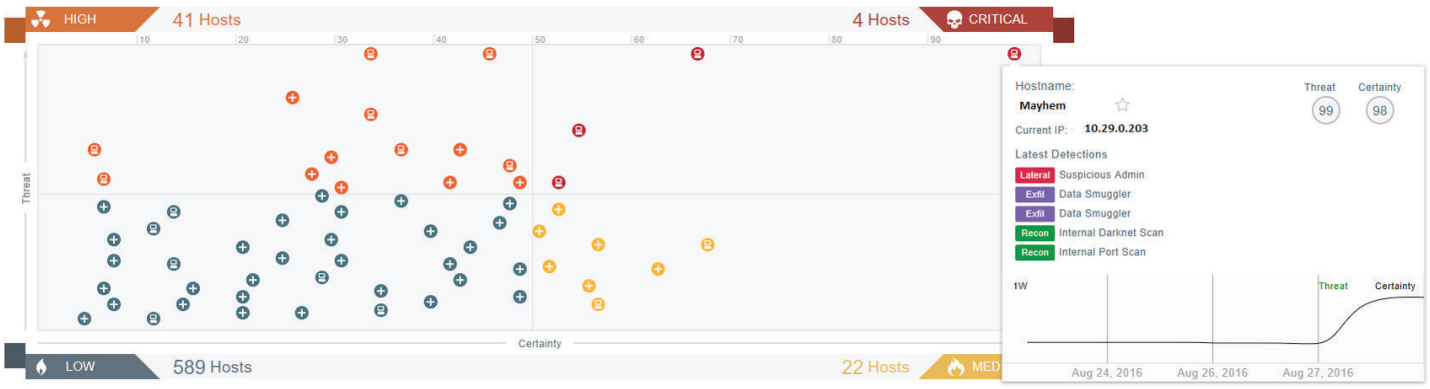
VECTRA®

Security that thinks.®

MESTERSÉGES INTELLIGENCIA ALAPÚ AUTOMATIKUS TÁMADÁSKEZELÉS ÉS ÖNVÉDELEM



Vectra Cognito™

DIÓHÉJBAN

- **Felfedi az aktív kibertámadásokat és azonnali reakciót biztosít**
- **Automatizálja a biztonsági üzemeltetést, kész válaszokkal**
- **Kevés szakértővel is sokkal magasabb szintű biztonságot nyújt**
- **Folyamatosan követi a támadások minden fázisát**
- **Minden hálózati forgalmat ellenőriz: belsőt és internet felé irányulót**
- **Elemzi a biztonsági naplókat, autentikációs logokat és SaaS alkalmazások naplóit**
- **Minden eszköz és minden operációs rendszer működését felügyeli**
- **Teljes fizikai és virtuális infrastruktúra védelmét biztosítja**
- **Együttműködik SIEM, tűzfal, NAC és végpontvédelmi gyártókkal**

A Vectra Cognito™ a leggyorsabb és leghatékonyabb eszköze a védelmen átjutott kibertámadások megállításának. Komplex mesterséges intelligenciája segítségével valós idejű láthatóságot biztosít a támadások minden fázisában, és műveletre kész részleteket szolgáltat az azonnali beavatkozáshoz.

A fejlett gépi tanulási technológiákat (például mély tanulás és neurális hálózatok) a folyamatosan fejlesztett támadási viselkedés modellekkel egyesítve a Vectra Cognito gyorsan és hatékonyan fedezi fel az ismeretlen támadásokat, még mielőtt azok valódi kárt okozhatnának.

