OPIS PRZEDMIOTU ZAMÓWIENIA

w postępowaniu o udzielenie zamówienia publicznego

pn. Zakup oprogramowania klasy SIEM wraz z wdrożeniem i szkoleniem w ramach realizacji grantu „Cyberbezpieczny Samorząd" w Starostwie Powiatowym w Płońsku

1. Niniejszy załącznik stanowi szczegółowy opis przedmiotu zamówienia. Zaoferowane przez Wykonawcę rozwiązania muszą spełniać minimalne wymagania postawione w niniejszym załączniku oraz zostać dostarczone na warunkach określonych poniżej.

2. Zamówienie obejmuje kompleksową dostawę, wdrożenie oraz konfigurację systemu SIEM objętego niniejszym zamówieniem. Wykonawca zobowiązany będzie do zapewnienia pełnego wdrożenia systemu, weryfikacji poprawności działania zgodnie z opisem przedmiotu zamówienia. W ramach realizacji przedmiotu zamówienia Wykonawca zapewni także gwarancję, wsparcie powdrożeniowe oraz przeprowadzi szkolenie dla minimum dwóch administratorów IT wyznaczonych przez Zamawiającego, w sposób umożliwiający im samodzielną i efektywną obsługę oraz zarządzanie wdrożonym systemem.

3. Zamawiający wymaga, aby wszystkie elementy oprogramowania dostarczone w ramach realizacji przedmiotu zamówienia stanowiły standardowe, komercyjne oprogramowanie producenta, pochodzące z oficjalnego kanału dystrybucji producenta oraz objęte pełnym, komercyjnym wsparciem technicznym producenta.

4. Zamawiający nie dopuszcza dostarczenia:

- **a.** oprogramowania typu open source;
- **b.** oprogramowania freeware, shareware, community edition, trial, beta, release candidate lub innych wersji testowych;
- **c.** rozwiązań, których kluczowe funkcjonalności realizowane są przez komponenty nieobjęte pełnym, komercyjnym wsparciem producenta.

5. Przez oprogramowanie typu open source Zamawiający rozumie oprogramowanie udostępniane na licencjach otwartego kodu źródłowego, w szczególności GNU GPL, LGPL, AGPL, Apache, MIT, BSD lub licencjach równoważnych, niezależnie od sposobu jego dystrybucji.

6. Powyższe wymaganie wynika z konieczności zapewnienia:

- **a.** pełnej odpowiedzialności producenta za rozwój i utrzymanie rozwiązania;
- **b.** regularnego i terminowego usuwania podatności oraz dostarczania aktualizacji bezpieczeństwa;
- **c.** gwarantowanego wsparcia technicznego i jednoznacznej ścieżki eskalacji problemów;
- **d.** ciągłości działania systemu wykorzystywanego do realizacji zadań publicznych;
- **e.** spełnienia wymagań w zakresie zarządzania ryzykiem i cyberbezpieczeństwa wynikających z Ustawa o krajowym systemie cyberbezpieczeństwa, w szczególności obowiązku stosowania odpowiednich i proporcjonalnych środków technicznych i organizacyjnych.

7. W przypadku stwierdzenia, że zaoferowane rozwiązanie nie spełnia wymagań określonych w niniejszym punkcie, oferta zostanie uznana za niezgodną z warunkami zamówienia i odrzucona zgodnie z Prawo zamówień publicznych.

8. Zamawiający wymaga, aby dostarczony w ramach zamówienia system został przez Wykonawcę wdrożony i skonfigurowany w sposób zapewniający jego pełną funkcjonalność oraz zgodność z wymaganiami określonymi w opisie przedmiotu zamówienia. Wdrożenie musi uwzględniać integrację systemu w ramach spójnej infrastruktury informatycznej. Zamawiający nie precyzuje na tym etapie szczegółowych ustawień konfiguracyjnych – zostaną one ustalone pomiędzy stronami w trakcie realizacji umowy, w zależności od potrzeb i warunków technicznych środowiska Zamawiającego. Wykonawca będzie zobowiązany do wykonania wszystkich niezbędnych prac konfiguracyjnych, umożliwiających prawidłowe i bezpieczne użytkowanie dostarczonych rozwiązań.

9. W ramach ceny zakupu systemów Wykonawca zapewnia gwarancję jakości obejmującą: usuwanie usterek i awarii, prawo do aktualizacji i poprawek bezpieczeństwa, dostęp do pomocy technicznej producenta lub autoryzowanego partnera (telefonicznej, mailowej, zdalnej), konsultacje techniczne niezbędne dla prawidłowego działania systemu, dostarczanie nowych wersji oprogramowania (upgrade/patch), jeśli zostaną wydane w okresie gwarancji.

10. Wszelkie dostarczane w ramach zamówienia oprogramowanie musi być fabrycznie nowe, nieużywane oraz nieaktywowane wcześniej na żadnym urządzeniu. Wykonawca zobowiązany jest dostarczyć je w najnowszej stabilnej wersji, dostępnej na dzień składania ofert, pochodzącej wyłącznie z oficjalnego kanału dystrybucyjnego producenta. Oprogramowanie nie może być obciążone żadnymi prawami osób trzecich, a jego nośniki – o ile występują – muszą być wolne od wad fizycznych i prawnych.

11. Dostarczone oprogramowanie musi być objęte gwarancją producenta lub autoryzowanego partnera serwisowego, realizowaną na terenie Polski. Gwarancja obejmuje w szczególności: usuwanie usterek i awarii, prawo do aktualizacji i poprawek bezpieczeństwa, dostęp do pomocy technicznej w języku polskim (telefonicznej, mailowej, zdalnej), a także świadczenie usług serwisowych. przez certyfikowany personel. Czas reakcji serwisu nie może przekraczać następnego dnia roboczego od momentu zgłoszenia. Wszystkie usługi serwisowe muszą być realizowane zgodnie z wymaganiami producenta, dobrymi praktykami inżynierskimi oraz w oparciu o certyfikaty jakości (w szczególności ISO 9001 i ISO 27001) posiadane przez podmiot serwisujący.

12. Szkolenie ma być prowadzone równolegle z procesem wdrożenia. Szkolenie musi być prowadzone przez osobę posiadającą odpowiednią wiedzę, doświadczenie i kwalifikacje potwierdzające kompetencje w zakresie danej tematyki.

13. Pod pojęciem „okresu wsparcia powdrożeniowego" Zamawiający rozumie czas, w którym Wykonawca zapewnia swoją dostępność w celu dokonania niezbędnych poprawek konfiguracyjnych mogących wystąpić w pierwszym okresie po wdrożeniu, a także udziela wsparcia w zakresie utrwalania wiedzy zdobytej podczas szkoleń oraz dodatkowych konsultacji związanych z prawidłowym użytkowaniem dostarczonych rozwiązań. Kryterium to nie dotyczy podstawowych świadczeń serwisowych w ramach gwarancji (które Wykonawca i tak jest zobowiązany zapewnić zgodnie z ofertą), lecz właśnie dostępności Wykonawcy w zakresie doradztwa, korekt i utrwalenia wiedzy, które mają kluczowe znaczenie dla pełnego i skutecznego wykorzystania rezultatów projektu „Cyberbezpieczny Samorząd".

14. Prace wdrożeniowe i konfiguracyjne muszą być prowadzone przez Wykonawcę w siedzibie Zamawiającego. Wykonanie prac w formie zdalnej możliwe jest wyłącznie za zgodą Zamawiającego.

WYMAGANIA MINIMALNE CENTRALNEGO SYSTEMU BEZPIECZEŃSTWA (system klasy SIEM)

1. LICENCJA

1.1. W ramach postępowania Wykonawca jest zobowiązany dostarczyć oprogramowanie klasy SIEM (oprogramowanie Systemu Bezpieczeństwa, dalej SB) wraz z licencją bezterminową.

1.2. Oprogramowanie musi posiadać gwarancję jakości (m.in. ze wsparciem technicznym i prawem do aktualizacji oprogramowania) przez okres co najmniej 12 miesięcy

1.3. Licencje na oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej.

1.4. Dostarczona licencja na Oprogramowanie Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji ze zgromadzonych danych.

1.5. Infrastruktura objęta systemem:

a) 155 hostów (w tą liczbę wliczone są stacje robocze, laptopy i serwery),

b) urządzenia aktywne w sieci posiadające adres IP w ilości 10 hostów (typu przełączniki, UTMy)

c) 65 hostów (drukarki)

2. WYMAGANIA DOT. SYSTEMU BEZPIECZEŃSTWA

2.1. Automatyczne Odkrywanie: Centralny System Bezpieczeństwa (dalej CSB) musi używać różnych metod, takich jak skanowanie sieci, obsługa protokołów SNMP, IPMI, i JMX, aby automatycznie wykrywać i konfigurować urządzenia w sieci.

2.2. Monitorowanie Wysokiej Wydajności: CSB musi umożliwiać monitorowanie wydajności przy wykorzystaniu rozwiązań agentowych lub bez agentowych metodami monitorowania (np. przez SNMP, ICMP, IPMI), CSB musi efektywnie zbierać dane o wydajności i dostępności urządzeń. System powinien posiadać skalowalną architekturę dostosowaną do ilości urządzeń obsługiwanych w infrastrukturze Zamawiającego w ilości 170 urządzeń końcowych.

2.3. Elastyczne Wyzwalacze: Wyzwalacze (akcje) w CSB powinny być wyrażeniami logicznymi, które określają warunki dla powiadomień alarmowych. W systemie musi być możliwość definiowania złożonych warunków dla generowania alertów, na przykład po przekroczeniu pewnych progów lub w przypadku wystąpienia określonych wzorców.

2.4. Wizualizacja Danych: CSB powinien posiadać intuicyjny i przejrzysty interface, umożliwiający wizualizację danych pod kontem ich analizy. System musi umożliwiać wizualizację przy wykorzystaniu m.in interaktywnych wykresów i grafik ponadto system musi posiadać wbudowaną zaawansowaną wyszukiwarkę umożliwiającą odfiltrowywanie danych i ich wizualizację wg. wybranych kategorii (np. poziom istotności).

2.5. Alerty i Powiadomienia: CSB powinien umożliwiać konfigurację zaawansowanych scenariuszy powiadomień, które mogą być wysyłane poprzez e-mail, SMS czy integracje z systemami biletowymi. Użytkownicy powinni mieć możliwość ustawiania różnych poziomów priorytetów dla alertów, a także definiowania eskalacji dla poważniejszych problemów.

2.6. Raportowanie: CSB powinien umożliwiać użytkownikom generowanie szczegółowych raportów dotyczących wydajności i dostępności monitorowanych systemów.

