

Bei RSA NetWitness® Orchestrator auf Basis von ThreatConnect™ handelt es sich um eine umfassende Sicherheits- und Automatisierungstechnologie, die vollständiges Fallmanagement, intelligente Automatisierung und Orchestrierung sowie kooperative Ermittlungen kombiniert. RSA NetWitness Orchestrator sorgt für Konsistenz und Effizienz bei der Bedrohungsermittlung, -suche und -reaktion. Durch die Nutzung von Playbooks und integrierter Threat Intelligence ergänzt das Tool nicht nur den Workflow, sondern automatisiert zudem den Workflow, die Zusammenarbeit und die Reaktion der Analysten. RSA NetWitness Orchestrator fungiert als Bindeglied für die RSA NetWitness Platform – und stellt das gesamte Sicherheitsarsenal für das Security Operations Team.

Threat Intelligence im Zentrum von Orchestrierung und Automatisierung



RSA NetWitness Orchestrator – Systemanforderungen

Physische Instanz

- Physische Serveranforderungen
  - — Anwendungsserver (keine Playbooks)
    - Arbeitsspeicher: 16 GB
    - CPU-Cores 8 (2 GHz)
    - Geschätzter Speicher: 50 GB
  - — Anwendungsserver (Playbooks)
    - Arbeitsspeicher: 48 GB
    - CPU-Cores 8 (2 GHz)
    - Geschätzter Speicher: 150 GB
  - — Datenbankserver (< 2 Millionen Indikatoren)
    - Arbeitsspeicher: 12 GB
    - CPU-Cores 6 (2 GHz)
    - Massenspeicher: 20 GB
  - — Datenbankserver (2-5 Millionen Indikatoren)
    - Arbeitsspeicher: 16 GB
    - CPU-Cores 8 (2 GHz)
    - Massenspeicher: 40 GB
  - — Datenbankserver (5-10 Millionen Indikatoren)
    - Arbeitsspeicher: 32 GB
    - CPU-Cores 12 (2 GHz)
    - Massenspeicher: 60 GB
  - — Elasticsearch®-Server (< 2 Millionen Indikatoren)
    - Arbeitsspeicher: 12 GB
    - CPU/vCPU-Cores: 6 (2 GHz)
    - Massenspeicher: 20 GB
  - — Elasticsearch-Server (2-5 Millionen Indikatoren)
    - Arbeitsspeicher: 16 GB
    - CPU/vCPU-Cores: 8 (2 GHz)
    - Massenspeicher: 40 GB
  - — Elasticsearch-Server (5-10 Millionen Indikatoren)
    - Arbeitsspeicher: 32 GB
    - CPU/vCPU-Cores: 12 (2 GHz)
    - Massenspeicher: 60 GB

Incident-Management neu definiert

RSA NetWitness Orchestrator ermöglicht es Security Operations Teams, isolierte Warnmeldungen aus dem Sicherheitsarsenal des Unternehmens zu erfassen und sie in kontextreiche, korrelierte Incidents mit kritischen Daten umzuwandeln. Auf Basis von Nutzerruf, System, IP, Netzwerk, zugehörigen Incidents, Wiederholungstätern und Threat Intelligence können Analysten schnell fundierte Entscheidungen treffen. Mit dem gut strukturierten, konsistenten und automatisch dokumentierten Incident-Management-Prozess, der Sicherheitswarnmeldungen über den gesamten Incident-Management-Lebenszyklus zusammenführt, korreliert und ergänzt, ist das die Basis für fundierte Entscheidungen im Bereich Security Operations.

Bekanntes automatisieren. Unbekanntes erkennen.

