DARKTRACE

Cyber Intelligence

Hatékony védelem az ismeretlen ellen

DARKTRACE

Vezetői áttekintés

A Darktrace kiberintelligencia rendszere megteremti az ismeretlen, még felfedezetlen támadások elleni védelem lehetőségét. A rendszer gépi tanulás útján a támadásokkal járó elkerülhetetlen rendellenességek felfedezését biztosítja: amikor egy sikeres külső vagy belső támadás megváltoztat egy normál viselkedésmintát, ezt a Darktrace rögtön azonosítja. A hatékony kiberintelligencia segítségével a külső támadók és a belsős segítők több hónapos észrevétlen káros tevékenysége percek alatt azonosítható, még mielőtt érdemi kárt okozhatnának a megtámadott hálózatban.

Nincs áthatolhatatlan védelem

Száz százalékos kibervédelmet megvalósítani a mai komplex IT környezetben gyakorlatilag kivitelezhetetlen, ebben évek óta egyetért az IT biztonsági szakma. Már régóta az sem kérdés, hogy egy adott védelem áthatolható-e egyáltalán, csak az, hogy mennyi idő alatt, illetve hogy tudomást szerzünk-e a sikeres támadásról.

Míg a tűzfalak, a vírusvédelmi rendszerek, a sebezhetőség-menedzsment vagy épp egy fejlett végpontvédelem alapvető fontosságú a többrétegű biztonsági rendszer szemléletében, egyetlen gyártó sem vállal garanciát áthatolhatatlan védelemre. A valódi kérdést inkább az jelenti, hogyan készülhetünk fel az összes védelmi rendszeren sikeresen átjutó támadásra, és hogyan hatástalaníthatjuk időben, minimalizáljuk az okozott kárt.

„A hálózati ökoszisztéma sebezhetőségeire és fenyegetéseire való folyamatos betekintés segít felkészülni és tervezni olyan kockázatok kezelésére, amelyek a kevésbé tájékozottaknak fel sem tűnhet." **PWC**

A reakcióra és szignatúrákra alapuló védelmi rendszerek évtizedek óta támadási adatbázis frissítéseken keresztül megbízhatóan védenek a máshol már azonosított kártevők és támadásminták ellen. Viszont szükséges velejárójuk, hogy célzott, egyedi és korábban sehol nem látott támadásokat egyáltalán nem tudnak kezelni.

Ráadásul a támadások nem mindig járnak azonosítható kártevőkkel vagy támadásmintákkal; gondoljunk például egy ellopott jelszóra, vagy egy korrupt belsős segítőre. A helyes jelszót minden behatolásvédelmi rendszer átengedi, míg a belső, megfelelő jogosultságok tulajdonában történő szándékos károkozás teljes mértékben a védelmi rendszerek engedélye mellett történhet.

Adatvédelem vagy rugalmasság?

A modern vállalatok és közintézmények lételeme az adat, amely összekötött, egyre komplexebb hálózatokon keresztül utazik különféle szolgáltatások, felhők és adatbázisok között. A felhasználók, beszállítók és ügyfelek között folyamatosan mozgó adatok átfogó védelme minden IT biztonsági felelős alapvető kihívása.

Üzleti adatai mellett számos vállalat legfontosabb erőforrását az alkalmazottai adják, viszont a legnagyobb veszélyt is ők jelentik a kezelt adatokra: egy önállóan végzett csalássorozat vagy külső segítőkkel való együttműködés beláthatatlan kárt okozhat.

Az új fenyegetések láttán sok esetben logikus óvintézkedésnek tűnhet még szigorúbb szabályozás, még granulárisabb adatvédelem és még több korlát, ellenőrzőpont bevezetése, viszont ez sok oldalról ütközhet komoly ellenállásba.

A modern IT biztonsági felelős igazi kihívását ezért egy olyan kibervédelmi rendszer megalkotása jelenti, amely nem korlátozza a vállalatot a fejlődésben, nem jár versenyhátránnyal és az IT biztonság folyamatos fejlesztése nem ütközik újabb ellenállásokba.

Valós idejű, az incidensek konkrét és gyors megoldását jól támogató kiberintelligencia nélkül pedig ez a cél gyakorlatilag elérhetetlen.

Túl kevés, túl későn

A kibertámadások napjainkban folyamatosan a vezető hírek között szerepelnek, hétről hétre történik újabb adatlopás és derül fény sikeres támadásokra. Az érintett vállalatok reakciója, a támadás szükségszerű kivizsgálása és a felelősségre vonás általában tipikusan „túl kevés, túl késő" ahhoz, hogy visszaszerezze az elveszített bizalmat, míg az okozott kárt sem fogja jóvátenni.

