*Załącznik Nr 1*

***Parametry techniczne i funkcjonalne systemu SIEM***

|  |  |  |  |
| --- | --- | --- | --- |
| ***Lp.*** | ***Parametr*** | ***Wymagany*** | ***Oferowany*** |
|  | 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. | TAK |  |
|  | 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.  | TAK |  |
|  | 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. 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.  | TAK |  |
|  | 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.  | TAK |  |
|  | 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.   | TAK |  |
|  | Kod źródłowy dostarczonego rozwiązania musi być wyłączną własnością producenta systemu klasy SIEM i SOAR. Kod źródłowy musi być zamknięty. **System musi pracować w oparciu o architekturę Microsoft Windows.** | TAK |  |
|  | System musi umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji infrastruktury IT również w formie tabelarycznej.   | TAK |  |
|  | 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 (Owners) oraz zespół IT odpowiedzialny za jego obsługę (Custodians).  | TAK |  |
|  | 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. | TAK |  |
|  | 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. | TAK |  |
|  | System musi pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci.  | TAK |  |
|  | 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, MS Word, MS Excel, jpg, png.  | TAK |  |
|  | 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.   | TAK |  |
|  | 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.  | TAK |  |
|  | 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.   | TAK |  |
|  | 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.   | TAK |  |
|  | 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).   | TAK |  |
|  | Mechanizmy modułu dokumentacji elektronicznej muszą umożliwiać powiązanie danych o zasobach z informacjami pozyskanymi w rezultacie skanowania podatności.  | TAK |  |
|  | 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).  | TAK |  |
|  | 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. | TAK |  |
|  | 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. | TAK |  |
|  | 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.  | TAK |  |
|  | System w razie wykrycia incydentów o poważnych konsekwencjach dla organizacji umożliwi automatyczne powiadamianie o incydencie wskazanych pracowników, m.in. za pomocą email i SMS.  | TAK |  |
|  | System powinien umożliwiać automatyczne wyszukiwanie pojedynczych, potencjalnych punktów awarii sieci i systemów IT, których uszkodzenie może spowodować zablokowanie krytycznych usług w organizacji. | TAK |  |
|  | System ma posiadać narzędzia do modelowania zagrożeń, umożliwiając symulowanie potencjalnych scenariuszy bezpieczeństwa. Interfejs mapy sieci musi pozwalać m.in. na:  a. wyznaczenie źródła zagrożenia zasobu teleinformatycznego wraz z wynikiem analizy ryzyka dla tego zagrożenia wyliczanym w sposób automatyczny,   b. wyświetlanie zabezpieczeń zasobu teleinformatycznego przed potencjalnymi źródłami zagrożenia,   c. wyświetlanie zabezpieczeń chroniących zasoby teleinformatyczne przed określonym źródłem zagrożenia,   d. wyświetlanie lokalizacji zasobów określonego rodzaju,   e. wyświetlanie najbardziej narażonych zasobów teleinformatycznych,   f. wyświetlanie ważnych zasobów teleinformatycznych narażonych na awarie.  | TAK |  |
|  | 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). | TAK |  |
|  | 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.   | TAK |  |
|  | System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym. | TAK |  |
|  | System musi umożliwiać wykorzystanie baz reputacyjnych w regułach korelacyjnych. | TAK |  |
|  | 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. | TAK |  |
|  | 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.  | TAK |  |
|  | 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).  | TAK |  |
|  | System musi umożliwiać wykorzystanie baz reputacyjnych w ramach scenariuszy obsługi incydentów (ang. Playbook). | TAK |  |
