esecure | SECUREVISIO

TECHNOLOGIA AUTOMATYZACJI PROCESU WSPOMAGANIA DECYZJI DOTYCZĄCYCH BEZPIECZEŃSTWA

OPIS TECHNOLOGII

SecureVisio to nowoczesne rozwiązanie Real TimeGRC przeznaczone do każdej organizacji, pozwalające na automatyzację wielu złożonych i pracochłonnych procesów zarządzania bezpieczeństwem, ułatwiające spełnienie wymagań prawa i standardów bezpieczeństwa (m.in. KNF, PCIDSS, RODO). Cechy i funkcjonalności systemu: RealTime GRC (Governance, Risk Management, Compliance) System działa w czasie rzeczywistym odczytując alarmy z SIEM i zabezpieczeń technicznych poddając je automatycznej analizie przy uwzględnieniu zarówno kontekstu technicznego jak i biznesowego. Narzędzie posiada edytor reguł bezpieczeństwa, który pozwala przeprowadzić analizę potencjalnych konsekwencji naruszeń bezpieczeństwa, automatyczną analizę ryzyka oraz skorelować dowolne parametry techniczne z biznesowymi. W przypadku dopasowania przychodzącego zdarzenia o zdefiniowanej regule, system aktualizuje bieżący incydent bezpieczeństwa lub zakłada nowy, nadaje mu odpowiedni priorytet i powiadamia jednocześnie odpowiedni zespół obsługi.

KOMPONENTY SYSTEMU:

Elektroniczna dokumentacja IT – interaktywna, elektroniczna dokumentacja sieci, systemów i zabezpieczeń IT wyposażona w graficzne narzędzie do edycji, przeszukiwania i analizy danych istotnych dla bezpieczeństwa organizacji.

Ekspert bezpieczeństwa IT „z pudełka" – zaimplementowana baza wiedzy eksperckiej, pełniącej rolę zespołu specjalistów z różnych obszarów bezpieczeństwa. Dostarcza informację na temat efektywności zastosowanych zabezpieczeń lokalnych i sieciowych oraz informacji istotnych z punktu widzenia zarządzania bezpieczeństwem.

Modelowanie scenariuszy włamań – zaimplementowane funkcje modelowania zagrożeń i audytowania bezpieczeństwa względem wykrytych lub potencjalnych wektorów ataku. Dodatkowo pozwala zwizualizować i przeanalizować zagrożenia dowolnego zasobu względem innego prezentując ryzyko i konsekwencje przełamania zabezpieczeń.

Translator bezpieczeństwa IT dla biznesu – zapewnia możliwość komunikacji podczas obsługi incydentów bezpieczeństwa oraz przy codziennych działaniach IT.

Biznesowa ocena podatności – system identyfikuje luki bezpieczeństwa w systemach IT odczytując je na bieżąco z bazy CVE® oraz poprzez integrację ze skanerami podatności tworzy harmonogram skanowania, a następnie je wykonuje. Dodatkowo system automatycznie analizuje ważność podatnych systemów IT dla organizacji oraz informacje techniczne związane z tymi zagrożeniami i wyznacza dla podatnych systemów odpowiednie priorytety.

Zautomatyzowany SOC – monitoring logi w trybie 24/7 oraz koordynacja działania w SOC realizowane jest poprzez scenariusze obsługi incydentów. Integruje się oraz koreluje informacje z SIEM oraz innych systemów zabezpieczeń, skanerów podatności oraz bazy CVE. Wykorzystanie systemu automatyzuje więc pracę w SOC, zwiększając jego efektywność działania, pozwalając na skuteczne unikanie naruszeń bezpieczeństwa.

Adaptacyjne scenariusze obsługi- zarządzanie scenariuszami obsługi podatności oraz incydentów bezpieczeństwa, które są uruchamiane po spełnieniu zdefiniowanych warunków oraz budowane w zależności od kontekstu przebiegu (workflow).

ZALETY I KORZYŚCI Z KORZYSTANIA

Zwykle wiedza na ten temat bezpieczeństwa, zachodzących w organizacji procesów biznesowych, danych przechowywanych w systemach IT, wiedza ekspercka i algorytmy zarządzania ryzykiem, znajduje się w głowach wielu ludzi i dziesiątkach często nieaktualnych dokumentów. Technologia SecureVisio w jednym miejscu utrzymuje informacje potrzebne do zarządzania bezpieczeństwem IT w organizacji, dzięki budującym ją komponentom. SecureVisio pokazuje całościowy obraz bezpieczeństwa IT organizacji w obszarze technicznym i biznesowym oraz zapewnia efektywne zarządzanie bezpieczeństwem ukierunkowane na systemy IT o krytycznym znaczeniu dla organizacji.

