**OPIS PRZEDMIOTU ZAMÓWIENIA**

„WSPARCIE ORAZ ROZSZERZENIE LICENCJI SYSTEMU SECUREVISIO LUB DOSTARCZENIE ROZWIĄZANIA RÓWNOWAŻNOEGO”

1. Przedmiotem zamówienia jest rozszerzenie licencji oraz przedłużenie wsparcia dla posiadanego przez Sąd Apelacyjny we Wrocławia systemu SecureVisio lub dostarczenie rozwiązania równoważnego.
2. Zamawiający jest w posiadaniu Systemu SecureVisio składającego się z następujących modułów i narzędzi:
3. SecureVisio SIEM/UEBA – wykrywanie zdarzeń i incydentów bezpieczeństwa,
4. SecureVisio SOAR – automatyzacja zarządzania zdarzeniami, incydentami bezpieczeństwa, wsparcie procesu zarządzania podatnościami w oparciu o kontekst organizacji,
5. SecureVisio PDP – zarządzanie obszarem danych osobowych (Personal Data Protection),
6. IT GRC/IRM SecureVisio – obsługa analizy ryzyka IT i Compliance w celu priorytetyzacji kontekstowej alarmów
7. Wymienione komponenty Systemu pozwalają obecnie na obsługę 650 assetów (zasobów).
8. Posiadany System objęty jest wsparciem producenta do 31.12.2024 r.
9. Zamawiający posiada licencję wieczystą z odnawialnym wsparciem (licencja odpłatna, niewyłączna, nieograniczona czasowo i terytorialnie).
10. W ramach realizacji zmówienia posiadane licencje zostaną rozszerzone o dodatkowe 50 assetów (do łącznej liczby 700 assetów).
11. Całość systemu (700 assetów) zostanie objęta usługą wsparcia producenta Systemu do 31.12.2027 r.
12. Usługa wsparcia obejmie minimum:
    1. aktualizacje systemu, wprowadzające nowe rozwiązania funkcjonalne i poprawki;
    2. wsparcie techniczne w ramach realizacji zgłoszeń dotyczących awarii i błędów systemu;
    3. wsparcie dedykowanego konsultanta powdrożeniowego w ramach powdrożeniowej adopcji systemu.
13. Szczegółowy opis wymagań w zakresie usługi wsparcia zawiera załącznik nr 1 do OPZ.
14. Szczegółowy wykaz funkcjonalności posiadanego Systemu zawiera załącznik nr 2 do OPZ.
15. W przypadku dostarczenia rozwiązania równoważnego, Zamawiający wymaga spełnienia wymagań opisanych w załącznikach nr 1 i nr 2 oraz wdrożenia systemu zgodnie z wymaganiami opisanymi w załączniku nr 3 do OPZ
16. Termin realizacji Zamówienia: 21 dni od podpisania umowy.

Załącznik nr 1 do OPZ:

**ZAKRES WSPARCIA TECHNICZNEGO PRODUCENTA SYSTEMU SECUREVISIO**

1. Wsparcie techniczne realizowe przez Producenta Systemu, zakłada pomoc techniczną w zakresie zgłoszeń, związanych z wykrytymi przez Zamawiającego błędami systemowymi oraz dostęp do nowych wersji oprogramowania, a także pakietów z poprawkami.
2. Usługa Wsparcia jest świadczona w dni robocze, tj. od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy w godzinach od 8.00 do 16.00 i obejmuje usunięcie awarii/usterki/błędu w sposób umożliwiający funkcjonowanie Systemu, bądź jego elementu, zgodnie z przeznaczeniem oraz przywrócenie stanu sprzed awarii.
3. Kategorie błędów systemowych zostały rozpisane w poniższej tabeli i każdorazowo są zgłaszane poprzez dedykowany system zgłoszeniowy udostępniony przez Producenta Systemu. Zamawiający może zgłaszać błędy samodzielnie lub zlecać ich zgłaszanie autoryzowanemu dostawcy, który zajmuje się wdrażaniem i konfiguracją Systemu.

