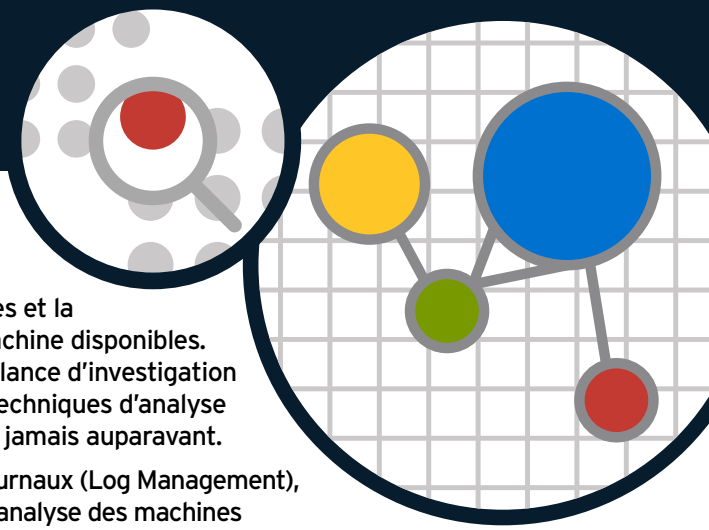
LA PLATE-FORME POUR L'ANALYSE DE LA SÉCURITÉ

LogRhythm™



La protection contre les menaces actuelles qui évoluent rapidement nécessite une visibilité profonde de l'ensemble de l'environnement informatique. Les menaces et les risques arrivent sous de nombreux angles et la preuve de leur existence se retrouve dans les données de journal et de machine disponibles. Une visibilité plus profonde, et essentielle, est obtenue grâce à une surveillance d'investigation d'hôtes et de réseaux ciblés. Lorsque cela est appliqué à de nombreuses techniques d'analyse automatique de machine, les menaces et les risques sont exposés comme jamais auparavant.

LogRhythm combine de façon unique une solution SIEM, une gestion des journaux (Log Management), une surveillance de l'intégrité des fichiers (File Integrity Monitoring) et une analyse des machines (Machine Analytics) à l'échelle de l'entreprise avec une investigation des hôtes et des réseaux (Host Forensics et Network Forensics) dans une plate-forme d'analyse de la sécurité (Security Analytics) totalement intégrée. La solution de LogRhythm offre une visibilité profonde des menaces et des risques que les organisations ne sauraient voir autrement. Conçue pour aider à prévenir les atteintes à la sécurité avant qu'elles ne se produisent, l'analyse de la sécurité de LogRhythm détecte de façon précise un large éventail d'indicateurs précoces de menaces, ce qui permet une réponse rapide pour atténuer leurs répercussions. La visibilité et la compréhension profondes fournies par l'analyse de la sécurité de LogRhythm permet aux entreprises de sécuriser leurs réseaux et de satisfaire aux exigences réglementaires.

Un niveau plus élevé en matière de SIEM et d'analyse de la sécurité

LogRhythm offre une nouvelle génération de capacités de détection, de défense et de réponse en ce qui concerne les cybermenaces et les risques associés. La plate-forme d'analyse de la sécurité de LogRhythm offre les avantages suivants :

- SIEM et gestion des journaux (Log Management) de nouvelle génération
- Investigation des hôtes (Host Forensics) et surveillance de l'intégrité des fichiers (File Integrity Monitoring) indépendantes
- Investigation des réseaux (Network Forensics) avec identification des applications et capture complète des paquets
- Analyse des machines de pointe
  - Corrélation avancée et reconnaissance de formes
  - Détection des anomalies de comportement des utilisateurs/hôtes/réseaux (User/Host/Network Behavior Anomaly Detection) multidimensionnelle
- Recherche intelligente et rapide
- Analyse de grandes quantités de données par analyse visuelle, pivotement et exploration
- Réponse automatique compatible avec le flux de travaux via Smart**Response**™ de LogRhythm
- Gestion intégrée des cas

L'analyse de toutes les données de journal et de machine disponibles, combinée avec une profonde vision d'investigation, tant au niveau de l'hôte que du réseau, offre une véritable visibilité. Celle-ci est optimisée par AI Engine, notre technologie d'analyse des machines (Machine Analytics) brevetée, pour fournir une analyse continue automatique de toute l'activité observée dans l'environnement informatique. AI Engine permet aux organisations d'identifier les menaces et les risques non détectés jusqu'à maintenant. L'architecture intégrée garantit que lorsque des menaces sont détectées, les clients peuvent accéder rapidement à une vision globale de l'activité, ce qui permet un renseignement de sécurité exceptionnel et une réponse rapide. LogRhythm Security Analytics est la seule solution à offrir les capacités de renseignement actionnable et de réponse aux incidents nécessaires pour faire face aux cybermenaces actuelles les plus sophistiquées.

