OP-IV.272.84.2020.BRP **Zmieniony załącznik nr 1**

Opis przedmiotu zamówienia

Przedmiotem zamówienia jest wdrożenie Systemu do zarządzania bezpieczeństwem teleinformatycznym wraz z 36-miesięcznym wsparciem serwisowym, spełniającym poniższe minimalne wymagania funkcjonalne:

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:
    a) obsługa minimum 500 urządzeń definiowanych poprzez adres IPv4,
    b) dla minimum 15 administratorów pracujących jednocześnie, bez ograniczenia ilości użytkowników nazwanych i stacji roboczych, bez ograniczeń na ilość danych wprowadzanych do Systemu.
3. Zainstalowanie i skonfigurowanie Systemu w środowisku Zamawiającego - środowisko wirtualne. Wykonawca dostarczy licencję na niezbędny do działania systemu silnik bazy danych oraz system operacyjny dla środowiska złożonego z 2 serwerów dwuprocesorowych 8 rdzeniowych działających w klastrze VMWare. Wykonawca odpowiada za właściwe sparametryzowanie zarówno systemu operacyjnego jak i silnika bazy danych.
4. Przeszkolenie administratorów Systemu w zakresie korzystania z jego pełnej funkcjonalności. Szkolenia muszą się odbyć w siedzibie Zamawiającego.
5. Dostarczenie mechanizmu (w postaci skryptu, bądź innego rozwiązania programowego) do archiwizacji całości Systemu umożliwiającego odtworzenie kompletnego Systemu na dowolny dzień.
6. 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.

7. 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.
8. System musi umożliwiać generowanie raportów oraz musi być możliwość eksportu generowanych raportów do formatu plików .xlsx, .pdf.
9. 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.
10. System musi posiadać zaimplementowane mechanizmy ochrony danych, w tym: rozliczalności, autentykację oraz uwierzytelnianie.
11. 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).
12. System musi być dostarczony jako jedna lub wiele aplikacji oferujących narzędzia wspierające osoby odpowiedzialne za bezpieczeństwo teleinformatyczne w co najmniej następujących obszarach:
    a) nadzór nad bezpieczeństwem Urzędu,
    b) zarządzanie ryzykiem organizacji w obszarze teleinformatycznym,
    c) zapewnienie zgodności systemów teleinformatycznych z wymaganiami bezpieczeństwa (zgodnie z rozporządzeniem KRI i ustawą o KSC).
13. System musi posiadać zaimplementowane narzędzia umożliwiające co najmniej:
    a) pełnienie nadzoru nad bezpieczeństwem procesów oraz danych elektronicznych wskazanych przez Zamawiającego,
    b) zarządzanie ryzykiem organizacji w obszarze teleinformatycznym,
    c) zapewnienie zgodności systemów teleinformatycznych z wymaganiami norm

bezpieczeństwa ISO-27001.

14. Rozwiązanie ma gwarantować możliwość elastycznej rozbudowy o dalsze zasoby, które w przyszłości zostaną objęte jego działaniem.
15. System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych.
16. 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.
17. Rozwiązanie musi zawierać narzędzia graficzne do tworzenia i przeszukiwania elektronicznej dokumentacji prezentujące wyniki na schemacie mapy logicznej oraz fizycznej.
18. System musi być wyposażony w mechanizmy zautomatyzowanego, dynamicznego uzupełniania elektronicznej dokumentacji na podstawie danych pozyskanych z logów i informacji o ruchu sieciowym (Netflow), protokołów SNMP, WMI, SSH, skanerów podatności oraz skryptów PowerShell za pomocą których musi istnieć możliwość precyzyjnego określenia zakresu danych, które mają zostać uzupełnione. System musi posiadać repozytorium gotowych skryptów oraz graficzny interfejs pozwalający na tworzenie nowych skryptów, obejmujący możliwość przekazywania do nich parametrów wejściowych.
19. Mechanizmy automatycznego uzupełniania dokumentacji elektronicznej muszą uwzględniać informacje o typach zasobów (np. serwer WWW, baza danych, serwer plików, stacja robocza) oraz zależnościach między tymi zasobami (np.: stacja robocza łączy się do serwera baz danych).
20. Elektroniczna dokumentacja infrastruktury teleinformatycznej musi pozwalać na wprowadzenie informacji o procesach biznesowych oraz technicznych oraz określania powiązań procesów z elementami infrastruktury (np.: serwer X związany jest z procesami A i B).
21. Interfejs systemu elektronicznej dokumentacji musi umożliwiać wizualizację informacji o infrastrukturze teleinformatycznej. Wizualizacja musi obejmować interaktywną mapę logiczną sieci z zaznaczonymi strefami sieci, strefami bezpieczeństwa, urządzeniami

sieciowymi, połączeniami, systemami zabezpieczeń IT oraz procesami.

