Karta informacyjna FortiEDR MITRE ATT&CK Evaluation

Fundacja MITRE co roku przeprowadza test produktów zabezpieczających punkty końcowe o nazwie ATT&CK Enterprise Evaluations. Przejrzysty proces oceny i publicznie dostępne wyniki pomagają organizacjom zidentyfikować rozwiązania najlepiej spełniające ich potrzeby związane z cyberbezpieczeństwem. Rozwiązania nie są klasyfikowane, a oceny koncentrują się na technicznych możliwościach rozwiązania w zakresie reagowania na znane zachowania przeciwników. Rozwiązanie FortiEDR uczestniczy w MITRE ATT&CK Evaluations od dwóch lat.

FortiEDR blokuje wszystkie ataki

Rozwiązanie FortiEDR skutecznie zablokowało wszystkie ataki w każdej rundzie testów, w których uczestniczyło — co potwierdza zobowiązanie FortiEDR do redukcji powierzchni ataku i powstrzymywania ataków na każdym ich etapie.

Ochrona bez sygnatur[1]

Rozwiązanie FortiEDR nie tylko blokowało każdy atak w każdym teście, w którym uczestniczyliśmy (Windows: testy 1–6 i 8–9). Były one blokowane od razu, bez konieczności stosowania sygnatur wymaganych przez inne rozwiązania. Zabezpieczenia oparte na sygnaturach wprowadzają luki w ochronie. Zalecamy, aby organizacje przejrzały zrzuty ekranu z testów ochrony każdego rozważanego dostawcy i poszukały śladów sygnaturowego antywirusa (AV), jeśli jest to kwestia istotna dla danej organizacji.

Wykrywanie 97% podtechnik

Z 90 podtechnik użytych w ośmiu testach systemu Windows, w których uczestniczyło rozwiązanie FortiEDR, wykryto 87 z nich, uzyskując wynik Visibility Rating na poziomie 97%. Plasuje to FortiEDR w pierwszej piątce spośród trzydziestu ocenionych dostawców. Taki poziom wiarygodnej widoczności pomaga organizacjom dostrzec pełen zakres aktywności cyberprzestępców.

Wskaźnik dokładności analiz na poziomie 94%

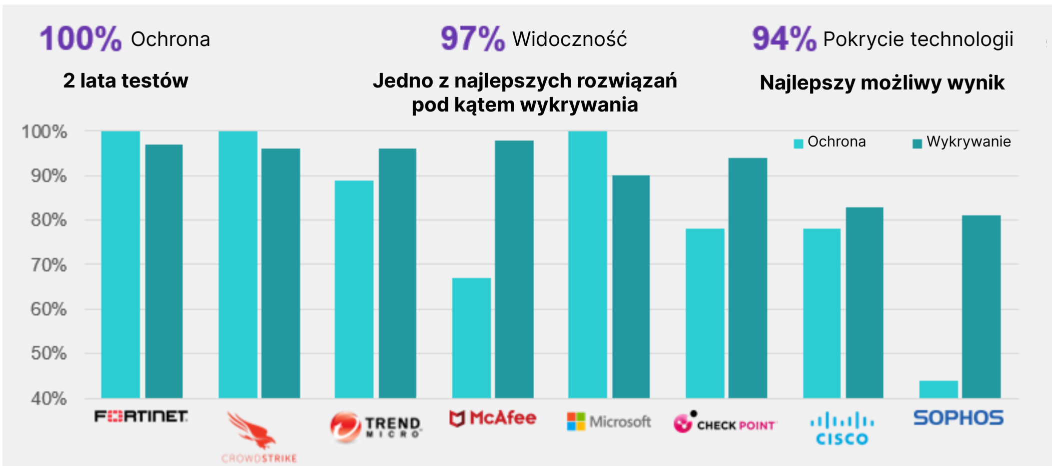
Spośród tych samych 90 podtechnik rozwiązanie FortiEDR rozpoznało również poprawną technikę w 94% przypadków. Tak wysoki wskaźnik wykrywalności sprawia, że administratorzy otrzymują dokładne informacje z wykorzystaniem terminologii branżowej, dzięki czemu mogą szybko zrozumieć, co widzi FortiEDR i podjąć odpowiednie działania.

Brak opóźnionych zmian konfiguracji

Zmiany konfiguracji występują z różnych powodów, a niektóre można zignorować (np. zmiany w logice). Osoby analizujące wyniki MITRE ATT&CK Evaluation powinni zwrócić uwagę na zmiany konfiguracji, które powodują opóźnienia, takie jak oczekiwanie na werdykt analityka lub systemu sandbox. Takie opóźnienia mogą czasami pozwolić na kontynuację cyklu życia ataku, potencjalnie negatywnie wpływając na organizację. W przypadku FortiEDR nie wykazano żadnych opóźnionych zmian konfiguracyjnych.

Podsumowanie

Drugi rok z rzędu rozwiązanie FortiEDR zablokowało wszystkie ataki bez użycia sygnatur i uzyskało wynik w pierwszej piątce pod względem wykrywalności całkowitej i analitycznej. Szczegółowy przewodnik po raporcie można znaleźć w naszym opracowaniu [Jak interpretować wyniki MITRE ATT&CK Evaluations].



[i] Warto zauważyć, że w rundzie czwartej rozwiązanie FortiEDR nie uczestniczyło w teście siódmym dla systemu Linux, ponieważ funkcjonalność Threat Hunting dla tego systemu operacyjnego znajdowała się w fazie beta w momencie przeprowadzania testu. Fortinet liczy na udział we wszystkich testach w kolejnej rundzie.

www.fortinet.com

22 grudnia, 2022 2:26 PM

1636692-0-0-PL