ZAŁĄCZNIK NR 2 DO SWZ **nr postępowania SPZOZ/TP/19/2022**

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

ZAKUP I WDROŻENIE SYSTEMÓW DLA POPRAWY CYBERBEZPIECZEŃSTWA W SAMODZIELNYM PUBLICZNYM ZESPOLE OPIEKI ZDROWOTNEJ W SANOKU

ZAWARTOŚĆ:

Pakiet nr 1. Dostawa i wdrożenie platformy do zarządzania bezpieczeństwem (systemy typu SIEM i SOAR) wraz z jej wdrożeniem

I. Wymagania funkcjonalne dla systemu

1. System musi zawierać narzędzia do zautomatyzowanego tworzenia elektronicznej, interaktywnej dokumentacji infrastruktury teleinformatycznej uwzględniając schematy architektury zabezpieczeń sieci tzn. mapy pokazującej urządzenia zabezpieczeń, strefy bezpieczeństwa, zasoby teleinformatyczne, połączenia i topologię sieci LAN/WAN), prezentującej informacje nt. bezpieczeństwa w ujęciu technicznym oraz w odniesieniu do procesów działania organizacji.
2. System musi zawierać bazę wiedzy eksperckiej (tzw. Knowledge Base) uwzględniającej wiedzę, która pozwoli ocenić poprawność projektu zabezpieczeń, identyfikując efektywność zastosowanych mechanizmów sieciowych oraz lokalnych w stosunku do potencjalnych wektorów ataków oraz w przypadku ich niezastosowania zidentyfikować ryzyka, które się z tym wiążą.
3. Dostarczone rozwiązanie musi być systemem klasy SIEM (Security Information Event Management), do którego głównych funkcji należą gromadzenie i korelacja zdarzeń przesyłanych lub pobieranych z innych systemów lub urządzeń. Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł, agregację i wzbogacanie danych. Korelacja odbywa się na podstawie zdefiniowanych reguł określających te zależności.
4. Dostarczone rozwiązanie musi być systemem klasy SOAR (Security Orchestration, Automation And Response). Moduł obsługi incydentów może stanowić integralną część systemu SIEM lub być dostarczony w ramach odrębnego, zintegrowanego z systemem SIEM, rozwiązania.
5. Interfejs systemu elektronicznej dokumentacji musi umożliwiać wizualizację informacji o infrastrukturze teleinformatycznej. Wizualizacja musi obejmować interaktywną mapę logiczną sieci z zaznaczonymi strefami sieci, strefami bezpieczeństwa, urządzeniami sieciowymi, połączeniami, systemami zabezpieczeń IT oraz procesami.
6. System musi umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji infrastruktury IT również w formie tabelarycznej.
7. System musi prezentować techniczne informacje nt. bezpieczeństwa IT z perspektywy działalności organizacji, w tym zapisywanie, wyszukiwanie i prezentowanie co najmniej następujących informacji: procesy biznesowe organizacji oraz wspierające je usługi i powiązane z nimi zasoby IT, klasyfikacja zbiorów informacji przetwarzanych w ramach wskazanych procesów oraz przez wskazane zasoby IT, ważność zasobów IT dla organizacji ze względu na typ przetwarzanych danych oraz wspierane procesy, właścicieli zasobów oraz zespół IT odpowiedzialny za jego obsługę.
8. System musi umożliwiać generowanie elektronicznej dokumentacji sieci i systemów w sposób automatyczny (minimum na podstawie danych pozyskanych z logów oraz poprzez API) lub za pomocą interfejsu graficznego i tabelarycznego.
9. Interfejs interaktywnej mapy sieci musi umożliwiać wyświetlanie i modyfikowanie szczegółowych informacji o każdym elemencie infrastruktury IT oraz posiadać mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT, który został zdefiniowany w elektronicznej dokumentacji.
10. System musi pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci.

11. System musi pozwalać na dodawanie i przechowywanie załączników powiązanych z obiektami zgromadzonymi w bazie elektronicznej dokumentacji sieci. System powinien akceptować załączniki między innymi w formatach: pdf, doc, xls, jpg, png.
12. Dla zdarzeń zawierających adresy IP interfejs musi umożliwiać wyświetlenie dodatkowych informacji o zasobach powiązanych z tymi adresami m.in.: nazwa zasobu, rodzaj zasobu, powiązane usługi, właściciel zasobu, podatności zasobu, powiązane incydenty, lokalizacja.
13. 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.
14. Dla zarejestrowanych zdarzeń/incydentów system automatycznie wyznaczy ścieżkę ataku i zaprezentuje ją w formie graficznej na schemacie sieci organizacji. Ścieżka ataku pokazuje wszystkie urządzenia zabezpieczeń na drodze pomiędzy celem a źródłem zdarzenia lub incydentu.
15. Dla zdarzeń zawierających adresy IP interfejs musi umożliwiać wyświetlenie dodatkowych informacji o zasobach powiązanych z tymi adresami m.in.: nazwa zasobu, rodzaj zasobu, powiązane usługi, właściciel zasobu, powiązane incydenty, lokalizacja.
16. Informacje o procesach muszą uwzględniać ważność procesów dla organizacji, typy danych przetwarzanych w ramach procesów (np. dane osobowe, informacje poufne itp.), właścicieli procesów, relacje między procesami (np. proces A zależy od procesu B, przy czym zależności powinny być prezentowane w formie graficznej) oraz czas trwania procesów (np. proces praca biurowa w organizacji jest aktywny od poniedziałku do piątku od 8:00 do 16:00).
17. Mechanizmy modułu dokumentacji elektronicznej muszą umożliwiać powiązanie danych o zasobach z informacjami pozyskanymi w rezultacie skanowania podatności.
18. 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).
19. W ramach obsługi zdarzeń/incydentów/podatności system powinien prezentować informacje o wynikach szacowania ryzyka dla zasobów związanych z incydentem oraz ocenę wpływu incydentu na organizację w przypadku materializacji zagrożenia.
20. System musi pozwalać na zautomatyzowane szacowanie ryzyka dla wszystkich systemów IT zdefiniowanych w elektronicznej dokumentacji. Szacowanie ryzyka powinno odbywać się względem zagrożeń natury informatycznej, np. przełamanie zabezpieczeń, wyciek danych, infekcja złośliwym programem, podsłuch sieciowy.
21. System w razie wykrycia incydentów o wysokim ryzyku materializacji zagrożenia natury technicznej (m.in. przełamanie zabezpieczeń, infekcja złośliwym oprogramowaniem) umożliwi automatyczne powiadamianie o incydencie wskazanych pracowników, m.in. za pomocą email i SMS.
22. System w razie wykrycia incydentów o poważnych konsekwencjach dla organizacji umożliwi automatyczne powiadamianie o incydencie wskazanych pracowników, m.in. za pomocą email i SMS.
23. System powinien umożliwiać automatyczne wyszukiwanie pojedynczych, potencjalnych punktów awarii sieci i systemów IT, których uszkodzenie może spowodować zablokowanie krytycznych usług w organizacji.
24. System ma posiadać narzędzia do modelowania zagrożeń, umożliwiając symulowanie potencjalnych scenariuszy bezpieczeństwa. Interfejs mapy sieci musi pozwalać m.in. na:

- wyznaczenie źródła zagrożenia zasobu teleinformatycznego wraz z wynikiem analizy ryzyka dla tego zagrożenia wyliczanym w sposób automatyczny,
- wyświetlanie zabezpieczeń zasobu teleinformatycznego przed potencjalnymi źródłami zagrożenia,
- wyświetlanie zabezpieczeń chroniących zasoby teleinformatyczne przed określonym źródłem zagrożenia,
- wyświetlanie lokalizacji zasobów określonego rodzaju,
- wyświetlanie najbardziej narażonych zasobów teleinformatycznych,
- wyświetlanie ważnych zasobów teleinformatycznych narażonych na awarie.