|  |  |  |  |
| --- | --- | --- | --- |
| Kategoria Błędu/ Priorytet | Opis | Poziom uciążliwości | Czas Reakcji |
| Awaria | Awaria - zdarzenie, które wystąpiło w Systemie lub w Narzędziach Bazodanowych z przyczyn nie leżących po stronie ZAMAWIAJĄCEGO, skutkujące brakiem jakiejkolwiek możliwości użytkowania Systemu przez wszystkich Użytkowników Końcowych | Krytyczny | 2h |
| Błąd krytyczny | Błąd Krytyczny – nieprawidłowe powtarzalne działanie Systemu powstałe z przyczyn nie leżących po stronie ZAMAWIAJĄCEGO, powodujące niezdolność do realizacji w Systemie wszystkich czynności bądź zamodelowania w Systemie dowolnego z procesów opisanych w Dokumentacji Systemu przez wszystkich Użytkowników Końcowych w ramach danej Roli oraz uniemożliwiające pracę w Systemie wszystkim Użytkownikom Końcowym w ramach danej Roli. | Krytyczny | 2h |
| Błąd funkcjonalny/wada funkcjonalna | Błąd Funkcjonalny / Wada Funkcjonalna – nieprawidłowe powtarzalne działanie Systemu powstałe z przyczyn nie leżących po stronie ZAMAWIAJĄCEGO, polegające na niezgodności realizacji w Systemie pewnych (niektórych) czynności bądź niezgodności modelowania w Systemie pewnych (niektórych) procesów z tymi opisanymi w Dokumentacji Systemu, występujące u wszystkich Użytkowników Końcowych w ramach danej Roli, nie uniemożliwiające jednak pracy w Systemie tym Użytkownikom Końcowym w ramach danej Roli. | Wysoki | 24h |
| Błąd | Błąd – nieprawidłowe powtarzalne działanie Systemu powstałe z przyczyn nie leżących po stronie ZAMAWIAJĄCEGO, powodujące niezdolność do realizacji w Systemie pewnych (niektórych) czynności bądź zamodelowania w Systemie pewnych (niektórych) procesów opisanych w Dokumentacji Systemu przez kilku lub wszystkich Użytkowników Końcowych w ramach danej Roli, nie uniemożliwiające jednak pracy w Systemie tym Użytkownikom Końcowym. | Średni | 48h |
| Wada | Wada – nieprawidłowe powtarzalne działanie Systemu powstałe z przyczyn nie leżących po stronie ZAMAWIAJĄCEGO, powodujące niezdolność do realizacji w Systemie pewnych (niektórych) czynności bądź zamodelowania w Systemie pewnych (niektórych) procesów opisanych w Dokumentacji Systemu przez jednego lub kilku Użytkowników Końcowych w ramach danej Roli, nie uniemożliwiające jednak pracy w Systemie tym Użytkownikom Końcowym. | Niski | 48h |

Załącznik nr 2.

**SPECYFIKACJA FUNKCJONALNOŚCI POSIADANEGO SYSTEMU**

1. System zapewnia narzędzia do tworzenia elektronicznej, interaktywnej dokumentacji systemu teleinformatycznego, w tym schematów architektury zabezpieczeń sieci (tzn. mapy pokazującej urządzenia zabezpieczeń, strefy bezpieczeństwa, zasoby IT, połączenia i topologię sieci), prezentującej informacje nt. bezpieczeństwa w ujęciu technicznym oraz w odniesieniu do procesów działania organizacji.

2. System zapewnia narzędzia umożliwiające dokonanie oceny wpływu incydentu bezpieczeństwa IT na działalność organizacji, m.in. po wpisaniu adresu IP zasobu IT związanego z incydentem bezpieczeństwa system wyszukuje i prezentuje informacje nt. procesów organizacji i klasyfikowanych informacji (m.in. danych osobowych), które mogły zostać naruszone w wyniku incydentu oraz wyświetlać przewidywane istotne dla organizacji konsekwencje naruszenia bezpieczeństwa.

