Załącznik Nr 1 do SIWZ

OPIS PRZEDMIOTU ZAMÓWIENIA – SPECYFIKACJA TECHNICZNA

Zakup i wdrożenie rozwiązań zwiększających poziom bezpieczeństwa systemów informacyjnych i sieci teleinformatycznej Starostwa Powiatowego w Kielcach w ramach projektu „Poprawa poziomu cyberbezpieczeństwa Starostwa Powiatowego w Kielcach w ramach projektu grantowego CYBERBEZPIECZY SAMORZĄD", dofinansowanego z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Część 1. Dostawa oprogramowania służącego do przeciwdziałania cyberzagrożeniom, oferująca możliwości wykrywania i obsługi zdarzeń, incydentów oraz podatności na potrzeby Starostwa Powiatowego w Kielcach.

Część 2. Dostawa systemu zarządzania hasłami i dostępem uprzywilejowanym na potrzeby Starostwa Powiatowego w Kielcach.

Część 3. Dostawa i wdrożenie zabezpieczenia sieciowego w postaci rozwiązania typu Firewall na potrzeby Starostwa Powiatowego w Kielcach.

Spis treści

1. **Dostawa oprogramowania służącego do przeciwdziałania cyberzagrożeniom, oferująca możliwości wykrywania i obsługi zdarzeń, incydentów oraz podatności, na potrzeby Starostwa Powiatowego w Kielcach.**

1.1 Ilości.

Oprogramowanie	ILOŚĆ
Dostawa oprogramowania (licencja wieczysta) służącego do przeciwdziałania cyberzagrożeniom, oferująca możliwości wykrywania i obsługi zdarzeń, incydentów oraz podatności na potrzeby Starostwa Powiatowego w Kielcach.	1 szt.

1.2 Postanowienia ogólne.

Przedmiotem zamówienia jest zakup, dostarczenie i wdrożenie łącznie z przeprowadzonym szkoleniem dla minimum trzech pracowników działu IT, w środowisku informatycznym Zamawiającego systemu przeciwdziałającemu cyberzagrożeniom, umożliwiającego ich wykrywanie przy wsparciu mechanizmów uczenia maszynowego oraz zapewniającego automatyzację i orkiestrację ich obsługi.

Poprzez wdrożenie systemu rozumie się dostarczenie, instalację nowego oprogramowania oraz wykonanie konfiguracji w pełni zgodnej z wymaganiami Zamawiającego, sprawdzenie ustawień, przetestowanie i wyeliminowanie ewentualnych nieprawidłowości oraz pozostawienie dokumentacji technicznej i konfiguracyjnej systemu.

Świadczenie usług serwisu gwarancyjnego przez Producenta musi być realizowane min. do dnia 30.06.2026, obejmujących usuwanie zgłoszonych awarii i usterek dla oprogramowania Zamawiającego, a w razie konieczności jego wymianę

W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

W przypadku awarii wymiana lub udostępnienie oprogramowania lub rozwiązania zastępczego najpóźniej następnego dnia roboczego, na czas trwania naprawy. Dostarczone oprogramowanie zastępcze musi posiadać konfiguracje zgodną z wymaganiami Zamawiającego. Zamawiający zobowiązuje się do udostepnienia konfiguracji oprogramowania na czas awarii. Ponadto oprogramowanie zastępcze musi być uruchomione i przetestowane w siedzibie Zamawiającego.

1.3 Opis parametrów technicznych oprogramowania objętego dostawą na potrzeby Starostwa Powiatowego w Kielcach.

1. System musi umożliwić odbieranie logów wygenerowanych przez systemy zabezpieczeń, systemy sieciowe, systemy operacyjne i aplikacje następującymi protokołami: Syslog, TLS syslog, NetFlow, Windows Event Forwarding;

2. Logi pozyskiwane z systemów Microsoft Windows nie mogą wymagać instalowania dedykowanego oprogramowania bezpośrednio na tych systemach;
3. System musi posiadać wbudowane mechanizmy zapewniające możliwość pobierania zdarzeń poprzez wykorzystanie RestFull-API, sterownika ODBC, agenta do czytania plików płaskich, protokołów IMAPS, POP3S, MAPI do pobierania wiadomości ze skrzynek poczty elektronicznej oraz obsługi zapytań WQL w ramach protokołu WMI;
4. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych;
5. System musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych zdarzeń umożliwiający ich podział na poszczególne pola, na podstawie których może odbywać się dalsze przetwarzanie oraz wyszukiwanie ich w systemie;
6. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, obejmującą zmianie wartości tych pól lub dodanie nowych w oparciu o ich wartości lub wzorzec wyszukiwania. Cały proces musi odbywać się na bieżąco na etapie rejestrowania danych w systemie;
7. Proces normalizacji musi wspierać następujące typy składni: CEF, LEEF, URI, SYSLOG (zgodny z RFC 3164) i automatycznie tworzyć na ich podstawie pola i ich wartości zgodne z zasadami określonymi przez te składnie. Parsowanie powyższych składni nie może być realizowane za pomocą wyrażeń regularnych;
8. Normalizacja musi umożliwiać automatyczne nadawanie kategorii zdarzeń w formie nowych pól, np.: logowanie, wylogowanie, zmiana uprawnień, błąd konfiguracji, wykryte skanowanie systemu czy zablokowany malware;
9. Normalizacja logów musi posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól o nazwę lub kod kraju korzystając z wbudowanej w produkt bazy;
10. System musi posiadać predefiniowany zestaw parserów oraz umożliwiać ich wersjonowanie, aby po wgraniu nowej wersji parsera, w razie przypadku, gdy będzie to konieczne przywrócić jedną z poprzednich wersji;
11. System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) dla zdarzeń z niestandardowych źródeł danych, w oparciu o następujące składnie: CEF, LEEF, URI, XML, JSON, SYSLOG, REGEX. System musi umożliwiać zastosowanie wszystkich typów składni dla pojedynczego zdarzenia, przykładowo pole „msg" znormalizowane automatycznie według standardu CEF powinno mieć możliwość dalszej normalizacji np.: zgodnej z URI lub REGEX;
12. Proces normalizacji musi posiadać możliwość optymalizacji, poprzez automatyczny dobór odpowiedniego parsera dla źródła logów w zależności od składni, w której te logi są przesyłane. Przykładowo, jeżeli logi są przesyłane w standardzie CEF system dobierze odpowiedni parser, w przypadku, gdy źródło zmieni format generowania zdarzeń na LEEF system musi automatycznie zmienić parser bez ingerencji operatora;
13. System musi rejestrować i przechowywać pozyskane logi w postaci surowej (RAW) oraz znormalizowanej;
14. System musi być wyposażony w graficzny interfejs umożliwiający określenie miejsca składowania logów (wskazania właściwego repozytorium logów) w zależności od zwartości tych logów, gdzie reguły przekierowania muszą umożliwiać definiowanie warunków po wszystkich sparsowanych polach. Przykładowo, jeżeli w zdarzeniu znajduje się informacja o danych poufnych to zdarzenie to zostanie przekierowane do repozytorium A, natomiast w przypadku, gdy tej informacji nie będzie to zdarzenie zostanie przekierowane do repozytorium B;
15. Każde z repozytorium logów musi mieć możliwość definiowania własnych zasad retencji uwzględniających zdefiniowanie okresu przechowywania lub ilości miejsca przeznaczonego na

dane repozytorium. Dla każdego z repozytorium w przypadku jego zapełnienia musi być możliwa konfiguracja, która zapewni automatyczne przeniesienie logów do archiwum lub umożliwi ich nadpisanie;

16. System musi umożliwiać fizyczne rozdzielenie repozytoriów logów pobieranych z systemów informatycznych od repozytoriów zdarzeń generowanych w ramach systemu, w tym m.in. odseparowanie zdarzeń korelacyjnych na oddzielne repozytoria danych składowane na osobnych serwerach i dedykowanych do tego celu zasobów dyskowych od wszelkich repozytoriów logów;
17. Ze względu na możliwość wygenerowania dużej ilości danych przez algorytmy uczenia maszynowego system musi mieć możliwość rozdzielenia ich składowania na osobny serwer i dedykowane zasoby dyskowe;
18. System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych w postaci skompresowanej;
19. System musi zapewnić mechanizmy bezpieczeństwa dla danych przechowywanych w repozytoriach uniemożliwiające ich nieautoryzowaną modyfikację oraz zapewnić operatorom mechanizmy weryfikacyjne integralność danych;
20. System musi udostępniać możliwość konfiguracji automatycznego odrzucenia logów niezawierających istotnych dla zamawiającego informacji. Definiowanie, które logi mają zostać odrzucone i niezapisane w repozytorium logów musi być realizowane za pomocą reguł, które pozwolą zdefiniować warunki po wszystkich sparsowanych polach;
21. System musi być wyposażony w graficzny interfejs umożliwiający przeglądanie i przeszukiwanie zarejestrowanych zdarzeń 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;
22. System musi zapewniać możliwość utrzymywania dokumentacji sieci, systemów oraz usług, umożliwiającej na gromadzenie i edycję danych istotnych w kontekście oceny generowanych przez system zdarzeń bezpieczeństwa;
23. Elektroniczna dokumentacja musi posiadać możliwość wizualizacji w formie interaktywnej mapy sieci, gdzie na pierwszym planie będą widoczne urządzenia zabezpieczeń, strefy bezpieczeństwa oraz połączenia sieciowe wskazujące jakie mechanizmy zabezpieczeń chronią poszczególne strefy bezpieczeństwa. „Kliknięcie" na dowolny z obiektów na pierwszym planie musi pozwolić na podgląd oraz edycję parametrów tego obiektu. Przykładowo po kliknięciu na strefę bezpieczeństwa musi istnieć możliwość definiowania komputerów należących do tej strefy, ich adresacji oraz innych z nimi związanych parametrów;
24. System musi umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji również w formie tabelarycznej;
25. System musi pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci, np.: poziom krytyczności systemów oraz usług;
26. System musi umożliwiać generowanie elektronicznej dokumentacji sieci i systemów w sposób automatyczny na podstawie dostarczonych przez producenta reguł wykrywania oraz edytora graficznego pozwalającego utworzyć dodatkowe reguły;

27. System musi zawierać narzędzia służące do ustalania wrażliwych zbiorów informacji, jakie są narażone w razie incydentu bezpieczeństwa. Ma umożliwiać definiowanie własnego schematu klasyfikacji danych w organizacji (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;
28. Definiowanie reguł wykrywania musi bazować na sparsowanych polach oraz wyszukanych zależnościach między różnymi zdarzeniami z wielu źródeł oraz po aktywacji automatycznie uzupełnić elektroniczną dokumentację o następujące informacje:

a) nowe zasoby wykryte w sieci,
b) typy wykrytych zasobów (np.: serwer lub stacja robocza),
c) zastosowane na nich zabezpieczenia,
d) usługi z którymi się komunikują,
e) nowe usługi wykryte na zasobie,
f) komunikację do usług wykrytych na zasobie.

29. System musi umożliwiać uwiarygodnianie uzyskiwanych informacji na bazie wartości progowych osiągniętych w zadanej jednostce czasu i dopiero po ich uwiarygodnieniu uzupełniać automatycznie elektroniczną dokumentację;
30. System powinien posiadać zestaw predefiniowanych reguł do automatycznego uzupełniania elektronicznej dokumentacji, których uruchomienie będzie automatycznie aktualizować elektroniczną dokumentację bez ingerencji operatora;
31. Interfejs interaktywnej mapy sieci musi posiadać mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT który został zdefiniowany w elektronicznej dokumentacji oraz nazwę usługi której ta komunikacja dotyczy;
32. System musi posiadać wbudowaną bazę wskaźników kompromitacji, która umożliwi zbieranie, przechowywanie oraz przypisywanie wskaźników kompromitacji (IoC) do incydentów. Baza powinna obsługiwać protokół TLP w wersji 2.0 oraz obsługiwać następujące typy wskaźników:

a) fqdn,
b) e-mail,
c) nazwa pliku,
d) ścieżka do pliku,
e) hash,
f) adres IP,
g) klucz rejestru,
h) cmd.

33. System musi umożliwiać synchronizację wskaźników kompromitacji (IOC) z platformami dostępnymi publicznie. Wymagane jest aby produkt posiadał gotowy mechanizm pobierania wskaźników z platformy MISP (https://www.misp-project.org/);
34. System musi umożliwiać definiowanie list referencyjnych zarówno z jedną wartością jak i łączących unikalne wartości w pojedynczym wierszu (np: obraz pliku, hash, nazwa procesu);
35. Listy referencyjne muszą mieć możliwość synchronizacji z listami publikowanymi publicznie (np.: „Malicious IPs", „Malicious domain" czy „Tor Exit Nodes");
36. System musi być zintegrowany z usługą katalogową Microsoft Active Directory celem pobrania informacji o poświadczeniach oraz atrybutach użytkowników i komputerów zarejestrowanych w domenie. Minimum to: nazwa komputera wraz z systemem operacyjnym, nazwa użytkownika, login, e-mail, przynależność do grup, przełożonego, jednostkę organizacyjną oraz listę kont uprzywilejowanych;

37. System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać możliwość jej synchronizacji z usługą katalogową Microsoft Active Directory;
38. System musi umożliwiać analizę konfiguracji systemów IT poprzez ich skanowanie bezpośrednio w ramach mechanizmów dostępnych w samym rozwiązaniu oraz poprzez integrację ze skanerami podatności. Oczekiwanym wynikiem analizy jest lista niezgodności (np: czy na zasobie jest ustawione wymuszanie zmiany haseł w zadanym okresie czasu);
39. System powinien posiadać zestaw predefiniowanych reguł weryfikacji konfiguracji zasobów IT;
40. System musi zawierać mechanizm integracji ze skanerami podatności co najmniej trzech producentów. W ramach integracji system musi mieć możliwość uruchamiania skanowania podatności, importowania jego wyników zawierających listę podatności i ich atrybuty oraz możliwość kasowania ze skanera zaimportowanych wcześniej skanów. Wszystkie powyższe operacje muszą być konfigurowalne z poziomu graficznego interfejsu systemu;
41. Rozwiązanie musi zawierać mechanizm pasywnej analizy podatności, obejmującej systemy IT uzupełnione o informację zgodne z słownikiem CPE (ang. Common Platform Enumeration), umożliwiającą import wykrytych podatności zasobu do systemu z publicznie dostępnej bazy CVE (ang. Common Vulnerabilities and Exposures) i dalszą obsługę tych podatności w systemie;
42. System musi umożliwiać mapowanie zdarzeń bezpieczeństwa na poszczególne techniki z bazy wiedzy MITRE ATT&CK® oraz zapewniać mechanizmy filtrowania zdarzeń po tych technikach oraz wyświetlania szczegółów związanych z daną techniką, w szczególności:
    a) id techniki,
    b) taktykę,
    c) platformy których dotyczy,
    d) potencjalne źródła,
    e) opis zagrożenia,
    f) mityzację,
    g) sposób detekcji,
    h) referencje.
43. System w swoim działaniu musi korzystać z wbudowanych algorytmów uczenia maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników i komputerów;
44. Modele zachowania użytkowników (UBA) i komputerów (EBA) muszą być tworzone automatycznie na bazie zdarzeń historycznych ze skonfigurowanego (wskazanego) okresu lub zdefiniowanej ilości zdarzeń wymaganych do ukończenia procesu nauczania. Algorytm nauczania musi mieć możliwość konfiguracji sposobu odrzucania wartości skrajnych mogących wpłynąć negatywnie na wyniki procesu nauczania oraz umożliwić odrębne uczenie w ramach zdefiniowanych zakresów czasowych (np.: rozdzielenie zdarzeń do nauczania w godzinach pracy od zdarzeń po godzinach pracy);
45. System musi posiadać zestaw predefiniowanych i konfigurowalnych reguł do automatycznego przyporządkowania użytkowników i zasobów do właściwych profili nauczania, reguły te muszą zapewnić minimum:
    a) rozdzielenie procesu nauczania zachowania użytkowników uprzywilejowanych od użytkowników nieuprzywilejowanych;
    b) rozdzielenie procesu nauczania zachowania stacji roboczych od serwerów;
    c) rozdzielenie serwerów świadczących usługi w sieci Internet od serwerów świadczących usługi lokalnie w organizacji;
    d) rozdzielenie procesu nauczania serwerów należących do domeny od pozostałych serwerów.