25. System musi umożliwiać uwzględnianie danych zgromadzonych w elektronicznej dokumentacji infrastruktury teleinformatycznej w mechanizmach korelacji zdarzeń. Wykryte zdarzenia/ incydenty będą priorytetyzowane w odniesieniu do ważności dla organizacji zasobów, których dotyczą (np. wspomaganych procesów, przetwarzanych informacji klasyfikowanych).
26. Rozwiązanie musi umożliwić korelację zdarzeń pochodzących z różnych urządzeń, punktów końcowych i aplikacji z anomaliami wykrywanymi w przepływach sieciowych oraz podatności pozyskanych bezpośrednio ze skanerów aplikacyjnych i bazy CVE.
27. System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.
28. System musi umożliwiać wykorzystanie baz reputacyjnych w regułach korelacyjnych.
29. System musi umożliwiać automatyczne dodawanie i usuwanie list referencyjnych na podstawie reguł korelacyjnych umożliwiających zdefiniowanie warunków na podstawie których listy te będą modyfikowane. System musi umożliwiać definiowanie list referencyjnych łączących unikalne wartości w pojedynczym wierszu np. login, adres IP, aplikacja.
30. System musi być wyposażony w mechanizmy reguł opartych na mechanizmach behawioralnych z możliwością agregacji danych oraz punktowania poszczególnych zdarzeń w wyznaczonych oknach czasowych. W rezultacie działania reguł behawioralnych, system powinien tworzyć incydenty związane z przekroczeniem dozwolonych zakresów punktacji dla zdarzeń zaobserwowanych w oknie czasowym agregacji.
31. System musi umożliwiać uwzględnianie danych zgromadzonych w elektronicznej dokumentacji infrastruktury teleinformatycznej w scenariuszach obsługi incydentów. Scenariusze obsługi incydentów muszą być uzależnione od ważności dla organizacji zasobów, których dotyczą (np. wspomaganych procesów, przetwarzanych informacji klasyfikowanych).
32. System musi umożliwiać wykorzystanie baz reputacyjnych w ramach scenariuszy obsługi incydentów.
33. System musi zapewnić graficzny interfejs wspierający proces obsługi incydentów, którego zadaniem będzie wspieranie użytkownika w realizacji zadań związanych z selekcją zdarzeń, analizą incydentów, oceną wpływu i reakcją na incydenty. Do zadań tych należą między innymi:
    - wzbogacanie danych kontekstowych,
    - gromadzenie artefaktów danych związanych z incydentem,
    - wykonywanie czynności związanych z reakcją na incydent,
    - raportowanie przebiegu incydentu.
34. System musi być wyposażony w graficzny interfejs prezentujący w formie wykresów dane statystyczne związane z procesem obsługi incydentów/podatności. Wykresy muszą umożliwiać prezentację danych uwzględniających co najmniej: ilość incydentów w czasie w podziale na priorytety, czasy reakcji i obsługi oraz bieżące ilości incydentów obsługiwanych przez poszczególnych użytkowników.
35. System powinien posiadać zestaw predefiniowanych scenariuszy obsługi.

36. System musi pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących.
37. System powinien pozwalać na przekazywanie aktywnych linków pomiędzy zintegrowanymi systemami, a otwarcie linku powinno bezpośrednio przekierowywać operatora do konsoli systemu zewnętrznego.
38. System powinien umożliwiać automatyczną zmianę statusu incydentu na podstawie informacji pobranych z innych systemów np. identyfikacja wskaźników kompromitacji systemu (IoC).
39. System musi umożliwiać zbieranie, przechowywanie i przypisywanie wskaźników kompromitacji (IoC) do incydentów.
40. System powinien udostępniać automatyczny raport z wszystkich podjętych działań w ramach incydentu.
41. System musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych danych przez ich podział na pola, na podstawie których może odbywać się dalsze przetwarzanie oraz wyszukiwanie danych. Mechanizm musi umożliwiać m.in. parsowanie warunkowe, parsowanie hierarchiczne, wzbogacanie zdarzeń o dodatkowe pola, mapowanie wartości, czy wykorzystanie gotowych parserów przy tworzeniu nowych.
42. Parsowanie warunkowe i hierarchiczne musi być konfigurowalne i obsługiwać następujące metody normalizacji: REGEX, JSON, XML, CEF, LEEF, SYSLOG. Musi umożliwiać wykorzystanie gotowych parserów jako elementów podrzędnych hierarchii oraz wykorzystywanie ich w warunkach.
43. Proces normalizacji musi odbywać się na bieżąco na etapie rejestrowania danych w systemie.
44. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, np. dzięki zmianie wartości tych pól oraz wzbogacaniu tych danych o dodatkowe pola bazując na całych wartościach lub wzorcach wyszukiwania.
45. System musi zapewnić normalizację (parsowanie) logów protokołami Syslog, TLS Syslog, Netflow, obsługiwać pliki płaskie (ang. flat file), zapytania do bazy danych poprzez sterownik ODBC oraz odbierać wiadomości email.
46. Oferowane rozwiązanie powinno zapewniać możliwość zbierania logów z systemów Microsoft Windows poprzez mechanizm Windows Event Forwarding (WEF) bez konieczności instalowania dedykowanego oprogramowania w tych systemach.
47. Normalizacja logów musi posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól o nazwę lub kod kraju korzystając z wbudowanej w produkt bazy.
48. Normalizacja musi uwzględniać możliwość nadawania kategorii zdarzeń na podstawie wartości parsowanych pól, np. logowanie, wylogowanie, zmiana uprawnień, malware, vulnerability.
49. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych.
50. System musi posiadać predefiniowany zestaw parserów.
51. System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) logów z niestandardowych źródeł danych, w oparciu o składnię wyrażeń regularnych oraz formaty JSON, XML, CIS, LEEF, Syslog. System musi umożliwiać zastosowanie wszystkich typów składni dla pojedynczego zdarzenia.
52. System w swoim działaniu musi korzystać z wbudowanych algorytmów uczenia maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników i komputerów.
53. System musi umożliwiać definiowanie zakresu i czasu uczenia, np. analiza logowania użytkowników po godzinach pracy, analiza alarmów systemu SIEM. Po wdrożeniu nie będzie wymagane żadne dostrojenie systemu.
54. System musi mieć możliwość wzbogacania kontekstu odbiegającego od normalnego zachowania użytkownika korzystając z danych zewnętrznych, minimum: Threat Intelligence, Active Directory. Przykładowe zastosowanie integracji zakłada wykorzystanie zasobów zewnętrznych, z których dane mogą podnieść skumulowaną ocenę ryzyka dla sesji użytkownika.