22. System musi umożliwiać uwzględnianie danych zgromadzonych w elektronicznej dokumentacji infrastruktury teleinformatycznej w mechanizmach korelacji zdarzeń. Wykryte zdarzenia/incydenty będą priorytetyzowane w odniesieniu do ważności dla organizacji zasobów, których dotyczą (np.: wspomaganych procesów, przetwarzanych informacji klasyfikowanych).
23. 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.
24. 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.
25. System powinien zapewnić mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu teleinformatycznego zdefiniowanego w elektronicznej dokumentacji oraz prezentację tych informacji w formie graficznej.
26. 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.
27. 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.
28. System musi posiadać interfejs pozwalający na definiowanie nowych warunków szacowania ryzyka wpływających bezpośrednio na wynik dotychczasowej analizy.
29. Mechanizmy modułu dokumentacji elektronicznej muszą umożliwiać powiązanie danych o zasobach z informacjami pozyskanymi w rezultacie skanowania podatności.
30. System musi korelować zdarzenia wysyłane z innych systemów, w tym systemów zabezpieczeń, względem informacji zawartych w elektronicznej dokumentacji.

31. 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).
32. 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.
33. System, moduł dokumentacji elektronicznej oraz moduł obsługi incydentów SOAR muszą być wyposażone w interfejsy API umożliwiające dwustronną integrację z systemami zewnętrznymi.
34. System musi zawierać elektroniczną dokumentację umożliwiającą prowadzenie rejestru czynności i kategorii czynności przetwarzania danych osobowych, opisanych w artykule 30 RODO.
35. System powinien pozwalać na zdefiniowanie tak zwanego Zarządzania Incydentami to znaczy powinien co najmniej wspierać użytkowników poprzez mechanizmy podpowiedzi, wskazywania procedur wspierających rozwiązanie danego typu incydentu, wraz z możliwością odznaczania każdego z wykonanych kroków.
36. System musi mieć możliwość tworzenia nowych incydentów automatycznie, na podstawie zdarzeń z innych systemów, oraz ręcznie.
37. System musi być wyposażony w moduł obsługi incydentów SOAR (Security Orchestration, Automation And Response) raportowanych przez mechanizmy korelacji zdarzeń. Moduł obsługi incydentów może stanowić integralną część systemu lub być dostarczony w ramach odrębnego, zintegrowanego z systemem rozwiązania.
38. System musi być wyposażony w mechanizmy reguł opartych na mechanizmach behawioralnych z możliwością agregacji danych oraz punktowania poszczególnych zdarzeń w wyznaczonych oknach czasowych. W rezultacie działania reguł behawioralnych system powinien tworzyć incydenty związane z przekroczeniem dozwolonych zakresów punktacji dla

zdarzeń zaobserwowanych w oknie czasowym agregacji.

39. System musi zawierać mechanizm definiowania scenariuszy obsługi incydentów uruchamianych na podstawie co najmniej następujących kryteriów:
    a) w przypadku gdy zasób przetwarza zdefiniowane informacje klasyfikowane (np. dane osobowe),
    b) w przypadku gdy zasób jest elementem określonego procesu organizacji,
    c) w przypadku gdy zasób zlokalizowany jest w danej lokalizacji,
    d) w przypadku gdy na zasobie może dojść do określonej konsekwencji naruszenia bezpieczeństwa,
    e) w przypadku gdy na zasobie jest zainstalowany określony system operacyjny lub oprogramowanie,
    f) w przypadku określonego statusu.
40. W ramach obsługi incydentów bezpieczeństwa system musi umożliwić przygotowanie gotowych scenariuszy obejmujących co najmniej:
    a) definiowanie warunków wykonania oraz sposób ich obsługi,
    b) zmianę operatora,
    c) uruchomienie skryptu PowerShell,
    d) skryptu np. bash, sh, zdalnie logując się przy użyciu protokołu SSH,
    e) uruchomienie komendy z linii poleceń,
    f) uruchomienie zdefiniowanej wcześniej strony internetowej,
    g) wysłanie powiadomienia,
    h) aktualizację dokumentu wraz z jego automatycznym wersjonowaniem.
41. System musi automatycznie podpowiadać odpowiednie scenariusze obsługi incydentów. Scenariusze obsługi muszą mieć możliwość ich symulacji i weryfikacji, m.in. na przykładowym zasobie teleinformatycznym.
42. Moduł obsługi incydentów musi wspierać proces obsługi incydentów. W ramach procesu każdy incydent musi przejść proces selekcji, analizy, oceny wpływu i reakcji. W ramach procesu każdy incydent musi przyjmować stany właściwe dla etapów procesu obsługi incydentów np.: nowe zdarzenie, incydent, fałszywy alarm, incydent zamknięty.
43. Moduł obsługi incydentów musi umożliwiać przydzielanie zadań w ramach obsługi incydentu.