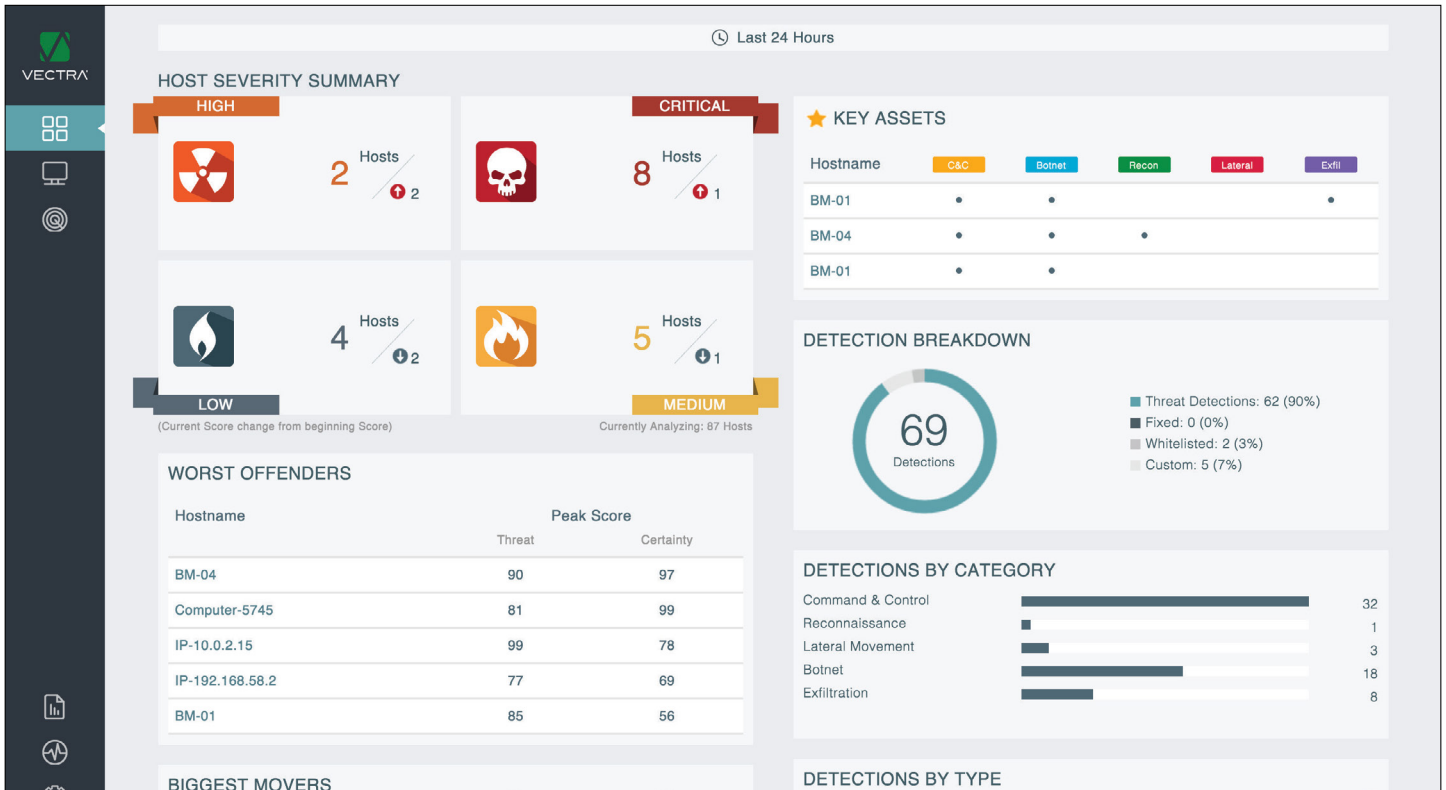
A Vectra Cognito a teljes hálózati forgalom, a biztonsági naplók, autentikációs logok és SaaS-alkalmazás naplók folyamatos elemzésével megszünteti a biztonsági vakfoltokat. A teljes láthatóság a hálózattól az IoT eszközökön át a felhőig terjed, ezért a Vectra előtt nem maradhat kibertámadás felfedezetlen.

A szoftveres és fáradhatatlan biztonsági szakértő

A Vectra Cognito automatizálja a kibertámadások felderítését, megmutatja hol rejtőzködnek a támadók és éppen mit csinálnak. A kockázati besorolás alapján a Vectra mesterséges intelligenciája kiemeli a veszélyes hosztokat, így az emberi üzemeltetők megállíthatják a legsúlyosabb támadásokat, mielőtt kárt okoznának.

A kézzel végzett riasztás- és naplóelemzés teljes automatizálásával a Vectra megoldása több heti emberi munkát végez el percek alatt, a biztonsági üzemeltetést megközelítőleg 30x hatékonyabbá teszi. A változatlan létszámú üzemeltetői csapat így lényegesen több biztonsági incidenst sokkal gyorsabban képes kezelni, valóban felkészítve a védelmet az egyre növekvő számú és egyre komplexebb kibertámadásra.