55. System musi posiadać funkcję „automatycznej korelacji”, tzn. posiadać zaszyte mechanizmy i reguły korelacji, które po wdrożeniu i „nauce środowiska zamawiającego”, będą przedstawiać właściwe incydenty dla operatorów bez dodatkowej ingerencji w reguły.
56. System musi zapewniać możliwość budowania modeli zachowania użytkowników dla zebranych danych historycznych ze skonfigurowanego (wskazanego) okresu.
57. System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych.
58. Dostarczone rozwiązanie musi być objęte wsparciem producenta lub producentów. Wsparcie musi obejmować bezpłatne dostarczanie aktualizacji oprogramowania, reagowanie na zgłaszane błędy systemowe, oraz opiekę dedykowanego konsultanta technicznego. 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).
59. Rozwiązania SIEM, SOAR, narzędzia elektronicznej dokumentacji, narzędzie analizy ryzyka cyberzagrożeń oraz baza wiedzy mogą być dostarczone w ramach odrębnych rozwiązań, jednakże muszą być zintegrowane w sposób umożliwiający spełnienie wszystkich wymagań z poziomu jednej konsoli. Dostarczone rozwiązanie/rozwiązania, za wyjątkiem skanera podatności, nie mogą działać w oparciu o technologię typu open-source.
60. Interfejs użytkownika Systemu musi być w języku polskim. Musi być przejrzysty i konfigurowalny, poprzez pogrupowanie zawartości w bloki tematyczne, co ma umożliwić łatwe i szybkie wyszukiwanie odpowiednich danych.
61. Funkcjonowanie rozwiązania musi być oparte w całości o architekturę „on-premise”, w której przetwarzane dane nie są przesyłane poza infrastrukturę Zamawiającego.
62. System musi umożliwiać instalację na platformach systemowych Microsoft Windows (minimum Server 2016), Redhat/Oracle Linux (minimum 7.x).
63. Dopuszczalne jest dostarczenie rozwiązania jako tzw. virtual appliance pod warunkiem, że obraz appliance jest udostępniany do pobrania przez producenta dostarczonego rozwiązania na jego oficjalnej stronie internetowej w postaci utwardzonego rozwiązania, łącznie z dedykowanym systemem operacyjnym, dla którego producent regularnie dostarcza aktualizacje, w tym poprawki bezpieczeństwa.
64. System musi zapewniać możliwość współpracy z popularnymi bazami danych, a w tym co najmniej z MS SQL lub Oracle.
65. System powinien umożliwiać nadawanie uprawnień do obiektów/modułów systemu dla poszczególnych operatorów lub grup operatorów.
66. System musi zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role.
67. System musi dokonywać automatycznej integracji z usługą katalogową Microsoft Active Directory celem pobrania informacji o poświadczeniach i zasobach zarejestrowanych w domenie AD. Minimum to: nazwa użytkownika, login, e-mail, nazwa komputera, przynależność do grup, przełożonego, jednostkę organizacyjną oraz konta uprzywilejowane.
68. System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać możliwość jej synchronizacji z usługą katalogową Microsoft Active Directory.
69. Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień do definiowalnych grup odbiorców (co najmniej: powiadamianie email oraz SMS, opcjonalnie czat).
70. System musi być dostępny z poziomu dedykowanego klienta aplikacji lub obsługiwany za pomocą dowolnej przeglądarki internetowej (Chrome, Edge, Firefox), bez konieczności instalowania jakichkolwiek dodatków dla prawidłowego jego działania.
71. System musi umożliwiać przypisanie poziomów krytyczności do monitorowanych zasobów, które będą brane pod uwagę w ewaluacji zagrożeń.

72. System musi umożliwiać mapowanie zdarzeń korelacyjnych na framework Mitre ATT&CK.
73. System musi być wyposażony w graficzny interfejs umożliwiający przeglądanie i przeszukiwanie zarejestrowanych danych w formie znormalizowanej i pierwotnej. Interfejs musi prezentować wyniki wyszukiwania z zastosowaniem filtrów opartych na wartościach pól, złożonych wyrażeniach logicznych, wskazaniach zakresu czasowego i źródła danych. Interfejs wyszukiwania musi umożliwiać zapisywanie zapytań z możliwością ich ponownego wykorzystania w przyszłości. Tworzenie zapytań musi być możliwe poprzez bezpośrednie wskazanie pola zdarzenia za pomocą wskaźnika myszy i dodanie tego pola do filtra wyszukiwania, wraz z określeniem warunków wyszukiwania przez wyrażenie logiczne.
74. Tworzenie raportów PDF musi posiadać opcje automatycznego harmonogramu, który w zadanym wcześniej momencie pozwoli na wysyłkę utworzonego raportu do zdefiniowanych odbiorców poczty email. Konfiguracja harmonogramu tworzenia raportów PDF i ich wysyłki powinna być dostępna poprzez graficzny interfejs użytkownika.
75. System musi rejestrować i przechowywać pozyskane dane w wersji pierwotnej oraz w wersji znormalizowanej.
76. System musi zapewniać klasyfikację zdarzeń za pomocą notacji punktowej definiującej ich poziom zagrożenia (ryzyko).
77. Interfejs systemu powinien umożliwiać z poziomu jednego okna widoku weryfikację wszystkich działań użytkownika na osi czasu, które spowodowały wzrost ryzyka. Z poziomu tego widoku system umożliwi przejście do opisu konkretnego zdarzenia.
78. System powinien w formie graficznej prezentować podsumowanie aktualnego stanu bezpieczeństwa, m.in. usługi zagrożone przez incydenty oraz podatności, średni czas obsługi incydentu lub podatności.
79. System pozwoli na prezentację danych w postaci tzw. „Dashboard", tj. dostosuje zakres i prezentacje danych do potrzeb administratora czy też zalogowanego użytkownika.
80. System musi automatycznie wyodrębnić konta użytkowników oraz ich kontekst, minimum przynależność do odpowiednich grup domenowych, konta serwisowe, użytkowników uprzywilejowanych, użytkowników w randze kierowniczej i zarejestrowane stacje robocze celem automatycznej dystrybucji tych danych do odpowiednich narzędzi systemu.
81. System musi umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach.
82. System musi umożliwiać przechowywanie katalogu incydentów zawierających dowody, próbki, logi oraz inne powiązane z danym incydentem informacje.
83. System musi potrafić wczytywać informacje z innych systemów bezpieczeństwa i traktować je, jako elementy/dowody w katalogach incydentów.
84. System musi umożliwiać powiązanie każdego zdarzenia/incydentu z odpowiednim priorytetem (definiowanym automatycznie z możliwością manualnej zmiany).
85. System powinien posiadać możliwość rejestracji zgłoszeń i przekształcenia ich w incydenty bezpieczeństwa z możliwością rozdzielenia uprawnień dla obu tych czynności.
86. System powinien mieć logikę automatycznego przypisywania zgłoszeń, minimum na podstawie dostępności operatora, jego obciążenia, oraz cech zasobu którego dotyczy incydent, minimum typ zasobu (np. serwer lub stacja robocza), krytyczność oraz realizowane z jego udziałem usługi z katalogu usług.
87. System musi umożliwiać grupowanie manualne w jeden incydent bezpieczeństwa zdarzenia podobne/powiązane np. wielokrotnie raportowane, przez systemy źródłowe, wielokrotnie zgłoszone przez użytkowników.