3. System zapewnia narzędzia prezentujące techniczne informacje nt. bezpieczeństwa IT z perspektywy działalności organizacji. Umożliwiać zapisywanie, wyszukiwanie i prezentowanie co najmniej następujących informacji: procesy działania organizacji, klasyfikacja zbiorów informacji, ważność zasobu IT dla organizacji, właściciel zasobu IT oraz zespół obsługi.

4. System zapewnia narzędzia służące do ustalania wrażliwych zbiorów informacji, jakie są narażone w razie incydentu bezpieczeństwa. Umożliwiać definiowanie własnego schematu klasyfikacji danych w organizacji (np. własność intelektualna, dane osobowe, dane finansowe) oraz umożliwiać wyszukiwanie lokalizacji zasobów IT, gdzie znajdują się dane określonej kategorii oraz wskazywać je na graficznej mapie systemu teleinformatycznego.

5. System zapewnia narzędzia do modelowania zagrożeń umożliwiające symulowanie różnych potencjalnych scenariuszy incydentów bezpieczeństwa IT. Dostępne narzędzia działające na graficznej mapie systemu teleinformatycznego mają służyć do m.in.:

• wyznaczania źródła zagrożenia zasobu IT wraz z wynikiem analizy ryzyka dla tego zagrożenia wyliczanym w sposób automatyczny,

• wyświetlania zabezpieczeń zasobu IT przed potencjalnymi źródłami zagrożenia,

• wyświetlania zabezpieczeń chroniących zasoby IT przed określonym źródłem zagrożenia,

• wyświetlania lokalizacji zasobów określonego rodzaju,

• wyświetlania najbardziej narażonych zasobów IT,

• wyświetlania ważnych zasobów IT narażonych na awarie.

6. System zapewnia graficzne narzędzia do definiowania wymagań bezpieczeństwa organizacji (m.in. środków ochrony wymaganych dla określonych elementów i obszarów systemu teleinformatycznego) oraz narzędzia do audytowania bezpieczeństwa względem tych wymagań. Narzędzia systemu mają umożliwić m.in.:

• zweryfikowanie, czy stan bezpieczeństwa systemu teleinformatycznego odpowiada specyficznym wymaganiom organizacji,

• wyznaczanie zasobów IT o wysokim poziomie ryzyka, które nie posiadają wymaganych zabezpieczeń,

• wskazywanie zasobów IT o krytycznym znaczeniu dla organizacji, które nie posiadają odpowiednich zabezpieczeń

7. System zapewnia narzędzia graficzne do tworzenia i przeszukiwania elektronicznej dokumentacji prezentujące wyniki na schemacie mapy logicznej oraz fizycznej. Umożliwiać rozbudowę elektronicznej dokumentacji o nowe parametry oraz dołączane dokumenty, odnoszące się m.in. do stref bezpieczeństwa, systemów zabezpieczeń, urządzeń fizycznych oraz zasobów informacyjno-usługowych.

8. System posiada możliwość wykrywania topologii sieci fizycznej oraz jej wizualizacji na podstawie następujących protokołów sieciowych: SNMP v2 i v3, LLDP, CDP.

9. System posiada mechanizmy umożliwiające rozpoznanie systemów IT oraz zapisywać wyniki w module elektronicznej dokumentacji, zapewniając:

• możliwość wykrywania zasobów oraz ich parametrów na podstawie wyników przynajmniej jednego skanera podatności,

• możliwość wykrywania zasobów oraz ich parametrów na podstawie wyników przynajmniej jednego skanera sieciowego,

• możliwość wykrywania zasobów oraz ich parametrów przy wykorzystaniu protokołu WMI,

• możliwość wykrywania zasobów oraz ich parametrów przy wykorzystaniu skryptów SSH oraz PowerShell,

10. System posiada bazę wiedzy eksperckiej zawierającej wiedzę pozwalającą ocenić poprawność projektu zabezpieczeń identyfikując efektywność zastosowanych mechanizmów sieciowych oraz lokalnych w stosunku do potencjalnych wektorów ataków oraz w przypadku ich nie zastosowania zidentyfikować ryzyka, które się z tym wiążą.

