

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

Skanery podatności takie jak: OpenVAS¹, Tenable Nessus² czy Rapid7 Nexpose³ 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 rozwiązań 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

SECUREVISIO INFO | USTAWIENIA Wyszukaj Tadeusz Kowalczyk

Podatności mapy - Mapa logiczna

ID	PRIORYTET	STAN	BASE SCORE	AV	WAŻNOŚĆ	NAZWA ZASOBU	ADRESY IP	KOD	TYTUŁ	CZAS REAKCJI	CZAS REALIZACJI	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	Sredni		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 26S	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 48M 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*.

VULNERABILITY DETAILS (70D 9H 58M 8S)

SCADA_OT
PLC3
 192.168.30.52
 CRITICAL

Base Score: 10,0
 Exploitability: 3,9
 Impact: 10,0

Reaction time: 47D 2H 38M 36S
 Execution time: 23D 7H 19M 31S
 Service time: 70D 9H 58M 8S

1086 : snmp-read-0002/udp/161 - Default or Guessable SNMP community names: private

Compliance | Potential financial losses | Risk analysis | Incident consequences | Files
 History | Details | Hosts | Rapid7 Report | Additional informations | Tasks

← Choice of Incident response plan

Vulnerability removal requires remediation | Asset: -/1 | Localization: -/0 | Bussiness proc.: -/1 | Consequences: -/1 | Threats: -/5 | Informations.: -/0

Add comment...

Remediation required

- Remediation required
- Mitigated
- Accepted
- Remediation accepted
- Ignored

New

- Left to solve 1 of 1 hosts.
- Host was added to the vulnerability - name: rsti, address: 192.168.30.52
- The vulnerability added automatically from Rapid7 report

System Administrator , 2018-09-26 15:11:32
 System Administrator , 2018-09-26 15:11:30
 System Administrator , 2018-09-26 15:11:30
 System Administrator , 2018-08-10 12:32:54
 System Administrator , 2018-08-10 12:32:54
 System Administrator , 2018-08-10 12:32:54

Verification | Remediation required | Ignored | Closed

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).

VULNERABILITY DETAILS (70D 10H 23M 16S)

SCADA_OT
PLC3
192.168.30.52
CRITICAL

CVSS v2: 10,0
CVSS v3: 3,9
Impact: 10,0

Reaction time: 47D 2H 38M 36S
Execution time: 23D 7H 44M 40S
Service time: 70D 10H 23M 16S

1086 : snmp-read-0002/udp/161 - Default or Guessable SNMP community names: private

History | Details | Hosts | Rapid7 Report | Additional informations | Tasks
Compliance | Potential financial losses | Risk analysis | Incident consequences | Files

Incident consequences for resource:

- Loss of reputation
- Disruption of important process of the organization:
 - SCADA_OT

Incident consequences for safety zone:

SCADA_OT

- SCADA_Operator
 - Loss of reputation
 - Disruption of important process of the organization:
 - Sales
 - SCADA_OT
- PLC1
 - Loss of reputation
 - Disruption of important process of the organization:
 - SCADA_OT
- PLC2
 - Loss of reputation
 - Disruption of important process of the organization:
 - SCADA_OT
- SYSTEM_30
- SYSTEM_200
 - Loss of reputation