88. System powinien grupować automatycznie w jeden incydent bezpieczeństwa zdarzenia podobne/powiązane np. wielokrotnie raportowane, przez systemy źródłowe, wielokrotnie zgłoszone przez użytkowników.
89. System powinien umożliwiać obsługę tzw. lawinowych incydentów (incydenty takie same, lecz pochodzące od różnych użytkowników lub systemów) poprzez podłączanie ich do jednego głównego incydentu oraz nadanie odpowiedniego priorytetu tego typu zdarzeniom. Zamkniecie głównego incydentu/zdarzenia powinno umożliwiać zamykanie powiązanych z nim incydentów/zdarzeń w trybie manualnym (operator) lub automatycznym (system). W podglądzie incydentu powinna się pojawić informacja o podpiętych incydentach.
90. System musi pozwalać na określenie automatycznych oraz inicjowanych przez operatora reakcji na incydenty bezpieczeństwa i/lub zdarzenia, polegających na integracji z systemami zewnętrznymi w celu uzyskania dodatkowych informacji, dotyczących incydentu/zdarzenia lub podjęcia akcji zapobiegawczych.
91. System musi umożliwiać wykonywanie działań remediacyjnych na stacjach roboczych/serwerach (pobieranie logów, uruchamianie skryptów, weryfikacja rejestrów, itp.).
92. System musi umożliwiać przypisywanie i przekazywanie incydentów do operatorów lub grup operatorów.
93. System musi pozwalać na zbieranie danych i reputacji z systemów klasy FQDN, URL, Hash.
94. System powinien pozwalać, przy użyciu języków skryptowych ogólnie dostępnych (np. Python lub/i PowerShell), na skonfigurowanie nowych, nie uwzględnionych przez producentów rozwiązania możliwości integracyjnych z zewnętrznymi systemami.
95. System powinien umożliwiać przeglądanie listy zasobów (urządzeń, systemów, osób, itp.) pod kątem poziomu i ilości incydentów, które są z nimi powiązane.
96. System musi mieć możliwość automatycznego informowania o zmianie statusu incydentu (minimum: wygenerowaniu, przypisaniu, przekroczeniu czasu SLA oraz zamknięciu karty incydentu).
97. System powinien umożliwiać ustawienie parametrów SLA bazując na ustalonym automatycznie priorytecie zdarzania/incydentu/podatności. System musi dokonywać automatycznego pomiaru tych czasów i weryfikacji ich do zdefinowanych wymagań SLA. Wyniki pomiaru czasu powinny być stale aktualizowane i prezentowane w interfejsie systemu.
98. System powinien umożliwiać dodawanie, modyfikację i usuwanie umów SLA, które zawierają co najmniej następujące parametry: data rozpoczęcia i zakończenia obowiązywania umowy, jednostka organizacyjna (struktura jednostek), której dotyczy umowa, lista usług z katalogu usług, których dotyczy umowa.
99. System musi być zawierać mechanizm integracji ze skanerami podatności co najmniej dwóch producentów oraz co najmniej jednym skanerem podatności dostępnym na zasadach open source. W ramach integracji system musi mieć możliwość uruchamiania skanowania podatności i importowania jego wyników. Silnik skanujący, będący źródłem podatności musi zostać dołączony do oferty. Wykonawca dokona instalacji i konfiguracji skanera podatności dostępnego na zasadzie open source.
100. Interfejs modułu obsługi incydentów musi prezentować listę podatności zasobów związanych z incydentem.
101. System musi automatycznie ustalać priorytety podatności w odniesieniu do ważności podatnych systemów IT dla organizacji oraz oceny technicznej zagrożenia bazującej na wartości CVSS lub wartości pozyskanej bezpośrednio z silnika skanera.
102. System powinien uwzględniać w ocenie zdarzeń i incydentów, informacje o podatnościach technicznych wykrytych przez narzędzia do zarządzania podatnościami zarówno przez import raportu jak i integrację przez API.

103. System musi zawierać mechanizm definiowania harmonogramów skanowania podatności oraz na ich podstawie automatycznie uruchamiać procesy skanowania i analizowania uzyskanych raportów.
104. System musi umożliwiać obsługę podatności w ramach scenariuszy obsługi.
105. System SIEM oraz wszystkie moduły towarzyszące muszą umożliwiać równoczesną pracę co najmniej 10 operatorów oraz objąć monitoringiem min. 500 zasobów IT. Przez zasób IT rozumie się serwery fizyczne lub serwery wirtualne oraz komputery użytkowników. Ilość danych przekazywanych do systemu, tj. EPS (Events Per Second) oraz ilość kolektorów agregujących i parsujących nie może powodować zmian w zakresie licencjonowania. Wykonawca udzieli Zamawiającemu wieczystej, nieograniczonej czasowo licencji na zakupiony System.
106. System ma gwarantować możliwość elastycznej rozbudowy o dalsze zasoby IT, które w przyszłości zostaną objęte jego działaniem.
107. Zamówienie realizowane będzie w okresie min 61 miesięcy od dnia zawarcia umowy, zgodnie ze wzorem umowy. Wykonanie zamówienia zostanie podzielone na etapy:
    - Etap I – wdrożenie – w terminie do 1 miesiąca od dnia podpisania umowy z Wykonawcą. Szczegółowy zakres i wytyczne Etapu I określa pkt II;
    - Etap II – utrzymanie i wsparcie systemu – w okresie min. 60 miesięcy, od dnia podpisania protokołu odbioru.
108. Po zakończonym wdrożeniu, Wykonawca przeprowadzi dla wskazanych osób i w miejscu wskazanym przez Zamawiającego instruktaż stanowiskowy w zakresie obejmującym wdrożony system. W ramach instruktażu, Wykonawca przekaże uczestnikom pełną wiedzę niezbędną do poprawnego użytkowania systemu SIEM i SOAR oraz urządzeń. Przeprowadzenie instruktaży zostanie potwierdzone protokołami sporządzonymi w dwóch jednobrzmiących egzemplarzach, po jednym dla Zamawiającego i Wykonawcy, zawierającym:
    - zakres instruktażu,
    - datę przeprowadzonego instruktażu,
    - imienną listę osób uczestniczących,
    - imię i nazwisko osób prowadzących instruktaż.
109. Wykonawca przekaże Zamawiającemu wszelkie, niezbędne do poprawnego korzystania z wdrożonego rozwiązania, informacje o specyfice systemu oraz informacje techniczne na temat jego prawidłowej eksploatacji (tj. dokumentację powdrożeniową oraz instrukcję/instrukcje obsługi).

II. Szczegółowy zakres i wytyczne procesu wdrożenia systemu

1. Proces wdrożenia systemu określony w Etapie I powinien zostać zrealizowany zgodnie z opisanymi niżej wytycznymi oraz zatwierdzonym harmonogramem, umożliwiając efektywne wdrożenie rozwiązania w okresie 1 miesiąca.
2. Proces wdrożeniowy podzielony zostanie na obszary:
    - Obszar Analizy, zakładający stworzenie elektronicznej dokumentacji organizacji wraz z podłączeniem i skonfigurowaniem mechanizmów szacowania ryzyka pod kątem kluczowych zasobów IT i procesów organizacji (budowa kontekstu organizacji);
    - Obszar Detekcji, zakładający podłączenie i konfigurację narzędzi odpowiedzialnych za wykrywanie zdarzeń i incydentów bezpieczeństwa w ramach zainstalowania modułu SIEM;
    - Obszar Reakcji, zakładający podłączenie i konfigurację mechanizmów wspomagających proces automatyzacji reakcji na wykryte zdarzenia, incydenty bezpieczeństwa i podatności w ramach zainstalowania modułu SOAR.