Vectra Cognito fontossági sorrendbe sorolja az aktív kibertámadásokat, összeveti a kulcsfontosságú erőforrásokkal és pontosan felfedi, hogy éppen mit tesznek a támadók.



Hogy működik a Vectra Cognito?

Bővített metaadatok

A Vectra Cognito a hálózati csomagok metaadatait, valamint a rendszernaplókat feldolgozva valós idejű láthatóságot biztosít a teljes hálózati forgalomban.

A metaadatok elemzése egyaránt kiterjed a házon belüli, munkaállomások, szerverek, virtuális infrastruktúrák közötti horizontális és az internet, illetve felhőszolgáltatók felé irányuló vertikális forgalomra. A Vectra Cognito az összes IP címmel rendelkező eszközt követi és ellenőrzi a hálózatban.

A Vectra számára így minden eszköz látható: laptopok, szerverek, nyomtatók, BYOD és IoT eszközök, adatközponti virtuális infrastruktúrák mellett a felhők és SaaS alkalmazások egyformán a Vectra védelme alá kerülnek.

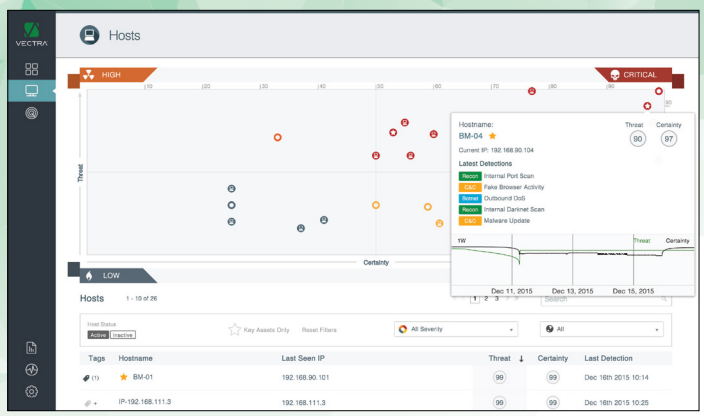
A rendszernaplók, autentikációs és SaaS logok segítségével a mesterséges intelligencia képes azonosítani az egyes támadásokban érintett felhasználókat és rendszereket is.

A STIX threat intelligence használatával a Vectra Cognito a már ismert támadásokat is megbízhatóan azonosítja, és hajszálpontosan megjelöli a támadásban érintett hosztokat, valamint fontossági sorrendbe sorolja őket kockázat és veszélyesség alapján.

Támadások azonosítása

Az összegyűjtött adatokat a Vectra viselkedés-elemző algoritmusai vizsgálják rejtett és még ismeretlen támadások után kutatva. Egy támadási szignatúra helyett a támadók viselkedésére fókuszálva egy komplex kibertámadást lépésenként azonosít a Vectra: például távoli hozzáférést, rejtett tunneleket, hátsókapuk telepítését, jogosultságokkal való visszaélést, belső felderítést vagy épp belső hosztok közötti mozgást.

Miután a Vectra Cognito megtanulta a fizikai és a virtuális hálózatok felépítését, a mesterséges intelligencia folyamatosan



Vectra Threat Certainty Index™

adaptálódik a változó helyi környezethez. Így képes azonosítani a normálistól eltérően viselkedő, fertőzött gépeket, valamint a belső veszélyek első jeleit.

A Vectra ezért az összes kibertámadás ellen bevethető a ‚cyber killchain' minden lépésében:

- **Command & control és rejtett kommunikáció azonosítása**
- **Belső felderítés felfedezése**
- **Belső hosztok közötti mozgás azonosítása**
- **Jogosultságokkal való visszaélés detektálása**
- **Adatszivárogtatás vagy adatlopás észlelése**
- **Zsaroló(vírus) támadások előkészületeinek azonosítása**
- **Botnet tevékenységek felfedése**
- **Támadáskampányok azonosítása, az összes érintett számítógép támadási térképen való megjelenítésével**

A Vectra Cognito ezen felül a felhasználók viselkedését is folyamatosan elemzi és azonosítja a potenciális belső veszélyforrásokat, mint például a felhőtárolók használata, USB eszközökre való adatmásolás vagy a gyanús hálózati adatmozgások.

