# RSA NETWITNESS® ORCHESTRATOR

## FONCTIONNALITÉS PRINCIPALES

- Intégration avec RSA NetWitness Platform
- Gestion des incidents optimisée par l'intelligence sur les menaces
- Identification de la pertinence des indicateurs de compromission
- Contrôle amélioré des playbooks pour une meilleure qualité de service
- Exécution en temps réel
- Collaboration rationalisée entre les équipes et les outils
- Documentation automatique
- Plate-forme multiclient évolutive et sécurisée
- Cadre d'intégration extensible
- Déploiement flexible sur site et dans le Cloud

## PRINCIPAUX AVANTAGES

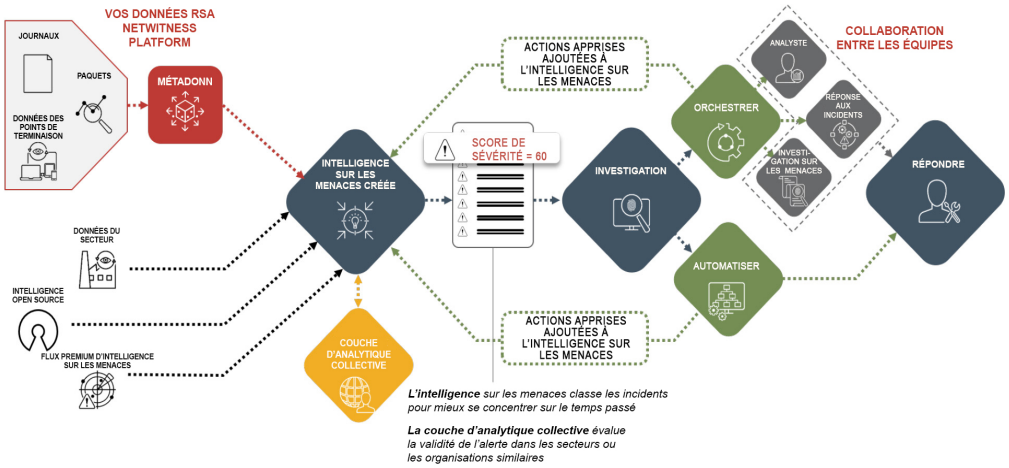
- Automatisation : donnez la capacité aux logiciels d'effectuer des tâches « humaines » et d'automatiser la recherche des menaces
- Orchestration : automatisez ou systématisez la prise de décision
- Tableau de bord et création de rapports : visualisez les indicateurs optimisés par l'intelligence sur les menaces
- Gestion des incidents et collaboration : proposez la gestion des incidents de bout en bout
- Temps de réponse : accélérez le temps de réponse et réduisez les erreurs en améliorant la productivité des analystes et en réduisant le temps moyen de correction (MTTR, Mean Time to Remediation)

## DONNER LA PRIORITÉ AUX MENACES LES PLUS IMPORTANTES

À l'heure où les surfaces d'attaque se multiplient, il est devenu de plus en plus complexe et chronophage de se protéger contre les attaquants, qu'il s'agisse de logiciels malveillants courants, de menaces et de logiciels criminels provenant de personnel interne jusqu'aux attaques parrainées par l'état, ou encore d'attaques d'hacktivistes et de terroristes. Toutes les menaces ne sont pas égales et ne méritent pas la même attention. Pourtant, les silos déconnectés des technologies de prévention, de surveillance et d'investigation ne parviennent pas à éradiquer les faux positifs, à éliminer les actions manuelles répétitives, et à cibler les réponses. Les équipes de sécurité ont besoin d'une solution complète qui permet aux centres d'opérations de sécurité (SOC, Security Operations Centers) d'automatiser efficacement les processus, et de détecter et de répondre aux menaces les plus importantes.

La solution RSA NetWitness® Orchestrator, optimisée par ThreatConnect™, est une technologie complète d'automatisation et d'opérations de sécurité qui allie gestion intégrale des incidents, automatisation et orchestration intelligentes, et investigation collaborative. RSA NetWitness Orchestrator apporte cohérence et efficacité à l'investigation, à la recherche et à la réponse aux menaces. En tirant profit des playbooks et de l'intelligence intégrée sur les menaces, la solution enrichit autant qu'elle automatise le flux de travail, la collaboration et la réponse des analystes. RSA NetWitness Orchestrator joue le rôle de connecteur pour RSA NetWitness Platform et d'arsenal de sécurité complet pour l'équipe des opérations de sécurité.