Dostępne na chwilę obecną narzędzia do zarządzania bezpieczeństwem systemów teleinformatycznych to rozwiązania ograniczone, które nie uwzględniają całej złożoności systemów IT gdyż m.in.:

- nie podają informacji jakie procesy są sterowane przez systemy, które padły ofiarą incydentu i jakie mogą być tego konsekwencje
- nie podają informacji czy incydent może rozprzestrzenić się na inne elementy SAP i które procesy mogą zostać zablokowane lub zakłócone,
- nie posiadają funkcji oceny wpływu incydentu bezpieczeństwo w SAP, ani informacji przydatnych w procesie ich obsługi w tych systemach.
- nie pozwalają na wykonanie symulacji naruszeń bezpieczeństwa i oceny ryzyka w trakcie modernizacji SAP.

KORZYŚCI:

Automatyzacja kluczowych procesów zarządzania bezpieczeństwem IT

- Efektywne zarządzanie bezpieczeństwem skoncentrowane na systemach IT o krytycznym znaczeniu dla organizacji
- Automatyzacja wielu złożonych i czasochłonnych procesów zarządzania bezpieczeństwem
- Baza wiedzy eksperckiej wspomaga podejmowanie trudnych decyzji i zmniejsza ryzyko błędów
- Działa jako niezależne rozwiązanie IT GRC w organizacji lub inteligentna platforma do budowy Security Operations Center (SOC)
- Pomoc w spełnieniu wymagań prawa i standardów bezpieczeństwa (m.in. KNF, GIODO, ISO-27001, PCI-DSS)

Łatwa w utrzymaniu elektroniczna dokumentacja sieci, systemów i zabezpieczeń IT:

- Elektroniczna dokumentacja wyposażona w dedykowane narzędzia do tworzenia logicznej architektury zabezpieczeń IT oraz szczegółowych schematów sieci fizycznej
- Funkcja Asset Discovery umożliwia automatyczne wykrywanie, rozpoznawanie oraz dokumentowanie systemów IT
- Graficzne narzędzia edycji i wyszukiwania parametrów zabezpieczeń, sieci i systemów IT oraz kreator generowania raportów
- Efektywne kosztowo planowanie bezpieczeństwa dzięki bazie wiedzy eksperckiej oraz funkcjom szacowania ryzyka i modelowania zagrożeń

Unikanie incydentów w systemach IT o krytycznym znaczeniu dla organizacji:

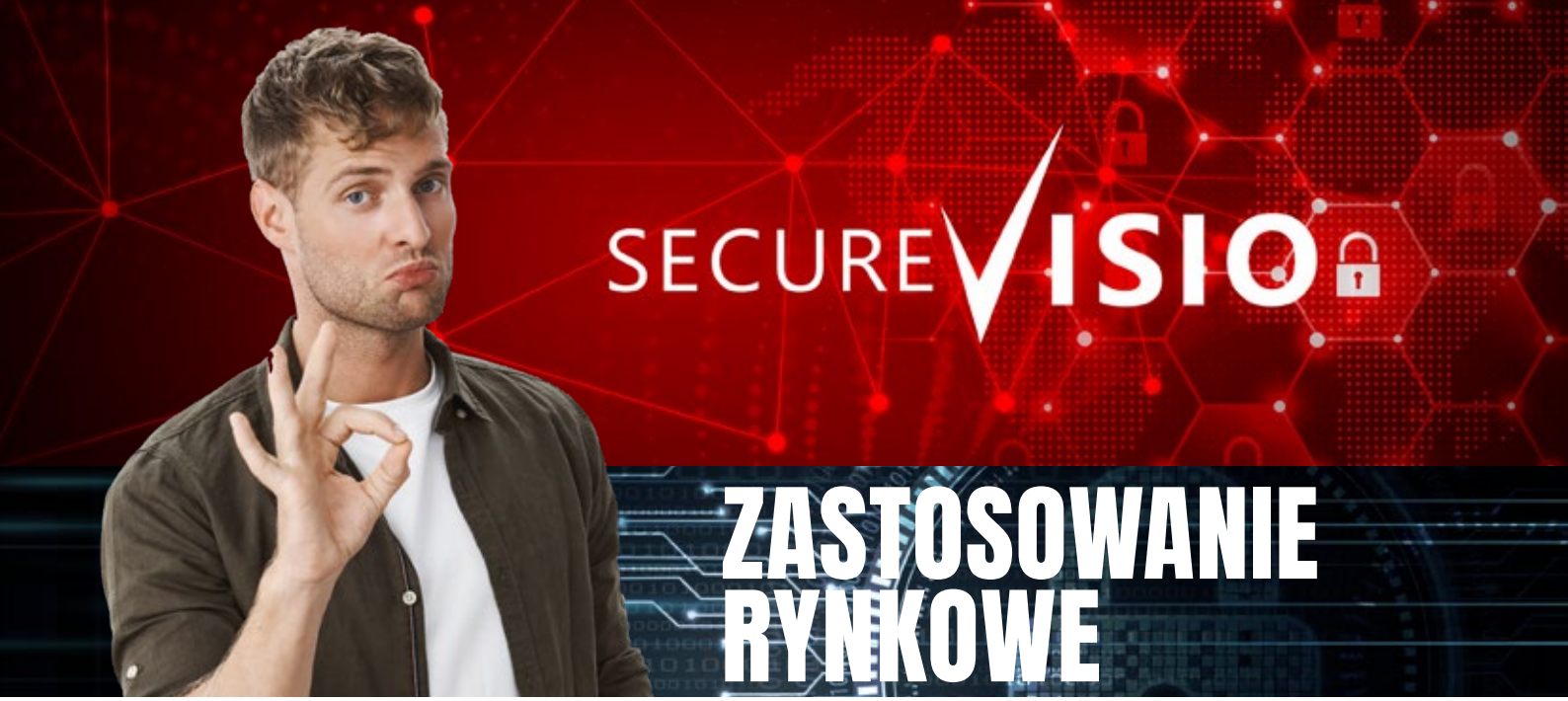
- Identyfikacja podatności (luk bezpieczeństwa) w systemach IT krytycznych dla działalności biznesowej organizacji
- Automatyczny odczyt nowych podatności z bazy CVE® oraz integracja z narzędziami Vulnerability Assessment
- Audytowanie projektu zabezpieczeń IT pod kątem wykrywania krytycznych procesów biznesowych nie posiadających wymaganych zabezpieczeń
- Symulacja awarii sieci, zabezpieczeń i systemów IT i ocena czy skutki awarii są akceptowalne dla organizacji