VECTRA MESTERSÉGES INTELLIGENCIA

Bővített metaadatok

- Hálózati forgalom
- Rendszer, auth. és SaaS naplók
- IoC-k (STIX)

Támadások azonosítása

- Gépi tanulás
- Viselkedés analitika
- Hálózati elemzés

Automatikus analízis

- Támadások és érintett gépek csoportosítása
- Sorrendbe állítás veszélyesség szerint
- Támadás-kampányok azonosítása

Válasz, azonnali reakció

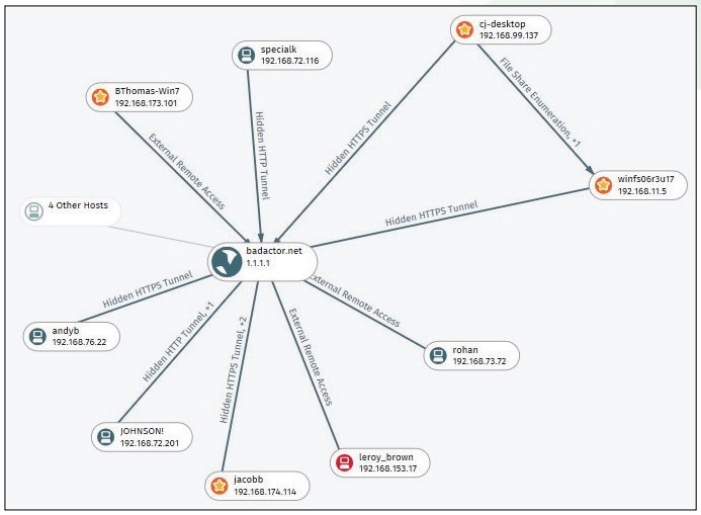
- Intuitív kezelőfelület, gyorsan áttekinthető
- Automatikus reakció
- Tűzfal, végpontvédelem, SIEM és NAC integráció

Automatikus analízis

A Vectra Threat Certainty Index™ több ezer esemény és előzmény adat felhasználásával határozza meg a legveszélyesebb aktív támadásokat és az érintett számítógépeket.

A Vectra Cognito nem áraszt el riasztásokkal, az óriási adattömeget feldolgozva csak a legveszélyesebb és legvalószínűbb behatolásokra segít fókuszálni. Sőt, a Vectra automatikus választ is kiválthat például a végpont lezárásával, vagy egy SIEM-en keresztül azonnal értesítheti a biztonsági üzemeltetést.

A támadási kampányok automatikus összegzésével a Vectra Cognito térképre rajzolja a teljes kibertámadás lefolyását, az



Vectra Cognito láthatóvá teszi a teljes, összetett kibertámadást.

összes érintett hoszt összekötésével és kapcsolataik pontos elemzésével. Így a Vectra felfedi az összetett, rejtett command-and-control infrastruktúrákat és láthatóvá teszi a komplex, lassan haladó és rejtőzködő kibertámadásokat is.

Ahogy a támadók felderítik a belső hálózatot és gépről gépre haladva jutnak közelebb a célponthoz, a Vectra Cognito felismeri a kill chain lépéseit, összefüggéseit és térképen vizuálisan megjeleníti a teljes támadás folyamatát.

Az interaktív térképen mozogva minden érintett hoszt előélete is követhető, így pontosan meghatározható a támadás lefolyása és az érintett adatok, személyek pontos köre.

Válasz és azonnali reakció

A gyors beavatkozáshoz a Vectra Cognito minden releváns információt összesít és az azonnali döntéshez szükséges minden lényeges összefüggést feltár. A Vectra detekciókat más, hasonló megoldások riasztásaival szemben nem szükséges manuálisan elemezni, hiszen a mesterséges intelligencia automatizálja a veszélyelemzést és pótolja ezt az emberi munkát.

A Vectra Cognito a detekció részleteit – a hoszt környezetét, packet capture fájlokat és kockázati besorolást – egyetlen kattintással elérhetővé teszi. Sőt, az azonosított veszély pontos és részletes jellemzése bárkinek segít eligazodni egy ismeretlen támadás részletein is, az informatív súgót követve minden új és tapasztalt üzemeltető pontosan képbe kerülhet a támadás valódi okával és kockázataival.