2.7. Wsparcie dla Szyfrowania: CSB musi być systemem bezpiecznym, umożliwiającym szyfrowaną komunikację między agentami a serwerem, co zapewnia bezpieczeństwo danych monitorowania.

2.8. Skalowalność: Architektura CSB powinna być zaprojektowana z myślą o skalowalności, co powinno pozwalać na łatwą adaptację do rosnących wymagań w miarę rozwoju infrastruktury IT.

2.9. Przetwarzanie i Wyszukiwanie Danych: CSB pod kątem agregacji logów musi być oparty na technologii, która umożliwia indeksowanie, wyszukiwanie i analizowanie dużych ilości danych w czasie rzeczywistym. Użytkownicy powinni móc wykonywać skomplikowane zapytania, aby szybko odnaleźć konkretne informacje.

2.10. Szybkość i Wydajność: Zaprojektowany do szybkiego przetwarzania dużych ilości danych, co jest kluczowe w środowiskach produkcyjnych z intensywnym ruchem danych.

2.11. Elastyczne Zbieranie Danych: CSB musi gromadzić dane z różnych źródeł jednocześnie (co najmniej urządzenia sieciowe, serwery, urządzenia klienckie).

2.12. Przetwarzanie i Wzbogacanie Danych: CSB musi posiadać bogaty zestaw filtrów do przetwarzania danych.

2.13. Odkrywanie i Analiza Danych: System musi umożliwia użytkownikom przeszukiwanie, przeglądanie i analizowanie zgromadzonych danych ułatwiając identyfikację wzorców i trendów.

2.14. Wsparcie dla Wielu Platform: CSB musi być kompatybilny z wieloma systemami operacyjnymi, co najmniej Linux, Windows, macOS.

2.15. Treści pojawiające się w interfejsie użytkowników CSB będą spełniać standardy WCAG 2.1 na poziomie AA.

2.16. Cały interfejs użytkownika powinien być dostosowany pod aktualne wymagania prawne związane z dostępnością serwisów użyteczności publicznej dla osób z niepełnosprawnościami.

2.17. Na podstawie uzyskanych efektów serwis będzie mógł być udostępniony publicznie.

2.18. Treści multimedialne muszą być dostępne z poziomu klawiatury i oprogramowania dla osób niepełnosprawnych. Multimedia, które nie mogą być z przyczyn technicznych tak zbudowane, by uczynić je dostępnymi dla wszystkich użytkowników muszą posiadać alternatywny opis tekstowy, który wyjaśnia ich cel i funkcje zastosowania na stronie.

2.19. Zgodność ze standardami HTML i CSS całego serwisu www.

2.20. Kontrast kolorystyczny między tłem, a tekstem musi być zgodny z zaleceniami WCAG 2.1 AA.

2.21. System CSB musi rejestrować zdarzenia akcje i reakcje użytkowników w CSB. Historia akcji poszczególnych użytkowników musi być raportowana i możliwa do odtworzenia w logach systemowych – chronologicznie.

System musi posiadać budowę modułową, która będzie umożliwiać dodawanie nowych modułów oraz wyłączanie już uruchomionych. Dostarczony i uruchomiony system będzie posiadał co najmniej moduły:

3. MODUŁ ANALIZY PODATNOŚCI

3.1. Integracja ze stale aktualizowaną bazą danych CVE (Common Vulnerabilities and Exposures), gromadzącą informację na temat podatności urządzeń i oprogramowania.

3.2. System musi być zintegrowany z publicznym i stale aktualizowanym rejestrem gromadzącym i udostępniającym informację na temat znanych podatności w urządzeniach obsługiwanych przez system oraz

oprogramowaniu zainstalowanym na urządzeniach Zamawiającego (np. UTM). Połączenie z bazą danych CVE odbywać się ma przy wykorzystaniu udostępnionego API i nie powinno wymagać od użytkowników końcowych konfiguracji.

3.3. Synchronizacja z bazą CVE oraz sprawdzenie dodania do niej nowych podatności dotyczących sprzętu i oprogramowania zainstalowanego w infrastrukturze sieciowej jednostki musi odbywać się przynajmniej raz dziennie. Po zalogowaniu do CSB i wybraniu modułu analizy podatności powinny być wyświetlane wszystkie zsynchronizowane informacje wraz z danymi historycznymi. Podatności "nowe", których użytkownik wcześniej nie widział powinny być w systemie oznaczone np. poprzez pogrubioną czcionkę lub inny kolor.

3.4. Automatyczne sprawdzenie możliwości występowania podatności w infrastrukturze sieciowej na podstawie zinwentaryzowanych urządzeń i oprogramowania.

3.5. System musi automatycznie sprawdzać możliwość wystąpienia nowej podatności tylko na urządzeniach i oprogramowaniu znajdującym się w infrastrukturze sieciowej jednostki, a dokładniej wyszczególnionych (dodanych) w module inwentaryzacji.

3.6. Powiadamianie użytkownika o nowych podatnościach występujących w jego środowisku IT.

3.7. System musi informować użytkownika/administratora o nowych podatnościach występujących w infrastrukturze sieciowej jednostki. System powinien posiadać możliwość włączenia powiadomień na przeglądarkę internetową oraz wskazany przez użytkownika/administratora adres e-mail. Ponadto użytkownik po zalogowaniu się do systemu i wybraniu modułu analizy podatności musi być powiadomiony przez system o występujących nowych podatnościach na poszczególnych hostach infrastruktury sieciowej poprzez np. graficzne wyróżnienie hosta i oprogramowania na nim zainstalowanego. System musi informować użytkownika o treści podatności oraz jej sklasyfikowania (np. podatność krytyczna).

4. MODUŁ MONITORINGU ZASOBÓW

4.1. Monitorowanie zasobów hostów na podstawie zinwentaryzowanych w systemie urządzeń (monitoring obciążenia dysków, procesorów, ruchu sieciowego itp.)

4.2. System musi posiadać możliwość monitorowania zasobów wszystkich hostów dodanych w module inwentaryzacji. Monitorowanie, zbieranie informacji na temat obciążenia wybranego hosta musi odbywać się w sposób ciągły w ustalonych krótkich (co najmniej minutowych) odstępach czasowych. Użytkownik po zalogowaniu się do systemu i wybraniu modułu inwentaryzacji musi mieć możliwość wyświetlenia w formie graficznej (wykresów), przebiegów czasowych istotnych parametrów hosta, co najmniej takich jak: obciążenie procesora, obciążenie pamięci, obciążenie dysków, obciążenie ruchu sieciowego, skoki na procesorze, czas oczekiwania na dysk i odczyt i zapis na dysku. Ponadto system musi na bieżąco informować o aktualnym statusie hosta (dostępny, niedostępny).

4.3. Grupowanie hostów i korelacja obciążeń zasobów pomiędzy hostami.

4.4. System musi mieć możliwość wyświetlania zgrupowanych wykresów hostów należących do tej samej grupy. Hosty muszą być pogrupowane w zasugerowany przez administratora sieci sposób w celu skorelowania ze sobą istotnych parametrów zasobów, co umożliwi porównanie zachowań poszczególnych hostów na tle grupy. Hosty powinny być podzielone co najmniej, na urządzenia sieciowe (np. serwery) oraz urządzenia końcowe (np. komputery pracowników). Użytkownik musi mieć możliwość filtrowania wykresów na poziomie poszczególnych hostów oraz tworzenia w systemie nowych grup i wykresów parametrów dostępnych z wybieralnej listy.

4.5. Wysyłanie alertów i powiadomień dotyczących problemów i zdarzeń występujących na hostach.

4.6. System musi posiadać funkcjonalność umożliwiającą użytkownikowi/administratorowi skonfigurowanie wysyłania alertów i powiadomień dotyczących problemów i zdarzeń. W systemie musi być możliwość ustawienia wysyłania wiadomości i powiadomień, poprzez wysyłanie komunikatów na przeglądarkę internetową, wysyłanie wiadomości e-mali lub wiadomości sms (w systemie powinna być możliwość dodania bramki sms - Zamawiający dopuszcza wykorzystanie autorskiej bramki sms lub wskażę zew. bramkę/serwis sms). Wysyłane przez system wiadomości muszą zawierać co najmniej informacje na temat występującego zdarzenia/problemu tj. opis, sklasyfikowanie (np. błąd, ostrzeżenie, informacja), data i godzina. Użytkownik/Administrator powinien mieć możliwość ustawienia odbiorcy wiadomości poprzez podanie adresu e-mail, czy w przypadku wiadomości SMS numeru telefonu. Użytkownik musi mieć możliwość wyboru w systemie, przy jakiego typu zdarzeniach i problemach będzie wysyłana wiadomość.

4.7. Funkcja korelacji występujących problemów na hostach z modułem analizy logów.

4.8. Moduł monitoringu zasobów oprócz przebiegów czasowych parametrów hostów powinien również zawierać informację na temat występujących problemów i zdarzeń na poszczególnych hostach. Użytkownik/Administrator po zalogowaniu się do systemu, wybraniu Modułu Monitoringu zasobów i wyborze konkretnego hosta musi

posiadać możliwość prześledzenia zdarzeń i problemów naniesionych na osi czasu. Na osi czasu powinny być wyświetlane tylko "nowe" problemy i zdarzenia oraz te, których status nie został zmieniony na "rozwiązany" bądź "anulowany". Użytkownik/Administrator musi mieć możliwość zmiany statusu wybranego zdarzenia czy problemu wraz z dodaniem krótkiego opisu w jaki sposób problem został rozwiązany. Użytkownik/Administrator musi mieć możliwość stłumienia często powielającego się problemu, którego jest świadomy i musi poczekać na jego rozwiązanie (po włączeniu opcji tłumienia problemu, system przez pewien czas nie będzie o nim informował/alertował). Wszystkie problemy i zdarzenia raportowane w systemie muszą być skorelowane z logami pochodzącymi z konkretnych hostów. Użytkownik/Administrator po wybraniu w systemie konkretnego problemu występującego na konkretnym hoście po wybraniu zakładki logi musi zostać przekierowany do modułu analizy logów, w którym automatycznie wyświetlone będą tylko logi dotyczące hosta, na którym wystąpił problem. Ponadto użytkownik/administrator w ramach tego modułu powinien mieć możliwość zgłoszenia wystąpienia konkretnego problemu do np. zewnętrznego wsparcia IT. W systemie powinna być możliwość integracji systemu z zewnętrznym systemem typu: "help-desk", przynajmniej poprzez podanie adresu e-mail, na który zostanie wysłane zgłoszenie.