11. System zapewnia możliwość definiowania procesów organizacji oraz zależności od innych procesów, a także zapewnić możliwość definiowania czasów ich aktywności (np. proces praca biurowa w organizacji jest aktywny od poniedziałku do piątku od 8:00 do 16:00). Zależności mają być prezentowane w postaci graficznej.

12. System posiada mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT zdefiniowanego w elektronicznej dokumentacji oraz prezentacji tych informacji w formie graficznej.

13. Elektroniczna dokumentacja zapisana w systemie umożliwia automatyczne wyszukiwanie pojedynczych punktów awarii sieci i systemów IT (tzn. elementów bez redundancji), których uszkodzenie spowoduje zablokowanie ważnych procesów organizacji.

14. System umożliwia automatyczne szacowanie ryzyka dla wszystkich systemów IT zdefiniowanych w elektronicznej dokumentacji. Szacowanie ryzyka odbywa się względem zagrożeń natury informatycznej, np. włamane, infekcja złośliwym programem, podsłuch sieciowy, awaria.

15. System w formie graficznej prezentuje podsumowanie aktualnego stanu bezpieczeństwa, m.in. procesy organizacji zagrożone przez pojedyncze punkty awarii.

16. System zapewnia parsowanie spływających do niego zdarzeń w następujących formatach:

• SYSLOG;

• Wiadomości e-mail;

• Dziennika zdarzeń Windows (WEF – Windows Event Forwarding);

Przez parsowanie zdarzeń rozumie się proces analizy zdarzenia i rozkład na elementy składowe takie jak np.: adres IP źródłowy, adres IP docelowy, data, czas, użytkownik, treść zdarzenia itp.

17. System posiada predefiniowany zestaw parserów zdarzeń

18. System zapewnia mechanizmy umożliwiające mu pozyskanie zdarzeń z baz danych oraz plików płaskich;

19. System posiada wbudowany interfejs graficzny do tworzenia własnych parserów umożliwiający następujące funkcjonalności:

• Parsowanie warunkowe;

• Parsowanie hierarchiczne;

• Wzbogacanie zdarzeń o dodatkowe pola;

• Mapowanie wartości;

• Zastosowanie wyrażeń regularnych;

• Wsparcie dla formatów JSON oraz XML;

• Wykorzystanie gotowych praserów przy tworzeniu nowych;

• Mechanizmy wyszukiwania w polach zdarzeń;

20. System zapewnia możliwość zbierania i przetwarzania informacji dotyczących przepływów sieciowych [ang. Netflow].

21. System posiada mechanizm definiowania scenariuszy obsługi incydentów uruchamianych na podstawie następujących kryteriów:

• w przypadku gdy zasób przetwarza zdefiniowane informacje klasyfikowane (np. dane osobowe),

• w przypadku gdy zasób jest elementem określonego procesu organizacji,

• w przypadku gdy zasób zlokalizowany jest w danej lokalizacji,

• w przypadku gdy na zasobie może dojść do określonego cyberzagrożenia;

• w przypadku gdy na zasobie może dojść do określonej konsekwencji naruszenia bezpieczeństwa;

• w przypadku gdy na zasobie jest zainstalowany określony system operacyjny lub oprogramowanie

22. W ramach scenariuszy obsługi incydentów system umożliwia wykonanie następujących akcji i powiązanie ich z poszczególnymi krokami:

• zmianę operatora;

• zmianę statusu;

• zmianę priorytetu;

• przekazywanie i pobieranie parametrów z innych systemów poprzez skrypty SSH/PowerShell oraz REST API);

• wysłanie powiadomień;

• aktualizację dokumentów wraz z ich automatycznym wersjonowaniem;

• gromadzenie informacji na bazie podręcznego schowka oraz dołączenia plików wraz z wyliczaniem dla nich funkcji skrótu;

• aktualizację list referencyjnych;

• edycję bazy wiedzy zarówno w kontekście określonego wątku jak i definiowania nowych;

• założenie zadania;

23. System automatycznie proponuje odpowiednie scenariusze obsługi incydentów. Scenariusze obsługi zawierają możliwość ich symulacji i weryfikacji, m.in. na przykładowym zasobie IT.

