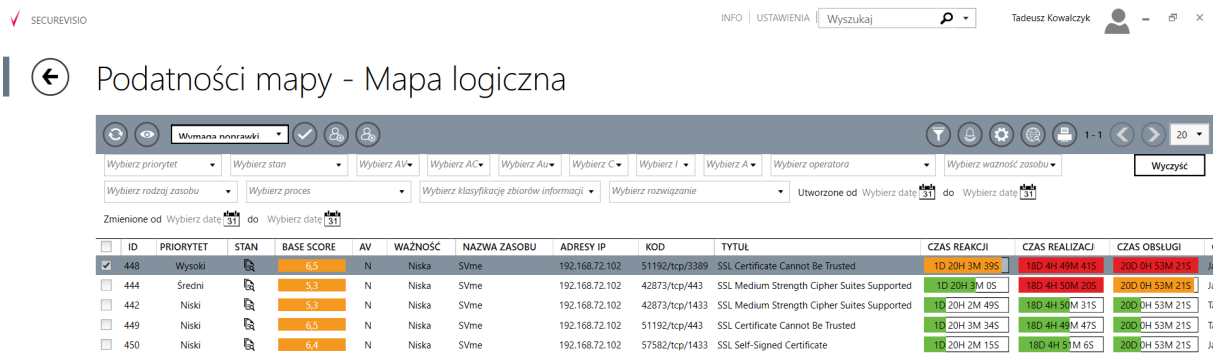
Techniczne możliwości Platformy Zarządzania Podatnościami SecureVisio™: Jak zwiększyć użyteczność skanerów podatności?

Skanery podatności takie jak: OpenVAS[1], Tenable Nessus[2] czy Rapid7 Nexpose[3] służą wykrywaniu podatności (tzw. dziur bezpieczeństwa), zgodnie ze zdefiniowanym wcześniej harmonogramem. Poniżej zostały wymienione główne narzędzia SecureVisio, które rozszerzają funkcjonalność i użyteczność skanerów podatności w procesie zarządzania bezpieczeństwem organizacji.

1. Workflow uporządkowujący pracę osób odpowiedzialnych za zarządzanie podatnościami.

SecureVisio zapewnia zarządzanie obsługą podatności poprzez Workflow umożliwiając m.in. przydzielenie obsługi określonej osobie, zmianę statusu, wykonanie akcji (np. skrypt do aktualizacji/weryfikacji podatności), uruchomienie narzędzi, aktualizację bazy wiedzy czy dokumentów oraz definiowanie warunków przejścia, zarówno kontekstowych jak i związanych z interakcją użytkownika.

Konsola rozwiązania umożliwia zaawansowane sortowanie oraz przeszukiwanie listy podatności po wszystkich wartościach zdefiniowanych w kolumnach obejmujących m.in. priorytet techniczny (CVSS Score) oraz biznesowy. Dodatkowo, dzięki zaawansowanym filtrom możemy zawęzić kryterium wyszukiwania m.in. o określony proces biznesowy czy kategorię danych np.: dane osobowe.[4]

