**Opis Przedmiotu Zamówienia**

**Usługa wdrożenia Systemu do zarządzania bezpieczeństwem teleinformatycznym wraz z 36-miesięcznym wsparciem serwisowym**

Warunki niezbędne do wykonania usługi wdrożenia Systemu do zarządzania bezpieczeństwem teleinformatycznym oraz szczegółowy opis Systemu.

1. Wykonawca dostarczy wszystkie wymagane licencje uprawniające Zamawiającego do instalacji i poprawnej eksploatacji całości dostarczonego Systemu na potrzeby własne lub jednostek podległych z zastrzeżeniem ilości obsługiwanych urządzeń.
2. Udzielenie Zamawiającemu bezterminowej licencji dla Systemu na następujących warunkach:

- obsługa minimum **150** urządzeń definiowanych poprzez adres IPv4,

- dla minimum 8 administratorów pracujących jednocześnie, bez ograniczenia ilości użytkowników nazwanych i stacji roboczych, bez ograniczeń na ilość danych wprowadzanych do Systemu.

1. Zainstalowanie i skonfigurowanie Systemu w środowisku Zamawiającego - środowisko wirtualne   
   (8 core, 32 GB RAM, 2 TB HDD) wraz z licencją na systemem operacyjnym MS Windows Server 2016 dostarcza Zamawiający. Odpowiednią bazę danych, na potrzeby Systemu, dostarcza Wykonawca. Wykonawca odpowiada za właściwe sparametryzowanie zarówno systemu operacyjnego jak i silnika bazy danych.
2. Przeszkolenie administratorów Systemu w zakresie korzystania z jego pełnej funkcjonalności. Szkolenia muszą się odbyć w siedzibie Zamawiającego. Minimalny czas szkoleń określa się na 16 godziny. Szkolenie jednorazowo nie może trwać dłużej niż 6 godzin.
3. Dostarczenie mechanizmu (w postaci skryptu, bądź innego rozwiązania programowego) do archiwizacji całości Systemu umożliwiającego odtworzenie kompletnego Systemu na dowolny dzień.
4. Przekazanie Zamawiającemu wszelkich, niezbędnych do poprawnego korzystania z wdrożonego rozwiązania, informacji o specyfice Systemu oraz informacji technicznych na temat jego prawidłowej eksploatacji – szczegółowa dokumentacja powdrożeniowa oraz instrukcję/instrukcje obsługi.
5. Etapy wdrożenia oraz świadczenia usług serwisowych Systemu:

Etap 1 – Analiza przedwdrożeniowa - cykl prac analitycznych i organizacyjnych ustalający szczegółowy zakres oraz sposób realizacji wdrożenia oraz harmonogram i zakres szkoleń.

Na podstawie Etapu 1 Wykonawca opracuje i przedstawi do akceptacji Zamawiającemu projekt harmonogramu i metodologii wdrożenia.

Etap 2 - Instalacja i uruchomienie Systemu w środowisku produkcyjnym Zamawiającego – po uzyskaniu akceptacji Etapu 1. Celem tego etapu jest uzyskanie dynamicznego raportu audytowego pokazującego potencjalne możliwości przełamania zabezpieczeń w infrastrukturze Urzędu. Po zakończeniu tego etapu musi zostać sporządzony protokół bez uwag podpisany przez obie strony.

Etap 3 - Optymalizacja Systemu – Celem tego etapu jest dostrojenie scenariuszy obsługi zaimplementowanych w Etapie 2, w szczególności poprzez przeprowadzenie symulacji i analizie wyników przeprowadzonych symulacji, dotyczących procesów krytycznych (określonych w Etapie 2) Urzędu. Po zakończeniu tego etapu musi zostać sporządzony protokół bez uwag podpisany przez obie strony.

Etap 4 - Przeszkolenie administratorów/ użytkowników Systemu z uruchomionych funkcjonalności.

Po zakończeniu tego etapu musi zostać sporządzony protokół bez uwag podpisany przez obie strony obejmujący imienną listę przeszkolonych osób.

Etap 5 – Wsparcie serwisowe -36 miesięcy od zakończenia prac przewidzianych w Etapie 4.