24. Możliwość konfiguracji systemu w ramach której przebieg scenariusza dostosuje się dynamicznie do pozyskanych w ramach jego obsługi informacji umożliwiając następujące funkcjonalności:

• Automatyzację wykonania wielu kroków nie wymagających reakcji operatora;

• Warunkowe wykonywanie kroków w zależności od informacji zawartej zarówno w elektronicznej dokumentacji jak i informacji pozyskanej z innych systemów;

• Warunkowe wykonywanie kroków w zależności od odpowiedzi operatora na zdefiniowane pytanie;

25. System odczytuje alarmy wysyłane z innych systemów w tym systemów zabezpieczeń, dla których na podstawie informacji zawartych w elektronicznej dokumentacji automatycznie oszacowuje konsekwencje incydentów bezpieczeństwa, m.in. jakie procesy organizacji mogą zostać zakłócone, jakie informacje klasyfikowane mogą zostać skradzione przez przestępców.

26. System posiada mechanizm definiowania reguł analizy incydentów dla każdego odbieranego zdarzenia. Reguły umożliwiają korelację informacji technicznych wyciągniętych ze zdarzenia przekazanego z innych systemów (m.in. adres IP, kategoria, severity) z parametrami zdefiniowanymi w elektronicznej dokumentacji (m.in. ważność zasobu, klasyfikowane informacje, procesy organizacji) oraz aktualnymi incydentami bezpieczeństwa.

27. System umożliwia detekcję anomalii poprzez osiągnięcie określonej liczby punktów na danym zasobie wyliczonych z sumy punktów wszystkich zdarzeń na nim występujących w określonym przedziale czasu. W tym celu wynik działania reguł korelacyjnych jest oceniany w skali punktowej w odniesieniu do rodzaju zasobu oraz jego parametrów. Przykładowo zdarzenie będzie inaczej oceniane jeżeli będzie dotyczyło komputera a inaczej jeżeli będzie miało miejsce na serwerze usług.

28. System pozwala na budowanie profili aktywności użytkowników oraz zasobów poprzez wielowartościowe listy referencyjne przykładowo: nazwa użytkownika, aplikacja i adres docelowy oraz umożliwia wykorzystywanie ich w regułach korelacyjnych.

29. Wykryte incydenty mają być priorytetyzowane w odniesieniu do ważności dla organizacji zasobów których dotyczą (tzn. wspomaganych procesów, przetwarzanych informacji klasyfikowanych). System udostępnia graficzny edytor pozwalający na dostosowanie reguł wyznaczania priorytetów obsługi względem dowolnych parametrów zawartych w elektronicznej dokumentacji;

30. Dla zarejestrowanych incydentów system automatycznie wyznacza ścieżkę ataku i prezentuje ją w formie graficznej na schemacie sieci. Ścieżka ataku pokazuje wszystkie urządzenia zabezpieczeń na drodze pomiędzy sprawcą i ofiarą ataku.

31. System w razie wykrycia incydentów o poważnych konsekwencjach dla organizacji umożliwia automatyczne powiadamianie o zdarzeniu wskazanych pracowników, m.in. za pomocą email i SMS.

32. System w formie graficznej prezentuje podsumowanie aktualnego stanu bezpieczeństwa, m.in. procesy organizacji zagrożone przez incydenty bezpieczeństwa.

33. System udostępnia możliwość prezentacji danych w postaci tzw. „dashboard” czyli pozwala dostosować zakres i prezentacje danych do potrzeb administratora czy też zalogowanego użytkownika

34. Dla wykrytych podatności odbywa się ich priorytetyzacja w odniesieniu do ważności podatnych systemów IT dla organizacji (tzn. wspomaganych procesów, przetwarzanych informacji klasyfikowanych). System udostępnia graficzny edytor pozwalający na dostosowanie reguł priorytetyzacji względem dowolnych parametrów zawartych w elektronicznej dokumentacji;

35. System zapewnia integrację za pomocą API z przynajmniej dwoma producentami skanerów podatności, w tym ze skanerem Tenable Nessus Professional, w którego posiadaniu jest Zamawiający, rozumianą jako możliwość harmonogramowania i uruchamiania procesu skanowania podatności oraz automatycznego pobierania wyników w celu dalszego ich przetwarzania.

