

# SecureVisio - technologia automatyzacji procesu wspomaganego decyzji dotyczących bezpieczeństwa

Baza dawców technologii

4 lutego 2021

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 informacje 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).



**side\_option.exchange\_advertiser**

Esecure Sp. z o.o.

**Dane teleadresowe**

Klementyny Hoffmanowej 19

35-016 Rzeszów, Polska

tel.: [667661621](tel:667661621)

[krzysztof.gortat@esecure.pl](mailto:krzysztof.gortat@esecure.pl)