Załącznik nr 10 do SWZ

Numer postępowania: IGI.271.1.2025

**Opis Przedmiotu Zamówienia**

Niniejszy dokument stanowi szczegółowy opis przedmiotu zamówienia pn.: **„Dostawa i wdrożenie serwera i oprogramowania SIEM/SOAR w ramach realizacji projektu Cyberbezpieczna Gmina Stary Dzików”**

**Ogólne warunki realizacji zamówienia**

1. Dostarczany sprzęt i oprogramowanie muszą być fabrycznie nowe, nieużywane, nieuszkodzone i nieobciążone prawami osób trzecich.
2. Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą znajdować się na liście „end-of-sale” oraz „end-of-support” producenta.
3. Dla dostaw sprzętu informatycznego z systemem operacyjnym Zamawiający wymaga fabrycznie nowego systemu operacyjnego (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego systemu operacyjnego nieużywanego oraz nigdy wcześniej nieaktywowanego na innym urządzeniu oraz pochodzącego z legalnego źródła sprzedaży. W przypadku systemu operacyjnego naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.
4. Dostarczany sprzęt i oprogramowanie muszą pochodzić z oficjalnego kanału dystrybucyjnego w UE.
5. O ile inaczej nie zaznaczono, wszelkie zapisy OPZ zawierające parametry techniczne należy odczytywać jak parametry minimalne. Brak określenia „minimum” oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach.
6. Dostarczany sprzęt musi mieć okablowanie, zasilacze oraz wszystkie inne komponenty, zapewniające właściwą instalację i użytkowanie (np. przewody zasilające itp.).
7. Sprzęt musi być dostarczony ze wszystkimi niezbędnymi do działania i zapewnienia wymaganych funkcjonalności bezterminowymi licencjami na używanie tych funkcjonalności.
8. Sprzęt będzie współpracować z siecią energetyczną o parametrach: 230 V ±10%, 50 Hz.
9. Wykonawca dostarczy przedmiot zamówienia na własny koszt i ryzyko do siedziby Zamawiającego.

**Specyfikacja zamawianego sprzętu i oprogramowania**

Tabela nr 1

|  |  |  |  |
| --- | --- | --- | --- |
| |  | | --- | | **Dostawa i wdrożenie serwera tworzącego platformę sprzętową dla SOC** | | | |
| **Lp.** | **Parametry wyposażenia** |
|  | Pamięć RAM o pojemności minimum 128GB w kościach DDR4, o taktowaniu minimum 3200MHz, kości pamięci wyposażone w system kodowania korekcyjnego ECC, możliwość rozszerzenia pamięci RAM maksymalnie do 12 TB (6TB na procesor). |
|  | Zainstalowane dwa procesory 16 rdzeniowe/32 wątkowe o taktowaniu minimalnym 2.4GHz i TDP max 135W, każdy procesor powinien osiągać wynik minimum 28500 pkt benchmark w teście cpubenchmark.net w okresie nie wcześniej niż 14 dni przed terminem składania ofert. Do oferty należy załączyć wydruk z ww. strony, dopuszcza się wydruk w języku angielskim. |
|  | Zainstalowane dedykowane do danego serwera chłodzenie procesorów umożliwiające poprawną pracę systemu. |
|  | Powinien posiadać mechanizm hot-swap i obsługiwać do 12 dysków. |
|  | Zainstalowany dedykowany kontroler RAID, posiadający możliwość obsługi co najmniej 4 dysków w tym SATA/SAS, kontroler musi wspierać minimum RAID 0,1,5,6,10,50,60. |
|  | Zainstalowane co najmniej dwa dyski SSD klasy enterprise, o pojemności nie mniejszej niż 480GB każdy, dyski przeznaczone na system operacyjny powinny pracować w RAID 1. |
|  | Zainstalowane co najmniej dwa dyski HDD klasy enterprise, o pojemności nie mniejszej niż 4TB każdy. |
|  | Karta sieciowa 10Gb posiadająca minimum 2 porty RJ45. |
|  | Do zestawu dołączony napęd DVD, dopuszczony jest także napęd zewnętrzny. |
|  | Serwer powinien posiadać minimum 4 porty USB 2.0. |
|  | Serwer powinien posiadać zasilanie redundantne z dwoma zasilaczami klasy minimum Platinium o mocy minimum 1300W każdy, dedykowane do danego modelu serwera, zasilacze powinny posiadać mechanizm hot-swap, do zasilaczy dołączone 2 przewody zasilające. |
|  | System operacyjny (przeznaczony dla serwera) opublikowany w 2021 r. lub nowszy, posiadający licencje na obsługę wszystkich rdzeni zamontowanych procesorów oraz utworzenie środowiska wirtualnego obsługującego minimum 6 maszyn wirtualnych. |
|  | Jeżeli dostarczony system operacyjny wymaga dodatkowych licencji dostępowych Wykonawca dostarczy 30 licencji dostępowych przeznaczonych dla urządzeń. |
|  | Serwer powinien być wyposażony w moduł TPM 2.0 lub równoważny. |
|  | Płyta główna dedykowana do serwera posiadająca obsługę minimum 2 procesorów, płyta musi mieć możliwość rozszerzenia funkcjonalności serwera o kolejne karty rozszerzeń pod złącza PCI-e. |
|  | Zintegrowana karta graficzna ze złączem VGA lub pokrewnym, |
|  | Serwer powinien mieć możliwość optymalizacji pod kątem wirtualizacji. |
|  | Sprzęt wyprodukowany zgodnie z normami ISO 9001 lub równoważna, ISO 14001 lub równoważna oraz CE lub równoważna, |
|  | Możliwość weryfikacji na stronie producenta specyfikacji serwera, okresu gwarancji oraz pobrania najnowszych sterowników po podaniu numeru seryjnego sprzętu. |
|  | Zintegrowana karta zdalnego zarządzania posiadająca dedykowany port RJ45. |
|  | Serwer powinien posiadać umożliwiać montaż w szafie RACK, wysokość serwera max 2U, do serwera dołączone szyny montażowe w zestawie. |
|  | Gwarancja na okres minimum 24 miesiące, świadczona na miejscu u klienta (on-site) z czasem reakcji 48h (w dni robocze). Serwis musi być świadczony zgodnie z wymaganiami norm ISO 9001 i ISO 27001 dla serwisu rozwiązań informatycznych. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym gwarancją, uszkodzony dysk twardy pozostaje u Zamawiającego. |
|  | Możliwość rozszerzenia gwarancji do minimum 5 lat w trakcie jej trwania |
|  | Serwis realizowany przez producenta lub autoryzowanego partnera w języku polskim. |
|  | Do obowiązków Wykonawcy będzie należało przygotowanie serwera pod platformę SOC w siedzibie Zamawiającego. Poprzez przygotowanie rozumie się: montaż serwera w szafie serwerowej, skonfigurowanie dysków SSD i HDD w macierze RAID 1, zainstalowanie systemu operacyjnego i utworzenie sześciu serwerów wirtualnych na potrzeby zakupowanego w niniejszym postępowaniu systemu SIEM/SOAR i innych systemów, które będą zakupione w późniejszym czasie. |
|  | Wymagania dodatkowe:  - Gwarantowany czas naprawy – maksymalnie 14 dni roboczych od dnia zgłoszenia wady  - Wymiana wyposażenia na nowe, w przypadku, gdy ta sama wada będzie naprawiana więcej niż 3 razy  - Dostarczenie wyposażenia zastępczego, o parametrach nie gorszych niż będące przedmiotem naprawy, jeżeli czas naprawy wadliwego urządzenia będzie dłuższy niż 7 dni roboczych od dnia zgłoszenia wady  - Wymiana urządzenia lub jego części na wolne od wad, w przypadku wystąpienia wad niemożliwych do usunięcia – w terminie maksymalnie 14 dni roboczych od dnia zgłoszenia wady |

Tabela nr 2

|  |  |
| --- | --- |
| **Dostawa i kompleksowe wdrożenie systemu do wykrywania i zarządzania incydentami, podatnościami i ryzykiem SIEM/SOAR (Security Information and Event Management / Security Orchestration, Automation and Response) z wszystkimi koniecznymi licencjami, umożliwiającego wykrywanie incydentów przy wsparciu mechanizmów uczenia maszynowego oraz zapewniającego automatyzację i orkiestrację ich obsługi** | |
| **Lp.** | **Parametry systemu** |
|  | System powinien 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 |
|  | System powinien 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. |
|  | Dostarczone rozwiązanie powinno 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. |
|  | Dostarczone rozwiązanie powinno 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. |
|  | Interfejs systemu elektronicznej dokumentacji powinien umożliwiać wizualizację informacji o infrastrukturze teleinformatycznej. Wizualizacja powinna obejmować interaktywną mapę logiczną sieci z zaznaczonymi strefami sieci, strefami bezpieczeństwa, urządzeniami sieciowymi, połączeniami, systemami zabezpieczeń IT oraz procesami. |
|  | System powinien umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji infrastruktury IT również w formie tabelarycznej. |
|  | System powinien prezentować techniczne informacje nt. bezpieczeństwa IT z perspektywy działalności organizacji, w tym zapisywanie, wyszukiwanie i prezentowanie co najmniej następujących informacji: procesy biznesowe organizacji oraz wspierające je usługi i powiązane z nimi zasoby IT, klasyfikacja zbiorów informacji przetwarzanych w ramach wskazanych procesów oraz przez wskazane zasoby IT, ważność zasobów IT dla organizacji ze względu na typ przetwarzanych danych oraz wspierane procesy, właścicieli zasobów oraz zespół IT odpowiedzialny za jego obsługę. |
|  | System powinien 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. |
|  | Interfejs interaktywnej mapy sieci powinien 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. |
|  | System powinien pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci. |
|  | System powinien 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. |
|  | Dla zdarzeń zawierających adresy IP interfejs powinien 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. |
|  | System powinien 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. |
|  | 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. |