36. System zapewnia automatyczny odczyt danych związanych z nowymi podatności opublikowanymi w bazie CVE oraz posiadać możliwość definiowania oprogramowania na zasobach (system operacyjny oraz zainstalowane oprogramowanie) zapewniając tym samym identyfikację podatności na tych zasobach bez potrzeby użycia skanera podatności.

37. System na podstawie wyników skanowania umożliwia identyfikowanie komputerów na podstawie ich nazw pozwalając tym samym na procesowanie podatności danego komputera nawet przy dynamicznym adresie IP pobieranym z serwera DHCP.

38. System posiada mechanizm definiowania scenariuszy obsługi podatności uruchamianych na podstawie następujących kryteriów:

• w przypadku gdy zasób przetwarza zdefiniowane informacje klasyfikowane (np. dane osobowe),

• w przypadku gdy zasób jest elementem określonego procesu organizacji,

• w przypadku gdy zasób zlokalizowany jest w danej lokalizacji,

• w przypadku gdy na zasobie może dojść do określonego cyberzagrożenia;

• w przypadku gdy na zasobie może dojść do określonej konsekwencji naruszenia bezpieczeństwa;

• w przypadku gdy na zasobie jest zainstalowany określony system operacyjny lub oprogramowanie

39. W ramach scenariuszy obsługi podatności system umożliwia:

• zmianę operatora;

• zmianę statusu;

• zmianę priorytetu;

• przekazywanie i pobieranie parametrów z innych systemów poprzez skrypty SSH/PowerShell oraz REST API);

• wysłanie powiadomień;

• aktualizację dokumentów wraz z ich automatycznym wersjonowaniem;

• gromadzenie informacji na bazie podręcznego schowka oraz dołączenia plików wraz z wyliczaniem dla nich funkcji skrótu;

• aktualizację list referencyjnych;

• edycję bazy wiedzy zarówno w kontekście określonego wątku jak i definiowania nowych;

• założenie zadania;

40. System automatycznie proponuje odpowiednie scenariusze obsługi podatności. Scenariusze obsługi zawierają możliwość ich symulacji i weryfikacji, m.in. na przykładowym zasobie IT.

41. System w razie wykrycia podatności o poważnych konsekwencjach dla organizacji umożliwia automatyczne powiadamianie o zdarzeniu wskazanych pracowników, m.in. za pomocą email i SMS.

42. System w razie wykrycia podatności na podstawie informacji wyciągniętej z wyniku skanu potrafi automatycznie przydziela odpowiedni zespół obsługi dla danego zdarzenia (np.: przedzielenie osób dla podatności dotyczących oprogramowania Microsoft SQL Server). Podczas procesu przydzielania podatności dla zespołów obsługi system może brać uwagę ilość aktualnie obsługiwanych podatności przez członków zespołów (osoby które mają mniejszą ilość podatności będą mieli w pierwszej kolejności przypisywane nowe podatności, następnie będą one rozkładane pomiędzy osobami równomiernie).

43. System w formie graficznej prezentuje podsumowanie aktualnego stanu bezpieczeństwa, m.in. procesy organizacji zagrożone przez podatności.

44. System umożliwia stworzenie kompletnych w zasoby informacji rejestrów spełniających wymogi art. 30 RODO i wykazów spełniających wymogi art. 35 ustawy z dnia z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (dalej rejestry i wykazy), zawierających informacje przewidziane w ww. przepisach

45. System umożliwia ewidencjonowanie umów powierzenia przetwarzania danych osobowych zarówno dla danych, których użytkownik jest Administratorem jak i Procesorem.

46. System umożliwia prowadzenie rejestru udostępnień danych osobowych.

47. System pozwala na nadawanie upoważnień dla osób przetwarzających dane osobowe w sposób indywidualny jak i zbiorczy. Ponadto posiada wbudowany elektroniczny obieg dokumentów (tzw. workflow) procesu nadawania i akceptacji upoważnień.