46. System uczenia maszynowego musi posiadać wbudowane mechanizmy nie wymagające żadnej dodatkowej konfiguracji, które po zakończeniu procesu nauki umożliwią detekcję anomalii zachowania użytkowników oraz zasobów (UEBA);
47. Wykryte przez mechanizmy uczenia maszynowego anomalie muszą generować zdarzenia, zawierające minimum informację o użytkowniku lub adresie IP na którym została wykryta anomalia oraz wykorzystany algorytm. System musi umożliwiać wykorzystanie tych zdarzeń w celu dalszej korelacji;
48. System musi pozwalać na zautomatyzowaną ocenę wpływu incydentu bezpieczeństwa IT na działalność organizacji względem zagrożeń natury informatycznej (np: utrata wizerunku, związana z zagrożeniem przełamania zabezpieczeń serwera webowego organizacji dostępnego z sieci Internet);
49. System musi zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role;
50. Dostarczone rozwiązanie musi umożliwiać gromadzenie i korelacje zdarzeń przesyłanych lub pobieranych z innych systemów. Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł oraz ich agregację;
51. System musi posiadać interfejs graficzny do tworzenie własnych reguł korelacyjnych odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie. Korelacja musi odbywać się na bieżąco na etapie rejestrowania danych w systemie a mechanizm tworzenie reguł musi uwzględniać:
    a) sparsowane pola oraz ich wartości,
    b) listy referencyjne,
    c) atrybuty użytkowników z Active Directory,
    d) atrybuty komputerów z Active Directory,
    e) bazę wskaźników kompromitacji (IOC),
    f) informacje z elektronicznej dokumentacji,
    g) anomalie w zachowaniu użytkowników (UBA),
    h) anomalie w zachowaniu zasobów (EBA),
    i) podatności na zasobach,
    j) wyniki analizy konfiguracji,
    k) techniki MITRE ATT&CK®.
52. Reguły korelacyjne bazujące na sparsowanych polach i ich wartościach muszą umożliwić:
    a) wykrycie dowolnej treści w logach,
    b) wykrycie zmiany jednego z kilku pól,
    c) wykrycie zaniku wiadomości,
    d) wykrycie nowej wartości pola w zadanym okresie czasu,
    e) wykrycie incydentu będącego pochodną zdarzeń występujących w określonej kolejności,
    f) wykrycie zdefiniowanej ilości przesłanych danych w zadanym okresie czasu,
    g) wykrycie chwilowego wzrostu ilości przesłanych danych (tzw. peek) w stosunku do całkowitej ilości przesłanych danych w zadanym okresie czasu,
    h) wykrycie sumarycznego wzrostu przesłanych danych w zdefiniowanej strefie bezpieczeństwa,
    i) wykrycie zdefiniowanej ilości przesyłanych pakietów w zadanym okresie czasu,
    j) wykrycie chwilowego wzrostu (tzw. peek) w stosunku do ilości przesyłanych pakietów w zadanym okresie czasu,

k) wykrycie sumarycznego wzrostu ilości pakietów przesyłanych w zdefiniowanej strefie bezpieczeństwa,
l) wykrycie ilości uruchomionych procesów w zadanym okresie czasu,
m) wykrycie skanowania portów.

53. Reguły korelacyjne bazujące na listach referencyjnych muszą umożliwić:

a) wykrycie wystąpienia wartości pola na wybranej liście,
b) wykrycie niewystępowania wartości pola na wybranej liście,
c) wykrycie wystąpienia pary wartości na wybranej liście (np.: proces i obraz pliku, z którego został uruchomiony),
d) wykrycie niewystąpienia pary wartości na wybranej liście
e) (np.: nazwa użytkownika wraz aplikacją, z którą się wcześniej nie łączył).

54. Reguły korelacyjne wykorzystujące atrybuty użytkowników z Active Directory muszą umożliwić:

a) wykrycie czy zdarzenie pochodzi od użytkownika posiadającego konto w Active Directory,
b) wykrycie czy zdarzenie pochodzi od użytkownika posiadającego uprzywilejowane konto w Active Directory,
c) wykrycie czy zdarzenie pochodzi od użytkownika podszywającego się pod konto użytkownika Active Directory (np.: którego e-mail zdefiniowany w Active Directory różni się od e-maila ze zdarzenia mimo, zgodności pozostałych atrybutów konta).
d) wykrycie czy zdarzenie pochodzi od użytkownika należącego do wybranej grupy w Active Directory (np.: Domain Admins),
e) wykrycie czy zdarzenie pochodzi od użytkownika nie należącego do wybranej jednostki organizacyjnej.

55. Reguły korelacyjne wykorzystujące atrybuty komputerów z Active Directory muszą umożliwić:

a) wykrycia czy zdarzenie pochodzi z komputera należącego do domeny Active Directory,
b) wykrycia czy zdarzenie pochodzi z komputera z systemem operacyjnym zdefiniowanym w Active Directory,
c) wykrycia czy zdarzenie pochodzi z komputera z wybranej jednostki organizacyjnej.

56. Reguły korelacyjne wykorzystujące bazę wskaźników kompromitacji (IOC) muszą umożliwić:

a) wykrycie czy źródłowy adres IP nie jest oznaczony w systemie jako wskaźnik kompromitacji;
b) wykrycie czy HASH występujący w zdarzeniu nie jest oznaczony w systemie jako wskaźnik kompromitacji;
c) wykrycie czy docelowa nazwa hosta (FQDN) nie jest oznaczona w systemie jako wskaźnik kompromitacji;

57. Reguły korelacyjne wykorzystujące informacje z elektronicznej dokumentacji muszą umożliwić:

a) wykrycie połączenia z serwera do stacji roboczej w przypadku braku informacji o rodzajach zasobu w korelowanym zdarzeniu,
b) wykrycie połączenia do usługi przez nieautoryzowanego użytkownika,
c) wykrycie nieautoryzowanej usługi na serwerze,
d) wykrycie nieautoryzowanego połączenia do usługi na serwerze,
e) wykrycie nieautoryzowanego połączenia z serwera usług,
f) wykrycie nieautoryzowanego połączenia do sieci Internet.

58. Reguły korelacyjne wykorzystujące anomalie w zachowaniu użytkowników (UBA) muszą umożliwić:

a) wykrycie anomalii ilościowej związanej z kontem użytkownika wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania,
b) wykrycie anomalii związanej ze zmianą zachowania na koncie użytkownika, wskazującej na potencjalny atak APT/Ransomware,
c) wykrycie różnych typów anomalii na koncie użytkownika wskazujących na możliwe przejecie konta użytkownika przez cyberprzestępcę lub złośliwe oprogramowanie,
d) wykrycie anomalii związanych z logowaniami użytkowników w ramach sesji VPN.

59. Reguły korelacyjne wykorzystujące anomalie w zachowaniu zasobów (EBA) muszą umożliwić:

a) wykrycie anomalii ilościowej związanej z komputerem wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania,
b) wykrycie anomalii związanej ze zmianą zachowania komputera, wskazującej na potencjalny atak APT/Ransomware,
c) wykrycie różnych typów anomalii na komputerze, wskazujących na możliwe przejecie komputera przez cyberprzestępcę lub złośliwe oprogramowanie,
d) wykrycie anomalii związanych z procesami uruchamianymi na serwerach.

60. Reguły korelacyjne wykorzystujące podatności na zasobach muszą umożliwić:

a) wykrycie skanowania portów z zasobu posiadającego krytyczne podatności,
b) wykrycie wielokrotnych prób połączeń do zasobu posiadającego krytyczne podatności,
c) wykrycie zdarzeń o wysokim „severity" na zasobach posiadającego krytyczne podatności,
d) wykrycie zdarzeń o wysokim „severity" do zasobów posiadających krytyczne podatności.

61. Reguły korelacyjne wykorzystujące wyniki analizy konfiguracji muszą pozwalać na:

a) wykrycie wielokrotnych prób nieudanego logowania do komputera, umożliwiającego ustawienie hasła zawierającego mniej niż 14 znaków,
b) wykrycie wielokrotnych prób nieudanego logowania do komputera, który umożliwia tworzenie haseł niespełniających następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny.

62. Reguły korelacyjne wykorzystujące technikach MITRE ATT&CK® muszą umożliwić:

a) wykrycie zdefiniowanej ilości technik w zdarzeniach dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP,
b) wykrycie zdefiniowanej ilości zdarzeń w ramach jednej techniki dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP,
c) wykrycie incydentu będącego pochodną zdarzeń z technik występujących w określonej kolejności na wybranym adresie IP lub zasobie identyfikowanym po nazwie.

63. Pojedyncza reguła korelacyjna musi mieć możliwość wzajemnej korelacji wszystkich powyższych mechanizmów umożliwiając, m.in.:

a) wykrycie anomalii na koncie uprzywilejowanym użytkownika,

b) wykrycie ruchu z serwera domenowego do skompromitowanej domeny wykazanej w liście referencyjnej,
c) wykrycie wielu typów anomalii na komputerze z krytyczną podatnością,
d) wykrycie złośliwego oprogramowania na bazie wskaźnika kompromitacji stanowiącego HASH procesu, z którego następuje nieautoryzowana próba dostępu do usługi,
e) wykrycie wielokrotnych prób nieudanego logowania na konto uprzywilejowane, którego hasło nie spełnia następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny.

64. System przy wykorzystaniu reguł kwalifikacyjnych musi automatycznie selekcjonować zdarzenia wygenerowane przez reguły korelacyjne, wybierając do obsługi tylko zdarzenia spełniające zdefiniowane warunki (tzw. zdarzenia w obsłudze). Pozostałe zdarzenia powinny być wykluczone z obsługi, ale równocześnie pozostać w systemie, zachowując możliwość ich obsługi na żądanie operatora. Zastosowane reguły selekcji zdarzeń do obsługi muszą równocześnie umożliwiać wyliczenie właściwego dla nich priorytetu. Reguły selekcji i priorytetyzacji zdarzeń w obsłudze muszą uwzględniać:

a) sparsowane pola oraz ich wartości,
b) atrybuty użytkowników z Active Directory,
c) atrybuty komputerów z Active Directory,
d) informacje z elektronicznej dokumentacji.

65. Zdarzenia w obsłudze, muszą obsługiwać opcje grupowania polegającą na tym, iż każde kolejne zdarzenie wynikające z reguł korelacyjnych, spełniających tą samą regułę w zdefiniowanym okresie czasu będzie automatycznie dodawane do tego samego zdarzenia w obsłudze. Grupowanie musi odbywać się po:

a) adresie IP,
b) koncie domenowym użytkownika,
c) strefie bezpieczeństwa,
d) zakresie adresów IP.

66. Obsługiwane zdarzenia muszą posiadać zestaw predefiniowanych scenariuszy obsługi (ang. Playbook) oraz pozwalać na tworzenie własnych scenariuszy obsługi oraz ich edycję z poziomu interfejsu graficznego. System musi wspierać funkcję „Drag and Drop" umożliwiającą m.in. na zamianę kolejności realizacji poszczególnych kroków poprzez ich przenoszenie za pomocą myszki komputerowej.

67. System musi potrafić wczytywać informacje z innych systemów bezpieczeństwa i traktować je, jako elementy/dowody dla zdarzeń w obsłudze.

68. Zdarzenia w obsłudze muszą umożliwiać gromadzenie dodatkowych informacji wygenerowanych podczas ich obsługi oraz umożliwiać do nich dostęp bezpośrednio z poziomu tych zdarzeń, obejmujących m.in.

a) wszystkie skorelowane zdarzenia,
b) korespondencja pocztowa,
c) załączniki z próbkami lub dowodami,
d) wskaźniki kompromitacji (IoC),
e) informacje pozyskane z innych systemów.

69. System powinien posiadać możliwość rejestracji zgłoszeń przez stronę webową udostępnianą przez system dla użytkowników z innych jednostek organizacyjnych oraz umożliwić ich przekształcenie w zdarzenia w obsłudze z możliwością rozdzielenia uprawnień dla obu tych czynności. System musi umożliwiać scenariusz, gdzie użytkownik zgłasza incydent, który zanim zostanie zakwalifikowany do dalszej obsługi musi zostać autoryzowany przez uprawnionego do tego celu operatora.

70. Dla obsługiwanych zdarzeń system powinien umożliwiać automatyczne pozyskanie informacji z innych systemów oraz bazując na uzyskanej od nich odpowiedzi automatycznie zmieniać ich status, np.: na podstawie pozyskanego wskaźnika kompromitacji (IoC) zmienić status zdarzenia na incydent bezpieczeństwa.

71. Dla zdarzeń w obsłudze dotyczących ruchu sieciowego pomiędzy źródłem a celem transmisji, system musi automatycznie wyznaczyć wektor zagrożenia i zaprezentować go w formie graficznej, na której będą zwizualizowane następujące dane:

a) identyfikację celu i źródła zagrożenia,
b) nazwę oraz adres IP źródła zagrożenia,
c) rodzaj zasobu będący źródłem zagrożenia np.: urządzenie mobilne, stacja robocza,
d) lokalizację z które pochodzi zagrożenie np.: Internet,
e) strefę bezpieczeństwa z której pochodzi zagrożenie,
f) prawdopodobieństwo zagrożenia ze strefy stanowiącej jego źródło,
g) wszystkie urządzenia sieciowe chroniące cel zagrożenia i zastosowane na nich mechanizmy zabezpieczeń (np.: Application Control, Network Firewall, User Identification),
h) nazwę oraz adres IP celu zagrożenia,
i) zabezpieczenia lokalne chroniące cel zagrożenia,
j) strefę bezpieczeństwa w której znajduje się cel zagrożenia.

72. Dla każdego wektora zagrożenia system musi automatycznie wyliczać efektywność zastosowanych mechanizmów zabezpieczeń, pozwalającą w ramach wbudowanych w system edytowalnych reguł ocenić prawdopodobieństwo materializacji się cyberzagrożeń. Na przykład: dla serwera webowego dostępnego ze strefy Internet zagrożenie przełamania zabezpieczeń ma niskie prawdopodobieństwo w przypadku, gdy jest on zabezpieczony przez rozwiązanie klasy WAF (Web Application Firewall).