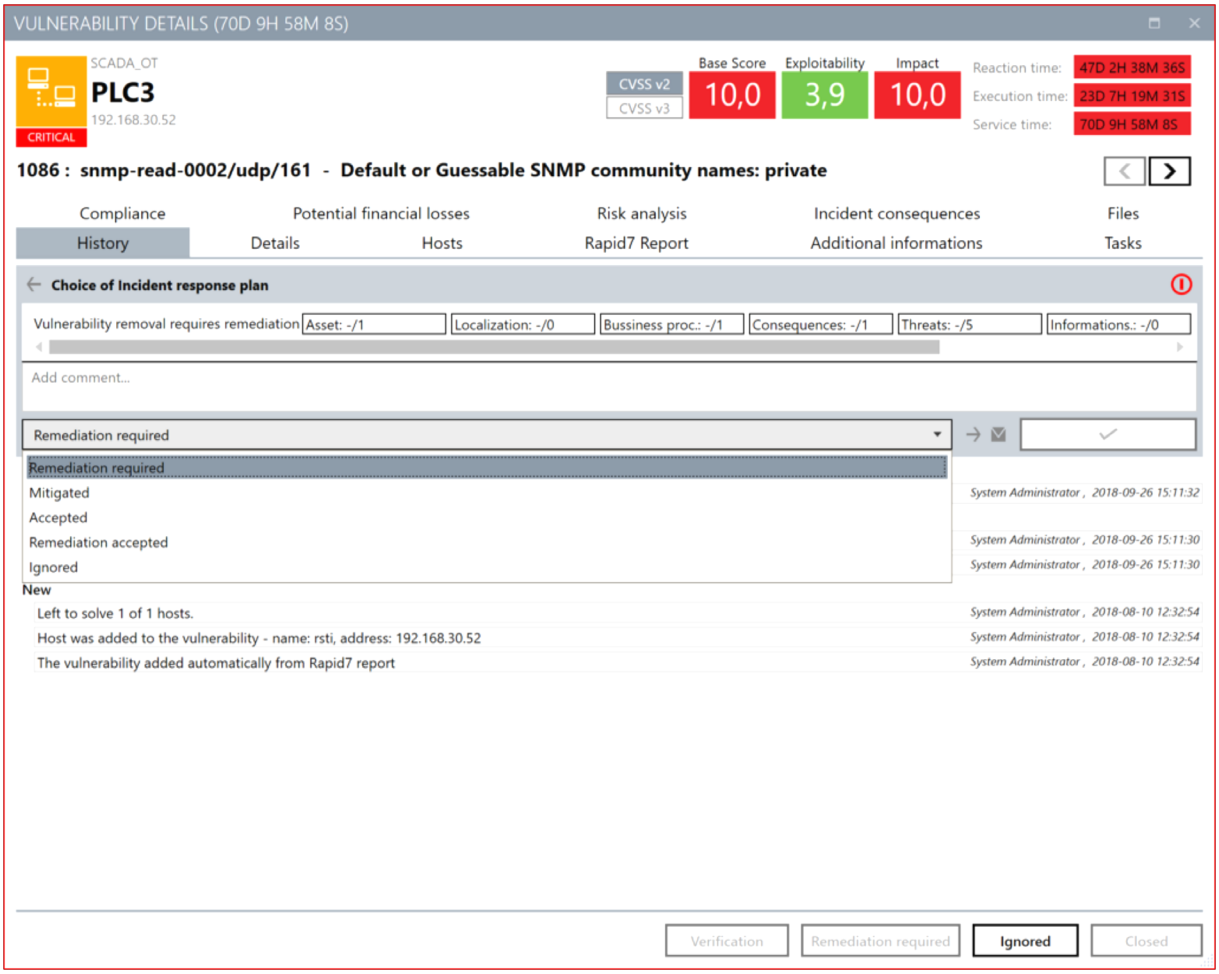


ID	PRIORYTET	STAN	BASE SCORE	AV	WAŻNOŚĆ	NAZWA ZASOBU	ADRESY IP	KOD	TYTUŁ	CZAS REAKCJI	CZAS REALIZACJ	CZAS OBSŁUGI
448	Wysoki		6,5	N	Niska	SVme	192.168.72.102	51192/tcp/3389	SSL Certificate Cannot Be Trusted	1D 20H 3M 39S	18D 4H 49M 41S	20D 0H 53M 21S
444	Średni		5,3	N	Niska	SVme	192.168.72.102	42873/tcp/443	SSL Medium Strength Cipher Suites Supported	1D 20H 3M 0S	18D 4H 50M 20S	20D 0H 53M 21S
442	Niski		5,3	N	Niska	SVme	192.168.72.102	42873/tcp/1433	SSL Medium Strength Cipher Suites Supported	1D 20H 2M 49S	18D 4H 50M 31S	20D 0H 53M 21S
449	Niski		6,5	N	Niska	SVme	192.168.72.102	51192/tcp/443	SSL Certificate Cannot Be Trusted	1D 20H 3M 34S	18D 4H 49M 47S	20D 0H 53M 21S
450	Niski		6,4	N	Niska	SVme	192.168.72.102	57582/tcp/1433	SSL Self-Signed Certificate	1D 20H 2M 15S	18D 4H 51M 6S	20D 0H 53M 21S

[1] OpenVAS, http://www.openvas.org
[2] Tenable Nessus, https://www.tenable.com/products/nessus/nessus-professional
[3] Rapid7 Nexpose, https://www.rapid7.com/products/nexpose/
[4] *Niektóre skanery podatności posiadają możliwość definiowania listy zadań do wykonania w celu usunięcia podatności. Narzędzia te nie oferują jednak możliwości interaktywnej pracy dla zespołu ludzi i w praktyce wymagają integracji z zewnętrznym systemem ticketowym, a tym samym oznaczają równoczesną pracę na dwóch konsolach (system ticketowy nie posiada informacji dotyczących przedmiotu analizy ani zintegrowanych narzędzi, co wpływa też negatywnie na efektywność procesu).*

2. Playbook automatyzujący i ułatwiający pracę osób odpowiedzialnych za zarządzanie podatnościami.

Playbook oferuje gotowe do natychmiastowego użycia narzędzia obsługi incydentów, m.in. bibliotekę skryptów SSH i WMI/PowerShell do analizy i wiarygodnej eliminacji *false positive*.



3. Swoboda wyboru skanera podatności – platforma SecureVisio umożliwia wybór skanera (m.in. OpenVAS, Tenable Nessus, Rapid7 Nexpose) lub używanie równocześnie wielu skanerów różnych dostawców.

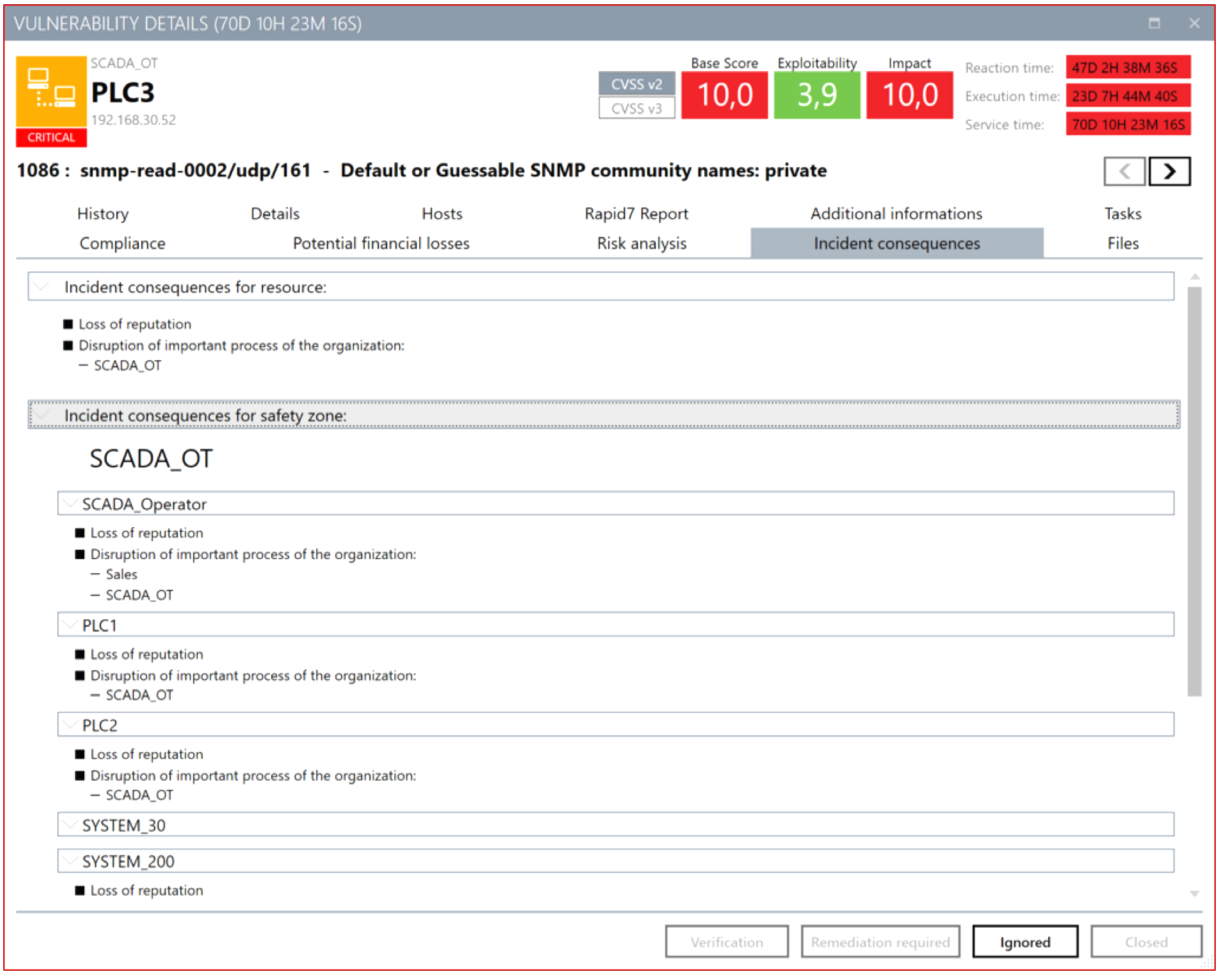
Organizacja nie jest skazana wyłącznie na jednego producenta narzędzi zarządzania podatnościami. SecureVisio w ramach wbudowanej platformy do zarządzania podatnościami, pozwala korzystać z różnych skanerów komercyjnych oraz open-source (istnieje możliwość swobodnej zmiany i dodawania skanerów).

