PRÉSENTATION DU PRODUIT

Network Monitor

LogRhythm™

Un véritable renseignement de sécurité d'entreprise nécessite une connaissance en temps réel et une compréhension de toutes les données passant sur le réseau. Network Monitor de LogRhythm offre une connaissance au niveau de l'application et des informations détaillées sur la session réseau, fournissant une visibilité du réseau à l'échelle de l'entreprise. À partir de nombreuses métadonnées totalement consultables, Network Monitor offre un accès rapide à des preuves d'investigation de grande valeur, ce qui se traduit par une compréhension rapide et en profondeur de l'activité réseau. En outre, la capacité de Network Monitor à réaliser une capture complète des paquets offre un accès aux données brutes concernant les paquets de chaque session pour obtenir des preuves d'investigation supplémentaires.

Network Monitor de LogRhythm fournit une visibilité fondamentale pour détecter et combattre les menaces avancées actuelles. Il permet aux organisations de mener les actions suivantes :

- Établir des références de comportement pour identifier immédiatement une activité anormale
- Détecter une activité d'application non autorisée ou suspecte
- Accélérer les investigations du réseau
- Réaliser une capture complète des paquets d'une session pour une investigation avancée
- Prévenir la perte de données sensibles
- Surveiller la consommation de bande passante d'une application

Véritable identification des applications – identifie plus de 2 100 applications pour une analyse poussée, en effectuant une inspection de paquets en profondeur et en appliquant plusieurs méthodes de classification afin de déterminer la véritable identité de l'application. Une véritable identification d'application offre la visibilité nécessaire pour détecter les activités critiques comme les transferts de données suspects, les violations de politique d'utilisation du réseau et les attaques avancées.

SmartFlow™ – offre de nombreuses métadonnées par paquets provenant de chaque session réseau, en fonction du type d'application utilisé. Le haut degré de détail disponible dans SmartFlow™, obtenu en cataloguant chaque session sur le réseau, offre une compréhension profonde de l'activité réseau d'une application sous un format rapidement accessible.

Recherche non structurée, analyse puissante – offre un accès rapide aux informations de SmartFlow™ à l'aide d'un puissant moteur de recherche, semblable à celui de Google, qui rationnalise et simplifie les investigations réseau. Les résultats sont présentés dans des vues très détaillées et des couches personnalisées, permettant une analyse extrêmement rapide des données par paquets du réseau.

Capture complète des paquets d'une session – capture complètement l'en-tête des paquets des couches 2 à 7 et les données utiles de chaque session pour un enregistrement complet de l'activité réseau. Toutes les informations sont organisées par session, offrant un contexte complet des communications et des contenus d'application transférés sur le réseau.

SmartCapture™ – offre une capture complète de paquets sans les importantes exigences de stockage des solutions classiques, en ne retenant que les sessions d'intérêt.

Intégration simplifiée – fournit une alimentation en temps réel de nombreuses données SmartFlow™ à Security Intelligence Platform de LogRhythm et à d'autres solutions tierces.

Intelligence de sécurité de LogRhythm

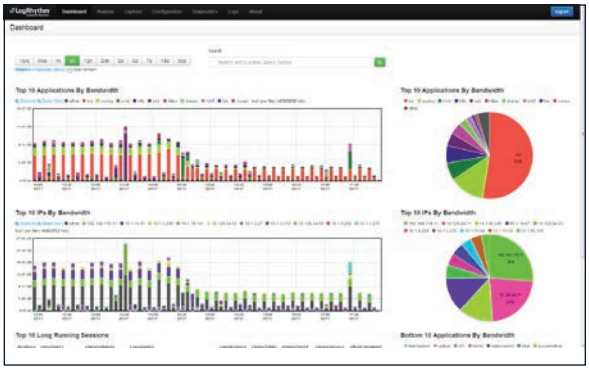
Network Monitor de LogRhythm peut être déployé de façon autonome ou comme un élément totalement intégré de la solution SIEM primée de LogRhythm, offrant une intelligence de sécurité sans égale dans toutes les activités réseau. La plate-forme intégrée comprend les éléments suivants :

- Une analyse de la sécurité en temps réel dans toutes les données d'investigation reconnaissant les événements très sensibles dans :
  - Les données de journal et de vérification sur tout le réseau
  - L'activité d'hôte collectée de manière indépendante via System Monitor de LogRhythm
  - L'activité réseau collectée de manière indépendante via Network Monitor de LogRhythm
- Des capacités complètes prêtes à être utilisées pour la détection des anomalies de comportement réseau (NBAD - Network Behavior Anomaly Detection)
- Une recherche et une visualisation puissantes, comprenant l'exploration, le pivotement et la corrélation pour accélérer les investigations
- Le déclenchement d'une capture complète des paquets d'une session par SmartCapture™ de Network Monitor en réponse à des activités très prioritaires reconnues par la solution SIEM.