Sichtbarkeit ist der Schlüssel zur effektiven Bedrohungserkennung. RSA NetWitness Orchestrator bietet über 500 Apps und Integrationen für zahlreiche Sicherheitsmaßnahmen, darunter gemeinsame transparente Ermittlungen, mit denen sich die Incident-Behebungszeit verkürzen lässt. Mithilfe von umfassenden Daten über Protokolle, Netzwerke, Endpunkte, Sicherheits- und nicht sicherheitsbasierte Lösungen hinweg können Sicherheitsanalysten die unternehmensweite Bedrohungserkennung und -reaktion beschleunigen. Nutzen Sie ein umfangreiches vorkonfiguriertes Playbook oder passen Sie ein eigenes für die konsistente und präzise Incident-Reaktion an Mit RSA NetWitness Orchestrator können Sie die Behandlung von bekannten und risikoarmen Bedrohungen automatisieren und das Eindämmen und Beseitigen beschleunigen, damit Analysten Zeit haben, sich mit risikoreicheren Problemen zu befassen.

Auf Threat Intelligence basierte Orchestrierung und Automatisierung

Im Gegensatz zu Lösungen, die Intelligence nur zum Auslösen bestimmter Workflows verwenden, setzt RSA NetWitness Orchestrator Threat Intelligence bei allen Orchestrierungs- und Automatisierungsfunktionen für umfangreichen Kontext und Playbooks, die kontinuierlich angepasst werden, ein. Die Plattform nutzt zudem den vollen Wert aller Intelligence-Daten und unterstützt die teamübergreifende Koordination in Workflows.

Durch die Kombination von Threat Intelligence, Orchestrierung, Automatisierung und Reaktion bietet RSA NetWitness Orchestrator einen ganzheitlichen und systemweiten Einblick und ermöglicht Folgendes für Security Operations:

- **Warnmeldungen, Blockieren und Isolieren auf Basis von relevanter Threat Intelligence.** Relevante Threat Intelligence ist auch für Aufgaben auf niedrigerer Ebene, wie z. B. Warnmeldungen und Blockierungen wichtig. Sie können die Erkennung und Prävention automatisieren, aber Sie brauchen zuverlässige Threat Intelligence aus mehreren Quellen, um sicherzustellen, dass Sie Warnmeldungen für die richtigen Dinge erhalten und diese blockieren.
- **Mehr Genauigkeit, Zuverlässigkeit und Präzision.** Situationsbewusstsein und historischer Kontext sind für die Entscheidungsfindung elementar. Wenn Sie Threat Intelligence direkt nutzen, können Sie schneller arbeiten und mehr Angriffe vor ihrem Auftreten verhindern. Je mehr Sie im Vorfeld automatisieren, desto proaktiver können Sie sein. Durch die Eliminierung von falsch positiven Ergebnissen und die Nutzung von validierter Intelligence können Sie präzisere Aktionen durchführen, was wiederum die Geschwindigkeit und die Präzision verbessert.

RSA NetWitness Orchestrator – Systemanforderungen

- Betriebssystem: Red Hat® Linux-Variante – entweder Red Hat Enterprise Linux (RHEL) oder Community Operating System (CentOS) 6 oder 7
- Oracle® Java® Development Kit (JDK): Zugriff auf eine lokale Installation von Oracle Java 8 oder OpenJDK (JDK-Version 1.8)
- Java Cryptography Extension: Version 8
- Elasticsearch: Elasticsearch-Server 6.3.0
- Python®: Nur Installation von Python 3.6.x: Bezieht sich auf CPython
- Python-SDK: TCEX-Version 1.0+
- Redis: Installation von Redis 4.0.10
- Datenbank (wählen Sie eine der folgenden Optionen aus):
  - MySQL®: Installation von MySQL 5.7.x Community oder Enterprise Edition
  - SAP S/4HANA®: Installation von SAP S/4HANA 2.0 SPS 02
  - PostgreSQL: Installation von PostgreSQL v11

HINWEIS: Installieren Sie nur eines davon als aktive Datenbank.