Court délai de rentabilité

Que vous protégiez un petit réseau d'entreprise ou que vous dirigiez un centre de gestion de la sécurité à l'échelle mondiale, le délai de rentabilité et le coût total de propriété sont importants. L'architecture intégrée de LogRhythm, combinée à l'attention portée à la facilité d'utilisation, aide les clients à tirer rapidement parti des capacités performantes tout en contrôlant les coûts à long terme. Nous sommes fiers de transformer des problèmes complexes en solutions faciles à utiliser.

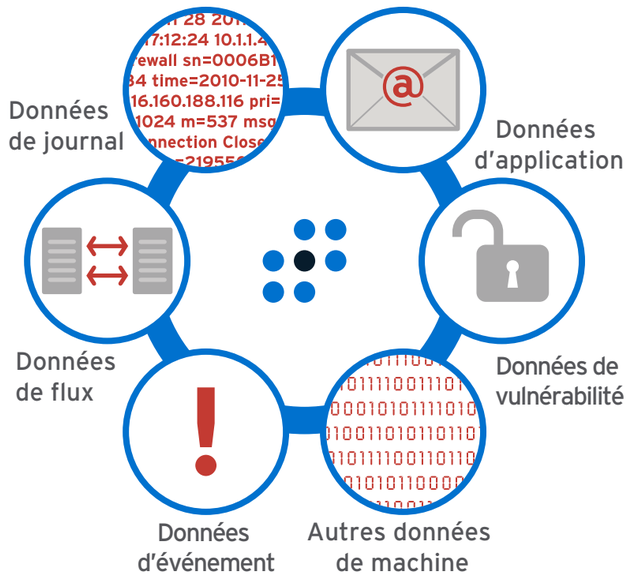
LogRhythm Labs™ dispose de capacités essentielles prêtes à être utilisées qui s'adaptent aux déploiements des clients pour leur permettre d'atteindre leurs objectifs d'affaires. Fournie automatiquement et mise à jour de façon continue avec les dernières avancées de la recherche sur les menaces et la conformité, la large base de connaissances de LogRhythm permet aux clients de s'armer rapidement contre les menaces émergentes, tout en restant au fait des exigences de conformité et de vérification. La base de connaissances présente les avantages suivants :

- Analyse des journaux et règles de normalisation pour plus de 600 systèmes d'exploitation, applications, bases de données, dispositifs, etc.
- Suites d'automatisation de la conformité pour un large éventail de réglementations (PCI, SOX, HIPAA, FISMA, GLBA, ISO27001, DODI 8500.1, NERC-CIP, etc.)
- Modules d'analyse de la sécurité (Security Analytics)
  - Surveillance des utilisateurs privilégiés (Privileged User Monitoring)
  - Menaces persistantes avancées (Advanced Persistent Threat - APT)
  - Défense des applications internet (Web Application Defense)
  - Détection des anomalies de comportement des utilisateurs/hôtes/réseaux (User/Host/Network Behavior Anomaly Detection)
  - Et bien d'autres encore...