3. Obszar Analizy ma na celu identyfikację potencjalnych cyberzagrożeń oraz możliwych konsekwencji na jakie narażona jest organizacja. Zakres prac powinien uwzględniać kolejno:
   - Pracę z konsultantem (w zakresie m.in. wprowadzenia do metodyki, uzupełnienia ankiety przedwdrożeniowej oraz przygotowania i zatwierdzenia harmonogramu prac);
   - Uruchomienie systemu w infrastrukturze zamawiającego, w tym:
     - konsultacje w przygotowaniu infrastruktury Zamawiającego do instalacji systemu,
     - przygotowanie przez Zamawiającego połączenia zdalnego,
     - instalację lub import maszyny wirtualnej typu „software appliance",
     - aktywację licencji,
     - konfigurację systemów,
     - import/wprowadzenie tabeli adresacji znaczących stref bezpieczeństwa, wymaganych przez mechanizmy wykrywania (np. sieci serwerów, sieci DMZ, sieci LAN);
   - Podłączenie głównego źródła zdarzeń opisującego komunikację sieciową, w tym:
     - przekierowanie logów opisujących transmisje sieciową (traffic) z zapór sieciowych (Firewall) na kolektor systemu,
     - uruchomienie reguł wykrywania;
   - Prace audytowe, w tym:
     - pasywną analizę transmisji sieciowej:
       - ruch z/do serwerów webowych i aplikacyjnych,
       - ruch z/do serwerów baz danych,
       - ruch z/do serwerów pocztowych,
       - ruch z/do kontrolerów domenowych,
       - ruch z/do serwerów usług podstawowych (m.in. DNS/NTP),
       - ruch z/do zasobów zidentyfikowanych na bazie charakterystyki i wolumenu ruchu oraz możliwości identyfikacji aplikacji,
     - konsultacje w ramach otrzymanych wyników;
     - zebranie danych audytowych wymaganych do sporządzenia raportu;
   - Analizę podatności, w zakresie:
     - integracji po API ze wskazanym przez zamawiającego komercyjnym skanerem/ skanerami podatności lub zainstalowanie skanera podatności typu open source;
     - przygotowanie reguł priorytetów i importu krytycznych podatności;
   - Przygotowanie dynamicznego raportu audytowego w oparciu o dostępne w systemie narzędzia elektronicznej dokumentacji i szacowania ryzyka obejmującego analizę prawdopodobieństwa przełamania zabezpieczeń organizacji. Raport powinien zawierać:
     - zidentyfikowane zagrożenia oraz prawdopodobieństwo ich wystąpienia;
     - potencjalne wektory ataków dla wykrytych zagrożeń;
     - wizualizacja graficzna wykrytych źródeł zagrożeń oraz wektorów ataków;
     - rekomendacja zabezpieczeń;
     - zidentyfikowane zagrożenia związane z podatnościami oraz prawdopodobieństwo wykorzystania ich do przełamania zabezpieczeń;
4. Obszar Detekcji ma na celu uruchomienie i dostrojenie mechanizmów wykrywania zagrożeń. Zakres prac powinien uwzględniać kolejno:
   - Podłączenie (przekierowanie przez Zamawiającego do systemu) źródeł zdarzeń i ich dalszą konfigurację w systemie. Kluczowe źródła zdarzeń obejmują:
     - zapory sieciowe w punkach styku z siecią Internet (Firewall brzegowy);
     - sieciowe systemy bezpieczeństwa dedykowane do wykrywania incydentów bezpieczeństwa (np. Sandbox, IDP/IPS, AntySpam);

- centralne systemy, dedykowane do kontroli złośliwego oprogramowania na stacjach końcowych/Serwerach, umożliwiające wykrywanie aktywności złośliwego oprogramowania (np. AntyWirus, EDR);
- kontroler domenowy oraz system zarządzania dostępem uprzywilejowanym;
- systemy detekcji anomalii w przepływach lub zdarzeniach (np. NBA);
- system SIEM;
- źródła, muszą zostać powiązane z parserami, pozwalającymi na detekcję zgodną z wbudowanymi w system regułami korelacji;

- Adaptację reguł profilowych, pozwalających na dostosowanie zdarzeń do zasobów, których dotyczą;
- Podłączenie reguł detekcji;
- Podłączenie i konfiguracja mechanizmów UEBA:
  - integracja z Active Directory,
  - adaptacja profili użytkowników UBA,
  - adaptacja profili hostów EBA,
  - import reguł bezpieczeństwa UEBA, uruchomienie procesu uczenia.

5. Obszar Reakcji ma na celu uruchomienie i dostrojenie mechanizmów automatyzacji w działaniach reagowania na wykryte zagrożenia bezpieczeństwa. Zakres prac powinien uwzględniać:
   - import gotowych scenariuszy obsługi,
   - konfigurację zespołów obsługi, celem właściwej adresacji podatności oraz zdarzeń wymagających obsługi,
   - konfigurację mechanizmów powiadamiania.

III. Opis rozwiązania i konfiguracji systemu

1. Producent oferowanego rozwiązania musi być obecny na rynku od co najmniej 5 lat.
2. Wykonawca musi dostarczyć, zainstalować, skonfigurować oraz uruchomić kompletne rozwiązanie wraz ze wszystkimi niezbędnymi podzespołami, osprzętem, przewodami, oprogramowaniem i dokumentacją. Jeżeli do uzyskania wymaganych parametrów i funkcjonalności potrzebne są dodatkowe licencje, to Wykonawca musi je dostarczyć. Zamawiający nie może ponosić dodatkowych kosztów z wykorzystaniem całej funkcjonalności na niezmienionym poziomie przez cały okres użytkowania. Wszystkie dostarczone licencje muszą być bezterminowe.
3. Przedmiot zamówienia musi być dostarczany, wdrożony i zainstalowany w całości w siedzibie Zamawiającego, w wyznaczonych przez niego lokalizacjach i punktach (w sposób umożliwiający ich prawidłową wentylację).
4. Oferowany sprzęt nie może być na liście produktów, dla których wsparcie Producenta zostanie zakończone w ciągu najbliższych 24 miesięcy.
5. Wykonawca dostarczy licencje na niezbędne do działania systemu silnik bazy danych oraz systemy operacyjne. Wykonawca odpowiada za właściwe sparametryzowanie zarówno systemu operacyjnego jak i silnika bazy danych.
6. Oferowane rozwiązanie musi być produktem gotowym, posiadającym na moment składania oferty wszystkie wymagane przez Zamawiającego funkcjonalności. Do oferty należy załączyć listę wszystkich komponentów urządzenia / systemu. Lista musi zawierać co najmniej nazwy urządzeń, modeli oraz inne informacje pozwalające w sposób jednoznaczny zidentyfikować poszczególne komponenty sprzętowe i programowe.

7. Oferowane urządzenia i wszystkie jego elementy składowe muszą pochodzić od autoryzowanego Dostawcy producenta i być fabrycznie nowe oraz objęte gwarancją producenta.
8. Wraz z rozwiązaniem musi być dostarczony komplet dokumentacji producenta w formie papierowej lub elektronicznej. Dokumentacja papierowa powinna być czytelna. Zamawiający dopuszcza dostawę dokumentacji producenta rozwiązania w językach polskim lub angielskim.
9. Wykonawca oświadcza, że podczas realizacji Umowy, a także podczas korzystania z systemu w zakresie i na zasadach opisanych Umową, Zamawiający nie będzie zobowiązany do nabywania żadnych usług ani uprawnień innych niż wyraźnie zdefiniowane Umową. W szczególności zobowiązanie Wykonawcy oznacza, że nie jest konieczne nabycie przez Zamawiającego żadnych dodatkowych licencji ani uprawnień poza opisanymi Umową, w tym w szczególności związanych z korzystaniem z infrastruktury technicznej, i objętych wynagrodzeniem, a korzystanie z systemu nie spowoduje konieczności nabycia takich licencji lub uprawnień. Wszelkie ryzyka związane z szacowaniem ilości potrzebnych licencji lub innych uprawnień koniecznych do korzystania z systemu zgodnie z Umową obciążają Wykonawcę.
10. Warunki gwarancyjne dotyczące dostarczonego sprzętu:
    - min. 3 lata gwarancji producenta czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia,
    - możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta lub dedykowaną do tego celu platformę elektroniczną.

IV. Wsparcie

Wykonawca przedstawi koszt pakietu 1 z podziałem na:
1. Dostarczenie, wdrożenie, konfigurację, instruktaże stanowiskowe oraz licencje na oferowane oprogramowanie.
2. Wsparcie techniczne.

W ramach wsparcia Wykonawca zapewnia:
1. Udostępnienie poprawek do wdrożonego oprogramowania, w przypadku stwierdzenia przez Zamawiającego błędnego działania.
2. Zgłoszenie nieprawidłowości przez Zamawiającego odbywać się będzie poprzez: witrynę internetową Wykonawcy, poprzez kontakt e-mail lub telefonicznie.
3. Wprowadzanie zmian oraz nowych funkcjonalności we wdrożonym oprogramowaniu. Wykonawca jest zobowiązany do przekazania Zamawiającemu informacji o nowych wersjach oprogramowania.

Pakiet nr 2. Zakup oprogramowania antywirusowego centralnie zarządzanego, klasy EDR

I. Wymagania ogólne

Wykonawca dostarczy oprogramowanie o poniżej wymienionych parametrach funkcjonalnych z licencją na 500 stanowisk na okres min. 36 miesięcy.