73. Dla wyznaczonych w czasie obsługi wektorów zagrożeń przedstawiane wyniki szacowania prawdopodobieństwa muszą być zwizualizowane operatorowi w formie listy zagrożeń z oszacowanymi dla nich poziomami. Przykładowe wartości z listy to: wysoki poziom prawdopodobieństwa włamania na serwer oraz średni poziom prawdopodobieństwa infekcji złośliwym oprogramowaniem.

74. Dla zdarzeń w obsłudze zarówno w odniesieniu do adresów źródłowych jak i docelowych system musi umożliwiać operatorowi uzupełnianie pozyskanych informacji, dotyczących zarówno źródła jak i celu zagrożenia w następującym zakresie:

a) nazwy zasobu,
b) rodzaju zasobu,
c) ważności zasobu dla organizacji,
d) rodzaj przetwarzanych informacji,
e) usług, które ten zasób świadczy,

f) lokalizację użytkowników, którzy z niego korzystają,
g) usługi, z których zasób korzysta.

75. System powinien mieć logikę automatycznego przypisywania zdarzeń zakwalifikowanych do obsługi wraz z powiadomieniem operatora, któremu zostało ono przydzielone (min. e-mail, SMS). Kwalifikacja musi uwzględniać m.in. dostępność operatora, jego obciążenia oraz parametry zasobu, którego dotyczy zdarzenie, typ zasobu (np.: serwer lub stacja robocza), jego krytyczność oraz realizowane z jego udziałem usługi z katalogu usług. Na przykład: zdarzenie przypisane do krytycznego serwera realizującego usługę DNS powinny trafić do innego operatora niż zdarzenia dotyczące pozostałych serwerów usług sieciowych.

76. Zdarzenia w obsłudze muszą obejmować statusy właściwe dla procesu obsługi zdarzeń, minimum to:

a) nowe zdarzenie – jako zdarzenie zarejestrowane w systemie,
b) segregacja – segregacja i kwalifikacja zdarzeń,
c) incydent bezpieczeństwa – zdarzenie zakwalifikowane jako incydent bezpieczeństwa,
d) fałszywy alarm – zdarzenie zakwalifikowane jako fałszywy alarm,
e) zdarzanie obsłużone – zdarzenie, które zostało obsłużone w systemie.

System musi także zapewniać możliwość ich edycji w zakresie dodawania (np.: wydzielenie z segregacji statusu kwalifikacji) lub usuwania statusów oraz konfiguracji przejść pomiędzy nimi. Przykładowo: umożliwiać przejście ze statusu „incydent bezpieczeństwa" do statusu „zdarzenie zamknięte", ale zablokować zmianę ze statusu „incydent bezpieczeństwa" na status „fałszywy alarm".

77. System powinien umożliwiać definiowanie parametrów SLA dla wszystkich statusów obsługi zdarzeń oraz dokonywać automatycznego pomiaru tych czasów i ich weryfikacji względem zdefiniowanych wartości. Wyniki pomiarów czasów SLA powinny być stale aktualizowane i prezentowane na liście zdarzeń zakwalifikowanych do obsługi.

78. System musi umożliwiać grupowanie manualne dla zdarzeń w obsłudze, których powiązanie zostanie wykryte przez operatorów w trakcie obsługi i umożliwiać zgrupowanie ich do jednego zdarzenia. Zgrupowane zdarzenia muszą być podrzędne w stosunku do zdarzenia, z którym są grupowane oraz synchronizować z nim statusy. Dla zdarzeń przetwarzanych przez operatora, zmiana statusu głównego zdarzenia musi wymusić zmianę statusu pozostałych. Na przykład: zamknięcie nadrzędnego zdarzenia musi zamykać też wszystkie podrzędne. Na liście zdarzeń oraz w podglądzie każdego zdarzenia powinna się pojawić informacja o zdarzeniach z nim powiązanych.

79. Obsługiwane zdarzenia muszą zapewniać historyczność, obejmującą wszystkie aktywności realizowane w ramach poszczególnych statusów. Aktywności muszą uwzględniać zarówno akcje realizowane w ramach samego systemu (m.in. zmiana priorytetu czy przekazanie zdarzenia innemu operatorowi). Dodatkowo historia musi też zawierać wszelkie komentarze wpisywane przez operatorów.

80. Dla każdego obsługiwanego zdarzenia system powinien udostępniać automatyczny raport obejmujący wszystkie podjęte działania wraz z komentarzami operatorów.

81. W ramach obsługi zdarzeń system musi automatycznie porównywać wskaźniki kompromitacji zidentyfikowane w bieżącym zdarzeniu względem wszystkich wskaźników pozyskanych do tej pory w ramach dotychczasowej obsługi. Na przykład: jeżeli w obsługiwanym zdarzeniu znajduje się FQDN oraz HASH to system musi automatycznie porównać je ze wszystkimi wskaźnikami typu FQDN oraz

HASH, zebranymi do tej pory w obsługiwanych zdarzeniach bez względu na to czy wskaźniki te zostały wpisane ręcznie czy zostały pozyskane automatycznie z innych systemów.

82. System powinien pozwalać, przy użyciu języków skryptowych ogólnie dostępnych (np. Python lub PowerShell), na skonfigurowanie nowych integracji z zewnętrznymi systemami oraz zapewnić dla tych systemów mechanizmy bezpiecznego zarządzania i przechowywania danych związanych z tymi integracjami, m.in. loginy, hasła oraz klucze API.

83. W ramach obsługi zdarzenia dla operatora powinien być dostępny dedykowany panel analityczny pozwalający mu na:

a) podgląd aktywności zagrożonego zasobu na linii czasu,
b) w przypadku zagrożenia sieciowego podgląd aktywności zarówno ofiary jak i celu ataku,
c) w przypadku identyfikacji użytkownika podgląd jego aktywności na linii czasu,
d) podgląd reguły korelacyjnej, która wygenerowała zdarzenie,
e) w przypadku wykrytej techniki MITRE ATT&CK® jej szczegółowy opis,
f) listowanie podpiętych zdarzeń wraz z mechanizmami filtrowania po nich,
g) gotowe i proste w użyciu filtry rozszerzajcie analizę zdarzeń o:

- listę wszystkich zdarzeń pomiędzy celem a źródłem ataku w zadanym okresie czasowym, np.: godzinę przed oraz 2 godziny po,
- listę wszystkich zdarzeń dotyczących źródła lub celu ataku w zadanym okresie czasowym,
- gotowe i proste w użyciu filtry rozszerzajcie analizę logów o:
- listę wszystkich logów pomiędzy celem a źródłem ataku w zadanym okresie czasowym,
- listę wszystkich logów dotyczących źródła lub celu ataku w zadanym okresie czasowym.

84. Dla zdarzeń w obsłudze system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących:

a) warunki powiadomień:

- zdarzeń o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi,
- zdarzeń o przekroczonych czasach SLA o definiowalny okres,
- zdarzeń ze zbliżającym się i definiowalnym terminem przekroczenia SLA,
- zdarzeń, których priorytet osiągnął określoną wartość,
- zdarzeń zakwalifikowanych jako incydent bezpieczeństwa,
- zdarzeń, na których doszło do naruszenia bezpieczeństwa,
- zdarzeń powstałych poprzez zdefiniowaną regułę korelacyjną,
- zdarzeń realizujących zdefiniowaną usługę,
- zdarzeń przetwarzających sklasyfikowane informację,
- zdarzeń przetwarzanych na krytycznych zasobach,

b) odbiorców powiadomień, w tym:

- operatora, któremu zostało przydzielone zdarzenie,
- właściciela zasobu, na którym wystąpiło zdarzenie,
- zespół obsługi, który odpowiada za obsługę zdarzeń,
- właściciela usługi, która jest realizowana na zasobie na którym wystąpiło zdarzenie,
- podmiot zewnętrzny, jeżeli zdarzenie dotyczy zasobu obsługiwanego przez firmę zewnętrzną.

c) kanały powiadomień, m.in. e-mail, sms, komunikator,
d) zastosowanie mechanizmów grupowania:

- grupowanie wielu powiadomień w jednej wiadomości,
- ograniczenie liczby wierszy powiadomienia do określonej wartości.

85. System powinien posiadać gotowe szablony powiadomień pozwalające na wysyłanie powiadomień jego operatorom w przypadku, gdy system przydzieli im zdarzenia do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach:

a) utworzenia nowego zdarzenia z określonym priorytetem,
b) utworzenia nowego zdarzenia na zasobie krytycznym,
c) utworzenia nowego zdarzenia na zasobie realizującym zdefiniowaną usługę,
d) utworzenie nowego zdarzenia na zasobie przetwarzającym dane osobowe,
e) utworzenie nowego zdarzenia na podstawie zdefiniowanej reguły korelacyjnej,
f) modyfikacji przydzielonego operatorowi zdarzania przez innego operatora,
g) zamknięcia przydzielonego operatorowi zdarzania przez innego operatora,
h) przejęcia przydzielonego operatorowi zdarzania przez innego operatora.

86. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora umożliwiającego:

a) wybór raportu, który ma zostać wysłany,
b) zdefiniowanie jego tytułu,
c) zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny,
d) możliwość ograniczenia cyklu do dni powszednich,
e) określenie daty przesłania pierwszego raportu,
f) możliwości ograniczenia okresu przez jaki raport będzie przesyłany, do:
g) zdefiniowanej daty końcowej,
h) określnej liczby raportów,
i) określenie odbiorców raportu.

87. System musi umożliwiać obsługę podatności w ramach scenariuszy obsługi (Playbook).

88. Importowane do systemu podatności muszą być przeanalizowane pod względem ryzyka jakie mogą wygenerować dla organizacji. W tym celu musi być dostępny mechanizm ich automatycznej priorytetyzacji bazujący na regułach, które wyznaczą dla podatności wymagających obsługi priorytet w oparciu o następujące parametry:

a) strefę bezpieczeństwa w której została wykryta podatność,
b) prawdopodobieństwo obecności intruza lub złośliwego oprogramowania w tej strefie,
c) rodzaj zasobu, którego dotyczy ta podatność,
d) ważność tego zasobu dla organizacji,
e) przetwarzane na tym zasobie informacje, np.: dane osobowe,
f) usługi realizowane przez ten zasób, np.: DNS,
g) wartość parametrów CVSS dla podatności, np.: „Confidentiality Impact" = High,
h) poprawność konfiguracji zasobu, na którym została wykryta podatność, np.: brak reguł wymuszenia złożoności haseł,
i) szacowane prawdopodobieństwo przełamania zabezpieczeń ze zdefiniowanej strefy, która jest autoryzowana do dostępu do tego zasobu, np.: wysokie prawdopodobieństwa zagrożenia ze strefy Internet dla zasobu z wykrytą podatnością, który świadczy usługę w strefie Internet.

89. W systemie musi być dostępny predefiniowany zestaw reguł automatycznej priorytetyzacji wszystkich importowanych podatności oraz interfejs umożliwiający definiowanie własnych reguł umożliwiających zarówno zakwalifikowanie podatności do obsługi jaki i możliwość ich wyłączenia z obsługi w przypadku znikomego zagrożenia dla organizacji.

90. Obsługiwane w systemie podatności muszą być dostępne w formie listy umożliwiającej ich filtrowanie po następujących wartościach:

a) wyliczonym priorytecie podatności,
b) aktualnym statusie obsługi,
c) ważności zasobu, na którym została wykryta,
d) adresie IP tego systemu,
e) parametrów SLA związanych z tym statusem,
f) przetwarzanych na zasobach informacji, np.: lista podatności dotycząca tylko systemów przetwarzających dane osobowe,
g) parametrach CVSS, np.: lista podatności których „Access Complexity (AC)" = „low" oraz „Access Vector (AV) = „Network".

91. System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień dla kadry zarządzającej, obejmujących eskalacje oraz monitorowanie SLA. Szablony powinny uwzględniać powiadomienia kierowników jednostek organizacyjnych w następujących sytuacjach:

a) przekroczenia czasu reakcji o określony czas np.: o godzinę,
b) możliwości przekroczenia czasu reakcji, np.: została godzina, aby rozpocząć obsługę zdarzenia i uchronić się przed przekroczeniem czasu reakcji,
c) przekroczenia czasu reakcji dla zdarzenia na zasobie przetwarzającym dane osobowe,
d) przekroczenia czasu reakcji dla zdarzenia na zasobie krytycznym,
e) przekroczenia czasu reakcji dla zdarzenia na zasobie realizującym krytyczną usługę,
f) przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów przetwarzających dane osobowe,
g) przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów krytycznych,
h) przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów realizujących krytyczną usługę,
i) przekroczenia czasu reakcji dla podatności na zasobie przetwarzającym dane osobowe,
j) przekroczenia czasu reakcji dla podatności na zasobie krytycznym,
k) przekroczenia czasu reakcji dla podatności na zasobie realizującym krytyczną usługę.

92. Dla obsługiwanych podatności system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących:

a) warunki powiadomień,
b) podatności o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi,
c) podatności o przekroczonych czasach SLA o definiowalny okres,
d) podatności ze zbliżającym się i definiowalnym terminem przekroczenia SLA,
e) podatności, których priorytet osiągnął określoną wartość,
f) zdarzeń realizujących zdefiniowaną usługę,
g) zdarzeń przetwarzających sklasyfikowane informację,

h) zdarzeń przetwarzanych na krytycznych zasobach,
i) odbiorców powiadomień, w tym:
j) operatora, któremu została przydzielona podatność,
k) właściciela zasobu, na którym wystąpiła podatność,
l) zespół obsługi, który odpowiada za obsługę podatności,
m) właściciela usługi, na która jest realizowana na zasobie, na którym wystąpiła podatność,
n) podmiot zewnętrzny, jeżeli zdarzenie dotyczy podatności na zasobie obsługiwanym przez firmę zewnętrzną.
o) kanały powiadomień, m.in. e-mail, sms, komunikator,
p) zastosowanie mechanizmów grupowania:
q) grupowanie wielu powiadomień w jednej wiadomości,
r) ograniczenie liczby wierszy powiadomienia do określonej wartości.

93. System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień jego operatorom w przypadku, gdy system przydzieli im podatności do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach:

a) przydzielenia nowej podatności do obsługi z określonym priorytetem,
b) przydzielenia nowej podatności do obsługi na zasobie krytycznym,
c) przydzielenia nowej podatności do obsługi na zasobie realizującym zdefiniowaną usługę,
d) przydzielenia nowej podatności do obsługi na zasobie przetwarzającym dane osobowe,
e) modyfikacji przydzielonej operatorowi podatności przez innego operatora,
f) zamknięcia przydzielonej operatorowi podatności przez innego operatora,
g) przejęcia przydzielonej operatorowi podatności przez innego operatora.

94. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora pozwalającego na:

a) wybór raportu, który ma zostać wysłany,
b) zdefiniowanie jego tytułu,
c) zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny,
d) możliwość ograniczenia cyklu do dni powszednich,
e) określenie daty przesłania pierwszego raportu,
f) określenie okresu przez jaki będą one przesyłane, poprzez:
g) zdefiniowanie daty końcowej,
h) bez daty końcowej,
i) określenie liczby raportów,
j) określenie odbiorców raportu.

95. System powinien w formie graficznej prezentować podsumowanie aktualnego stanu bezpieczeństwa organizacji w postaci tzw. „Dashboard'u", tj. dostosowywać zakres i prezentacje danych do potrzeb zalogowanego użytkownika.