Verification | Remediation required | Ignored | Closed

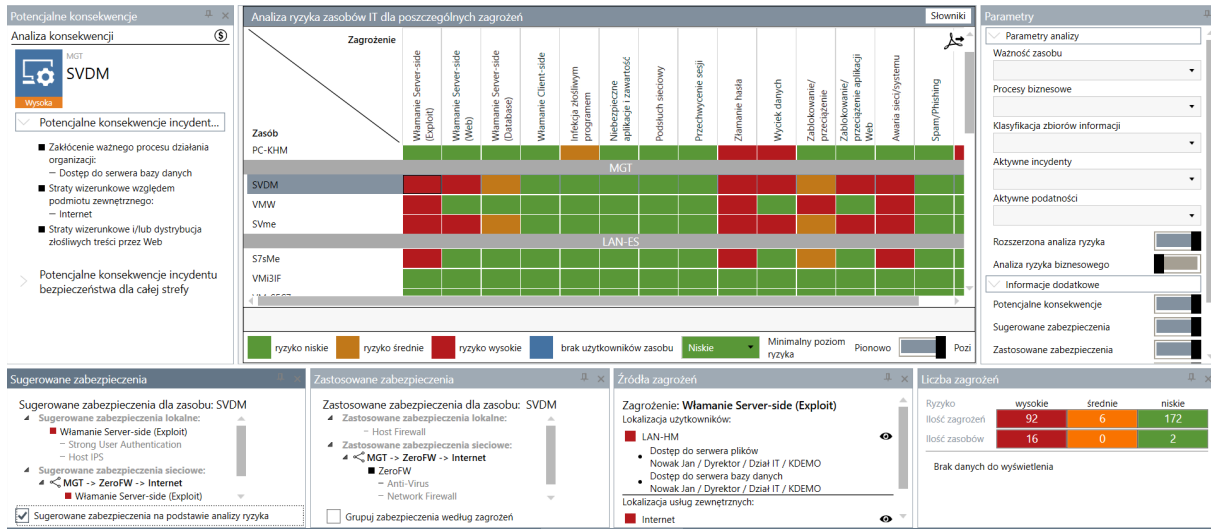
Niektóre skanery posiadają możliwość ręcznego dopisywania do adresów IP tagów, oznaczających ich ważność dla organizacji. Takie działania wymagają niestety wykorzystania zewnętrznego źródła wiedzy o takich zasobach oraz dokonania ręcznej synchronizacji z tymże źródłem.

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.

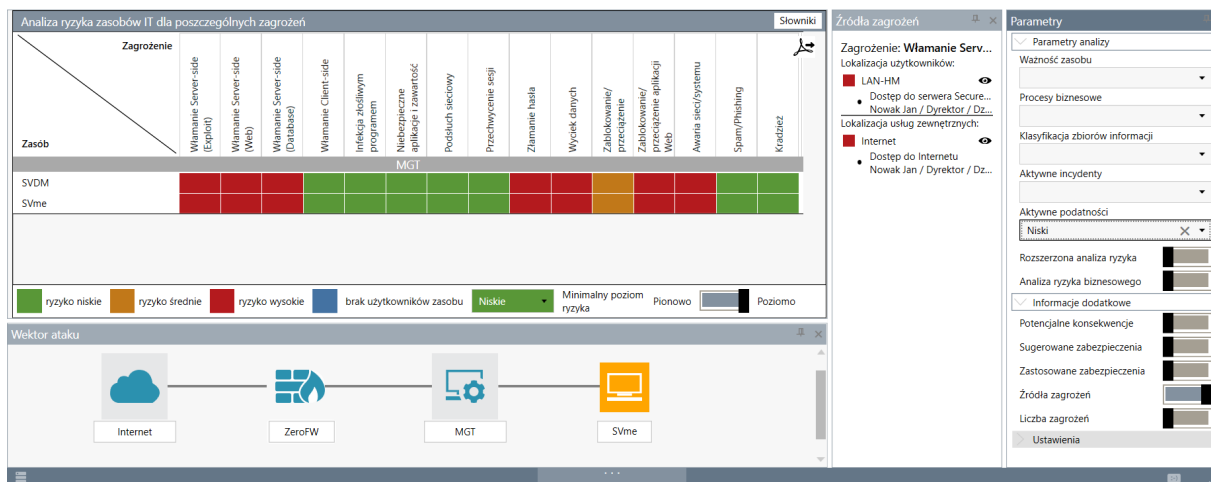
SecureVisio wskazuje kierunek występowania największego prawdopodobieństwa ataku, przedstawia potencjalne straty biznesowe dla organizacji oraz rekomenduje wzmocnienie zabezpieczeń na podstawie bazy wiedzy eksperckiej.

