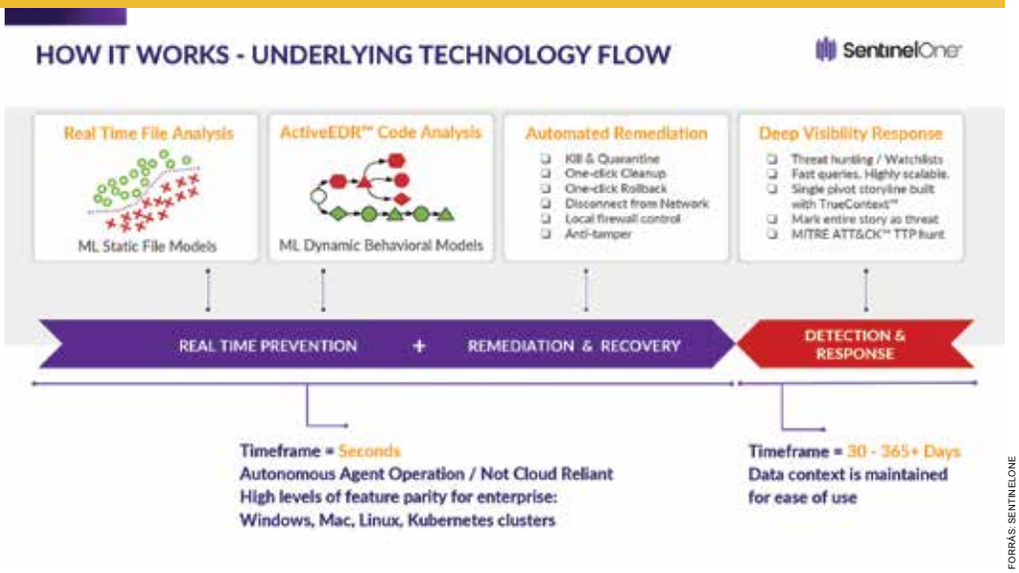
VAN ÉLET A RANSOMWARE-TÁMADÁS UTÁN!

Mire képes egy fejlett XDR-megoldás IT-biztonsági incidensek esetén?

Sokszor halljuk, hogy még a nagy cégeket is képes egy ransomware-támadás térdre kényszeríteni. Mára már azt is tudjuk, hogy a szervereket ért támadásokból van megoldás rövid idő alatt, egyszerű módszerrel, mentésből visszaállni, feltéve, hogy volt rendes backup. Viszont a legtöbb szervezetnél a gond a laptopokkal és munkaállomásokkal akad, ezeket általában használhatatlanná teszi a támadás. Még ha nincs is rajtuk érzékeny adat, az IT-csapat erőforrásait nagyban leköti az újratelepítés, miközben ezzel párhuzamosan kellene megoldaniuk a szerverek visszaállítását is.



FORRÁS: SENTINELONE

Többek között ezen a problémán is segít a SentinelOne végpontvédelmi XDR-megoldása, amely a fejlett védelmi és incidens kezelő képességek mellett lehetőséget nyújt arra, hogy egy ransomware-támadás esetén vissza lehessen állítani a munkaállomásokat – mindez pedig a Windows VSS (Volume Shadow Copy) biztonsági mentésére és ezeknek a mentéseknek a védelmére épül. Sok esetben a malware-ek egyik első lépése éppen ezeknek a mentéseknek törlése, hiszen így tudnák a legegyszerűbben megakadályozni a roncsolt vagy betitkosított fájlok gyors visszaállítását. Ezzel a védelmi lépéssel amellett, hogy a SentinelOne rendszer képes megakadályozni a támadás kezdeti szakaszát, és megkönnyíteni a visszaállítást, egyúttal riaszt is, hogy valami megpróbálta törölni a visszaállítási pontunkat, és megpróbált előkészíteni egy támadást.

Mindez már önmagában is praktikus funkció, de azt sem árt tudni, hogy ez a védelmi megoldás nemcsak a VSS-mentések esetén kerül bevetésre, hanem különböző, fontos rendszerfájlok és -folyamatok esetén is segít megelőzni a bajt. Sok esetben hasznos, hogy láthatjuk, melyik folyamatok és fájlok voltak érintettek egy támadásban, illetve automatizált módon elvégzi nekünk az úgynevezett „root cause”-elemzést, amelyből megtudhatjuk, honnan indult a támadás. Ezt az elemzést természetesen nemcsak Windows, hanem Mac, Linux és Kubernetes rendszerek esetén is használhatjuk.

Alkalmazásával könnyen visszamehetünk az időben, és felépíthetünk egy eseményvonalat. A támadás életciklusából kiderül, hogy sikerült-e időben megállítani az ostromot vagy szükséges-e utólag beavatkozni. Az idővonal és a nyomozási képességek használatához szerencsére nincs szükség bonyolult scriptelési vagy rendszerelemzői tudásra, mert a felület könnyen használható és a nyílt API-knak köszönhetően egyszerűen integrálható automatizációs rendszerekbe.

A nyomozás megkönnyítése mellett a SentinelOne XDR-megoldása olyan hatékony védelmi rendszer, amely a támadások megelőzésében is kiemelkedő képességekkel bír. Használatával megelőzhetjük, hogy fölöslegesen sok riasztás kerüljön az IT-biztonsági csapatunk elé, és a legtöbb esetben a rendszer egyszerűen definiálható szabályrendszer alapján képes azonnal beavatkozni – az elvárásainknak megfelelően! Emellett viselkedés és machine learning alapú megelőzésre is alkalmas, illetve a már jól ismert, új generációs antivírus képességeket is tartalmazza. Természetesen a sokszor felmerülő USB- és eszközkontrollt, illetve EDR típusú felügyeleti lehetőségeket is megtalálhatjuk a SentinelOne funkciói között. Ha pedig már megtörtént a baj, úgy könnyen, pár kattintásból álló parancsokkal akár az egész cégre kiterjedő műveleteket hajthatunk végre. A folyamatosan fejlődő XDR-technológiának köszönhetően emellett már akár automatizált hálózatfelderítésre is használhatjuk a telepített agentünket a megfelelő licencek megléte esetén. *(X)*