48. System wspomaga proces inwentaryzacji obszarów przetwarzania danych osobowych poprzez wyszukiwanie systemów IT przetwarzających tego typu dane jak również grup i kategorii danych osobowych.

49. System wyznacza dostępne zabezpieczenia techniczne w odniesieniu do potencjalnych źródeł zagrożenia dla systemów IT przetwarzających dane osobowe.

50. System automatycznie wykonuje analizę ryzyka danych osobowych w odniesieniu do zagrożeń natury informatycznej oraz wykonuje ocenę skutków dla ochrony danych dla trzech głównych ryzyk: ryzyka utraty poufności, integralności oraz dostępności danych osobowych. Analiza ryzyka obejmuje również aspekty nieinformatyczne i jest wyliczana zgodnie z wytycznymi opisanymi standardem ISO 29134.

51. System wykonuje analizę ryzyka dla przetwarzanych danych osobowych wraz z określeniem zarówno zagrożeń jak i konsekwencji na jakie narażone są osoby fizyczne z związku z przetwarzaniem ich danych osobowych.

52. System umożliwia szacowanie ryzyka od momentu wdrażania organizacyjnych i technicznych środków bezpieczeństwa poprzez cały proces przetwarzania danych osobowych w organizacji. Proces monitorowania poziomu zagrożeń oraz zapewniania rozliczalności w odniesieniu do zastosowanych zabezpieczeń jest w Systemie procesem ciągłym i na bieżąco dostrajanym.

53. System zapewnia spełnienie wymagań formalno-prawnych dotyczących raportowania naruszeń bezpieczeństwa danych osobowych zgodnie z art. 33 pkt 5 RODO, umożliwiając w pełni automatyczne generowanie „Raportu naruszenia ochrony danych osobowych dla organu nadzorczego” łącznie z wyznaczeniem możliwych konsekwencji naruszenia bezpieczeństwa

54. System automatyzuje wykonywanie oceny skutków dla ochrony danych osobowych wraz z automatycznym generowaniem raportów w obszarze analizy ryzyka cyberzagrożeń (art. 35 RODO)

55. System umożliwia rejestrację zgłoszeń incydentów dotyczących danych osobowych związanych ze zbiorami danych osobowych, jednostkami organizacyjnymi, osobami, lokalizacjami oraz zasobami informatycznymi.

56. System umożliwia obsługę incydentów związanych z przetwarzaniem danych osobowych zapewniając możliwość automatycznego ich wykrywania na podstawie logów z systemów informatycznych biorących udział w ich przetwarzaniu. System umożliwia dostrojenie reguł wykrywania zarówno w kontekście informacji pozyskanych z logów jak i parametrów elektronicznej dokumentacji związanej z ich przetwarzaniem.

57. System zapewnia możliwość rejestracji i obsługi wniosków i roszczeń osób związanych z przetwarzaniem danych osobowych np.: żądanie usunięcia czy sprostowania danych osobowych oraz żądanie otrzymania kopii tych danych.

58. System umożliwia eksport w formatach: .pdf, .xlsx, .csv, oraz drukowanie prowadzonych rejestrów i wykazów, rejestrów powierzeń oraz udostępnień jak również pojedynczych rekordów z wymienionych rejestrów.

59. System pozwala opracowywać plany postępowania z ryzykiem wraz z określeniem terminowości, ustanowieniem poszczególnych zadań, przypisaniem zespołów obsługi oraz pełną ich rozliczalnością.

60. System pozwala na przechowywanie dokumentów dotyczących systemu ochrony danych osobowych umożliwiając użytkownikom śledzenie zmian w dokumentach, informowanie o zmianach oraz pełnym nadzorem nad dostępem do dokumentów.

61. System umożliwia prowadzenie wykazów programów i systemów informatycznych, służących przetwarzaniu danych osobowych.

62. System jest dostępny z poziomu dowolnej przeglądarki internetowej (Chrome, Edge, Firefox).

63. Interfejs użytkownika Systemu jest w języku polskim. Jest przejrzysty i konfigurowalny, pogrupowany w bloki tematyczne, co umożliwia łatwe i szybkie wyszukiwanie odpowiednich danych.

