Panda Adaptive Defense összehasonlítása más technológiákkal

Kritikus végpontvédelmi adottságok

	Adaptive Defense	AV	Anti exploit	Anti ransom	Sand boxing
VÉDELEM A TÁMADÁSOK DINAMIKÁJA ELLEN, MINT:					
Ismert kártevők, ismeretlen kártevők és nulladik napi támadások, amelyek lehet zsarolóvírusok vagy annak változatai	●	◒			◒
Fejlett Állandó Fenyegetések (APTs), célzott támadások és kiber-kémkedés	●				
Ismert és ismeretlen exploit támadások, beleértve a kártevő nélküli támadásokat	●		●		
Botnet támadások, amelyek átveszik a felügyeletet a számítógépek felett Control és Command (C&C) szerverek által	●				◒
ÚJGENERÁCIÓS VÉGPONTVÉDELEM (NGEP)					
Megakadályozza a rosszindulatú szoftvereket, kiszűri a támadásokat mielőtt aktiválódnak és megelőzi a visszatérő támadásokat	●	◒	◒	◒	
Folyamatosan monitorozza a futó folyamatokat, minden alkalmazást osztályoz és megállít, ha valamelyik nem megbízható	●				
Folyamatosan alkalmazkodik az új támadás dinamikájához a Machine Learning technikák segítségével Big Data környezetben	●	◒			◒
Tartós támadásra irányuló fókusz, amely kiszűri és dinamikusan blokkolja az eszközöket, taktikákat, technikákat és a rosszindulatú folyamatokat (TPPs)	●				
DETEKTÁLÁS, BEHATÁROLÁS ÉS DÖNTÉS					
Ha valamit nem megfelelőnek minősít, vagy gyanúsan viselkedik, blokkolja és valós időben riasztást ad róla	●				
Valós időben ad információt a támadó aktivitásáról: eredetéről, okáról, támadott eszközről és a megtett lépésekről	●				
Automatikus döntések, rosszindulatú file-ok törlése, változások kijavítása és kompromittált folyamatok megszüntetése	●	◒	◒	●	◒
Operatív információt szolgáltat az elvégzett feladatokról és a jövőbeni támadások ellen megtett lépésekről	●				
MENEDZSELT SECURITY SZOLGÁLTATÁS					
Az automatizálás (Machine Learning, Big Data) csökkenti az IT security csoport terhelését és a detektálás -válasz közt eltelt időt is	●				
A szolgáltatást tovább erősítik az új támadások felfedésének területén dolgozó szakértők (“threat hunters”)	●	◒			
A támadók aktivitásának 24 órás felügyelete és monitorozása az év minden egyes napján	●	◒			◒
INCIDENS KIVIZSGÁLÓ ESZKÖZÖK					
Megmutatja a támadás idővonalát (file-ok, bejegyzések, driverek, stb.) azok üzleti hatásait (pl. érintett vagyontárgyak, zombie gépek, számítástechnikai eszközök)	●				
Hozzáférést biztosít a részletes, felhasználókhoz köthető információkhoz, megőrizve azok bizalmas jellegét	●				
Teljes integráció más feltáró eszközökkel és főként SIEM-mel (Security Information & Event Management)	●				
KOCKÁZATMENEDZSMENT KÉPESSÉG					
A rendszer teljes áltáthatósága: futó szoftverek, sebezhető alkalmazások, felhasználói viselkedés, adatforgalom stb.	●				
Kereső eszközök a külső támadások, vagy belső felhasználók okozta anomáliák feltárására vagy a cég erőforrásainak nem megfelelő használatára	●				
Felhő alapú platformon Big Data-t alkalmazó eszközök, amelyek minimalizálják a működési költséget és a válaszidőt	●				
KÖNNYŰ TELEPÍTÉS ÉS KEZELÉS					
Könnyű telepíteni, frissíteni és kezelni a felhőből, ami lehetővé teszi, hogy távoli rendszereket úgy védjen meg mintha a hálózatban lennének	●	●	●	●	◒
Skálázható bevezetés a szolgáltatások megszakítása nélkül, öntanulás és a céghez történő integrálás (up & running in hours) átlátható módon	●				
Többféle integrált technológia, melyek a tökéletes együttműködésnek köszönhetően nem terhelik a rendszert	●	●			
Minimális hatással van a rendszerre, a védett eszközökre, és maximum 5% -kal a rendszer teljesítményére.	●	◒	◒	◒	
Minimális kellemetlenséget okoz a végfelhasználóknak, csökkenti az IT részleg túlterheltségét, így az incidensek kezelésére tudnak fókuszálni	●	◒	◒	◒	
VALÓS IDŐBEN TÖRTÉNŐ FELDOLGOZÁSI KÉPESSÉG					
Machine Learning technika Big Data környezetben, mint kizárólagos módszer a folyamatok valós időben történő osztályozására	●				
A felhő használat és a számítógépes határok nélküli adatbányászat csökkenti a rendszerek összetettségét és támogatja a hatékony kockázatkezelést	●	◒			