|  | 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: a. wzbogacanie danych kontekstowych, b. gromadzenie artefaktów danych związanych z incydentem, c. współpraca z innymi członkami zespołu, d. komunikacja w ramach zespołu, e. wykonywanie czynności związanych z reakcją na incydent, f. raportowanie przebiegu incydentu.  | TAK |  |
|  | 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. | TAK |  |
|  | System powinien posiadać zestaw predefiniowanych scenariuszy obsługi (ang. Playbook). | TAK |  |
|  | System musi pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących. | TAK |  |
|  | System powinien pozwalać na przekazywanie aktywnych linków pomiędzy zintegrowanymi systemami, a otwarcie linku powinno bezpośrednio przekierowywać operatora do konsoli systemu zewnętrznego. | TAK |  |
|  | System powinien umożliwiać automatyczną zmianę statusu incydentu na podstawie informacji pobranych z innych systemów np.: identyfikacja IoC. | TAK |  |
|  | System musi umożliwiać zbieranie, przechowywanie i przypisywanie wskaźników kompromitacji (IoC) do incydentów. | TAK |  |
|  | System powinien udostępniać automatyczny raport z wszystkich podjętych działań w ramach incydentu. | TAK |  |
|  | 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. | TAK |  |
|  | 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. | TAK |  |
|  | Proces normalizacji musi odbywać się na bieżąco na etapie rejestrowania danych w systemie. | TAK |  |
|  | 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. | TAK |  |
|  | 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.  | TAK |  |
|  | 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. | TAK |  |
|  | Normalizacja logów musi posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól o nazwę lub kod kraju korzystając z wbudowanej w produkt bazy. | TAK |  |
|  | Normalizacja musi uwzględniać możliwość nadawania kategorii zdarzeń na podstawie wartości parsowanych pól, np. logowanie, wylogowanie, zmiana uprawnień, malware, vulnerability. | TAK |  |
|  | System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych. | TAK |  |
|  | System musi posiadać predefiniowany zestaw parserów. | TAK |  |
|  | 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.  | TAK |  |
|  | System w swoim działaniu musi korzystać z wbudowanych algorytmów uczenia maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników i komputerów. | TAK |  |
|  | 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. | TAK |  |
|  | 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. | TAK |  |
|  | 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. | TAK |  |
|  | System musi zapewniać możliwość budowania modeli zachowania użytkowników dla zebranych danych historycznych ze skonfigurowanego (wskazanego) okresu. | TAK |  |
|  | System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych.  | TAK |  |
|  | Dostarczone rozwiązanie musi być objęte 36 miesięcznym wsparciem producenta lub producentów. Wsparcie musi obejmować bezpłatne dostarczanie aktualizacji oprogramowania oraz reagowanie na zgłaszane błędy systemowe. 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).  | TAK |  |
|  | Rozwiązania SIEM, narzędzia elektronicznej dokumentacji, oraz baza wiedzy mogą być dostarczone w ramach odrębnych rozwiązań, jednakże muszą być zintegrowane w sposób umożliwiający spełnienie wszystkich wymagań z poziomu jednej konsoli. | TAK |  |
|  | Interfejs użytkownika Systemu musi być w języku polskim lub umożliwiać wgranie plików językowych tłumaczących interfejs na język polski. Musi być przejrzysty i konfigurowalny, poprzez pogrupowanie zawartości w bloki tematyczne, co ma umożliwić łatwe i szybkie wyszukiwanie odpowiednich danych.   | TAK |  |
|  | Funkcjonowanie rozwiązania musi być oparta w całości o architekturę „on-premise”, w której przetwarzane dane nie są przesyłane poza infrastrukturę Zamawiającego. | TAK |  |
|  | System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows (minimum Server 2016), Redhat/Oracle Linux (minimum 7.x). | TAK |  |