Ráadásul a támadások a kiberbűnözés fejlődésével egyre egyszerűbbé és könnyebbé válnak. Komplett alvilági szolgáltatások vásárolhatók meg egyedi kártevők létrehozására és laborokban való tesztelésére, míg a cél hálózatokba való bejutást a sebezhetőségek és támadások adás-vételét biztosító, virágzó feketepiac egyszerűsíti. Megfelelő erőforrásokkal vagy pénzzel egyre több bűnöző vagy akár állami hírszerző készíthet el tesztelt, védelmeken áthatoló kártevőt, amely jó alapot biztosít a fejlett, célzott kibertámadások végrehajtásához.

Ezért a célhálózatba való behatolás mára egyszerű feladattá vált, a további károkozás pedig csak a támadók kreativitásától és valódi céljaitól függ. A lassú, fokozatos felderítés és támadás jó eséllyel elveszik a hálózat „zajában". Ha egy-egy naplósor készül is a tevékenységéről, a nagy forgalom és a sok hibajelzés miatt nem valószínű, hogy lebuktatja a támadót. Ráadásul amíg a biztonsági felelős napi feladatai mellett, leterhelten próbája felügyelni a hálózatot és kivizsgálni a riasztásokat, a támadó minden idejét felhasználhatja adatgyűjtésre, megfigyelésre, a védelem kijátszására és a következő lépés pontos megtervezésére.

Sajnos a statisztika is szomorú képet fest: egy külső fejlett kibertámadás felfedezése átlagosan 170 nap, míg egy belső segítővel történő célzott károkozás átlagosan 259 napig marad felfedezetlen.

Mindezek ellenére a veszélyt sokan csak az utolsó pillanatban hajlandók tudomásul venni, amikor az okozott kár már észrevehető, vagy egy rendszerleállásban érezhető. Ilyenkor elindul a „tűzoltás" és a kapkodás a kár minimalizálásra; a támadás minél gyorsabb elhárítására. Minden egyes különböző kibertámadásra előre felkészülni viszont a folyamatosan változó IT környezetben gyakorlatilag lehetetlen.

Ugyanakkor még bőven lenne idő, akár több hónap is a veszélyes támadásokat hatástalanítani és a kezdeti stádiumban, bármi nemű okozott kár nélkül elhárítani. Pontosan erre szolgál a Darktrace: valódi eszközt ad a biztonsági üzemeltetők kezébe a támadások időben történő azonosítására és elhárítására.

Mesterséges intelligenciával az ismeretlen támadások ellen

A Darktrace működéséből adódóan teljes láthatóságot biztosít minden hálózati adatmozgás felett. Minél „többet lát" a rendszer, annál jobban tud döntéseket támogatni, és annál tisztább összefüggésekkel tudja felfedezni a kibertámadások szükséges előkészületeit.

A fejlett matematikai modelleken, gépi tanuláson alapuló megközelítéssel a Darktrace folyamatosan figyeli a hálózat működését, és modellezi (vagyis megtanulja) az egyes emberek, eszközök és alhálózatok viselkedését. Amikor ez a megfigyelt viselkedés bármilyen okból is megváltozik, a Darktrace rögtön riaszt. Megbízhatóvá úgy válik, hogy a dinamikusan formálódó környezetet naprakészen követi és adaptálódik a környezet változásaihoz. A gépi tanulás alapú matematikai modellezés pontosan ezt biztosítja a Darktrace számára, így az óriási rendelkezésre álló adatmennyiségben megbízhatóan azonosítja a valódi viselkedés anomáliákat.

„A jó kiberbiztonságnak nem csupán egy nagyon erős külső falról, hanem egyfajta belső immunrendszerről kell szólnia."

Sir Jonathan Evans, ex-főigazgató, MI5

Szemben a hagyományos támadásminta és riasztás alapú biztonsági rendszerekkel, a jövőben naprakész és hatékony kiberbiztonsági információkat csak olyan rendszer tud biztosítani, amely öntanulással, valószínűségek folyamatos elemzésével és a változó környezethez való adaptációval képes a több ezer riasztás helyett a kevés valódi anomáliára fókuszálni.