4.9. Kategoryzacja istotności zdarzeń występujących w infrastrukturze sieciowej.

4.10. Wszystkie zdarzenia i problemy raportowane w systemie muszą być skategoryzowane według ich poziomu istotności (priorytetów). W systemie powinny być identyfikowane problemy z priorytetami w co najmniej 4 stopniowej skali, np. : Krytyczny, Wysoki, Średni, Niski. Ponadto, system powinien zapewniać dodatkowe dwa priorytety - zdarzenia nie istotne powinny być również sklasyfikowane w systemie jako informacja, a zdarzenia trudne do sklasyfikowania powinny posiadać priorytet o wartości (niesklasyfikowany).

4.11. Lista predefiniowanych zdarzeń najczęściej występujących w środowiskach IT.

4.12. System musi być wyposażony w listę wcześniej zdefiniowanych zdarzeń/scenariuszy, które najczęściej występują w środowiskach IT. Użytkownik/Administrator powinien mieć możliwość wybrania konkretnego hosta lub grupy hostów i przypisania im predefiniowanych zdarzeń (np. brak miejsca na dyskach, czy zbyt wysoki ruch sieciowy). W predefiniowanych zdarzeniach/scenariuszach użytkownik/administrator powinien mieć możliwość ustawienia/edycji reguł oraz zmiany wykonywanych operacji, gdy warunki reguł zostaną spełnione. Użytkownik powinien mieć możliwość używania w regułach operatorów logicznych takich jak AND i OR oraz operatorów relacyjnych takich jak: "==", "<=", ">=", "!=". Użytkownik/Administrator systemu musi mieć możliwość ustawienia operacji różnego typu takich jak.: wysłanie wiadomości e-mail, wysłanie wiadomości SMS (Zamawiający dopuszcza wykorzystanie autorskiej bramki sms lub wskażę zew. bramkę/serwis sms), wysłanie zapytania (Request), czy uruchomienie predefiniowanego skryptu.

4.13. Dobór oraz dodawanie zdarzeń do konkretnego środowiska IT.

4.14. System musi umożliwiać użytkownikowi/administratorowi dodawanie własnych zdarzeń/ scenariuszy dostosowanych do jego konkretnych potrzeb. Tworzenie nowego zdarzenia w systemie powinno się odbywać poprzez podanie jego unikalnej nazwy, wybranie hosta lub grupy hostów, których dotyczy tworzone zdarzenie, zdefiniowanie warunków opisujących zdarzenie, oraz podanie operacji jakie mają być wykonane, gdy warunki zostaną spełnione. Warunki powinny korzystać z operatorów logicznych takich jak AND i OR oraz operatorów relacyjnych takich jak: "==", "<=", ">=", "!=". Użytkownik/Administrator systemu musi mieć możliwość ustawienia operacji różnego typu takich jak.: wysłanie wiadomości e-mail, wysłanie wiadomości SMS (Zamawiający dopuszcza wykorzystanie autorskiej bramki sms lub wskażę zew. bramkę/serwis sms), wysłanie zapytania (Request), czy uruchomienie predefiniowanego skryptu.

4.15. Zdalny dostęp do urządzeń końcowych.

4.16. System musi umożliwiać zdalne połączenie się do wybranego hosta/urządzenia, które zostało wcześniej odpowiednio skonfigurowane. Zdalny dostęp musi odbywać się poprzez przeglądarkę internetową bez konieczności instalowania dodatkowego oprogramowania. Połączenie zdalne musi być możliwe przy wykorzystaniu co najmniej dwóch protokołów, konkretnie RDP i SSH.

4.17. Wywoływanie predefiniowanych skryptów na urządzeniach końcowych.

4.18. System musi dawać możliwość wywołania podstawowych skryptów na hostach końcowych, na których został zainstalowany jego agent. Predefiniowane w systemie skrypty muszą obejmować co najmniej: wyłączenie i restart hosta, wysłanie wiadomości tekstowej do hosta, włączenie i wyłączenie blokady ruchu sieciowego, włączenie i wyłączenie trybu izolacji z infrastruktury sieciowej hosta z możliwością zdalnego połączenia się z nim.

4.19. Analiza ruchu sieciowego.

4.20. System musi posiadać możliwość śledzenia logów pochodzących z urządzeń sieciowych typu UTM zwłaszcza tych najczęściej używanych i polecanych w środowiskach informatycznych. Użytkownik systemu/administrator

musi mieć możliwość filtrowania wyświetlanych informacji, co najmniej poprzez podanie przedziału czasowego i wyboru nazwy zinwentaryzowanego urządzenia typu UTM.

4.21. Monitorowanie problemów i zdarzeń występujących na drukarkach.

4.22. System musi umożliwiać monitorowanie problemów występujących na drukarkach sieciowych wykorzystujących protokół SNMP. System powinien zbierać informacje na temat występujących problemów w osi czasu, umożliwiać tłumienie problemów, wskazywać ich istotność. Ponadto w systemie powinny znajdować się możliwe do pobrania wartości parametrów drukarki oraz informacji na temat dostępności urządzenia.

5. MODUŁ ANALIZY LOGÓW

5.1. Przegląd i analiza logów pochodzących z inwentaryzowanych urządzeń/maszyn.

5.2. Moduł Analizy Logów i Moduł Monitoringu Zasobów musi być powiązany z Modułem Inwentaryzacji i wykorzystywać informację przez niego posiadane. Użytkownik/Administrator systemu musi posiadać możliwość przeglądania i analizowania logów pochodzących z wszystkich hostów dodanych w Module inwentaryzacji. W ramach modułu system musi agregować logi pochodzące z systemów operacyjnych, aplikacji i systemów dziedzinowych. Agregacja logów powinna odbywać się w sposób ciągły i po osiągnięciu limitu związanego z zasobami dyskowymi serwera nadpisywać historyczne logi, począwszy od najstarszych.

5.3. Możliwość analizy tzw. „customowych" logów pochodzących z dowolnego oprogramowania, w tym systemów dziedzinowych.

5.4. System musi posiadać możliwość analizy logów pochodzących z dowolnego oprogramowania, a przede wszystkim z oprogramowania dziedzinowego stosowanego przez Zamawiającego. Użytkownik/Administrator musi mieć możliwość dodawania w module nazwy, lokalizacji i typu tzw. "customowych" logów, które będą agregowane w systemie, w celu późniejszej ich analizy. Zdefiniowane przez Użytkownika/Administratora logi powinny być skorelowane z problemami występującymi na hostach w module monitoringu zasobów. Jeśli wystąpi jakiś problem związany z działaniem np. systemu dziedzinowego, to użytkownik/administrator analizując problemy musi mieć opcję automatycznego przekierowania do logów związanych z tym system.

5.5. Zawansowane filtrowanie, zarówno po hostach jak i zainstalowanym na nich oprogramowaniu.

5.6. Moduł analizy logów musi być wyposażony w zaawanasowaną wyszukiwarkę umożliwiającą użytkownikowi/administratorowi wyszukiwanie i filtrowanie konkretnych logów. System powinien umożliwiać odfiltrowanie logów dla konkretnego hosta, grupy hostów, oprogramowania (w szczególności oprogramowania dziedzinowego - "customlogów"), kategorii, dowolnie wpisanej frazy oraz zakresu czasu (data – godzina, od -do). W Systemie muszą być zastosowane mechanizmy stronicowania, umożliwiające płynne przeglądanie dużej ilości informacji.

5.7. Przegląd i analiza logów dotyczących działań użytkowników.

5.8. W module analizy logów muszą być agregowane logi dotyczące działań użytkowników. W zależności od rodzaju systemu czy oprogramowania zainstalowanego na hoście w logach znajdują się informacje dotyczące różnej aktywności użytkowników (m.in. data zalogowania się użytkownika do systemu, data wylogowania, czy wybór konkretnej funkcjonalności). Użytkownik/Administrator CSB musi mieć możliwość sprawdzenia tych aktywności poprze wyszukanie i odfiltrowanie logów po nazwie użytkownika, typie aktywności, czy dowolnie wpisanej frazie.

5.9. Dostęp do logów historycznych.

5.10. System oprócz dostępu do aktualnych logów musi uwzględniać również logi historyczne. Użytkownik/Administrator musi mieć możliwość przeglądania wszystkich logów agregowanych na zasobach dyskowych. Ilość oraz zakres czasowy agregowanych logów limitowany ma być tylko zarezerwowaną przestrzenią dyskową na serwerze. Po osiągnięciu założonego limitu, system powinien nadpisywać logi począwszy od najstarszych. Użytkownik/Administrator podobnie jak w przypadku logów aktualnych musi mieć możliwość przeszukiwania oraz filtrowania logów historycznych po hostach, oprogramowaniu, czasie i dowolnie wpisanej frazie.

5.11. Informowanie i powiadomienia dotyczące pojawienia się nowych istotnych logów w obrębie całej infrastruktury sieciowej.

5.12. System musi być wyposażony w mechanizmy powiadamiające użytkownika/administratora o pojawieniu się istotnych logów pochodzących z urządzeń infrastruktury sieciowej. System musi posiadać możliwość konfiguracji tych powiadomień pod katem istotności pojawiającego się wpisu w lagach oraz wyboru typu logu (m.in. log systemowy, log "customowy"). Ponadto CSB musi informować użytkownika/administratora o "nowych" zagregowanych logach z poszczególnego hosta. Informacja ta powinna być wyświetlana w systemie po zalogowaniu

użytkownika/administratora, a "nowe" logi to logi dodane do systemu od czasu ostatniego logowania użytkownika/administratora.

5.13. Kategoryzacja istotności logów (np.: informacja, ostrzeżenie, błąd).

5.14. System musi być wyposażony w mechanizmy kategoryzujące logi pod kontem ich istotności. System w szczególności powinien informować użytkownika/administratora o pojawieniu się logów dotyczących nieprawidłowości działania poszczególnych hostów czy oprogramowania na nich zainstalowanych. Następnie w zależności od potrzeb użytkownika/administratora system powinien informować o pojawieniu się ostrzeżeń w oprogramowaniu kluczowym dla użytkownika. Jeśli log dotyczy tylko informacji takiej jak zalogowanie się, czy wyłączenie hosta, to użytkownik/administrator nie powinien otrzymywać powiadomienia (alertu), z wyjątkiem logów które użytkownik/administrator uzna za istotne (pomimo tego, że są skategoryzowane jako informacja).

6. MODUŁ EDR/XDR

6.1. System musi posiadać moduł EDR/XDR, stanowiący zintegrowane rozwiązanie bezpieczeństwa, którego główne funkcje to: monitorowanie i gromadzenie danych o aktywnościach użytkowników i oprogramowania na urządzeniach końcowych, analiza tych danych w celu identyfikacji wzorców zagrożeń.

6.2. Moduł musi posiadać podgląd informacji, alertów i zdarzeń- występujących w środowisku IT. W CSB powinna być możliwość podglądnięcia statystyk incydentów/zdarzeń oraz ich kategorie. Użytkownik/Administrator z poziomu CSB powinien mieć możliwość uzyskania takich informacji jak rodzaj, nazwa lub źródło incydentu, opis, data wykrycia oraz kategoria/priorytet.