|  | Dopuszczalne jest dostarczenie rozwiązania jako tzw. wirtualnego 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. | TAK |  |
|  | System musi zapewniać możliwość współpracy z popularnymi bazami danych, a w tym co najmniej z: MS SQL lub Oracle. | TAK |  |
|  | System powinien umożliwiać nadawanie uprawnień do obiektów/modułów systemu dla poszczególnych operatorów lub grup operatorów. | TAK |  |
|  | System musi zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role. | TAK |  |
|  | 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. | TAK |  |
|  | System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać możliwość jej synchronizacji z usługą katalogową Microsoft Active Directory. | TAK |  |
|  | Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień do definiowalnych grup odbiorców (co najmniej: powiadamianie email oraz SMS, opcjonalnie czat). | TAK |  |
|  | 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.   | TAK |  |
|  | System musi umożliwiać przypisanie poziomów krytyczności do monitorowanych zasobów, które będą brane pod uwagę w ewaluacji zagrożeń. | TAK |  |
|  | System musi umożliwiać mapowanie zdarzeń korelacyjnych na framework Mitre ATT&CK. | TAK |  |
|  | 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.   | TAK |  |
|  | 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. | TAK |  |
|  | System musi rejestrować i przechowywać pozyskane dane w wersji pierwotnej oraz w wersji znormalizowanej.   | TAK |  |
|  | System musi zapewniać klasyfikację zdarzeń za pomocą notacji punktowej definiującej ich poziom zagrożenia (ryzyko). | TAK |  |
|  | 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. | TAK |  |
|  | System powinien w formie graficznej prezentować podsumowanie aktualnego stanu bezpieczeństwa, m.in. usługi zagrożone przez incydenty oraz podatności, średni czas obsługi incydentu lub podatności.  | TAK |  |
|  | System pozwoli na prezentację danych w postaci tzw. „Dashboard”, tj. dostosuje zakres i prezentacje danych do potrzeb administratora czy też zalogowanego użytkownika.  | TAK |  |
|  | 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. | TAK |  |
|  | System musi umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach. | TAK |  |
|  | System musi umożliwiać przechowywanie teczek incydentów zawierających dowody, próbki, logi oraz inne powiązane z danym incydentem informacje. | TAK |  |
|  | System musi potrafić wczytywać informacje z innych systemów bezpieczeństwa i traktować je, jako elementy/dowody w teczkach Incydentów. | TAK |  |
|  | System musi umożliwiać powiązanie każdego zdarzenia/incydentu z odpowiednim priorytetem (definiowanym automatycznie z możliwością manualnej zmiany). | TAK |  |
|  | System powinien posiadać możliwość rejestracji zgłoszeń i przekształcenia ich w incydenty bezpieczeństwa z możliwością rozdzielenia uprawnień dla obu tych czynności. | TAK |  |
|  | 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. | TAK |  |
|  | System musi umożliwiać grupowanie manualne w jeden incydent bezpieczeństwa zdarzenia podobne/powiązane np. wielokrotnie raportowane, przez systemy źródłowe, wielokrotnie zgłoszone przez użytkowników. | TAK |  |
|  | System powinien grupować automatycznie w jeden incydent bezpieczeństwa zdarzenia podobne/powiązane np. wielokrotnie raportowane, przez systemy źródłowe, wielokrotnie zgłoszone przez użytkowników. | TAK |  |
|  | 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. | TAK |  |
|  | 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.  | TAK |  |
|  | System musi umożliwiać wykonywanie działań remediacyjnych na stacjach roboczych/serwerach (pobieranie logów, uruchamianie skryptów, weryfikacja rejestrów, itp.). | TAK |  |
|  | System musi umożliwiać przypisywanie i przekazywanie incydentów do operatorów lub grup operatorów | TAK |  |
|  | System musi pozwalać na zbieranie danych i reputacji z systemów klasy Threat Intelligence minimum to IP, FQDN, URL, Hash. | TAK |  |
