



exabeam

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.



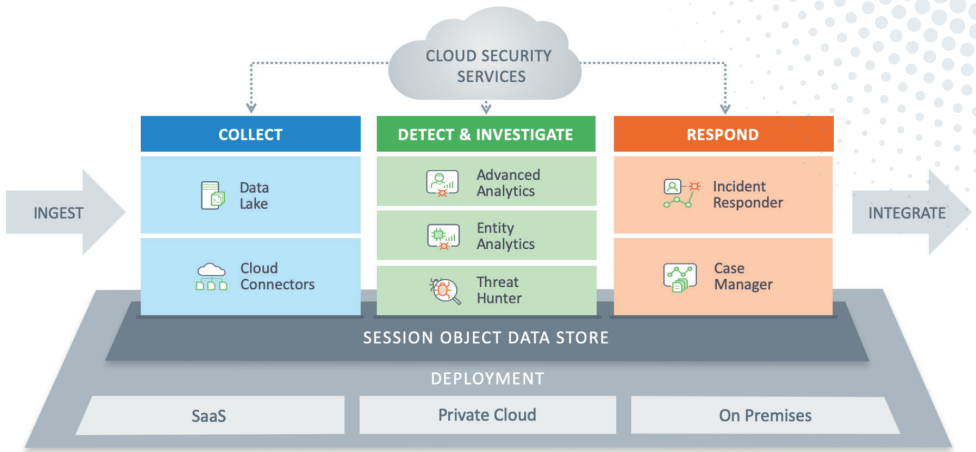
Fonctionnalités :

- 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 de 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, there's a navigation bar with 'HOME', 'INCIDENTS', 'METRICS', and 'PLAYBOOKS'. Below that, the user profile for 'Barbara Salazar' is shown, along with a 'TOP PEER GROUP' (jobvite) and a 'MANAGER' (Tu Petersen). A 'LAST SCORE' of 269 is displayed. The main content area shows a session titled 'Activity on Wednesday, 2 May' with a start time of 11:52 and an end time of 18:03. A summary table shows: REASONS: 28, EVENTS: 16, ALERTS: 1, ACCOUNTS: 2, ASSETS: 24, ZONES: 1, and SCORE: 266. Below this, a list of events is shown with their details and scores:

Time	Event Description	Score
11:52	VPN login from Ukraine	+20
	First time activity from country Ukraine	+20
	First activity from country Ukraine for organization	+15
	First activity from ISP VELTON-TELECOM Ltd	+15
	First VPN connection from device cc559 for organization	+10
	Risk transfer from past sessions	+8
	First activity from country Ukraine for group usa	+3
12:01	Remote access to li-basalzar-888	+5
	Abnormal communication from network zone atlanta office for the user	+5
12:48	Tx Remote access	
14:03	Remote access to src_n490_dev	+10
	First access to src_n490_dev for Barbara Salazar	+10
14:31	Account switch to sa on colo-sysdb-wp1	+40
	Credential switch to a privileged or executive account sa	+40

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