4. Konsola zarządzania i raporty dostępne jednocześnie w polskiej i angielskiej wersji językowej.

SecureVisio pozwala m.in. wygenerować raporty w języku polskim, co może być szczególnie ważne w sytuacji kontroli wynikającej z RODO, Rekomendacji D KNF czy Ustawy o krajowym systemie cyberbezpieczeństwa.

5. Priorytet techniczny (CVSS Score) rozszerzony o priorytet biznesowy oraz niebezpieczeństwo (konsekwencje) wykorzystania podatności na szkodę organizacji.

Dzięki połączeniu priorytetu technicznego z biznesowym, osoby zarządzające podatnościami są w stanie natychmiastowo rozpoznać i przystąpić do działania nad kluczowymi lukami bezpieczeństwa (operatorzy dostrzegają możliwe skutki wykorzystania wspomnianych podatności np. ryzyko kradzieży danych osobowych i konsekwencje RODO, ryzyko zablokowania usług kluczowych objętych Ustawą o krajowym systemie cyberbezpieczeństwa).

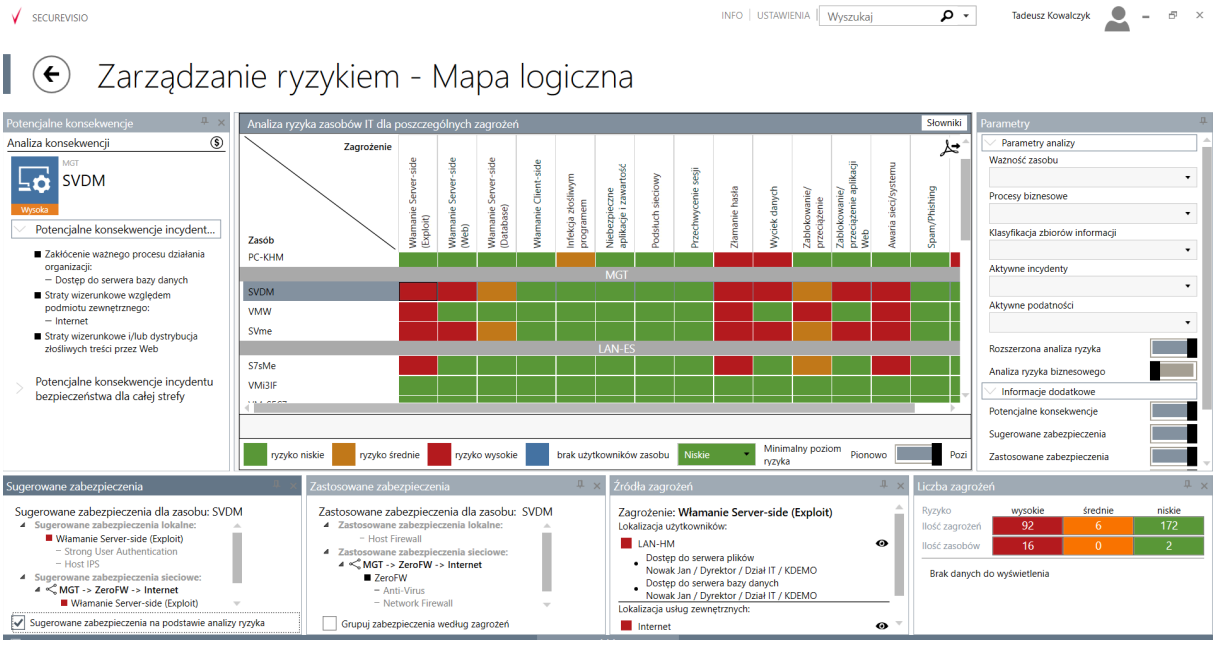


Niektóre skanery posiadają możliwość ręcznego dopisywania do adresów IP tagów, oznaczających ich ważność dla organizacji. Takie działania wymagają niestety wykorzystania zewnętrznego źródła wiedzy o takich zasobach oraz dokonania ręcznej synchronizacji z tymże źródłem.

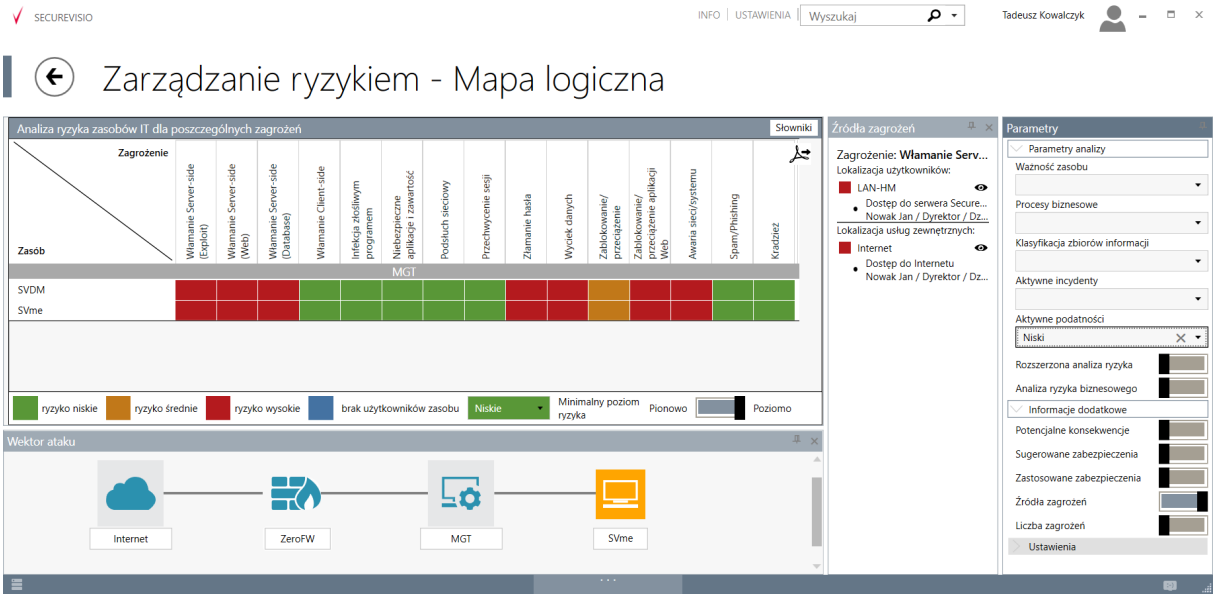
SecureVisio wykonuje automatycznie operację Business Impact Analysis (BIA) dla systemów IT gdzie wykryto podatności, a także systemów IT, które znajdują się w tej samej strefie bezpieczeństwa (cyberprzestępcy, po włamaniu się do systemu IT mają ułatwione możliwości atakowania innych systemów, znajdujących się w ramach jednej strefy bezpieczeństwa). SecureVisio wykonuje także automatyczne szacowanie ryzyka i przygotowuje jego wizualizację w kontekście potencjalnych wektorów ataków z poziomu zasobu, na którym została zidentyfikowana podatność.