44. Moduł obsługi incydentów musi zapewnić graficzny interfejs wspierający proces obsługi incydentów, którego zadaniem będzie wspieranie użytkownika w realizacji zadań związanych z selekcją zdarzeń, analizą incydentów, oceną wpływu i reakcją na incydenty. Do zadań tych należą między innymi:
    a) wzbogacanie danych kontekstowych,
    b) gromadzenie artefaktów danych związanych z incydentem,
    c) współpraca z innymi członkami zespołu,
    d) komunikacja w ramach zespołu,
    e) wykonywanie czynności związanych z reakcją na incydent,
    f) raportowanie przebiegu incydentu.
45. Interfejs modułu obsługi incydentów musi prezentować dane na temat incydentu:
    a) zdarzenia związane z incydentem,
    b) informacje o zasobach związanych z incydentem na podstawie danych zgromadzonych w elektronicznej dokumentacji infrastruktury teleinformatycznej;
    c) informacje o wynikach szacowania ryzyka dla zasobów związanych z incydentem,
    d) informacje o zadaniach wyznaczonych w ramach obsługi incydentu,
    e) listę powiązanych incydentów,
    f) listę podatności zasobów związanych z incydentem.
46. Moduł obsługi incydentów musi być wyposażony w mechanizmy automatycznego dopasowania scenariuszy do incydentów. Dopasowanie musi uwzględniać co najmniej:
    a) priorytet incydentu wynikający z rezultatów działania reguł korelacji zdarzeń,
    b) ważność zasobu związanego z incydentem ustalana automatycznie na podstawie informacji uzyskanych z modułu dokumentacji elektronicznej,
    c) typ zasobu, którego dotyczy incydent ustalony automatycznie na podstawie informacji pozyskanych z modułu dokumentacji elektronicznej,
    d) aktualny status zdarzenia bądź incydentu w procesie obsługi incydentu.
47. Moduł obsługi incydentów musi rejestrować wszystkie czynności wykonane przez użytkownika w ramach realizacji scenariuszy.
48. Moduł obsługi incydentów musi umożliwiać ustalanie przewidzianych czasów reakcji i czasów obsługi dla incydentów ze względu na ich priorytet. System musi dokonywać automatycznego pomiaru czasów reakcji na incydenty oraz czasów obsługi incydentów.

Wyniki pomiaru czasu powinny być stale aktualizowane i prezentowane w interfejsie systemu.

49. Moduł obsługi incydentów musi być wyposażony w mechanizm automatycznego powiadamiania wskazanych adresatów o nowych incydentach, zmianach statusów incydentów, przekroczeniach czasów reakcji i obsługi.
50. Moduł obsługi incydentów powinien umożliwiać automatyczne przesyłanie powiadomień do osób wskazanych w elektronicznej dokumentacji infrastruktury teleinformatycznej jako właściciele zasobów i właściciele procesów.
51. System musi być wyposażony w graficzny interfejs prezentujący w formie wykresów dane statystyczne związane z procesem obsługi incydentów. Wykresy muszą umożliwiać prezentację danych uwzględniających co najmniej:
    a) ilość incydentów w czasie, w podziale na priorytety,
    b) czasy reakcji i obsługi,
    c) ilości incydentów obsługiwanych przez poszczególnych użytkowników.
52. 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.
53. System w razie wykrycia incydentów o poważnych konsekwencjach dla organizacji umożliwia automatyczne powiadamianie o zdarzeniu wskazanych pracowników, m.in. za pomocą email i SMS.
54. Incydenty powinny być oznaczane pod względem istotności i priorytetu w oparciu o informacje pozyskane ze zdarzeń, zawartość elektronicznej dokumentacji oraz szacowanie ryzyka.
55. 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.