Zarządzanie ryzykiem - Mapa logiczna



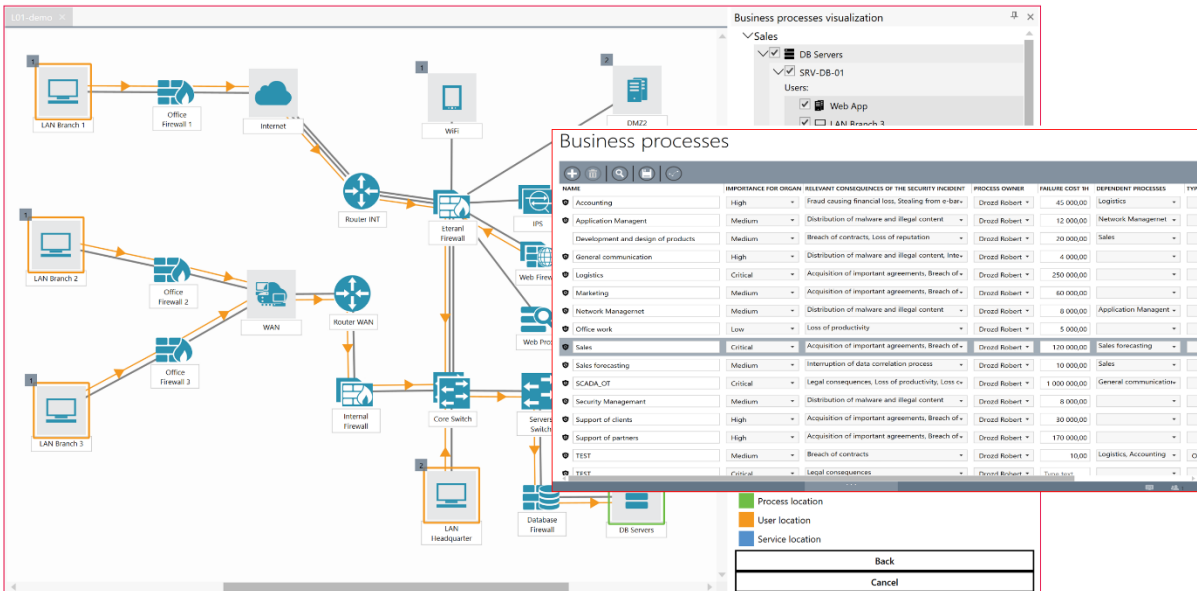
7. Graficzna prezentacja potencjalnych ścieżek ataków ułatwia rzeczywistą ocenę ryzyka ich wystąpienia w oparciu o wykorzystanie podatności z różnych obszarów sieci.