II. Obsługiwane systemy

1. System operacyjny Windows
   - Systemy operacyjne komputerów (pełne wsparcie)
     - Windows 11,
     - Windows 10,
     - Windows 8.1,
     - Windows 8,
     - Windows 7 SP1.
   - Windows Tablet oraz systemy wbudowane (pełne wsparcie)
     - Windows 10 IoT Enterprise,
     - Windows Embedded 8.1 Industry,
     - Windows Embedded 8 Standard,
     - Windows Embedded Standard 7,
     - Windows Embedded Compact 7,
     - Windows Embedded POSReady 7,
     - Windows Embedded Enterprise 7.
   - Systemy operacyjne serwera (pełne wsparcie)
     - Windows Server 2022,
     - Windows Server 2019 Core,
     - Windows Server 2019,
     - Windows Server 2016,
     - Windows Server 2016 Core,
     - Windows Server 2012 R2,
     - Windows Server 2012,
     - Windows Small Business Server (SBS) 2011,
     - Windows Server 2008 R2.
2. Systemy operacyjne Linux
   - RHEL 7.x & 8.x ; 3.10.0-957 - 4.18.0,
   - Oracle Linux 7.x (UEK +RHCK) ; 3.10.0-957 - 4.18.0,
   - Oracle Linux 8.x (UEK +RHCK) ; 3.10.0-957 - 4.18.0,
   - CentOS 7.x ; 3.10.0-957 - 4.18.0,
   - CentOS 8.x ; 3.10.0-957 - 4.18.0,
   - Debian 10 ; 4.19,
   - Debian 11 ; 5.10,
   - Ubuntu 16.04.x ; 4.8 / 4.10 / 4.13 / 4.15,
   - Ubuntu 18.04.x ; 5.0 / 5.3 / 5.4,
   - Ubuntu 20.04.x ; 5.4 / 5.8 / 5.11 / 5.13,
   - SLES 12 SP4 ; 4.12.14-x,

- SLES 12 SP5 ; 4.12.14-x,
- SLES 15 SP1 ; 4.12.14-x,
- SLES 15 SP2 ; 5.3.18-x,
- SLES 15 SP3 ; 5.3.18-x,
- openSUSE Leap 15.2 ; 5.3.18,
- Google COS Milestones 77, 81, 85 ; 4.19.112 / 5.4.49.

3. Systemy Operacyjne Mac OS X
   - macOS Monterey (12.x),
   - macOS Big Sur (11.x),
   - macOS Catalina (10.15),
   - macOS Mojave (10.14),
   - macOS High Sierra (10.13),
   - macOS Sierra (10.12).
4. Ochrona środowisk wirtualnych
   - Możliwość zastosowania zewnętrznego silnika skanującego w postaci maszyny wirtualnej
   - Maszyna wirtualna pełniąca rolę silnika skanującego może być pobrana w formacie:
     - OVA
     - XVA
     - VHD
     - VMDK
   - Środowiska wspierane:
     - VMware vSphere & vCenter Server 7.0 update 1, 7.0, 6.7 update 3, update 2a, update 1, 6.7, 6.5, 6.0, 5.5, 5.1, 5.0,
     - VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x,
     - VMware Workstation 11.x, 10.x, 9.x, 8.0.6,
     - VMware Player 7.x, 6.x, 5.x,
     - Citrix XenServer 8.x, 7.x, 6.5, 6.2, 6.0, 5.6 or 5.5 (including Xen Hypervisor),
     - Citrix Virtual Apps and Desktops 7 1808, 7 1811, 7 1903, 7 1906,
     - Citrix XenApp and XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR,
     - Citrix VDI-in-a-Box 5.x,
     - Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2, 2016, 2019 or Windows Server
     - 2008 R2, 2012, 2012 R2, 2016, 2019 (including Hyper-V Hypervisor),
     - Red Hat Enterprise Virtualization 3.0 (including KVM Hypervisor),
     - Oracle VM 3.0,
     - Oracle VM VirtualBox 5.2, 5.1.

III. Ochrona antywirusowa i antyspyware

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami;
2. Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona w języku polskim;
3. Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi;
4. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.;
5. Wbudowana technologia do ochrony przed rootkitami;
6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików;
7. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie";

8. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym;
9. Możliwość skanowania dysków sieciowych i dysków przenośnych;
10. Skanowanie plików spakowanych i skompresowanych;
11. Możliwość dodawania wykluczeni na podstawie: plik, folder, rozszerzenie, proces, hash pliku, hash certyfikatu, nazwa zagrożenia, wiersz poleceń, IP/maska;
12. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express;
13. Skanowanie i oczyszczanie poczty przychodzącej POP3 "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego);
14. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji;
15. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie;
16. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta;
17. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji;
18. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać;
19. Program umożliwia skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS;
20. Program skanuje ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe;
21. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program będzie pytał o hasło;
22. Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji: „O programie” możliwość zdefiniowania przez administratora danych do pomocy technicznej jak: adres strony pomocy, adres e-mail do administratora ochrony, numer telefonu do administratora ochrony;
23. W GUI programu na punkcie końcowym możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników;
24. W GUI programu możliwość wyświetlenia kiedy była przeprowadzana ostatnia aktualizacja z dokładnością co do dnia i sekundy jej uruchomienia;
25. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń;
26. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy;
27. Praca programu musi być niezauważalna dla użytkownika;
28. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej;
29. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet;
30. Oprogramowanie klienckie posiada wbudowana funkcje do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej;
31. Możliwość odblokowania ustawień programu po wpisaniu hasła;
32. Oprogramowanie posiada możliwość odblokowania ustawień lokalnych konfiguracji po doinstalowaniu odpowiedniego modułu;
33. Wbudowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego interfejsu w komputerze zostanie podłączone urządzenie);

34. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, na podstawie wykrytych urządzeń lub wpisanych ręcznie ID urządzenia lub ID produktu;
35. Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: adresy e-mail, Piny, Konta bankowe, hasła itp.;
36. Funkcja Ochrony danych konfigurowana zdalnie przez administratora;
37. Jedna wersja instalacyjna na stacje robocze i serwery plików Windows;
38. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego;
39. Wbudowany IDS;
40. Możliwość zainstalowania silnika pełnego, lekkiego ze sprawdzaniem reputacji plików w chmurze, lub wykorzystanie dodatkowej maszyny wirtualnej która przejmie rolę silnika skanującego;
41. Maszyna która przejmuję rolę silnika skanującego musi działać w trybach redundancji lub równej dystrybucji;
42. Aktualizacja maszyny skanującej musi obejmować oddzielną aktualizację nowych funkcji, ulepszeń, poprawek oraz oddzielną aktualizację systemu operacyjnego urządzenia wirtualnego;
43. Możliwość tworzenia list sieci zaufanych;
44. Możliwość dezaktywacji funkcji zapory sieciowej.
45. Możliwość ustawienie skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu.
46. Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware
47. Mechanizm który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji
48. Użytkownik na punkcie końcowym ma możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań(konfigurowalne w politykach bezpieczeństwa)
49. Automatyczne zezwolenie na dostęp dla użytkowników Active Directory z grupy security groups
50. Wymuszenie połączenia szyfrowanego dla punktów końcowych Windows oraz Linux do serwera zarządzającego.
51. System zarządzania ryzykiem – Zintegrowany z konsolą zarządzającą system który pozwala oszacować podatność środowiska na atak na podstawie punktów ryzyka. Punkty ryzyka powinny być przydzielane np. od 0 do 100 gdzie liczba mniejsza stanowi mniejsze ryzyko a liczba większa większe ryzyko. System ponadto musi posiadać:
    - Funkcję która pozwala wykrywać błędne konfiguracje oraz naprawiać je lub ignorować z podziałem na typ błędnej konfiguracji:
        - Ochrony przeglądarki internetowej
        - Sieć i poświadczenia
        - Błędna konfiguracja systemu operacyjnego

      System ponadto musi określać nasilenie tych błędnych konfiguracji w oparciu o punkty procentowe.
    - System zarządzania ryzykiem który powinien wykrywać luki w aplikacjach podając przy tym numer CVE tych luk.
    - System który pozwala na śledzenie i wykrywanie niezwyczajnych działań jakie podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem ilu użytkowników takie działanie dotyczy oraz jakie jest jego nasilenie.
    - System pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na podstawie harmonogramu lub pojedynczo utworzonego zadania.
    - System pozwala na raportowanie na ilu urządzeniach wykryto błędną konfigurację i luki w aplikacjach oraz jaka jest ilość takich podatności i ich nasilenie wyrażone w procentach.