|  | 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). |
|  | Mechanizmy modułu dokumentacji elektronicznej muszą umożliwiać powiązanie danych o zasobach z informacjami pozyskanymi w rezultacie skanowania podatności. |
|  | System powinien 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). |
|  | 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. |
|  | System powinien 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. |
|  | 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. |
|  | System w razie wykrycia incydentów o poważnych konsekwencjach dla organizacji umożliwi automatyczne powiadamianie o incydencie wskazanych pracowników, m.in. za pomocą email i SMS. |
|  | System powinien umożliwiać automatyczne wyszukiwanie pojedynczych, potencjalnych punktów awarii sieci i systemów IT, których uszkodzenie może spowodować zablokowanie krytycznych usług w organizacji. |
|  | System ma posiadać narzędzia do modelowania zagrożeń, umożliwiając symulowanie potencjalnych scenariuszy bezpieczeństwa. Interfejs mapy sieci powinien pozwalać m.in. na:   1. wyznaczenie źródła zagrożenia zasobu teleinformatycznego wraz z wynikiem analizy ryzyka dla tego zagrożenia wyliczanym w sposób automatyczny, 2. wyświetlanie zabezpieczeń zasobu teleinformatycznego przed potencjalnymi źródłami zagrożenia, 3. wyświetlanie zabezpieczeń chroniących zasoby teleinformatyczne przed określonym źródłem zagrożenia, 4. wyświetlanie lokalizacji zasobów określonego rodzaju, 5. wyświetlanie najbardziej narażonych zasobów teleinformatycznych, 6. wyświetlanie ważnych zasobów teleinformatycznych narażonych na awarie. |
|  | System powinien 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) |
|  | Rozwiązanie powinno 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 |
|  | Importowane do systemu podatności muszą być przeanalizowane pod względem ryzyka jakie mogą wygenerować dla organizacji. W tym celu musi być dostępny mechanizm ich automatycznej priorytetyzacji bazujący na regułach, które wyznaczą dla podatności wymagających obsługi priorytet w oparciu o następujące parametry:   1. strefę bezpieczeństwa w której została wykryta podatność, 2. prawdopodobieństwo obecności intruza lub złośliwego oprogramowania w tej strefie, 3. rodzaj zasobu którego dotyczy ta podatność, 4. ważność tego zasobu dla organizacji, 5. przetwarzane na tym zasobie informacje, np.: dane osobowe, 6. usługi realizowane przez ten zasób, np.: DNS, 7. wartość parametrów CVSS dla podatności, np.: „Confidentiality Impact” = High, 8. poprawność konfiguracji zasobu na którym została wykryta podatność, np.: brak reguł wymuszenia złożoności haseł, 9. szacowane prawdopodobieństwo przełamania zabezpieczeń ze zdefiniowanej strefy, która jest autoryzowana do dostępu do tego zasobu, np.: wysokie prawdopodobieństwa zagrożenia ze strefy Internet dla zasobu z wykrytą podatnością, który świadczy usługę w strefie Internet. |
|  | W systemie musi być dostępny predefiniowany zestaw reguł automatycznej priorytetyzacji wszystkich importowanych podatności oraz interfejs umożliwiający definiowanie własnych reguł umożliwiających zarówno zakwalifikowanie podatności do obsługi jaki i możliwość ich wyłączenia z obsługi w przypadku znikomego zagrożenia dla organizacji. |
|  | System musi posiadać interfejs graficzny do tworzenie własnych reguł korelacyjnych odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie. |
|  | System powinien pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym. |
|  | System musi rejestrować i przechowywać pozyskane logi w postaci surowej (RAW) oraz znormalizowanej. |
|  | System musi posiadać wbudowane mechanizmy zapewniające możliwość pobierania zdarzeń poprzez wykorzystanie RestFull-API, sterownika ODBC, agenta do czytania plików płaskich, protokołów IMAPS, POP3S, MAPI do pobierania wiadomości ze skrzynek poczty elektronicznej oraz obsługi zapytań WQL w ramach protokołu WMI. |
|  | System powinien umożliwiać wykorzystanie baz reputacyjnych w regułach korelacyjnych. |
|  | System musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych zdarzeń umożliwiający ich podział na poszczególne pola, na podstawie których może odbywać się dalsze przetwarzanie oraz wyszukiwanie ich w systemie. |
|  | System musi być wyposażony w graficzny interfejs umożliwiający określenie miejsca składowania logów (wskazania właściwego repozytorium logów) w zależności od zwartości tych logów, gdzie reguły przekierowania muszą umożliwiać definiowanie warunków po wszystkich sparsowanych polach. Przykładowo jeżeli w zdarzeniu znajduje się informacja o danych poufnych to zdarzenie to zostanie przekierowane do repozytorium A, natomiast w przypadku gdy tej informacji nie będzie to zdarzenie zostanie przekierowane do repozytorium B. |
|  | Każde z repozytorium logów musi mieć możliwość definiowania własnych zasad retencji uwzględniających zdefiniowanie okresu przechowywania lub ilości miejsca przeznaczonego na dane repozytorium. Dla każdego z repozytorium w przypadku jego zapełnienia musi być możliwa konfiguracja, która zapewni automatyczne przeniesienie logów do archiwum lub umożliwi ich nadpisanie. |
|  | System musi umożliwiać fizyczne rozdzielenie repozytoriów logów pobieranych z systemów informatycznych od repozytoriów zdarzeń generowanych w ramach systemu, w tym m.in. odseparowanie zdarzeń korelacyjnych na oddzielne repozytoria danych składowane na osobnych serwerach i dedykowanych do tego celu zasobów dyskowych od wszelkich repozytoriów logów. |
|  | Ze względu na możliwość wygenerowania dużej ilości danych przez algorytmy uczenia maszynowego system musi mieć możliwość rozdzielenia ich składowania na osobny serwer i dedykowane zasoby dyskowe. |
|  | System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych w postaci skompresowanej. |
|  | System musi zapewnić mechanizmy bezpieczeństwa dla danych przechowywanych w repozytoriach uniemożliwiające ich nieautoryzowaną modyfikację oraz zapewnić operatorom mechanizmy weryfikacyjne integralność danych. |
|  | System musi udostępniać możliwość konfiguracji automatycznego odrzucenia logów niezawierających istotnych dla zamawiającego informacji. Definiowanie, które logi mają zostać odrzucone i niezapisane w repozytorium logów musi być realizowane za pomocą reguł, które pozwolą zdefiniować warunki po wszystkich sparsowanych polach. |
|  | System musi być wyposażony w graficzny interfejs umożliwiający przeglądanie i przeszukiwanie zarejestrowanych zdarzeń w formie znormalizowanej i pierwotnej. Interfejs musi prezentować wyniki wyszukiwania z zastosowaniem filtrów opartych na wartościach pól, złożonych wyrażeniach logicznych, wskazaniach zakresu czasowego i źródła danych. Interfejs wyszukiwania musi umożliwiać zapisywanie zapytań z możliwością ich ponownego wykorzystania w przyszłości. Tworzenie zapytań musi być możliwe poprzez bezpośrednie wskazanie pola zdarzenia za pomocą wskaźnika myszy i dodanie tego pola do filtra wyszukiwania, wraz z określeniem warunków wyszukiwania przez wyrażenie logiczne. |
|  | System musi zapewniać możliwość utrzymywania dokumentacji sieci, systemów oraz usług, umożliwiającej na gromadzenie i edycję danych istotnych w kontekście oceny generowanych przez system zdarzeń bezpieczeństwa. |
|  | Elektroniczna dokumentacja musi posiadać możliwość wizualizacji w formie interaktywnej mapy sieci, gdzie na pierwszym planie będą widoczne urządzenia zabezpieczeń, strefy bezpieczeństwa oraz połączenia sieciowe wskazujące jakie mechanizmy zabezpieczeń chronią poszczególne strefy bezpieczeństwa. „Kliknięcie” na dowolny z obiektów na pierwszym planie musi pozwolić na podgląd oraz edycję parametrów tego obiektu. Przykładowo po kliknięciu na strefę bezpieczeństwa musi istnieć możliwość definiowania komputerów należących do tej strefy, ich adresacji oraz innych z nimi związanych parametrów. |
|  | System powinien umożliwiać automatyczne dodawanie i usuwanie list referencyjnych na podstawie reguł korelacyjnych umożliwiających zdefiniowanie warunków na podstawie których listy te będą modyfikowane. System powinien umożliwiać definiowanie list referencyjnych łączących unikalne wartości w pojedynczym wierszu np.: login, adres IP, aplikacja, hash, nazwa procesu. |
|  | System powinien 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. |
|  | System powinien 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). |
|  | System powinien umożliwiać wykorzystanie baz reputacyjnych w ramach scenariuszy obsługi incydentów (ang. Playbook). |
|  | System powinien 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:   1. wzbogacanie danych kontekstowych, 2. gromadzenie artefaktów danych związanych z incydentem, 3. współpraca z innymi członkami zespołu, 4. komunikacja w ramach zespołu, 5. wykonywanie czynności związanych z reakcją na incydent, 6. raportowanie przebiegu incydentu. |
|  | System powinien 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. |
|  | System powinien posiadać zestaw predefiniowanych scenariuszy obsługi (ang. Playbook). |