Wsparcie serwisowe dla Systemu – co najmniej usunięcie awarii/usterki/błędu w sposób umożliwiający funkcjonowanie Systemu, bądź jego elementu, zgodnie z przeznaczeniem i przywrócenie stanu sprzed awarii bądź, o ile zaistnieje taka potrzeba, stanu takiego jakby awarii w ogóle nie było. Naprawa ma na celu umożliwienie Zamawiającemu korzystanie z Systemu zgodnie z jego przeznaczeniem i właściwościami o niezmienionej wydajności. Czas usunięcia awarii/usterki/błędu nie może być dłuższy niż 48 godzin od zgłoszenia. Wykonawca musi wskazać nr kontaktowy oraz mail (lub stronę internetową CRM) służący do wysyłania zgłoszeń.

Wsparcie serwisowe obejmuje również wszelkie niezbędne modyfikacje Systemu w związku z koniecznością zapewnienia zgodności z obowiązującymi przepisami i normami oraz związane z aktualizacjami użytych do budowy Systemu komponentów.

1. System musi działać jako klient aplikacji lub strona WWW dostępna w dowolnej przeglądarce internetowej (Chrome, Edge, Firefox), bez konieczności instalowania jakichkolwiek dodatków dla prawidłowego jego działania.
2. Interfejs użytkownika Systemu musi być w języku polskim. Musi być przejrzysty i konfigurowalny, poprzez pogrupowanie zawartości w bloki tematyczne, co ma umożliwić łatwe i szybkie wyszukiwanie odpowiednich danych.
3. System musi posiadać zaimplementowane mechanizmy ochrony danych, w tym: rozliczalności, autentykację oraz uwierzytelnianie.
4. System musi być zgodny z przepisami o ochronie danych osobowych, w tym: Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE oraz Ustawy o ochronie Danych Osobowych z dn. 10.05.2018r. Na czas świadczenia usług wsparcia serwisowego Wykonawca jest podmiotem, któremu powierza się przetwarzanie danych osobowych w rozumieniu art. 28 ww rozporządzenia (co jest potwierdzone stosownymi zapisami umownymi).
   * + 1. System musi być dostarczony jako jedna lub wiele aplikacji oferujących narzędzia wspierające osoby odpowiedzialne za bezpieczeństwo teleinformatyczne w co najmniej następujących obszarach:

- nadzór nad bezpieczeństwem Urzędu,

- zarządzanie ryzykiem organizacji w obszarze teleinformatycznym,

- zapewnienie zgodności systemów teleinformatycznych z wymaganiami bezpieczeństwa.

1. System musi posiadać zaimplementowane narzędzia umożliwiające co najmniej:

- pełnienie nadzoru nad bezpieczeństwem procesów oraz danych elektronicznych wskazanych przez Zamawiającego,

- zarządzanie ryzykiem organizacji w obszarze teleinformatycznym,

- zapewnienie zgodności systemów teleinformatycznych z wymaganiami norm bezpieczeństwa ISO-27001.

1. System musi zawierać narzędzia do tworzenia elektronicznej, interaktywnej dokumentacji systemu teleinformatycznego (co najmniej schematów architektury zabezpieczeń sieci tzn. mapy pokazującej urządzenia zabezpieczeń, strefy bezpieczeństwa, zasoby teleinformatyczne, połączenia i topologię sieci LAN/WAN), prezentującej informacje nt. bezpieczeństwa w ujęciu technicznym oraz w odniesieniu do procesów działania organizacji.
2. System musi umożliwić dokonanie oceny wpływu incydentu bezpieczeństwa teleinformatycznego na działalność Urzędu, m.in. po wpisaniu adresu IP zasobu teleinformatycznego związanego z incydentem bezpieczeństwa system wyszuka i zaprezentuje informacje na temat procesów organizacji i klasyfikowanych informacji (m.in. danych osobowych), które mogły zostać naruszone w wyniku powstałego incydentu oraz wyświetla przewidywane, istotne dla Urzędu, konsekwencje naruszenia bezpieczeństwa.
3. System musi prezentować techniczne informacje na temat bezpieczeństwa teleinformatycznego z perspektywy działalności Urzędu, w tym zapisywanie, wyszukiwanie i prezentowanie co najmniej następujących informacji: procesy działania organizacji, klasyfikacja zbiorów informacji, ważność zasobu teleinformatycznych dla Urzędu, właściciel zasobu teleinformatycznego oraz zespół obsługi.
4. Rozwiązanie musi zawierać narzędzia służące do ustalania wrażliwych zbiorów informacji, jakie są narażone w razie incydentu bezpieczeństwa. Umożliwić definiowanie własnego schematu klasyfikacji danych w Urzędzie (np. własność intelektualna, dane osobowe, dane finansowe) oraz zapewnić wyszukiwanie lokalizacji zasobów teleinformatycznych, gdzie znajdują się dane określonej kategorii ze wskazaniem ich na graficznej mapie systemu teleinformatycznego.
5. System powinien zapewnić narzędzia do modelowania zagrożeń umożliwiające symulowanie różnych potencjalnych scenariuszy incydentów bezpieczeństwa teleinformatycznego, w tym narzędzia działające na graficznej mapie systemu teleinformatycznego służące m.in. do:

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

- wyświetlania zabezpieczeń zasobu teleinformatycznego przed potencjalnymi źródłami zagrożenia,

- wyświetlania zabezpieczeń chroniących zasoby teleinformatyczne przed określonym źródłem zagrożenia,

- wyświetlania lokalizacji zasobów określonego rodzaju,

- wyświetlania najbardziej narażonych zasobów teleinformatycznych,

- wyświetlania ważnych zasobów teleinformatycznych narażonych na awarie.

1. System powinien zapewnić 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 powinny umożliwić m.in.:

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

- wyznaczanie zasobów teleinformatycznych o wysokim poziomie ryzyka, które nie posiadają wymaganych zabezpieczeń,

- wskazywanie zasobów teleinformatycznych o krytycznym znaczeniu dla organizacji, które nie posiadają odpowiednich zabezpieczeń.

1. Rozwiązanie musi zawierać narzędzia graficzne do tworzenia i przeszukiwania elektronicznej dokumentacji prezentujące wyniki na schemacie mapy logicznej oraz fizycznej.
2. System musi umożliwiać rozbudowę elektronicznej dokumentacji o nowe parametry oraz dokumenty, odnoszące się m.in. do stref bezpieczeństwa, systemów zabezpieczeń, urządzeń fizycznych oraz zasobów informacyjno-usługowych.
3. System musi zawierać bazę wiedzy eksperckiej zawierającej wiedzę pozwalającą ocenić poprawność projektu zabezpieczeń. Ocena powinna obejmować efektywność zastosowanych mechanizmów sieciowych oraz lokalnych w odniesieniu do potencjalnych wektorów ataków oraz w przypadku stwierdzenia ich braku umożliwi zidentyfikować ryzyka, które się z tym wiążą.
4. System powinien zapewnić 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 powinny być prezentowane w postaci graficznej.
5. System powinien zapewnić mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu teleinformatycznego zdefiniowanego w elektronicznej dokumentacji oraz prezentację tych informacji w formie graficznej.
6. Elektroniczna dokumentacja zapisana w systemie musi umożliwić automatyczne wyszukiwanie pojedynczych punktów awarii sieci i systemów teleinformatycznych (na przykład elementów bez redundancji), których uszkodzenie spowoduje zablokowanie ważnych procesów organizacji.
7. System musi pozwalać na automatyczne szacowanie ryzyka dla wszystkich systemów teleinformatycznych zdefiniowanych w elektronicznej dokumentacji. Szacowanie ryzyka powinno odbywać się względem zagrożeń natury informatycznej, m.in. przełamanie zabezpieczeń, wyciek danych, infekcja złośliwym programem, podsłuch sieciowy.
8. System musi posiadać interfejs pozwalający na definiowanie nowych warunków szacowania ryzyka wpływających bezpośrednio na wynik dotychczasowej analizy.
9. System powinien w formie graficznej umożliwić prezentację aktualnego stanu bezpieczeństwa - na przykład procesy organizacji zagrożone przez pojedyncze punkty awarii.
10. System w formie graficznej musi umożliwić podsumowanie aktualnego stanu bezpieczeństwa, m.in. procesy organizacji zagrożone przez incydenty bezpieczeństwa, średni czas reakcji na incydent bezpieczeństwa oraz średni czas obsługi podatności.
11. System musi mieć możliwość prezentacji danych w postaci tzw. „Dashboard” pozwalając tym samym na dostosowanie zakresu i prezentacji danych do potrzeb administratora czy też zalogowanego użytkownika.
12. System musi być́ wyposażony w dostarczone przez producenta API, umożliwiające jego integrację z systemami zewnętrznymi.
13. System musi w sposób graficzny w formie mapy sieci przedstawić wpływ awarii urządzenia fizycznego (np.: przełącznika) na procesy biznesowe organizacji udzielając jednocześnie operatorowi informacji o lokalizacji tego urządzenia.