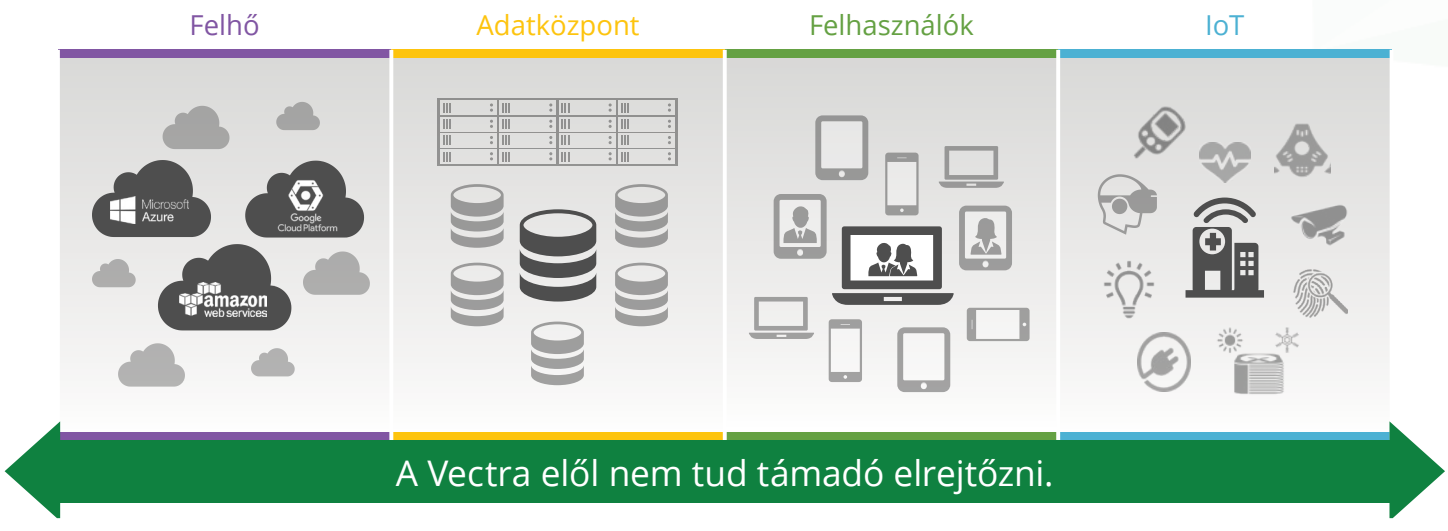
Ráadásul a Vectra Cognito együttműködik az új generációs tűzfalakkal, végpontvédelmekkel és NAC megoldásokkal, amelyek automatikusan és azonnal képesek elhárítani a mesterséges intelligencia által azonosított támadásokat.