6. Automatyczne szacowanie ryzyka (wg metodyki ISO-27005) i prezentacja wielkości ryzyka w odniesieniu do różnych typów zagrożeń jako podstawa oceny skuteczności zabezpieczeń, zapobiegających wykorzystaniu podatności przez cyberprzestępców.

SecureVisio wskazuje kierunek występowania największego prawdopodobieństwa ataku, przedstawia potencjalne straty biznesowe dla organizacji oraz rekomenduje wzmocnienie zabezpieczeń na podstawie bazy wiedzy eksperckiej.

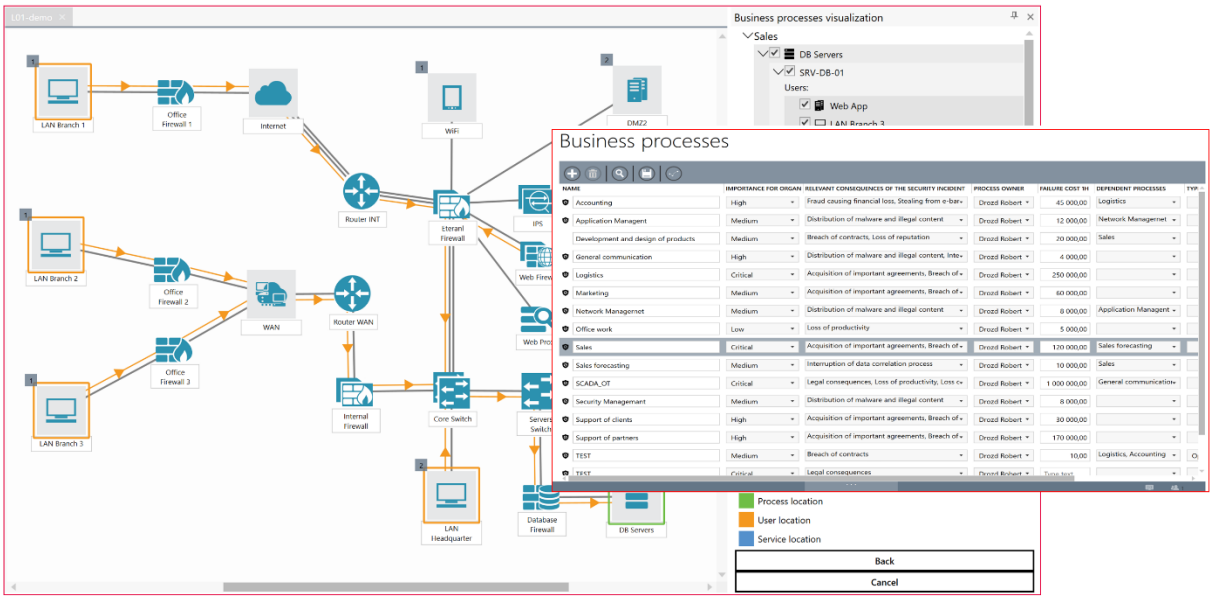


7. Graficzna prezentacja potencjalnych ścieżek ataków ułatwia rzeczywistą ocenę ryzyka ich wystąpienia w oparciu o wykorzystanie podatności z różnych obszarów sieci.

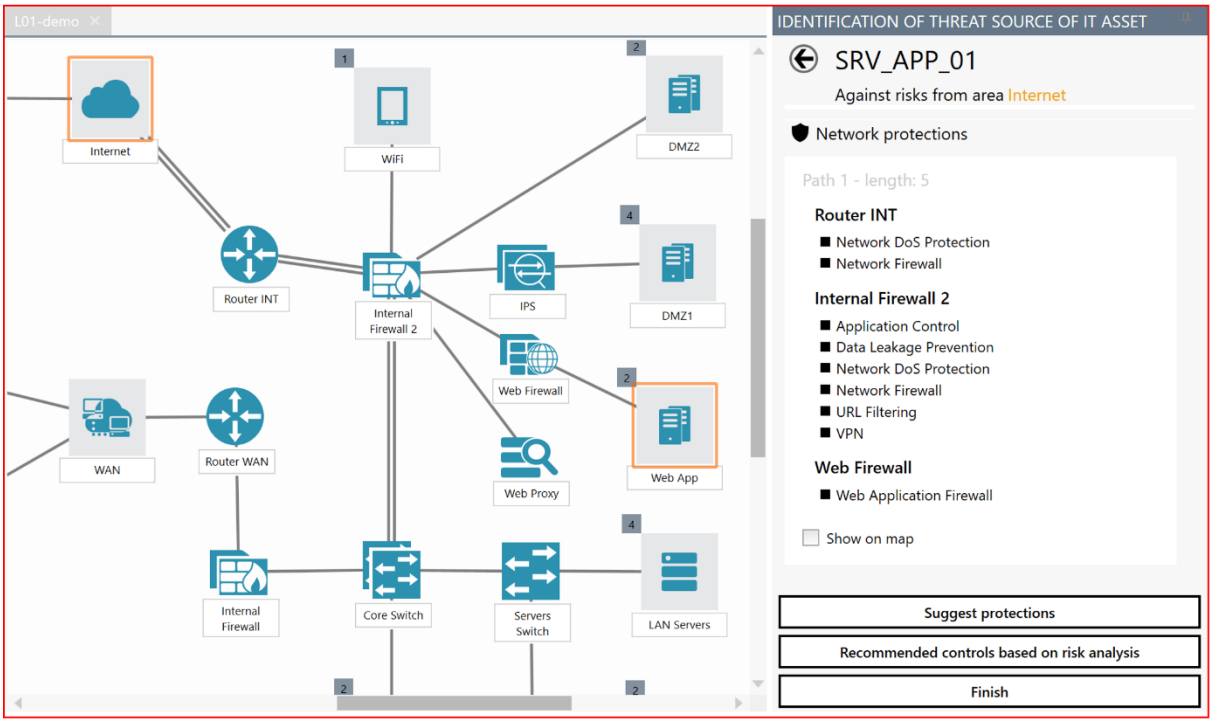


8. Wizualizacja na mapie sieci procesów biznesowych, zagrożonych przez podatności uławia podejmowanie decyzji, dotyczących minimalizacji realnego zagrożenia dla organizacji.

