Ochrana identit v přímém přenosu

Pokud sázíte na holistický přístup k bezpečnosti, víte, že nestačí jen sbírat data z koncových stanice, ale potřebujete další detekční plochy, které vám umožní účinnější vyšetřování incidentů kyberbezpečnosti.

V roce 2021 měli dodavatelé XDR připraveny systémy, které byly spíše směsicí funkcí a vizí, že nakonec nahradí SIEM systémy jakožto hlavní technologii v bezpečnostním operačním centru SOC. XDR systémy stále nemohou plně konkurovat systémům SIEM upraveným na míru pro koncového uživatele, s funkcemi, jako je kontrola dodržování shody, pokročilé federativní vyhledávání nad nestrukturovanými daty anebo přizpůsobení implementace SIEM systému na unikátní prostředí a systémy zákazníka. Již nyní ale mnozí dodavatelé XDR systémů dosáhli bodu integrace a produktových schopností v takové míře, že zákazníci mohou začít vizi náhrady SIEM systémů za XDR realizovat. K tomu nedávné otřesy na trhu SIEM jsou pro dodavatele XDR příležitostí ukázat zákazníkům toužícím po změně, jak by mohl nový přístup v otázce bezpečnosti vypadat.

Nejen zákazníci dosavadních SIEM řešení, ale i klienti řešící bezpečnost svých organizací chtějí dnes pokrytí bezpečnosti přes pokud možno celé své IT prostředí. A přesně stejným směrem jdou také dodavatelé bezpečnostních platforem XDR, kteří díky přidávání dalších bezpečnostních telemetrií zajišťují zvýšení kvality detekce pokrytím různorodých platforem. Přitom ale normalizace dat a stanovení priorit není vůbec triviální. Proto také dodavatelé, kteří neomezují detekční plochy jen na koncové body, ale využívají k detekci například i cloudové úlohy, chování mobilních zařízení nebo bezpečnost identit, poskytují bezpečnostním analytikům lepší prostor pro investigaci, a to také díky rozšířené vizualizaci incidentů, obohacené o rozšířenou telemetrii.

Identity threat detection and response

Detekce a reakce na hrozby v oblasti identit (ITDR) je disciplína, která zahrnuje nástroje a osvědčené postupy, jež chrání samotnou infrastrukturu identit před útoky. ITDR dokáže blokovat a detekovat hrozby, reagovat na různé typy útoků a v případě potřeby obnovit normální provoz. Ochrana identit integruje detekci a reakci na hrozby pro identity společně s rozšířenou detekcí a reakcí v rámci XDR platformy a poskytuje komplexní ochranu všech vašich identit včetně této infrastruktury. Pomocí ITDR získáte komplexní viditelnost napříč lokálními uživateli AD, uživateli Entra ID, účty služeb a tokeny služeb k rychlé identifikaci a řešení anomálií. Sjednocení informací z ostatních bezpečnostních nástrojů s podrobnými informacemi o chování uživatelů vám umožňuje komplexní pochopení potenciálních rizik a proaktivní správu.

Bitdefender přináší tuto ochranu do své unifikované bezpečnostní platformy GravityZone, kde dochází ke sjednocení dat o hrozbách ze všech zdrojů identit do jediného přehledu a bezpečnostním týmům je umožněno rychle identifikovat a reagovat na tyto hrozby napříč koncovými body, e-maily, cloudovými aplikacemi a nástroji pro spolupráci. Platforma GravityZone poskytuje konzistentní ochranu lidských i strojových identit, zastavuje laterální pohyb a odhaluje kompromitaci identit. Díky sledování chování uživatelů v reálném čase a rychlému zmírňování rizik, díky neustálému monitorování a poskytování okamžité nápravy zajistíte, aby byla vaše organizace v bezpečí.

Průběžné monitorování a okamžitá náprava

Dnes nám již nestačí jen vlastní detekce, dnes chceme na problémy rychle reagovat. GravityZone se bezproblémově integruje například s Entra ID pro výměnu informací o rizicích v reálném čase, s možností označení uživatelů jako ohrožených a se spuštěním automatické izolace uživatelů. S využitím senzoru XDR Identity vytváří platforma GravityZone XDR rozšířené incidenty s podrobnými údaji souvisejícími s identitou, a to i bez zapojení spravovaného koncového bodu. Navíc můžete při analýze hrozeb využívat nástroj Pomocník s incidenty – Incident Advisor, který vám předá výsledky analýzy incidentu v grafické konzoli včetně návrhu doporučené reakce na konkrétní incident.

Bitdefender GravityZone XDR prostřednictvím ochrany identit ITDR detekuje a blokuje hrozby identit během laterálního pohybu v reálném čase, přičemž koreluje data z koncových bodů a identit, a tím výrazně zlepšuje dobu odezvy, a pokrývá tak všechny úhly pohledu na hrozby ležícími mezi zařízeními a identitami. GravityZone automaticky sestavuje celý řetězec útoku a prezentuje bezpečnostním analytikům shrnutí incidentu v lidsky čitelném formátu. To usnadňuje pochopení a vzbuzuje ve vašem týmu důvěru k přijetí rozhodných opatření.

Více na: *https://www.youtube.com/watch?v=ReBDrsyyiSY &list=TLGGBmVEIAvZXdYyNzA4MjAyNA*