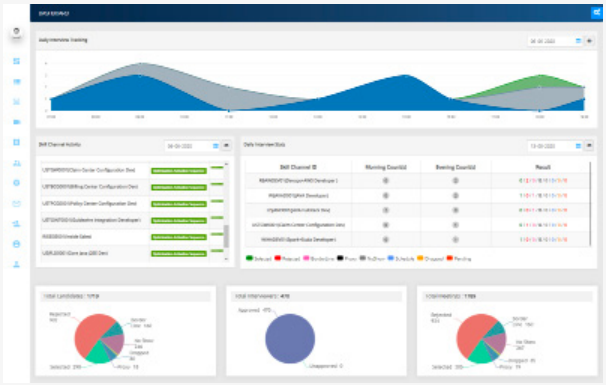
Privileged Behavior Analytics

Détecter des violations et vols de données avant qu'ils ne se produisent – grâce au cloud

Améliorez la sécurité et réduisez les risques

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.

Privileged Behavior Analytics permet aux administrateurs IT et de sécurité à détecter rapidement les violations avant qu'elles ne se produisent, d'analyser la distribution des comptes à privilèges et des accès à votre organisation et d'ajouter un niveau de sécurité au déploiement de votre solution Secret Server. Dégagez du temps pour vous concentrer sur la découverte, la gestion et la protection des informations d'identification de vos comptes à privilèges.



Lorem ipsum dolar caption

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 potentiellement 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 d'initié 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, sur l'analyse de la distribution des comptes à privilèges et des accès à votre organisation et l'ajout d'un niveau de sécurité au déploiement de votre solution Secret Server. Dégagez du temps pour vous concentrer sur la découverte, la gestion et la protection des informations d'identification de vos comptes à privilèges.

Détecter des violations avant qu'elles ne se produisent

Selon Forrester, on estime que 80 % des violations impliquent des comptes à privilèges. Certaines de 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 du machine learning pour analyser les comportements des utilisateurs privilégiés dans Secret Server, notre solution de gestion des comptes à privilèges, afin d'alerter rapidement votre équipe de sécurité en cas de comportement anormal, un signe précurseur d'abus ou de compromission.

Qui a accès à quels comptes ?

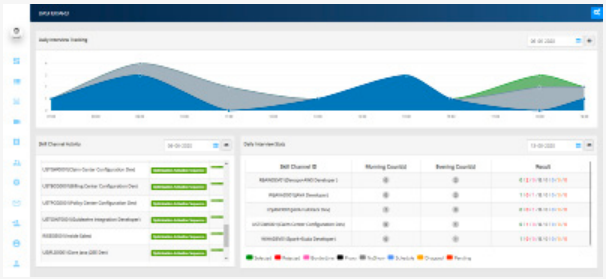
Avec Privileged Behavior Analytics vous pouvez rapidement voir une carte de vos comptes à privilèges et de tous les utilisateurs qui y ont accès. En outre, les utilisateurs et secrets sont groupés dans des « Communautés » qui font office de mini-écosystèmes. Vous pouvez rapidement voir si un secret est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

Y a-t-il des personnes accédant à des comptes à privilèges à 3h du matin ?

Privileged Behavior Analytics et Secret Server vous permettent d' analyser rapidement le comportement dans le temps de vos utilisateurs et donc d'identifier rapidement toute activité anormale à des heures inhabituelles. 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.

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.



Lorem ipsum dolar caption

Delinea

Delinea is torit essequi quam la doloriatecto volorem volum doluptas eveliquia quam ilicimo commoluptas erum labo. Temoluptas ut explat. Agnis magnam faccum sequaec tectotamenim il enectia sequaer oribusam faccull atiur. Nis et es coribusant et evelene ssitae poriae nihiliat fugitia necab iuntium aspelenistis dit pliquides alit odit fugiam di ut officia dipsaere volumqui cus. **delinea.com**