- System pozwala na raportowanie u ilu użytkowników wykryto podejrzane działania oraz jakie jest ich nasilenie

52. Wbudowana ochrona przed exploitami wyposażona w minimum 15 różnych technik wykrycia exploitów z możliwością włączenia lub wyłączenia każdej z nich oraz dająca możliwość dodania własnych procesów. Funkcja umożliwia również:
    - Możliwość wymuszenia funkcji DEP systemu Windows
    - Możliwość wymuszenia relokacji modułów (ASLR)
53. Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochroną przed technikami takimi jak:
    - Wczesny dostęp
    - Dostęp do poświadczeń
    - Wykrycie
    - Crimeware
54. Ochrona przed ransomware - możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym oraz utworzenie kopii zapasowej plików a w przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji.
    Formaty plików jakie mogą być odzyskane:
    3fr|ai|arw|bay|cab|cdr|cer|cr2|crt|crw|dcr|der|dgn|dll|dng|doc|docm|docx|dwg|dxf|dxg|eps|erf|exe|indd|ini|jpe|jpeg|jpg|mdf|mef|mrw|msg|msi|nef|nrw|odb|odc|odm|odp|ods|odt|orf|p12|p7b|p7c|pdd|pdf|pef|pem|pfx|png|ppt|pptm|pptx|psd|pst|ptx|py|r3d|raf|rtf|rw2|rwl|sr2|srf|srw|tsf|wb2|wpd|wps|x3f|xlk|xls|xlsb|xlsm|xlsx|xml|
    Oprogramowanie daje możliwość odzyskania plików na żądanie lub automatycznego odzyskiwania.
55. Ochrona proaktywna oparta o maszynowe uczenie która działa w fazie poprzedzającej wykonanie, ochrona ta musi wy wykrywać zagrożenia takie jak:
    - Ukierunkowane ataki
    - Podejrzane pliki i ruch w sieci
    - Exploity
    - Ransomware
    - Grayware
56. Moduł ochrony proaktywnej musi posiadać oddzielne działania jakie będzie podejmował dla plików i oddzielne dla ruchu sieciowego.
57. Moduł ochrony proaktywnej musi działać w trybach które administrator może dowolnie zmieniać na:
    - Tolerancyjny
    - Normalny
    - Agresywny
58. Zintegrowany sandbox po stronie producenta który pozwala na analizę pliku
    - Plik może zostać wysłany automatycznie ze stacji roboczej jeżeli oprogramowanie uzna go za podejrzany lub ręcznie z poziomu konsoli przez administratora
    - Możliwość przesłania archiwum zabezpieczonego hasłem
    - Możliwość przesłania adresu URL
    - W przypadku przesłania wielu plików jednorazowo, możliwość detonacji próbek pojedynczo.
59. Wbudowany sandbox musi działać w trybie monitorowania i blokowania

60. Wbudowany sandbox musi oferować działania naprawcze takie jak dezynfekcja lub przeniesienie do kwarantanny
61. Wbudowany sandbox musi oferować opcję wstępnego filtrowania zawartości która skanuje pliki, argumenty wiersza poleceń i adresy URL pod kątem podejrzanego zachowania.
62. Wbudowany sandbox musi posiadać opcję która pozwala na dodanie określonych rozszerzeń do wyjątków, pliki z tym rozszerzeniem nie zostaną przesłane do sandboxa.
63. Minimalny rozmiar pliku jaki może zostać przesłany do sandboxa to 1KB.

IV. Maszyny wirtualne

1. Możliwość w kliencie instalowanym na stacji roboczej wirtualnej ustawienie informacji do pomocy technicznej, takiej jak: (strona pomocy, adres e-mail, numer telefonu)
2. Możliwość określenia jak długo maja być przechowywane zdarzenia na stacji roboczej.
3. Możliwość zabezpieczenia hasłem klienta przed odinstalowaniem
4. Wersja kliencka nie pełni roli ochrony antywirusowej, jest tylko agentem dla Security Servera.
5. Dla maszyn z systemem Linux możliwość wskazania katalogów które mogą być chronione w czasie rzeczywistym.
6. Możliwość określenia co jaki czas mają być wysyłane pliki z kwarantanny do producenta.
7. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.
8. Możliwość wskazania do jakiego serwera ochrony maja się łączyć klienci maszyn wirtualnych.

V. Stacje robocze i serwery Windows

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
3. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
4. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
5. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
6. Skanowanie plików spakowanych i skompresowanych.
7. Oprogramowanie zawiera monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
8. Oprogramowanie posiada możliwość zablokowania hasłem odinstalowania programu.
9. Produkt oraz sygnatury muszą być aktualizowane nie rzadziej niż raz na godzinę.
10. Oprogramowanie musi posiadać możliwość raportowania zdarzeń informacyjnych.
11. Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
12. Program musi posiadać możliwość skanowania jedynie nowych nie zmienionych plików.
13. Program musi mieć wbudowany skaner wyszukiwania rootkitów
14. Możliwość odblokowania ustawień programu po wpisaniu hasła
15. Możliwość uruchomienia zadania skanowania z niskim priorytetem
16. Możliwość wykorzystania dodatkowej maszyny wirtualnej która przejmie role silnika skanującego.
17. Możliwość określenia jak długo maja być przechowywane zdarzenia na stacji roboczej.
18. Możliwość zabezpieczenia hasłem klienta przed odinstalowaniem

19. Dla maszyn z systemem Linux możliwość wskazania katalogów które mogą być chronione w czasie rzeczywistym.
20. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.

VI. Konsola zdalnej administracji

1. Dwa typy konsoli administracyjnej:
   - Konsola w chmurze – serwer administracyjny po stronie producenta
   - Konsola lokalna – lokalny serwer administracyjny
2. Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów plikowych Windows.
3. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, oraz zaporą osobistą (tworzenie reguł obowiązujących dla wszystkich stacji) zainstalowanymi na stacjach roboczych w sieci korporacyjnej z jednego serwera zarządzającego.
4. Możliwość integracji Domeny Active Directory w obu typach konsoli.
5. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.
6. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie, Zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki).
7. Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi.
8. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, wersji systemu operacyjnego.
9. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.
10. Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej.
11. Możliwość zmiany konfiguracji na stacjach i serwerach z poziomu centralnej konsoli zarządzającej lub z poziomu punktu końcowego po włączeniu odpowiedniej opcji w politykach bezpieczeństwa.
12. Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej.
13. Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) i wyeksportowanie go do formatu: pdf i csv
14. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie również zbiorczo w formie archiwum zip.
15. Możliwość generowania raportu co godzinę.
16. Po instalacji oprogramowania antywirusowego nie jest wymagane ponowne uruchomienie komputera do prawidłowego działania programu.
17. Aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej.
18. Możliwość dodania etykiety do stacji roboczej.
19. Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji zdalnej.
20. Możliwość przechowywania kwarantanny: 180 dni
21. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.
22. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.
23. W całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej.
24. Możliwość aktualizacji serwera administracyjnego bez potrzeby przeinstalowywania.