Dostępny w SecureVisio Kreator Procesów Biznesowych umożliwia sprawne definiowanie procesów i ich dowiązane do systemów IT na mapie sieci. Automatyczne szacowanie i priorytetyzacja biznesowa podatności odbywa się na podstawie kryterium ważności danych oraz procesów biznesowych, znajdujących się w określonych systemach IT lub przez nie wspieranych.

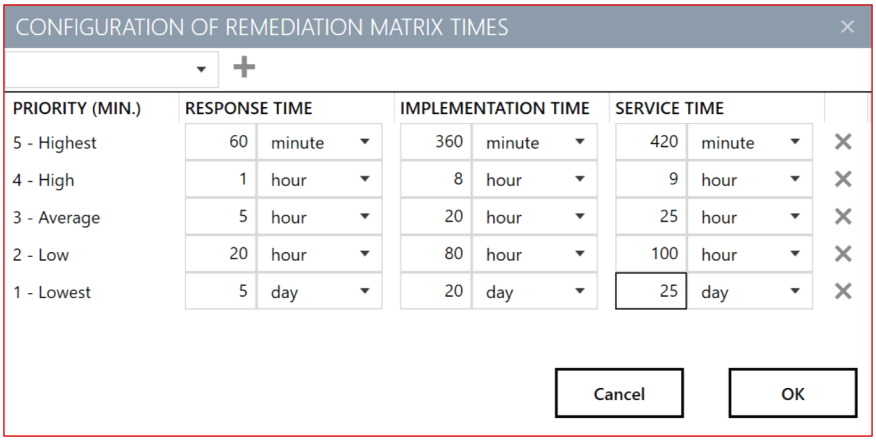


SecureVisio ukazuje zabezpieczenia dostępne dla wskazanych systemów IT, ułatwiając podjęcie realnej oceny stanu bezpieczeństwa systemów IT w obszarach występowania podatności.

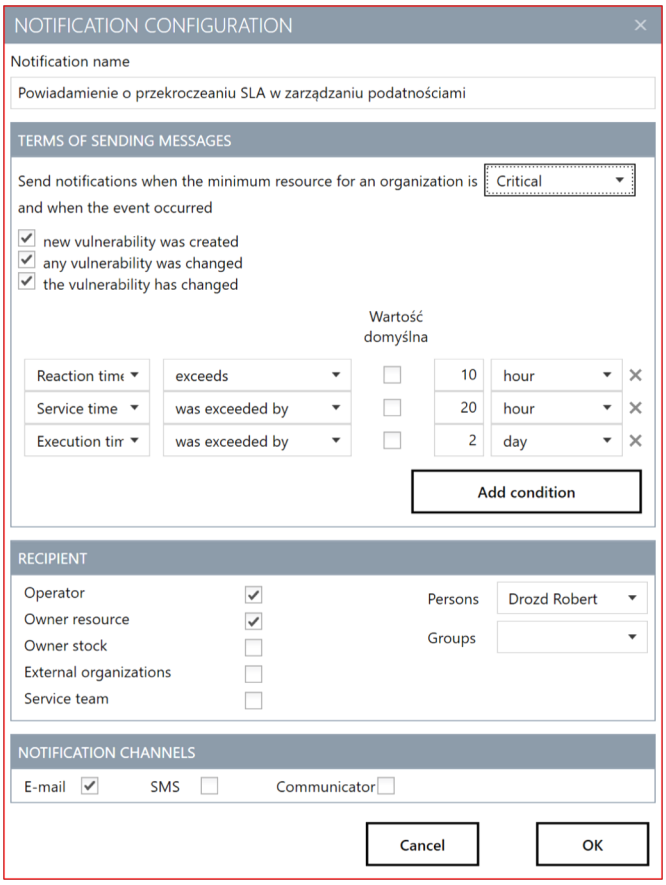


9. Definiowanie czasów SLA w procesie obsługi podatności względem biznesowego ryzyka podatności dla organizacji.

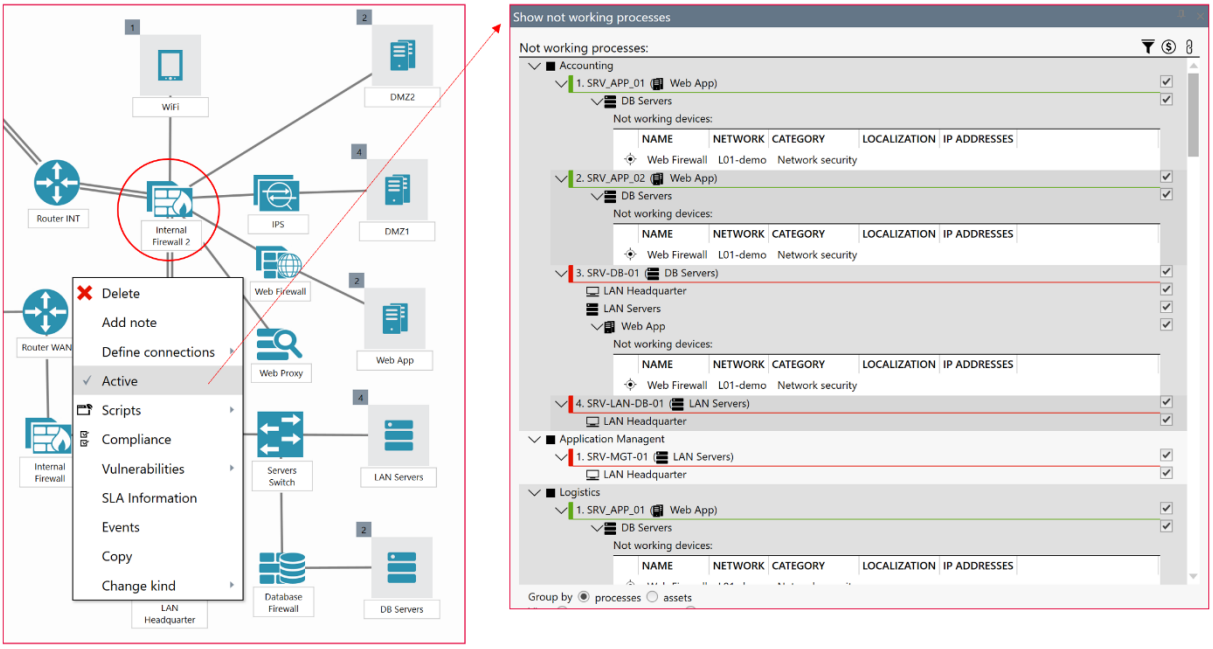
SecureVisio na bieżąco sprawdza spełnienie SLA i umożliwia automatyczne powiadamianie osób odpowiedzialnych.