> « Les capacités prêtes à être utilisées de NBAD permettent de détecter et d'étudier le trafic suspect pour identifier un large éventail de problèmes, allant de la présence de logiciels malveillants à une consommation excessive de bande passante par vidéoconférence. »
>
> *Vaughn Adams* Responsable informatique, InterDigital.

Network Monitor en action

Network Monitor de LogRhythm exécute des cas d'utilisation réels pour résoudre les problèmes de sécurité critiques et mettre en évidence les anomalies réseau et des activités inappropriées d'utilisateurs. Quelle que soit votre préoccupation, les logiciels malveillants personnalisés, l'espionnage ou l'utilisation frauduleuse courante des réseaux, LogRhythm offre la vision profonde nécessaire pour détecter un large éventail de menaces tout en permettant des réponses éclairées beaucoup plus efficaces.



Vol de données

Reconnaitre rapidement les événements pertinents liés à une violation peut aider à réduire l'exposition et le coût de correction.

1. Le tableau de bord de Network Monitor met en évidence les sessions SSH de longue durée.
2. Les informations SmartFlow™ de Network Monitor indiquent que le protocole SSH est utilisé pour percer un tunnel vers l'hôte, offrant un accès à distance au système.
3. Des mesures supplémentaires peuvent alors être prises pour protéger des hôtes ciblés et pour refuser l'accès au réseau du système à l'origine de l'attaque.

Détection de réseaux zombie

Aujourd'hui, les appels de réseaux zombie utilisent des ports standard et probablement des applications légitimes pour déguiser leur trafic afin d'éviter d'être détectés.

1. Network Monitor observe le trafic non-HTTP sur le port 80 et identifie la véritable application ou expose les en-têtes de paquets HTTP malformés.
2. La capture complète des paquets de la session révèle des contenus supplémentaires non identifiés par les outils de sécurité classiques, permettant d'aller au-delà dans l'analyse et la vérification des menaces identifiées.

> « Grâce à Network Monitor, nous avons amélioré matériellement nos capacités de défense, de détection et de réponse pour de nombreux environnements de données sécurisés. »
>
> *Erin Osminer*
> Ingénieur réseau
> StoneRiver

Utilisation de réseau inappropriée

Sans renseignement de sécurité supplémentaire à celui que les flux de données classiques fournissent, il est difficile de distinguer l'activité légitime d'un comportement suspect.

1. L'analyse de flux classique identifie une utilisation excessive de la bande passante depuis un site Internet sur http, mais ne fournit aucune information supplémentaire.
2. Network Monitor obtient de nombreuses métadonnées de la session réseau qui identifient des informations comme l'existence du téléchargement d'un grand fichier, l'URL source ou de destination, et le nom des fichiers transférés.
3. Accès rapide aux informations SmartFlow™ grâce à la recherche intuitive de Network Monitor, qui identifie rapidement une activité inappropriée, comme le transfert de contenus protégés par des droits d'auteur ou l'utilisation d'une application de partage en nuage non autorisée.

Déploiement

Network Monitor utilise une IU Internet simple et intuitive pour gérer l'installation et les mises à jour. Disponible comme appareil spécialisé ou logiciel à installer, Network Monitor est déployé hors bande sur TAP ou SPAN, ou bien par intégration avec des solutions de courtier de paquets réseau de tiers. Network Monitor commence immédiatement à analyser le trafic et à reconnaître les applications, offrant une recherche en temps réel semblable à celle de Google dans toutes les captures de paquets et les métadonnées. Il offre également la possibilité d'envoyer les informations SmartFlow™ de la couche 7 à la solution SIEM ou à d'autres solutions pour une analyse supplémentaire.

Logiciel

Le logiciel Network Monitor de LogRhythm peut être facilement déployé sur le matériel client.

Matériel

SÉRIE D'APPAREILS	TRAITEMENT MAX.	UNITÉ CENTRALE	MÉMOIRE	STOCKAGE	CHÂSSIS	PUISSANCE	ETHERNET	DIMENSIONS	POIDS
LR-NM3330	500 Mbps	2,1 GHz	64 GO	2 TO	1 U	100-240 V	4 X 1 GO	H 4,28 CM X L 48,24 CM X P 67,73 CM	19,3 kg
LR-NM3350	1 Gbps	2,1 GHz	64 GO	2 TO	1 U	100-240 V	4 X 1 GO	H 4,28 CM X L 48,24 CM X P 67,73 CM	19,3 kg

Des options de stockage adjoint direct supplémentaire sont disponibles, offrant une capacité étendue pour le stockage des données SmartFlow™ et les captures de paquets bruts. Network Monitor prend également en charge le déplacement des captures de paquets vers SAN ou un autre stockage pour une rétention à long terme.