VECTRA®
Security that thinks®

A VECTRA® A VILÁG VEZETŐ MESTERSÉGES INTELLIGENCIÁJÁT FEJLESZTI

a kibertámadások valós idejű detektálására és azonnali reakció biztosítására

A Vectra Cognito™ mesterséges intelligencia minden szervezetet képes ellátni azonnali, automatizált hálózati támadás detekció képességével, ráadásul bármilyen előzetes veszély információ/adatbázis nélkül. Így a kibertámadások késlekedés nélkül, valós időben hatástalaníthatók, mielőtt kárt okoznának – akár a felhőben, adatközpontban, munkaállomásokon vagy IoT eszközökön.

Az ilyen átfogó, minden hálózati végpontot egyformán lefedő támadás detekció képességének megteremtése a szenzitív adatok és a hálózatok komplexitásának folyamatos növekedésével napról napra kritikusabb feladatot jelent. A Vectra Cognito mellett egyetlen másik termék sem képes a biztonsági kockázatok hasonlóan radikális csökkentésére a proaktív, teljesen automatizált, minden végpontra kiterjedő, mesterséges intelligencián alapuló támadó vadászat megvalósításával.

I am artificial intelligence.
The driving force behind the hunt for cyberattackers.
I am Cognito.

Mi teszi a Vectrát egyedülállóvá?

Még a leghatékonyabb tűzfal és végpontvédelem is csak azt képes megmutatni amit blokkolt: a sikeresen átjutott támadások láthatatlanok maradnak számára. A Vectra Cognito folyamatosan felügyeli a teljes hálózati forgalmat (a kibertámadások valódi forrását) és perceken belül képes a védelmen átjutott, rejtett, még ismeretlen támadások pontos azonosítására, gyakorlatilag téves riasztások nélkül.

Mivel a támadók könnyen tudnak eszközöket váltani, ezért a Vectra nem a konkrét kártevőket, káros honlapokat, csatolmányokat vagy programokat blokkolja, hanem kizárólag a támadási viselkedésre összpontosít. A konkrét eszköz vagy kártevő gyors kicserélésével szemben támadási módszert váltani rendkívül nehéz, míg teljesen új kibertámadási metodikát találni a kibertér egyik legnagyobb kihívását jelenti.

A Cognito előfizetés részeként a Vectra folyamatosan fejleszti a mesterséges intelligencia képességeit és az új támadási viselkedések elleni detekciókat, hogy a védelem előnye mindig megmaradjon.

Cognito™ a legjobb mesterséges intelligencia kibertámadások detektálására és azonnali reakcióra

I am artificial intelligence.
The driving force behind the hunt for cyberattackers.
I am Cognito.

Cognito Detect: *automatizált támadás keresés*

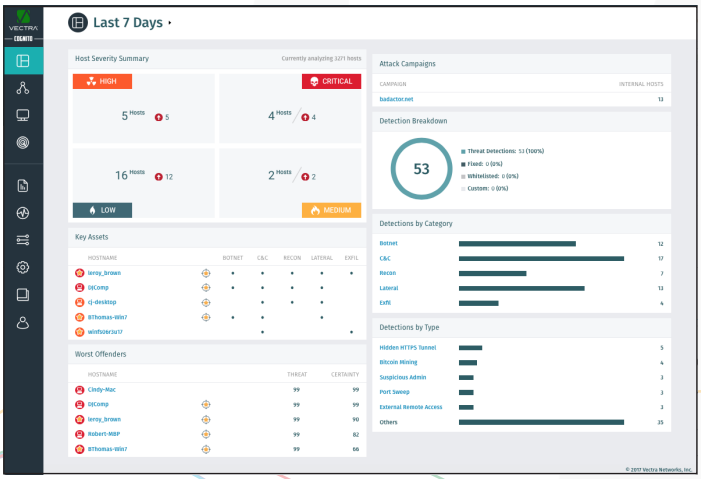
A folyamatosan adaptálódó, gépi tanulás és mesterséges intelligencia alapú támadási viselkedés modellek valós időben azonosítják a rejtett és eddig ismeretlen kibertámadásokat. Így lehetővé válik az azonnali, automatikus elhárítás, vagy a helyzet részletes, magasabb szintű emberi elemzése.

Cognito Recall: *hálózati visszajátszás és elemzés*

A Cognito platform kiegészítőjével részletes visszatekintő elemzést végezhet a különböző Cognito detekciók körülményeivel kapcsolatban, akár pontosan visszajátszva a hálózati forgalmat.

Teljes hálózati lefedettség

A Cognito a kibertámadások valódi forrását, az egész hálózati forgalmat feldolgozza, így nem naplókból, NetFlow adatokból vagy másodlagos adatforrásokból dolgozik. A teljes hálózati forgalomban nem marad vakfolt, így a Cognito figyelme a felhőtől az utolsó IP címmel rendelkező IoT eszközig terjed.



A Cognito felületén a támadási detekciók fontossági sorrendben, a kill chain alapján korrelálva, érintett eszközönként és támadási módszerenként lebontva láthatók.

Pontos detekciók, pontos részletekkel

A Vectra Cognito téves riasztások helyett rendkívül pontos, releváns detekciókkal alapozza meg a hatékony biztonsági üzemeltetést, így a támadás teljes kontextusa, a kapcsolódó események is átláthatók a biztonsági üzemeltetés számára.

Napok helyett pár perc egy incidens vizsgálata

Számos Vectra ügyfél számol be arról hogy a korábbi több órás vagy több napos incidens vizsgálati időtartam néhány percre rövidül a Cognito detekciói alapján. Így az üzemeltető csapat plusz humán erőforrás nélkül tud nagyságrendekkel több incidenst hatékonyabban kivizsgálni.

Segít áthidalni az üzemeltetői tapasztalat hiányát

Míg a fejlett támadások, APT-k elleni védelmi eszközök tipikusan a biztonsági szakértők top 1 százalékának készülnek, a Cognito mindenkinek szól. Érthető magyarázatokkal, részletes támadási leírásokkal és infografikákkal egy junior üzemeltető is képes egy senior elemző eredményét elérni.

Automatikus és azonnali támadás elhárítás

A Cognito detekciói teljesen automatizált beavatkozást is lehetővé tesznek: a mesterséges intelligencia valós időben képes a tűzfalat, switch portokat, EDR-t, NAC-ot vagy más biztonsági megoldásokat irányítani, így akár perceken belül ki tudja zárni az azonosított támadót. Míg a régiónkban 101 nap az átlagos rejtett kibertámadás detektálási idő, ezt a Vectra képes percekre rövidíteni. (Forrás: FireEye M-Trends 2018)

24x7 Security Operation Center „egy dobozban"

A Cognito platform tökéletes alapot ad az SOC létrehozásához, és felruház egy kis létszámú, ezért folyamatos támadás keresésre manuálisan képtelen csapatot egy 24x7 SOC biztonsági elemző képességével. Ez a Cognito mesterséges intelligencia valódi célja.

VECTRA®
Security that thinks®

Hazai disztribútorunk a Yellow Cube
vectra.ai – yellowcube.eu