64. System posiada możliwość prowadzenia rejestru zrealizowanych oraz planowanych szkoleń z zakresu ochrony danych osobowych. Rejestr prezentowany jest w formie tabeli, której każdy wiersz odpowiada szkoleniu dla konkretnego pracownika a kolumny zawierają informacje o przedmiocie szkolenia.

65. System umożliwia tworzenie i edycję profili danych, wykorzystywanych w procesie dodawania nowych wpisów do rejestrów i wykazów, co ma na celu łatwiejsze i szybsze wprowadzanie danych do rejestrów i wykazów.

66. System posiada matrycę uprawnień, będącą narzędziem konfiguracyjnym w procesie nadawania upoważnień do przetwarzania danych osobowych. Matryca wyświetla uprawnienia z podziałem na procesy biznesowe i formę przetwarzania danych. Dla formy elektronicznej definiowane są również nazwy Oprogramowania, Zasobów informacyjno – usługowych wraz z ich lokalizacją na konkretnej mapie logicznej sieci IT.

67. System zawiera Słowniki wykorzystywane w bieżącej obsłudze obszaru danych osobowych.

68. System umożliwia tworzenie i edycję struktury organizacyjnej, w tym informacji dotyczących lokalizacji, stanowisk, kontaktów oraz grup osób.

69. System ochrony danych osobowych integruje się z modułami służącymi wykrywaniu/ reagowaniu na incydenty bezpieczeństwa i podatności systemowe (SecureVisio SIEM i SecureVisio SOAR), wykorzystując wprowadzone w aplikacji desktop informacje zawarte w elektronicznej dokumentacji, w szczególności dotyczące procesów biznesowych (np. uwzględniających ważność procesów dla organizacji, typy danych przetwarzanych w ramach procesów, jak dane osobowe, informacje poufne itp., właścicieli procesów, relacje między procesami, czas trwania procesów) oraz analizy ryzyka cyberzagrożeń.

70. Wykorzystując integrację z modułami wykrywania i reagowania na incydenty bezpieczeństwa oraz podatności (SecureVisio SIEM i SecureVisio SOAR), System umożliwia automatyczne powiadamianie o wykrytym zagrożeniu cybernetycznym odpowiednich pracowników (np. administratora danych), m.in. za pomocą email i SMS.

Załącznik nr 3 do OPZ:

**WDROŻENIE ROZWIĄZANIA RÓWNOWAŻNEGO**

1. System zostanie zainstalowany na maszynach wirtualnych uruchomionych w środowisku Zamawiającego działających pod kontrolą Windows Server 2019 lub SUSE Linux Enterprise Server.
2. Wykonawca dokona pełnej instalacji i konfiguracji dostarczonego rozwiązania wraz z migracją danych z systemu SecureVisio.
3. W szczególności przeniesione zostaną:
   1. słowniki,
   2. struktura organizacyjna (jednostki organizacyjne i stanowiska pracowników),
   3. źródła logów wraz z konfiguracją paserów,
   4. użytkownicy i uprawnienia,
   5. rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania,
   6. procesy biznesowe,
   7. upoważnienia, udostępnienia i powierzenia przetwarzania danych osobowych,
   8. reguły zawiązane z analizą ryzyka i DPIA,
   9. mapy sieci (strefy bezpieczeństwa, zasoby IT, połączenia i topologia sieci),
   10. zgłoszenia podatności,
   11. zgłoszenia incydentów,
   12. zespoły obsługi,
   13. raporty, powiadomienia, dashboardy.
4. Wykonawca dostarczy dokumentację powdrożeniową opisującą konfigurację oraz funkcjonalność wdrożonego rozwiązania.
5. Wykonawca przeprowadzi szkolenie powdrożeniowe dla inspektora ochrony danych oraz administratorów i operatorów – dla maksymalnie 10 osób (forma do ustalenia przez strony, dopuszczalne szkolenie on-line, stacjonarne, w tym również w formie voucherów do wykorzystania do 12 miesięcy po zakończeniu wdrożenia).