14. System powinien zapewnić możliwość wykrywania topologii sieci fizycznej oraz jej wizualizacji na podstawie następujących protokołów sieciowych: SNMP (w wersji 2 i 3), LLDP.
15. System musi zapewnić parsowane spływających do niego zdarzeń w formacie SYSLOG. Przez parsowane zdarzeń rozumie się proces analizy zdarzenia i rozkład na elementy składowe w tym.: adres IP źródłowy, adres IP docelowy, data, czas, użytkownik, treść zdarzenia itp.
16. Rozwiązanie musi umożliwiać́ definiowanie parserów dla niestandardowych formatów logów.
17. System musi posiadać interfejs pozwalający na tworzenie własnych reguł parsujących w oparciu o składnię wyrażeń regularnych.
18. System musi posiadać predefiniowany zestaw parserów zdarzeń.
19. Rozwiązanie musi umożliwiać́ przeszukiwanie logów z uwzględnieniem filtracji po sparsowanych polach.
20. System musi posiadać funkcjonalność korelacji danych w czasie rzeczywistym w celu wyszukiwania powiązań pomiędzy zdarzeniami z różnych systemów. Wszystkie logi powinny być normalizowane, kategoryzowane oraz poddawane kontroli zdefiniowanym regułom wyszukiwania incydentów.
21. System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń które mają zostać odrzucone, poddane regułom korelacyjnych lub zagregowane.
22. System musi pozwolić na definiowanie różnych wartości okien czasowych w zależności od rodzajów przetwarzanych zdarzeń celem efektywnego wykorzystania zasobów sprzętowych w regułach korelacji.
23. Rozwiązanie musi umożliwić korelację zdarzeń pochodzących z różnych urządzeń, punktów końcowych i aplikacji z anomaliami wykrywanymi w przepływach sieciowych oraz podatności pozyskanych bezpośrednio ze skanerów aplikacyjnych i bazy CVE.
24. System musi korelować zdarzenia wysyłane z innych systemów, w tym systemów zabezpieczeń, względem informacji zawartych w elektronicznej dokumentacji.
25. Silnik korelacyjny musi bazować na informacjach z elektronicznej dokumentacji oraz algorytmach umożliwiając tym samym szczegółową analizę potencjalnego wektora ataku w kontekście braku adekwatnych zabezpieczeń, ryzyka przełamania zabezpieczeń oraz potencjalnych konsekwencji naruszeń bezpieczeństwa (Business Impact Analysis).
26. System powinien posiadać mechanizm definiowania reguł analizy incydentów dla każdego odbieranego zdarzenia. Reguły muszą umożliwiać 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 musi posiadać predefiniowany zestaw reguł analizy incydentów.
28. Rozwiązanie musi mieć możliwość kategoryzacji każdego rodzaju przetwarzanych logów. (przypisania zdarzenia do określonej kategorii np. logowanie, wylogowanie, zmiana uprawnień́, atak brute force, malware, exploit, suspicious, vulnerability, DOS, recon itp.).
29. System powinien zapewnić mechanizmy umożliwiające rozpoznanie systemów teleinformatycznych (Asset Discovery) oraz zapisanie wyników 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,

- możliwość wykrywania parametrów urządzeń fizycznych na bazie protokołu SNMP w wersji 2 i 3.

1. System powinien pozwalać na zdefiniowanie tak zwanego Zarządzania Incydentami to znaczy powinien co najmniej wspierać́ użytkowników poprzez mechanizmy podpowiedzi, wskazywania procedur wspierających rozwiązanie danego typu incydentu, wraz z możliwością̨ odznaczania każdego z wykonanych kroków.
2. System musi mieć możliwość tworzenia nowych incydentów automatycznie, na podstawie zdarzeń z innych systemów, oraz ręcznie.
3. System musi zawierać mechanizm definiowania scenariuszy obsługi incydentów uruchamianych na podstawie co najmniej 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 określonej konsekwencji naruszenia bezpieczeństwa,

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

- w przypadku określonego statusu.