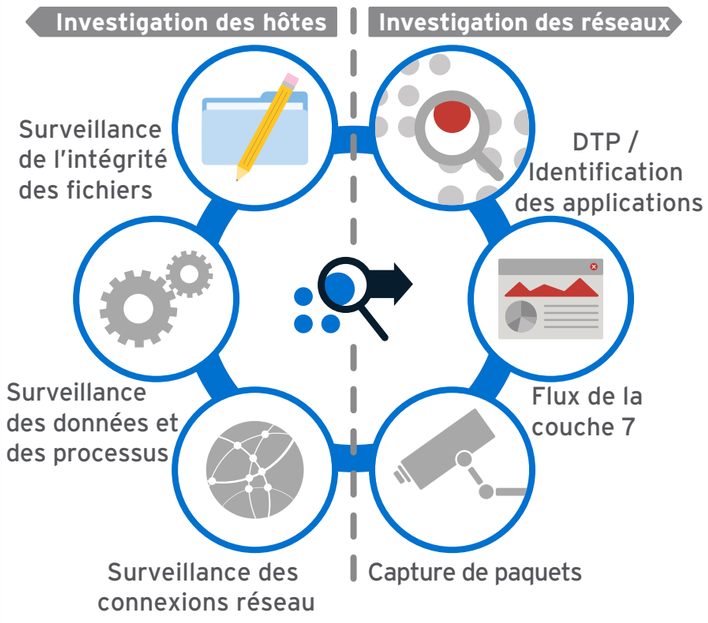
LA PLATE-FORME POUR LES ANALYSES DE SÉCURITÉ

Entrée

COLLECTE DE DONNÉES D'INVESTIGATION



GÉNÉRATION DE DONNÉES D'INVESTIGATION



LogRhythm Analytics™

TRAITEMENT

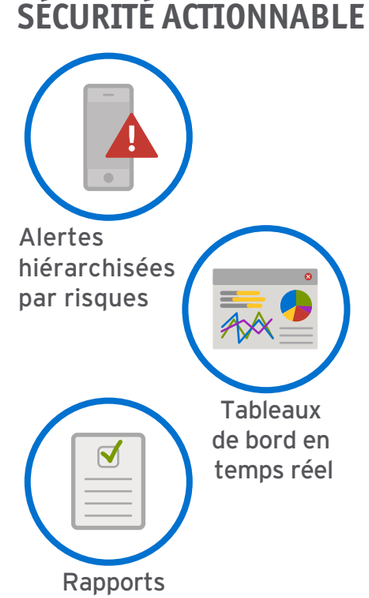
ANALYSE EN TEMPS RÉEL

ANALYSE D'INVESTIGATION

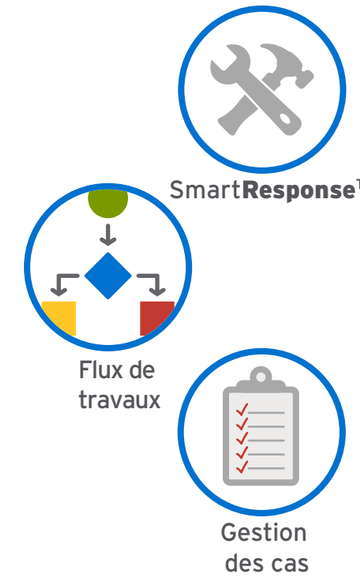
CYBERDÉFENSE ADAPTATIVE

Sortie

RENSEIGNEMENT DE SÉCURITÉ ACTIONNABLE



RÉPONSE AUX INCIDENTS



Options de déploiement souples

Appareils hautes performances

	ALL-IN-ONE (XM) (comprend EM, LM, AIE)		EVENT MANAGER (EM) SPÉCIALISÉ (comprend la licence d'AI Engine)			LOG MANAGER(LM) SPÉCIALISÉ			AI ENGINE (AIE) SPÉCIALISÉ			SITE LOG FORWARDER (SLF)	NETWORK MONITOR (NM)
Série d'appareils	4300	6300	3300 [3]	5300 [4]	6300 [5]	3300	5300	7300	5300	7300	9300	3310	3300
Vitesses d'archivage max.	10 000 MPS	25 000 MPS	S.O.	S.O.	S.O.	10 000 MPS	25 000 MPS	50 000 MPS	S.O.	S.O.	S.O.	S.O.	S.O.
Vitesses de traitement max.	1 000 MPS	5 000 MPS	S.O.	S.O.	S.O.	2 000 MPS	5 000 MPS	15 000 MPS	5 000 MPS	30 000 MPS	75 000 MPS	S.O.	1 Gops

[1] MPS = Messages par seconde. [2] Les vitesses individuelles varient en fonction de l'environnement informatique/des exigences du client. [3] Comprend une licence AIE intégrée de 2 000 MPS. [4] Comprend une licence AIE intégrée de 10 000 MPS. [5] Comprend une licence AIE intégrée de 20 000 MPS.