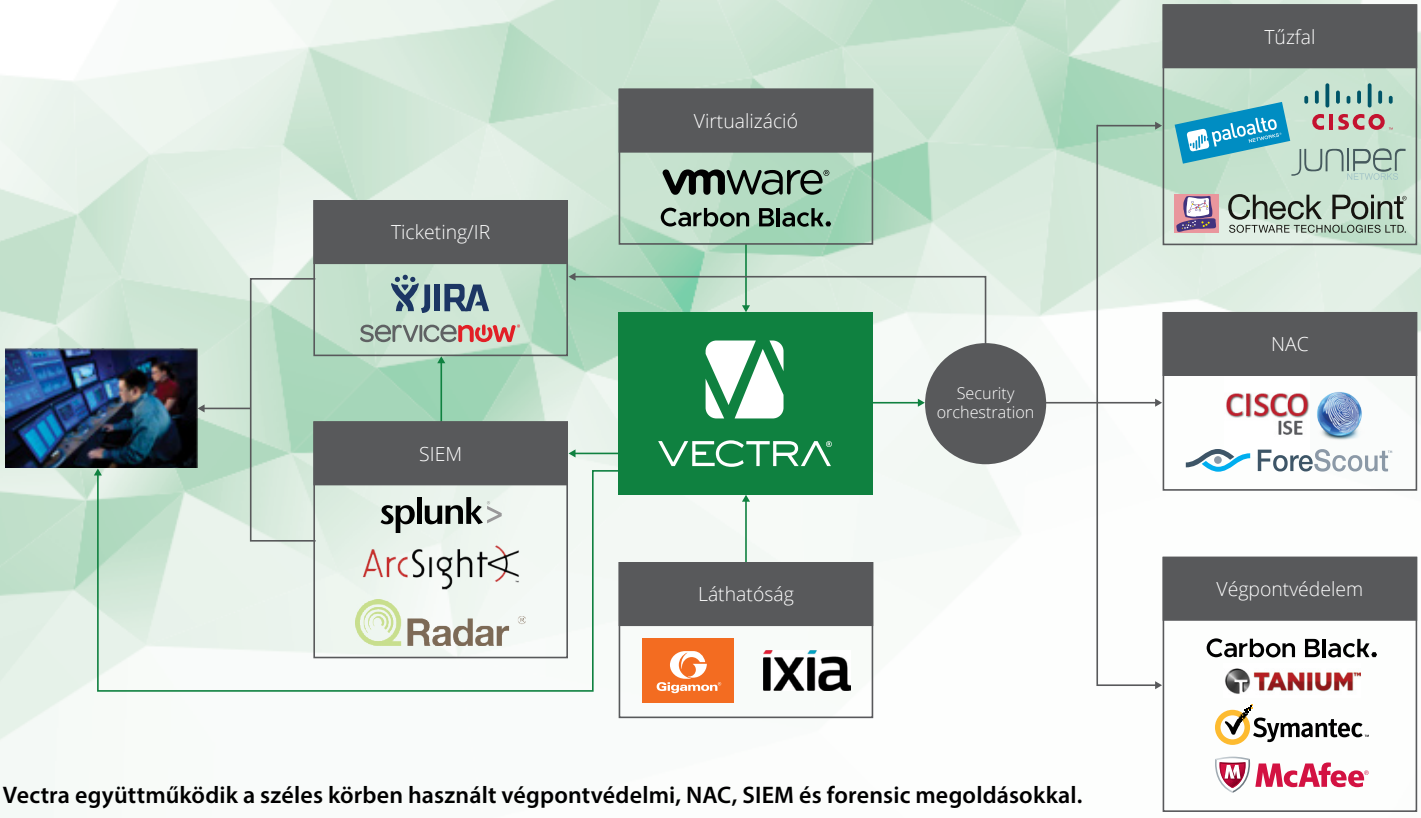
A Vectra Cognito jól kiegészíti a SIEM és forensic eszközöket is, és minden biztonsági vizsgálathoz hiteles kiindulópontot ad.

Gondolkodó biztonság: Security that thinks®

Több biztonság, kevesebb emberi erőforrással

A Vectra elsődleges célja a túlterhelt, ostrom alatt álló biztonsági üzemeltetés munkájának megreformálása, a biztonsági események elemzésének teljes automatizálása. Mesterséges intelligenciájával non-stop keresi az ismeretlen támadásokat, így az értékes szakemberek a véget nem érő manuális elemzés helyett a valódi támadások felszámolásával foglalkozhatnak.





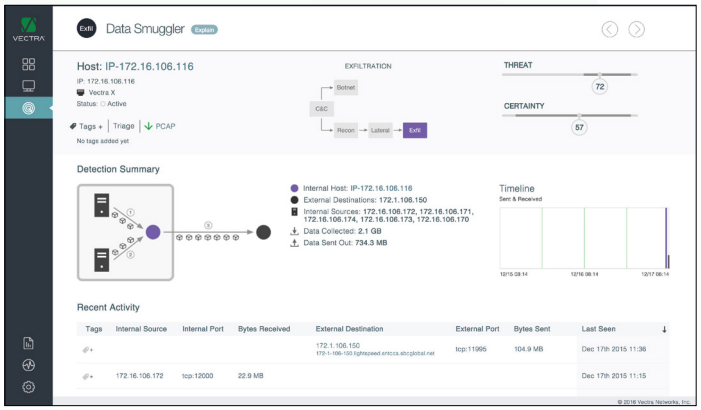
A Vectra együttműködik a széles körben használt végpontvédelmi, NAC, SIEM és forensic megoldásokkal.

Minden detekcióról részletes magyarázatot is biztosít a Vectra Cognito, kiemelve a támadás előzményeit és a detekcióhoz vezető utat. A biztonsági elemzők így rögtön, vizuálisan összekapcsolva láthatják a támadáshoz kapcsolódó összes hosztot és minden eddig rejtett tevékenységet vagy kommunikációt.