96. System musi pozwalać na tworzenie dedykowanych dashboard'ów obejmujących:

a) zestaw wykresów dla bieżącego użytkownika,
b) zestaw wykresów dla wybranego użytkownika,
c) zestaw wykresów dla roli zdefiniowanej w systemie, np.: administratorzy systemu,
d) zestaw wykresów dla wybranego zespołu obsługi, np.: operatorzy SOC (Security Operations Center).

97. System musi zapewniać zestaw predefiniowanych dashboard'ów obejmujących następujące wykresy:

a) wykres przedstawiający status klasyfikacji zdarzeń, który uwzględnia:
- ilość zdarzeń nowych i niesklasyfikowanych,
- ilość zdarzeń sklasyfikowanych jako incydenty bezpieczeństwa,
- ilość zdarzeń sklasyfikowanych jako fałszywe alarmy,
- wykres przedstawiający skale zagrożeń, który uwzględnia:
- ilość zasobów krytycznych na których są obsługiwane zdarzenia,
- ilość zasobów niekrytycznych na których są obsługiwane zdarzenia,

b) wykres przedstawiający źródła zagrożeń, który uwzględnia:
- ilość nowych zdarzeń dotyczących użytkowników,
- ilość podjętych zdarzeń dotyczących użytkowników,
- ilość nowych zdarzeń dotyczących zasobów,
- ilość podjętych zdarzeń dotyczących zasobów,

c) wykres przedstawiający poziom zagrożeń, który uwzględnia:
- ilość nowych zdarzeń w podziale na priorytety,
- ilość podjętych zdarzeń w podziale na priorytety,

d) wykres przedstawiający czas obsługi zagrożeń, który uwzględnia:
- ilość zdarzeń zarejestrowanych w bieżącym dniu,
- ilość zdarzeń zarejestrowanych w ostatnim tygodniu,
- ilość zdarzeń zarejestrowanych w ostatnim miesiącu,
- ilość zdarzeń zarejestrowanych wcześniej niż w ostatnim miesiącu,

e) wykres przedstawiający zagrożone usługi, który uwzględnia:
- ilość usług krytycznych zagrożonych przez obsługiwane zdarzenia,
- ilość pozostałych usług zagrożonych przez obsługiwane zdarzenia,

f) wykres przedstawiający zagrożone dane, który uwzględnia:
- ilość nowych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje,
- ilość podjętych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje,
- ilość nowych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje,
- ilość podjętych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje,

g) wykres przedstawiający skale podatności, który uwzględnia:
- ilość zasobów krytycznych na których są obsługiwane podatności,
- ilość zasobów niekrytycznych na których są obsługiwane podatności,

h) wykres przedstawiający czas obsługi podatności, który uwzględnia:
- ilość podatności zarejestrowanych w bieżącym dniu,
- ilość podatności zarejestrowanych w ostatnim tygodniu,
- ilość podatności zarejestrowanych w ostatnim miesiącu,
- ilość podatności zarejestrowanych wcześniej niż w ostatnim miesiącu,

i) wykres przedstawiający wagę podatności, który uwzględnia:
- ilość nowych podatności w podziale na priorytety,
- ilość podjętych podatności w podziale na priorytety.

98. Nawigacja w ramach „Dashboard'u" musi wspierać opcję typu „Drill down" w następującym zakresie:

a) „kliknięcie" wartości prezentowanej na wykresie, dotyczącej zdarzeń w obsłudze musi przenieść operatora systemu do listy tych zdarzeń z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
b) „kliknięcie" wartości prezentowanej na wykresie, dotyczącej podatności musi przenieść operatora systemu do listy tych podatności z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
c) „kliknięcie" wartości prezentowanej na wykresie, dotyczącej użytkowników (UBA) musi przenieść operatora systemu do listy tych użytkowników z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
d) „kliknięcie" wartości prezentowanej na wykresie, dotyczącej zasobów (EBA) musi przenieść operatora systemu do listy tych zasobów z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
e) „kliknięcie" wartości prezentowanej na wykresie, dotyczącej wybranych zdarzeń korelacyjnych musi przenieść operatora systemu do listy prezentującej te zdarzenia z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
f) „kliknięcie" wartości prezentowanej na wykresie, dotyczącej wybranych logów musi przenieść operatora systemu do listy prezentującej te logi z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres.

99. Rozwiązanie może być dostarczone w ramach odrębnych rozwiązań, jednakże muszą być one zintegrowane w sposób umożliwiający spełnienie wszystkich wymagań z poziomu jednej konsoli.

100. Rozwiązanie musi zapewniać elastyczną i skalowalną architekturę, której rozbudowa nie będzie wymagała zakupu dodatkowych licencji, zapewniając tym samym możliwość wydzielania następujących warstw funkcjonalnych zwanych dalej kolektorami, do instalacji na osobnych serwerach bądź maszynach wirtualnych:

a) kolektor parsujący;
b) kolektor logów;
c) kolektor korelacyjny;
d) kolektor zdarzeń;
e) kolektor sztucznej inteligencji;
f) kolektor reakcyjny;
g) kolektor kontrolujący.

101. Kolektor parsujący powinien być odpowiedzialny za odbieranie i parsowanie logów a następnie ich przesyłanie zarówno postaci surowej jak i sparsowanej do odpowiednich kolektorów logów, zgodnie z regułami ich przekierowania zdefiniowanymi w jednym miejscu dla wszystkich kolektorów w interfejsie graficznym. Pojedynczy kolektor parsujący musi zapewniać wydajność co najmniej 20 tysięcy zdarzeń na sekundę w trybie ciągłym oraz posiadać bufor do obsługi natłoku w rozmiarze miliona zdarzeń.

102. Kolektor logów powinien być odpowiedzialny za przechowywanie logów zarówno w postaci surowej jak i sparsowanej oraz przechowywać pliki indeksów. Logi muszą być przechowywane w

postaci skompresowanej oraz kolektor musi zapewnić mechanizmy zabezpieczające je przed nieautoryzowaną modyfikacją (np.: Certyfikat cyfrowy czy funkcja skrótu). Pojedynczy kolektor logów powinien mieć wydajność co najmniej 10 tyś zdarzeń na sekundę w trybie ciągłym oraz posiadać bufor do obsługi natłoku w rozmiarze miliona zdarzeń.

103. Kolektor korelujący powinien umożliwiać korelację logów oraz ich agregację zgodnie z regułami korelacyjnymi zdefiniowanymi w jednym miejscu dla wszystkich kolektorów w interfejsie graficznym.

104. Kolektor zdarzeń powinien umożliwiać składowanie zdarzeń stanowiących wyniki korelacji oraz umożliwiać ponowne wykorzystanie tych zdarzeń w kolejnych regułach umożliwiając tym korelację zależności pomiędzy nimi. Zdarzenia muszą być przechowywane w postaci skompresowanej oraz kolektor musi zapewnić mechanizmy zabezpieczające je przed nieautoryzowaną modyfikacją (np.: Certyfikat cyfrowy czy funkcja skrótu).

105. Kolektor sztucznej inteligencji powinien zawierać wiedzę pozyskaną ze środowiska obejmującą zarówno linię trendu zachowania użytkowników oraz zasobów obejmujące mechanizmy uczenia maszynowego jak i algorytmy sztucznej inteligencji pozwalające na wypracowanie nowej wiedzy wynikającej z korelacji wyników wiedzy wypracowanej poprzez inne metody.

106. Kolektor reakcyjny musi umożliwiać automatyczną reakcję na wykryte zagrożenia, która nie będzie wymagała żadnej interakcji ze strony użytkownika, chyba że taka będzie dodatkowo zdefiniowana. W celu automatyzacji reakcji musi posiadać funkcjonalność systemu PAM lub być z nim dostarczony w celu przechowywania danych uwierzytelniających oraz kluczy API potrzebnych do automatyzacji reakcji.

107. Architektura rozwiązania musi w pełni wspierać konfigurację niezawodnościową, zapewniającą zarówno pełną redundancję w zakresie, odbierania logów i ich przechowywania, korelacji oraz reakcji na zagrożenia jak i możliwość zastosowania konfiguracji o ograniczonej redundancji do najważniejszych dla zamawiającego źródeł danych.

108. Konfiguracja niezawodnościowa musi wspierać możliwość zastosowania stosu kolektorów zastępczych które zostaną uruchomione w przypadku awarii stosu podstawowego, przy czym wszystkie one muszę być zarządzane centralnie z poziomu tej samej konsoli co kolektory podstawowe.

109. Kolektory muszą mieć zapewnione mechanizmy automatycznej aktualizacji zarówno w zakresie parserów czy reguł korelacyjnych jak i wersji oprogramowania, przy czym aktualizacja musi odbywać się z poziomu centralnego systemu zarządzania.

110. Rozwiązanie musi zapewnić konsole do aktualizacji pozwalającą na wybór dodatkowych pakietów reguł czy parserów udostępnianych w ramach aktywnego wsparcia producenta w formie usługi, każda aktualizacja musi wspierać mechanizm wersjonowania pozwalający zarówno aktualizację jaki i przywracanie poprzednich wersji reguł i parserów.

111. Rozwiązanie musi mieć możliwość skalowania się poprzez dodawanie kolejnych maszyn wirtualnych lub maszyn fizycznych z nowymi typami kolektorów, przy czym dodawanie nowych komponentów nie może wiązać się z koniecznością zakupu nowej licencji, ani posiadać ograniczeń licencyjnych związanych z ilością lub rozmiarem przechowywanych zdarzeń i/lub danych. Jedynym ograniczeniem w tym zakresie (dotyczącym przechowywanych danych) może być rozmiar przestrzeni dyskowej.

112. Skalowanie przez dodawanie nowych kolektorów musi zwiększać wydajność rozwiązania zgodnie z wartościami zadeklarowanymi przez producenta, przykładowo dwa kolektory logów muszą zapewnić dwukrotną wydajność rozwiązania, czyli minimum 20 tyś zdarzeń na sekundę. Przy czym całe rozwiązanie nie może ograniczać ilość zastosowanych kolektorów.

113. Rozwiązanie nie może posiadać ograniczeń licencyjnych związanych z rozmiarem gromadzonych danych w jednostce czasu. Przykładowo nie może być limitowana licencyjnie ilość bajtów danych w jednostce czasu (KB, GB, etc.)

114. Poszczególne kolektory zdarzeń oraz logów muszą zapewniać przechowywanie danych zarówno na maszynach wirtualnych jak i na dyskach sieciowych.

115. Kolektor logów musi mieć możliwość składowania zbieranych danych zarówno w formie surowej (raw event log) jak i w formie sparsowanych danych (parsed event log) znormalizowanych.

116. Rozwiązanie nie może Przechowywanie logów oraz zdarzeń nie może wykorzystywać klasycznej relacyjnej bazy danych (w tym, choć nie tylko: MS SQL, PostgreSQL, MySQL, Oracle, itp.) celem gromadzenia i przechowywania danych związanych ze zbieranymi zdarzeniami. Rozwiązanie musi wykorzystywać w tym celu nowoczesną bazę taką jak na przykład noSQL lub OLAP lub autorskie rozwiązanie producenta.

117. Rozwiązanie musi zapewniać możliwość zbudowania większej ilości replik danych, aby zapewnić niezawodność przechowywania oraz możliwość zbudowania struktury rozproszonej, zapewniającej większą wydajność zapisu i wyszukiwania.

118. Klasyczne relacyjne bazy danych mogą być wykorzystywane jedynie do przechowywania szablonów, raportów, konfiguracji, bazy CMDB oraz innych ustrukturyzowanych informacji.

119. Rozwiązanie musi zapewniać możliwość automatycznego budowania kontekstu poprzez wykrywanie urządzeń oraz komputerów mających swoją reprezentację w bazie urządzeń (Configuration Management Database - CMDB).

120. Wymagane jest, aby kolektor odpowiedzialny za parsowanie pozwalał na odrzucanie danych, które uznane są za nieistotne lub niepotrzebne. Mechanizm ten nie może mieć żadnego wpływu na model licencjonowania.

121. Musi istnieć możliwość samodzielnej modyfikacji i poprawiania wszystkich parserów

122. Tworzenie własnych parserów musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI)

123. Tworzenie nowych atrybutów (sparsowanych zmiennych), urządzeń oraz rodzajów zdarzeń (events) musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI).

124. Parsery mają być tworzone z wykorzystaniem narzędzi wspierających dla XML (XML framework) i jednocześnie zapewniać następujące właściwości:

a) zdolność do definiowania wzorców które powtarzają się jako zmienne;
b) zdolność do definiowania funkcji pozwalających na identyfikację par wartości kluczowych;
c) zdolność do testowania poszczególnych funkcji;
d) zdolność do przekształcania danych w trakcie ich parsowania.

125. Rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Windows (Windows Agent), które posiadają nie mniej niż następujące możliwości:

a) centralne zarządzanie i możliwość aktualizacji z głównej konsoli zarządzającej;
b) możliwość zbierania logów z plików tekstowych na urządzeniach z zainstalowanym systemem z rodziny Windows;
c) możliwość zbierania logów dotyczących zdarzeń rodzajów innych niż: Security, System, Application;
d) zdolność do monitorowania integralności plików;
e) zdolność do monitorowania rejestru systemowego;
f) zdolność do monitorowania urządzeń zewnętrznych (removable devices);
g) agent instalowany na systemach z rodziny Windows musi komunikować się z poszczególnymi komponentami rozwiązania SIEM w sposób zaszyfrowany z wykorzystaniem protokołu HTTPS;
h) musi istnieć możliwość monitorowania stanu agentów w konsoli zarządzającej systemu;
i) musi istnieć możliwość przygotowania różnych zestawów konfiguracji agenta, a następnie przypisywania ich niezależnie do dowolnej ilości (jeden lub więcej) systemów źródłowych. Np. inne konfiguracje dla kontrolerów domeny, a inne dla serwerów DNS;
j) musi umożliwiać automatyzację reakcji na zagrożenie, jak blokowanie zdefiniowanego ruchu sieciowego czy blokada procesu.

126. System musi mieć możliwość realizacji funkcjonalności UEBA (User Entity Behaviour Analysis) zarówno w oparciu o dedykowanego Agenta na systemy Windows oraz w oparciu o logi z systemu Windows. Metadane lub logi dotyczące funkcji UEBA nie mogą podlegać licencjonowaniu ze względu na EPS lub rozmiar.

127. Rozwiązanie musi zapewniać wsparcie dla zarządzania w oparciu o role (Role Based Administration) celem ograniczania dostępu do danych oraz do GUI.

128. System musi być zintegrowany z zewnętrznymi bazami o zagrożeniach (Threat Inteligence Feeds - TI) oraz zawierać już zintegrowany zestaw niekomercyjnych (open source) lub komercyjnych baz zagrożeń.

129. Rozwiązanie musi mieć możliwość korelacji informacji z baz zagrożeń z danymi otrzymywanymi w czasie rzeczywistym. Korelacja ta ma odbywać się w pamięci systemu względem otrzymywanych danych o zdarzeniach (event data).

130. System musi mieć możliwość korelacji informacji z baz zagrożeń z danymi historycznymi

131. System musi mieć możliwość odpytywania (ręcznego lub automatycznego) zewnętrznych źródeł reputacji takich jak np.VirusTotal.

123. System musi mieć możliwość wizualizacji informacji w oparciu o kategorie MITRE ATT&CK dla standardowego zbioru wbudowanych reguł.