6.3. Oprócz posiadanego modułu EDR/XDR, system musi być otwarty tj. posiadać możliwość integracji z rozwiązaniami EDR/XDR innych producentów (co najmniej ESET, WithSecure, Bitdefender). System musi umożliwiać bezpośrednie przekierowanie do zaawansowanych opcji zintegrowanego systemu EDR/XDR (panelu administracyjnego). Dzięki integracji w module musi znajdować się funkcjonalność umożliwiająca użytkownikowi/administratorowi przejście do panelu administracyjnego systemu EDR/XDR udostępniającego zaawansowane opcje takie jak automatyczne reagowanie na zidentyfikowane zagrożenia w celu ich usunięcia lub powstrzymania, powiadamianie personelu bezpieczeństwa o zidentyfikowanych anomaliach.

7. MODUŁ INWENTARYZACJI

7.1. Automatyczny (przy wykorzystaniu agentów), półautomatyczny (przy wykorzystaniu pliku CSV) lub ręczny sposób dodawania hostów oraz oprogramowania zainstalowanego w infrastrukturze sieciowej.

7.2. System musi dawać użytkownikowi/administratorowi możliwość dodawania hostów/urządzeń/ oprogramowania należących do infrastruktury sieciowej na trzy różne sposoby. Pierwszy dotyczy automatycznego wykrywania i dodawania przy wykorzystaniu usług katalogowych. Wszystkie hosty i urządzenia należące do wybranej domeny powinny być automatycznie dodane do CSB wraz z zainstalowanym na nich oprogramowaniem. Drugi i trzeci sposób natomiast ma umożliwiać użytkownikowi/administratorowi dodanie urządzeń/hostów/oprogramowania nie należących do domeny poprzez "ręczne" wpisanie informacji (wypełnienie formularza) lub wczytanie pliku w formacie CSV posiadającego usystematyzowaną strukturę. Moduł inwentaryzacji musi być ściśle skorelowany (powiązany) z pozostałymi modułami systemu CSB.

7.3. Gromadzenie pełnych informacji na temat urządzeń (tj. nazwa hosta, adres IP, główny użytkownik) jak i oprogramowania (nazwa, wersja).

7.4. Informacje o urządzeniach/hostach/oprogramowaniu, które muszą znaleźć się zarówno w formularzu jak i pliku CSV to m.in. dla hosta/urządzenia: nazwa, adres IP, przypisany użytkownik, typ urządzenia/hosta oraz lista zainstalowanego na nim oprogramowania wraz z wersjami. Przy wprowadzaniu "ręcznym" system musi umożliwiać użytkownikowi/administratorowi wybór nazwy i wersji oprogramowania z listy znajdującej się bazie CVE, bądź wpisanie własnych wartości.

7.5. Generowanie raportu w formacie PDF, CSV zawierającego aktualne informację na temat urządzeń oraz oprogramowania zainstalowanego w infrastrukturze sieciowej.

7.6. Moduł musi być wyposażony w funkcjonalności umożliwiającą użytkownikowi/administratorowi wygenerowania raportów z całej dodanej w systemie CSB infrastruktury sieciowej. Raporty powinny być generowane w co najmniej dwóch formatach tj. PDF i CSV oraz powinny zawierać wszystkie istotne informację na temat urządzenia/hosta/oprogramowania m. in takie jak: nazwa, adres, główny użytkownik, lista oprogramowania wraz z wersjami. Ponadto raport musi zawierać m.in. datę i godzinę wygenerowania, nazwę jednostki organizacyjnej oraz imię i nazwisko osoby generującej raport. Dokładny wzór (wizualny) generowanego raportu zostanie ustalony przez zamawiającego w trakcie realizacji zamówienia. Moduł musi umożliwiać generowanie

raportów zarówno z całości jak i z odfiltrowanych urządzeń/hostów/oprogramowania. Użytkownik/Administrator musi mieć możliwość odfiltrowania informacji według co najmniej takich kategorii jak: nazwa użytkownika, grupa urządzeń, dowolnie wpisana fraza.

8. MODUŁ ZGŁASZANIA INCYDENTÓW (e-mail, system help-deskowy)

8.1. Integracja z systemem tiketowym.

8.2. System CSB musi w prosty i intuicyjny sposób umożliwiać użytkownikowi/administratorowi integrację z systemem typu: help-desk. Integracja powinna odbywać się poprzez ustawienie w konfiguracji CSB odpowiedniego adresu e-mail systemu help-deskowego, na który będą wysyłane zgłoszenia dotyczące problemów. Wysyłanie wiadomości ma się odbywać automatycznie po wybraniu przez użytkownika/administratora konkretnego zdarzenia w systemie CSB. Wiadomość e-mail powinna zwierać minimum nazwę jednostki organizacyjnej wysyłającej zgłoszenie, treść zgłoszenia oraz dane zgłaszającego: Imię Nazwisko, adres e-mail, numer telefonu.

8.3. Zgłaszanie incydentu/problemu, który został namierzony przez system.

8.4. Moduł zgłaszania incydentu powinien być ściśle powiązany z modułem monitoringu zasobów, a dokładniej z funkcjonalnością wyświetlającą zidentyfikowane na urządzeniach/hostach problemy. Użytkownik/Administrator systemu powinien posiadać możliwość wyboru problemu namierzonego przez CSB i automatycznego zgłoszenia go do help-desk, poprzez wybranie np. przycisku “Zgłoś Problem”. Po wybraniu opcji zgłoszenia system powinien automatycznie wysyłać do systemu tiketowego zgłoszenie zawierające pełne informacje dotyczące wybranego problemu.

8.5. Bezpośrednie zgłaszane zagrożeń/cyberataków do CSIRT NASK.

8.6. System powinien umożliwiać generowanie co najmniej pliku w formacie pdf ze zgłoszeniem zagrożenia/incydentu/ cyberataku zgodnego z formularzem udostępnianym przez NASK.

9. MODUŁ WYKRYWANIA ZAGROŻEŃ

9.1. Wykrywanie zagrożeń na podstawie powszechnie znanych taktyk i technik wykorzystywanych przez cyberprzestępców udostępnione w ogólnodostępnej bazie danych MITRE ATT&CK.

9.2. System musi umożliwiać użytkownikowi/administratorowi włączenie reguł sprawdzających, czy w jego infrastrukturze sieciowej nie zostały zastosowane taktyki i techniki różnego rodzaju cyberataków. System musi być zintegrowany z powszechnie dostępną bazą danych MITRE ATT&CK zawierającą zbiór taktyk i technik zaobserwowanych przez specjalistów na całym świecie. System powinien posiadać wbudowane reguły umożliwiające wykrycie wielu zagrożeń opisanych w matrycy MITRE ATT&CK, system powinien wskazywać użytkownikowi, przed jakiego rodzaju taktykami i technikami jest chronione jego środowisko IT. System musi pokazywać ilość wbudowanych w nim reguł wraz z ilością włączonych reguł. Użytkownik/Administrator systemu musi mieć możliwość sprawdzenia w systemie, ile reguł dotyczących konkretnej techniki jest włączonych, a ile jeszcze pozostało do wyłączenia. System musi pokazywać pokrycie matrycy MITRE ATT&CK ilościom włączonych/wyłączonych reguł wykrywających cyberzagrożenia.

9.3. Kategoryzacja oraz prezentacja wykrytych zagrożeń.

9.4. System musi umożliwiać użytkownikowi/administratorowi sprawdzenie zagrożeń wykrytych na poszczególnych hostach/urządzeniach zinwentaryzowanych w module inwentaryzacji. Wykryte w systemie zagrożenia musza zawierać informację na temat: daty i czasu ich wystąpienia, rodzaju/treści oraz poziomu istotności. System powinien kategoryzować zagrożenia w co najmniej czterostopniowej skali: poziom zagrożenia niski, średni, wysoki, krytyczny.

9.5. Historia wykrytych zagrożeń.

9.6. System musi posiadać możliwość sprawdzenia historii występowania zagrożeń na hostach/urządzeniach. System musi być wyposażony w rozbudowaną wyszukiwarkę hostów i zagrożeń umożliwiającą między innymi: wyszukanie hosta po nazwie, adresie IP, kategorii/priorytetów, daty wykrycia (przedziału czasowego).

9.7. Wsparcie/automatyczna ochrona po wykryciu zagrożenia.

9.8. System musi posiadać możliwość włączenia “automatycznej ochrony” w wybrane dni tygodnia i w wybranych godzinach. Użytkownik/administrator musi mieć możliwość ustawienia automatycznej ochrony przed wybranymi taktykami i technikami działań cyberprzestępców poza godzinami jego pracy. System musi mieć możliwość ustawienia reakcji na wykrycie zagrożenia w zależności od wybranego poziomu istotności/priorytetu. Ponadto użytkownik/administrator musi mieć możliwość wybrania operacji/akcji z listy predefiniowanych operacji/akcji, która zostanie wykona w razie wykrycia zagrożenia o wybranym priorytecie. Lista operacji/akcji musi umożliwiać

co najmniej wyłączenie/restart hosta/urządzenia, na którym wykryto zagrożenie, przesłanie informacji o wystąpieniu zagrożenia do użytkownika/administratora przy wykorzystaniu poczty e-mail bądź bramki sms, blokowanie hosta, na którym występuje zagrożenie.

10. MODUŁ RAPORTÓW

10.1. Tworzenie zestawień i raportów z danych pochodzących z pozostałych modułów.

10.2. System musi posiadać możliwość tworzenie różnego rodzaju zestawień prowadzących do sporządzenia i wyeksportowania raportu w co najmniej dwóch formatach: csv, pdf. Podczas tworzenia zestawienia użytkownik/administrator musi mieć możliwość wyboru konkretnych hostów bądź grupy hostów, dla których tworzony jest raport. Użytkownik musi posiadać możliwość wyboru modułów oraz priorytetów zdarzeń w nich występujących. Ponadto użytkownik przez administrator musie mieć możliwość wyboru przedziału czasowego, dla którego zostanie wykonany raport.

11. PANEL UŻYTKOWNIKA

11.1. Intuicyjny i przejrzysty panel użytkownika dostępny z dowolnej lokalizacji poprzez stronę www.

11.2. Panel użytkownika CSB powinien być przejrzysty i intuicyjny oraz wykonany przy wykorzystaniu najnowszych standardów i technologii stosowanych we współczesnych systemach informatycznych. Panel użytkownika/administratora sytemu musi być dostępny poprzez podanie odpowiedniego adresu w przeglądarce internetowej. Dostęp do panelu użytkownika musi być bezpieczny poprzez szyfrowanie (zabezpieczenie certyfikatem SSL) oraz tzw. białą listę adresów IP - która pozwala użytkownikowi/administratorowi systemu blokować dostęp z nie znajdujących się na niej adresów. Panel użytkownika powinien również spełniać wymagania związane z dostępnością serwisów użyteczności publicznej dla osób z niepełnosprawnościami - WCAG 2.1 AA.

