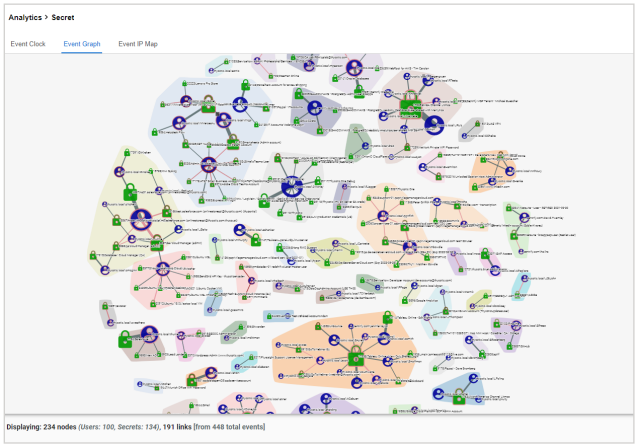
Privileged Behavior Analytics

Détecter des violations et vols de données avant qu'ils ne se produisent

Réduisez les risques de sécurité

Réduire les risques de sécurité menaçant votre organisation en améliorant la sécurité fera gagner du temps, de l'argent et des ressources à votre service tout en maximisant votre investissement actuel dans Secret Server et Privilege Manager.

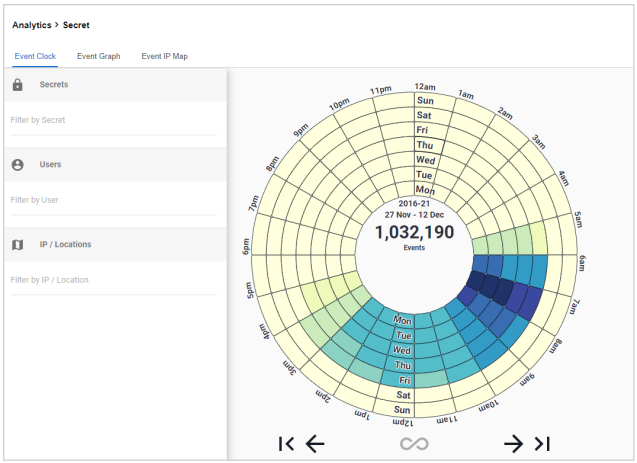
Privileged Behavior Analytics permet aux administrateurs IT et de sécurité de détecter rapidement les violations avant qu'elles ne se produisent, d'analyser la distribution des comptes à privilèges et leur accès au sein de votre organisation et d'ajouter un niveau de sécurité au déploiement de vos solutions Secret Server et Privilege Manager.



Détectez les premiers signes de violation

Un accès à 3h du matin à un compte à privilèges puissant est-il considéré comme un comportement approprié dans votre organisation ?

Le comportement soudainement inhabituel d'un utilisateur peut être le signe précoce d'une violation de données ou d'une menace d'initié. Privileged Behavior Analytics peut rapidement détecter les comportements anormaux et alerter instantanément votre équipe de sécurité d'une cyberattaque ou d'une menace interne avant que la violation de données ne se produise.



Priorisez les alertes les plus importantes

Comment pouvez-vous savoir quelle activité ou alerte de sécurité est la plus importante ?

Le machine learning et la reconnaissance des modèles de comportement permettent de hiérarchiser les activités de votre système, en vous alertant sur ce qui est le plus important. Soyez informé d'une activité suspecte au moment précis où elle se produit, afin de pouvoir agir rapidement. Triez vos alertes en fonction de leur score de menace afin de vous concentrer d'abord sur les alertes critiques.

Détecter des violations avant qu'elles ne se produisent

Selon Forrester, on estime que 80 % des violations impliquent des comptes à privilèges. Ces violations sont liées à des comptes à privilèges compromis ou atteints par des menaces internes. En plus de la protection de tous vos comptes à privilèges, il est important de suivre et d'analyser qui a accès à quels comptes ainsi que le moment et le type d'utilisation.

Privileged Behavior Analytics de Delinea vous aide à détecter une violation potentielle avant qu'elle ne se produise. Notre solution basée sur le cloud utilise la technologie de machine learning pour analyser les comportements d'utilisateurs privilégiés dans Secret Server, notre solution de gestion des accès privilèges, afin d'alerter rapidement votre équipe de sécurité en cas de comportement anormal, un signe précurseur d'abus ou de compromission.

Privileged Behavior Analytics et Secret Server, vous permettent d'analyser le comportement temporaire de vos utilisateurs et donc d'identifier rapidement tout activité inhabituelle. Privileged Behavior Analytics s'accompagne d'un « Secret Access Clock » qui permet aux équipes de sécurité d'analyser rapidement les comportements d'accès. Ces outils d'analyse peuvent être filtrés de manière plus détaillée pour visualiser un secret spécifique ou le comportement d'un utilisateur, sur une période donnée

Delinea se concentre sur le vecteur d'attaque le plus vulnérable – les comptes privilégiés. Avec Delinea, vous pouvez adopter une approche multicouche qui couvre vos besoins en matière de sécurité des privilèges des postes de travail aux informations d'identification, en assurant la protection à chaque étape.

Qui a accès à quels comptes ?

Avec Privileged Behavior Analytics,, vous pouvez voir une carte de vos comptes à privilèges et de tous les utilisateurs qui y ont accès. Les utilisateurs et secrets sont groupés dans des « Communautés » qui font office de mini-écosystèmes. Vous pouvez rapidement voir si un secret est limité à un groupe de personnes ou si des utilisateurs accèdent à des secrets qui sont dans d'autres services.

Quelles sont les alertes les plus importantes ?

Privileged Behavior Analytics s'appuie sur un comportement standard qui sert de référence pour les accès utilisateur. Ce standard est créé par plusieurs algorithmes de machine learning qui prennent en compte les comportements des utilisateurs selon les périodes, les accès, la sensibilité des informations d'identification et les comportements d'utilisateur similaires. Si un utilisateur dévie de cette référence, il reçoit, en fonction des algorithmes, un score de menace. Le système priorise ces scores de menace afin que vous puissiez d'abord vous concentrer sur ces alertes ayant le risque potentiel le plus élevé pour votre organisation.

Delinea

Delinea est un fournisseur majeur de solutions de gestion des accès à privilèges (PAM) pour les entreprises modernes et hybrides. Delinea Platform étend de manière intuitive les solutions PAM en fournissant des autorisations pour toutes les identités, en contrôlant l'accès à l'infrastructure cloud hybride la plus critique et aux données sensibles d'une entreprise pour aider à réduire les risques, à garantir la conformité et à simplifier la sécurité. Delinea supprime la complexité et définit les limites de l'accès pour des milliers de clients dans le monde. Nos clients vont des PME aux plus grandes institutions financières, agences de renseignement et sociétés du monde entier spécialisées dans les infrastructures critiques. **delinea.com/fr/**