25. Możliwość przypisywania polityk automatycznie po zalogowaniu do systemu operacyjnego w zależności od tego jaki użytkownik domenowy się zalogował lub do jakiej grupy domenowej on należy.
26. Możliwość automatycznego przypisywania polityk na podstawie reguły lokalizacji, możliwość określenia lokalizacji na podstawie
    - Zakres adresów IP/IP
    - Adres bramy
    - Adres serwera WINS
    - Adres serwera DNS
    - Połączenie DHCP sufiksów DNS
    - Punkt końcowy może rozwiązać hosta
    - Typ sieci
    - Nazwa hosta
27. Uwierzytelnienie dwuskładnikowe realizowane np. wyłącznie przez aplikację Google Authenticator,
28. Możliwość utworzenia reguły która będzie usuwała punkty końcowe z konsoli zarządzającej jeżeli punkt końcowy nie połączył się z konsolą przez określoną liczbę dni. Funkcja ta pozwala również na określenie wzoru nazw maszyn które automatycznie będą usuwane oraz pozwala na okrślenie godziny kiedy te maszyny będą usuwane.
29. Każdy z rodzajów ochrony musi być rozdzielony w osobnych oknach konfiguracyjnych, komputery fizyczne, Urządzenia mobilne.
30. Serwer centralnej administracji musi posiadać funkcje przełączenia się miedzy widokiem maszyn fizycznych i urządzeń mobilnych. Tak by wyświetlana była jedynie wskazana grupa urządzeń chronionych.
31. Tworzenie osobnych polityk dla fizycznych komputerów, urządzeń mobilnych oraz maszyn wirtualnych.
32. Możliwość zarządzania ochroną na serwerach Exchange, tworzenie polityk i konfiguracji zdalnej ochrony.
33. Możliwość przypisywania polityk w zależności od zalogowanego użytkownika domenowego.
34. Możliwość wygenerowania i pobrania logów ze stacji roboczej z poziomu konsoli zarządzającej.
35. Funkcja kontroli aplikacji może działać w trybie testowym lub produkcyjnym.
36. Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta.
37. Możliwość wyświetlenia czy punkt końcowy jest serwerem czy stacją roboczą.
38. Możliwość wyświetlenia informacji czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux, MacOS.
39. Możliwość wyświetlenia wersji systemu operacyjnego zainstalowanego na punkcie końcowym.
40. Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni.
41. Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows, Linux, MacOS
42. Oprogramowanie umożliwia pobranie oddzielnego pakietu instalacyjnego dla systemów MacOS z Intel x86 oraz oddzielnego dla Apple M1
43. 62.Oprogramowanie umożliwia ochronę kontenerów instalowaną bezpośrednio na hoście kontenera oferuje wgląd w złośliwą aktywność serwera Linux i kontenerów w czasie rzeczywistym.

VII. EDR – Endpoint Detection and Response

Produkt zapewnia szczegółowe informacje o wykrytych incydentach, interaktywną mapę incydentów i działania naprawcze.

1. Wspierane systemy operacyjne
   - Systemy desktopowe
     - Windows 10 May 2019 Update (19H1)
     - Windows 10 October 2018 Update (Redstone 5)
     - Windows 10 April 2018 Update (Redstone 4)
     - Windows 10 Fall Creators Update (Redstone 3)
     - Windows 10 Creators Update (Redstone)
     - Windows 10 Anniversary Update (Redstone 1)
     - Windows 10 November Update (Threshold 2)
     - Windows 10
     - Windows 8.1
     - Windows 8
     - Windows 7
   - Systemy operacyjne dla serwerów
     - Windows Server 2019
     - Windows Server 2016
     - Windows Server 2012
     - Windows Server 2008 R2
   - MacOS
     - OS X El Capitan (10.11.x) i nowsze
   - Linux
     - Ubuntu 14.04 lub nowszy
     - CentOS 7.3 lub nowszy
2. Komponenty EDR

Główne elementy:

- Czujnik EDR, który gromadzi i przetwarza dane w celu raportowania danych dotyczących punktu końcowego i zachowania aplikacji.
- Security Analytics, komponent służący do interpretacji metadanych gromadzonych przez czujnik EDR.

  Możliwość instalacji dodatkowego, lekkiego agenta z czujnikiem EDR dla urządzeń z systemem Windows, aby rozszerzyć już zainstalowaną ochronę. Agent posiada też ochronę urządzenia i ruchu sieciowego oraz filtr stron internetowych.

3. Wykrywanie podejrzanej aktywności

Monitorowanie zdarzeń na punktach końcowych w poszukiwaniu oznak ataku i wywoływanie incydentów po wykryciu takiej aktywności.

- Bazowanie na systemach bazujących na wskaźnikach ataku MITRE i własnej inteligencji.
- Zgłaszanie wszystkich naruszeń jako incydent w module EDR.

4. Badanie incydentów i wizualizacja
   - Produkt zapewnia wsparcie analizy incydentów poprzez dostarczenie narzędzi, które pomagają filtrować, badać i podejmować działania dotyczące wszystkich zdarzeń bezpieczeństwa wykrytych przez czujnik EDR w określonym przedziale czasu.
   - Produkt integruje się z bazą wiedzy ATT & CK firmy MITRE i odpowiednio oznacza zdarzenia bezpieczeństwa.

- Produkt zapewnia zaawansowaną wizualizację zdarzeń bezpieczeństwa z określonymi informacjami lub działaniami z następującymi informacjami:
    - Karta Podsumowanie zawiera przegląd wpływu zdarzenia i szczegółowe informacje o każdym węźle zdarzenia.
    - Funkcja osi czasu zbiera informacje o rozwoju zdarzenia bezpieczeństwa w kolejności chronologicznej.
    - Działania naprawcze gromadzą informacje o działaniach blokujących automatycznie podejmowanych przez produkt w związku z bieżącym zdarzeniem bezpieczeństwa.

5. Incydenty

Oprogramowanie pozwala na informowanie o zagrożeniach wykrytych i zablokowanych w formie grafu i linii zdarzeń oraz daje możliwość:

- Filtrowania zdarzeń
- Blokowania procesów
- Dodawanie procesów do czarnej listy
- Dodawanie procesów do białej listy
- Izolacja hosta
- Aktualizacja oprogramowania firm trzecich na hoście (wymagany add-on)
- Przesłanie pliku do Sandbox
- Sprawdzenie informacji o pliku w Google
- Sprawdzenie informacji o pliku w VirusTotal

Filtrowanie zdarzeń odbywa się na podstawie:

- Ocena zagrożenia np. od 10 do 100 punktów
- Data wykrycia
- Status
- ID
- Nazwa punktu końcowego
- Typ ataku
    - Ransomware
    - Potencjalnie niechciana aplikacja
    - Malware
    - Exploit
    - Fileless
    - Password stealer
    - Downloader
    - Inne
    - Zdefiniowane przez użytkownika
- Wyszukiwanie zdarzeń może odbywać się na podstawie:
    - Nazwa alertu
    - IP punktu końcowego
    - Hash MD5
    - Hash SHA256
    - Nazwa użytkownika
- Możliwość szybkiego podglądu otwartych incydentów, najczęstszych powiadomień, urządzeń które mają najczęściej problem.
- Możliwość wyświetlenia 10,20,30,50,100 zdarzeń na jednej stronie.
- Możliwość wyświetlenia zablokowanych hashy plików.
- Możliwość dodania własnych hashy MD5 oraz SHA256

- Możliwość importu hashy z pliku CSV
- Możliwość filtrowania dodanych hashy na podstawie:
  - Typu hashu
  - Wartości hash
  - Źródło dodania
  - Informacje o źródle
  - Nazwa pliku
  - Firma której dotyczy wpis
  - Możliwość wyboru wpisów do wyświetlenia (np. 10, 20, 30, 50, 100) na jednej stronie.