133. Pulpity administracyjne (dashboards) muszą mieć możliwość wspólnej prezentacji.

134. Rozwiązanie musi mieć możliwość integracji z innymi systemami do obsługi zgłoszeń poprzez API (ticketing system) oraz mieć wbudowany mechanizm obsługi zgłoszeń (ticketing system) niezależny od obsługi alarmów/incydentów.

135. System musi wpierać mechanizmy typu Machine Learning w oparciu o zgromadzone zdarzenia. Musi być możliwe użycie przynajmniej 4 różnych rodzajów mechanizmów Machine Learning wraz z możliwością ich ręcznego wybrania oraz działania w trybie automatycznym. W wyniku działania opisanych mechanizmów Machine Learning system SIEM ma tworzyć model bazowy zachowania oraz umożliwiać wykrycie odchyleń i anomalii od niego. Zadania Machine Learning mają mieć możliwość dystrybuowania ich pomiędzy elementy warstwy korelującej i/lub zarządzającej. Mechanizmy Machine Learning mają również umożliwiać wsparcie dla podejmowania decyzji przy rozwiązywaniu incydentów w systemie SIEM.

136. Dostarczone rozwiązanie nie może działać w oparciu o oprogramowanie otwarte (ang: open source) w następującym zakresie funkcjonalnym: składowanie, parsowanie, korelacja logów, algorytmy uczenia maszynowego, analiza zachowania użytkowników i zasobów (UEBA), mechanizmy reakcji/ scenariusze reakcji (SOAR). Zamawiający nie zaakceptuje systemu, który wykorzystuje mechanizmy typu open source np.: Elastic Search, OSSIM, Snort, The Hive, AlienVault itd. lub został stworzony przez modyfikację oprogramowania otwartego.

137. W celach weryfikacji zgodności produktu z wymaganiami, musi być on dodatkowo oferowany przez autoryzowanego dystrybutora, dostarczającego produkty z obszaru cyberbezpieczeństwa na rynku polskim, który w przypadku jakichkolwiek wątpliwości Zamawiającego, związanych z wymaganymi funkcjonalności będzie mógł je potwierdzić lub im zaprzeczyć.

138. W związku z tym, że obsługa systemu ma objąć także użytkowników nieposługujących się biegle językiem angielskim, interfejs użytkownika musi umożliwiać obsługę w języku polskim lub posiadać możliwość wgrania plików językowych tłumaczących interfejs na język polski. Pliki tłumaczące interfejs na język polski muszą zostać wgrane w trakcie wdrożenia systemu, przed jego zakończeniem.

139. Zamawiający na obecnym etapie nie jest w stanie zmierzyć ilości danych przekazywanych do systemu, tj. EPS (Events Per Second) oraz nie zna wymagań związanych z architekturą proponowanego rozwiązania, dlatego oferowana licencje nie może nakładać limitów w tym zakresie.

140. Produkt musi umożliwiać równoczesną pracę co najmniej 10 operatorów oraz obsługiwać 450 źródeł logów dotyczących wszystkich zdarzeń związanych z komputerami oraz serwerami wykorzystywanymi w organizacji oraz zapewnić dla tych źródeł detekcję i obsługę cyberzagrożeń w ramach wszystkich oferowanych w tym postępowaniu funkcjonalności.

141. System ma gwarantować możliwość elastycznej rozbudowy o kolejne źródła logów.

142. Funkcjonowanie rozwiązania musi umożliwiać konfigurację „on-premise", w której wszystkie funkcjonalności oraz przetwarzanie danych będzie się odbywać całkowicie w infrastrukturze zamawiającego, zapewniając tym samym możliwość konfiguracji systemu w strefie odseparowanej od sieci Internet.

143. System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows (minimum Server 2016), Redhat/Oracle Linux (minimum 7.x).

144. Dostarczone rozwiązanie musi być objęte 24 miesięcznym wsparciem producenta lub producentów. Wsparcie musi obejmować bezpłatne dostarczanie aktualizacji oprogramowania, reagowanie na zgłaszane błędy systemowe oraz usługę konsultacji powrdrożeniowej w formie spotkań z dedykowanym inżynierem, certyfikowanym z procesu konfiguracji i obsługi oferowanego systemu. Przez błąd systemowy Zamawiający rozumie błędy krytyczne (zakłócenie uniemożliwiające

działanie rozwiązania), błędy poważne (zakłócenie uniemożliwiające działanie części rozwiązania), błędy zwykłe (inne zakłócenia nie stanowiące błędu krytycznego lub poważnego).

145. Wykonawca musi zapewnić usługę obejmującą proces aktualizacji oprogramowania oraz kontekstu systemu (dotyczy to zwłaszcza bazy reguł korelacyjnych, bazy parserów, bazy dostępnych aktualizacji). Dostęp do centralnej usługi aktualizacyjnej ma pozwalać na automatycznie wyświetlanie i pobieranie z poziomu interfejsu systemu dostępnych aktualizacji. Dla pobranych w procesie aktualizacji reguł oraz parserów musi być dostępne wersjonowanie, pozwalające uruchomić nową wersję reguły korelacyjnej oraz parsera z poziomu interfejsu systemu. Automatyczne wersjonowanie ma umożliwiać wczytanie starszej wersji reguły lub parsera, a zmiana reguł i parserów musi być możliwa z poziomu graficznego systemu.

146. Wykonawca zapewni bezpłatne szkolenia w zakresie użytkowania i administrowania wdrożonego systemu lub systemów. Szkolenie ma zostać przeprowadzone dla min. 3 osób i muszą być zakończone przyznaniem certyfikatu, potwierdzającego wspomniane umiejętności wydanym przez producenta systemu/ systemów. Szkolenia mogą odbyć się w formie zdalnej.

147. Zmawiający wymaga by wraz ofertą Wykonawca dostarczył próbkę systemu (np. w postaci przekierowania do wersji demonstracyjnej systemu) z odpowiednią dokumentacją (np. w postaci karty produktu oraz niezbędnych instrukcji). Zamawiający maksymalnie w ciągu dwóch dni roboczych, zweryfikuje zgodność oferowanego systemu na podstawie próbki systemu i dostarczonej dokumentacji, porównując je ze wszystkimi wymaganiami określonymi w powyższych punktach OPZ. W przypadku gdy Zamawiający uzna niezgodność próbki i dokumentacji z wymaganiami OPZ, lub gdy Zamawiający nie odnajdzie określonego wymagania w próbce systemu i dokumentacji, oferta Wykonawcy zostanie odrzucona. W przypadku gdy Wykonawca nie dołączy do oferty próbki systemu wraz z dokumentacją, oferta zostanie odrzucona.

148. Wykonawca musi dostarczyć oferowane rozwiązanie w formie demonstracyjnej, aby umożliwić weryfikację przez Zamawiającego wybranych wymagań OPZ, co do których Zamawiający nie uzyskał wystarczających informacji potwierdzających ich zgodność. Rozwiązanie musi być skonfigurowane w sposób umożliwiający jego weryfikację z wymaganiami OPZ oraz pozwalać na zdalny dostęp. W ramach dostępu do rozwiązania, Wykonawca musi przygotować odpowiednią instrukcję oraz zapewnić wsparcie konsultanta technicznego. Procedura weryfikacji spełnienia wymagań OPZ będzie przebiegać następująco:

a. Zamawiający dokona wyboru min. 10 wymagań OPZ, które zostaną zaprezentowane przez Wykonawcę na systemie demonstracyjnym;
b. Wykonawca w terminie 2 dni od wyboru wymagań OPZ (ppkt a.) dostarczy zwięzły opis do każdego z wybranych wymagań, określający zakres planowanych testów demonstracyjnych;
c. Wykonawca w terminie 3 dni od dostarczenia opisu (ppkt b.) dokona przygotowania systemu demonstracyjnego, w tym: dokona odpowiedniej konfiguracji systemu (umożliwiającego weryfikację wskazanych wymagań OPZ), przygotuje instrukcję dostępową do systemu demonstracyjnego; opracuje instrukcję realizacji zaproponowanych scenariuszy testowania;

149. System XDR powinien posiadać następujące cechy i funkcjonalności

a) Powinien posiadać możliwość instalacji agenta XDR na systemach: - Windows 10 i nowsze,
b) - Windows Server 2016 i nowsze. Agent umożliwia: zbieranie logów ze stacji końcowej/serwera do modułu SIEM, dodawania i wyłączanie reguł zapory sieciowej na stacji końcowej/serwerze, zawieszanie i odwieszanie procesu na stacji końcowej/serwerze. Dodatkowo zapewnia

mechanizm do instalacji oraz zarządzania konfiguracją narzędzia Microsoft Sysmon na stacjach końcowych/serwerach, w celu rozszerzenia logów systemowych o aktywność procesów, plików oraz rejestrów.

c) System powinien być wyposażony w serwer aplikacji udostępniający konsolę graficzną dla operatorów oraz sterujący działaniem orkiestratora oraz kontrolera
d) System powinien posiadać Orkiestrator służący do wykonania akcji na innych systemach niż komputery, na których zainstalowany jest agent XDR, np.: zablokowanie ruchu wychodzącego na Firewall dla hosta, na którym zainstalowany jest agent służy do zarządzania agentami XDR i jest odpowiedzialny zarówno za ich monitorowanie, aktualizację oraz zlecanie im zadań, np.: izolacja procesu czy izolacja sieciowa
e) Agent XDR powinien wzbogacać analizę zdarzeń na nim występujących o pełne dane telemetryczne.
f) System powinien posiadać centralny kontroler zarządzający agentami XDR oraz monitorujący ich pracę
g) System powinien posiadać mechanizm wykrywania zagrożeń zgodny z taktykami i technikami Mitre Att&ck™
h) System powinien umożliwiać wykrywanie zagrożeń na komputerze na bazie wielu wskaźników naruszeń bezpieczeństwa (IoC)
i) System powinien umożliwiać centralną korelację zdarzeń z komputera względem innych zdarzeń (sieć, chmura, Threat Intel)
j) System powinien być wyposażony w mechanizmy uczenia maszynowego obejmujące analizę behawioralną komputera oraz jego użytkownika
k) System powinien posiadać wiele algorytmów wykrywania anomalii oraz profilowania komputera i jego użytkownika
l) System powinien umożliwiać rozszerzoną analizę behawioralną użytkownika komputera względem pracy innych użytkowników
m) System powinien umożliwiać kontrolę aplikacji zainstalowanych na stacjach roboczych i serwerach
n) System powinien umożliwiać kontrolę podatności, zgodności oraz zainstalowanych poprawek
o) System powinien mieć możliwość zaawansowanej analizy zdalnej np.: uruchomione procesy czy połączenia sieciowe
p) System powinien posiadać mechanizmy automatyzujące reakcję na komputerze z poziomu agenta, np.: wstrzymanie procesu, blokada portu
q) System powinien posiadać funkcjonalność dostosowania reakcji na zagrożenia w zależności od rodzajów zagrożeń (konfigurowalne playbooki)
r) System musi być wyposażony w autonomiczny mechanizm oceny ryzyka dla wykrytych zagrożeń
s) System powinien umożliwiać zarządzanie zgodnością (Compliance): KSC/KRI/GDRP
t) System powinien posiadać panel do zarządzania incydentami oraz podatnościami wsparty playbookami
u) System powinien posiadać przejrzyste dashbordy z możliwości drążenia danych oraz wizualizacji zagrożeń
v) System powinien posiadać możliwości powiadamiania o zagrożeniach poprzez e-mail, sms.

Wymagania dodatkowe

1. Wykonawca przekaże Zamawiającemu dostęp do systemu demonstracyjnego na okres 3 dni w celu analizy zgodności z OPZ oraz weryfikacji intuicyjności obsługi.
2. Zamawiający oceni każde z 10 wybranych wymagań, uwzględniając:
   - Intuicyjność (25%)
   - Zgodność (75%)
3. Każde z wymagań może uzyskać maksymalną ocenę 100%. Wymaganie uznaje się za niespełnione, gdy jego ocena zostanie określona przez Zamawiającego poniżej poziomu 75%. Procentowa suma wszystkich wymagań nie może być niższa niż 90%.
4. Wykonawca w okresie 3 dni od otrzymania oceny 75% do 89% ze strony Zamawiającego (ppkt. f) ma możliwość wyznaczenia spotkania w formie zdalnej (np. za pomocą platformy: Teams, Zoom lub Webex), podczas którego odniesie się on do wyników oceny zgodności i intuicyjności systemu, opracowanych przez Zamawiającego. Jeśli w wyznaczonym terminie Wykonawca nie zorganizuje spotkania i/lub nie przedstawi odpowiedzi na ocenę Zamawiającego zostanie uznane, że oferowane rozwiązanie nie spełnia wymagań OPZ.

2. Dostawa systemu zarządzania hasłami i dostępem uprzywilejowanym na potrzeby Starostwa Powiatowego w Kielcach.

2.1 Ilości.

Oprogramowanie	ILOŚĆ
Dostawa systemu zarządzania hasłami i dostępem uprzywilejowanym (licencja wieczysta) na potrzeby Starostwa Powiatowego w Kielcach	1 szt.

2.2 Postanowienia ogólne.

Przedmiotem zamówienia jest zakup, dostarczenie i wdrożenie łącznie z przeprowadzonym szkoleniem dla minimum trzech pracowników działu IT w środowisku informatycznym Zamawiającego systemu zarządzania hasłami i dostępem uprzywilejowanym na potrzeby Starostwa Powiatowego w Kielcach.

Poprzez wdrożenie systemu rozumie się dostarczenie, instalację nowego oprogramowania oraz wykonanie konfiguracji w pełni zgodnej z wymaganiami Zamawiającego, sprawdzenie ustawień, przetestowanie i wyeliminowanie ewentualnych nieprawidłowości oraz pozostawienie dokumentacji technicznej i konfiguracyjnej systemu.

Świadczenie usług serwisu gwarancyjnego przez Producenta musi być realizowane min. do dnia 30.06.2026 obejmujących usuwanie zgłoszonych awarii i usterek dla oprogramowania Zamawiającego, a w razie konieczności jego wymianę

W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

W przypadku awarii wymiana lub udostępnienie oprogramowania lub rozwiązania zastępczego najpóźniej następnego dnia roboczego, na czas trwania naprawy. Dostarczone oprogramowanie zastępcze musi posiadać konfiguracje zgodną z wymaganiami Zamawiającego. Zamawiający zobowiązuje się do udostepnienia konfiguracji oprogramowania na czas awarii. Ponadto oprogramowanie zastępcze musi być uruchomione i przetestowane w siedzibie Zamawiającego.

2.3 Opis parametrów technicznych systemu zarządzania hasłami i dostępem uprzywilejowanym na potrzeby Starostwa Powiatowego w Kielcach.

Wymagania systemu, możliwości oraz funkcje:

1. Będzie obsługiwał bazy danych PostgreSQL oraz MSSQL.
2. Będzie działał na pojedynczej bazie danych.
3. Będzie działał bez agentów.
4. Będzie posiadał możliwość uwierzytelniania SAML 2.0 oraz umożliwia użycie SAML'a 2.0 dla SSO.
5. Będzie posiadał wbudowane moduły zarządzania hasłami, sesjami, dostępem uprzywilejowanym oraz podglądu uprawnień użytkowników w jednym produkcie.