11.3. Wizualizacja statystyk zdarzeń i logów.

11.4. Panel użytkownika CSB, powinien posiadać elementy umożliwiające prezentację statystyk zdarzeń i logów w sposób zrozumiały, ułatwiający analizę działania środowiska IT pod kątem cyberbezpieczeństwa. Wizualizacja statystyk zdarzeń i logów powinna dotyczyć przede wszystkim ilości “nowych” zdarzeń zarejestrowanych w systemie z podziałem na ich kategorię. Natomiast sposób prezentacji samych logów i zdarzeń musi być przejrzysty jasno podkreślający sklasyfikowanie zdarzenia czy wpisu do logów. Zdarzenia i logi powinny w systemie być wyświetlane w kolejności od najnowszych do najstarszych z możliwości odfiltrowania zakresu czasowego ich prezentowania.

11.5. Wykresy zdefiniowanych parametrów zasobowych aktualizowane na „żywo”.

11.6. Wykresy prezentujące parametry zasobów urządzeń/hostów powinny być aktualizowane w systemie na “żywo”, a dokładnie w zależności od ustaleń z zleceniodawcą system musi aktualizować wykresy w określonych odstępach czasowych (co najmniej, co minutę).

11.7. Filtrowanie wyświetlanych danych wg. hostów, oprogramowania, kategorii zdarzeń itd.

11.8. Panel użytkownika powinien być tak zaprojektowany, aby użytkownik/administrator w sposób intuicyjny mógł filtrować istotne dla niego informacje dotyczące zarówno obciążeń zasobów, zdarzeń (problemów, ostrzeżeń), czy logów. Panel użytkownika musi być wyposażony w wyszukiwarkę umożliwiająca filtrowanie informacji wg. m.in. nazwy hosta/urządzenia, nazwy oprogramowania czy kategorii zdarzeń i logów. Wyszukiwarka w panelu użytkownika powinna znajdować się w widocznym miejscu i posiadać precyzyjnie oznaczone możliwości filtrowania. Użytkownik/Administrator powinien mieć możliwość nakładania na siebie różnych filtrów.

11.9. Intuicyjny panel zarządzania regułami i definiowania “customowych” logów.

11.10. Panel użytkownika powinien być wyposażony w przejrzysty i intuicyjny panel zarządzania regułami (akcjami), na podstawie których użytkownik/administrator informowany jest o zaistniałym w środowisku IT problemie. W panelu tym musi znaleźć się między innymi lista już zdefiniowanych reguł z możliwością ich usunięcia i edycji oraz opcja umożliwiająca dodanie nowej reguły. Reguły w panelu użytkownika powinny być dodawane przy wykorzystaniu przejrzystego i intuicyjnego formularza, w którym użytkownik/administrator musi podać nazwę reguły, dodać warunku oraz wybrać rodzaj operacji, która zostanie wykonana, gdy warunki będą spełnione. Użytkownik/administrator CSB musi mieć możliwość wyboru zarówno warunków, reguł jak i operacji z udostępnionych w systemie opcji. Ponad to panel użytkownika musi być wyposażony w panel zarządzania “customowymi” logami, w którym podobnie jak w przypadku reguł, użytkownik/administrator może wyświetlić listę zdefiniowanych “customlogów” wraz z możliwością ich usunięcia, edycji oraz zdefiniowania nowych. Dodanie do systemu “customlogów” musi być intuicyjne i ma polegać na podaniu unikalnej nazwy definiowanych logów, jego ścieżki (lub ścieżek) dostępu oraz nazwy hosta lub grupy hostów, których ma on dotyczyć.

12. MODUŁ ANALIZY DANYCH AI

12.1. System musi posiadać moduł analizy AI (sztucznej inteligencji) ułatwiający analizę danych agregowanych w systemie. Sztuczna inteligencja w postaci wirtualnego asystenta musi analizować szereg danych pochodzących z pozostałych modułów systemu, co najmniej modułu monitoringu zasobów, modułu logów oraz modułu wykrywania zagrożeń. Wirtualny asystent musi analizować dane pod kątem cyberbezpieczeństwa z naciskiem na określenie poziomu ryzyka oraz sposobu zabezpieczenia.

12.2. Analiza bieżących logów.

12.3. Moduł musi umożliwiać użytkownikowi uruchomienie asystenta AI do przeanalizowania logów po kątem cyberbezpieczeństwa. Asystent po uruchomieniu musi przeanalizować bieżące logi uwzględniając w analizie co najmniej logi skategoryzowane w systemie jako błędy. Asystent AI musi przeanalizować logi pochodzące z każdego hosta/urządzenia dodanego w module inwentaryzacji. Ponadto Asystent AI musi szacować ryzyko zagrożenia określając jego poziom (Ryzko: wysokie, średnie, niskie) podawać wynik analiz w postaci opisu przeanalizowanych błędów (na co wskazują i czego dotyczą) oraz sugerować reguły, które należy włączyć, aby zmniejszyć ryzyko cyberataku. Asystent AI musi pytać użytkownika, czy włączyć automatycznie zabezpieczenia (reguły), których włączenie zaleca po analizie logów. Wynik analizy powinien również sugerować i krótko opisać techniki (z matrycy Mitre ATT&CK) cyberataków, których mogą dotyczyć.

12.4. Analiza wykrytych zagrożeń.

12.5. Moduł musi umożliwić użytkownikowi uruchomienie asystenta AI w celu dokonania analizy raportowanych wpisów w module wykrywania zagrożeń. Asystent do analizy powinien brać wszystkie zagrożenia wykryte obecnego dnia z poszczególnych hostów dodanych w module inwentaryzacji. Wynikiem analizy musi być podsumowanie (opis) najważniejszych informacji zawierający w szczególności dane na temat możliwości wystąpienia cyberataku. Asystent musi sugerować, co należy zrobić, aby przeciwdziałać wykrytym zagrożeniom.

12.6. Analiza problemów.

12.7. Moduł musi umożliwić użytkownikowi uruchomienie asystenta AI w celu przeanalizowania problemów występujących na poszczególnych hostach zaraportowanych w module monitoringu zasobów. Asystent musi dokonać analizy wszystkich problemów niezależnie od ich priorytetów zgłoszonych w danym dniu. W wyniku analizy asystent AI musi sugerować działania ułatwiające użytkownikowi rozwiązanie zgłoszonych w systemie problemów. Sugestie te powinny zawierać informację na temat możliwych przyczyn występowania tych problemów oraz opisać zalecane czynności umożliwiające ich rozwiązanie.

13. MODUŁ THREAT INTELLIGENCE

13.1. System musi mieć moduł umożliwiający analizę danych dotyczących potencjalnych zagrożeń oraz wskaźników kompromitacji (IoC) zidentyfikowanych przez źródła zewnętrzne takie jak AbuseCH. Moduł musi uwzględniać różne kategorie danych (wskaźników kompromitacji) dotyczących co najmniej informacji o złośliwym oprogramowaniu (malware), zagrożeniach sieciowych oraz zgłoszonych złośliwych adresach URL.

13.2. Lista wskaźników – MALWARE.

13.3. Lista wskaźników dotyczących złośliwego oprogramowania musi zawierać istotne informację na temat zgłoszonego zdarzenia. Na liście tej muszą się znaleźć co najmniej informację na temat: czasu zdarzenia, wskaźnika wykrycia, rozmiaru pliku, typu pliku, kategorii zdarzenia, nazwy źródła, daty pierwszego wykrycia, Hash MD5, Hash ssdeep, Hash TLSH. Ponadto użytkownik systemu musi mieć możliwość dodania wybranego zawirusowanego pliku do listy blokowanych plików oraz jeśli dany wskaźnik kompromitacji został określony i opublikowany np. na witrynie virustotal.com, to użytkownik musi mieć możliwość automatycznego przekierowania do źródła z odfiltrowaniem danych do wybranego zdarzenia.

13.4. Lista wskaźników – zagrożenia sieciowe.

13.5. Lista wskaźników dotyczących zagrożeń sieciowych musi zawierać istotne informację na temat zgłoszonego zdarzenia. Lisa ta musi zawierać co najmniej informację na temat: czasu zdarzenia, nazwy złośliwego oprogramowania, opisu zagrożenia, poziomu zaufania, adresu (portu) bądź Hashu pliku, typu wskaźnika, kategorii zdarzenia, czasu pierwszego wykrycia, nazwy źródła oraz dostawcy wskaźnika. Ponadto podobnie jak w przypadku wskaźników malware użytkownik powinien mieć dostęp z poziomy modułu do źródła zawierającego więcej szczegółowych informacji.

13.6. Lista wskaźników – złośliwe adresy URL.

13.7. Lista wskaźników dotyczących złośliwych adresów URL musi zawierać istotne informację na temat zgłoszonych zdarzeń. Lista ta musi zawierać informację dotyczące co najmniej: czasu zdarzenia, adresu URL, statusu adresu, rodzaju zagrożenia, typu wskaźnika, kategorii zdarzenia, nazwy źródła, czasu pierwszego wystąpienia, dostawcy wskaźnika, listy Spamhaus DBL oraz listy SURBL. Ponadto podobnie jak w przypadku poprzednich wskaźników użytkownik powinien mieć dostęp z poziomy modułu do źródła zawierającego więcej szczegółowych informacji.

13.8. Lista blokowanych plików.

13.9. Moduł powinien umożliwiać użytkownikowi wyświetlenie listy plików przez niego zablokowanych na liście wskaźników typu malware. Umieszczone na tej liście pliki muszą być wykrywane przez agentów systemu i blokowane w celu ochronienia poszczególnych hostów. Użytkownik powinien mieć również możliwość ręcznego dodawania plików do tej listy poprzez podanie formatu hash pliku, nazwy, krótkiego opisu, hashu pliku oraz systemu operacyjnego. Użytkownik musi mieć możliwość dodawania do blokady plików dla co najmniej trzech głównych systemów operacyjnych tj. Windows, linux, MAC IOS.

13.10. Wyszukiwanie i filtrowanie.

13.11. Moduł dotyczący wskaźników kompromitacji musi być wyposażony w intuicyjną wyszukiwarkę umożliwiającą zaawansowane wyszukiwanie po treści informacji oraz filtrującej po kategoriach danych oraz wybranym zakresie dat.

