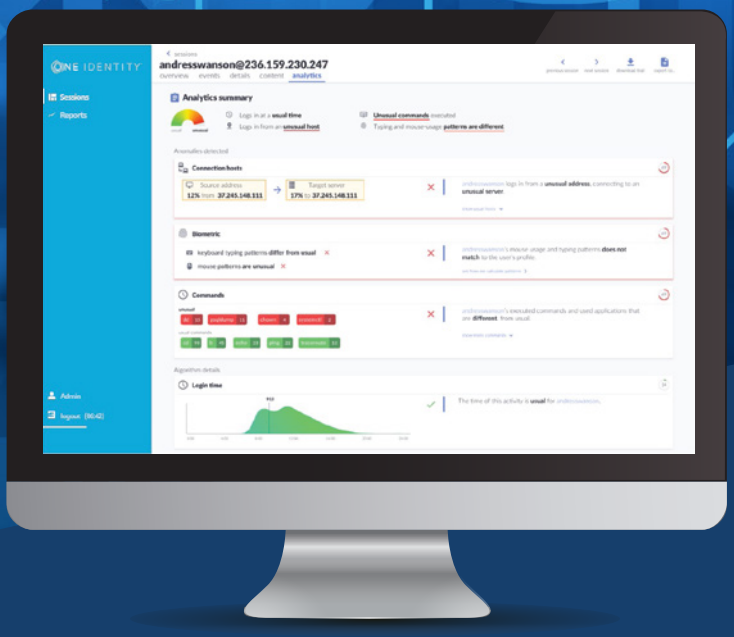
BALASYS



One Identity Safeguard for Privileged Analytics

Derítse fel és előzze meg a privilegizált felhasználókhoz köthető biztonsági incidenseket

Mint azt IT biztonsági szakértőként nyilván tudja, hogy a privilegizált felhasználókkal kapcsolatos incidensek rendkívül magas kockázatot jelentenek. Ma, a szervezeteknek átlagosan 206 napjába telik felderíteni egy incidenst. Ez az idő pénz – és kockázat. Így teljesen mindegy, hogy az incidenst egy feltört privilegizált felhasználói fiók, vagy egy rosszindulatú adminisztrátor okozta, minél tovább marad felderítetlen, annál több ideje marad a támadóknak arra, hogy megkeressék és ellopják az üzleti titkokat és bizalmas adatokat. Ezenfelül a büntetések és a vizsgálati költségek is magasabbak lesznek.

Önnek valószínűleg már kellett privilegizált hozzáférést adni a megbízható rendszergazdáin kívül másoknak is. Ez talán olyan külsős adminisztrátorokat, vagy tanácsadókat is magába foglalt, akik bárhol lehettek a világon. De hogyan lehet biztosítani, hogy az adminisztrátorok a privilegizált hozzáférésüket csak jóra használják?

A One Identity Safeguard for Privileged Analytics segítségével megtudhatja, hogy kik a legkockázatosabb felhasználói, folyamatosan szemmel tarthatja az új külső és belső fenyegetéseket, és észlelheti a privilegizált felhasználók szokatlan viselkedését. Ez az erőteljes megoldás teljes rálátást biztosít a privilegizált felhasználók tevékenységére, és – ha problémák merülnek fel – azonnali beavatkozásra is lehetőséget nyújt, így előnyös helyzetet teremt az adatvesztések megelőzéséhez.

ELŐNYÖK

- A felhasználói tevékenység folyamatos felügyeletével és megjelenítésével teljes rálátást biztosít IT környezetére.
- Folyamatos authentikációt nyújt a gépelés és az egérmozgás elemzésének segítségével.
- Gépi tanulással azonosítja a felhasználói profiltól való szokatlan eltéréseket.
- Csökkenti a biztonsági incidensek felderítéséhez szükséges időt a felvett munkamenetek kockázat alapú priorizálásával.
- Csökkenti a riasztások zaját, így Ön arra figyelhet, ami igazán fontos.
- Potenciálisan káros tevékenység észlelésekor megszakítja a kapcsolatot, ezzel javítva a biztonságot.