|  | Obsługiwane zdarzenia muszą posiadać zestaw predefiniowanych scenariuszy obsługi (ang. Playbook) oraz pozwalać na tworzenie własnych scenariuszy obsługi oraz ich edycję z poziomu interfejsu graficznego. System musi wspierać funkcję „Drag and Drop” umożliwiającą m.in. na zamianę kolejności realizacji poszczególnych kroków poprzez ich przenoszenie za pomocą myszki komputerowej. |
|  | System powinien pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących. |
|  | System powinien pozwalać na przekazywanie aktywnych linków pomiędzy zintegrowanymi systemami, a otwarcie linku powinno bezpośrednio przekierowywać operatora do konsoli systemu zewnętrznego. |
|  | System powinien umożliwiać automatyczną zmianę statusu incydentu na podstawie informacji pobranych z innych systemów np.: identyfikacja IoC. |
|  | System powinien umożliwiać zbieranie, przechowywanie i przypisywanie wskaźników kompromitacji (IoC) do incydentów. Baza powinna obsługiwać protokół TLP w wersji 2.0 oraz obsługiwać następujące typy wskaźników:   1. fqdn, 2. e-mail, 3. nazwa pliku, 4. ścieżka do pliku, 5. hash, 6. adres IP, 7. klucz rejestru, 8. cmd. |
|  | System musi umożliwiać synchronizację wskaźników kompromitacji (IOC) z platformami dostępnymi publicznie. Wymagane jest aby produkt posiadał gotowy mechanizm pobierania wskaźników z platformy MISP (https://www.misp-project.org/). |
|  | Listy referencyjne muszą mieć możliwość synchronizacji z listami publikowanymi publicznie (np.: „Malicious IPs”, „Malicious domain” czy „Tor Exit Nodes”). |
|  | System powinien udostępniać automatyczny raport z wszystkich podjętych działań w ramach incydentu. |
|  | System powinien 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 powinien umożliwiać m.in. parsowanie warunkowe, parsowanie hierarchiczne, wzbogacanie zdarzeń o dodatkowe pola, mapowanie wartości, czy wykorzystanie gotowych parserów przy tworzeniu nowych. |
|  | System musi umożliwić odbieranie logów wygenerowanych przez systemy zabezpieczeń, systemy sieciowe, systemy operacyjne i aplikacje następującymi protokołami: Syslog, TLS syslog, NetFlow, Windows Event Forwarding. |
|  | Parsowanie warunkowe i hierarchiczne powinno 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. |
|  | Proces normalizacji musi posiadać możliwość optymalizacji, poprzez automatyczny dobór odpowiedniego parsera dla źródła logów w zależności od składni w której te logi są przesyłane. Przykładowo jeżeli logi są przesyłane w standardzie CEF system dobierze odpowiedni parser, w przypadku gdy źródło zmieni format generowania zdarzeń na LEEF system musi automatycznie zmienić parser bez ingerencji operatora. |
|  | System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, obejmującą zmianie wartości tych pól lub dodanie nowych w oparciu o ich wartości lub wzorzec wyszukiwania. Cały proces musi odbywać się na bieżąco na etapie rejestrowania danych w systemie. |
|  | Proces normalizacji powinien wspierać następujące typy składni: CEF, LEEF, URI, SYSLOG (zgodny z RFC 3164) i automatycznie tworzyć na ich podstawie pola i ich wartości zgodne z zasadami określonymi przez te składnie. Parsowanie powyższych składni nie może być realizowane za pomocą wyrażeń regularnych. |
|  | System powinien 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. |
|  | System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) dla zdarzeń z niestandardowych źródeł danych, w oparciu o następujące składnie: CEF, LEEF, URI, XML, JSON, SYSLOG, REGEX. System musi umożliwiać zastosowanie wszystkich typów składni dla pojedynczego zdarzenia, przykładowo pole znormalizowane automatycznie według standardu CEF powinno mieć możliwość dalszej normalizacji np.: zgodnej z URI lub REGEX. |
|  | System powinien 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. |
|  | 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. |
|  | Normalizacja logów powinna posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól o nazwę lub kod kraju korzystając z wbudowanej w produkt bazy. |
|  | Normalizacja powinna uwzględniać możliwość nadawania kategorii zdarzeń na podstawie wartości parsowanych pól, np. logowanie, wylogowanie, zmiana uprawnień, malware. |
|  | System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych. |
|  | System musi posiadać predefiniowany zestaw parserów oraz umożliwiać ich wersjonowanie, aby po wgraniu nowej wersji parsera, w razie przypadku gdy będzie to konieczne przywrócić jedną z poprzednich wersji. |
|  | Modele zachowania użytkowników (UBA) i komputerów (EBA) muszą być tworzone automatycznie na bazie zdarzeń historycznych ze skonfigurowanego (wskazanego) okresu lub zdefiniowanej ilości zdarzeń wymaganych do ukończenia procesu nauczania. Algorytm nauczania musi mieć możliwość konfiguracji sposobu odrzucania wartości skrajnych mogących wpłynąć negatywnie na wyniki procesu nauczania oraz umożliwić odrębne uczenie w ramach zdefiniowanych zakresów czasowych (np.: rozdzielenie zdarzeń do nauczania w godzinach pracy od zdarzeń po godzinach pracy). |
|  | System w swoim działaniu powinien korzystać z wbudowanych algorytmów uczenia maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników i komputerów. |
|  | System musi posiadać zestaw predefiniowanych i konfigurowalnych reguł do automatycznego przyporządkowania użytkowników i zasobów do właściwych profili nauczania, reguły te muszą zapewnić minimum:   1. rozdzielenie procesu nauczania zachowania użytkowników uprzywilejowanych od użytkowników nieuprzywilejowanych, 2. rozdzielenie procesu nauczania zachowania stacji roboczych od serwerów, 3. rozdzielenie serwerów świadczących usługi w sieci Internet od serwerów świadczących usługi lokalnie w organizacji, 4. rozdzielenie procesu nauczania serwerów należących do domeny od pozostałych serwerów. |
|  | System uczenia maszynowego musi posiadać wbudowane mechanizmy nie wymagające żadnej dodatkowej konfiguracji, które po zakończeniu procesu nauki umożliwią detekcję anomalii zachowania użytkowników oraz zasobów (UEBA). |
|  | Wykryte przez mechanizmy uczenia maszynowego anomalie muszą generować zdarzenia, zawierające minimum informację o użytkowniku lub adresie IP na którym została wykryta anomalia oraz wykorzystany algorytm. System musi umożliwiać wykorzystanie tych zdarzeń w celu dalszej korelacji. |
|  | Reguły korelacyjne bazujące na sparsowanych polach i ich wartościach muszą umożliwić:   1. wykrycie dowolnej treści w logach, 2. wykrycie zmiany jednego z kilku pól, 3. wykrycie zaniku wiadomości, 4. wykrycie nowej wartości pola w zadanym okresie czasu, 5. wykrycie incydentu będącego pochodną zdarzeń występujących w określonej kolejności, 6. wykrycie zdefiniowanej ilości przesłanych danych w zadanym okresie czasu, 7. wykrycie chwilowego wzrostu ilości przesłanych danych (tzw. peek) w stosunku do całkowitej ilości przesłanych danych w zadanym okresie czasu, 8. wykrycie sumarycznego wzrostu przesłanych danych w zdefiniowanej strefie bezpieczeństwa, 9. wykrycie zdefiniowanej ilości przesyłanych pakietów w zadanym okresie czasu, 10. wykrycie chwilowego wzrostu (tzw. peek) w stosunku do ilości przesyłanych pakietów w zadanym okresie czasu, 11. wykrycie sumarycznego wzrostu ilości pakietów przesyłanych w zdefiniowanej strefie bezpieczeństwa, 12. wykrycie ilości uruchomionych procesów w zadanym okresie czasu, 13. wykrycie skanowania portów. |
|  | Reguły korelacyjne bazujące na listach referencyjnych muszą umożliwić:   1. wykrycie wystąpienia wartości pola na wybranej liście, 2. wykrycie niewystępowania wartości pola na wybranej liście, 3. wykrycie wystąpienia pary wartości na wybranej liście (np.: proces i obraz pliku z którego został uruchomiony), 4. wykrycie niewystąpienia pary wartości na wybranej liście (np.: nazwa użytkownika wraz aplikacją z którą się wcześniej nie łączył). |
|  | Reguły korelacyjne wykorzystujące atrybuty użytkowników z Active Directory muszą umożliwić:   1. wykrycie czy zdarzenie pochodzi od użytkownika posiadającego konto w Active Directory, 2. wykrycie czy zdarzenie pochodzi od użytkownika posiadającego uprzywilejowane konto w Active Directory, 3. wykrycie czy zdarzenie pochodzi od użytkownika podszywającego się pod konto użytkownika Active Directory (np.: którego e-mail zdefiniowany w Active Directory różni się od e-maila ze zdarzenia mimo, zgodności pozostałych atrybutów konta). 4. wykrycie czy zdarzenie pochodzi od użytkownika należącego do wybranej grupy w Active Directory (np.: Domain Admins), 5. wykrycie czy zdarzenie pochodzi od użytkownika nie należącego do wybranej jednostki organizacyjnej. |
|  | Reguły korelacyjne wykorzystujące atrybuty komputerów z Active Directory muszą umożliwić:   1. wykrycia czy zdarzenie pochodzi z komputera należącego do domeny Active Directory, 2. wykrycia czy zdarzenie pochodzi z komputera z systemem operacyjnym zdefiniowanym w Active Directory, 3. wykrycia czy zdarzenie pochodzi z komputera z wybranej jednostki organizacyjnej. |
|  | Reguły korelacyjne wykorzystujące bazę wskaźników kompromitacji (IOC) muszą umożliwić:   1. wykrycie czy źródłowy adres IP nie jest oznaczony w systemie jako wskaźnik kompromitacji; 2. wykrycie czy HASH występujący w zdarzeniu nie jest oznaczony w systemie jako wskaźnik kompromitacji; 3. wykrycie czy docelowa nazwa hosta (FQDN) nie jest oznaczona w systemie jako wskaźnik kompromitacji; |
