ZERO-FALSE POSITIVE VULNERABILITY MANAGEMENT

Czy wiesz, że większość eksploitowanych podatności to te klasyfikowane przez CVSS jako 9 i 10?

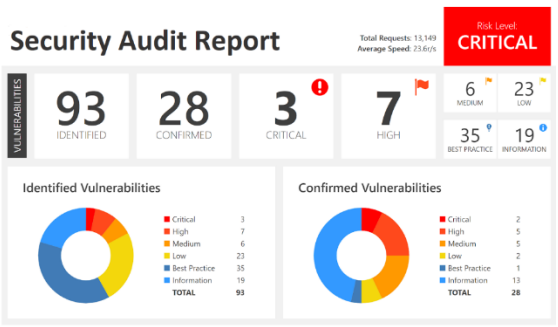
Tylko kilka procent tych podatności jest realnie wykorzystywanych w atakach. Podatności klasyfikowane przez CVSS jako „severity" 9 i 10 są uważane za krytyczne i wymagają natychmiastowej interwencji. Jednakże, badania pokazują, że tylko niewielki procent tych podatności jest rzeczywiście wykorzystywany w atakach. To oznacza, że wiele organizacji skupia się na niewłaściwych podatnościach a to prowadzi do marnowania czasu i zasobów na ich pilne usuwanie, podczas gdy realne ryzyko może wystąpić zupełnie gdzieś indziej.

Problem

Tylko skąd wiadomo, które to są konkretnie w Twoim przypadku? Klasyczne systemy zarządzania podatnościami też tego niestety nie podpowiedzą. Klasyczne systemy zarządzania podatnościami nie są w stanie określić, które z podatności mają rzeczywisty wpływ na organizację. Nie zapewniają one również praktycznych wskazówek, jak skutecznie chronić systemy przed atakami.

Jak zatem zarządzać bezpieczeństwem IT, aby nie walczyć "w ciemno" z setkami podatności systemów, które wyglądają na krytyczne, ale często nie są tymi najważniejszymi w mojej organizacji?

Tradycyjne testy penetracyjne wykonywane przez człowieka są czasochłonne, kosztowne i wymagają wysokiego poziomu wiedzy specjalistycznej. Tutaj pojawia się alternatywa w postaci zautomatyzowanego testu penetracyjnego opartego na uczeniu maszynowym, oferującego możliwość szybkiego i dokładnego skanowania systemów, wykrywania luk i podatności, a także identyfikacji i analizy zagrożeń bezpieczeństwa. Dzięki zastosowaniu uczenia maszynowego, systemy te potrafią adaptować się do zmieniającego się krajobrazu zagrożeń, a także uczyć się na bieżąco, co pozwala na skuteczne i proaktywne zapobieganie atakom na infrastrukturę IT.

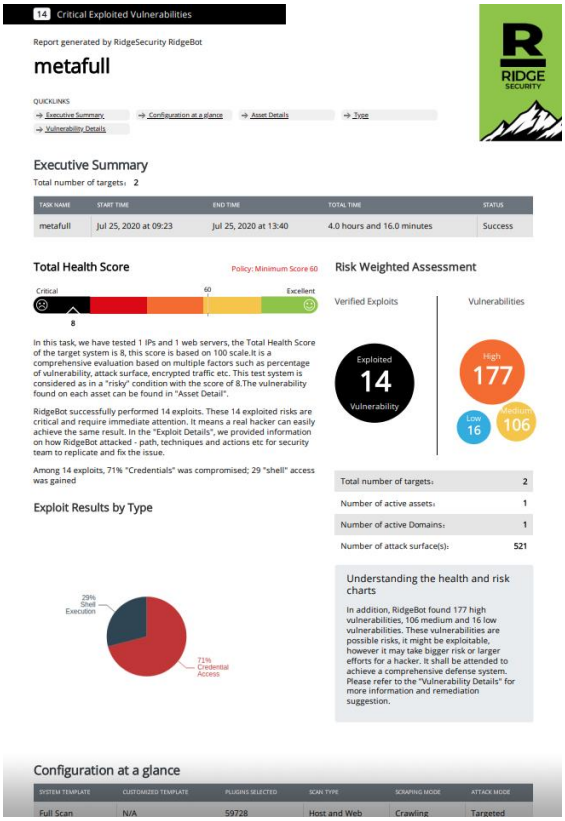


Dystrybucja w Polsce

PRIANTO

Rozwiązanie

Aby skutecznie zarządzać bezpieczeństwem IT, organizacje powinny wykorzystywać podejście oparte na ryzyku. Oznacza to, że należy skupić się na tych podatnościach, które stanowią największe zagrożenie dla organizacji. Jak można zautomatyzować proces zarządzania realnymi podatnościami, zweryfikować praktyczną skuteczność posiadanych zabezpieczeń w infrastrukturze i jak dzięki temu jeszcze lepiej wykorzystać posiadane zasoby?



Istnieją narzędzia, które umożliwiają automatyzację procesu zarządzania i weryfikacji podatności. Sztandarowym przykładem jest test penetracyjny z użyciem realnych kontrolowanych ataków, który pozwala na identyfikację rzeczywistych podatności i weryfikację skuteczności posiadanych zabezpieczeń. Dzięki temu organizacje mogą lepiej wykorzystać swoje zasoby i skuteczniej chronić swoje systemy przed atakami.

Dystrybucja w Polsce

PRIANTO