DARKTRACE

Darktrace és SIEM

Kiegészíti vagy kivált egy SIEM rendszert?

DARKTRACE

Miben különbözik a Darktrace és egy SIEM?

Míg a SIEM a különböző preventív biztonsági rendszerek és naplófájlok adatainak aggregációjával keres veszélyeket, a Darktrace öntanuló rendszere az ismeretlen, ezért nem kereshető, a SIEM számára sokszor teljesen láthatatlan veszélyeket is felfedi. A Darktrace így jelentős űrt foltozhat be a SIEM működésében, vagy önmagában telepítve azonnali, valós idejű kibervédelmi központot nyújt egy időigényes és költségesebb SIEM bevezetés helyett.

A SIEM (Security Information and Event Management) megoldások működésének alapját a biztonsági adatok és naplók aggregációja jelenti. A SIEM-ek számos elérhető adatforrásból egyesítik a biztonsággal kapcsolatos információkat: a szerverektől a munkaállomásokon át a különböző hálózati eszközökig minden rendszer biztonsági felügyeletét egyetlen helyen összpontosítják. Sok SIEM biztosít a gyors áttekinthetőségért és a riasztások egy helyen történő kezeléséért vezérlőpultokat, valamint vizualizációval, grafikonokkal szemlélteti a biztonsági állapotot. Ezen felül a SIEM-ek általában hosszú időre képesek megőrizni a biztonsági adatokat és naplókat, így utólagos lehetőséget adnak egy incidens kivizsgálására.

A SIEM rendszerek tipikusan a bázist, a kiindulópontot alkotják a biztonsági üzemeltetés számára, ahol az összes biztonsági rendszer minden riasztása egyetlen helyről felügyelhetővé válik. Az üzemeltetői csapatok számára a SIEM riasztásokat is tud küldeni – emailben, mobil eszközön vagy a vezérlőpultokon keresztül – így a biztonsági felelősök a riasztások vizsgálatával megtehetik a szükséges válaszlépéseket. Ezért egy komplex kibervédelmi rendszer naplóinak és biztonsági adatainak rendszerezett feldolgozására ideális megoldást nyújt a SIEM.

Egy SIEM jó működését a releváns riasztások adják, amelyekre időben tud reagálni a biztonsági üzemeltetés és meg tudja akadályozni a nagyobb károkat. Sok riasztással, nagy zajjal vagy túl késő detekcióval elveszhet a SIEM legfontosabb értéke. A SIEM rendszerek riasztási képességeit az alábbi három megközelítés kombinációja adja:

1. Külső forrásból származó támadásminták korrelációja az összegyűjtött adatokkal és támadás-szignatúrák keresése
2. Saját, komplex keresések és korrelációs szabályok létrehozása, amely rávilágít egy speciális támadásra vagy megfelelőségbeni hiányosságra
3. Más preventív eszközök (szintén tipikusan támadási szignatúra vagy szabály-alapú) riasztásainak kiértékelése

Ez a három megközelítés viszont súlyos rést hagy az ismeretlen, mintával nem azonosítható támadásokkal, amelyek átcsúsznak a preventív védelmi rendszereken és egyúttal elkerülik a SIEM figyelmét.

A Darktrace teljesen új működési elvével pontosan ezt az űrt képes betölteni. Ahelyett, hogy naplókat elemezne, a Darktrace a teljes hálózati forgalmat feldolgozza, minden egyes felhasználó és eszköz tevékenységét valós időben érzékeli és megtanulja a komplex, folyamatosan változó kapcsolatokat közöttük. Mivel a Darktrace képes megtanulni és azonosítani a normális, hétköznapi, munkával kapcsolatos viselkedést, így meg tudja különböztetni és valós időben felismeri a

legújabb, még nem látott támadásformákat, amelyek sikeresen átjutnak a preventív védelmi rendszereken.

A Darktrace leváltja a SIEM-eket?

Mivel a SIEM rendszerek és a Darktrace működése alapjaiban eltérő, ezért a „leváltás" nem a legalkalmasabb kifejezés. A Darktrace együtt tud működni a SIEM megoldásokkal és sokkal pontosabbá, megbízhatóbbá tudja tenni őket.