|  | Reguły korelacyjne wykorzystujące informacje z elektronicznej dokumentacji muszą umożliwić:   1. wykrycie połączenia z serwera do stacji roboczej w przypadku braku informacji o rodzajach zasobu w korelowanym zdarzeniu, 2. wykrycie połączenia do usługi przez nieautoryzowanego użytkownika, 3. wykrycie nieautoryzowanej usługi na serwerze, 4. wykrycie nieautoryzowanego połączenia do usługi na serwerze, 5. wykrycie nieautoryzowanego połączenia z serwera usług, 6. wykrycie nieautoryzowanego połączenia do sieci Internet. |
|  | Reguły korelacyjne wykorzystujące anomalie w zachowaniu użytkowników (UBA) muszą umożliwić:   1. wykrycie anomalii ilościowej związanej z kontem użytkownika wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania, 2. wykrycie anomalii związanej ze zmianą zachowania na koncie użytkownika, wskazującej na potencjalny atak APT/Ransomware, 3. wykrycie różnych typów anomalii na koncie użytkownika wskazujących na możliwe przejecie konta użytkownika przez cyberprzestępcę lub złośliwe oprogramowanie, 4. wykrycie anomalii związanych z logowaniami użytkowników w ramach sesji VPN. |
|  | Reguły korelacyjne wykorzystujące anomalie w zachowaniu zasobów (EBA) muszą umożliwić:   1. wykrycie anomalii ilościowej związanej z komputerem wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania, 2. wykrycie anomalii związanej ze zmianą zachowania komputera, wskazującej na potencjalny atak APT/Ransomware, 3. wykrycie różnych typów anomalii na komputerze, wskazujących na możliwe przejecie komputera przez cyberprzestępcę lub złośliwe oprogramowanie, 4. wykrycie anomalii związanych z procesami uruchamianymi na serwerach. |
|  | Reguły korelacyjne wykorzystujące podatności na zasobach muszą umożliwić:   1. wykrycie skanowania portów z zasobu posiadającego krytyczne podatności, 2. wykrycie wielokrotnych prób połączeń do zasobu posiadającego krytyczne podatności, 3. wykrycie zdarzeń o wysokim „severity” na zasobach posiadającego krytyczne podatności, 4. wykrycie zdarzeń o wysokim „severity” do zasobów posiadających krytyczne podatności. |
|  | Reguły korelacyjne wykorzystujące wyniki analizy konfiguracji muszą pozwalać na:   1. wykrycie wielokrotnych prób nieudanego logowania do komputera, umożliwiającego ustawienie hasła zawierającego mniej niż 14 znaków, 2. wykrycie wielokrotnych prób nieudanego logowania do komputera, który umożliwia tworzenie haseł nie spełniających następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny |
|  | Reguły korelacyjne wykorzystujące technikach MITRE ATT&CK® muszą umożliwić:   1. wykrycie zdefiniowanej ilości technik w zdarzeniach dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP, 2. wykrycie zdefiniowanej ilości zdarzeń w ramach jednej techniki dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP, 3. wykrycie incydentu będącego pochodną zdarzeń z technik występujących w określonej kolejności na wybranym adresie IP lub zasobie identyfikowanym po nazwie. |
|  | Pojedyncza reguła korelacyjna musi mieć możliwość wzajemnej korelacji wszystkich powyższych mechanizmów umożliwiając, m.in.:   1. wykrycie anomalii na koncie uprzywilejowanym użytkownika, 2. wykrycie ruchu z serwera domenowego do skompromitowanej domeny wykazanej w liście referencyjnej, 3. wykrycie wielu typów anomalii na komputerze z krytyczną podatnością, 4. wykrycie złośliwego oprogramowania na bazie wskaźnika kompromitacji stanowiącego HASH procesu, z którego następuje nieautoryzowana próba dostępu do usługi, 5. wykrycie wielokrotnych prób nieudanego logowania na konto uprzywilejowane, którego hasło nie spełnia następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny. |
|  | System przy wykorzystaniu reguł kwalifikacyjnych musi automatycznie selekcjonować zdarzenia wygenerowane przez reguły korelacyjne, wybierając do obsługi tylko zdarzenia spełniające zdefiniowane warunki (tzw. zdarzenia w obsłudze). Pozostałe zdarzenia powinny być wykluczone z obsługi, ale równocześnie pozostać w systemie, zachowując możliwość ich obsługi na żądanie operatora. Zastosowane reguły selekcji zdarzeń do obsługi muszą równocześnie umożliwiać wyliczenie właściwego dla nich priorytetu. Reguły selekcji i priorytetyzacji zdarzeń w obsłudze muszą uwzględniać:   1. sparsowane pola oraz ich wartości, 2. atrybuty użytkowników z Active Directory, 3. atrybuty komputerów z Active Directory, 4. informacje z elektronicznej dokumentacji. |
|  | Zdarzenia w obsłudze, muszą obsługiwać opcje grupowania polegającą na tym, iż każde kolejne zdarzenie wynikające z reguł korelacyjnych, spełniających tą samą regułę w zdefiniowanym okresie czasu będzie automatycznie dodawane do tego samego zdarzenia w obsłudze. Grupowanie musi odbywać się po:   1. adresie IP, 2. koncie domenowym użytkownika, 3. strefie bezpieczeństwa, 4. zakresie adresów IP. |
|  | System musi umożliwiać grupowanie manualne dla zdarzeń w obsłudze, których powiązanie zostanie wykryte przez operatorów w trakcie obsługi i umożliwiać zgrupowanie ich do jednego zdarzenia. Zgrupowane zdarzenia muszą być podrzędne w stosunku do zdarzenia z którym są grupowane oraz synchronizować z nim statusy. Dla zdarzeń przetwarzanych przez operatora, zmiana statusu głównego zdarzenia musi wymusić zmianę statusu pozostałych. Na przykład: zamknięcie nadrzędnego zdarzenia musi zamykać też wszystkie podrzędne. Na liście zdarzeń oraz w podglądzie każdego zdarzenia powinna się pojawić informacja o zdarzeniach z nim powiązanych. |
|  | Obsługiwane zdarzenia muszą zapewniać historyczność, obejmującą wszystkie aktywności realizowane w ramach poszczególnych statusów. Aktywności muszą uwzględniać zarówno akcje realizowane w ramach samego systemu (m.in. zmiana priorytetu czy przekazanie zdarzenia innemu operatorowi). Dodatkowo historia musi też zawierać wszelkie komentarze wpisywane przez operatorów. |
|  | Dla każdego obsługiwanego zdarzenia system powinien udostępniać automatyczny raport obejmujący wszystkie podjęte działania wraz z komentarzami operatorów. |
|  | W ramach obsługi zdarzeń system musi automatycznie porównywać wskaźniki kompromitacji zidentyfikowane w bieżącym zdarzeniu względem wszystkich wskaźników pozyskanych do tej pory w ramach dotychczasowej obsługi. Na przykład: jeżeli w obsługiwanym zdarzeniu znajduje się FQDN oraz HASH to system musi automatycznie porównać je ze wszystkimi wskaźnikami typu FQDN oraz HASH, zebranymi do tej pory w obsługiwanych zdarzeniach bez względu na to czy wskaźniki te zostały wpisane ręcznie czy zostały pozyskane automatycznie z innych systemów. |
|  | System powinien 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. |
|  | System powinien 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. |
|  | System powinien 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. |
|  | System powinien zapewniać możliwość budowania modeli zachowania użytkowników dla zebranych danych historycznych ze skonfigurowanego (wskazanego) okresu. |
|  | Rozwiązanie musi zapewniać elastyczną i skalowalną architekturę, której rozbudowa nie będzie wymagała zakupu dodatkowych licencji, zapewniając tym samym możliwość wydzielania następujących warstw funkcjonalnych zwanych dalej kolektorami, do instalacji na osobnych serwerach bądź maszynach wirtualnych:   1. kolektor parsujący; 2. kolektor logów; 3. kolektor korelacyjny; 4. kolektor zdarzeń; 5. kolektor sztucznej inteligencji; 6. kolektor reakcyjny; 7. kolektor kontrolujący. |
|  | Kolektor parsujący powinien być odpowiedzialny za odbieranie i parsowanie logów a następnie ich przesyłanie zarówno postaci surowej jak i sparsowanej do odpowiednich kolektorów logów, zgodnie z regułami ich przekierowania zdefiniowanymi w jednym miejscu dla wszystkich kolektorów w interfejsie graficznym. Pojedynczy kolektor parsujący musi zapewniać wydajność co najmniej 20 tysięcy zdarzeń na sekundę w trybie ciągłym oraz posiadać bufor do obsługi natłoku w rozmiarze miliona zdarzeń. |
|  | Kolektor logów powinien być odpowiedzialny za przechowywanie logów zarówno w postaci surowej jak i sparsowanej oraz przechowywać pliki indeksów. Logi muszą być przechowywane w postaci skompresowanej oraz kolektor musi zapewnić mechanizmy zabezpieczające je przed nieautoryzowaną modyfikacją (np.: Certyfikat cyfrowy czy funkcja skrótu). Pojedynczy kolektor logów powinien mieć wydajność co najmniej 10 tyś zdarzeń na sekundę w trybie ciągłym oraz posiadać bufor do obsługi natłoku w rozmiarze miliona zdarzeń. |
|  | Kolektor korelujący powinien umożliwiać korelację logów oraz ich agregację zgodnie z regułami korelacyjnymi zdefiniowanymi w jednym miejscu dla wszystkich kolektorów w interfejsie graficznym. |
|  | Kolektor zdarzeń powinien umożliwiać składowanie zdarzeń stanowiących wyniki korelacji oraz umożliwiać ponowne wykorzystanie tych zdarzeń w kolejnych regułach umożliwiając tym korelację zależności pomiędzy nimi. Zdarzenia muszą być przechowywane w postaci skompresowanej oraz kolektor musi zapewnić mechanizmy zabezpieczające je przed nieautoryzowaną modyfikacją (np.: Certyfikat cyfrowy czy funkcja skrótu). |
