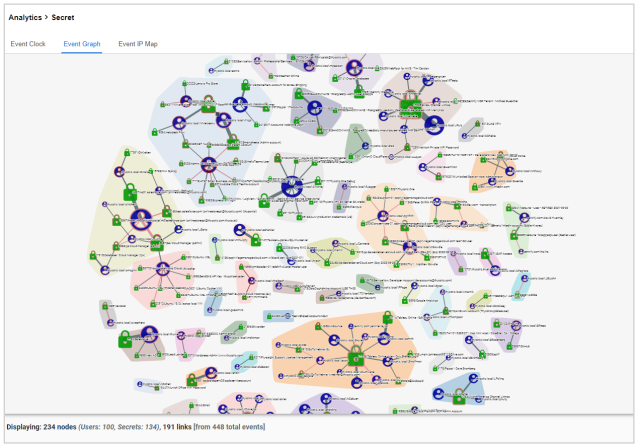
Privileged Behavior Analytics

Wykrywanie ataków „Account Take Over” na wczesnym etapie, zanim dojdzie do nieuprawnionego wykorzystania tych kont

Zmniejszanie zagrożeń

Zmniejszenie zagrożeń dla Twojej firmy lub instytucji dzięki lepszym zabezpieczeniom oszczędzi czas, pieniądze i zasoby Twojego działu oraz pozwoli maksymalnie wykorzystać inwestycję w Secret Server i Privilege Manager.

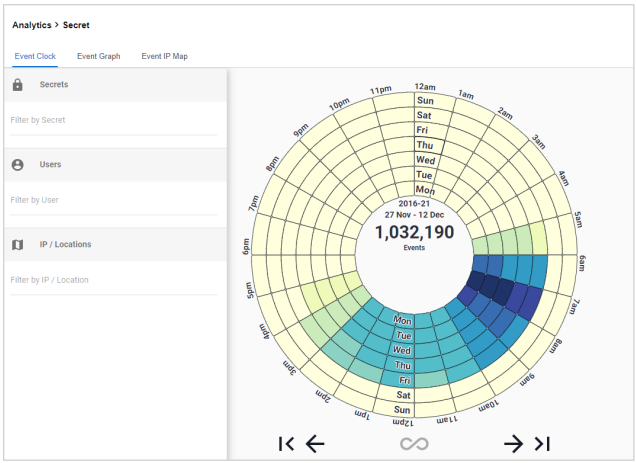
Korzystając z Privileged Behavior Analytics, administratorzy działu IT i bezpieczeństwa mogą szybko wykrywać włamania — jeszcze zanim do nich dojdzie, analizować rozkład kont z uprawnieniami i dostęp do nich w skali całej organizacji, a także dodatkowo zwiększyć bezpieczeństwo wdrożeń rozwiązań Secret Server i Privilege Manager.



Wykrywanie wczesnych symptomów włamań

Czy uzyskiwanie dostępu do konta o szerokich uprawnieniach o 3:00 rano jest typowe w Twojej firmie?

Nieoczekiwane i nietypowe zachowanie użytkownika może być wczesnym symptomem włamania lub zagrożenia wewnętrznego. Privileged Behavior Analytics może szybko wykrywać takie anomalie i błyskawicznie powiadamiać zespół ds. zabezpieczeń o możliwym cyberataku albo zagrożeniu wewnętrznym, zanim dojdzie do kradzieży danych.



Priorytet dla najważniejszych alertów

Jak wybrać ważne alerty lub działania, na których trzeba się skoncentrować w pierwszej kolejności?

W nadawaniu priorytetu aktywności w Twoim systemie pomoże uczenie maszynowe i analiza wzorców zachowań. Dzięki temu będziesz otrzymywać powiadomienia o tym, co najważniejsze. Dowiaduj się o podejrzanej aktywności na bieżąco, aby móc szybko zareagować. Sortuj powiadomienia na podstawie poziomów zagrożenia i koncentruj się w pierwszej kolejności na alertach krytycznych.

Wykrywanie włamań, zanim do nich dojdzie

Z szacunków firmy Forrester wynika, że do około 80% włamań dochodzi przy użyciu kont uprzywilejowanych. Do takich ataków dochodzi poprzez konta z przejętymi danymi logowania albo należących do przestępców działających wewnątrz naszej organizacji. Oprócz ochrony wszystkich kont z uprawnieniami trzeba koniecznie śledzić i analizować, kto ma dostęp do których kont oraz jak i kiedy są one używane.

Rozwiązanie Privileged Behavior Analytics firmy Delinea pomaga w wykrywaniu potencjalnych włamań, zanim do nich dojdzie. Nasze rozwiązanie chmurowe wykorzystuje uczenie maszynowe do analizy zachowań z uprawnieniami w ramach Secret Server — naszego produktu do zarządzania dostępem uprzywilejowanym. Dzięki temu może szybko powiadamiać Twój zespół ds. zabezpieczeń o nietypowych zachowaniach świadczących o naruszeniu zabezpieczeń lub nadużyciach.

Produkty Privileged Behavior Analytics oraz Secret Server umożliwiają analizę zachowania użytkowników w czasie oraz szybką identyfikację nietypowej aktywności. Privileged Behavior Analytics zawiera narzędzie Secret Access Clock dla zespołów ds. bezpieczeństwa, które umożliwia szybką analizę zachowań związanych z dostępem. Te narzędzia analityczne pozwalają na dogłębne filtrowanie w celu sprawdzenia wykorzystania klucza tajnego lub zachowań użytkownika w wybranym okresie.

Delinea koncentruje się na najwrażliwszym wektorze ataku — kontach uprzywilejowanych. Dzięki produktom firmy Delinea można stosować wielowarstwowe podejście zaspokajające potrzeby firmy w zakresie bezpieczeństwa uprawnień — od punktów końcowych po poświadczenia. W ten sposób można zapewnić sobie ochronę na każdym etapie.

Kto ma dostęp do których kont?

Privileged Behavior Analytics prezentuje mapę kont uprzywlejowanych oraz wszystkich użytkowników, którzy mają do nich dostęp. Użytkowników i klucze tajne grupuje się w „Społeczności" stanowiące miniaturowe ekosystemy. Dzięki temu można szybko sprawdzić, czy klucz tajny jest wykorzystywany tylko w określonej grupie osób, czy też użytkownicy uzyskują dostęp do kluczy tajnych przeznaczonych dla innych działów.

Które alerty są najważniejsze?

Privileged Behavior Analytics wykorzystuje analizę zachowań użytkownika wykorzystującą uczenie maszynowe w odniesieniu do zachowań chwilowych, metod dostępu, czułości poświadczeń i zachowań innych użytkowników danego systemu. Kiedy zachowanie użytkownika odbiega od punktu odniesienia, algorytmy określają poziom zagrożenia. System nadaje priorytet poziomom zagrożenia, więc w pierwszej kolejności można się skoncentrować na alertach o potencjalnie największym ryzyku dla organizacji.

Delinea

Delinea jest przodującym producentem rozwiązań do zarządzania dostępem uprzywilejowanym (PAM, privileged access management) dla nowoczesnych, hybrydowych przedsiębiorstw. Upraszczamy dostęp uprzywilejowany, podnosząc równocześnie poziom bezpieczeństwa, zapewniając zgodność z regulacjami prawnymi i minimalizujemy ryzyko. Delinea zapewnia bezpieczeństwo ponad 14 000 klientom z całego świata. Do grona naszych klientów należą największe na świecie instytucje finansowe, agencje wywiadowcze oraz firmy z branży infrastruktury o znaczeniu krytycznym. **delinea.com**