Efektywny kosztowo rozwój bezpieczeństwa IT zgodnie z wymaganiami działalności organizacji:

- Automatyczne szacowanie ryzyka oraz ustalanie najbardziej narażonych systemów IT o krytycznym znaczeniu dla organizacji
- Automatyczne ustalenie systemów IT o krytycznym znaczeniu dla organizacji, które są narażone na awarie (Single Point of Failure)
- Wydatki na bezpieczeństwo IT wynikające z rzeczywistych wymagań działalności organizacji
- Optymalizacja czasu pracy i zmniejszenie stresu osób odpowiedzialnych za bezpieczeństwo

Pomoc w utrzymaniu ciągłości działania krytycznych procesów organizacji

- Alarmowanie o podejrzanych zdarzeniach i incydentach w systemach IT posiadających krytyczne znaczenie dla organizacji
- Odczyt i analiza alarmów nt. incydentów bezpieczeństwa z systemów SIEM i innych zabezpieczeń technicznych (NGFW, IPS, itp.)
- Funkcja Business Impact Analysis wykonuje automatycznie ocenę wpływu incydentu na działalność organizacji (przydatna także w projektach BCP)
- Szybki dostęp do informacji potrzebnych do odtwarzania działania procesów biznesowych po incydenci



ZASTOSOWANIE RYNKOWE

Ochrona infrastruktury dotyczy przede wszystkim zachowania integralności i ciągłości działania procesów, które dane jednostki bezpośrednio zapewniają lub pośrednio wspierają. Ważnym zagadnieniem w tym temacie staje się więc wsparcie procesów zabezpieczeń, które obecnie są niewłaściwie opisane, skatalogowane i aktualizowane, co czyni je dziurawymi i podatnymi na ataki. Ten istotny temat został uwzględniony w KIS, a rozwiązanie problemu zapewnienia bezpieczeństwa infrastruktury przemysłowej, zapewniała będzie innowacyjna technologia SecureVisio. Implementacja do praktyki gospodarczej modelu pozwoli podjąć walkę z cyberprzestępczością dzięki zastosowaniu mechanizmów zarządzania bezpieczeństwem dostosowanych do potrzeb poszczególnych zasobów i różnorodnych, wdrożonych w organizacjach systemów automatyki. Dodatkowo projektowany system będzie zaliczany do technologii smart security, gdyż sam w zależności od zapotrzebowania dobierał będzie odpowiednie techniki zabezpieczeń, co pozwoli na automatyzację procesu nadzoru (audyty), monitorowanie, integrację z systemami bezpieczeństwa SIEM i internetową bazą podatności CVE oraz obsługę incydentów bezpieczeństwa. Osiągnięte to zostanie dzięki wprowadzeniu do zasobów sieciowych dokumentacji związanej z przemysłowymi systemami i powiązanie jej ze sobą poprzez sieć zależności; zarządzanie zgromadzoną informacją oraz korelację różnych źródeł danych.

Precyzując, zastosowanie rozwiązania pozwoli kupującemu zarządzać bezpieczeństwem w formie Security Operations Center (centrum zarządzania bezpieczeństwem). Faktem jest, że małe firmy nie stać na zatrudnianie ekspertów do analizy bezpieczeństwa, występuje niezrozumienie w zakresie posiadanych rozwiązań antywirusowych, analiza zdarzeń bezpieczeństwa praktycznie nie występuje. Wykorzystanie Oprogramowania SecureVisio pomoże profesjonalnie zarządzać bezpieczeństwem za niewielkie pieniądze o efektywności stosowanej w dużych podmiotach.

esecure ul. Hoffmanowej 19, PL-35016 Rzeszów

Contact: +48 17 779 6246
biuro@esecure.pl