10. Automatyczne powiadamianie osób odpowiedzialnych o nowych podatnościach krytycznych dla biznesu organizacji (np. zagrożenia dla krytycznych procesów biznesowych, zagrożenie wycieku danych osobowych i innych wrażliwych danych) oraz przekroczeniu SLA w obsłudze podatności.



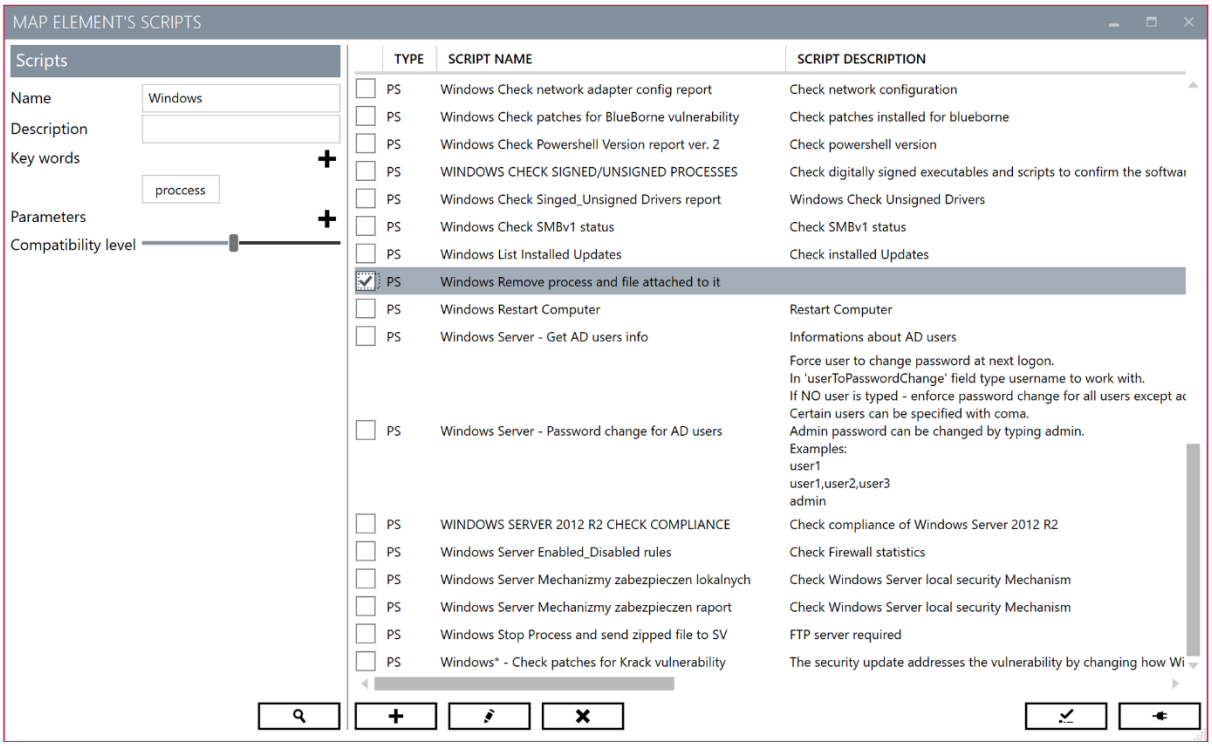
11. Symulacja konsekwencji biznesowych dla organizacji w razie wykorzystania przez cyberprzestępców podatności do zablokowania określonych urządzeń w sieci.



12. Obliczanie i wizualizacja wskaźników efektywności oraz wskaźników ryzyka biznesowego w procesie zarządzania podatnościami.

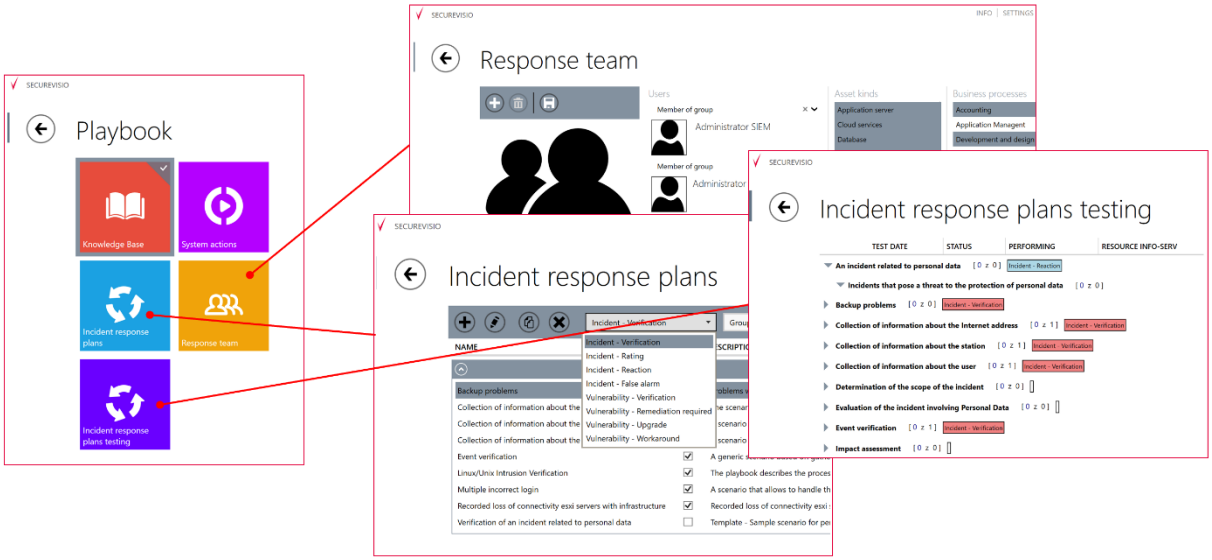
SecureVisio na bieżąco oblicza wskaźniki Key Performance Indicators (KPI) i Key Risk Indicators (KRI), informujące osoby odpowiedzialne o stanie obsługi podatności oraz trendach wzrostu/spadku ryzyka (np. wzrost podatności w systemach IT wspomagających krytyczne procesy biznesowe).