Zarządzanie ryzykiem - Mapa logiczna

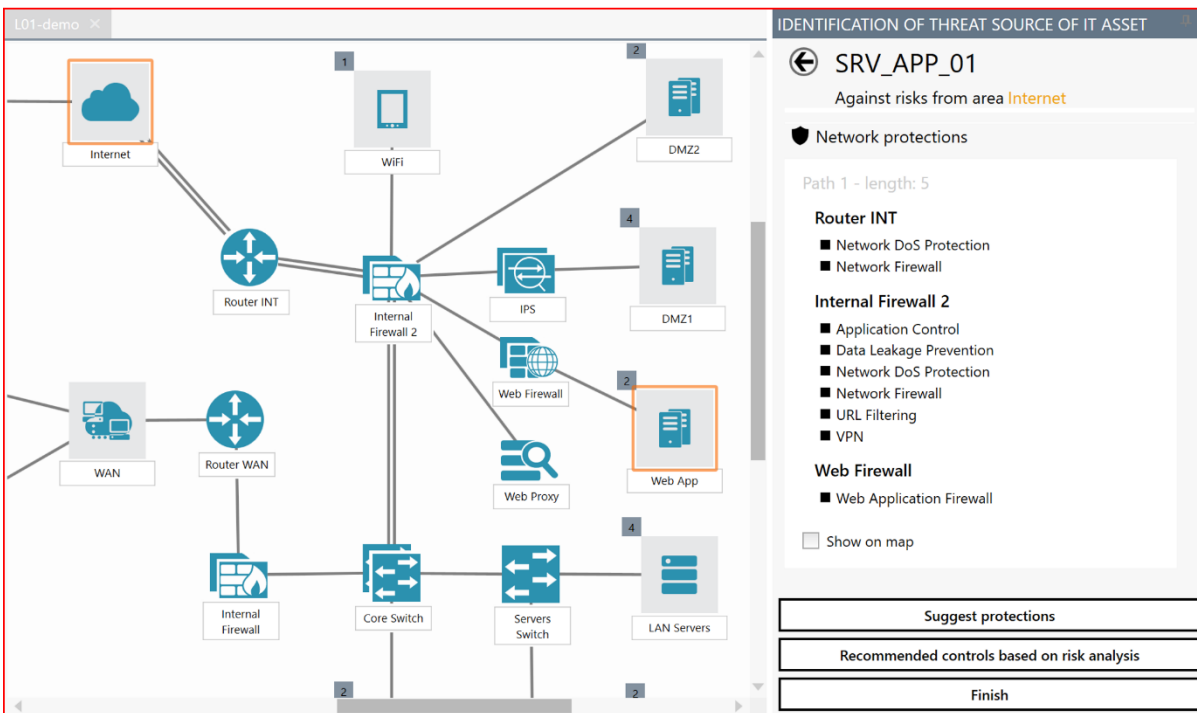


8. Wizualizacja na mapie sieci procesów biznesowych, zagrożonych przez podatności ułatwia podejmowanie decyzji, dotyczących minimalizacji realnego zagrożenia dla organizacji.

Dostępny w SecureVisio Kreator Procesów Biznesowych umożliwia sprawne definiowanie procesów i ich dowiązanie 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.

CONFIGURATION OF REMEDIATION MATRIX TIMES ✕

PRIORITY (MIN.)	RESPONSE TIME	IMPLEMENTATION TIME	SERVICE TIME	
5 - Highest	60 minute	360 minute	420 minute	✕
4 - High	1 hour	8 hour	9 hour	✕
3 - Average	5 hour	20 hour	25 hour	✕
2 - Low	20 hour	80 hour	100 hour	✕
1 - Lowest	5 day	20 day	25 day	✕

Cancel
OK

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.

NOTIFICATION CONFIGURATION ✕

Notification name

TERMS OF SENDING MESSAGES

Send notifications when the minimum resource for an organization is and when the event occurred

new vulnerability was created
 any vulnerability was changed
 the vulnerability has changed

Wartość domyślna

Reaction time	exceeds	<input type="checkbox"/>	10	hour	✕
Service time	was exceeded by	<input type="checkbox"/>	20	hour	✕
Execution time	was exceeded by	<input type="checkbox"/>	2	day	✕