6. Będzie posiadał funkcje importowania użytkowników AD/LDAP/Azure AD.
7. Będzie posiadał możliwość tworzenia i konfiguracji ról uwzględniając konta, reset haseł, kontrolę dostępu, zasoby grup, przydzielanie haseł, dostęp do kluczy SSH, konfigurację ustawień audytu, ustawień generowania raportów oraz ustawień administracyjnych.
8. Będzie posiadał obsługę IE, Chrome, Firefox.
9. Będzie posiadał możliwość połączenia zdalnego z bazą danych SQL.
10. Będzie posiadał REST API, które może być wykorzystane do komunikacji z programami trzecimi.
11. Będzie posiadał moduł do połączeń zdalnych.
12. Będzie posiadał Multi-Tenant Architecture.
13. Będzie posiadał możliwość podwójnego szyfrowania plików i haseł.
14. Będzie posiadał wbudowane skrypty, które pozwalają na:
    - Backup bazy danych
    - Odtworzenie bazy danych
    - Zmianę bazy danych
15. Będzie posiadał możliwość podłączenie certyfikatu w formie .PFX(PKSC12).
16. Będzie posiadał możliwość dostępu do systemu dla użytkownika jest zapewniony za pośrednictwem konsoli webowej.
17. Będzie posiadał możliwość logowania z dowolnej przeglądarki wspierającej protokół HTML5 dla sesji Windows RDP, VNC, SQL, SSH i Telnet bez konieczności instalacji agentów.
18. Będzie umożliwiał połączenie z ADSelfService, DesktopCentral, ServiceDesk Plus.
19. Będzie umożliwiał dwupoziomową autentykację, za pomocą Phone Factor, RSA SecurID, Google Aunthenticator, Microsoft Aunthenticator, Okta Verify, Radius Authenticator, Duo Security, YubiKey, Zoho OneAuth Authenticator, Oracle Authenticator oraz wysyłanie jednorazowego hasła na wybraną skrzynkę pocztową.
20. Będzie posiadał wbudowaną opcję przeglądania głównych informacji w postaci dashboard'u.
21. Będzie posiadał funkcjonalność centralnego repozytorium haseł przechowywany w zabezpieczony sposób.
22. Będzie posiadał funkcje definiowania właścicieli haseł.

Domyślnie administrator dodający hasło musi zostać jego właścicielem.

Właściciel ma możliwość przydzielania poziomów uprawnień:

- Tylko do przeglądu
- Przegląd i modyfikacja

23. Będzie umożliwiał dostęp do systemu dla użytkownika jest zapewniony za pośrednictwem konsoli webowej.
24. Będzie umożliwiał zdalny reset haseł dla systemów Windows, domeny Windows, systemów Linux, IBM AIX, HP UNIX, Solaris, Mac OS, MS SQ, MySQL, Oracle DB, Sybase ASE, urządzeń HP ProCurve, Cisco (IOS, CatOS, Pix).
    Zdalny reset haseł jest możliwy bezagentowo lub za pośrednictwem agenta.
25. Będzie umożliwiał dostęp do tworzenia statycznych i dynamicznych grup jak i ich usuwanie oraz zbiorczą konfigurację.
26. Będzie umożliwiał modyfikację atrybutów dla wybranej grupy w środowisku domenowym.
27. Będzie posiadał wbudowaną funkcję definiowania polityki haseł pracowników.
28. Będzie zapewniał integrację szeregu systemu ticketowych w celu automatycznej weryfikacji zgłoszeń serwisowych, związanych z uprzywilejowanym dostępem.

29. Będzie umożliwiał export danych grupy do pliku „xlsx" lub w formie zaszyfrowanej w postaci pliku „html", jak i do Dropboxa, Boxa oraz Amazona S3 dla urządzeń mobilnych.
30. Będzie wyposażony w notyfikację w przypadku uruchomienia procedury resetu haseł.
31. Będzie umożliwiał generowanie raportu dla wybranej grupy, a w szczególności:

    -Spisu haseł

    -Zgodności polityk

    -Wygasłych haseł

33. Będzie umożliwiał zdalne logowanie z dowolnej przeglądarki wspierającej protokół HTML5 dla sesji Windows RDP, VNC, SQL, SSH i Telnet bez konieczności instalacji agentów.
34. Zdalne sesje będą tunelowane przez serwer centralny systemu zarządzania hasłami bez konieczności bezpośredniej komunikacji urządzenia użytkownika z urządzeniem docelowym.
35. Zdalne sesje muszą dawać administratorowi możliwość śledzenia sesji otwartej przez innego użytkownika, na żywo, tzw. Session shadowing.
36. Zdalne sesje użytkownika mogą być przerwane w dowolnym momencie przez administratora.
37. Będzie umożliwiał nagrywanie sesji użytkownika.
38. Sesje musza mieć możliwość eksportu.
39. Sesje mogą być usuwane po określonym czasie.
40. Sesje Oraz wykonany chat podczas sesji musza mieć możliwość wybiórczego usuwania.
41. Oprogramowanie będzie umożliwiać zarządzanie kluczami SSH dla łatwiejszego połączenia z serwerem, a w szczególności: tworzenie, usuwanie, importowanie, przypisywanie, odłącznie, zamianę i przeglądanie histori klucza SSH.
42. Będzie posiadał możliwość generowania powiadomienia Każdej operacji na haśle
    - Z możliwością definiowania powiadomień email
    - Z możliwością generowania pułapek SNMP lub rejestrów syslog i przesłania ich do systemów SIEM (Security Information and Event Management)
    - Z możliwością generowania zdarzeń w ramach rejestrów syslog

43. Będzie posiadał możliwość dodawania, tworzenia, przypisywania, skanowania certyfikatu na podatność/wrażliwość, tworzenia grupy dla certyfikatu, sprawdzania daty wygaśnięcia domeny, zaznaczenie jako „root", synchronizacja z CMDB, Importowania klucza, edytowanie certyfikatu, udostępnienia użytkownikom lub grupie użytkowników, raport udziały oraz usuwanie certyfikatu.
44. Będzie pozwalał na łatwe wykrycie certyfikatów za pomocą adresu IP/pliku/Subnet'u, certyfikatów serwerów email, modułu równoważenia obciążenia (Load Balancer) oraz angetów.

45. Będzie pozwalał na dodawanie, usuwanie i zarządzanie próśb przydzieleń certyfikatów nadesłanych przez użytkowników.
46. Będzie pozwalał na podłączenie certyfikatu w formie .PFX(PKSC12)
47. Oprogramowanie będzie umożliwiać certyfikowanie:
    - „Let's Encrypt"
    - „GoDaddy"
    - „The SSL Store"
48. System będzie umożliwiał integrację z systemem Windows Active Directory (AD), usługami LDAP oraz Azure AD.
49. Będzie umożliwiał logowanie do systemu zarządzania hasłami za pośrednictwem wyżej wymienionych usług katalogowych.
50. Będzie uwzględniał restrykcje uwierzytelniania AD/LDAP/Azure AD podczas logowania.
51. Administrator systemu zarządzania hasłami musi mieć możliwość importowania użytkowników/ grup użytkowników z AD/LDAP/Azure AD do systemu.
52. Oprogramowanie musi umożliwiać automatyczne dodawanie użytkownika do systemu, po utworzeniu go w AD/LDAP/Azure AD.
53. System będzie posiadał możliwość:
    - definiowania polityk haseł, jak: długość hasła, wymuszanie cyfr i ich ilość, wymuszanie znaków specjalnych i ich ilość, zabronione znaki czy hasło może zawierać login, czy hasło ma się zaczynać literą alfabetu, jak długo może utrzymywać się jedno hasło oraz jak długo nie można użyć ponownie tego samego hasła.
    - tworzenia, definiowania i przypisywania ról dla wybranych użytkowników
54. System będzie posiadał narzędzie do wyszukiwanie zmian haseł
55. Będzie posiadał Rebrand- dostosowywanie wyglądu strony
56. Będzie posiadał możliwość konfiguracji szablonu wyglądu wiadomości email, pluginu resetu hasła, konfigurację komend SSH
57. Będzie umożliwiał dwupoziomową autentykację, za pomocą Phone Factor, RSA SecurID, Google Aunthenticator, Microsoft Aunthenticator, Okta Verify, Radius Authenticator, Duo Security YubiKey oraz wysyłanie jednorazowego hasła na wybraną skrzynkę pocztową poprzez konfigurację SSO dzięki użyciu protokołu SAML w wersji 2.0, za pomocą smart card'ów, PKI oraz certyfikatów.
58. Administrator haseł może mieć status 'super administratora' po przydzieleniu przez innego administratora (statusu tego nie można przydzielić samemu sobie) - 'super administrator'

posiada uprawnienia zarządzania wszystkimi zasobami dodanymi do systemu zarządzania hasłami przez wszystkich administratorów/użytkowników.

59. System będzie pozwalał na dwa typy wyświetlania logów: „DEBUG" - pokazuje wszystkie przypisy wiadomości - oraz „INFO" - wyświetla tylko informacje o wiadomościach.
60. Będzie zapewniał wiele opcji do bezpiecznego dostępu offline oraz określone opcje eksportu dla użytkowników.
61. Będzie zapewniał konfigurację skrzynki pocztowej, dla powiadomień użytkowników.
62. Będzie umożliwiał konfigurację serwera proxy.
63. Będzie zapewniał backup'owanie bazy danych, wraz z możliwością ustawień powtarzalności, godziny, kiedy ma być wykonany backup i ile backup'ów ma być trzymanych na przeznaczonym do tego folderze. Będzie pozwalał też na odtworzenie bazy danych oraz zmianę bazy danych
64. Będzie umożliwiał definiowanie dopuszczalnych IP oraz tych, które mają być blokowane.
65. Będzie posiadał moduł API (Application Programming Interface), którego wykorzystanie będzie zapewniać programowalne wykonanie zapytań przez aplikacje lub skryptu o pozyskanie hasła z systemu zarządzania hasłami, aby nawiązać połączenie z inną aplikacją czy bazą danych.
66. Będzie zapisywał bazę danych haseł w wybranym serwerze i szyfruje je za pomocą AES-256
67. Będzie posiadał możliwość szyfrowania za pomocą Safenet HSM, gdzie zaszyfrowany klucz będzie znajdował się na oddzielnym urządzeniu.
68. Będzie umożliwiał powiadomienie wszystkich użytkowników za pomocą wiadomości email, dla osób nieposiadających konta lub alertu online.
69. Będzie umożliwiał tworzenie harmonogramów zadań lub użycie pre-definiowanych harmonogramów.
70. Będzie zapewniał podgląd próśb użytkowników o dostęp haseł
71. Będzie zapewnia integrację:

- Chmurową
- Z platformami CI/CD:
- Jenkins
- Ansible
- Chef
- Puppet

Z innymi programami ManageEngine:

- ServiceDesk Plus
- ADSelfService Plus
- Analyticks Plus

- Eventlog
- Analyzer
- Log360
- UEBA
- ADManage
- r Plus

72. System będzie zapewniał możliwość instalacji agenta, dla:
    - Windows Agent w wersji 32- lub 64-bitowej
    - Windows Domain Agent w wersji 32- lub 64-bitowej
    - Linux Agent w wersji 32- lub 64-bitowej
73. System będzie umożliwiał audyt operacji, jak:
    - Audyt zasobów - wszystkie operacje związane z zasobami, grupami zasobów, kontami, hasłami, udziałami i politykami
    - Audyt użytkowników - wszystkie operacje wykonane w systemie zarządzania hasłami przez jego użytkowników
    - Audyt zadań - rejestr zdefiniowanych zadań
    - Odtwarzanie nagranych sesji
    - Audyt nagranych połączeń
    - Audyt aktywnych sesji
    - Audyt przypisanych kluczy
74. Będzie posiadał możliwość włączenia dodatkowej kontroli dostępu do zasobów oraz ograniczenia możliwości łączenia zdalnej sesji spoza systemu. W tym:

a) Możliwość włączenia i wyłączenia zatwierdzania dostępu

b) Możliwość wyłączenia podglądu haseł

c) Możliwość automatycznego resetowania haseł po każdej sesji

d) Możliwość automatycznego przydzielania dostępu

e) System posiada możliwość natychmiastowego wyłączenia w przypadku sytuacji awaryjnej, w tym wyłączenia wszelkiej komunikacji z agentami oraz po API

75. Będzie posiadał możliwość zdefiniowania raportów oraz zabezpieczenia wspierające zgodność z RODO, w tym: Kontrola IP, z jakich następuje połączenie z aplikacją, zarówno sesji webowej jak i API, dostęp, aktywność oraz raport użytkowników, nieprzydzielonych do żadnej grupy, podsumowanie dostępu haseł, działań i naruszeń zasad, przynależności, tworzenia i dokładny obieg kluczy SSH wykonanych w PAM360

76. Będzie posiadał możliwość wyłączenia podglądu danych osobowych.
77. Będzie zapewniał możliwość zaszyfrowanego eksportu danych.
78. Będzie pozwalał „ponawiać" okresowe resetowanie hasła grup zasobów, konfigurując ustawienia ponownych prób resetowania hasła, które obejmują ich liczbę i interwał.
79. Będzie umożliwiał organizacjom klienckim tworzenie własnych konfiguracji SAML.
80. Będzie pozwalał zaimplementować ograniczenia kont domeny dla zasobów docelowych, tj. użytkownikom kont domeny Windows można przyznać dostęp tylko do określonych zasobów, do których faktycznie chcą uzyskać dostęp, zamiast do wszystkich współdzielonych z nimi zasobów.
81. Będzie posiadał interfejsy RESTAPI: Fetch User GroupID, Configure Remote Password Reset for Linux resources, Share Resource i Share account to User Group.
82. Będzie pozwalał przeglądać wszystkie certyfikaty skojarzone z określonym agentem.
83. Będzie pozwalał wykrywać certyfikaty wydane przez określony „Microsoft Certificate Authoritory" wprowadzając podczas wykrywania nazwę MSCA w odpowiednim polu tekstowym. Dostępne dla PAM360 na serwerach z systemem Windows.
84. Będzie pozwalał na dodanie nazwy Wildcard w polu SAN podczas tworzenia CSR lub certyfikatu z podpisem własnym. Dzięki certyfikatom Wildcard można zabezpieczyć nieograniczoną liczbę subdomen dla zarejestrowanej domeny bazowej.
85. Będzie obsługiwał zaplanowane zadania wykrywania SSL i MS Certificate Store Discovery za pomocą agenta KMP.
86. Będzie pozwalał na dostosowanie liczby dni na automatyczne odnawianie certyfikatów przed ich wygaśnięciem.
87. Będzie pozwalał podczas podpisywania CSR certyfikatów SSL za pomocą agenta KMP na określenie wartości limitu czasu agenta w sekundach.
88. Będzie pozwalał użytkownikom wybierać określone certyfikaty lub grupy certyfikatów podczas generowania typu harmonogramu „SSL Certificates Report".
89. Będzie umożliwiał użytkownikom dodawanie i edytowanie listy wdrożonych serwerów. Nowo dodane serwery zostaną zmapowane z najnowszą wersją certyfikatu w repozytorium certyfikatów.
90. Będzie obsługiwał wykrywanie zakresów adresów IP na potrzeby wykrywania magazynu certyfikatów MS przy użyciu usługi PAM360 z kontem administratora domeny, co będzie pozwalać administratorom wykrywać certyfikaty w sieciach.
91. Będzie obsługiwał wykrywanie certyfikatów „Load Balancer" dla urządzeń Citrix.
92. Będzie obsługiwał zaplanowane wykrywanie certyfikatów z systemów równoważnia obciążenia opartych na systemie Linux, takich jak BIG-IP F5, Nginx i Citrix.

