AV-Comparatives považuje Bitdefender za strategického lídra v oblasti EPR

V nejnovější zprávě „Endpoint Prevention and Response (EPR) reportu“, vydávané nezávislou organizací AV-Comparatives, byl Bitdefender potvrzen jako strategický lídr.

Test hodnotil a porovnával výkonnost deseti řešení kybernetické bezpečnosti koncových bodů včetně Bitdefender GravityZone Business Security Enterprise.

Efektivita

Zpráva EPR je ambiciózní, komplexní hodnocení, které odráží každodenní realitu případů použití v podnikové sféře, a spojuje schopnosti prevence i detekce do jediného hodnocení.

V testu bylo celkem spuštěno padesát scénářů proti každému bezpečnostnímu řešení a výsledky byly vyhodnoceny v kontextu celého řetězce útoku. Dodavatelé řešení předem nevěděli, kdy přesně test nastane, a neznali žádné další podrobnosti o útocích.

Zpráva EPR rozlišuje mezi aktivní reakcí (akci je zabráněno) a pasivní reakcí (akce je zjištěna a nahlášena, ale vyžaduje lidskou interakci). Útok postupoval třemi různými fázemi a prevence a detekce se měří pro každou z nich zvlášť:

- **Fáze 1 (kompromitace a opěrný bod)** – počáteční přístup, provedení, perzistence
- **Fáze 2 (interní šíření)** – zvýšení oprávnění, vyhnutí se obraně, přístup k pověření, objevování, laterální pohyb
- **Fáze 3 (napadení infrastruktury)** – shromažďování, řízení a kontrola, exfiltrace, působení

Cílem je zablokovat útok dříve, než se dostane do třetí, tedy konečné fáze, kdy útočníci začnou naplňovat svůj hlavní cíl. Pokud prevence a detekce v této závěrečné fázi selžou, útočníci dosáhli narušení bezpečnosti, aniž byli odhaleni. V letošním roce se polovině zúčastněných dodavatelů nepodařilo narušení bezpečnosti zabránit a rozhodli se zůstat v anonymitě a ve zprávě EPR nejsou zmíněni. Řešení Bitdefender dosáhlo kumulativní míry aktivní odezvy 100 % a zabránilo narušení bezpečnosti ve všech testovaných scénářích!

Měření falešně pozitivních výsledků, ROI a TCO

Spojení prevence a detekce do jedné hodnoticí zprávy je jedním z jedinečných rysů tohoto testování. Problémem tohoto přístupu je, že dodavatelé mohou konfigurovat řešení pro agresivní ochranu, čímž uměle zlepšují hodnocení prevence, ale také generují mnoho šumu a falešných poplachů.

Důležitými kritérii pro hodnocení zabezpečení koncových bodů jsou přesnost, možnost akce a detekce falešných poplachů. Vysoký počet falešných výstrah má dopad na různé části organizace, od koncových uživatelů (zabezpečení by nemělo omezovat produktivitu) přes obchodní oddělení (zvýšení TCO/ROI) až po samotný bezpečnostní tým (přepracovaný tým).

Zpráva EPR se tímto problémem zabývá tak, že obsahuje údaje o provozní přesnosti a nákladech na zpoždění pracovních postupů. Provozní přesnost simuluje typickou činnost uživatele (otevírání souborů, prohlížení) a zároveň sleduje, zda řešení zabezpečení koncových bodů ovlivňuje produktivitu (falešné poplachy). Měření zpoždění pracovního procesu přidává sankce za používání sandboxového zařízení. Řešení Bitdefender mělo nízký dopad na provoz a bylo jediným dodavatelem bez penalizace nákladů v oblasti provozní přesnosti. Ve všech testovaných scénářích dosáhl produkt Bitdefender nulových falešných poplachů.

Informace z testování účinnosti se ve zprávě kombinují s údaji o nákladech na produkt a o jeho přesnosti, aby bylo možné vypočítat celkové náklady na vlastnictví. Řešení Bitdefender získalo certifikaci Strategic Leader díky velmi vysoké návratnosti investic a nízkým celkovým nákladům na vlastnictví.

Akceschopnost

Zpráva EPR obsahuje kvantifikovatelné údaje, jako jsou falešně pozitivní výsledky, ale existují i subjektivnější prvky, které zvyšují efektivitu a akceschopnost bezpečnostních týmů.

V EPR reportu AV-Comparatives uvedla o platformě Bitdefender následující: „Je třeba poznamenat, že produkt má velmi dobré korelační schopnosti a vizualizaci včetně časové osy popisující šíření hrozeb. Například když byly některé útoky zjištěny v pozdější fázi, produkt je vystopoval až k jejich původu a poskytl velmi podrobné informace.“

Řešení Bitdefender pro detekci a reakci (Bitdefender GravityZone XDR) bylo navrženo jako nativní řešení XDR. Jde o řešení, které má hotovou integraci s dalšími zdroji telemetrie (síť, AD, AWS, o365 atd.), což usnadňuje nasazení s kratší dobou návratnosti investice. Jednou z výhod nativního XDR je lepší přesnost, což se potvrdilo nulovým počtem falešně pozitivních výsledků v testech.

Jednou z nejdůležitějších funkcí je poradce pro incidenty – přehled, který na jedné stránce shrnuje nejdůležitější informace o incidentu. Incident Advisor koreluje data z různých zdrojů a prezentuje je ve formátu, který minimalizuje čas potřebný k vyšetřování a reakci. Zahrnuje informace o tom, co se stalo, kdo byl zasažen, jak k incidentu došlo, a obsahuje doporučená opatření. Pro další vyšetřování je k dispozici rozšířená analýza kořenových příčin včetně vizualizace řetězce příčin incidentu, která umožňuje bezpečnostnímu analytikovi přerušit jej ještě předtím, než se plně rozvine.

V průběhu vyšetřování Bitdefender řešení nabízí doporučení a řízené i automatizované reakce. V závislosti na nasazených senzorech jsou k dispozici různé kategorie akcí, což usnadňuje identifikaci akcí, které může použít i juniorský analytik.

Závěr

Nezávislé testování s přesně definovanou metodikou nabízí neocenitelné informace o schopnostech předních dodavatelů kybernetické bezpečnosti, které umožňuje rozhodování na základě informací. Kybernetická bezpečnost je hra na kočku a myš, obě strany neustále inovují a zdokonalují nástroje a techniky a dodavatelé bezpečnostních řešení musejí prokázat, že jejich řešení jsou účinná, přesná a poskytují konzistentní výsledky. Bitdefender to dokazuje dlouhodobě a opakovaně.