56. 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:
    a) wyznaczania źródła zagrożenia zasobu teleinformatycznych wraz z wynikiem analizy ryzyka dla tego zagrożenia wyliczanym w sposób automatyczny,
    b) wyświetlania zabezpieczeń zasobu teleinformatycznego przed potencjalnymi źródłami zagrożenia,
    c) wyświetlania zabezpieczeń chroniących zasoby teleinformatyczne przed określonym źródłem zagrożenia,
    d) wyświetlania lokalizacji zasobów określonego rodzaju,
    e) wyświetlania najbardziej narażonych zasobów teleinformatycznych,
    f) wyświetlania ważnych zasobów teleinformatycznych narażonych na awarie.
57. Musi istnieć funkcjonalność, umożliwiająca dołączanie do informacji o incydencie dodatkowych załączników i linkowania do zewnętrznych systemów np. klasy forensics analysis.
58. System musi posiadać predefiniowany zestaw reguł analizy incydentów.
59. Dla zdarzeń zawierających adresy IP interfejs musi umożliwiać wyświetlenie dodatkowych informacji o zasobach powiązanych z tymi adresami m.in.: nazwa zasobu, rodzaj zasobu, powiązane procesy, właściciel zasobu, podatności zasobu, powiązane incydenty, lokalizacja.
60. System musi umożliwić zbieranie i przetwarzanie informacji dotyczących przepływów sieciowych [ang. Netflow].
61. System powinien zapewnić możliwość wykrywania topologii sieci fizycznej oraz jej wizualizacji na podstawie następujących protokołów sieciowych: SNMP (w wersji 2 i 3), LLDP lub CDP.
62. System musi zapewnić odbiór lub pobieranie danych za pośrednictwem protokołów SYSLOG oraz NetFlow, mechanizmu Windows Event Forwarding (WEF) oraz sterownika ODBC. System musi umożliwiać odbieranie i automatyczne przetwarzanie wiadomości email.
63. System musi umożliwiać automatyczne pobieranie logów audytowych systemów baz danych.
64. System musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych danych przez ich podział na pola, na podstawie których może odbywać się dalsze

przetwarzanie oraz wyszukiwanie danych. Mechanizm musi umożliwiać m.in. parsowanie warunkowe, parsowanie hierarchiczne, wzbogacanie zdarzeń o dodatkowe pola, mapowanie wartości, czy wykorzystanie gotowych parserów przy tworzeniu nowych.

65. Proces normalizacji (parsowania) musi odbywać się na bieżąco na etapie rejestrowania danych w systemie.
66. Normalizacja musi uwzględniać możliwość nadawania kategorii zdarzeń na podstawie wartości parsowanych pól.
67. System musi posiadać predefiniowany zestaw reguł normalizacji (parsowania) logów dla popularnych źródeł logów takich jak: urządzenia sieciowe, systemy bezpieczeństwa, systemy Windows i Linux, Active Directory.
68. System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) logów z niestandardowych źródeł danych, w oparciu o składnię wyrażeń regularnych, JSON oraz XML. System musi umożliwiać zastosowanie wszystkich typów składni dla pojedynczego zdarzenia.
69. 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.
70. System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń które mają zostać odrzucone, poddane regułom korelacyjnych lub zagregowane.
71. System musi pozwolić na definiowanie różnych wartości okien czasowych w zależności od rodzajów przetwarzanych zdarzeń celem efektywnego wykorzystania zasobów sprzętowych w regułach korelacji.
72. 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.
73. System musi umożliwiać uwzględnianie wyników szacowania ryzyka w mechanizmach korelacji zdarzeń.
74. Rozwiązanie musi mieć możliwość kategoryzacji każdego rodzaju przetwarzanych logów

(przypisania zdarzenia do określonej kategorii np. logowanie, wylogowanie, zmiana uprawnień, atak brute force, malware, exploit, suspicious, vulnerability, DOS, recon itp.).