13. Biblioteka skryptów SSH i WMI/PowerShell do analizy i wiarygodnej eliminacji false positive.



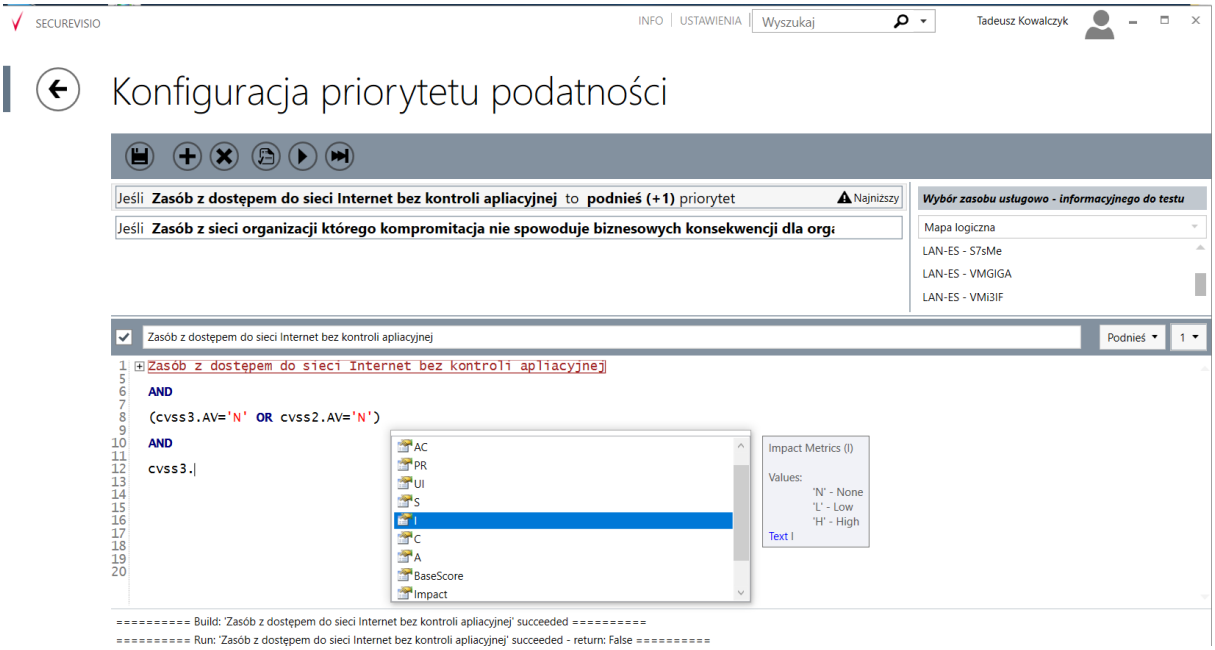
14. Narzędzia definiowania organizacji zespołu obsługi podatności i rozszerzenia jego zadań o zarządzanie incydentami.

SecureVisio oferuje gotowy do użycia Playbook do zarządzania podatnościami, a także Playbook do zarządzania incydentami.



15. Zawansowane reguły priorytetów

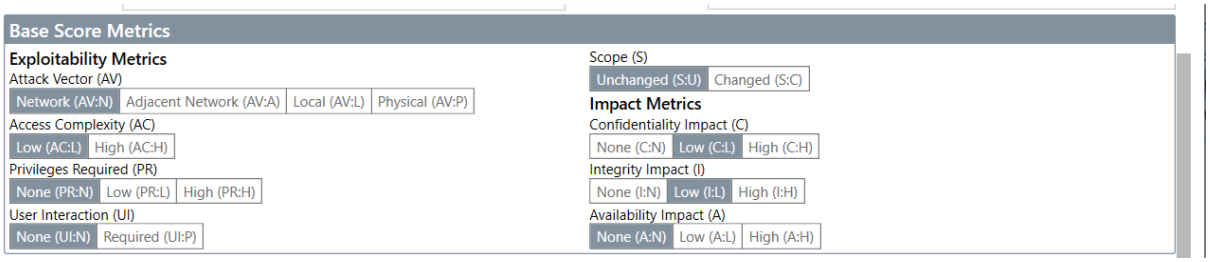
SecureVisio w oparciu o zgromadzony lub uzupełniony kontekst organizacji umożliwia zbudowanie reguł, które pozwalają zdefiniować warunki obniżenia lub podwyższenia priorytetu podatności, bądź nadanie mu określonej wartości. Podczas importu z silnika skanera wyniki skanowania są poddawane regułom SIEM względem każdej wykrytej podatności, modyfikując jej priorytet.



Reguły mają dostęp do danych związanych z podatnościami (wsparcie dla obu wersji CVSS2 i CVSS3), dzięki czemu istnieje możliwość utworzenia reguł, które dokonają odpowiedniej modyfikacji priorytetu w przypadku, gdy wykorzystanie podatności wymaga np.:

- uwierzytelnienia (funkcja: cvss3.PR)
- dostępu lokalnego lub sieciowego (funkcja: cvss3.AC)
- wpływu na dostępność zasobu (funkcja: A)

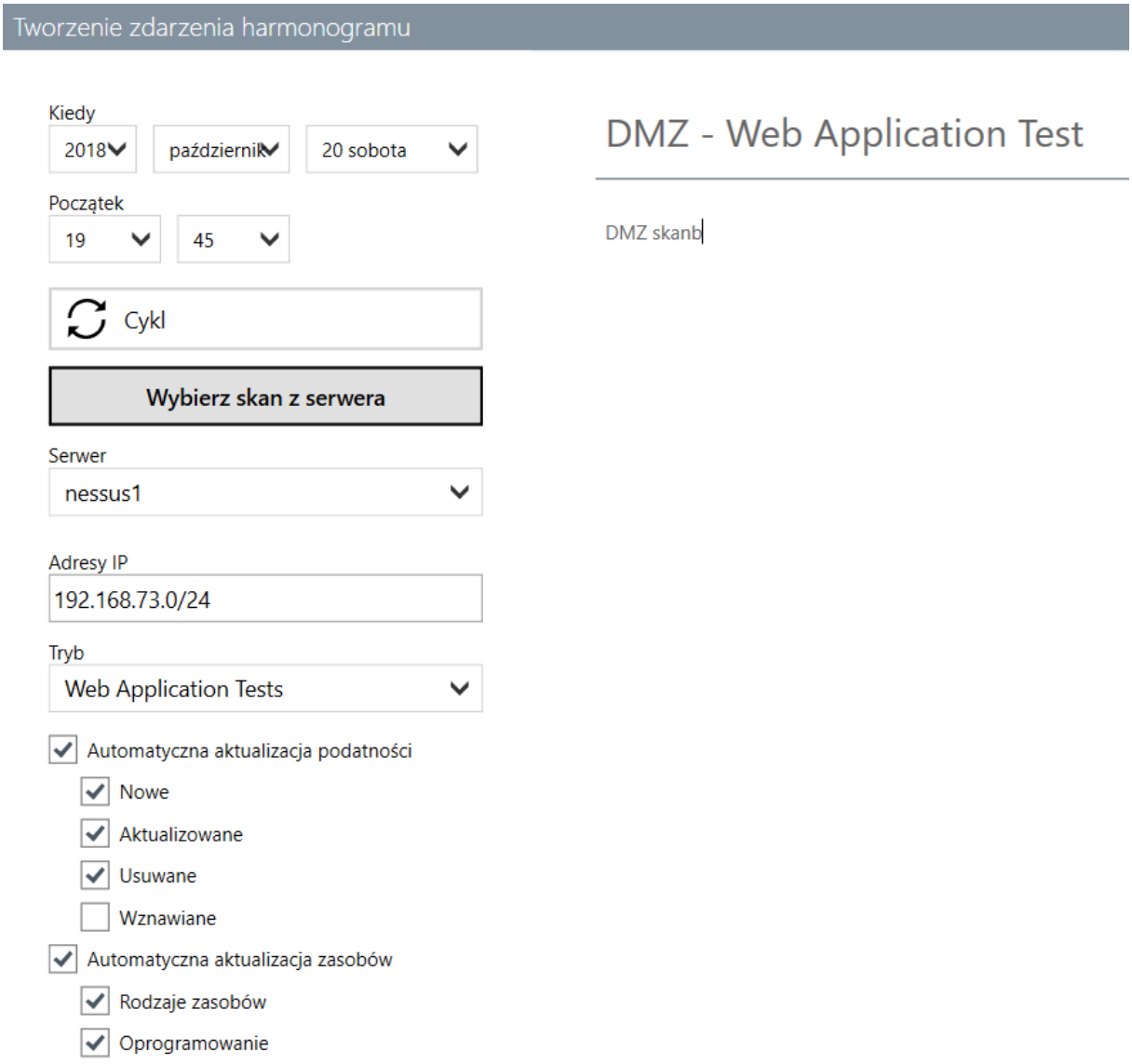
Pozostałe funkcje związane z CVSS ver3, które mogą wpłynąć na priorytet podatności i zostać wykorzystane w regułach, są dostępne z poziomu każdej podatności w zakładce Szczegóły (sekcja Base Score Metrics):