1. W ramach obsługi incydentów bezpieczeństwa system musi umożliwić przygotowanie gotowych scenariuszy obejmujących co najmniej:

- definiowanie warunków wykonania oraz sposób ich obsługi,

- zmianę operatora,

- uruchomienie skryptu PowerShell,

- uruchomienie skryptu SSH,

- uruchomienie komendy z linii poleceń,

- uruchomienie zdefiniowanej wcześniej strony internetowej,

- wysłanie powiadomienia,

- aktualizację dokumentu wraz z jego automatycznym wersjonowaniem.

1. System musi automatycznie podpowiadać odpowiednie scenariusze obsługi incydentów. Scenariusze obsługi muszą mieć możliwość ich symulacji i weryfikacji, m.in. na przykładowym zasobie teleinformatycznym.
2. Rozwiązanie musi posiadać́ funkcjonalność́ wysyłania powiadomień́ do innych systemów bądź́ zdefiniowanych użytkowników (m.in. powiadamianie email, SMS).
3. Musi istnieć́ funkcjonalność́, umożliwiająca dołączanie do informacji o incydencie dodatkowych załączników i linkowania do zewnętrznych systemów np. klasy forensics analysis.
4. System musi zapewniać́ rozliczalność́ działań́ wykonanych przez każdego z użytkowników i możliwość́ przeglądania zdarzeń́ powiązanych z danym incydentem, użytkownikiem, bądź́ obiektem.
5. Dla incydentów w systemach teleinformatycznych system umożliwi automatyczne wyznaczenie ścieżki ataku i zaprezentuje ją w formie graficznej na schemacie sieci. Ścieżka ataku pokazuje wszystkie urządzenia zabezpieczeń na drodze pomiędzy sprawcą i ofiarą ataku.
6. System w razie wykrycia incydentów o poważnych konsekwencjach dla organizacji umożliwia automatyczne powiadamianie o zdarzeniu wskazanych pracowników, m.in. za pomocą email i SMS.
7. Incydenty powinny być́ oznaczane pod względem istotności i priorytetu w oparciu o informacje pozyskane ze zdarzeń, zawartość elektronicznej dokumentacji oraz szacowanie ryzyka.
8. System musi zawierać mechanizm definiowania harmonogramów skanowania podatności (tzn. narzędzi Vulnerability Assessment) oraz na ich podstawie automatycznie uruchamiać procesy skanowania i analizować pozyskane raporty.
9. Wykryte podatności muszą być odpowiednio priorytetyzowane w odniesieniu do ważności podatnych systemów teleinformatycznych dla Urzędu oraz oceny technicznej zagrożenia bazującej na wartości CVSS lub wartości pozyskanej bezpośrednio z silnika skanera.
10. System musi zapewnić możliwość integracji z przynajmniej dwoma producentami skanerów podatności, rozumianą jako możliwość harmonogramowania i uruchamiania procesu skanowania podatności oraz automatycznego pobierania wyników w celu ich dalszego procesowania.
11. System musi zapewnić 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.
12. System na podstawie wyników skanowania powinien umożliwiać identyfikowanie komputerów na podstawie ich nazw, pozwalając tym samym na procesowanie podatności danego komputera, nawet przy dynamicznym adresie IP pobieranym z serwera DHCP.
13. System musi zawierać możliwość definiowania scenariuszy obsługi podatności uruchamianych na podstawie co najmniej 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 określonej konsekwencji naruszenia bezpieczeństwa;

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

- w przypadku określonego statusu.

1. W ramach obsługi podatności system musi umożliwić przygotowanie gotowych scenariuszy obejmujących:

- definiowanie warunków wykonania oraz sposób ich obsługi,

- zmianę operatora,

- uruchomienie skryptu PowerShell,

- uruchomienie skryptu SSH,

- uruchomienie komendy z linii poleceń,

- uruchomienie zdefiniowanej wcześniej strony internetowej,

- wysłanie powiadomienia,

- aktualizację dokumentu wraz z jego automatycznym wersjonowaniem.