75. System powinien zapewnić mechanizmy umożliwiające rozpoznanie systemów teleinformatycznych (Asset Discovery) oraz zapisanie wyników w module elektronicznej dokumentacji, zapewniając:
    a) możliwość wykrywania zasobów oraz ich parametrów na podstawie wyników przynajmniej jednego skanera podatności,
    b) możliwość wykrywania zasobów oraz ich parametrów na podstawie wyników przynajmniej jednego skanera sieciowego,
    c) możliwość wykrywania zasobów oraz ich parametrów przy wykorzystaniu protokołu WMI,
    d) możliwość wykrywania zasobów oraz ich parametrów przy wykorzystaniu skryptów powłoki systemowej zdalnie lub przy użyciu klienta protokołu SSH lub PowerShell,
    e) możliwość wykrywania parametrów urządzeń fizycznych na bazie protokołu SNMP w wersji 2 i 3.
76. 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).
77. System musi zapewnić możliwość wykrywania ilościowego odchylenia natężenia zdarzeń od ich typowego rozkładu (dobowego, tygodniowego, miesięcznego, etc.).
78. System musi zawierać możliwość definiowania alarmów związanych z ilościowym odchyleniem natężenia zdarzeń w stosunku do komunikacji działającej w ramach zdefiniowanych procesów biznesowych.
79. 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.
80. System w formie graficznej musi umożliwić podsumowanie aktualnego stanu

bezpieczeństwa, m.in. procesy organizacji zagrożone przez incydenty bezpieczeństwa, procesy organizacji zagrożone przez pojedyncze punkty awarii, średni czas reakcji na incydent bezpieczeństwa oraz średni czas obsługi podatności.

81. 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.
82. 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.
83. 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.:
    a) zweryfikowanie, czy stan bezpieczeństwa systemu teleinformatycznego odpowiada specyficznym wymaganiom organizacji,
    b) wyznaczanie zasobów teleinformatycznych o wysokim poziomie ryzyka, które nie posiadają wymaganych zabezpieczeń,
    c) wskazywanie zasobów teleinformatycznych o krytycznym znaczeniu dla organizacji, które nie posiadają odpowiednich zabezpieczeń.
84. System musi być wyposażony w graficzny interfejs umożliwiający przeglądanie i przeszukiwanie zarejestrowanych danych w formie znormalizowanej i pierwotnej. Interfejs musi prezentować wyniki wyszukiwania z zastosowaniem filtrów opartych na wartościach pól, złożonych wyrażeniach logicznych, wskazaniach zakresu czasowego i źródła danych. Interfejs wyszukiwania musi umożliwiać zapisywanie zapytań z możliwością ich ponownego wykorzystania w przyszłości. Tworzenie zapytań musi być możliwe poprzez bezpośrednie wskazanie pola zdarzenia za pomocą wskaźnika myszy i dodanie tego pola do filtra wyszukiwania, wraz z określeniem warunków wyszukiwania przez wyrażenie logiczne.
85. Informacje o procesach muszą uwzględniać ważność procesów dla organizacji, typy danych przetwarzanych w ramach procesów (np. dane osobowe, informacje poufne itp.), właścicieli

procesów, relacje między procesami (np. proces A zależy od procesu B, przy czym zależności powinny być prezentowane w formie graficznej) oraz czas trwania procesów (np. proces praca biurowa w organizacji jest aktywny od poniedziałku do piątku od 8:00 do 16:00).

86. System musi zawierać możliwość definiowania scenariuszy obsługi podatności uruchamianych na podstawie co najmniej następujących kryteriów:
    a) w przypadku gdy zasób przetwarza zdefiniowane informacje klasyfikowane (np. dane osobowe),
    b) w przypadku gdy zasób jest elementem określonego procesu organizacji,
    c) w przypadku gdy zasób zlokalizowany jest w danej lokalizacji,
    d) w przypadku gdy na zasobie może dojść do określonej konsekwencji naruszenia bezpieczeństwa,
    e) w przypadku gdy na zasobie jest zainstalowany określony system operacyjny lub oprogramowanie,
    f) w przypadku określonego statusu.
87. W ramach obsługi podatności system musi umożliwić przygotowanie gotowych scenariuszy obejmujących:
    a) definiowanie warunków wykonania oraz sposób ich obsługi,
    b) zmianę operatora,
    c) uruchomienie skryptu PowerShell,
    d) skryptu np. bash, sh, zdalnie logując się przy użyciu protokołu SSH,
    e) uruchomienie komendy z linii poleceń,
    f) uruchomienie zdefiniowanej wcześniej strony internetowej,
    g) wysłanie powiadomienia,
    h) aktualizację dokumentu wraz z jego automatycznym wersjonowaniem.
88. System musi automatycznie podpowiadać odpowiednie scenariusze obsługi podatności. Scenariusze obsługi muszą mieć możliwość ich symulacji i weryfikacji, m.in. na przykładowym zasobie teleinformatycznym.
89. 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.
90. 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).