> Un produit fantastique et une valeur tout aussi fantastique. Nous en avons fait notre **MEILLEUR ACHAT.**
>
> SC MAGAZINE

> LogRhythm est généreux en termes de **FONCTIONS ET DE SOUPLESSE.**
>
> INFOWORLD

Logiciels | Virtualisation

Les solutions logicielles de LogRhythm peuvent être facilement déployées sur le matériel client et la plupart des plates-formes de virtualisation, dont :

vmware · Windows Server 2008 Hyper-V · CITRIX XenServer

Services de LogRhythm

LogRhythm offre des services d'assistance et professionnels de calibre mondial visant de façon unique à fournir des solutions pratiques et à apporter de la valeur. De la plus grande organisation au monde aux petites et moyennes entreprises, LogRhythm maintient son engagement de maximiser le succès et la satisfaction des clients.

LogRhythm Labs

LogRhythm Labs agit comme une équipe de recherche sur les menaces virtuelles de sécurité et la conformité, qui travaille pour le client. Il offre un renseignement de sécurité prêt à être utilisé et une expertise intégrée pour la gestion avancée des menaces ainsi que l'automatisation et la garantie de la conformité. L'équipe est formée de spécialistes qui se consacrent à la sécurité des informations, dont des experts en la matière qui couvrent un large éventail de domaines, notamment la détection des intrusions, les logiciels malveillants avancés, la réponse aux incidents, la vérification et la conformité informatiques. Les chercheurs de LogRhythm Labs détiennent un grand nombre de certifications du secteur (par exemple, CISSP, CISA, CEH, etc.). Grâce à une formation continue et à une recherche approfondie, ils restent au fait des dernières avancées en matière de menaces, de méthodes, de conformité et de meilleures pratiques.

LogRhythm en action

Détection de logiciels malveillants personnalisés avec la détection des anomalies de comportement des hôtes (Host Behavior Anomaly Detection)

Défi : les logiciels malveillants liés aux attaques zero-day sont spécifiquement conçus pour éluder les solutions de sécurité classiques qui sont créées pour détecter des signatures spécifiques et des comportements malveillants connus.

1. LogRhythm établit une référence de comportement « normal » pour les hôtes et crée une liste blanche de l'activité de processus acceptable.
2. La surveillance de l'activité des hôtes (Host Activity Monitoring) détecte indépendamment le lancement d'un nouveau processus.
3. LogRhythm reconnaît automatiquement que le nouveau processus ne figure pas sur la liste blanche.
4. L'analyse des machines de LogRhythm corrobore l'événement, par rapport à l'activité associée, comme un trafic réseau anormal et identifie précisément l'activité comme à haut risque.
5. Une alarme est envoyée à un administrateur de la sécurité, qui accède facilement aux informations d'investigation pour étudier le problème.

Exposition des identifiants compromis avec la détection des anomalies de comportement des utilisateurs (User Behavior Anomaly Detection)

Défi : en raison des défis organisationnels comme un personnel de plus en plus mobile et l'adoption croissante du BYOD, les entreprises ont du mal à distinguer un comportement « normal » d'une activité indiquant que les identifiants d'un utilisateur ont été compromis.

1. LogRhythm établit automatiquement un profil pour des utilisateurs spécifiques, comprenant des listes blanches d'activité acceptable et des références de comportement à partir des activités observées pour ces utilisateurs.
2. AI Engine détecte lorsqu'un utilisateur lance une activité anormale, comme une ouverture de session depuis un lieu suspect, ou se dévie d'une norme de comportement, comme l'accès à des données ou volumes de donnés significativement différents et le téléchargement de ces données vers une application de partage en nuage ne figurant pas sur la liste blanche.
3. SmartResponse™ désactive automatiquement le compte ou met la réponse en attente pour validation après une investigation plus détaillée de l'activité de l'utilisateur.

Identification de l'exfiltration de données avec la détection des anomalies de comportement des réseaux (Network Behavior Anomaly Detection)

Défi : le flux constant de données entrant et sortant de l'entreprise rend difficile de détecter lorsque des données sensibles sortent du réseau de l'entreprise.

1. Network Monitor offre une visibilité critique des points d'entrée/sortie du réseau, en générant des données SmartFlow™ qui fournissent une visibilité profonde des paquets dans chaque session de réseau observée et dans les applications utilisées.
2. L'analyse des machines de LogRhythm établit plusieurs références de comportement pour les activités observées sur le réseau en tirant parti des métadonnées de paquet étendues fournies par SmartFlow™.
3. Les anomalies de réseau sont identifiées et corroborées par rapport à d'autres données de journal et de machine pour fournir une visibilité précise de l'activité à haut risque.
4. SmartCapture™ capture automatiquement tous les paquets associés aux sessions suspectes pour une investigation complète des paquets.