A Vectra Cognito képes további metaadatokat (pl.: VirusTotal információk) biztosítani a vizsgált forgalomhoz, így tovább gyorsítja a biztonsági incidens elemzést és a reakciót.

Automatizálja a teljes biztonsági rendszert

Legyen szó bármilyen kiberbiztonsági kihívásról, a Vectra Cognito jelentősen megnöveli a már meglévő biztonsági rendszerek hatékonyságát: a tűzfallal, végpontvédelemmel, NAC, SIEM és más rendszerekkel való együttműködéssel sokkal hatásosabbá válik az aktív védelem, mint Vectra nélkül.



Valós idejű detekció egy folyamatban lévő adatlopásról

A Vectra Cognito integrációs lehetőségeivel és a részletes veszély információk felhasználásával a támadás alatt álló végpontok azonnal izolálhatók, és gyorsan megállíthatók az eddig észrevétlen támadások is.

Részletes API segítségével a Vectra detekciói lényegében bármilyen védelmi rendszer számára elérhetők és tetszőlegesen feldolgozhatók. Az API mellett syslog és CEF formátumú naplózás is bekapcsolható az egyes detekciókról.

A Vectra Cognito nem csak egy újabb naplóforrás: az egyetlen olyan pont a hálózatban, ami mesterséges intelligenciájával beavatkozásokat indít és valódi, rejtett kibertámadásokat tesz láthatóvá a védett hálózat bármely pontján.

Felügyeli a rendszergazdai jogosultságokat

Míg a támadások tipikusan egy átlagos munkaállomás fertőzésével kezdődnek, az igazi károkozás vagy adatlopás sokszor rendszergazdai vagy rendszerszintű jogosultságokat igényel. Éppen ezért a Vectra Cognito túllépve az egyszerű felhasználói viselkedés elemzésen, kiemelten foglalkozik a potenciálisan kompromittálódott rendszergazdák tevékenységével.

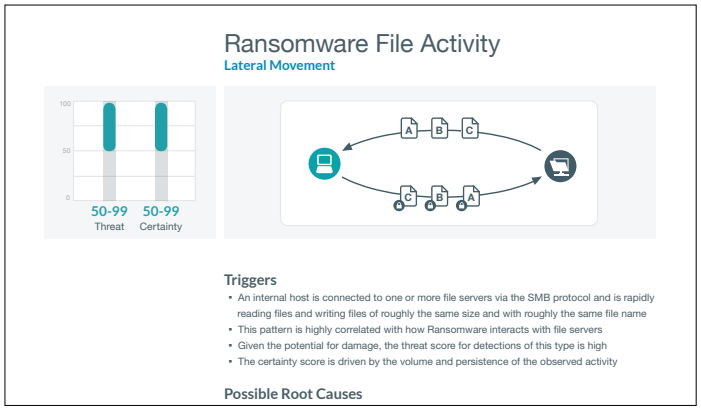
A Vectra pontosan követi az adminisztrációhoz használt protokollokat és megtanulja, hogy mely eszközöket mely rendszergazdák, milyen módon kezelnek. A folyamatosan adaptálódó felügyelet könnyen kiszűri a gyanús rendszergazdai belépéseket és potenciálisan eltulajdonított jogosultságokat, mielőtt még az így létrejövő támadások igazán veszélyessé válhatnának.

Teljes körű ransomware detekció

A zsaroló(vírus) támadásokat a Vectra Cognito minden egyes lépésben nyomon követi és lehetővé teszi az azonnali beavatkozást. Ráadásul, a teljes hálózati forgalom elemzésével a Vectra minden előkészületet észrevesz (például command-and-control kommunikáció létrehozása, fájlmegosztások szkennelése, kártevő terjesztése hosztok között) még mielőtt a zsaroló támadás valódi kárt okozhatna.

Hatékony védelem a privát felhőben

Míg a privát felhő alapú saját adatközpont tárolja számos vállalat minden üzleti adatát, biztonsági szempontból viszont sokszor vakfolt marad. Az adatközpontok forgalmának átlagosan 80 százaléka szerverek közötti, vagyis sosem hagyja el a belső hálózatot, ezért a határvédelmi eszközök számára láthatatlan marad.