93. Będzie pozwalał użytkownikom na ominięcie ustawień serwera proxy podczas wykrywania certyfikatów SSL.
94. Będzie pozwalał na automatyczne wdrożenie certyfikatów MSCA/self-signed, jeśli poświadczenia użytkownika są dostępne.
95. Będzie umożliwiał użytkownikom wybranie „Certificate type" [CER/DER/P7B/CRT] i „Keystore type" [JKS/PKCS/PEM/KEY] podczas wdrażania certyfikatów na komputerach z systemem Windows i Linux oraz podczas eksportowania certyfikatów.
96. Będzie pozwalał na odnowienie certyfikatów typu MSCA z nowym kluczem prywatnym, jeśli klucz prywatny nie jest jeszcze dostępny.
97. Będzie obsługiwał ClouDNS, aby zakończyć weryfikację kontroli domeny podczas uzyskiwania certyfikatów od publicznych urzędów certyfikacji.
98. Będzie obsługiwał magazyny kluczy PKCS12 z szyfrowaniem AES256 podczas dodawania magazynów kluczy certyfikatów.
99. Będzie pozwalał użytkownikom wybrać do pięciu szablonów certyfikatów podczas wykrywania certyfikatów lokalnych CA na podstawie agenta.
100. Będzie umożliwiał wyszukiwanie w niestandardowych kolumnach certyfikatów SSL i kluczy SSH.
101. Będzie pozwalał na dołączenie wielu serwerów dla certyfikatów w powiadomieniach o wygaśnięciu certyfikatu SSL.
102. Będzie umożliwiał użytkownikom bezpośrednio importować istniejące certyfikaty ze swojego konta GoDaddy do repozytorium.
103. Będzie posiadał możliwość skojarzenia kluczy lokalnie, jeśli zdalne skojarzenie nie powiedzie się dla użytkowników, których dostęp został przerwany.
104. Będzie posiadał interfejsy API REST „Get Password Policies" i "Get Resource Types".
105. Będzie obsługiwał wykrywanie certyfikatów SSL ze ścieżek współdzielonych UNC (Uniwersal Naming Convention) dla komputerów z systemem Windows, Linux i Mac OS.
106. Będzie umożliwiał wykrywanie certyfikatów SSL z katalogów na zdalnych maszynach, które nie są bezpośrednio dostępne przez PAM360 - wszystko za pośrednictwem agenta KMP.
    Opcja ta będzie również dostępna podczas zaplanowanego wykrywania certyfikatów
107. Będzie umożliwiał użytkownikom wdrażanie certyfikatów SSL w przeglądarkach dla następujących typów serwerów: Windows, Linux i MacOS.
108. Będzie umożliwiał ograniczenie użytkownikom bezpośredniego dostępu do użytkowników root poprzez wyłączenie logowania użytkownika root. Włączenie tej opcji podnosi poziom logowania

użytkownika z użytkownika innego niż root do użytkownika root i kojarzy klucze ze wszystkimi innymi użytkownikami na serwerze.

109. Będzie posiadał interfejs API REST „Deploy Certificate".
110. Będzie umożliwiał ponowne odnajdywanie certyfikatów SSL z tego samego źródła przy użyciu danych serwera wprowadzonych podczas poprzedniej operacji wykrywania.
111. Będzie integrował się z Buypass Go SSL i ZeroSSL - dwoma urzędami certyfikacji, które korzystają z protokołu Automatic Certificate Management Environment (ACME) w celu dostarczania bezpłatnych, bezpiecznych certyfikatów SSL. Użytkownicy mogą żądać, pozyskiwać, tworzyć, wdrażać, odnawiać i automatyzować kompleksowe zarządzanie certyfikatami SSL/TLS wydanymi przez Buypass Go SSL i ZeroSSL.
112. Będzie integrował się z ManageEngine Mobile Device manager (MDM) Plus. Integracja ta wykorzystuje interfejsy API ManageEngine MDM do wykrywania I wdrażania certyfikatów SSL na i z urządzeń mobilnych zarządzanych przez serwer MDM.
113. Będzie umożliwiał następnie filtrowanie wykrytych certyfikatów SSL na podstawie typu systemu operacyjnego, takiego jak: Android, Windows, Chrome OS, Mac OS i Apple tvOS. Możliwe będzie również eksportowanie raportów certyfikatów MDM zarządzanych w repozytorium systemu w wybranym okresie. Będzie można też zaplanować okresowe generowanie raportów certyfikatów MDM.
114. Będzie umożliwiał globalną modyfikację poziomu dostępu współdzielonych certyfikatów.
115. Będzie posiadał interfejsy API REST: 'Share SSL Certificate to User', 'Share SSL Certificate to User Group', 'Share SSL Certificate Group to User', 'Share SSL Certificate Group to User Group', 'Revoke SSL Certificate from User', 'Revoke SSL Certificate from User Group', 'Revoke SSL Certificate Group from User', 'Revoke SSL Certificate Group from User Group', 'Create SSL Certificate Group', 'Delete SSL Certificate Group', 'Edit SSL Certificate Group', 'Generate an Agent Install Key'.
116. Będzie posiadał dwa nowe agenty: agent C# dla Windows/Windows Domain i agent Go dla Linuxa. Będzie umożliwiał to użytkownikom ograniczenie kont użytkowników dodawanych za pośrednictwem agentów (tylko nowi agency) podczas wykrywania kont, przy użyciu wzorców regularnych.
117. Będzie posiadł security framework w najnowszej wersji, aby ograniczyć występowanie luk w zabezpieczeniach i poprawić ogólne bezpieczeństwo.
118. System posiadał serwer PostgreSQL, serwer Apache Tomcat, narzędzie Rubyrep, Apache Log4j.
119. Będzie obsługiwał platformę OpenJDK, sterownik Microsoft JDBC oprócz sterownika JTDS JDBC do łączenia z serwerem SQL.

120. Będzie obsługiwał weryfikacje integralności poprawki, która będzie wymagać importowania certyfikatu SSL za każdym razem, gdy produkt zostanie zaktualizowany przy pomocy pliku PPM.
121. Będzie pozwalał użytkownikom na dodawanie kont za pośrednictwem agenta domeny Windows, gdy filtr kont będzie dostarczany przy użyciu wzorców regularnych.
122. Będzie pozwalał administratorom ograniczyć użytkownikowi możliwość konfigurowania hasła szyfrowania dla jego haseł osobistych, użytkownik będzie mógł skonfigurować „klucz szyfrowania" dla swoich haseł osobistych na karcie „Osobiste". Będą mogli również swobodnie wybierać między przechowywaniem lub nieprzechowywaniem klucza szyfrowania, a korzystaniem z klucza szyfrowania aplikacji.
123. Będzie posiadał możliwość przeniesienia użytkowników RESTAPI do klienta. Obsługiwane organizacje klienckie z pełnym dostępem będą mogły zarządzać zasobami i kontami.
124. Będzie posiadał pojedynczy harmonogram „Kontroli czyszczenia i podsumowania", który będzie połączony z sześciu harmonogramów audytu: „Harmonogram czyszczenia audytu zasobów", „Harmonogram podsumowania audytu zasobów", „Harmonogram czyszczenia UserAudit", „Harmonogram czyszczenia UserAudit", „Harmonogram czyszczenia TaskAudit" i „Harmonogram podsumowania audytu TaskAudit". Będzie posiadał „Harmonogram aktywności wykresu tablicy rozdzielczej".
125. Będzie pozwalał na usunięcie starych rekordów - na podstawie daty z określeniem odpowiedniego typu operacji. Dla przykładu - system pozwoli na usunięcie danych audytowych starszych niż 365 dni, w których wykonano akcję restart hasła.
126. Będzie pozwalał administratorom MSP replikować ustawienia typu operacji inspekcji i ustawienia czyszczenia inspekcji we wszystkich organizacjach klienckich.
127. Będzie posiadał nową wersję API REST, którazawiera kilka nowych interfejsów dla następujących operacji: powiązanie zasobu z grupą zasobów, odpięcie zasobu od grupy zasobów, pobranie grup zasobów powiązanych z zasobem, usuwanie grup zasobów i pobieranie identyfikatora grup zasobów.
128. Będzie posiadał możliwość wprowadzenia nazwy hosta użytkownika interfejsu API bez uwzględnienia wielkości liter.
129. Będzie umożliwiał konfigurację harmonogramów automatycznego wykrywania kont uprzywilejowanych podczas wykrywania systemu: Linux, urządzeń sieciowych oraz VWware.
130. Będzie posiadał możliwość konfiguracji SAML w układzie High Availability.
131. Będzie posiadał Dropbox SDK w wersji min. 5.0.0
132. Będzie posiadał możliwość konfiguracji wiadomości powitalnej po rozpoczęci sesji zdalnej.

133. Będzie wspierał SAML Single Logout - który automatycznie kończy wszystkie powiązane sesje nawiązane za pomocą SAML SSO w chwili wylogowania użytkownika z interfejsu aplikacji.

    Funkcja rotowania kluczem szyfrującym będzie dostępna dla wszystkich edycji produktu.

134. Będzie umożliwiał na zdalne łączenie się bezpośrednio do aplikacji w systemie Windows przy pomocy RemoteApp
135. Będzie umożliwiał podnoszenie uprawnień dla użytkowników przy pomocy funkcji Just-in-time privilege elevation dla rozszerzeń plików CMD, EXE, MSI, MSC oraz BAT. Dzięki czemu użytkownik końcowy będzie w stanie uruchomić wyszczególnione aplikację z uprawnieniami administratora.
136. Będzie posiadał możliwość integracji z systemem ticketowym BMC Helix Remedyforce, a także możliwość integracji z rozwiązaniem Entrust nShield Hardware Security Module (HSM) oraz AWS Certificate Manager - zaufanym urzędem certyfikacji i menedżerem certyfikatów.
137. Będzie posiadał natywnego klienta (typu Remote Connect), który ułatwia nawiązanie bezpośredniego zdalnego dostępu do zasobów docelowych opartych na systemie Windows i SSH, bez potrzeby korzystania z wielu zdalnych klientów lub przeglądarek internetowych. Natywny klient będzie miał zdolność natywnego klienta pulpitu zdalnego systemu Windows i klienta SSH Putty do uruchamiania połączeń opartych na protokole RDP i SSH ze scentralizowanej konsoli.
138. Będzie posiadał integrację z rozwiązaniem Kubernetes oraz z rozwiązaniem SIEM Microsoft Sentinel
139. Będzie posiadał możliwość weryfikacji komend wpisywanych przez użytkowników podczas połączenia SSH oraz blokowania wybranych zachowań.
140. Będzie posiadał możliwość samoobsługowego podniesienia uprawnień dla systemu Linux
141. Będzie posiadał funkcję HTTPS Gateway, która pozwala użytkownikom uruchamiać uprzywilejowane połączenia HTTPS z wewnętrznymi i zewnętrznymi stronami internetowymi, które nie są bezpośrednio dostępne z urządzeń końcowych użytkowników.
142. Będzie posiadał możliwość skonfigurowania Zero Trust Approach, dzięki któremu możemy na podstawie wskaźnika zaufania użytkownika ograniczyć mu funkcję aplikacji.
143. Będzie umożliwiał regularne sprawdzanie stanu synchronizacji certyfikatów SSL wdrożonych bezpośrednio na wielu serwerach.

144. Będzie zawierał teraz kategorię „Narzędzia", która umożliwia użytkownikom niezależne przeprowadzanie konwersji certyfikatów, parsowanie SSL/CSR i skanowanie pod kątem luk w zabezpieczeniach bez dodawania certyfikatów do repozytorium.
145. Będzie pozwalał na zarządzanie całym cyklem życia certyfikatów MSCA
146. Będzie posiadał integrację z Azure Key Vault - usługą zarządzania certyfikatami SSL oferowaną przez firmę Microsoft, z Sectigo Certificate Manager - platformą zarządzania PKI stworzoną do zarządzania certyfikatami SSL/TLS, kluczami SSH i innymi tożsamościami cyfrowymi.
147. Będzie posiadał możliwość wdrażania certyfikatów w systemie Citrix ADC Load Balancer
148. Będzie pozwalał na obsługę wielu domen LDAP
149. Będzie posiadał interfejsy API REST: 'Fetch All Users', 'Fetch All User Groups', 'Bulk Share Resource Groups to Users or User Groups', 'Bulk Share Resources to Users or User Groups', 'Bulk Share Accounts to Users or User Groups'
150. Będzie posiadał typ zasobu typu RabbitMQ.
151. Będzie posiadał możliwość importowania użytkowników, zasobów, organizacji i haseł z plików Excel tak jak .xls, .xlsx
152. Będzie pozwalał na logowanie do aplikacji przy pomocy kodów QR
153. Będzie posiadł integrację z Zoho Flow, z ServiceDesk Plus Cloud
154. Będzie posiadał dashboard dotyczący bezpieczeństwa środowiska serwera oraz aplikacji
155. Będzie pozwalał na skonfigurowanie Time-Based One Time Password (TOTP) jako składnik uwierzytelniania 2FA dla użytkowników
156. Będzie obsługiwał SCIM 2.0 (System for Cross-domain Identity Management) w celu wymiany danych użytkownika pomiędzy dostawcami tożsamości obsługiwanymi przez SCIM a aplikacją
157. Będzie posiadał integrację w ramach DevOps, platform CI/CD lub innych mikrousług/oprogramowania w organizacjach
158. Będzie pozwalał na obsługiwanie języków Java i Python
159. Będzie pozwalał na bezpieczną i bezproblemową wymianę danych przy pomocy pakietów SDK
160. Będzie posiadał integrację Kubernetes (K8s) dla TLS Secrets, która pozwala na automatyczne wdrażania aplikacji kontenerowych, skalowanie i zarządzanie TLS Secrets
161. Będzie posiadał możliwość tworzenia i zarządzania certyfikatami przy pomocy funkcji Private CA (Intermediate CA)
162. Będzie pozwalał na zarządzenie kluczami TLS przechowywanymi w usłudze Microsoft Azure Key Vault
163. Będzie pozwalał na dodawanie własnych dostawców ACME w celu skuteczniejszego zarządzania cyklem życia certyfikatów

164. Będzie posiadał raporty zgodności z NIS2
165. Będzie posiadał integrację z ManageEngine IT Operations Management (ITOM)
166. Będzie posiadał możliwość zarządzania uprawnieniami w chmurze poprzez integrację z Cloud Infrastructure Entitlements Management (CIEM)

Wymagania dodatkowe

1. Wykonawca przekaże Zamawiającemu dostęp do systemu demonstracyjnego na okres 3 dni w celu analizy zgodności z OPZ oraz weryfikacji intuicyjności obsługi.
2. Zamawiający oceni każde z 10 wybranych wymagań, uwzględniając:
   - Intuicyjność (25%)
   - Zgodność (75%)
3. Każde z wymagań może uzyskać maksymalną ocenę 100%. Wymaganie uznaje się za niespełnione, gdy jego ocena zostanie określona przez Zamawiającego poniżej poziomu 75%. Procentowa suma wszystkich wymagań nie może być niższa niż 90%.
4. Wykonawca w okresie 3 dni od otrzymania oceny 75% do 89% ze strony Zamawiającego (ppkt. f) ma możliwość wyznaczenia spotkania w formie zdalnej (np. za pomocą platformy: Teams, Zoom lub Webex), podczas którego odniesie się on do wyników oceny zgodności i intuicyjności systemu, opracowanych przez Zamawiającego. Jeśli w wyznaczonym terminie Wykonawca nie zorganizuje spotkania i/lub nie przedstawi odpowiedzi na ocenę Zamawiającego zostanie uznane, że oferowane rozwiązanie nie spełnia wymagań OPZ.