## L'INTELLIGENCE SUR LES MENACES AU CŒUR DE L'ORCHESTRATION ET DE L'AUTOMATISATION



## RSA NETWITNESS ORCHESTRATOR : CONFIGURATION MATÉRIELLE

Instance physique

- Prérequis physiques pour les serveurs
  - — Serveur d'applications (sans playbooks)
    - Mémoire : 16 Go
    - Cœurs de processeur : 8 (2 GHz)
    - Stockage estimé : 50 Go
  - — Serveur d'applications (playbooks)
    - Mémoire : 48 Go
    - Cœurs de processeur : 8 (2 GHz)
    - Stockage estimé : 150 Go
  - — Serveur de base de données (< 2 millions d'indicateurs)
    - Mémoire : 12 Go
    - Cœurs de processeur : 6 (2 GHz)
    - Stockage : 20 Go
  - — Serveur de base de données (2-5 millions d'indicateurs)
    - Mémoire : 16 Go
    - Cœurs de processeur : 8 (2 GHz)
    - Stockage : 40 Go
  - — Serveur de base de données (5-10 millions d'indicateurs)
    - Mémoire : 32 Go
    - Cœurs de processeur : 12 (2 GHz)
    - Stockage : 60 Go
  - — Serveur Elasticsearch® (< 2 millions d'indicateurs)
    - Mémoire : 12 Go
    - Cœurs de processeur/ processeurs virtuels : 6 (2 GHz)
    - Stockage : 20 Go
  - — Serveur Elasticsearch (2-5 millions d'indicateurs)
    - Mémoire : 16 Go
    - Cœurs de processeur/ processeurs virtuels : 8 (2 GHz)
    - Stockage : 40 Go
  - — Serveur Elasticsearch (5-10 millions d'indicateurs)
    - Mémoire : 32 Go
    - Cœurs de processeur/ processeurs virtuels : 12 (2 GHz)
    - Stockage : 60 Go

## REDÉFINIR LA GESTION DES INCIDENTS

RSA NetWitness Orchestrator permet aux équipes chargées des opérations de sécurité de collecter des alertes isolées provenant de l'arsenal de sécurité de l'organisation et de les transformer en incidents corrélés, dotés de contexte, contenant des données stratégiques. Il tient compte des données sur la réputation de l'utilisateur, le système, l'adresse IP, le réseau, les incidents connexes, les récidivistes et l'intelligence sur les menaces, ce qui permet aux analystes de prendre rapidement des décisions éclairées. Il sert de base aux décisions relatives aux opérations de sécurité, avec un processus de gestion des incidents à la fois bien structuré, cohérent et documenté de manière automatique qui regroupe, met en corrélation et enrichit les alertes de sécurité tout au long du cycle de vie de la gestion des incidents.

## AUTOMATISER CE QUE L'ON CONNAÎT. DÉTECTER CE QUE L'ON NE CONNAÎT PAS.

La visibilité est la clé d'une détection efficace des menaces. RSA NetWitness Orchestrator propose plus de 500 applications et intégrations donnant lieu à d'innombrables actions de sécurité, notamment des enquêtes conjointes et transparentes qui réduisent le temps de résolution par incident. Les analystes de la sécurité peuvent accélérer la détection des menaces et organiser la réponse à l'échelle de l'entreprise grâce à des données complètes sur les journaux, le réseau, les points de terminaison et les solutions liées ou non au domaine de la sécurité. Tirez profit d'un playbook riche et préconfiguré, ou personnalisez votre propre solution pour une réponse aux incidents cohérente et précise. Utilisez RSA NetWitness Orchestrator pour automatiser la gestion des menaces connues et à faible risque, accélérer le confinement et l'éradication, et libérer les analystes afin qu'ils étudient les problèmes à plus haut risque.

## ORCHESTRATION ET AUTOMATISATION OPTIMISÉES PAR L'INTELLIGENCE SUR LES MENACES

Contrairement aux solutions qui utilisent l'intelligence uniquement pour déclencher des flux de travail spécifiques, RSA NetWitness Orchestrator tire parti de l'intelligence sur les menaces pour toutes les fonctions d'orchestration et d'automatisation, pour un contexte riche et des playbooks qui s'adaptent continuellement. La plate-forme exploite également toute la valeur des différentes formes d'intelligence, avec la prise en charge de la coordination entre les équipes au sein des flux de travail.

En combinant l'intelligence sur les menaces, l'orchestration, l'automatisation et la réponse, RSA NetWitness Orchestrator fournit des informations holistiques à l'échelle du système. Ainsi, les opérations de sécurité offrent les possibilités suivantes :

- **Alerter, bloquer et mettre en quarantaine en fonction des informations pertinentes d'intelligence sur les menaces.** Même pour les tâches de niveau inférieur telles que l'alerte et le blocage, il est important de collecter des informations pertinentes d'intelligence sur les menaces. Vous pouvez automatiser la détection et la prévention, mais vous avez besoin d'une solution validée d'intelligence sur les menaces, dotée de sources multiples, pour garantir des alertes (et des blocages) judicieux.

## RSA NETWITNESS ORCHESTRATOR : CONFIGURATION MATÉRIELLE

- Système d'exploitation : Variante Red Hat® Linux : Red Hat Enterprise Linux (RHEL) ou Community Operating System (CentOS) 6 ou 7
- Kit de développement d'Oracle® Java® : accès à une installation locale d'Oracle Java 8 ou OpenJDK (JDK version 1.8)
- Extension de chiffrement Java : version 8
- Elasticsearch : serveur Elasticsearch 6.3.0
- Python® : installation de Python 3.6.x uniquement, référence à CPython
- SDK Python : Version TCEX 1.0+
- Redis : installation de Redis 4.0.10
- Base de données (sélectionnez l'un des éléments suivants) :
  - MySQL® : installation de MySQL 5.7.x Community ou Enterprise Edition
  - SAP S/4HANA® : installation de SAP S/4HANA 2.0 SPS 02
  - PostgreSQL : installation de PostgreSQL v11

REMARQUE : n'installez qu'une seule base de données de travail.

