

Real Time GRC

Elektroniczna dokumentacja IT

Ekspert bezpieczeństwa IT „z pudełka”

Modelowanie scenariuszy włamań

Translator bezpieczeństwa IT dla biznesu

Biznesowa ocena podatności

Zautomatyzowany SOC

Adaptacyjne scenariusze obsługi

ESECURE SP. Z O.O.

ul. Hoffmanowej 19
PL-35016 Rzeszów
tel.: +4817 779 6246
email: biuro@esecure.pl

Jakie wyzwania w obszarze bezpieczeństwa adresuje SecureVisio™

Mnogość informacji w obszarze bezpieczeństwa nie pozwala na efektywne zarządzanie ryzykiem. Jesteśmy ograniczeni w zasobach ludzkich, jak również często nie wiemy jak skorelować powstające zagrożenia z realnym wpływem na biznes. Powstające ustawy czy rekomendacje są bardzo słuszne, ale ich przełożenie na wieloletni biznes i złożone procesy w organizacji nie należą do łatwości. Z tych powodów wysokiej klasy specjaliści bezpieczeństwa z międzynarodowym doświadczeniem zaczęli tworzyć w 2010 roku rozwiązanie, które zaadresuje powstające wyzwania. I tak powstało SecureVisio™.

SecureVisio™ to nowoczesne rozwiązanie Real Time GRC przeznaczone dla każdej organizacji, pozwalające na automatyzację wielu złożonych i czasochłonnych procesów zarządzania bezpieczeństwem. Zastosowanie systemu w organizacji zwiększa efektywność procesu zarządzania bezpieczeństwem oraz ułatwia spełnienie wymagań prawa i standardów bezpieczeństwa (m.in. KNF, PCI-DSS, RODO);

Real Time GRC (Governance, Risk Management, Compliance)

SecureVisio™ działa w czasie rzeczywistym odczytując alarmy z SIEM i zabezpieczeń technicznych poddając je automatycznej analizie uwzględniającej zarówno kontekst techniczny jak i biznesowy. Narzędzie posiada edytor reguł bezpieczeństwa, który pozwala przeprowadzić analizę potencjalnych konsekwencji naruszeń bezpieczeństwa (BIA), 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.

Filtr incydentu **i** Filtr odrzucenia Filtr agregacji

☒ ☐ ☐ ☐ ☐	Atak na serwer webowy	✓
☒ ☐ ☐ ☐ ☐	Wyciek danych osobowych	
☒ ☐ ☐ ☐ ☐	Wyciek klasyfikowanych informacji	