14. MODUŁ UEBA

14.1. System musi być wyposażony w moduł UEBA umożliwiający wykrywanie anomalii i podejrzanych zachowań użytkowników. System przy wykorzystaniu modeli ML (Machine Learning) musi automatycznie wykrywać podejrzane aktywności użytkowników UBA oraz nietypową pracę infrastruktury EBA.

14.2. Predefiniowane reguły wykrywania anomalii UEBA.

14.3. System musi być wyposażony predefiniowane reguły wykrywania anomalii przy wykorzystaniu modeli ML dotyczących zarówno analizy behawioralnej użytkowników UBA jak i działania infrastruktury EBA. System musi być wyposażony co najmniej w reguły dotyczące:

14.3.1. podejrzanej aktywności systemów, reguła musi analizować zdarzenia systemowe, takie jak zmiany w rejestrze, zmiany czasu systemowego, zmiany w konfiguracji rozruchu czy instalacje aktualizacji, w celu wykrycia nietypowych działań mogących sugerować próbę manipulacji lub nieautoryzowanego dostępu do systemu,

14.3.2. zapytań DNS do podejrzanych lokalizacji geograficznych, reguła musi analizować zapytania do serwerów DNS znajdujących się w nietypowych krajach w stosunku do standardowego ruchu organizacji, mogących wskazywać na działania związane z malwarem lub wyciekiem danych,

14.3.3. potencjalnego zachowania użytkowników wskazujące na atak typu DDoS, reguła musi umożliwiać detekcje nietypowej intensywności aktywności użytkownika, mogącej sugerować atak rozproszonego typu (DDoS) lub infekcję systemu,

14.3.4. nietypowych zachowań użytkowników w zdarzeniach bezpieczeństwa, reguła musi analizować nietypowe wzorce aktywności użytkowników, takie jak nagły wzrost liczby zdarzeń bezpieczeństwa lub działania poza standardowymi godzinami pracy,

14.3.5. podejrzanych logowań lub eskalacji uprawnień, reguła musi wykrywać anomalie, w zachowaniach takich jak logowania z nieznanych lokalizacji lub kont o wysokich uprawnieniach.

14.4. Parametryzacja i trenowanie zaimplementowanych modeli ML.

14.5. System musi dawać możliwość trenowania zaimplementowanych modeli ML oraz ich automatyczne douczanie. W systemie musi być możliwość wybrania detektora dla wybranej reguły UEBA i podglądnięcia jego parametrów. W systemie musi być możliwość sprawdzenia algorytmów użytych do analizy wraz z dopasowanymi parametrami i oceną ryzyka. Ponadto w ustawieniach detektorów muszą znaleźć się takie informację jak status modelu, data ostatniego treningu oraz metryki cech modelu użyte do analizy wraz ze statystykami (min, max, średnia, najczęstsza wartość itp.). Ponadto użytkownik systemu musi mieć możliwość zmiany parametrów detektora użytego w wybranej regule i przetrenowania modelu na nowo. W przypadku detektorów uczących się na bieżąco zmiany parametrów i uruchomienia detektora na nowo. Trenowanie detektorów musi odbywać się w tle i nie zaburzać działania systemu w zakresie pozostałych detektorów oraz funkcjonalności.

14.6. Prezentacja i wizualizacja wykrytych anomalii.

14.7. System musi umożliwiać użytkownikom prześledzenie rozkładu zdarzeń i anomalii w czasie zaprezentowanych na intuicyjnym wykresie. Ponadto w systemie musi być możliwość sprawdzenia wystąpienia anomalii w formie tabelarycznej. Lista anomalii musi zawierać dane używane w detektorach takie jak np. czas wystąpienia zdarzenia czy nazwa hosta, którego dotyczy zdarzenie. Ponadto system musi posiadać funkcjonalność umożliwiającą wybranie zgłoszonej anomalii i zatwierdzenia jej jako anomalii dopuszczonej przez administratora systemu. Zatwierdzone przez administratora anomalie stanowić mają wykluczenie dla detektorów w kolejnych analizach danych.

14.8. Wektor ataku.

14.9. System musi być wyposażony w funkcjonalność umożliwiającą wybranie zgłoszonej anomalii i sprawdzenie jak potencjalne zagrożenie przebiegało w infrastrukturze IT. Wektor ataku powinien być przedstawiony w postaci interaktywnej mapy sieci, przedstawiającej te elementy infrastruktury, przez które przeszedł potencjalny cyberatak.

14.10. Wyszukiwanie i filtrowanie.

14.11. Moduł musi być wyposażony w intuicyjną wyszukiwarkę umożliwiającą zaawansowane wyszukiwanie po danych biorących udział w analizie (cechy detektorów) oraz filtrującej po kategoriach danych oraz wybranym zakresie dat.

15. MODUŁ OBSŁUGI ZGŁOSZEŃ

15.1. System musi posiadać moduł obsługi zgłoszeń pozwalający na przeglądanie i obsługę zgłoszeń pochodzących od użytkowników z różnych jednostek organizacyjnych. Moduł musi umożliwiać pełną kontrolę nad cyklem życia zgłoszenia – od rejestracji, przez klasyfikację, aż po końcowe rozwiązanie. Moduł musi posiadać adres URL do formularza zgłoszeń umożliwiający użytkownikom z innych jednostek organizacyjnych zgłaszać incydenty lub podejrzane naruszania bezpieczeństwa. Formularz zgłoszeniowy musi zawierać następujące pola: imię i nazwisko, adres e-mail, temat, wiadomość. Wysyłanie zgłoszeń musi być zabezpieczone mechanizmem reCAPTCHA.

15.2. Moduł obsługi zgłoszeń musi posiadać filtr ułatwiający wyszukiwanie zgłoszeń po statusie: nowe, w obsłudze, odrzucone, obsłużone oraz zamknięte. Każde nowe zgłoszenie musi być widoczne w liście zgłoszeń posiadać identyfikator, datę utworzenia, dane zgłaszającego, zgłoszenie oraz status. Administrator musi mieć możliwość zmian statusów zgłoszeń wraz z dodaniem komentarza opisującego wykonane podczas obsługi czynności, a w przypadku odrzucenia zgłoszenia podania przyczyny. Wszystkie zmiany statusów muszą być zapisywane chronologicznie i być dostępne przy każdym zgłoszeniu. Zgłoszenia nie mogą być usuwane z systemu przez użytkowników, każde zgłoszenie musi pozostać w historii modułu.

15.3. Moduł obsługi zgłoszeń musi posiadać oddzielną wyszukiwarkę umożliwiającą użytkownikowi szybkie wyszukanie zgłoszenia.

16. MODUŁ SYMULACJI ATAKU

16.1. System musi być wyposażony w moduł symulacji ataku umożliwiający sprawdzenie zabezpieczeń wprowadzonych w jednostce. System musi dawać możliwość uruchomienia agenta testującego na co najmniej trzech typach systemów operacyjnych (Windows, Linux, iOS). W module symulacji powinna znajdować się krótka instrukcja instalacji agentów na wybranym środowisku operacyjnym. Moduł musi być wyposażony w wyszukiwarkę kontekstową przeszukująca po polach dostępnych dla listy agentów, Scenariuszy oraz utworzonych i wykonanych symulacji.

16.2. Scenariusze ataków.

16.3. System musi być wyposażony w co najmniej 25 różnych scenariuszy umożliwiających testowanie zabezpieczeń. Scenariusze te powinny testować możliwości takie jak min: Screen Capture, Copy Clipbard, Get Chrome Bookmarks, Record microphone, Create staging direcotry, Find files, Stage sensitive files, Compress staged directory, Exfil staged direcotry, Discover Antivirus programs, Scan WIFI networks, Sniff network traficc, Add bookmark, Avoid logs, Disable Windows Defender All, Move Powershell & trage, Clear Logs, Advanced File Search and Stager, Compress staged directory, Exfil Compressed Archive to FTP Server, WMIC Process Enumeration, tsklist Process Enumeration, PowerShell Process Enumeration, UAC Status, SysInternals PSToll Process Discovery, Identify active user, Collect ARP details, Identify system processes, Prefered WIFI, Disript WIFI, Rverse nslookup IP, View remote shares, Copy 54ndc47 (SMB), Start 54ndc47 (WMI), Parse SSH config, Dump history, View admin shares, Run PowerKatz, Find Hostname, Reverse nslookupIP, Mount Share, Start Agent (WinRM), UAC bypass registry, wow64log DLL Hijack, duser/osksupport DLL Hijack, Bypass UAC Medium,

Manx, Levarage Procdump for Isass memory, Signed Binary Execution – odbcconf, Signed Binary Execution – Mavinject oraz wiele innych. Wybór predefiniowanego scenariusza musi odbywać się z poziomu UI systemu.

16.4. Symulacje ataków.

16.5. System musi umożliwiać tworzenie symulacji ataków wykonywanych na dodanych agentach wg. wybranego scenariusza. Podczas dodawania nowej symulacji użytkownik systemu/administrator musi mieć możliwość podania co najmniej: nazwy symulacji, wyboru scenariusza z listy oraz wybrania algorytmu szyfrującego w celu utrudnienia wykrycia podejrzanych zachowań. Użytkownik musi mieć do wyboru, co najmniej algorytm Base64, Base64jumble, Base64noPadding lub wybrać przebieg symulacji bez szyfrowania. Po wykonaniu symulacji w systemie musi znajdować się informacją na temat jej przebiegu na dodanych agentach. Po wyświetleniu szczegółów przebiegu symulacji w systemie muszą znajdować się informację takie jak: Data rozpoczęcia symulacji, nazwa wykonywanej operacji (np. Current USer) nazwa taktyki/techniki z MITRE (np. discovery TI033 – Sytem Owner/User Discovery), nazwa agenta, PID, Status (wykonano, niepowodzenie, brak odpowiedzi) oraz wykonywane polecenie po i przed zaszyfrowaniem. Oprócz polecenia w systemie powinna być również zapisana odpowiedź z testowanego środowiska (agenta).

17. MODUŁ SLA

17.1. System musi być wyposażony w moduł SLA umożliwiający monitorowanie i obsługę incydentów przez administratorów systemu. W Module SLA musi być możliwość obsługi incydentów zgłaszanych przez system w pozostałych modułach, a w szczególności z podatności z Modułu analizy podatności, Problemów z Modułu monitoringu zasobów, zagrożeń z Modułu wykrywania zagrożeń oraz incydentów zgłaszanych przez zintegrowany system EDR w module EDR. Moduł musi być wyposażony w wyszukiwarkę kontekstową umożliwiającą wyszukanie zdarzenia po dostępnych w listach zdarzeń polach. Ponadto system musi umożliwiać filtrowanie zdarzeń SLA po ich statusach.