A Darktrace használatával sikeresen megtisztítható a biztonsági riasztások keltette egyre nagyobb zaj,

és a biztonsági üzemeltetés minden emberi erőforrással a valódi anomáliákra koncentrálhat. Ráadásul a Darktrace sosem téved: minden jelzett viselkedésminta-változás valódi, bizonyított és visszajátszható; mindössze az anomália biztonsági jelentőségét és a következő lépéseket szükséges mérlegelni.

A Darktrace működése

Technikailag a Darktrace egyszerűen működik: a tükrözött hálózati forgalmat elemzi, ezért nem befolyásolja a hálózat működését.

A Darktrace hasonlítható egy teljes épületet behálózó, majd a látottakat automatikusan elemző és riasztó kamerarendszerhez. Ez egyáltalán nem befolyásolja a végzett munkát, viszont teljes láthatóságot nyújt a biztonsági szolgálat számára. A Darktrace által azonosított viselkedés-anomáliák a kamerák felvételeihez hasonlóan visszajátszhatók, így lépésről-lépésre kielemezhető minden incidens.

A Darktrace telepítése általában nem vesz igénybe egyetlen óránál többet. Ezt követően a rendszer rögtön nekiáll a védett hálózat működését elemezni és a matematikai modelleket felépíteni. Mindössze egy hét elegendő az első anomáliák azonosításához, három héten belül pedig a Darktrace készen áll a mindennapi, valós-idejű felügyelet biztosítására. A rendszer ezt követően is folyamatosan, napról napra tanul és adaptálódik.

Az IT biztonsági rendszerek között

Működéséből adódóan a Darktrace nem helyettesít más IT biztonsági rendszert, a határvédelem, végpontvédelem és különböző felügyeleti megoldások nem veszítik el létjogosultságukat. A Darktrace kizárólag azokkal a támadásokkal foglalkozik, amelyek sikeresen átlépnek a kiépített védelmen, és lehetővé teszik a támadók hosszú, észrevétlen adatgyűjtését és felkészülését egy veszélyesebb műveletre.

A Darktrace ilyen szempontból nem illeszkedik a hagyományos hálózatbiztonsági megközelítésbe, inkább az összes jövőbeni veszélyre és felfedezetlen támadásra készíti fel a biztonsági üzemeltetést.

A Darktrace a kiberbiztonság logikus következő állomása: hatékony, öntanuló megoldást biztosít, hogy ne utólag vizsgáljunk ki kritikus incidenseket, hanem még időben azonosítsuk a külső és belső veszélyeket a kompromittált eszközök és felhasználók legapróbb viselkedés-változásából. Így időben hatástalaníthatók a veszélyek, mielőtt azok lavinaszerűen IT biztonsági katasztrófába torkollnának.

Cyber intelligence vs. Threat intelligence

‚Threat intelligence' névvel hivatkozunk az ismert támadási adatok megosztására, legyen szó például folyamatosan frissülő kártevő adatbázisokról, adathalász honlapcímekről vagy aktívan kihasznált sebezhetőségekről. A naprakész ‚threat intelligence' segít megvédeni bennünket az ismert veszélyektől, de működéséhez elengedhetetlen, hogy legalább egyszer a támadás a világon valahol sikeres legyen, és legalább egy vállalatnál kárt okozzon. Számukra ugyanakkor kevés nyugodalmat ad, hogy ők lehettek az elsők, akik a többieket felkészítették az új támadásra.

A ‚threat intelligence' működésének alapvető problémája tehát, hogy a múlt támadásai nem feltétlenül készítenek fel a jövő veszélyeire. Az is csupán feltételezés, hogy ugyanaz a támadásminta megismétlődik. Ráadásul amíg egy minta bekerül egy adatbázisba, addig a szervezet biztosan ki van téve az adott támadásnak, amit akár ki is használhattak. Legrosszabb szempontból a ‚threat intelligence' csak egy óriási adathalmaz, ami a múltbeli támadásoktól próbál megvédeni, de semmit nem ér a jövőre nézve.

Ugyanakkor a hatékony védelemhez testre szabott, az adott szervezet működéséhez frissen alkalmazkodó, naprakész kiberbiztonsági információ szükséges. Ezt jelenti a ‚cyber intelligence': olyan biztonsági szempontból hasznos, a Darktrace által valós időben nyújtott információ, ami alapján a biztonsági felelősök meghozhatják a szükséges döntéseket. A jó kiberintelligencia ráadásul azonnal átfogó, a környezethez alkalmazkodó képet nyújt egy adott folyamatban lévő fenyegetésről, ami alapján a szükséges beavatkozás gyorsan és szakszerűen megtörténhet.

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.