Add condition

RECIPIENT

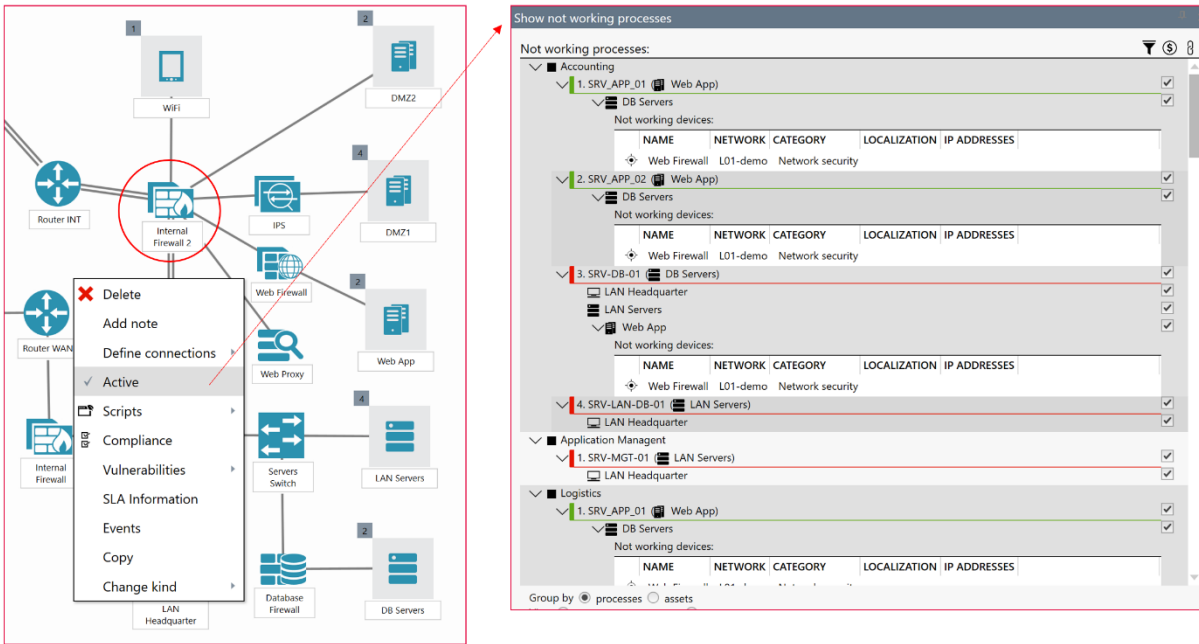
Operator	<input checked="" type="checkbox"/>	Persons	<input type="text" value="Drozd Robert"/>
Owner resource	<input checked="" type="checkbox"/>	Groups	<input type="text"/>
Owner stock	<input type="checkbox"/>		
External organizations	<input type="checkbox"/>		
Service team	<input type="checkbox"/>		