|  | 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. | TAK |  |
|  | System powinien umożliwiać przeglądanie listy zasobów (urządzeń, systemów, osób, itp.) pod kątem poziomu i ilości incydentów, które są z nimi powiązane. | TAK |  |
|  | System musi mieć możliwość automatycznego informowania o zmianie statusu incydentu (minimum: wygenerowaniu, przypisaniu, przekroczeniu czasu SLA oraz zamknięciu karty incydentu). | TAK |  |
|  | 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.  | TAK |  |
|  | 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. | TAK |  |
|  | System musi zawierać mechanizm integracji ze skanerami podatności co najmniej dwóch producentów oraz co najmniej jednym skanerem podatności dostępnym na zasadach open source. W ramach integracji system musi mieć możliwość uruchamiania skanowania podatności i importowania jego wyników. Silnik skanujący, będący źródłem podatności musi zostać dołączony do oferty systemu bezpieczeństwa. | TAK |  |
|  | Interfejs modułu obsługi incydentów musi prezentować listę podatności zasobów związanych z incydentem.  | TAK |  |
|  | 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.  | TAK |  |
|  | 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. | TAK |  |
|  | System musi zawierać mechanizm definiowania harmonogramów skanowania podatności oraz na ich podstawie automatycznie uruchamiać procesy skanowania i analizowania uzyskanych raportów. | TAK |  |
|  | System musi umożliwiać obsługę podatności w ramach scenariuszy obsługi (playbook). | TAK |  |
|  | System SIEM oraz wszystkie moduły towarzyszące muszą umożliwiać równoczesną pracę co najmniej 10 operatorów oraz objąć monitoringiem min. 200 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. | TAK |  |
|  | System ma gwarantować możliwość elastycznej rozbudowy o dalsze zasoby IT, które w przyszłości zostaną objęte jego działaniem. | TAK |  |
|  | W ramach zamówienia Wykonawca zapewni utrzymanie, aktualizacje i wsparcie systemu w okresie 36 miesięcy, od dnia podpisania protokołu odbioru.  | TAK |  |
|  | Po zakończonym wdrożeniu należy zapewnić bezpłatne 4-dniowe certyfikowane szkolenia (5 osób x 7h) w zakresie użytkowania i administrowania wdrożonego systemu lub systemów dostarczonych w ramach zamówienia. Szkolenie ma zostać prze-prowadzone dla maksymalnie 5 osób (pracownicy sekcji informatyki + IOD) i uwzględniać informacje z zakresu wdrożonego systemu SIEM i SOAR (m.in. zarządza-nie incydentami bezpieczeństwa; korzystanie ze scenariuszy obsługi incydentów, kompletowanie informacji potrzebnych do opracowania raportu o incydencie; szacowanie ryzyka itp.). Szkolenia muszą być zakończone egzaminem i certyfikatem potwierdzającym wspomniane umiejętności wydanym przez producenta systemu. Szkolenia mogą odbyć się w formie zdalnej. | TAK |  |
|  | Wykonawca przekaże Zamawiającemu wszelkie, niezbędne do poprawnego korzystania z wdrożonego rozwiązania, informacje o specyfice systemu oraz informacje techniczne na temat jego prawidłowej eksploatacji (tj. szczegółową dokumentację powdrożeniową oraz instrukcję/instrukcje obsługi). | TAK |  |
|  | W ramach zamówienia wykonawca dostarczy niezbędna licencję oprogramowania bazodanowego na potrzeby serwera bazy danych | TAK |  |
|  | W ramach zamówienia wykonawca uruchomi integracje między systemem SIEM a systemem powiadomień SMS VUTLAN w zakresie powiadomień SMS o zaniku napięcia na jednym urządzeniu UPS znajdującym się w serwerowni głównej. | TAK |  |
|  | Źródła danych - System musi zbierać, parsować i analizować dane niezależnie od tego czy dane będą przesyłane bezpośrednio z urządzenia czy też z dedykowanego serwera Zamawiającego z aplikacją syslog (syslog-NG) co najmniej z poniższych typów oprogramowania i urządzeń posiadanych przez Zamawiającego: a) Antywirus: ESET PROTECT Enterprise b) UTM: Stormshield N910c) systemy operacyjne: WINDOWS, LINUXd) urządzenia sieciowe typu SWITCH i UPS e) systemy aplikacyjne i bazodanowe: ORACLE, MS SQLf) systemy wirtualizacji: VMWARE | TAK |  |

**KOD CPV: 48730000-4**