Dostępne pola

Wybierz... Dostępne metody Reguły globalne

Nazwa

Atak na serwer webowy

Priorytet

☒ Zwiększ o 5

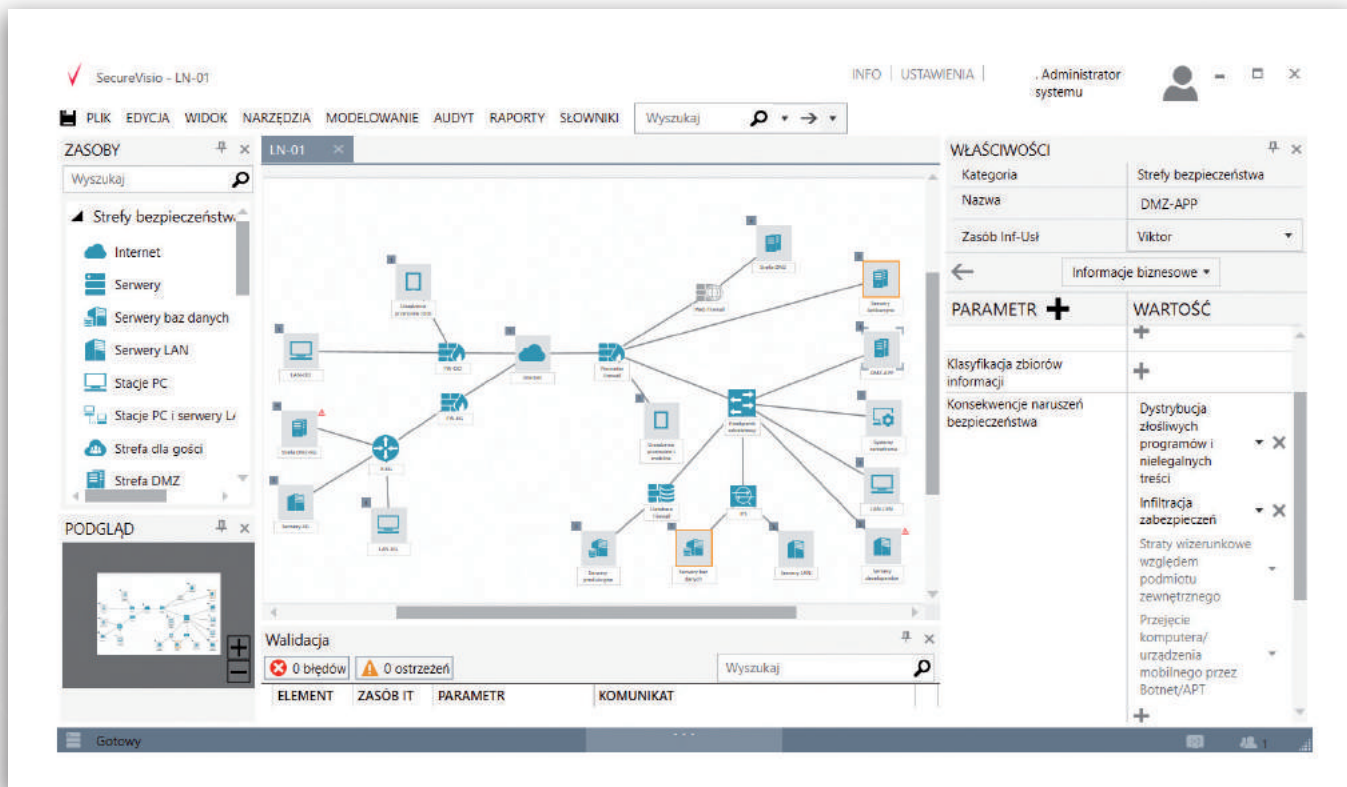
Załącz incydent na

`{Snort: kategoria Web Application Attack}`
AND
`{Zagrozenie serwera webowego}`

Rys. 1. SecureVisio™ – Edytor reguł bezpieczeństwa

Elektroniczna dokumentacja IT

Głównym komponentem SecureVisio™ jest interaktywna, elektroniczna dokumentacja sieci, systemów i zabezpieczeń IT wyposażona w graficzne narzędzia do edycji, przeszukiwania i analizy danych istotnych dla bezpieczeństwa organizacji. Funkcja Asset Discovery umożliwia automatyczne wykrywanie, rozpoznawanie oraz dokumentowanie systemów IT.



Rys. 2. SecureVisio™ – widok mapy logicznej

Ekspert bezpieczeństwa IT „z pudełka”

System wspiera decyzje użytkowników związane z zarządzaniem i monitorowaniem bezpieczeństwa dzięki zaimplementowanej bazie wiedzy eksperckiej, pełniącej rolę zespołu ekspertów z różnych obszarów bezpieczeństwa. Dostarcza im informacji na temat efektywności zastosowanych zabezpieczeń lokalnych i sieciowych w przeciwdziałaniu różnym metodom włamań i ataków oraz wiele innych informacji istotnych w zarządzaniu bezpieczeństwem.

Modelowanie scenariuszy włamań

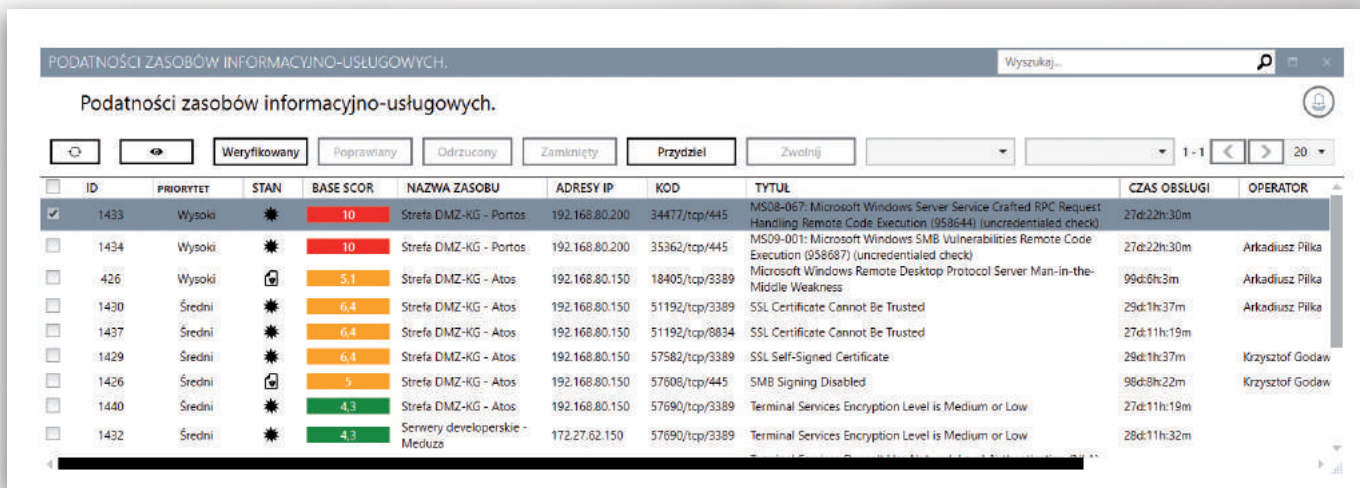
System posiada zaimplementowane funkcje modelowania zagrożeń i audytowania bezpieczeństwa względem wykrytych lub potencjalnych wektorów ataków. Pozwala zwizualizować i przeanalizować zagrożenia dowolnego zasobu względem innego prezentując jednocześnie ryzyko i konsekwencje przełamania zabezpieczeń.