1. System musi automatycznie podpowiadać odpowiednie scenariusze obsługi podatności. Scenariusze obsługi muszą mieć możliwość ich symulacji i weryfikacji, m.in. na przykładowym zasobie teleinformatycznym.
2. System w razie wykrycia podatności o poważnych konsekwencjach dla organizacji musi umożliwiać automatyczne powiadamianie o zdarzeniu wskazanych pracowników, m.in. za pomocą email i SMS.
3. System w razie wykrycia podatności na podstawie informacji wyciągniętej z wyniku skanu powinien umożliwiać automatycznie przydzielenie odpowiedniego zespołu obsługi dla danego zdarzenia (np.: przydzielenie osób dla podatności dotyczących oprogramowania Microsoft SQL Server).
4. Przydzielanie nowych podatności dla zespołów obsługi musi odbywać się automatycznie i uwzględniać ilość aktualnie obsługiwanych podatności przez członków zespołów. Rozwiązanie musi przydzielać je równomiernie pomiędzy osobami w ramach osób spełniających zdefiniowane w systemie kryteria pozwalające im na ich obsługę.
5. 59. System powinien w formie graficznej prezentować podsumowanie aktualnego stanu bezpieczeństwa, m.in. procesy organizacji zagrożone przez podatności, średni czas obsługi podatności.
6. System musi zawierać elektroniczną dokumentację umożliwiającą prowadzenie rejestru czynności i kategorii czynności przetwarzania danych osobowych, opisanych w artykule 30 RODO.
7. System musi umożliwiać szacowanie ryzyka wraz z oceną skutków dla ochrony danych osobowych (Data Protection Impact Assessment).
8. System musi umożliwiać zdefiniowanie obszarów przetwarzania zbiorów danych osobowych wraz z listą zastosowanych dla nich zabezpieczeń fizycznych.
9. System musi umożliwiać rejestrację zgłoszeń incydentów dotyczących danych osobowych związanych z poszczególnymi zbiorami, jednostkami organizacyjnymi, osobami, lokalizacjami oraz związanych z zasobami informatycznymi.
10. System powinien umożliwiać identyfikację i obsługę incydentów danych osobowych na podstawie danych pozyskanych ze zdarzeń m.in. z systemów zabezpieczeń czy serwerów oraz reguł bazujących na parametrach elektronicznej dokumentacji.
11. System powinien posiadać możliwość automatycznego przydzielenia zespołu obsługi do incydentu, dotyczącego zasobu przetwarzającego dane osobowe oraz uruchomieniu adekwatnego scenariusza obsługi, np.: dla konsekwencji wycieku danych osobowych.
12. System musi zapewnić możliwość rejestracji i obsługi roszczeń klientów związanych z przetwarzaniem danych osobowych np.: żądanie usunięcia danych osobowych oraz żądanie otrzymania kopii tych danych. Obsługa roszczeń pomiędzy operatorem systemu a zarządzającymi poszczególnymi zbiorami danych osobowych powinna odbywać się na bazie statusów i być rejestrowana w systemie.

1. System powinien zapewnić możliwość monitorowania aktywności stron internetowych, portów TCP, ICMP oraz mapowanie czasów ich dostępności / niedostępności bezpośrednio na procesy biznesowe oraz procesy zależne. W przypadku gdy system wykryje niedostępność monitorowanej usługi generuje automatycznie alarm powiadamiając jednoczenie właścicieli procesów biznesowych których procesy zależą w sposób pośredni lub bezpośredni od tej usługi (np.: e-mail, SMS, komunikator).
2. System musi umożliwić zbieranie i przetwarzanie informacji dotyczących przepływów sieciowych [ang. Netflow].
3. System musi zapewnić możliwość wykrywania ilościowego odchylenia natężenia zdarzeń́ od ich typowego rozkładu (dobowego, tygodniowego, miesięcznego, etc.).
4. System musi zawierać możliwość definiowania alarmów związanych z ilościowym odchyleniem natężenia zdarzeń w stosunku do komunikacji działającej w ramach zdefiniowanych procesów biznesowych.
5. Rozwiązanie ma gwarantować możliwość elastycznej rozbudowy o dalsze zasoby, które w przyszłości zostaną objęte jego działaniem.