Ransomware detekció a Vectra Cognitoval

A Vectra Cognito viszont folyamatosan felügyeli az adatok mozgását az alkalmazások és az infrastruktúra egyes elemei között, így a legfejlettebb kibertámadásokat is képes időben felfedezni. A Vectra Cognito teljes lefedettsége és virtuális szenzorokkal való VMware vSwitch integrációja biztosítja, hogy egyetlen virtuális szerver sem maradhat védelem nélkül.

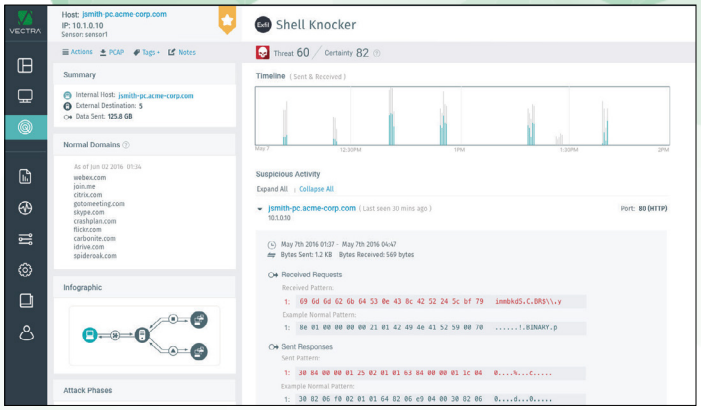
A Vectra Cognito a VMware vCenterrel integrálva egy mindig naprakész képet biztosít a teljes virtuális hálózat forgalmáról és a védelem állapotáról. Ráadásul a piacon a Vectra fejlesztett elsőként vCenter/adatközponti integrációt, amely ideális választássá teszi a teljes adatközpont védelmére és a fejlett, rejtőzködő támadások felfedésére.

Biztonság a vastól az alkalmazásig

A Vectra teljes adatközponti biztonsága a virtuális szerverek és alkalmazások mellett a hypervisorokra, a hardverekre, valamint a hálózati eszközök alacsony szintű sebezhetőségei és hátsókapui detektálására is kiterjed. A Vectra Cognito egyedülálló láthatóságot biztosít a vastól az alkalmazásszintig.

Például a Vectra Cognito Port Knocking detekció felfedi a hypervisorokba vagy hálózati eszközökbe beépülő rootkiteket és hátsókapukat, mélyen a virtuális szerverek alatt.

A tipikusan csak a hardverüzemeltetők által használt ILO (infrastructure-lights-out) menedzsment eszközök sebezhetőségei egyre kedveltebb célpontjai a támadóknak, amivel mélyen a virtualizáció és más biztonsági rendszerek alatt szerezhetnek mindig elérhető hátsókaput az adatközpont védett területén belül. Ezért a Vectra kiemelten kezeli az alacsony szintű menedzsment protokollokat, mint az IPMI és iDRAC használatát.



Shell-Knocker hátsókapu aktiváció a Vectra Cognito felületén

A teljes körű felügyelet a vCenter integráció segítségével automatikusan riasztást küld, ha egy új, védelem nélküli virtuális eszközt érzékel; így biztosítja, hogy a folyamatosan változó adatközpontban egyetlen eszköz sem marad a Vectra Cognito mesterséges intelligencia védelme nélkül.

Próbálja ki ingyenesen, kockázat nélkül!

A Vectra Cognito a hálózati forgalom tükrözésével pár perc alatt telepíthető, passzív működéséből adódóan hálózati fennakadás nélkül, kockázatmentesen tesztelhető.

Keresse Vectra partnerét és állítsa meg a hálózatában aktív, rejtett kibertámadásokat!

VECTRA®
Security that thinks®

Hazai disztribútor Yellow Cube Kft. **Web** www.vectra.ai **és** www.yellowcube.eu
Email kapcsolat@yellowcube.eu **Telefon** +36 20 932 1240

© 2017 Vectra Networks, Inc és Yellow Cube Kft. Minden jog fenntartva. A 'Vectra' és a 'Vectra Networks' logó, valamint a 'Security that thinks' a Vectra Networks Egyesült Államokban bejegyzett védjegyei, valamint a 'Vectra Threat Labs' és a 'Threat Certainty Index' szintén a Vectra Networks védjegyei. Minden más védjegy vagy bejegyzett védjegy az adott gyártó védjegye lehet.