NOTIFICATION CHANNELS

E-mail SMS Communicator

Cancel
OK

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

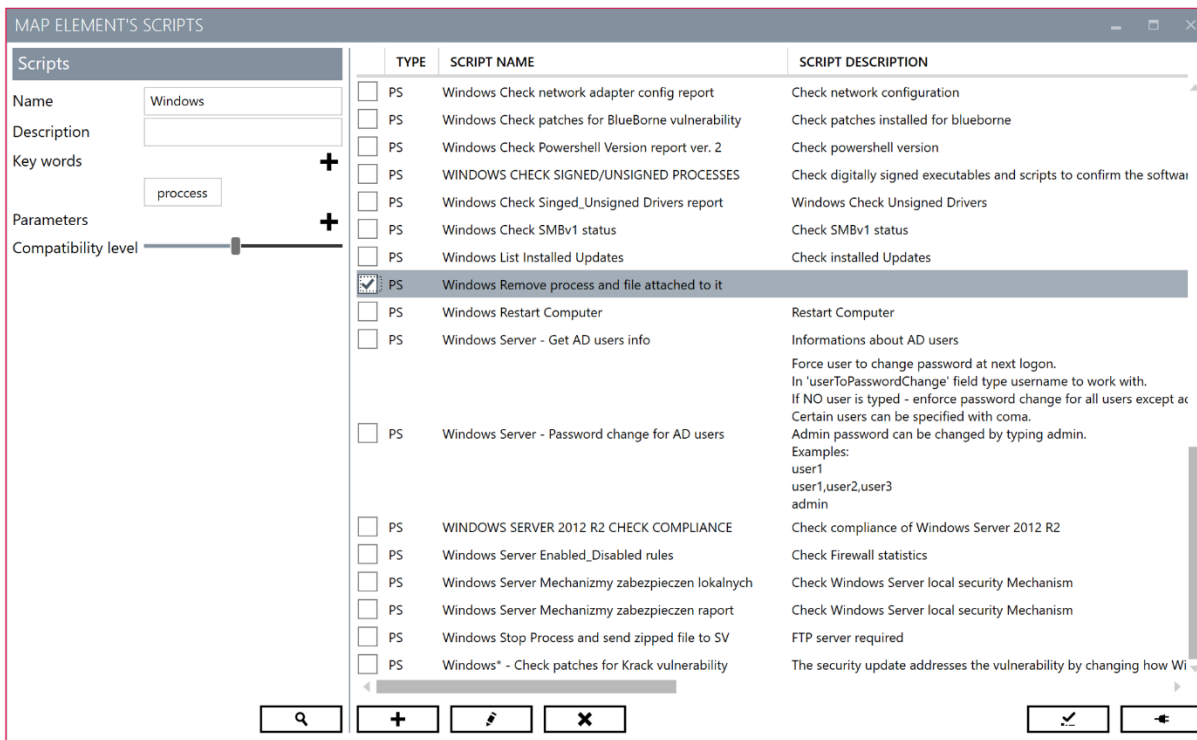


12. Obliczanie i wizualizacja wskaźników efektywności oraz wskaźników ryzyka biznesowego w procesie zarządzania podatnościami.

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).

