Blindspotter

ÚJ GENERÁCIÓS MONITORING ESZKÖZ A FELHASZNÁLÓI VISELKEDÉSEK VALÓS IDEJŰ ELEMZÉSÉRE

„A felhasználó lett az új határpont"

Az informatika elmúlt években végbement változásainak (például felhő szolgáltatások, mobil eszközök elterjedése) köszönhetően egyre kevésbé léteznek a vállalati informatikai rendszereknek olyan határvonalai, amelyek egzaktul képesek elkülöníteni az azon belül, illetve kívül elhelyezkedő felhasználókat. Emellett azt is fontos megjegyezni, hogy a közelmúlt legnagyobb publicitást kapott biztonsági incidensei azok a nagy horderejű támadások voltak, amelyek gondos tervezést, előkészítést, és egy felhasználói hozzáférés megszerzését követően hosszú időn keresztül a támadók informatikai rendszerben való szabad mozgásával zajlottak (APT – Advanced Persistent Threat). A hálózaton belül lévő rosszindulatú felhasználók pedig komoly előnnyel rendelkeznek, ugyanis a vállalatok elsődleges védelmi rendszereit arra tervezték, hogy a külső támadások ellen védjenek, nem pedig a megbízhatónak vélt alkalmazottakkal szemben. A célzott támadások az IT sérülékenységek, a social engineering és a hagyományos bűncselekmények kombinációjára építenek azzal a céllal, hogy felhasználói hozzáféréseket szerezzenek meg. Mindez pedig az informatikai biztonság szempontjából jelentős paradigmaváltást hozott, ugyanis a klasszikus értelemben vett hálózati határpontok és az infrastruktúra helyett magát a felhasználót helyezi a védekezés középpontjába. A Blindspotter ezt a megközelítést, a felhasználó fókuszú IT biztonságot testesíti meg, a belső és külső felhasználók informatikai rendszerben végzett tevékenységére koncentrál.

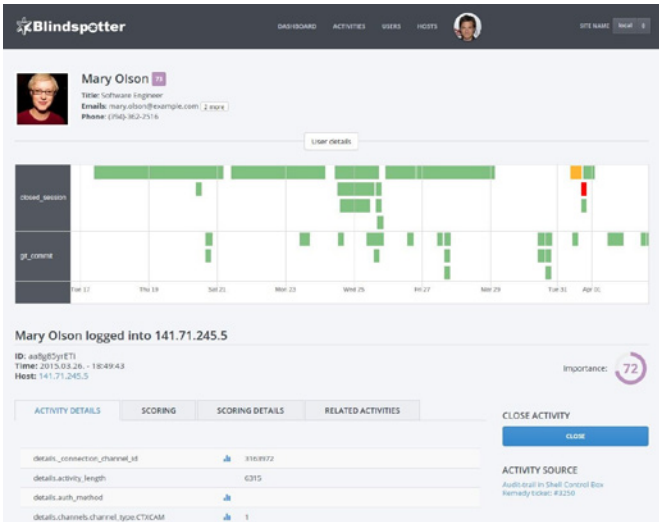
„Több monitoring, kevesebb kontroll"

A BalaBit egy 15 éves múlttal rendelkező magyar alapítású, IT biztonsági megoldásokat fejlesztő vállalat, mely a proxy technológiákra, a naplómenedzsment eszközökre és a kiemelt jogosultságú felhasználók monitorozására specializálódott. A Blindspotter a vállalat legújabb fejlesztése, egy új generációs monitoring eszköz, amely képes a felhasználók valamennyi aktivitását elemezni, és ezáltal az IT rendszerben előforduló gyanús eseményeket feltárni.

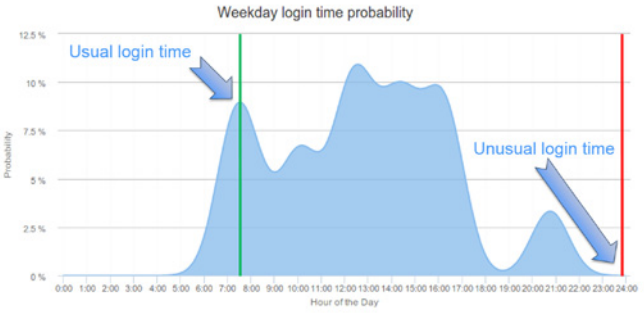
Az eszköz a megszokott, az egyes felhasználókra jellemző viselkedéstől való eltéréseket észleli, és ezekhez kockázati értékeket rendel, hozzásegítve ezzel a vállalatokat biztonsági erőforrásaik jobb optimalizálásához. Így a biztonsági osztályok az igazán fontos eseményekre fókuszálhatnak, és lehetővé válik a bevezetett ellenőrző jellegű intézkedések újratervezése és csökkentése az üzleti hatékonyság növelése érdekében. Az egyre több és több kontroll alapú biztonsági eszköz ugyanis folyamatos akadályokat gördít a munkavállalók útjába, ezzel a produktivitás mértékét jelentősen csökkenti, miközben a biztonsági szint érdemben nem javul.

A Blindspotter a biztonsági elemzések elsődleges információforrásául szolgáló sztenderd napló adatokat más forrásból származó, kontextuális információk széles skálájával integrálja, majd egyedi algoritmus készletével feldolgozza, és felhasználói profilokat generál, amelyeket gépi tanulás révén folyamatosan finomhangol. A felhasználói aktivitásokat ezt követően valós időben nyomon követi, és vizuálisan megjeleníti, ami lehetővé teszi az informatikai rendszerben zajló események egyszerűbb megértését. Az eszköz a kimeneti oldalon számos lehetőséget kínál a kockázatosnak vélt események grafikus felületen történő priorizált megjelenítésétől kezdve az automatikus beavatkozásig.