|  | Kolektor sztucznej inteligencji powinien zawierać wiedzę pozyskaną ze środowiska obejmującą zarówno linię trendu zachowania użytkowników oraz zasobów obejmujące mechanizmy uczenia maszynowego jak i algorytmy sztucznej inteligencji pozwalające na wypracowanie nowej wiedzy wynikającej z korelacji wyników wiedzy wypracowanej poprzez inne metody. |
|  | Kolektor reakcyjny musi umożliwiać automatyczną reakcję na wykryte zagrożenia, która nie będzie wymagała żadnej interakcji ze strony użytkownika, chyba że taka będzie dodatkowo zdefiniowana. W celu automatyzacji reakcji musi posiadać funkcjonalność systemu PAM lub być z nim dostarczony w celu przechowywania danych uwierzytelniających oraz kluczy API potrzebnych do automatyzacji reakcji. |
|  | Architektura rozwiązania musi w pełni wspierać konfigurację niezawodnościową, zapewniającą zarówno pełną redundancję w zakresie, odbierania logów i ich przechowywania, korelacji oraz reakcji na zagrożenia jak i możliwość zastosowania konfiguracji o ograniczonej redundancji do najważniejszych dla zamawiającego źródeł danych. |
|  | Konfiguracja niezawodnościowa musi wspierać możliwość zastosowania stosu kolektorów zastępczych które zostaną uruchomione w przypadku awarii stosu podstawowego, przy czym wszystkie one muszę być zarządzane centralnie z poziomu tej samej konsoli co kolektory podstawowe. |
|  | Kolektory muszą mieć zapewnione mechanizmy automatycznej aktualizacji zarówno w zakresie parserów czy reguł korelacyjnych jak i wersji oprogramowania, przy czym aktualizacja musi odbywać się z poziomu centralnego systemu zarządzania. |
|  | Rozwiązanie musi zapewnić konsole do aktualizacji pozwalającą na wybór dodatkowych pakietów reguł czy parserów udostępnianych w ramach aktywnego wsparcia producenta w formie usługi, każda aktualizacja musi wspierać mechanizm wersjonowania pozwalający zarówno aktualizację jaki i przywracanie poprzednich wersji reguł i parserów. |
|  | Rozwiązanie musi mieć możliwość skalowania się poprzez dodawanie kolejnych maszyn wirtualnych lub maszyn fizycznych z nowymi typami kolektorów, przy czym dodawanie nowych komponentów nie może wiązać się z koniecznością zakupu nowej licencji, ani posiadać ograniczeń licencyjnych związanych z ilością lub rozmiarem przechowywanych zdarzeń i/lub danych. Jedynym ograniczeniem w tym zakresie (dotyczącym przechowywanych danych) może być rozmiar przestrzeni dyskowej. |
|  | Skalowanie przez dodawanie nowych kolektorów musi zwiększać wydajność rozwiązania zgodnie z wartościami zadeklarowanymi przez producenta, przykładowo dwa kolektory logów muszą zapewnić dwukrotną wydajność rozwiązania czyli minimum 20 tyś zdarzeń na sekundę. Przy czym całe rozwiązanie nie może ograniczać ilość zastosowanych kolektorów. |
|  | System musi być zintegrowany z zewnętrznymi bazami o zagrożeniach (Threat Inteligence Feeds - TI) oraz zawierać już zintegrowany zestaw niekomercyjnych (open source) lub komercyjnych baz zagrożeń. |
|  | Rozwiązanie musi mieć możliwość korelacji informacji z baz zagrożeń z danymi otrzymywanymi w czasie rzeczywistym. Korelacja ta ma odbywać się w pamięci systemu względem otrzymywanych danych o zdarzeniach (event data). |
|  | System musi mieć możliwość korelacji informacji z baz zagrożeń z danymi historycznymi |
|  | System musi mieć możliwość odpytywania (ręcznego lub automatycznego) zewnętrznych źródeł reputacji takich jak np. VirusTotal. |
|  | System musi mieć możliwość wizualizacji informacji w oparciu o kategorie MITRE ATT&CK dla standardowego zbioru wbudowanych reguł. |
|  | Pulpity administracyjne (dashboards) muszą mieć możliwość wspólnej prezentacji. |
|  | Rozwiązanie musi mieć możliwość integracji z innymi systemami do obsługi zgłoszeń poprzez API (ticketing system) oraz mieć wbudowany mechanizm obsługi zgłoszeń (ticketing system) niezależny od obsługi alarmów/incydentów. |
|  | System musi wpierać mechanizmy typu Machine Learning w oparciu o zgromadzone zdarzenia. Musi być możliwe użycie przynajmniej 5 różnych rodzajów mechanizmów Machine Learning wraz z możliwością ich ręcznego wybrania oraz działania w trybie automatycznym. W wyniku działania opisanych mechanizmów Machine Learning system SIEM ma tworzyć model bazowy zachowania oraz umożliwiać wykrycie odchyleń i anomalii od niego. Zadania Machine Learning mają mieć możliwość dystrybuowania ich pomiędzy elementy warstwy korelującej i/lub zarządzającej. Mechanizmy Machine Learning mają również umożliwiać wsparcie dla podejmowania decyzji przy rozwiązywaniu incydentów w systemie SIEM. |
|  | W celach weryfikacji zgodności produktu z wymaganiami, musi być on dodatkowo oferowany przez autoryzowanego dystrybutora, dostarczającego produkty z obszaru cyberbezpieczeństwa na rynku polskim, który w przypadku jakichkolwiek wątpliwości Zamawiającego, związanych z wymaganymi funkcjonalności będzie mógł je potwierdzić lub im zaprzeczyć. |
|  | Dostarczone rozwiązanie nie może działać w oparciu o oprogramowanie otwarte (ang: open source) w następującym zakresie funkcjonalnym: składowanie, parsowanie, korelacja logów, algorytmy uczenia maszynowego, analiza zachowania użytkowników i zasobów (UEBA), mechanizmy reakcji/ scenariusze reakcji (SOAR). Zamawiający nie zaakceptuje systemu, który wykorzystuje mechanizmy typu open source np.: Elastic Search, OSSIM, Snort, The Hive, AlienVault itd. lub został stworzony przez modyfikację oprogramowania otwartego. |
|  | Interfejs użytkownika Systemu powinien 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. |
|  | Funkcjonowanie rozwiązania musi umożliwiać konfigurację „on-premise”, w której wszystkie funkcjonalności oraz przetwarzanie danych będzie się odbywać całkowicie w infrastrukturze Zamawiającego, zapewniając tym samym możliwość konfiguracji systemu w strefie odseparowanej od sieci Internet. |
|  | 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. |
|  | System powinien zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role. |
|  | System powinien 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. |
|  | System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać możliwość jej synchronizacji z usługą katalogową Microsoft Active Directory. |
|  | System musi umożliwiać analizę konfiguracji systemów IT poprzez ich skanowanie bezpośrednio w ramach mechanizmów dostępnych w samym rozwiązaniu oraz poprzez integrację ze skanerami podatności. Oczekiwanym wynikiem analizy jest lista niezgodności (np.: czy na zasobie jest ustawione wymuszanie zmiany haseł w zadanym okresie czasu). |
|  | System powinien posiadać zestaw predefiniowanych reguł weryfikacji konfiguracji zasobów IT. |
|  | Rozwiązanie powinno posiadać funkcjonalność wysyłania powiadomień do definiowalnych grup odbiorców (co najmniej: powiadamianie email oraz SMS, opcjonalnie czat). |
|  | System powinien 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. |
|  | System powinien umożliwiać przypisanie poziomów krytyczności do monitorowanych zasobów, które będą brane pod uwagę w ewaluacji zagrożeń. |
|  | Korelacja musi odbywać się na bieżąco na etapie rejestrowania danych w systemie a mechanizm tworzenie reguł musi uwzględniać:   1. sparsowane pola oraz ich wartości, 2. listy referencyjne, 3. atrybuty użytkowników z Active Directory, 4. atrybuty komputerów z Active Directory, 5. bazę wskaźników kompromitacji (IOC), 6. informacje z elektronicznej dokumentacji, 7. anomalie w zachowaniu użytkowników (UBA), 8. anomalie w zachowaniu zasobów (EBA), 9. podatności na zasobach, 10. wyniki analizy konfiguracji, 11. techniki MITRE ATT&CK®, |
|  | System musi umożliwiać mapowanie zdarzeń bezpieczeństwa na poszczególne techniki z bazy wiedzy MITRE ATT&CK® oraz zapewniać mechanizmy filtrowania zdarzeń po tych technikach oraz wyświetlania szczegółów związanych z daną techniką, w szczególności:   1. id techniki, 2. taktykę, 3. platformy których dotyczy, 4. potencjalne źródła, 5. opis zagrożenia, 6. mityzację, 7. sposób detekcji, 8. referencje. |
|  | Zdarzenia w obsłudze muszą obejmować statusy właściwe dla procesu obsługi zdarzeń, minimum to:   1. nowe zdarzenie – jako zdarzenie zarejestrowane w systemie, 2. segregacja – segregacja i kwalifikacja zdarzeń, 3. incydent bezpieczeństwa – zdarzenie zakwalifikowane jako incydent bezpieczeństwa, 4. fałszywy alarm – zdarzenie zakwalifikowane jako fałszywy alarm, 5. zdarzanie obsłużone – zdarzenie, które zostało obsłużone w systemie.   System musi także zapewniać możliwość ich edycji w zakresie dodawania (np.: wydzielenie z segregacji statusu kwalifikacji) lub usuwania statusów oraz konfiguracji przejść pomiędzy nimi. Przykładowo: umożliwiać przejście ze statusu „incydent bezpieczeństwa” do statusu „zdarzenie zamknięte”, ale zablokować zmianę ze statusu „incydent bezpieczeństwa” na status „fałszywy alarm”. |
|  | System pozwoli na prezentację danych w postaci tzw. „Dashboard”, tj. dostosuje zakres i prezentacje danych do potrzeb administratora czy też zalogowanego użytkownika. |