91. 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.
92. System powinien w formie graficznej prezentować podsumowanie aktualnego stanu bezpieczeństwa, m.in. procesy organizacji zagrożone przez podatności, średni czas obsługi podatności.
93. 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.
94. System musi automatycznie ustalać priorytety podatności w odniesieniu do ważności podatnych systemów IT dla organizacji oraz oceny technicznej zagrożenia bazującej na wartości CVSS lub wartości pozyskanej bezpośrednio z silnika skanera.
95. 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.
96. System musi zawierać mechanizm definiowania harmonogramów skanowania podatności (tzn. narzędzi Vulnerability Assessment) oraz na ich podstawie automatycznie uruchamiać procesy skanowania i analizować pozyskane raporty.
97. System musi umożliwiać szacowanie ryzyka wraz z oceną skutków dla ochrony danych osobowych (Data Protection Impact Assessment).
98. System musi umożliwiać zdefiniowanie obszarów przetwarzania zbiorów danych osobowych wraz z listą zastosowanych dla nich zabezpieczeń fizycznych.
99. System musi umożliwiać rejestrację zgłoszeń incydentów dotyczących danych osobowych związanych z poszczególnymi zbiorami, jednostkami organizacyjnymi, osobami, lokalizacjami oraz związanych z zasobami informatycznymi.

100. 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.

101. 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.

102. System w ramach modułu ochrony danych osobowych musi oferować możliwość:
   a) szacowania ryzyka cyber zagrożeń dla zasobów IT przetwarzających dane osobowe,
   b) szacowania ryzyka ryzyka utraty dostępności, poufności i integralności danych wykonywana dla poszczególnych celów przetwarzania (uwzględniająca zabezpieczenia techniczne i organizacyjne) wraz z oceną skutków dla ochrony danych osobowych (tzw. Data Protection Impact Assessment),
   c) prowadzenia wykazów programów i systemów informatycznych, służących przetwarzaniu danych osobowych,
   d) prowadzenia ewidencji osób upoważnionych, wraz z możliwością generowania upoważnień oraz oświadczeń o poufności,
   e) prowadzenia ewidencji udostępnień danych osobowych,
   f) rejestracji i obsługi roszczeń związanych z przetwarzaniem danych osobowych.

103. System musi być wyposażony w dostarczone przez producenta API (wraz z dokumentacją), umożliwiające jego integrację z systemami zewnętrznymi.

104. System musi zawierać mechanizm integracji ze skanerami podatności co najmniej dwóch producentów oraz co najmniej jednym skanerem podatności dostępnym na zasadach open source. W ramach integracji system musi mieć możliwość uruchamiania skanowania podatności i importowania jego wyników w celu ich dalszego procesowania.

105. 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.

106. System do zarządzania bezpieczeństwem teleinformatycznym musi umożliwiać integrację z używanym przez Zamawiającego systemem SIEM Splunk Enterprise Security w zakresie pobierania i aktualizowania incydentów. Integracja powinna być jednokierunkowa w zakresie:

a) pobrania nowych incydentów z systemu SIEM za pomocą m.in. syslog,

b) możliwości wykonywania zapytań w systemie SIEM w celu wzbogacenia informacji w trakcie prowadzenia śledztwa w Systemie zarządzania bezpieczeństwem,

c) możliwości synchronizacji komentarzy.

Realizacja powyższych funkcjonalności może zostać zrealizowana za pomocą API.

107. 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.

108. 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.

109. 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 7:30 do 15:30). Zależności powinny być prezentowane w postaci graficznej.

110. Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień do innych systemów bądź zdefiniowanych użytkowników (m.in. powiadamianie email, SMS).

111. System musi zapewniać rozliczalność działań wykonanych przez każdego z użytkowników i możliwość przeglądania zdarzeń powiązanych z danym incydentem, użytkownikiem, bądź obiektem.

112. System musi umożliwiać budowanie profili aktywności użytkowników oraz zasobów IT

poprzez wielowartościowe listy referencyjne i wykorzystywać je w regułach korelacyjnych.

113. System musi umożliwiać funkcjonalność retencji tj. zapewnić przechowywanie logów oraz danych historycznych, mogących umożliwiać korelację zdarzeń w różnych okresach i z różnych zdarzeń, w przypadku wystąpienia incydentu, przeprowadzenie dochodzenia dotyczącego zidentyfikowania naruszenia zasad bezpieczeństwa.

114. Wykonawca zobowiązuje się do zapewnienia odpowiedniego poziomu bezpieczeństwa informacji w dostarczanym przedmiocie zamówienia, zgodnie z zapisami zawartymi w § 20 ust. 2 pkt 12 i 13 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.