Translator bezpieczeństwa IT dla biznesu

Rozwiązanie problemu komunikacji podczas obsługi incydentów bezpieczeństwa oraz przy codziennych działaniach IT.

Biznesowa ocena podatności

SecureVisio™ Identyfikuje podatności (luki bezpieczeństwa) w systemach IT odczytując je na bieżąco z bazy CVE® oraz poprzez integrację ze skanerami podatności tworzy harmonogramy skanowania, a następnie je wykonuje. System automatycznie analizuje ważności podatnych systemów IT dla organizacji oraz informacje techniczne związane z tymi zagrożeniami (CVSS) wyznaczając dla podatnych systemów odpowiednie priorytety.



ID	PRIORYTET	STAN	BASE SCOR	NAZWA ZASOBU	ADRESY IP	KOD	TYTUŁ	CZAS OBSŁUGI	OPERATOR
1433	Wysoki	✱	10	Strefa DMZ-KG - Portos	192.168.80.200	34477/tcp/445	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (unauthenticated check)	27d:22h:30m	
1434	Wysoki	✱	10	Strefa DMZ-KG - Portos	192.168.80.200	35362/tcp/445	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (unauthenticated check)	27d:22h:30m	Arkadiusz Piłka
426	Wysoki	✱	5.1	Strefa DMZ-KG - Atos	192.168.80.150	18405/tcp/3389	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	99d:0h:3m	Arkadiusz Piłka
1430	Średni	✱	6.4	Strefa DMZ-KG - Atos	192.168.80.150	51192/tcp/3389	SSL Certificate Cannot Be Trusted	29d:1h:37m	Arkadiusz Piłka
1437	Średni	✱	6.4	Strefa DMZ-KG - Atos	192.168.80.150	51192/tcp/8834	SSL Certificate Cannot Be Trusted	27d:11h:19m	
1429	Średni	✱	6.4	Strefa DMZ-KG - Atos	192.168.80.150	57582/tcp/3389	SSL Self-Signed Certificate	29d:1h:37m	Krzysztof Godaw
1426	Średni	✱	5	Strefa DMZ-KG - Atos	192.168.80.150	57608/tcp/445	SMB Signing Disabled	98d:8h:22m	Krzysztof Godaw
1440	Średni	✱	4.3	Strefa DMZ-KG - Atos	192.168.80.150	57690/tcp/3389	Terminal Services Encryption Level is Medium or Low	27d:11h:19m	
1432	Średni	✱	4.3	Serwery rozwojowe - Meduza	172.27.62.150	57690/tcp/3389	Terminal Services Encryption Level is Medium or Low	28d:11h:32m	

Rys. 3. SecureVisio™ – Lista podatności

Zautomatyzowany SOC

SecureVisio™ monitoruje logi w trybie 24/7 oraz koordynuje działania w SOC poprzez scenariusze obsługi incydentów. Integruje się oraz koreluje informacje z SIEM oraz innych systemów zabezpieczeń, skanerów podatności oraz bazy CVE. Wykorzystanie SecureVisio™ automatyzuje pracę w SOC, zwiększając jego efektywność działania, co pozwoli skutecznie uniknąć naruszeń bezpieczeństwa.

Adaptacyjne scenariusze obsługi

SecureVisio™ zarządza scenariuszami obsługi podatności oraz incydentów bezpieczeństwa, które są uruchamiane po spełnieniu zdefiniowanych warunków oraz budowane w zależności od kontekstu przebiegu (workflow). W ramach scenariuszy użytkownicy mają dostępny szereg wbudowanych akcji m. in. edycję dokumentów z rejestrem zmian, wysyłanie powiadomień, zmianę operatora, wykonanie skryptu czy zlecenie zadań.

WDROŻENIE TRWA 1 – 3 MIESIĘCY

ZWROT Z INWESTYCJI 3 – 6 MIESIĘCY

NAJLEPSZY SERWIS – NOWE WERSJE PRODUKTU W RAMACH SERWISU

WIDOCZNE EFEKTY W PIERWSZYM DNIU PO WDROŻENIU

CENA ADEKWATNA DO WIELKOŚCI PRZEDSIĘBIORSTWA I WDROŻENIA