A Blindspotter egyik legnagyobb előnye, hogy nem igényel előre definiált korrelációs szabályokat, így folyamatos emberi beavatkozás nélkül is naprakész marad. A beépített algoritmusok testre szabható paraméterekkel rendelkeznek, amelyek lehetővé teszik az eredmények adatelemző kompetencia nélküli finomítását. A Blindspotter által használt algoritmusok az összes megszokott működéstől való eltérést azonosítják, melyeket egy grafikus irányítópulton rangsorolva jelennek meg. Lévén a teljes informatikai rendszert átfogóan monitorozza, segítségével az érzékeny, kritikus adatok integritását veszélyeztető potenciális biztonsági incidensek gyorsan feltárhatók és megakadályozhatók, legyen szó akár külső, akár belső elkövetőkről.



A Blindspotter teljes mértékben együttműködik és épít a syslog-ng naplómenedzsment eszköz által gyűjtött naplóüzenetekre, valamint a Shell Control Box monitoring eszköz képességeire, mely a felhasználói aktivitások teljes rögzítésén keresztül segíti elő a felhasználói profilok megalkotását. Ennek a két eszköznek a segítségével a Blindspotter a felhasználói aktivitások mélyebb megértését teszi lehetővé, mint bármely más, a piacon elérhető felhasználói viselkedéselemző (UBA – User Behavior Analytics) megoldás. Így a BalaBit egy rendkívül átfogó biztonsági elemző portfólióval képes védelmezni ügyfelei érzékeny adatait.



A legfontosabb előnyök

- A biztonsági incidensek valószínűségének és hatásának csökkentése
- A gyanús események felismerése és az ismeretlen fenyegetések azonosítása
- A biztonsági csapat hatékonyságának növelése
- Az üzleti hatékonyság növelése az alacsonyabb kontroll mellett megvalósított magasabb biztonsági szint révén

Felhasználási területek

A kompromittálódott felhasználói hozzáférések azonosítása

A Blindspotter képes a potenciális biztonsági incidensek bekövetkezésének valószínűségét és hatását csökkenteni, hatékony védelmet biztosítani az APT támadások ellen. Az ellopott felhasználói hozzáférésekkel visszaélő támadók viselkedése különbözik a valódi felhasználókétól, a Blindspotter pedig ezeket az eltéréseket ismeri fel. Ha ez egy bizonyos szintet meghalad, riasztást küld a biztonsági központba az esemény kivizsgálása érdekében. A gyanús események a jogosult felhasználó által egyszerűen jóváhagyhatók, így drámaian felgyorsul a felderítés, és csökken a téves riasztások kivizsgálására szánt idő.

A kiemelt jogosultságokkal való visszaélések feltárása

A Blindspotter segítségével nagymértékben csökkenthető a kiemelt jogosultságokkal való visszaélések száma. Amikor egy valódi munkavállaló követ el visszaélést, viselkedése szintén eltér a megszokott napi rutintól. Ha például egy felmondás alatt álló munkavállaló szeretne vállalati adatokat ellopni, a Blindspotter képes felismerni ezt a nem szokványos tevékenységet, és riasztani a biztonsági osztályt az esemény további kivizsgálása érdekében. Így a kiemelt jogosultságokkal végrehajtott adatlopások és más visszaélések is megelőzhetőek.

SIEM eszközök hatáskörének és felderítési képességének optimalizálása

A biztonsági osztály működési hatékonysága növelhető azáltal, hogy rálátást nyernek az eddig rejtve maradt aktivitásokra. Míg a SIEM-ek többsége a betörési kísérletekre, hibás bejelentkezésekre koncentrál, addig a Blindspotter a sikeresekre. Amíg a SIEM-ek többsége előre definiált szabályokat használ a már ismert incidensek azonosítására, addig a Blindspotter az alkalmazások naplóinak és más forrásokból származó információknak az elemzését végzi, annak érdekében, hogy anomáliákat és gyanús eseményeket találjon, így adva lehetőséget olyan incidensek felfedezésére is, amelyekre nem léteznek még definiált szabályok.

Az emberi és az automatizált tevékenységek egymástól való megkülönböztetése

A rendszer hozzáférések emberi használata, a személyes hozzáférések szkript vagy program által való használata és a megosztott hozzáférések egyaránt komoly biztonsági, beavatkozást igénylő problémát jelentenek a vállalat számára. Ha egy támadó megtalálja a módját, hogy megszerezze egy rendszer hozzáférést használó szkriptben tárolt felhasználói adatokat, akkor képes lesz minden rendszerhez hozzáférni, amihez a szkriptnek jogosultsága volt. A Blindspotter különbséget tud tenni az emberi és a gépi aktivitások között, és ennek észlelése esetén riasztani a biztonsági osztályt, mielőtt a visszaélés bekövetkezik.

Támogatja a biztonsági döntéseket azáltal, hogy megmutatja, miként használják az adminisztrátorok a rendszert

A nagy szervezeteknél komoly problémát jelent az a jelenség, mely során a felhasználók, különösen az informatikai osztályon dolgozók és a vezetők egyre több és több jogosultságot kapnak az újabb és újabb feladatok elvégzéséhez – ez biztonsági problémához vezethet. A Blindspotter áttekintést nyújt arról, hogy miként használják a különböző szolgáltatásokat a vállalatnál, és milyen jogosultságokkal kellene az egyes felhasználóknak rendelkeznie.

További információért látogassa meg a termék weboldalát. https://www.balabit.com/blindspotter