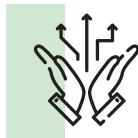




Le SIEM/UBA nouvelle génération



### Les avantages d'Exabeam :

- Un modèle de tarification prédictif.
- Une détection améliorée des menaces grâce au machine learning.
- Des analyses plus efficaces grâce à la diminution du nombre de faux positifs et l'automatisation des réponses.



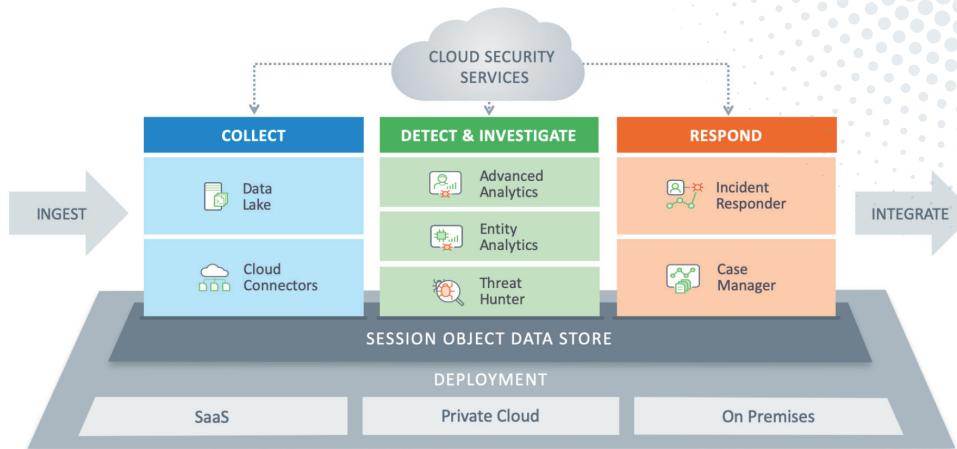
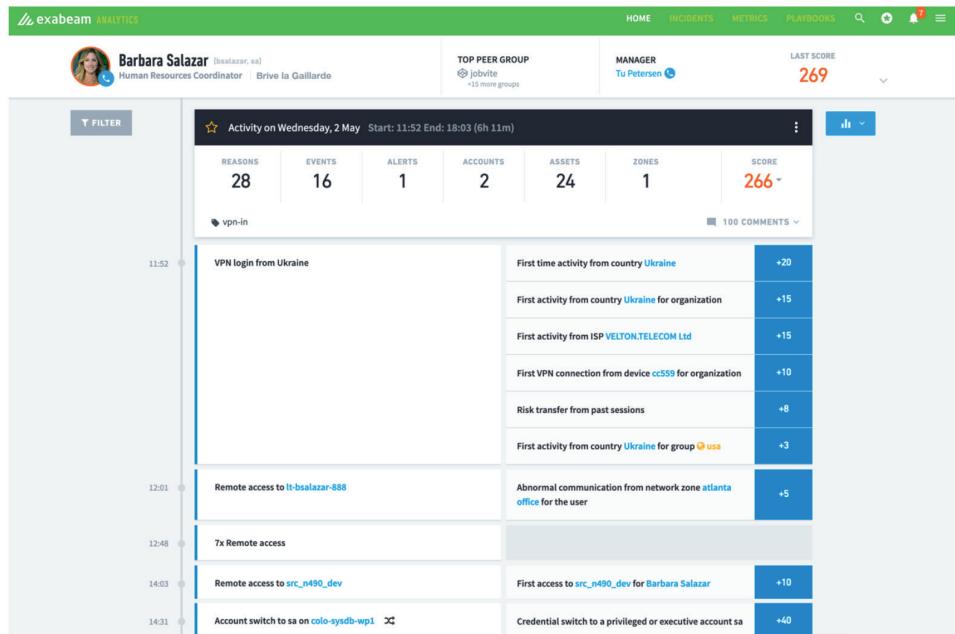
### Fonctionnalités :

- Modèle de « licencing » évolutif et prédictible, basé par utilisateur.
- Collecte simplifiée des données des solutions Cloud grâce aux Cloud Connectors (Office 365, Azure SFDC...).
- Analyse basée sur le comportement utilisateur afin de détecter les anomalies permettant d'identifier les problématiques complexes telles que les vulnérabilités de type "0-days" et les "credentials" compromis. Le moteur de gestion du risque permet aux analystes de se focaliser sur les utilisateurs et les machines les plus critiques.
- Correspondance automatique du compte utilisateur avec les IP qui lui sont associées afin de donner une vision compréhensible et complète de son activité (contexte utilisateur).
- Reconstitution des sessions utilisateurs avec toutes les actions pour augmenter la productivité des analystes en évitant des investigations longues et réduit le temps de réaction de la réponse aux attaques.
- Permet d'augmenter et d'améliorer les capacités des SIEMs existant en utilisant les fonctionnalités d'UBA d'EXABEAM.
- Réponse automatique aux incidents (SDAR).



### Marché cible :

- Clients équipés d'un SIEM classique ou data lake.
- Clients sans SIEM ou non satisfait du leur.
- Clients d'au moins 1 000 utilisateurs (ou à partir de 500 pour le Cloud uniquement).

The screenshot shows the exabeam Analytics interface. At the top, a green bar displays the exabeam logo and 'Analytics'. The top navigation bar includes 'HOME', 'INCIDENTS', 'METRICS', 'PLAYBOOKS', a search icon, a bell icon, and a user icon. The main area features a user profile for 'Barbara Salazar' (bsalazar, ssa) from 'Brive la Gaillarde'. It shows 'TOP PEER GROUP' (jobwite) with '+15 more groups', 'MANAGER' (Tu Petersen), and a 'LAST SCORE' of **269**. A 'FILTER' button is on the left. The main content area displays a timeline of activity from 11:52 to 14:31 on Wednesday, 2 May. The timeline shows various events such as 'VPN login from Ukraine', 'Remote access to lt-bsalazar-888', and 'Account switch to sa on colo-sysdb-wp1'. Each event is accompanied by a timestamp, a brief description, and a score. For example, the first event 'VPN login from Ukraine' has a score of +20. The interface also includes a '100 COMMENTS' link and a '⋮' button.

Reconstitution de tous les évènements associés aux utilisateurs au sein d'une session