FUNKCIÓK

Kockázatos felhasználók azonosítása

A Privileged Analytics összeveti a felhasználói jogosultságokat a kockázati besorolással, és így azonosítja a magas kockázatú felhasználókat. Proaktív riasztásokat küld, amikor egy felhasználót magas kockázati státuszú jogosultsággal ruháznak fel. Ez megszünteti a szükségtelen vagy „alvó" jogosultságok kihasználásának kockázatát, mielőtt a támadók használnák ki.

Ismeretlen fenyegetések valós idejű felismerése

A szabályokon alapuló biztonsági eszközök nem képesek érzékelni az új, külső támadási formákat, vagy a rosszindulatú belsősöket. A Safeguard for Privileged Analytics valós időben követi és vizualizálja a felhasználói tevékenységet, így jobb rálátást biztosít arra, hogy mi is történik az Ön IT környezetében. Nem igényel előre meghatározott korrelációs szabályokat; egyszerűen a meglevő session adatokkal dolgozik.

Sémamentes működés

A Safeguard for Privileged Analytics az ismert támadási sémákkal való összevetés helyett az Ön IT környezetéből származó adatokra támaszkodik az „ismert rossz" viselkedés észleléséhez. Felhasználói profilt készít a „normális" viselkedésről, és különböző gépi tanulási mechanizmusok segítségével érzékeli a profiltól való eltéréseket.

Képernyőtartalom elemzés

A munkamenetek képernyő tartalmának elemzésével, és a kiadott parancsok és ablakcímek értelmezésével, a Safeguard for Privileged Analytics képes a privilegizált felhasználók viselkedési profilját tovább gazdagítani. Ez a finomhangolt elemzés segíti a tipikus viselkedés azonosítását, és a privilegizált felhasználói azonosító lopás felderítését.

Viselkedési biometriák

Minden felhasználó egy egyedi, csak rá jellemző viselkedési mintával rendelkezik, amikor olyan ismétlődő cselekvést végez, mint például az egérmozgatás vagy a gépelés. A Safeguard for Privileged Analytics-be beépített algoritmusok megvizsgálják ezeket a viselkedési jellemzőket is. A billentyűzet dinamika és az egérmozgás elemzés segít a támadások azonosításában, sőt folyamatosan, biometrikus módszerekkel hitelesíti a felhasználót.

Könnyen felismerheti a kockázatos felhasználókat és tevékenységeiket

Az analitikai dashboard felület segítségével Ön könnyen ellenőrizheti, hogy egy felhasználó tevékenysége szokatlan vagy kockázatos. A dashboard-on jól láthatók a szokatlan parancsok és biometrikus tevékenységek, valamint az elért rendszerek.

Alacsonyabb riasztási zaj

A Privileged Analytics csökkenti a SIEM-ek riasztási zaját az események kockázatalapú rangsorolásával és a legkockázatosabb események kiemelésével. A riasztások elküldhetők a SIEM-nek, de a biztonsági elemzők akár a termék intuitív felhasználói felületén is követhetik az események rangsorolt listáját, ami lehetővé teszi, hogy csak a legfontosabbakra fókuszáljanak.

Automatikus beavatkozás

A legtöbb támadásnál a tényleges károkozást egy hosszú felderítési fázis előz meg. Ebben a fázisban a gyors felderítés és a beavatkozás kritikus fontosságú, hogy megakadályozzuk a káros tevékenységet. Safeguard for Privileged Sessions lehetővé teszi a munkamenet automatikus megszakítását szokatlanul gyanús esemény vagy rosszindulatú viselkedés észlelésekor.

A One Identity-ről

A One Identity segít a cégeknek a jogosultság és hozzáférés-kezelést (Identity and Access Management, IAM) jól csinálni. Jogosultság szabályozást (identity governance), hozzáférés-kezelést, kiemelt-felhasználó kezelést és jogosultságot, mint szolgáltatást (identity as a service) tartalmazó egyedi termékportfóliója támogatja a szervezeteket üzleti lehetőségeik teljes kihasználásában, mindezt biztonsági béklyók nélkül, mégis védelmet nyújtva a fenyegetések ellen.

ONE IDENTITY™