2023

secureVISIO

Podatności

Jedna platforma do wykrywania i zarządzania incydentami, podatnościami i ryzykiem

Zarządzanie podatnościami w oparciu o kontekst biznesowy za pomocą skanerów podatności i SecureVisio

Czym jest SecureVisio

SecureVisio to rozwiązanie dotyczące zarządzania bezpieczeństwem, głęboko zintegrowane z mechanizmami ochrony sieci, stworzone dla każdej organizacji, która chce zautomatyzować czasochłonny i skomplikowany proces zarządzania zabezpieczeniami IT, wliczając w to analizę wpływu biznesowego. Skuteczna strategia bezpieczeństwa zakłada, że specjaliści odpowiedzialni za bezpieczeństwo skupiają swoją uwagę na systemach IT o krytycznej ważności dla ich organizacji. SecureVisio rozumie techniczny aspekt bezpieczeństwa, ale też zna rolę biznesową najbardziej istotnych systemów w organizacji. Podczas użycia SecureVisio zintegrowanego ze skanerem podatności, jesteśmy natychmiast informowani o podatnościach, których wykorzystanie może mieć duży wpływ na działania biznesowe organizacji. Dzięki szybkiej identyfikacji nowych podatności, które automatycznie są łączone z ich kontekstem biznesowym, możliwe jest uniknięcie incydentów w ważnych systemach IT, które mogą prowadzić do bardzo poważnych konsekwencji (np. systemy przetwarzające dane osobowe, co może mieć swój skutek w karach wynikających z RODO). Rozwiązanie GRC SecureVisio wyposażone jest w mechanizm Auto-Discovery, elektroniczną dokumentację systemów IT, jak również zintegrowane zarządzanie podatnościami, incydentami, modelowanie zagrożeń oraz moduł audytu bezpieczeństwa. SecureVisio jest w stanie zautomatyzować czynności związane z zachowaniem bezpieczeństwa w każdej organizacji lub działać w formie inteligentnej platformy na bazie której można zbudować wyspecjalizowane centrum bezpieczeństwa (SOC).

Korzyści z integracji:

Kontekst biznesowy

obecny w zarządzaniu podatnościami pozwala w szybki sposób zidentyfikować podatności w krytycznych systemach IT, jak i o nich ostrzec

Symulacje awarii

sieci, bezpieczeństwa oraz elementów systemu IT i ocena czy ich konsekwencje lub awaria są w ramach tolerancji danej organizacji.

Zaplanowane dalsze skany

Zaplanowane przez SecureVisio dalsze skany weryfikują czy krytyczne w swoich konsekwencjach dla procesów biznesowych podatności zostały naprawione

Audyt zabezpieczeń

sieciowych bazuje na identyfikacji krytycznych procesów biznesowych oraz danych poufnych,

Automatyczne wykrywanie i priorytetyzacja

biznesowa nowych podatności opartych na regularnych skanach

Incydenty bezpieczeństwa są wynikiem istniejących w systemach IT podatności. Każdego dnia wykrywana jest olbrzymia ilość podatności - w systemach operacyjnych, aplikacjach, bazach danych i urządzeniach przenośnych.

Głównym problemem dotyczący zarządzaniem podatnościami jest kwestia tego, że organizacje nie są w stanie naprawić wszystkich podatności na czas.

Realistyczna strategia zarządzania podatnościami zakłada, że powinniśmy skoncentrować się na systemach IT krytycznych dla organizacji, w celu uniknięcia poważnych incydentów i konsekwencji.

Jak to działa?

W celu wykrycia podatności, SecureVisio wykorzystuje połączenie API ze skanerem podatności, przeprowadza analizę i w czasie rzeczywistym odczytuje informację na temat nowo odkrytej podatności dotyczącej różnych elementów systemu IT. Często liczba wykrytych podatności jest bardzo wysoka. SecureVisio odfiltrowuje dane z raportu bazując na ważności dla organizacji i wrażliwości danego systemu IT i powiadamia na temat podatności, które wymagają natychmiastowej konsultacji z pracownikami IT i kadrą zarządzającą. SecureVisio przeprowadza analizę podatności w oparciu na uprzednio zdefiniowane harmonogramy. Pozwala to organizacjom na zautomatyzowanie procesu skanowania podatności i mapowanie w czasie rzeczywistym podatności w systemach IT o krytycznej ważności dla organizacji. W rezultacie, osoby odpowiedzialne za bezpieczeństwo zasobów organizacji zawsze posiadają aktualne i kompletne informacje, jak również specjalistyczne narzędzia, które z kolei powodują, że ich praca jest mniej stresująca, a ryzyko podjęcia błędnych decyzji mniejsze.

Dodatkowo, ekspercka baza wiedzy dotycząca bezpieczeństwa pozwala SecureVisio na automatyczny audyt zastosowanych zabezpieczeń systemów IT, które nie posiadają adekwatnej ochrony. Menadżerowie podejmujący decyzje dotyczące rozbudowy mechanizmów bezpieczeństwa posiadają szybki i łatwy dostęp do szczegółowych raportów dotyczących prawnych i biznesowych konsekwencji potencjalnego złamania zabezpieczeń. W związku z powyższym, wydatki danej organizacji na cele bezpieczeństwa IT są uzasadnione przez prawnie i biznesowo.

Moduł Threat Modelling SecureVisio umożliwia symulację różnych typów awarii. Dla przykładu, możemy zasymulować awarię serwera fizycznego. SecureVisio natychmiast informuje o fakcie, które systemy IT są niedostępne jako konsekwencje tej awarii, jak również które procesy biznesowe zostały zakłócone. Podobnie, możemy zasymulować awarię sieci, jak i urządzeń ją zabezpieczających i bazując na tej informacji możemy w łatwy sposób zdecydować czy tego rodzaju ryzyko jest akceptowalne dla organizacji. Jest to szczególnie przydatne w przypadku efektywnym kosztowo planowaniu bezpieczeństwa IT, obsługi incydentów, jak i złożonych projektach, takich jak Business Continuity and Disaster Recovery.