exabeam

DATA SHEET

EXABEAM SECURITY MANAGEMENT PLATFORM

Les SIEM traditionnels ne satisfont plus aux besoins de la plupart des entreprises. Malgré des promesses plus séduisantes que jamais, telles que fournir une visibilité complète sur les menaces touchant un réseau et y répondre de manière automatisée et intelligente, la plupart des SIEM s'avèrent aujourd'hui dépassés et inefficaces. Ils reposent en effet sur des technologies propriétaires vieillissantes de gestion des logs qui sont (sur)tarifées en fonction des volumes de données, manquent de fonctions d'analyse intelligentes basées sur le machine learning et nécessitent des compétences techniques approfondies pour les mettre en œuvre. Afin d'illustrer ce constat, rappelons que la quasi-totalité des entreprises ayant été victimes d'une cyber-attaque ces dernières années comptaient alors sur un système SIEM. Les équipes de sécurité méritent bien mieux aujourd'hui !

EXABEAM – LE SMARTER SIEM™

Exabeam Security Management Platform (SMP) permet aux entreprises de détecter les cyberattaques, d'investiguer et d'y répondre plus efficacement afin que leurs équipes chargées des opérations de sécurité et des menaces internes puissent travailler plus efficacement, sans redoubler d'efforts. Finis les coûts excessifs de stockages des logs, les attaques distribuées ou les menaces inconnues non-détectées. Finis également les investigations et les mesures correctives manuelles fastidieuses. Grâce à Exabeam Security Management Platform, les analystes peuvent collecter un nombre illimité de logs, détecter les attaques grâce à l'analyse comportementale et automatiser la réponse aux incidents, que ce soit sur site ou dans le cloud.

UN PRIX PAR UTILISATEUR, ET NON PAR OCTET

Contrairement aux SIEM traditionnels, les prix d'Exabeam ne sont pas basés sur le volume des données. Exabeam Security Management Platform vous permet d'ingérer une quantité illimitée de données grâce à un modèle de tarification prévisible basé sur le nombre d'utilisateurs. Ainsi, vous n'avez plus à craindre que les sources de données volumineuses telles que les pare-feux, les EDR ou les proxies Web ne viennent gonfler le budget alloué à votre SIEM.

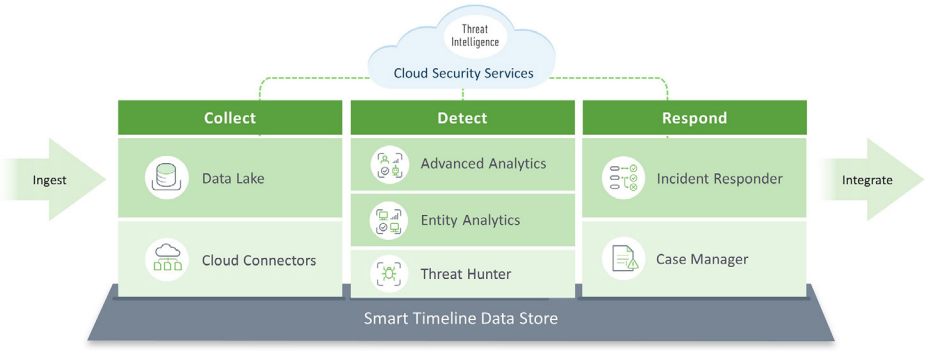
UNE DÉTECTION BASÉE SUR LE COMPORTEMENT, ET NON SUR DES RÈGLES

Exabeam détecte les menaces internes complexes en analysant le comportement des utilisateurs et des entités (UEBA). Cette approche de détection des menaces réduit les faux positifs et élimine les coûts de maintenance découlant de l'utilisation de règles traditionnelles basées sur des corrélation statiques. En plus d'identifier les anomalies à risque, l'UEBA recrée également les chaînes d'attaques entières grâce à la technologie Smart Timeline d'Exabeam, qui collecte les événements probants puis les assemble sous forme chronologique pour aider les analystes à comprendre la nature et l'impact des attaques.

UNE RÉPONSE EN QUELQUES MINUTES, ET NON EN JOURS

Exabeam augmente la productivité des équipes de réponse aux incidents (IR) et du centre des opérations de sécurité (SOC) en automatisant l'orchestration de tâches définies dans un playbook, via les API de solutions tierces (SOAR). Les playbooks et workflows d'incident prédéfinis ou personnalisés standardisent les procédures de réponse à partir du système de gestion d'incident inclus dans la solution. Cela garantit une réponse aux incidents à la fois rapide et reproductible qui renforce la productivité tout en minimisant les erreurs humaines.

EXABEAM SECURITY MANAGEMENT PLATFORM



Exabeam Security Management Platform comprend les solutions suivantes, fournies sous forme soit d'appliances physiques ou virtuels, soit de service cloud :

- **Exabeam Data Lake** – Collecte, indexation, recherche et affichage de toutes vos données de journaux, le tout à un prix prévisible
- **Exabeam Cloud Connectors** – Collecte fiable des jour**naux de plus de 40 services cloud**
- **Exabeam Advanced Analytics** – Analyse comportementale avancée visant à détecter les menaces complexes et les mouvements latéraux
- **Exabeam Entity Analytics** – Analyse comportementale pour les équipements connectés à un réseau et les serveurs
- **Exabeam Threat Hunter** – Investigation des menaces (threat hunting) via une interface intuitive génèrant des chronologies de manière automatique
- **Exabeam Incident Responder** – Réponse rapide et efficace grâce à des playbooks de sécurité automatisés
- **Exabeam Case Manager** – Outil de gestion d'incidents offrant de nombreuses fonctionnalités, et directement intégré avec les workflow de détection, d'investigation et de SOAR d'Exabeam

POUR SAVOIR COMMENT EXABEAM PEUT VOUS AIDER, VISITEZ EXABEAM.COM AUJOURD'HUI.