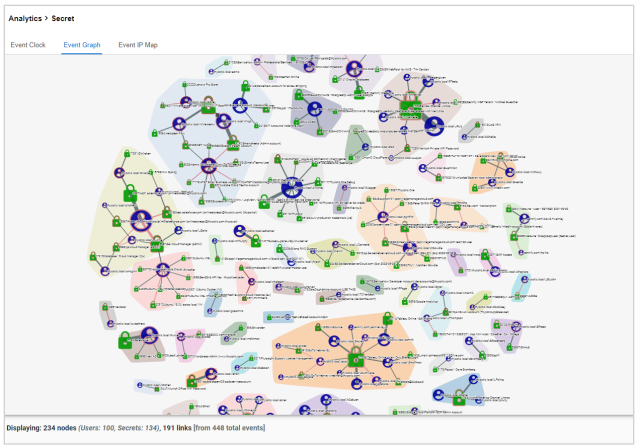
Privileged Behavior Analytics

Identificando violações e roubos de dados antes de acontecerem

Reduza riscos de segurança

A redução dos riscos na sua empresa por meio da melhoria da segurança vai ajudar a economizar tempo, dinheiro e recursos do seu departamento, além de maximizar seu investimento atual no Secret Server e no Privilege Manager.

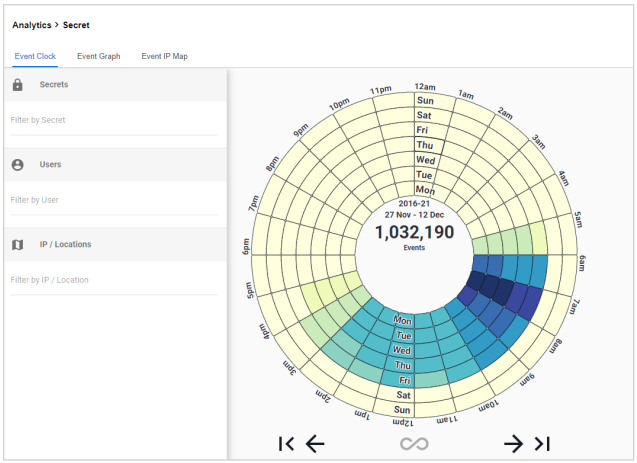
O Privileged Behavior Analytics permite que administradores de TI e de segurança detectem rapidamente violações antes delas acontecerem, analisem a distribuição e acesso de contas privilegiadas em toda a sua organização e adicionem uma camada de segurança à implementação do Secret Server e do Privilege Manager.



Identifique os primeiros sinais de uma invasão

O acesso a uma conta privilegiada às 3 da madrugada é um comportamento adequado na sua organização?

Um comportamento incomum e repentino de um usuário pode ser um sinal precoce de uma violação de dados ou de uma ameaça interna. O Privileged Behavior Analytics pode detectar rapidamente esse comportamento anormal e alertar imediatamente a sua equipe de segurança sobre um ataque cibernético ou um ameaça interna antes que a violação de dados aconteça.



Priorize os alertas que mais importam

Como você sabe qual alerta ou atividade de segurança deve ser tratado primeiro?

O aprendizado de máquina e o reconhecimento do padrão de comportamento ajudam a priorizar atividades no seu sistema, chamando atenção para o que é mais importante. Saiba o momento exato em que uma atividade suspeita está acontecendo para tomar medidas rapidamente. Classifique os alertas pela pontuação de ameaça e concentre-se nos alertas críticos primeiro.

Identificando violações antes de acontecerem

De acordo com a Forrester, estimam-se que 80% das violações envolvem contas privilegiadas. Essas violações acontecem quando contas privilegiadas são comprometidas ou quando as ameaças internas detêm sua propriedade. Além de proteger todas as suas contas privilegiadas, é crucial rastrear e analisar quem tem acesso a cada conta privilegiada, bem como quando e como elas estão sendo usadas.

O Privileged Behavior Analytics da Delinea ajuda você a detectar uma violação em potencial antes que ela aconteça. Nossa solução baseada na nuvem usa a tecnologia do aprendizado de máquina para analisar o comportamento privilegiado no Secret Server, nossa solução de Gerenciamento de Acesso Privilegiado, para alertar rapidamente a sua equipe de segurança sobre um comportamento anormal, uma indicação precoce de comprometimento ou um abuso.

Com o Privileged Behavior Analytics e o Secret Server, você pode analisar o comportamento temporal dos seus usuários, permitindo identificar rapidamente qualquer atividade incomum. O Privileged Behavior Analytics conta com o Secret Access Clock, um relógio de acesso secreto que permite que as equipes de segurança possam rapidamente analisar o comportamento de acesso. Essas ferramentas de análise podem ser ainda mais refinadas para visualizar um segredo ou um comportamento de usuário específico em um determinado intervalo de tempo.

A Delinea se concentra no vetor de ataque mais vulnerável: as contas privilegiadas. Com a Delinea, você pode adotar uma abordagem de múltiplas camadas que abrange suas necessidades de segurança de privilégios, de endpoints a credenciais, garantindo a proteção em todas as etapas.

Quem tem acesso a cada conta?

Com o Privileged Behavior Analytics, você pode ver um mapa das suas contas privilegiadas e todos os usuários que têm acesso a elas. Os usuários e segredos são agrupados em "Comunidades" que funcionam como pequenos ecossistemas. Assim, você pode rapidamente ver se um segredo está contido em um grupo de pessoas ou se usuários estão acessando segredos de outros departamentos.

Quais alertas são os mais importantes?

O Privileged Behavior Analytics usa um parâmetro comportamental para o acesso de usuário com base em algoritmos de aprendizado de máquina que observam o comportamento temporal, comportamento de acesso, confidencialidade de credenciais e outros comportamentos similares de usuário. Quando um usuário desvia desse parâmetro, dependendo dos algoritmos, eles recebem uma pontuação de ameaça. O sistema prioriza essas pontuações de ameaça para que você possa se concentrar primeiro nos alertas com maior risco de potencial para a sua empresa.

Delinea

Delinea é um fornecedor líder de soluções de Gerenciamento de Acesso Privilegiado (PAM) para a empresa moderna e híbrida. A Delinea Platform estende o PAM sem problemas, fornecendo autorização para todas as identidades, controlando o acesso à infraestrutura de nuvem híbrida mais crítica de uma organização e dados sensíveis para ajudar a reduzir riscos, garantir a conformidade e simplificar a segurança. O Delinea elimina a complexidade e define os limites de acesso para milhares de clientes em todo o mundo. Nossos clientes variam desde pequenas empresas até as maiores instituições financeiras, agências de inteligência e empresas de infra-estrutura crítica do mundo. **delinea.com/pt/**

 PBA-DS-0322-PT