Cisco Stealthwatch Cloud

cisco Partner
Gold Certified

dendrite
a bittnet company

Securizați-va rețeaua enterprise privată, cloud-ul public, și/sau mediul hybrid.

Numai 56% din alertele de securitate sunt investigate, iar dintre acestea mai mult de jumătate nu sunt remediate, conform Cisco 2017 Annual Cybersecurity Report. Răspunderea la aceste alerte este o muncă covârșitoare și majoritatea organizaților nu au o echipă de securitate care să țină pasul cu ele. Companii de toate mărimile se confruntă cu provocarea securizării mediului cloud public, dar și infracstructura locală privată.

Dendrio recomandă introducerea de măsuri de securitate eficace pentru procesele de afaceri (workloads) din cloud-ul public, folosind soluții care să reducă numărul de alerte false. Considerăm că este un obiectiv critic. Infrastructura cloud publică este extrem de diferită față de infrastructura locală privată. Un cloud public oferă mai puține capabilități de monitorizare a rețelei, în special în contextul unui ritm foarte mare de schimbare a activelor locale cu cele din cloud. Pentru a avea o securitate eficace, iar în același timp pentru a reduce numărul de alerte false, este nevoie de o nouă abordare.

Să ne imaginăm un scenariu în care credențialele de cloud ale unui angajat sunt compromise prin phishing sau orice altă metodă. Aveți mijloacele de a detecta faptul că acel angajat tocmai s-a autentificat din o altă țară? Cisco Stealthwatch Cloud vine cu capabilități de securitate inteligentă cu măsuri acționabile și cu vizibilitatea necesară pentru a putea identifica astfel de activități malițioase în timp real. Puteți reacționa rapid, înainte ca un incident de securitate să devină o breșă de securitate devastatoare.

Utilizând Stealthwatch Cloud, aveți capabilitățile să detectați amenințări externe și interne peste toată infrastructura IT a organizației, de la rețeaua privată din sediu, la sucursale, și până la cloud-ul public. Stealthwatch Cloud este o soluție de tip SaaS (Software-as-a-Service) implementată direct din cloud. Este foarte ușor de evaluat, cumpărat și implementat; iar operarea și mentenanța sunt ușor de efectuat. Când datele sunt primite de soluție, sunt necesare doar câteva configurări sau clasificări de echipamente. Toată analiza datelor este automată.

Beneficii

- Obțineți vizibilitatea întregului mediu IT, de la rețele private până la cloud-ul public.
- Detectați repede amenințări complexe și indicatori de compromitere al unui sistem.
- Creșteți capabilitățile de securitate în pas cu cele de business în timp ce reduceți costurile operaționale.
- Reduceți drastic numărul de alerte false cu alerte de o mai bună calitate, bazate pe observații ale comportamentului rețelei.
- Obțineți o postură de securitate mai puternică la nivelul întregii organizații, inclusiv în cloud-ul public.

Securizați-vă mediul IT cu entity modeling

Amenințările evoluează în mod constant. Pentru a detecta atacurile zilei de mâine, aveți nevoie de securitate care să fie mereu cu un pas înaintea lor. Stealthwatch Cloud utilizează o abordare care are la bază o modelare bazată pe comportament care detectează o amenitare, analizând comportamentul acesteia în rețea. De exemplu: dacă un domain controller începe să transfere date utilizând FTP (File Transfer Protocol), acesta este un prim indicator de compromitere a sistemului. Stealthwatch Cloud detectează acest comportament în timp real și te notifică prin alterte asupra acestui fapt.

Utilizând învățarea dinamică, Stealthwatch Cloud generează un model, un fel de simulare, pentru fiecare echipament sau entiate din rețea. Acest model este capabil să:

- Determine în mod dinamic rolul unei entități bazate pe comportament și să detecteze inconsecvențe cu acesta.
- Identifice anomalii și modificări neașteptate în comportament, atât în transmiterile de date cât și în modul de AAA (autentificare, autorizare și accounting) utilizat.
- Detecteze când o entitate se comportă diferit față de echipamente similare.
- Identifice când o entitate încalcă o politică a organizației, inclusiv tipul de protocol sau portul de rețea folsoit, caracteristica profilului de echipamente sau resursa, și comunicații clasificate după o listă neagră (blacklisted).
- Prezică comportamentul unui echipament sau al unei entități bazat pe activități anteriaore, și să compare comportamentul observat față de cel prezis.

Cu aceste capabilități, Stealthwatch Cloud va permite personalului Dvs. să dedice mai mult timp remediind probleme în loc să irosească timp analizând manual datele colectate pentru a determina cauza.

Detectați amenințări în cloud-ul public:

Pe măsură ce organizațiile mută mai multe resurse în cloud-ul public, au nevoie de vizibiliatea necesară detectării de agenți care vizează activele din cloud. În plus, au nevoie de o soluție eficientă, ușor de utilizat și administrat. Stealthwatch Cloud prin Public Cloud Monitoring oferă vizibilitatea și capabilitățile de detecție a amenințărilor de care aveți nevoie pentru a menține în siguranță procesele de afaceri implementate în cloud-urile AWS (Amazon Web Services) și Azure (Microsoft Azure).

Procesează toate sursele de telemetrie native AWS-ului, inclusiv flow-urile din Amazon VPC (Virtual Private Cloud), pentru a monitoriza toate activitățile din cloud fără a avea nevoie de agenți software. Stealthwatch Cloud poate să fie implementat în aceste medii cloud în câteva minute fără a perturba disponibilitatea serviciilor din cloud.

Stealthwatch Cloud utilizează aceste date ca să modeleze comportamentul fiecărei resurse din cloud, acesta tehnică numindu-se modelare de entități. Ca urmare, Stealthwatch Cloud este capabil să detecteze schimbările bruște de comportament, activitatea malițioasă și semnele care indică compromiterea.

Securizați-vă și rețeaua privată

Vizibilitatea în rețea și detecția de amenințări nu mai sunt doar pentru corporații mari. Conform unui studiu organizat de către Ponemon Institute pentru companii cu mai puțin de 1000 de angajați, 55% dintre ele au înregistrat un atac cibernetic în ultimul an și aproape o treime nu au avut capabilitățile necesare pentru a determina sursa brești de securitate. Stealthwatch Cloud prin Private Network Monitoring poate să ofere vizibilitatea necesară detectării amenințărilor din rețea în timp real, fără să fie nevoie de echipamente scumpe, resurse IT, sau timp amplu al echipei de securitate pentru implementare, operare și administrare.

Stealthwatch Cloud primește o mare varietate de telemetrie și log-uri. Soluția utilizează modelarea de entități pentru a determina rolul fiecărei entități din rețea și care este comportamentul normal al ei. Dacă o entiate manifestă un comportament nou, anormal, sau arată semne de compromitere, va fi generată o alertă, pentru ca personalul calificat de securiate să poată să investigheze și să răspundă.

Orice abordare are compania Dvs. în epoca digitalizării, Cisco Stealthwatch Cloud vă ajută să vă securizați toată infrastructura IT, fie ea privată sau într-un cloud public.

Pentru mai multe detalii sau pentru un demo, contactați-ne pe askformore@dendrio.com

cisco Partner
Gold Certified

dendrio
a bittnet company