17.2. Ustawienia SLA.

17.3. System musi być wyposażony w panel konfiguracyjny umożliwiający włączenie/wyłączenie kontroli SLA, nadanie czasu reakcji oraz czasu obsługi zdarzenia (incydentu). Ustawienia te muszą być możliwe dla statusów zdarzeń osobno. W systemie musi być możliwość skategoryzowania zdarzeń poprzez nadawanie im statusów. Każdy incydent pojawiający się w module SLA automatycznie musi być przypisany do kategorii nowe zdarzenie. administratorzy/użytkownicy systemu muszą mieć możliwość zmiany tego statusu na np. segregacja, incydent bezpieczeństwa, fałszywy alarm oraz zdarzenie obsłużone. Ponadto system musi dawać możliwość przypisywania różnych parametrów SLA dla zdarzeń pochodzących z różnych powyżej wymienionych modułów systemu. W ustawieniach SLA użytkownik systemu musi mieć możliwość ustawienia limitów dotyczących ilości wierszy w powiadomieniach, osobno dla powiadomień mailowych i osobno dla powiadomień sms'owych. Moduł SLA musi być również wyposażony w kreator reguł powiadomień SLA umożliwiający administratorom/ użytkownikom tworzenie własnych reguł powiadomień. W konfiguracji reguły musi być możliwość nadania nazwy własnej reguły, zdefiniowania odbiorców powiadomień min: Operator przypisany do typu zdarzenia, grupa odbiorców (np. użytkownicy należący do grupy Administratorzy), właściciela zasobu/usługi oraz zewnętrznego odbiorcy poprzez podanie adresu e-mail i/lub numeru telefonu, wybrania kanału powiadomienie email i/lub sms oraz dodanie warunku, po którego spełnieniu zostanie wysłane powiadomienie. Administrator/użytkownik systemu musi mieć możliwość tworzenia reguł wielowarunkowych, w których użytkownik wybiera operator logiczny OR lub AND określając przy tym czy wszystkie warunki muszą być spełnione, czy wystarczy tylko jeden z nich, aby powiadomienia zostały wysłane. Lista warunków powiadomień musi zawierać min.: Przekroczono czas reakcji SLA, Przekroczono czas obsługi SLA, Przekroczono SLA reakcji o określony czas, Przekroczono czas obsługi o określony czas, Zbliżenie do przekroczenia SLA reakcji, Zbliżenie do przekroczenia SLA obsługi, Osiągnięty priorytet dla CVE, Osiągnięty priorytet dla zagrożenia, osiągnięty priorytet dla alertu (problemu), krytyczny zasób, Zdarzenie na zasobie danych osobowych.

17.4. Lista zdarzeń dla podatności CVE.

17.5. Moduł SLA musi posiadać listę zdarzeń dotyczącą podatności CVE. Każde nowe zdarzenie CVE zgłoszone przez system musi zawierać informację na temat: Identyfikatora, Przypisanego Operatora, Daty utworzenia, numeru CVE, informacji na temat urządzenie i oprogramowania, którego dotyczy, czas reakcji i obsługi, status. W sytuacji, gdy czas reakcji lub obsługi został przekroczony system musi przedstawiać czas opóźnienia zaznaczając go kolorem czerwonym. W module administrator/użytkownik musi mieć możliwość wyświetlenia szczegółów CVE, którego to zdarzenie dotyczy, przypisania operatora, który jest odpowiedzialny za tego typu zdarzenie, przypisania zdarzenia do powiązanego zdarzenia w celu ich zgrupowania oraz reakcji na dane zdarzenie, przy każdym zmianie statusu zdarzenia użytkownik musi mieć możliwość pozostawienia notatki dotyczącej jego obsługi. Lista zdarzeń CVE

musi umożliwiać przeglądnięcie historii obsługi zdarzenia wraz ze wskazaniem zmiany statusu notatki oraz operatora, który zajął się obsługą.

17.6. Lista zdarzeń dla problemów.

17.7. Moduł SLA musi posiadać listę zdarzeń dotyczącą problemów zgłaszanych w module monitoringu zasobów. Każde nowe zdarzenie zgłoszone przez system musi zawierać informację na temat: Identyfikatora, Przypisanego Operatora, Daty utworzenia, treści problemu, informacji na temat urządzenia i oprogramowania, którego dotyczy, czas reakcji i obsługi, status. W sytuacji, gdy czas reakcji lub obsługi został przekroczony system musi przedstawiać czas opóźnienia zaznaczając go kolorem czerwonym. W module administrator/użytkownik musi mieć możliwość wyświetlenia szczegółów problemu, którego to zdarzenie dotyczy, przypisania operatora, który jest odpowiedzialny za tego typu zdarzenie, przypisania zdarzenia do powiązanego zdarzenia w celu ich zgrupowania oraz reakcji na dane zdarzenie, przy każdym zmianie statusu zdarzenia użytkownik musi mieć możliwość pozostawienia notatki dotyczącej jego obsługi. Lista zdarzeń dotyczących problemów musi umożliwiać przeglądnięcie historii obsługi zdarzenia wraz ze wskazaniem zmiany statusu notatki oraz operatora, który zajął się obsługą.

17.8. Lista zdarzeń dla zagrożeń.

17.9. Moduł SLA musi posiadać listę zdarzeń dotyczącą zagrożeń wykrytych w module wykrywania zagrożeń. Każde nowe zdarzenie zgłoszone przez system musi zawierać informację na temat: Identyfikatora, Przypisanego Operatora, Daty utworzenia, powodu wystąpienia zdarzenia, informacji na temat urządzenia, którego dotyczy, czas reakcji i obsługi, status. W sytuacji, gdy czas reakcji lub obsługi został przekroczony system musi przedstawiać czas opóźnienia zaznaczając go kolorem czerwonym. W module administrator/użytkownik musi mieć możliwość wyświetlenia szczegółów zagrożenia, którego to zdarzenie dotyczy, przypisania operatora, który jest odpowiedzialny za tego typu zdarzenie, przypisania zdarzenia do powiązanego zdarzenia w celu ich zgrupowania oraz reakcji na dane zdarzenie, przy każdym zmianie statusu zdarzenia użytkownik musi mieć możliwość pozostawienia notatki dotyczącej jego obsługi. Lista zdarzeń dotyczących zagrożeń musi umożliwiać przeglądnięcie historii obsługi zdarzenia wraz ze wskazaniem zmiany statusu notatki oraz operatora, który zajął się obsługą.

17.10. Lista Incydentów EDR.

17.11. Moduł SLA musi posiadać listę zdarzeń dotyczącą incydentów zgłoszonych w module EDR. Każde nowe zdarzenie zgłoszone przez system musi zawierać informację na temat: Identyfikatora, Przypisanego Operatora, daty utworzenia, zgłoszonej nazwy incydentu, informacji na temat urządzenia, którego dotyczył, czas reakcji i obsługi, status. W sytuacji, gdy czas reakcji lub obsługi został przekroczony system musi przedstawiać czas opóźnienia zaznaczając go kolorem czerwonym. W module administrator/użytkownik musi mieć możliwość wyświetlenia szczegółów incydentu, którego to zdarzenie dotyczy, przypisania operatora, który jest odpowiedzialny za tego typu zdarzenie, przypisania zdarzenia do powiązanego zdarzenia w celu ich zgrupowania oraz reakcji na dane zdarzenie, przy każdym zmianie statusu zdarzenia użytkownik musi mieć możliwość pozostawienia notatki dotyczącej jego obsługi. Lista zdarzeń dotyczących incydentów EDR musi umożliwiać przeglądnięcie historii obsługi zdarzenia wraz ze wskazaniem zmiany statusu notatki oraz operatora, który zajął się obsługą.

18. MODUŁ SOAR

18.1. Moduł SOAR musi stanowić rozszerzenie funkcjonalności systemu klasy SIEM i będzie odpowiadał za automatyzację oraz standaryzację reakcji na incydenty bezpieczeństwa raportowane w systemie SIEM. Moduł ten musi integrować ze sobą różne elementy systemu SIEM takie jak procesy detekcji MITRE, podatności CVE, reguły korelacyjne, czy anomalie UEBA z procesami działań reakcyjnych w jednym, spójnym środowisku. Podsumowując Moduł SOAR musi umożliwiać skrócenie czasu reakcji na incydenty bezpieczeństwa oraz automatyzację reakcji na ich wystąpienie bez konieczności ręcznej interwencji.

18.2. Automatyzacja reakcji na incydenty bezpieczeństwa.

18.3. System musi automatycznie inicjować odpowiednie scenariusze reakcji (playbooki) po wykryciu zdarzenia spełniającego zdefiniowane warunki. Scenariusze muszą uwzględniać co najmniej: korelację zdarzeń z wielu źródeł, poziomu ryzyka (poziom istotności) i priorytetyzację incydentów bezpieczeństwa oraz obszarów zagrożeń i zdefiniowanych grup, automatyczne wykonywanie działań naprawczych (np. izolacja hosta, blokada adresu IP, dezaktywacja kont użytkowników), możliwość warunkowa eskalacji incydentów oraz sposobu alertowania.

18.4. Wizualizacja procesów bezpieczeństwa.

18.5. System musi zapewniać graficzną wizualizację procesów reagowania (playbook) na wykryte incydenty bezpieczeństwa. System musi udostępniać intuicyjne mapy procesów , prezentujące:

- kolejne etapy obsługi incydentu,

- zależności pomiędzy poszczególnymi krokami,
- warunki logiczne,
- punkty automatyzacji oraz eskalacji i alertowania.

18.6. Zarządzanie playbookami.

18.7. Moduł SOAR musi posiadać centralną listę playbooków, zawierającą co najmniej następujące informacje:

- nazwę playbooka,
- datę i godzinę utworzenia,
- liczbę kroków,
- status playbooka (włączony/ wyłączony).

18.8. System musi umożliwiać:

- włączanie i wyłączanie playbooków,
- edycję playbooków,
- trwałe usuwanie playbooków,
- podgląd szczegółowej struktury playbooka.

18.9. Lista playbooków musi posiadać funkcje sortowania oraz eksportu do plików CSV, PDF oraz HTML.

18.10. Tworzenie i edycja playbooków.

18.11. Wymagane jest, aby tworzenie playbooków odbywało się w sposób standaryzowany, poprzez wprowadzenie unikalnej nazwy playbooka, definiowanie kroków reakcji poprzez wybór:

- wyzwalacza,
- skryptu,
- akcji z predefiniowanych list.