- **Kenntnis von Kontext und dessen Verbesserung im Laufe der Zeit.** Sie können Aufgaben auf der Basis von Threat-Intelligence-Schwellenwerten (z. B. Indikator-Reputationsbewertungen) automatisieren und dann sämtliche Informationen festhalten. Außerdem können Sie Ihre Prozesse strategisch betrachten und Verbesserungsmöglichkeiten erkennen.
- **Orchestrierung mit Sicherheit.** Native, sinnvolle Analysen von externer Threat Intelligence ermöglichen genauere Warnmeldungen mit weniger falsch positiven Ergebnissen, Blockierungen und Quarantänen. Leider können Sie nicht einfach einige Threat Intelligence Feeds übernehmen oder aufgrund von gemeinsamen Kompromittierungsindikatoren (IOCs) handeln. Sie müssen die Daten für sich sinnvoll nutzen, anpassbare Bewertungen und Kontextualisierungen für Maßnahmen verwenden und wissen, ob Maßnahmen erforderlich sind.
- **Aufbau von organischer Intelligence aus Security Operations und Reaktionen.** Ihr Team und Ihre Daten sind die ultimativen Quellen für Intelligence. Sie wollen Einblicke, Artefakte und Beobachtungen aus Operations- und Reaktionsmaßnahmen erfassen und diese dann sofort in Intelligence umwandeln, und zwar in Form von neuen IOCs, gegnerischen Taktiken und Techniken sowie Kenntnis von Sicherheitslücken.
- **Automatische Anpassung von Prozessen bei Informations- und Kontextänderungen.** Sie sollten in der Lage sein, ihre Orchestrierungsfunktionen an sich ändernde Threat Intelligence anzupassen und interne Prozesse automatisch als Reaktion auf die Indikatorklassifizierung und die Bedrohungsbewertung zu justieren. Diese Prozesse und Workflows werden dynamisch aktualisiert, damit die Arbeit des Teams relevanter und effektiver wird.

Flexible und skalierbare Bereitstellung

RSA NetWitness Orchestrator wurde von Anfang an für die Bereitstellung-sunterstützung in Umgebungen mit einem oder mehreren Mandanten oder wirklichen Vor-Ort-Umgebungen entwickelt. Unabhängig von der Bereitstellungsart werden die Daten sicher getrennt, mit einfachen Optionen für vertikale und horizontale Skalierung. RSA unterstützt die Orchestrierung über mehrere Netzwerkumgebungen hinweg mit zentralem Management.

Typische Technologien für Sicherheitsorchestrierung und -automatisierung haben Probleme, das Workload-Volumen und den Umfang zu skalieren, die für eine maximierte SOC-Automatisierung und -Ergänzung benötigt werden. Daher haben Sicherheitsteams nicht viel Spielraum und können nur wenige Anwendungsfälle automatisieren, sodass viele manuelle Workflows übrig bleiben. RSA NetWitness Orchestrator bietet eine wahrhaft skalierbare Architektur, in der Orchestrierungs- und Automatisierungs-Workloads zusammen mit dem SOC wachsen können. Sicherheitsteams können die Ausführung priorisieren, Ressourcen für bestimmte Playbooks bereitstellen und zusätzliche Playbook-Server hinzufügen, wenn die Workload-Anforderungen steigen.

Die RSA NetWitness Platform

Mit mehr als 30 Jahren Erfahrung im Sicherheitsbereich ist RSA mit einer innovativen Lösung für die größten Herausforderungen bei Security Operations in den größten Unternehmen weltweit der Branchenführer. Das neue Produkt RSA NetWitness Orchestrator erweitert die RSA NetWitness Platform und die Angebote für fortschrittliches SIEM und Threat Defense und bietet so umfassende Sichtbarkeit über Protokolle, Netzwerke und Endpunkte hinweg.

Informationen über RSA

RSA bietet unternehmensgesteuerte Sicherheitslösungen, mit denen Unternehmen einen einheitlichen Ansatz für das Management digitaler Risiken nutzen können, der auf integrierter Sichtbarkeit, automatisierten Einblicken und koordinierten Aktionen basiert. RSA-Lösungen sollen Unternehmen die effektive Erkennung und Abwehr komplexer Angriffe, das Management der Nutzerzugriffskontrolle sowie die Verringerung von Geschäftsrisiken, Betrug und Cyberkriminalität ermöglichen. RSA schützt Millionen Nutzer auf der ganzen Welt und trägt dazu bei, dass mehr als 90 % der Fortune 500-Unternehmen Erfolg haben und sich kontinuierlich an Transformationsänderungen anpassen. Weitere Informationen finden Sie unter rsa.com/de-de.