Budując reguły priorytetów w SecureVisio, organizacja ma również dostęp do dowolnej wartości elektronicznej dokumentacji oraz wyników działania wbudowanych algorytmów, dzięki czemu istnieje możliwość uzupełnienia kontekstu priorytetu podatności o inne zależności (np. priorytet może zostać podniesiony gdy podatność znajduje się na dowolnym serwerze bazy danych, której operatorzy pracują na stacjach z dostępem do sieci Internet).

16. Zawsze aktualna lista podatności

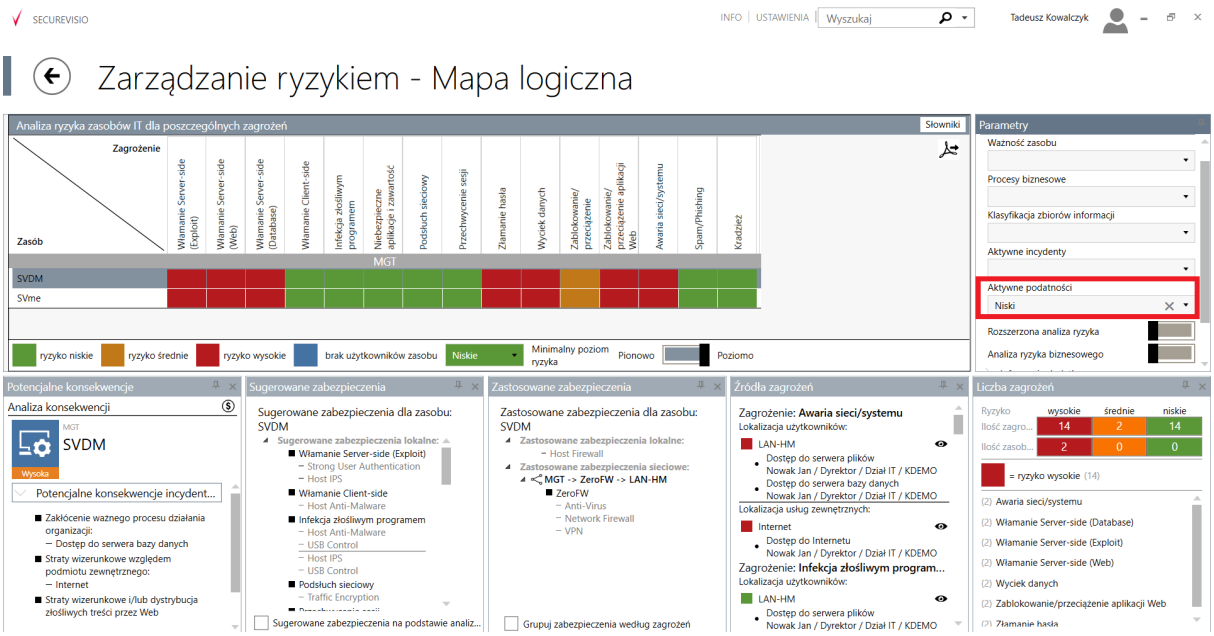
SecureVisio utrzymuje aktualną listę podatności bez względu na zastosowany silnik skanujący. W przypadku skanowania włączonego zasobu oraz zastosowania takiego samego typu skanu, który wcześniej wykrył daną podatność, system usuwa ją z listy aktualnych podatności poprzez zmianę jej statusu. Zachowanie jest konfigurowalne w oknie harmonogramu skanowania dla każdego wyniku skanowania oraz importu wyników skanowania z plików (checkbox „Usuwanie" dla automatycznej aktualizacji listy podatności):



Dodatkowo, bazując na wyniku skanowania, SecureVisio potrafi uaktualniać listę oprogramowania zidentyfikowanego na zasobach oraz ich rodzaje w sekcji „Automatyczna aktualizacja zasobów".

17. Wpływ podatności na automatyczne szacowanie ryzyka

Wykorzystując panel zarządzania ryzykiem można dokonać analizy ryzyka dla zasobów, które posiadają aktualne podatności. Wystarczy wybrać filtr „Aktywne podatności” wraz z ich priorytetem:



18. Wpływ podatności na zdarzenia bezpieczeństwa

SecureVisio pozwala na integrację z dowolnymi systemami zabezpieczeń m.in. systemami SIEM, urządzeniami, aplikacjami, bazami danych, e-mail’ami oraz systemami operacyjnymi. Wszystkie źródła zintegrowane z SecureVisio poddawane są regułom korelacyjnym, w których zdarzenia techniczne zostają poddane regułom uwzględniającym kontekst biznesowy zdarzenia (np.: automatyczne szacowanie ryzyka, analiza zagrożeń oraz potencjalnych konsekwencji dla organizacji).

Z poziomu reguł korelacyjnych organizacja otrzymuje dostęp do informacji o podatnościach. Umożliwia to dokonanie konkretnej weryfikacji, np. określenie czy zdarzenie dotyczy podatnego zasobu lub czy zasób ten może zostać skompromitowany poprzez sieć. Poniższy przykład przedstawia regułę wykorzystującą wspomnianą zależność.

Reguła - An intruder on a mobile device