18.12. System musi umożliwiać budowę playbooków wieloetapowych, zawierających jeden lub wiele warunków logicznych.

18.13. Wyzwalacze.

18.14. Moduł SOAR musi zawierać listę predefiniowanych wyzwalaczy, obejmujących w szczególności:

- wysokie użycie CPU,
- cykliczne uruchomienie playbooka,
- przeciążenie dysku,
- zbyt wysokie opóźnienia odczytu lub zapisu dysku,
- wysokie wykorzystanie pamięci RAM,
- wykrycie nowego zagrożenia wg. MITRE ATT&CK
- wykrycie nowego zagrożenia na podstawie zdefiniowanych reguł korelacyjnych
- wykrycie nowej podatności CVE,
- wykrycie potencjalnie niebezpiecznej wiadomości e-mail (MS Exchange),
- wykrycie anomalii behawioralnych (UEBA).

18.15. Skrypty.

18.16. Moduł SOAR musi umożliwiać uruchamianie skryptów, w tym w szczególności:

- analizę zajętości katalogów,
- pobieranie listy procesów,
- izolację hosta z sieci,
- zrzut pamięci procesu,
- zatrzymanie procesu,
- anulowanie izolacji hosta.

18.17. Akcje.

18.18. Moduł SOAR musi obsługiwać akcje lokalne oraz akcje wykonywane w systemach zewnętrznych, w szczególności:

- systemy pocztowe (MS Exchange),
- zapory sieciowe (FortiGate),
- systemy zarządzania infrastrukturą sieciową (HPE IMC).

18.19. System musi umożliwiać m.in.:

- zarządzanie wiadomościami e-mail i kwarantanną,
- blokowanie adresów IP na zaporach sieciowych,
- zmianę statusów interfejsów sieciowych,
- wysyłanie powiadomień,
- wykonywanie testów łączności (PING).

18.20. Incydenty SOAR.

18.21. Moduł SOAR powinien zawierać dedykowany obszar zarządzania incydentami SOAR , obejmujący pełny cykl życia incydentu:

- wykrycie zdarzenia,
- korelację,
- uruchomienie playbooków,
- realizację etapów reakcji,
- zatwierdzenie działań (jeśli wymagane),
- zamknięcie incydentu.

18.22. Lista incydentów SOAR.

18.23. System musi udostępniać listę incydentów, która:

- umożliwia filtrowanie po dacie,
- umożliwia wyszukiwanie rekordów,
- umożliwia sortowanie wyników,
- umożliwia eksport do CSV, PDF oraz HTML.

18.24. Każdy incydent musi zawierać:

- nazwę playbooka,
- nazwę hosta lub zasobu,
- opis incydentu,
- datę i godzinę utworzenia,
- typ lub identyfikator incydentu,
- liczbę zrealizowanych etapów.

18.25. Szczegóły incydentu.

18.26. System powinien umożliwiać szczegółowy podgląd incydentu, w tym:

- listę etapów playbooka,
- nazwę etapu,
- typ etapu (wyzwalacz / skrypt / akcja),
- opis,
- datę i godzinę uruchomienia,
- status wykonania,
- dane kontekstowe właściwe dla danego typu akcji (np. odbiorcy wiadomości).

19. WDROŻENIE

19.1. W ramach realizacji zamówienia Wykonawca zobowiązany jest do przeprowadzenia kompleksowego wdrożenia systemu klasy SIEM (Security Information and Event Management) w środowisku teleinformatycznym Zamawiającego, zapewniającego centralne gromadzenie, analizę oraz korelację zdarzeń bezpieczeństwa pochodzących z infrastruktury IT. Wdrożenie obejmuje w szczególności:

19.2. Analizę przedwdrożeniową, obejmującą:

- **19.2.1.** identyfikację źródeł logów i zdarzeń bezpieczeństwa w środowisku Zamawiającego,
- **19.2.2.** określenie zakresu monitorowanych systemów, urządzeń i usług,
- **19.2.3.** ustalenie polityk zbierania i retencji logów,
- **19.2.4.** przygotowanie planu wdrożenia.

19.3. Instalację i konfigurację systemu, w tym:

- **19.3.1.** instalację komponentów systemu klasy SIEM,
- **19.3.2.** konfigurację środowiska pracy systemu,
- **19.3.3.** konfigurację mechanizmów komunikacji z monitorowanymi zasobami,
- **19.3.4.** konfigurację licencji oraz parametrów pracy systemu.

19.4. Integrację z infrastrukturą Zamawiającego, obejmującą w szczególności:

- **19.4.1.** konfigurację zbierania logów z systemów operacyjnych, urządzeń sieciowych oraz innych wskazanych systemów,
- **19.4.2.** integrację z urządzeniami bezpieczeństwa (np. firewall, UTM),
- **19.4.3.** konfigurację zbierania zdarzeń z hostów i urządzeń sieciowych,
- **19.4.4.** integrację z innymi systemami wskazanymi przez Zamawiającego.

19.5. Konfigurację funkcji analitycznych systemu, w tym:

- **19.5.1.** konfigurację reguł korelacji zdarzeń,
- **19.5.2.** konfigurację mechanizmów detekcji incydentów bezpieczeństwa,
- **19.5.3.** konfigurację alertów i powiadomień,
- **19.5.4.** przygotowanie podstawowych dashboardów i raportów.

19.6. Konfigurację monitoringu zasobów i analizy podatności, obejmującą:

- **19.6.1.** uruchomienie mechanizmów wykrywania hostów i urządzeń w sieci,
- **19.6.2.** konfigurację monitoringu dostępności i parametrów systemowych,
- **19.6.3.** konfigurację modułu analizy podatności wraz z aktualizacją bazy podatności.

19.7. Testy powdrożeniowe, obejmujące:

- **19.7.1.** weryfikację poprawności zbierania logów,
- **19.7.2.** sprawdzenie działania reguł korelacji i alertów,
- **19.7.3.** testy integracji z wybranymi systemami,
- **19.7.4.** potwierdzenie prawidłowego działania funkcjonalności systemu.

19.8. Przygotowanie dokumentacji powdrożeniowej, obejmującej co najmniej:

- **19.8.1.** opis architektury wdrożonego systemu,
- **19.8.2.** konfigurację źródeł logów,
- **19.8.3.** opis reguł korelacji i alertów,
- **19.8.4.** instrukcję administracyjną dla Zamawiającego.

19.9. Wsparcie powdrożeniowe, polegające na konsultacjach technicznych oraz pomocy w konfiguracji systemu w początkowym okresie jego eksploatacji.

20. SZKOLENIE Z OBSŁUGI I ADMINISTRACJI SYSTEMEM KLASY SIEM

20.1. W ramach realizacji zamówienia Wykonawca przeprowadzi szkolenie dla minimum 2 administratorów wskazanych przez Zamawiającego w zakresie obsługi i administracji wdrożonym systemem klasy SIEM.

20.2. Szkolenie ma być realizowane równolegle z procesem wdrożenia i fakt przeprowadzenia szkolenia będzie odnotowany w protokole odbioru..

20.3. Zakres szkolenia powinien obejmować co najmniej:

20.3.1. Architekturę systemu klasy SIEM

20.3.1.1. podstawowe komponenty systemu,

20.3.1.2. przepływ danych i zdarzeń bezpieczeństwa,

20.3.1.3. zasady działania mechanizmów korelacji.

20.3.2. Administrację systemem

20.3.2.1. zarządzanie użytkownikami i uprawnieniami,

20.3.2.2. konfigurację podstawowych ustawień systemowych,

20.3.2.3. przegląd logów systemowych.

20.3.3. Zbieranie i analiza logów

20.3.3.1. konfigurację źródeł logów,

20.3.3.2. wyszukiwanie i filtrowanie zdarzeń,

20.3.3.3. analizę zdarzeń bezpieczeństwa.

20.3.4. Obsługę modułu analizy podatności

20.3.4.1. interpretację informacji o podatnościach,

20.3.4.2. analizę podatności w środowisku Zamawiającego,

20.3.4.3. wykorzystanie danych o podatnościach w procesie zarządzania bezpieczeństwem.

20.3.5. Konfigurację alertów i reguł korelacji

20.3.5.1. tworzenie reguł wykrywania zdarzeń bezpieczeństwa,

20.3.5.2. konfigurację progów alarmowych,

20.3.5.3. konfigurację powiadomień.

20.3.6. Tworzenie raportów i dashboardów

20.3.6.1. przygotowanie raportów bezpieczeństwa,

20.3.6.2. tworzenie widoków analitycznych i paneli monitorujących.

20.3.7. Podstawowe scenariusze reagowania na incydenty

20.3.7.1. analiza przykładowych zdarzeń bezpieczeństwa,

20.3.7.2. identyfikacja potencjalnych incydentów,

20.3.7.3. wykorzystanie systemu do wspomagania reagowania na incydenty.

21. ZAKRES WSPARCIA POWDROŻENIOWEGO

21.1. Pod pojęciem „okresu wsparcia powdrożeniowego" Zamawiający rozumie czas, w którym Wykonawca, poza świadczeniem podstawowej gwarancji, zapewnia swoją dostępność w zakresie:

21.2. wsparcia technicznego, obejmującego:

21.2.1. diagnozę i usuwanie błędów konfiguracyjnych,

21.2.2. wsparcie w zakresie optymalizacji działania systemów wdrożonych w ramach zamówienia,

21.2.3. doradztwo w zakresie dalszego dostosowywania parametrów rozwiązań do potrzeb użytkownika.

21.3. Wsparcia merytorycznego, obejmującego:

21.3.1. konsultacje w zakresie prawidłowego korzystania z funkcjonalności systemu,

21.3.2. odpowiedzi na pytania związane z eksploatacją wdrożonych rozwiązań,

21.3.3. wsparcie w tworzeniu i weryfikacji wewnętrznych procedur użytkownika dotyczących wdrożonych rozwiązań.

21.4. Zasady świadczenia wsparcia:

21.4.1. Wykonawca zobowiązany jest zapewnić wsparcie powdrożeniowe przez minimum 30 dni kalendarzowych od daty podpisania protokołu odbioru końcowego..

21.5. Łączny czas reakcji i realizacji otrzymanych zgłoszeń przez Wykonawcę:

21.5.1. dla zgłoszeń zwykłych –w terminie do 2 dni roboczych,

21.5.2. dla zgłoszeń krytycznych (tj. uniemożliwiających korzystanie z podstawowych funkcji systemu) – w ciągu 4 godzin roboczych.

21.6. Dostępność wsparcia:

21.6.1. od poniedziałku do piątku w godzinach pracy urzędu, tj. od 7:45 do 16:00 (z wyłączeniem dni ustawowo wolnych od pracy),

21.6.2. w ramach zaoferowanego okresu wsparcia Wykonawca pozostaje dostępny minimum przez 5 godzin tygodniowo.

21.7. Możliwe formy kontaktu ze wsparciem:

21.7.1. telefon kontaktowy,

21.7.2. adres e-mail dedykowany dla Zamawiającego,

21.7.3. panel zgłoszeń online lub inny system ticketowy.

21.8. Całe wsparcie powdrożeniowe musi być świadczone w języku polskim.