Zmawiający wymaga by wraz ofertą Wykonawca dostarczył próbkę systemu (np. w postaci przekierowania do wersji demonstracyjnej systemu) z odpowiednią dokumentacją (np. w postaci karty produktu oraz niezbędnych instrukcji). Zamawiający maksymalnie w ciągu dwóch dni roboczych, zweryfikuje zgodność oferowanego systemu na podstawie próbki systemu i dostarczonej dokumentacji, porównując je ze wszystkimi wymaganiami określonymi w powyższych punktach OPZ. W przypadku gdy Zamawiający uzna niezgodność próbki i dokumentacji z wymaganiami OPZ, lub gdy Zamawiający nie odnajdzie określonego wymagania w próbce systemu i dokumentacji, oferta Wykonawcy zostanie odrzucona. W przypadku gdy Wykonawca nie dołączy do oferty próbki systemu wraz z dokumentacją, oferta zostanie odrzucona.

3. Dostawa i wdrożenie zabezpieczenia sieciowego w postaci rozwiązania typu Firewall wraz z systemem analizy i logowania zdarzeń i ochrona poczty na potrzeby Starostwa Powiatowego w Kielcach.

System	ILOŚĆ
Dostawa i wdrożenie zabezpieczenia sieciowego w postaci rozwiązania typu Firewall z systemem analizy i logowania zdarzeń oraz ochroną poczty na potrzeby Starostwa Powiatowego w Kielcach.	1 szt.

3.1. Postanowienia ogólne.

Firewall: Przedmiotem zamówienia jest dostawa dwóch urządzeń do zabezpieczenia ruchu sieciowego w postaci rozwiązań typu Firewall oraz wdrożenie tego systemu. Całościowy system bezpieczeństwa musi być zrealizowany poprzez dwa urządzenia działające w klastrze niezawodnościowym. System realizujący funkcję Firewall musi zapewniać pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System bezpieczeństwa musi realizować wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza.

System musi umożliwiać budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.

Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego

Systemem analizy i logowania zdarzeń: W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje:

ESX/ESXi 6.0/6.5/7.0/8.0, Microsoft Hyper-V 2019/2022/2025, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, AWS (Amazon Web Services), Microsoft Azure, Google Cloud (GCP).

Ochrona poczty: W ramach postępowania wymaganym jest dostarczenie mechanizmu ochrony poczty. System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników.

Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić platformę w postaci odpowiednio zabezpieczonego systememu operacyjnego, na którym będzie instalowane rozwiązanie. Platformy muszą mieć możliwość uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 6.0/6.5/7.0/8.0, Microsoft Hyper-V 2019/2022/2025, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, AWS (Amazon Web Services), Microsoft Azure.

Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń.

Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:

1. Tryb Gateway.
2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).

Wymagania dodatkowe:

Zamawiający wymaga, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odnisieniu do produktów podwójnego zastosowania.

Zamawiający wymaga oświadczenia producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

Wdrożenie: Poprzez wdrożenie systemu rozumie się dostarczenie, instalację nowych urządzeń oraz wykonanie konfiguracji w pełni zgodnej z istniejącą na obecnie wykorzystywanej zaporze sieciowej, bez użycia narzędzi do automatycznych konwersji ustawień. Wykonanie backupu ustawień po sprawdzeniu, przetestowaniu i wyeliminowaniu ewentualnych nieprawidłowości oraz pozostawienie dokumentacji technicznej i konfiguracyjnej systemu. Wszystkie dostarczane urządzenia muszą zostać zainstalowane (tj. wypakowane, zmontowane, zamontowane w szafach RACK, uruchomione i skonfigurowane) w docelowym miejscu pracy (wskazanym przez Zamawiającego) w terminie

uzgodnionym z Zamawiającym (miejsce i termin instalacji należy uzgodnić na min. 5 dni roboczych przed planowaną dostawą urządzeń). Wszystkie opakowania zostaną zutylizowane przez i na koszt Wykonawcy.

Wszystkie dostarczone w ramach tego postępowania urządzenia przeznaczone do instalacji w szafie RACK, muszą być zainstalowane w szafie RACK. Zamawiający wydzieli pomieszczenie pod instalację infrastruktury, Wykonawca zainstaluje sprzęt w pomieszczeniu zgodnie z zaleceniami producenta dot. warunków pracy dla dochowania warunków gwarancji pod względem parametrów fizycznych otoczenia i zadba o spełnienie warunków fizycznych dla bezpieczeństwa instalowanej infrastruktury min. w okresie udzielonej gwarancji. Pomieszczenie jest klimatyzowane. Wszystkie niezbędne wkładki światłowodowe i przewody połączeniowe konieczne do uruchomienia dostarczonych urządzeń dostarcza oraz instaluje Wykonawca. Nowo dostarczony system bezp. musi zostać skonfigurowany zgodnie z zaleceniami Zamawiającego, w tym musi zostać przeniesiona konfiguracja z posiadanego przez Zamawiającego urządzenia na dostarczany klaster nowych urządzeń. W celu prawidłowego oszacowania warunków i zakresu prac instalacyjnych przy montowaniu i uruchamianiu urządzeń w pomieszczeniu Zamawiający wymaga wykonanie wizji lokalnej.

W okresie gwarancji zamawiający wymaga Asysty Technicznej Wykonawcy **w siedzibie zamawiającego** w zakresie obsługi sprzętu i oprogramowania będącego przedmiotem Umowy oraz aktualizacji oprogramowania w łącznej ilości ***200*** roboczogodzin. Przez „Roboczogodzinę" należy rozumieć pełną godzina zegarową pracy inżyniera w ramach usługi Asysty Technicznej, nie wliczając czasu dojazdu do siedziby zamawiającego.

Wizja lokalna: Zamawiający przewiduje obowiązek odbycia przez Wykonawcę wizji lokalnej w celu sprawdzenia warunków teleinformatycznych i teletechnicznych będących przedmiotem zamówienia (opisanych z dziale konfiguracja i uruchomienie sprzętu).
W celu umówienia wizji lokalnej należy kontaktować się z osobami wyznaczonymi do komunikowania się z Wykonawcami
Wizja ma charakter obligatoryjny tj. zgodnie z art. 226 ust. 1 pkt. 18 ustawy PZP Zamawiający odrzuci ofertę Wykonawcy, który jej nie odbył
Zamawiający przewiduje możliwość odbycia wizji lokalnej w dniach pracy Urzędu od poniedziałku do piątku, godz. 7.15- 15.15
Zamawiający podczas wizji, o której mowa powyżej wyda Wykonawcy oświadczenie o odbyciu wizji lokalnej (w formie protokołu), które Wykonawca zobowiązany jest załączyć do oferty.

Szkolenie: Zamawiający, w ramach całości wykonania zadania, wymaga przeprowadzenia szkolenia w siedzibie Zamawiającego w godzinach pracy urzędu tj. Pn-Pt 7.15-15.15 dla minimum trzech pracowników działu IT:

- szkolenie z firewalla min. 8 – maks. 10 godzin
- szkolenie z ochrony poczty min. 4 – maks. 8 godzin
- szkolenie z systemu analizy i logowania zdarzeń min. 4 – maks. 8 godzin

Gwarancja i wsparcie: Świadczenie usług serwisu gwarancyjnego przez Producenta musi być realizowane min. do dnia 30.06.2026r., obejmujących usuwanie zgłoszonych awarii i usterek dla sprzętu oraz oprogramowania Zamawiającego, a w razie konieczności jego wymianę

W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

W przypadku awarii wymiana lub udostępnienie sprzętu zastępczego najpóźniej następnego dnia roboczego, na czas trwania naprawy. Dostarczone urządzenie zastępcze musi posiadać konfiguracje zgodną z zabranym urządzeniem. Zamawiający zobowiązuje się do udostepnienia konfiguracji urządzenia na czas awarii. Ponadto urządzenie zastępcze musi być uruchomione i przetestowane w siedzibie Zamawiającego. Urządzenie zastępcze zostanie dostarczone za pośrednictwem kuriera lub dedykowanym transportem w trybie 24x7 na koszt Wykonawcy.

Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Dostęp do usługi serwisowej powinien być świadczony przez dedykowaną infolinię (należy podać numer telefonu) oraz przez dedykowany moduł internetowy (należy podać adres).

Usługa ta ma być świadczona prze podmiot posiadający certyfikat ISO 9001 w zakresie świadczenia usług serwisowych

3.2. Opis parametrów technicznych zabezpieczenia sieciowego typu firewall.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall musi zapewniać funkcję synchronizacji sesji.
2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej – min. 2 urządzenia w klastrze.
3. System musi posiadać monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
4. System musi posiadać monitoring stanu realizowanych połączeń VPN.
5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP oraz tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie (dla pojedynczego urządzenia):

1. System realizujący funkcję Firewall musi dysponować co najmniej poniższą liczbą i rodzajem interfejsów:
   - 10 portami Gigabit Ethernet RJ-45.
   - 4 gniazdami SFP 1 Gbps.

- 8 gniazdami SFP+ 10 Gbps.

2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.
3. System Firewall musi pozwalać skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie 2xAC.

Parametry wydajnościowe (dla pojedynczego urządzenia):

1. W zakresie Firewall'a obsługa nie mniej niż 11 mln jednoczesnych połączeń oraz 400 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 39 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 25 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 36 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 9 Gbps.
6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 6 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 7 Gbps.

Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.
13. Rozwiązanie musi posiadać wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień

do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall musi uwzględniać: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi realizować translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.
5. Polityka firewall musi umożliwiać filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS).
   - Microsoft Azure.
   - Cisco ACI.
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware NSX.
   - Kubernetes.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19, 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
   - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.

- Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
- Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
- Mechanizm „Split tunneling" dla połączeń Client-to-Site.

2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
3. Producent rozwiązania musi posiadać w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn musi być dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie musi zapewniać obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System musi umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN musi wspierać zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System musi posiadać możliwość określania pasma dla poszczególnych aplikacji.
3. System musi pozwalać zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy musi zapewniać skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.

3. W przypadku archiwów zagnieżdżonych musi istnieć możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.
4. System musi umożliwiać blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej.
8. System musi zapewniać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS musi opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System musi chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków musi zawierać minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi posiadać możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji musi zawierać minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) muszą być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur musi zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi posiadać możliwość definiowania wyjątków oraz własnych sygnatur.
6. Możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System musi posiadać możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW dostępne musza być kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem np.: Hazard.
4. Administrator musi posiadać możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW musi umożliwiać statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW musi mieć możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – musi przeciwdziałać pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System musi pozwalać określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. System musi posiadać możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego.
3. System musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.

4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Musi Istnieć możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System musi dawać możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

1. Elementy systemu bezpieczeństwa muszą posiadać logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall musi zapewniać przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto musi zapewniać możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System musi zapewniać możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów musi być możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku

parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni.

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

- Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android),

- Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen.

3.3. Opis parametrów technicznych centralnego systemu analizy i logowania.

Interfejsy, Dysk:

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 10 TB.

Parametry wydajnościowe:

1. System musi być w stanie przyjmować minimum 5 GB logów na dzień.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

Logowanie

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:

a. Listę najczęściej wykrywanych ataków.

b. Listę najbardziej aktywnych użytkowników.

c. Listę najczęściej wykorzystywanych aplikacji.

d. Listę najczęściej odwiedzanych stron www.

e. Listę krajów , do których nawiązywane są połączenia.

f. Listę najczęściej wykorzystywanych polityk Firewall.

g. Informacje o realizowanych połączeniach IPSec.

4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

Raportowanie

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

Korelacja logów

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
   - Malware.
   - Aplikacje sieciowe.
   - Email.
   - IPS.
   - Traffic.
   - Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.
4. Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie.

Zarządzanie

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.

a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.

2. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

Serwisy i licencje

1. Wsparcie: System musi być objęty serwisem producenta min do dnia 30.06.2026r, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

3.3. Ochrona poczty.

Parametry fizyczne systemu antyspamowego

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 1 TB.

Ogólne funkcje systemu ochrony poczty

Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:

1. Wsparcie dla co najmniej 20 domen pocztowych.
2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 25 tys. wiadomości/godzinę.
3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie.
7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
11. Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.
12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail.
13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.

16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
17. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.

Kontrola antywirusowa i ochrona przed malware

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Skanowanie antywirusowe wiadomości SMTP.
2. Kwarantannę dla zainfekowanych plików.
3. Skanowanie załączników skompresowanych.
4. Definiowanie komunikatów powiadomień w języku polskim.
5. Blokowanie załączników w oparciu o typ pliku.
6. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej.
7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.
8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
9. Ochronę typu wirus outbrake.
10. Ochronę przed zagrożeniami zawartymi wiadomościach pocztowych i w załącznikach (nie mniej niż: pliki MS Office, PDF, HTML, tekstowe) poprzez usuwanie treści będących zagrożeniem (makra, adresy URL zagnieżdżone w plikach, skrypty, ActiveX) i dostarczaniem oczyszczonych w ten sposób wiadomości.

Kontrola antyspamowa

System musi zapewniać poniższe funkcje i metody filtrowania spamu:

1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
3. Szczegółowa kontrola nagłówka wiadomości.
4. Analiza Heurystyczna.
5. Współpraca z zewnętrznymi serwerami RBL, SURBL.
6. Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.
7. Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników.
8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
9. Kontrola w oparciu o Greylisting oraz SPF.
10. Filtrowanie treści wiadomości i załączników.
11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
12. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej.
13. Ochrona typu outbrake.
14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).

15. Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata.
16. Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level)
17. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.

Ochrona przed atakami na usługę poczty

System musi zapewniać poniższe funkcje i metody filtrowania:

1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing).
2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
5. Weryfikacja poprawności adresu e-mail nadawcy.

Funkcje logowania i raportowania

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Logowanie do zewnętrznego serwera SYSLOG.
2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.
4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.
5. Możliwość analizy przebiegu sesji SMTP.
6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.

Funkcje pracy w trybie wysokiej dostępności (HA)

System ochrony poczty musi zapewniać poniższe funkcje:

1. Konfigurację HA w każdym z trybów: gateway, transparent.
2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.
3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
4. Monitorowanie stanu pracy klastra.

Aktualizacje sygnatur, dostęp do bazy spamu

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.
2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.

Zarządzanie

System ochrony poczty musi zapewniać poniższe funkcje:

1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
3. Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.

Certyfikaty

Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji:

1. VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified.

Serwisy i licencje

System musi być dostarczony w modelu „na własność" tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

1. Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake, Sandbox w chmurze, ochrona typu Click Protect, Content Disarm & Reconstruction, Business Email Compromise min. do dnia 30.06.2026.