- **Améliorer l'exactitude, la confiance et la précision.** La sensibilisation à la situation et le contexte historique sont essentiels à la prise de décision. Le lien direct avec l'intelligence sur les menaces vous permet de travailler plus rapidement et d'éviter de nouvelles attaques. Plus vous pouvez automatiser en amont, plus vous serez proactif. L'élimination des faux positifs et l'utilisation d'une intelligence validée vous aident à prendre des mesures plus précises qui, à leur tour, améliorent la rapidité et la précision.
- **Comprendre le contexte et permettre l'amélioration au fil du temps.** Automatisez les tâches sur la base de seuils d'intelligence sur les menaces (tels que les scores de réputation de l'indicateur), puis conservez toutes ces informations pour ensuite améliorer stratégiquement vos processus.
- **Orchestrer en toute confiance.** L'analytique logique en natif de l'intelligence sur les menaces externes permet d'effectuer des alertes plus précises avec moins de faux positifs, de blocs et de quarantaines. Malheureusement, vous ne pouvez pas simplement absorber de nombreux flux d'intelligence sur les menaces ou bien agir à partir d'un indicateur de compromission partagé. Vous devez donner du sens aux informations à grande échelle, à l'aide de scores et de mises en contexte pour prendre des mesures et savoir si une action est nécessaire.
- **Élaborer une intelligence organique à partir des opérations et réponses de sécurité.** Votre équipe et vos données sont les meilleures sources d'intelligence. Ce que vous souhaitez, c'est capturer des informations, artéfacts et vues provenant des engagements d'opérations et de réponse, puis les affiner immédiatement pour les convertir en intelligence, sous la forme de nouveaux indicateurs de compromission, de tactiques et techniques hostiles, et de connaissances sur les failles de sécurité.
- **Ajuster automatiquement les processus à mesure que les informations et le contexte changent.** Vous devriez être en mesure d'adapter vos fonctionnalités d'orchestration à l'évolution de l'intelligence sur les menaces, d'ajuster automatiquement les processus internes en fonction de la classification des indicateurs et des scores d'évaluation des menaces. Mettez à jour ces processus et ces flux de travail de manière dynamique pour rendre les efforts de votre équipe plus pertinents et plus efficaces.

## DÉPLOIEMENT FLEXIBLE ET ÉVOLUTIF

La solution RSA NetWitness Orchestrator est entièrement conçue pour prendre en charge les déploiements dans les environnements avec un ou plusieurs clients et les véritables environnements sur site. Quel que soit le déploiement, les données sont séparées en toute sécurité avec des options simples pour une mise à l'échelle verticale et horizontale. La technologie RSA prend en charge l'orchestration sur plusieurs environnements réseau avec une gestion centralisée.

Les technologies traditionnelles d'orchestration et d'automatisation de la sécurité ont du mal à évoluer afin de gérer le volume et l'étendue de la charge applicative nécessaire pour optimiser l'automatisation et l'enrichissement du centre d'opérations de sécurité (SOC). Avec ces technologies, les équipes de sécurité ne sont en mesure d'automatiser que quelques cas d'utilisation, ce qui laisse de nombreux flux de travail manuels. La solution RSA NetWitness Orchestrator propose une architecture véritablement évolutive qui permet aux charges applicatives d'orchestration et d'automatisation de se développer en même temps que le SOC. Les équipes de sécurité peuvent hiérarchiser l'exécution, dédier des ressources à des playbooks spécifiques et ajouter des serveurs de playbooks supplémentaires au fur et à mesure que les charges applicatives augmentent.

## RSA NETWITNESS PLATFORM

Avec plus de 30 ans d'expertise en matière de sécurité, RSA continue de diriger le marché à l'aide d'une solution innovante qui répond aux défis les plus exigeants en matière d'opérations de sécurité pour les plus grandes organisations au niveau mondial. La nouvelle solution RSA NetWitness Orchestrator étend la plate-forme RSA NetWitness Platform et ses offres avancées en matière de SIEM (gestion des événements et des informations de sécurité) et de défense contre les menaces, en tirant profit d'une visibilité omniprésente sur les journaux, le réseau et les points de terminaison.

## À PROPOS DE RSA

Les solutions RSA offrent aux organisations une approche unifiée de la gestion du risque numérique qui repose sur une visibilité intégrée, des informations automatisées et des actions coordonnées. Les solutions RSA sont conçues pour détecter et traiter efficacement les attaques avancées, gérer les contrôles d'accès des utilisateurs, et réduire les risques métiers, la fraude et la cybercriminalité. RSA protège des millions d'utilisateurs dans le monde entier et aide plus de 90 % des sociétés du classement Fortune 500 à prospérer et à s'adapter en permanence au changement transformationnel. Pour plus d'informations, accédez au site rsa.com/fr-fr.