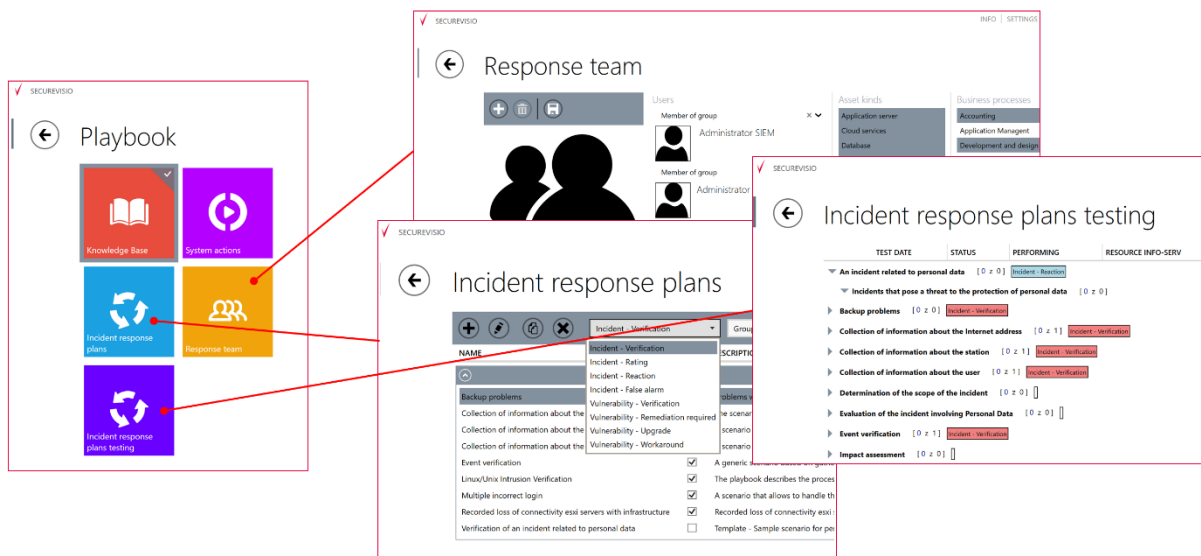


13. Biblioteka skryptów SSH i WMI/PowerShell do analizy i wiarygodnej eliminacji false positive.



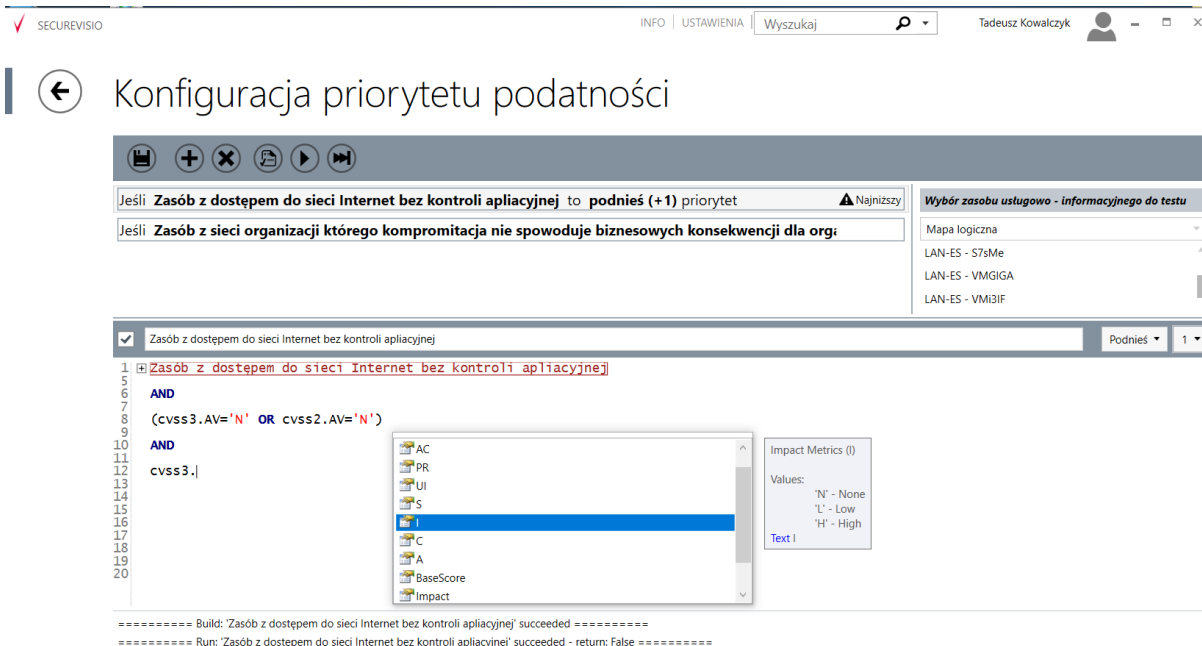
14. Narzędzia definiowania organizacji zespołu obsługi podatności i rozszerzenia jego zadań o zarządzanie incydentami.

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



15. Zawansowane reguły priorytetów

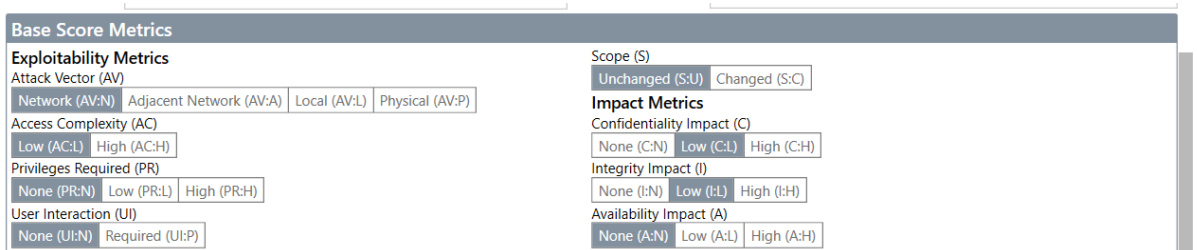
SecureVisio w oparciu o zgromadzony lub uzupełniony kontekst organizacji umożliwia zbudowanie reguł, które pozwalają zdefiniować warunki obniżenia lub podwyższenia priorytetu podatności, bądź nadanie mu określonej wartości. Podczas importu z silnika skanera wyniki skanowania są poddawane regułom SIEM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