|  | System musi pozwalać na tworzenie dedykowanych dashboard’ów obejmujących:   1. zestaw wykresów dla bieżącego użytkownika, 2. zestaw wykresów dla wybranego użytkownika, 3. zestaw wykresów dla roli zdefiniowanej w systemie, np.: administratorzy systemu, 4. zestaw wykresów dla wybranego zespołu obsługi, np.: operatorzy SOC (Security Operations Center). |
|  | System musi zapewniać zestaw predefiniowanych dashboard’ów obejmujących następujące wykresy:   1. wykres przedstawiający status klasyfikacji zdarzeń, który uwzględnia:  * ilość zdarzeń nowych i niesklasyfikowanych, * ilość zdarzeń sklasyfikowanych jako incydenty bezpieczeństwa, * ilość zdarzeń sklasyfikowanych jako fałszywe alarmy,  1. wykres przedstawiający skale zagrożeń, który uwzględnia:  * ilość zasobów krytycznych na których są obsługiwane zdarzenia, * ilość zasobów niekrytycznych na których są obsługiwane zdarzenia,  1. wykres przedstawiający źródła zagrożeń, który uwzględnia:  * ilość nowych zdarzeń dotyczących użytkowników, * ilość podjętych zdarzeń dotyczących użytkowników, * ilość nowych zdarzeń dotyczących zasobów, * ilość podjętych zdarzeń dotyczących zasobów,  1. wykres przedstawiający poziom zagrożeń, który uwzględnia:  * ilość nowych zdarzeń w podziale na priorytety, * ilość podjętych zdarzeń w podziale na priorytety,  1. wykres przedstawiający czas obsługi zagrożeń, który uwzględnia:  * ilość zdarzeń zarejestrowanych w bieżącym dniu, * ilość zdarzeń zarejestrowanych w ostatnim tygodniu, * ilość zdarzeń zarejestrowanych w ostatnim miesiącu, * ilość zdarzeń zarejestrowanych wcześniej niż w ostatnim miesiącu,  1. wykres przedstawiający zagrożone usługi, który uwzględnia:  * ilość usług krytycznych zagrożonych przez obsługiwane zdarzenia, * ilość pozostałych usług zagrożonych przez obsługiwane zdarzenia,  1. wykres przedstawiający zagrożone dane, który uwzględnia:  * ilość nowych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje, * ilość podjętych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje, * ilość nowych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje, * ilość podjętych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje,  1. wykres przedstawiający skale podatności, który uwzględnia:  * ilość zasobów krytycznych na których są obsługiwane podatności, * ilość zasobów niekrytycznych na których są obsługiwane podatności,  1. wykres przedstawiający czas obsługi podatności, który uwzględnia:  * ilość podatności zarejestrowanych w bieżącym dniu, * ilość podatności zarejestrowanych w ostatnim tygodniu, * ilość podatności zarejestrowanych w ostatnim miesiącu, * ilość podatności zarejestrowanych wcześniej niż w ostatnim miesiącu,  1. wykres przedstawiający wagę podatności, który uwzględnia:  * ilość nowych podatności w podziale na priorytety, * ilość podjętych podatności w podziale na priorytety, |
|  | Nawigacja w ramach „Dashboard’u” musi wspierać opcję typu „Drill down” w następującym zakresie:   1. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej zdarzeń w obsłudze musi przenieść operatora systemu do listy tych zdarzeń z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres, 2. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej podatności musi przenieść operatora systemu do listy tych podatności z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres, 3. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej użytkowników (UBA) musi przenieść operatora systemu do listy tych użytkowników z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres, 4. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej zasobów (EBA) musi przenieść operatora systemu do listy tych zasobów z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres, 5. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej wybranych zdarzeń korelacyjnych musi przenieść operatora systemu do listy prezentującej te zdarzenia z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres, 6. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej wybranych logów musi przenieść operatora systemu do listy prezentującej te logi z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres. |
|  | System powinien 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. |
|  | System powinien umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach. |
|  | Definiowanie reguł wykrywania musi bazować na sparsowanych polach oraz wyszukanych zależnościach między różnymi zdarzeniami z wielu źródeł oraz po aktywacji automatycznie uzupełnić elektroniczną dokumentację o następujące informacje:   1. nowe zasoby wykryte w sieci, 2. typy wykrytych zasobów (np.: serwer lub stacja robocza), 3. zastosowane na nich zabezpieczenia, 4. usługi z którymi się komunikują, 5. nowe usługi wykryte na zasobie, 6. komunikacje do usług wykrytych na zasobie. |
|  | System musi umożliwiać uwiarygodnianie uzyskiwanych informacji na bazie wartości progowych osiągniętych w zadanej jednostce czasu i dopiero po ich uwiarygodnieniu uzupełniać automatycznie elektroniczną dokumentację. |
|  | System powinien umożliwiać przechowywanie teczek incydentów zawierających dowody, próbki, logi oraz inne powiązane z danym incydentem informacje. |
|  | System powinien potrafić wczytywać informacje z innych systemów bezpieczeństwa i traktować je, jako elementy/dowody w teczkach Incydentów. |
|  | System powinien umożliwiać powiązanie każdego zdarzenia/incydentu z odpowiednim priorytetem (definiowanym automatycznie z możliwością manualnej zmiany). |
|  | System powinien posiadać możliwość rejestracji zgłoszeń i przekształcenia ich w incydenty bezpieczeństwa z możliwością rozdzielenia uprawnień dla obu tych czynności. |
|  | System powinien posiadać zestaw predefiniowanych reguł do automatycznego uzupełniania elektronicznej dokumentacji, których uruchomienie będzie automatycznie aktualizować elektroniczną dokumentację bez ingerencji operatora. |
|  | Interfejs interaktywnej mapy sieci musi posiadać mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT który został zdefiniowany w elektronicznej dokumentacji oraz nazwę usługi której ta komunikacja dotyczy. |
|  | Rozwiązanie nie może posiadać ograniczeń licencyjnych związanych z rozmiarem gromadzonych danych w jednostce czasu. Przykładowo nie może być limitowana licencyjnie ilość bajtów danych w jednostce czasu (KB, GB, etc.) |
|  | Poszczególne kolektory zdarzeń oraz logów muszą zapewniać przechowywanie danych zarówno na maszynach wirtualnych jak i na dyskach sieciowych. |
|  | Kolektor logów musi mieć możliwość składowania zbieranych danych zarówno w formie surowej (raw event log) jak i w formie sparsowanych danych (parsed event log)/danych znormalizowanych. |
|  | Rozwiązanie nie może wykorzystywać klasycznej relacyjnej bazy danych (tj.: MS SQL, Postgresql, MySQL, Oracle, itp.) celem gromadzenia i przechowywania danych związanych ze zbieranymi zdarzeniami. Rozwiązanie musi wykorzystywać w tym celu nowoczesną bazę taką jak na przykład noSQL lub OLAP lub autorskie rozwiązanie producenta. |
|  | Rozwiązanie musi zapewniać możliwość zbudowania większej ilości replik danych, aby zapewnić niezawodność przechowywania oraz możliwość zbudowania struktury rozproszonej, zapewniającej większą wydajność zapisu i wyszukiwania. |
|  | Klasyczne relacyjne bazy danych mogą być wykorzystywane jedynie do przechowywania szablonów, raportów, konfiguracji, bazy CMDB oraz innych ustrukturyzowanych informacji. |
|  | Rozwiązanie musi zapewniać możliwość automatycznego budowania kontekstu poprzez wykrywanie urządzeń oraz komputerów mających swoją reprezentację w bazie urządzeń (Configuration Management Database - CMDB). |
|  | Tworzenie własnych parserów musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI) |
|  | Tworzenie nowych atrybutów (sparsowanych zmiennych), urządzeń oraz rodzajów zdarzeń (events) musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI). |
|  | Parsery mają być tworzone z wykorzystaniem narzędzi wspierających dla XML (XML framework) i jednocześnie zapewniać następujące właściwości:   1. zdolność do definiowania wzorców które powtarzają się jako zmienne; 2. zdolność do definiowania funkcji pozwalających na identyfikację par wartości kluczowych; 3. zdolność do testowania poszczególnych funkcji; 4. zdolność do przekształcania danych w trakcie ich parsowania. |
|  | Rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Windows (Windows Agent), które posiadają nie mniej niż następujące możliwości:   1. centralne zarządzanie i możliwość aktualizacji z głównej konsoli zarządzającej; 2. możliwość zbierania logów z plików tekstowych na urządzeniach z zainstalowanym systemem z rodziny Windows; 3. możliwość zbierania logów dotyczących zdarzeń rodzajów innych niż: Security, System, Application; 4. zdolność do monitorowania integralności plików; 5. zdolność do monitorowania rejestru systemowego; 6. zdolność do monitorowania urządzeń zewnętrznych (removable devices); 7. agent instalowany na systemach z rodziny Windows musi komunikować się z poszczególnymi komponentami rozwiązania SIEM w sposób zaszyfrowany z wykorzystaniem protokołu HTTPS; 8. musi istnieć możliwość monitorowania stanu agentów w konsoli zarządzającej systemu; 9. musi istnieć możliwość przygotowania różnych zestawów konfiguracji agenta, a następnie przypisywania ich niezależnie do dowolnej ilości (jeden lub więcej) systemów źródłowych. Np. inne konfiguracje dla kontrolerów domeny, a inne dla serwerów DNS; 10. musi umożliwiać automatyzację reakcji na zagrożenie, jak blokowanie zdefiniowanego ruchu sieciowego czy blokada procesu. |