Ugyanakkor azon szervezetek, akik nem rendelkeznek még SIEM megoldással és nem szükséges számunkra akár több száz gigabájtnyi régi naplófájlt egy adatbázisban aggregálni, a Darktrace megközelítését sokszor hatékonyabbnak találják a biztonsági kockázatok azonnali kezelésére és valós idejű támadás-észlelésre. A Darktrace ezért alkalmas az erőforrás-igényes, komplex és hosszú bevezetési idővel járó SIEM projektek kiváltására.

Hogy működik együtt a Darktrace SIEM rendszerekkel?

A Darktrace minden népszerű SIEM megoldással együttműködik, amelyek támogatják az ipari szabványnak számító Common Event Format (CEF) és Log Event Extended Format (LEEF) adatformátumokat (például a Splunk, QRadar, ArcSight, McAfee vagy LogRhythm).

A Darktrace jelentések és riasztások a SIEM vezérlőpultokon is könnyen láthatóvá tehetők és vizualizálhatók, így minden új támadásról közvetlen SIEM értesítés küldhető.

Így a Darktrace riasztásokkal a megszokott módon, az eddigi üzleti folyamatok és kezelői lépések betartásával tud foglalkozni a SIEM üzemeltető csapat. Míg a SIEM korrelációkat keres a beérkezett adatokban az ismert támadásminták, külső adatforrások alapján, addig a Darktrace a támadások sokkal szélesebb körét képes azonosítani (legyen szó akár belső, akár külső veszélyekről), működése pedig nem függ külső szignatúráktól vagy frissítésektől.

Egyetlen SIEM-ben sem lehet anélkül keresni, hogy tudnánk pontosan mit keresünk. A Darktrace pontosan erre képes, megmutatja, hogy mi az a támadás amiről nem tudunk.

Konklúzió

A SIEM termékek megoldást nyújtanak a biztonsági rendszerek egyetlen helyen történő kezelésére, és a biztonsággal kapcsolatos adatok korrelációjára. Ugyanakkor egy SIEM a működési elvéből adódóan képtelen az új, ismeretlen, hálózati forgalomban és zajban elrejtőző, a biztonsági rendszereket megkerülő támadások és belső veszélyek azonosítására. Mivel egy ismeretlen támadásra a SIEM összes adata között sem lehet keresni, a Darktrace ezt az űrt tudja betölteni a biztonsági felügyeletben.

Hogy egy szervezet SIEM rendszer bevezetése mellett dönt, az elsősorban saját preferencia kérdése és függhet attól, hogy mennyire komplex a védelem, illetve szeretnék-e a naplófájlok feldolgozására alapozni a kibervédelmet. A veszélyek valós idejű azonosítására, azonnali reakciók elősegítésére ugyanakkor az elsődleges védelmet egy SIEM-jellegű megoldás helyett sokkal inkább egy hálózati „immunrendszer" szemléletű, a teljes hálózati forgalmat valós időben kiértékelő és riasztási zaj illetve tévedések nélkül feldolgozó, az abnormális működést azonnal azonosító rendszernek kell alkotnia.

További információ
www.darktrace.com

Hazai képviselet
és disztribúció
www.yellowcube.eu

A Darktraceről

A 2013-ban matematikusok és ex-kormányzati, titkosszolgálati kiberbiztonsági szakértők által alapított, cambridge-i székhelyű Darktrace a világ egyik leggyorsabban növekvő IT biztonsági vállalata. Egyedülálló öntanuló hálózati kibervédelmi rendszert fejleszt elsősorban energetikai, pénzügyi, telekommunikációs szektorbeli, kormányzati, katonai és kritikus infrastruktúrákat üzemeltető ügyfelei számára. A vállalat székhelye Cambridge és San Francisco, globális irodái New York, Auckland, London, Milán, Mumbai, Párizs, Szöul, Szingapúr, Sydney, Tokió, Toronto és Washington D.C. városaiban találhatók.