Tworzenie zdarzenia harmonogramu

Kiedy

2018▼ październik▼ 20 sobota▼

Początek

19▼ 45▼

 Cykl

Wybierz skan z serwera

Serwer

nessus1▼

Adresy IP

192.168.73.0/24

Tryb

Web Application Tests▼

Automatyczna aktualizacja podatności

- Nowe
- Aktualizowane
- Usuwane
- Wznawiane

Automatyczna aktualizacja zasobów

- Rodzaje zasobów
- Oprogramowanie

DMZ - Web Application Test

DMZ skanb|

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:

The screenshot displays the 'Zarządzanie ryzykiem - Mapa logiczna' (Risk Management - Logical Map) interface. The main area is a risk matrix with 'Zasób' (Asset) on the vertical axis and 'Zagrożenie' (Threat) on the horizontal axis. Assets listed include SVDM and SVme. Threats include Wiązanie Server-side (Exploit), Wiązanie Server-side (Web), Wiązanie Server-side (Database), Wiązanie Client-side, Infekcja złośliwym programem, Niebezpieczne aplikacje i zawartość, Podatność sieciowy, Przechwytywanie sesji, Złamanie hasła, Wyciek danych, Zabliwienie/przeciążenie, Zabliwienie/przeciążenie aplikacji Web, Awaria sieci/systemu, Spam/Phishing, and Kradzież. A legend at the bottom indicates risk levels: green for 'ryzyko niskie', orange for 'ryzyko średnie', and red for 'ryzyko wysokie'. Below the matrix are several panels: 'Potencjalne konsekwencje' (Potential consequences), 'Sugerowane zabezpieczenia' (Suggested security measures), 'Zastosowane zabezpieczenia' (Applied security measures), 'Źródła zagrożeń' (Sources of threats), and 'Liczba zagrożeń' (Number of threats). The 'Liczba zagrożeń' panel shows a table with risk levels and counts.

Ryzyko	wysokie	średnie	niskie
Ilość zagrożeń...	14	2	14
Ilość zasobów...	2	0	0

The 'Parametry' (Parameters) panel on the right shows filters for 'Ważność zasobu', 'Procesy biznesowe', 'Klasyfikacja zbiorów informacji', 'Aktywne incydenty', and 'Aktywne podatności' (highlighted in red), with 'Niski' selected.

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

The screenshot displays the configuration of a rule in the SecureVisio interface. The rule is defined as follows:

```
1 dotyczy zagrożenia z zasobu typu: Przenośne/Mobile --]
2
3
4
5
6 AND
7
8 zdarzenie z kategorii Threat deny]
9
10
11
12
13
14 na zasobie jest podatność, którą można wykorzystać zdalnie: AV=Network]
15
16
17 AND
18
19
20
21
22
23
24
25
26
27
28
29
30 podatność posiada wysoki priorytet zgodnie z oceną techniczną lub biznesową]
```

On the right side, the 'Reguły globalne' (Global Rules) section is visible, showing a list of rules with their impact types:

- Asset(Impact): Destination Impact - Konsekwencje prawne
- Asset(Impact): Destination Impact - Przejęcie komputera/urządzenia mobilnego przez Botnet/APT
- Asset(Impact): Destination Impact - Straty wizerunkowe i/lub dystrybucja złośliwych treści przez Web
- Asset(Impact): Destination Impact - Straty wizerunkowe względem podmiotu zewnętrznego
- Asset(Impact): Destination Impact - Wyciek klasyfikowanych informacji
- Asset(Impact): Destination Impact - Zakłócenie ważnego procesu działania organizacji
- Asset(Impact): Source Impact - Konsekwencje prawne
- Asset(Impact): Source Impact - Przejęcie komputera/urządzenia mobilnego przez Botnet/APT
- Asset(Impact): Source Impact - Straty wizerunkowe i/lub dystrybucja złośliwych treści przez Web
- Asset(Impact): Source Impact - Straty wizerunkowe względem podmiotu zewnętrznego
- Asset(Impact): Source Impact - Wyciek klasyfikowanych informacji
- Asset(Impact): Source Impact - Zakłócenie ważnego procesu działania organizacji