|  | System musi mieć możliwość realizacji funkcjonalności UEBA (User Entity Behaviour Analysis) zarówno w oparciu o dedykowanego Agenta na systemy Windows oraz w oparciu o logi z systemu Windows. Metadane lub logi dotyczące funkcji UEBA nie mogą podlegać licencjonowaniu ze względu na EPS lub rozmiar. |
|  | Zdarzenia w obsłudze muszą umożliwiać gromadzenie dodatkowych informacji wygenerowanych podczas ich obsługi oraz umożliwiać do nich dostęp bezpośrednio z poziomu tych zdarzeń, obejmujących m.in.   1. wszystkie skorelowane zdarzenia, 2. korespondencja pocztowa, 3. załączniki z próbkami lub dowodami, 4. wskaźniki kompromitacji (IoC), 5. informacje pozyskane z innych systemów. |
|  | System powinien posiadać możliwość rejestracji zgłoszeń przez stronę webową udostępnianą przez system dla użytkowników z innych jednostek organizacyjnych oraz umożliwić ich przekształcenie w zdarzenia w obsłudze z możliwością rozdzielenia uprawnień dla obu tych czynności. System musi umożliwiać scenariusz, gdzie użytkownik zgłasza incydent, który zanim zostanie zakwalifikowany do dalszej obsługi musi zostać autoryzowany przez uprawnionego do tego celu operatora. |
|  | Dla obsługiwanych zdarzeń system powinien umożliwiać automatyczne pozyskanie informacji z innych systemów oraz bazując na uzyskanej od nich odpowiedzi automatycznie zmieniać ich status, np.: na podstawie pozyskanego wskaźnika kompromitacji (IoC) zmienić status zdarzenia na incydent bezpieczeństwa. |
|  | Dla zdarzeń w obsłudze dotyczących ruchu sieciowego pomiędzy źródłem a celem transmisji, system musi automatycznie wyznaczyć wektor zagrożenia i zaprezentować go w formie graficznej, na której będą zwizualizowane następujące dane:   1. identyfikację celu i źródła zagrożenia, 2. nazwę oraz adres IP źródła zagrożenia, 3. rodzaj zasobu będący źródłem zagrożenia np.: urządzenie mobilne, stacja robocza, 4. lokalizację z które pochodzi zagrożenie np.: Internet, 5. strefę bezpieczeństwa z której pochodzi zagrożenie, 6. prawdopodobieństwo zagrożenia ze strefy stanowiącej jego źródło, 7. wszystkie urządzenia sieciowe chroniące cel zagrożenia i zastosowane na nich mechanizmy zabezpieczeń (np.: Application Control, Network Firewall, User Identification), 8. nazwę oraz adres IP celu zagrożenia, 9. zabezpieczenia lokalne chroniące cel zagrożenia, 10. strefę bezpieczeństwa w której znajduje się cel zagrożenia. |
|  | Dla każdego wektora zagrożenia system musi automatycznie wyliczać efektywność zastosowanych mechanizmów zabezpieczeń, pozwalającą w ramach wbudowanych w system edytowalnych reguł ocenić prawdopodobieństwo materializacji się cyberzagrożeń. Na przykład: dla serwera webowego dostępnego ze strefy Internet zagrożenie przełamania zabezpieczeń ma niskie prawdopodobieństwo w przypadku gdy jest on zabezpieczony przez rozwiązanie klasy WAF (Web Application Firewall). |
|  | Dla wyznaczonych w czasie obsługi wektorów zagrożeń przedstawiane wyniki szacowania prawdopodobieństwa muszą być zwizualizowane operatorowi w formie listy zagrożeń z oszacowanymi dla nich poziomami. Przykładowe wartości z listy to: wysoki poziom prawdopodobieństwa włamania na serwer oraz średni poziom prawdopodobieństwa infekcji złośliwym oprogramowaniem. |
|  | Dla zdarzeń w obsłudze zarówno w odniesieniu do adresów źródłowych jak i docelowych system musi umożliwiać operatorowi uzupełnianie pozyskanych informacji, dotyczących zarówno źródła jak i celu zagrożenia w następującym zakresie:   1. nazwy zasobu, 2. rodzaju zasobu, 3. ważności zasobu dla organizacji, 4. rodzaj przetwarzanych informacji, 5. usług, które ten zasób świadczy, 6. lokalizację użytkowników, którzy z niego korzystają, 7. usługi z których zasób korzysta |
|  | System powinien mieć logikę automatycznego przypisywania zdarzeń zakwalifikowanych do obsługi wraz z powiadomieniem operatora, któremu zostało ono przydzielone (min. e-mail, SMS). Kwalifikacja musi uwzględniać m.in. dostępność operatora, jego obciążenia oraz parametry zasobu którego dotyczy zdarzenie, typ zasobu (np.: serwer lub stacja robocza), jego krytyczność oraz realizowane z jego udziałem usługi z katalogu usług. Na przykład: zdarzenie przypisane do krytycznego serwera realizującego usługę DNS powinny trafić do innego operatora niż zdarzenia dotyczące pozostałych serwerów usług sieciowych. |
|  | System powinien umożliwiać grupowanie manualne w jeden incydent bezpieczeństwa zdarzenia podobne/powiązane np. wielokrotnie raportowane, przez systemy źródłowe, wielokrotnie zgłoszone przez użytkowników. |
|  | System powinien grupować automatycznie w jeden incydent bezpieczeństwa zdarzenia podobne/powiązane np. wielokrotnie raportowane, przez systemy źródłowe, wielokrotnie zgłoszone przez użytkowników. |
|  | 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. |
|  | System powinien 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. |
|  | W ramach obsługi zdarzenia dla operatora powinien być dostępny dedykowany panel analityczny pozwalający mu na:   1. podgląd aktywności zagrożonego zasobu na linii czasu, 2. w przypadku zagrożenia sieciowego podgląd aktywności zarówno ofiary jak i celu ataku, 3. w przypadku identyfikacji użytkownika podgląd jego aktywności na linii czasu, 4. podgląd reguły korelacyjnej, która wygenerowała zdarzenie, 5. w przypadku wykrytej techniki Mitre ATT@CK jej szczegółowy opis, 6. listowanie podpiętych zdarzeń wraz z mechanizmami filtrowania po nich, 7. gotowe i proste w użyciu filtry rozszerzajcie analizę zdarzeń o:  * listę wszystkich zdarzeń pomiędzy celem a źródłem ataku w zadanym okresie czasowym, np.: godzinę przed oraz 2 godziny po, * listę wszystkich zdarzeń dotyczących źródła lub celu ataku w zadanym okresie czasowym,  1. gotowe i proste w użyciu filtry rozszerzajcie analizę logów o:  * listę wszystkich logów pomiędzy celem a źródłem ataku w zadanym okresie czasowym, * listę wszystkich logów dotyczących źródła lub celu ataku w zadanym okresie czasowym. |
|  | System powinien umożliwiać wykonywanie działań remediacyjnych na stacjach roboczych/serwerach (pobieranie logów, uruchamianie skryptów, weryfikacja rejestrów, itp.). |
|  | System powinien umożliwiać przypisywanie i przekazywanie incydentów do operatorów lub grup operatorów |
|  | 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 oraz zapewnić dla tych systemów mechanizmy bezpiecznego zarządzania i przechowywania danych związanych z tymi integracjami, m.in. loginy, hasła oraz klucze API. |
|  | System powinien umożliwiać przeglądanie listy zasobów (urządzeń, systemów, osób, itp.) pod kątem poziomu i ilości incydentów, które są z nimi powiązane. |
|  | System powinien mieć możliwość automatycznego informowania o zmianie statusu incydentu (wygenerowaniu, przypisaniu, przekroczeniu czasu SLA oraz zamknięciu karty incydentu). |
|  | System powinien umożliwiać ustawienie parametrów SLA bazując na ustalonym automatycznie priorytecie zdarzenia/incydentu/podatności. System powinien dokonywać automatycznego pomiaru tych czasów i weryfikacji ich do zdefiniowanych wymagań SLA. Wyniki pomiaru czasu powinny być stale aktualizowane i prezentowane w interfejsie systemu. |
|  | 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. |
|  | System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień dla kadry zarządzającej, obejmujących eskalacje oraz monitorowanie SLA. Szablony powinny uwzględniać powiadomienia kierowników jednostek organizacyjnych w następujących sytuacjach:   1. przekroczenia czasu reakcji o określony czas np.: o godzinę, 2. możliwości przekroczenia czasu reakcji, np.: została godzina aby rozpocząć obsługę zdarzenia i uchronić się przed przekroczeniem czasu reakcji, 3. przekroczenia czasu reakcji dla zdarzenia na zasobie przetwarzającym dane osobowe, 4. przekroczenia czasu reakcji dla zdarzenia na zasobie krytycznym, 5. przekroczenia czasu reakcji dla zdarzenia na zasobie realizującym krytyczną usługę, 6. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów przetwarzających dane osobowe, 7. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów krytycznych, 8. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów realizujących krytyczną usługę, 9. przekroczenia czasu reakcji dla podatności na zasobie przetwarzającym dane osobowe, 10. przekroczenia czasu reakcji dla podatności na zasobie krytycznym, 11. przekroczenia czasu reakcji dla podatności na zasobie realizującym krytyczną usługę, |
