A FortiEDR blokkolja a támadások 100 százalékát

A FortiEDR sorozatban második éve blokkolja a támadások 100 százalékát a MITRE Engenuity ATT&CK® értékelés szerint.

A kiberbűnözők a FortiGuard Labs legújabb jelentése szerint „továbbra is számos új és korábban is ismert zsarolóvírussal támadják a vállalatokat (hetente körülbelül 150 000 egyedi észlelés)", ezért az idei MITRE ATT&CK® (Adversarial Tactics, Techniques & Common Knowledge) értékelések rendkívül fontosak. A MITRE ATT&CK közzétette a nagyvállalati elemzését melyben a Fortinet FortiEDR végpontvédelmi rendszer a támadások 100 százalékát blokkolta. Ez a második egymást követő év, amikor a FortiEDR az összes támadást blokkolta, egyben 32 százalékos növekedést mutatott a támadási lánc lépéseinek észlelési képességében – az összes technika közel 100 százalékának felismerésével.

Minden forgatókönyvben eredményes

A MITRE ATT&CK értékelés a kiberbiztonsági termékek ún. ellenséges viselkedés detektálási képességeit méri fel. Ehhez az ún. ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) tudásbázist használja a valós hackerviselkedést alkalmazó technikák modellezésére.

Az értékelés ezúttal a Wizard Spider és a Sandworm fenyegetéscsoportokra összpontosított. A Wizard Spider egy pénzügyileg motivált bűnözői csoport, amely 2018 augusztusa óta folytat zsarolóvírus-kampányokat különböző szervezetek ellen a nagyvállalatoktól kezdve a kórházakig. A Sandworm egy romboló szándékú csoport, amely olyan támadások végrehajtásáról ismert, mint az ukrán elektromos vállalatok elleni 2015-ös és 2016-os támadások, valamint a 2017-es NotPetya-támadások.

A FortiEDR az összes jelenleg elvégzett tesztforgatókönyvben részt vett. A kilenc szcenárióban a FortiEDR a tesztben használt 90 lépés 97 százalékát észlelte és katalogizálta, egyben minden támadást blokkolt.

A Gartner® megjegyzése szerint: „A fenyegetések felderítése nehéz feladat. A biztonsági és kockázatkezelési szakembereknek több száz ismert és valószínűleg még több ismeretlen fenyegetés ellen kell megvédeniük a vállalatokat. A MITRE ATT&CK keretrendszer úgy fejlődött, hogy rendszertant képezzen a fenyegetésekből és alapot nyújtson a fenyegetések észleléséhez."

E szabvány elfogadásával a FortiEDR intuitívabbá vált a kiberbiztonsági rendszereket üzemeltetők számára.

Mesterséges intelligencia és gépi tanulás erősíti

Az eredmények megmutatják, hogy a FortiEDR kiforrott kiberfenyegetés-észlelése hatékonyan használja a beépített mesterségesintelligencia- és gépi tanulási technológiákat. Mivel a FortiEDR nem támaszkodik szignatúrákra (de a felhőben továbbra is használja azokat), az értékelésben szereplőhöz hasonló támadási technikákat alkalmazó jövőbeli kibertámadásokat is valószínűleg blokkolja majd, még akkor is, ha nincs róluk előre meglévő kiberbiztonsági ismeret (azaz nem készült róluk szignatúra).

A FortiEDR egyedülálló képessége a rendszertevékenységek mély-elemzése, az ún. kódkövetés (code-tracing). Ennek a szabadalmaztatott technológiának az előnyei nyilvánvalóak voltak az értékelési eredményekben.

Annak érdekében, hogy észrevétlenek maradjanak, napjaink fejlett fenyegetései gyakran beavatkoznak az operációs rendszer egy vagy több legitim utasításába. Azáltal, hogy az operációs rendszer kimenő kommunikációs vagy fájlmódosítási utasításait az azt megelőző utasításfolyammal veti össze, a FortiEDR valós időben képes felismerni és megakadályozni a rosszindulatú műveleteket.

A MITRE ATT&CK-értékelések azt mutatják, hogy a viselkedésalapú végpontvédelmi platform, az EDR-megközelítés, valamint a FortiEDR-ben található kódkövetés (code-tracing) rendkívül jól működik a fenyegetések észlelése és megelőzése érdekében. *(X)*

FORTINET®