|  | Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora pozwalającego na:   1. wybór raportu który ma zostać wysłany, 2. zdefiniowanie jego tytułu, 3. zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny, 4. możliwość ograniczenia cyklu do dni powszednich, 5. określenie daty przesłania pierwszego raportu, 6. określenie okresu przez jaki będą one przesyłane, poprzez:  * zdefiniowanie daty końcowej, * bez daty końcowej, * określenie liczby raportów,  1. określenie odbiorców raportu |
|  | Dla obsługiwanych podatności system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących:   1. warunki powiadomień,  * podatności o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi, * podatności o przekroczonych czasach SLA o definiowalny okres, * podatności ze zbliżającym się i definiowalnym terminem przekroczenia SLA, * podatności, których priorytet osiągnął określoną wartość, * zdarzeń realizujących zdefiniowaną usługę, * zdarzeń przetwarzających sklasyfikowane informację, * zdarzeń przetwarzanych na krytycznych zasobach,  1. odbiorców powiadomień, w tym:  * operatora, któremu została przydzielona podatność, * właściciela zasobu na którym wystąpiła podatność, * zespół obsługi, który odpowiada za obsługę podatności, * właściciela usługi na która jest realizowana na zasobie na którym wystąpiła podatność, * podmiot zewnętrzny, jeżeli zdarzenie dotyczy podatności na zasobie obsługiwanym przez firmę zewnętrzną.  1. kanały powiadomień, m.in. e-mail, sms, komunikator, 2. zastosowanie mechanizmów grupowania:  * grupowanie wielu powiadomień w jednej wiadomości, * ograniczenie liczby wierszy powiadomienia do określonej wartości. |
|  | System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień jego operatorom w przypadku gdy system przydzieli im podatności do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach:   1. przydzielenia nowej podatności do obsługi z określonym priorytetem, 2. przydzielenia nowej podatności do obsługi na zasobie krytycznym, 3. przydzielenia nowej podatności do obsługi na zasobie realizującym zdefiniowaną usługę, 4. przydzielenia nowej podatności do obsługi na zasobie przetwarzającym dane osobowe, 5. modyfikacji przydzielonej operatorowi podatności przez innego operatora, 6. zamknięcia przydzielonej operatorowi podatności przez innego operatora, 7. przejęcia przydzielonej operatorowi podatności przez innego operatora. |
|  | System powinien posiadać gotowe szablony powiadomień pozwalające na wysyłanie powiadomień jego operatorom w przypadku gdy system przydzieli im zdarzenia do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach:   1. utworzenia nowego zdarzenia z określonym priorytetem, 2. utworzenia nowego zdarzenia na zasobie krytycznym, 3. utworzenia nowego zdarzenia na zasobie realizującym zdefiniowaną usługę, 4. utworzenie nowego zdarzenia na zasobie przetwarzającym dane osobowe, 5. utworzenie nowego zdarzenia na podstawie zdefiniowanej reguły korelacyjnej, 6. modyfikacji przydzielonego operatorowi zdarzania przez innego operatora, 7. zamknięcia przydzielonego operatorowi zdarzania przez innego operatora, 8. przejęcia przydzielonego operatorowi zdarzania przez innego operatora. |
|  | System musi zawierać mechanizm integracji ze skanerami podatności co najmniej trzech producentów. W ramach integracji system musi mieć możliwość uruchamiania skanowania podatności, importowania jego wyników zawierających listę podatności i ich atrybuty oraz możliwość kasowania ze skanera zaimportowanych wcześniej skanów. Wszystkie powyższe operacje muszą być konfigurowalne z poziomu graficznego interfejsu systemu. |
|  | Rozwiązanie musi zawierać mechanizm pasywnej analizy podatności, obejmującej systemy IT uzupełnione o informację zgodne ze słownikiem CPE (ang. Common Platform Enumeration), umożliwiającą import wykrytych podatności zasobu do systemu z publicznie dostępnej bazy CVE (ang. Common Vulnerabilities and Exposures) i dalszą obsługę tych podatności w systemie. |
|  | Interfejs modułu obsługi incydentów musi prezentować listę podatności zasobów związanych z incydentem. |
|  | System powinien 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. |
|  | Obsługiwane w systemie podatności muszą być dostępne w formie listy umożliwiającej ich filtrowanie po następujących wartościach:   1. wyliczonym priorytecie podatności, 2. aktualnym statusie obsługi, 3. ważności zasobu na którym została wykryta, 4. adresie IP tego systemu, 5. parametrów SLA związanych z tym statusem, 6. przetwarzanych na zasobach informacji, np.: lista podatności dotycząca tylko systemów przetwarzających dane osobowe, 7. parametrach CVSS, np.: lista podatności których „Access Complexity (AC)” = „low” oraz „Access Vector (AV) = „Network”. |
|  | 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. |
|  | System powinien zawierać mechanizm definiowania harmonogramów skanowania podatności oraz na ich podstawie automatycznie uruchamiać procesy skanowania i analizowania uzyskanych raportów. |
|  | System powinien umożliwiać obsługę podatności w ramach scenariuszy obsługi (playbook). |
|  | Zamawiający na obecnym etapie nie jest w stanie zmierzyć ilości danych przekazywanych do systemu, tj. EPS (Events Per Second) oraz nie zna wymagań związanych z architekturą proponowanego rozwiązania, dlatego oferowana licencje nie może nakładać limitów w tym zakresie. |
|  | Produkt musi umożliwiać równoczesną pracę co najmniej 3 operatorów oraz obsługiwać minimum 35 źródeł logów dotyczących wszystkich zdarzeń związanych z komputerami oraz serwerami wykorzystywanymi w organizacji oraz zapewnić dla tych źródeł detekcję i obsługę cyberzagrożeń w ramach wszystkich oferowanych w tym postępowaniu funkcjonalności. |
|  | System ma gwarantować możliwość elastycznej rozbudowy o dalsze zasoby IT, które w przyszłości zostaną objęte jego działaniem. |
|  | System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows (minimum Server 2016), Redhat/Oracle Linux (minimum 7.x). |
|  | Dostarczone rozwiązanie musi być objęte minimum 12-miesięcznym (liczonym od dnia podpisania protokołu odbioru) wsparciem producenta lub producentów. Wsparcie musi obejmować bezpłatne dostarczanie aktualizacji oprogramowania, reagowanie na zgłaszane błędy systemowe oraz usługę konsultacji powdrożeniowej w formie spotkań z dedykowanym inżynierem, certyfikowanym z procesu konfiguracji i obsługi oferowanego systemu. Przez błąd systemowy Zamawiający rozumie błędy krytyczne (zakłócenie uniemożliwiające działanie rozwiązania), błędy poważne (zakłócenie uniemożliwiające działanie części rozwiązania), błędy zwykłe (inne zakłócenia nie stanowiące błędu krytycznego lub poważnego). |
|  | Nie wykupienie wsparcia na kolejny okres nie może wpływać na dalsze funkcjonowanie dostarczonego rozwiązania. Rozwiązanie SIEM i SOAR musi zostać dostarczone z licencją wieczystą. |
|  | Wykonawca musi zapewnić usługę obejmującą proces aktualizacji oprogramowania oraz kontekstu systemu (dotyczy to zwłaszcza bazy reguł korelacyjnych, bazy parserów, bazy dostępnych aktualizacji). Dostęp do centralnej usługi aktualizacyjnej ma pozwalać na automatycznie wyświetlanie i pobieranie z poziomu interfejsu systemu dostępnych aktualizacji. Dla pobranych w procesie aktualizacji reguł oraz parserów musi być dostępne wersjonowanie, pozwalające uruchomić nową wersję reguły korelacyjnej oraz parsera z poziomu interfejsu systemu. Automatyczne wersjonowanie ma umożliwiać wczytanie starszej wersji reguły lub parsera, a zmiana reguł i parserów musi być możliwa z poziomu graficznego systemu. |
|  | Po zakończonym wdrożeniu należy zapewnić bezpłatne 3-dniowe certyfikowane szkolenia (3 x 8h) w zakresie użytkowania i administrowania wdrożonego systemu lub systemów dostarczonych w ramach zamówienia. Szkolenie ma zostać przeprowadzone dla minimum 1 osoby i uwzględniać informacje z zakresu wdrożonego systemu SIEM i SOAR (m.in. zarządzanie incydentami bezpieczeństwa; kompletowanie informacji potrzebnych do opracowania raportu o incydencie; szacowanie ryzyka itp.). Szkolenia muszą być zakończone certyfikatem potwierdzającym wspomniane umiejętności wydanym przez producenta systemu. Szkolenia powinny odbyć się w formie zdalnej. Szkolenia muszą być przeprowadzone w języku polskim. |
|  | Wykonawca przekaże Zamawiającemu wszelkie, niezbędne do poprawnego korzystania z wdrożonego rozwiązania, informacje o specyfice systemu oraz informacje techniczne na temat jego prawidłowej eksploatacji w języku polskim (tj. dokumentację powdrożeniową oraz instrukcję/instrukcje obsługi). |
|  | Zamawiający wymaga by wraz ofertą Wykonawca dostarczył próbkę systemu (np. w postaci przekierowania do wersji demonstracyjnej systemu) z odpowiednią dokumentacją (np. w postaci karty produktu oraz niezbędnych instrukcji). Zamawiający maksymalnie w ciągu pięciu dni roboczych, zweryfikuje zgodność oferowanego systemu na podstawie próbki systemu i dostarczonej dokumentacji, porównując je ze wszystkimi wymaganiami określonymi w powyższych punktach OPZ. W przypadku gdy Zamawiający uzna niezgodność próbki i dokumentacji z wymaganiami OPZ, lub gdy Zamawiający nie odnajdzie określonego wymagania w próbce systemu i dokumentacji, oferta Wykonawcy zostanie odrzucona.  W przypadku gdy Wykonawca nie dołączy do oferty próbki systemu wraz z dokumentacją, oferta zostanie odrzucona. |