Załącznik Nr 5

System klasy SIEM i SOAR - system do wykrywania i zarządzania incydentami, podatnościami oraz ryzykiem

Opis przedmiotu szacowania:

Przedmiotem zamówienia jest dostarczenie i wdrożenie w środowisku informatycznym Zamawiającego systemu klasy SIEM (z ang. Security Information and Event Management) i SOAR (z ang. Security Orchestration, Automation and Response) służącego do analizy logów i korelacji zdarzeń oraz automatycznego wykrywania incydentów i podatności wraz z wdrożeniem i uruchomieniem tego systemu w środowisku informatycznym Zamawiającego.

I. WYMAGANIA FUNKCJONALNE

1. 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.
2. 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.
3. System musi umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji również w formie tabelarycznej.
4. System musi pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci, np.: poziom krytyczności systemów oraz usług.
5. System musi umożliwiać generowanie elektronicznej dokumentacji sieci i systemów w sposób automatyczny na podstawie dostarczonych przez producenta reguł wykrywania oraz edytora graficznego pozwalającego utworzyć dodatkowe reguły.
6. 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.
7. 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) komunikację do usług wykrytych na zasobie.
8. System musi umożliwiać uwiarygodnianie uzyskiwanych informacji na bazie wartości progowych osiągniętych w zadanej jednostce czasu i dopiero po ich uwiarygodnieniu uzupełniać automatycznie elektroniczną dokumentację.
9. System powinien posiadać zestaw predefiniowanych reguł do automatycznego uzupełniania elektronicznej dokumentacji, których uruchomienie będzie automatycznie aktualizować elektroniczną dokumentację bez ingerencji operatora.
10. 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.
11. System musi posiadać wbudowaną bazę wskaźników kompromitacji, która umożliwi zbieranie, przechowywanie oraz przypisywanie wskaźników kompromitacji (IoC) do incydentów. Baza powinna obsługiwać protokół TLP w wersji 2.0 oraz obsługiwać następujące typy wskaźników:
    1) fqdn,
    2) e-mail,
    3) nazwa pliku,
    4) ścieżka do pliku,
    5) hash,

6) adres IP,
7) klucz rejestru,
8) cmd.

12. 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/).
13. System musi umożliwiać definiowanie list referencyjnych zarówno z jedną wartością jak i łączących unikalne wartości w pojedynczym wierszu (np: obraz pliku, hash, nazwa procesu).
14. Listy referencyjne muszą mieć możliwość synchronizacji z listami publikowanymi publicznie (np.: „Malicious IPs", „Malicious domain" czy „Tor Exit Nodes").
15. System musi umożliwiać zintegrowanie z usługą katalogową Microsoft Active Directory celem pobrania informacji o poświadczeniach oraz atrybutach użytkowników i komputerów zarejestrowanych w domenie. Minimum to: nazwa komputera wraz z systemem operacyjnym, nazwa użytkownika, login, e-mail, przynależność do grup, przełożonego, jednostkę organizacyjną oraz listę kont uprzywilejowanych.
16. System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać możliwość jej synchronizacji z usługą katalogową Microsoft Active Directory.
17. 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).
18. System powinien posiadać zestaw predefiniowanych reguł weryfikacji konfiguracji zasobów IT.
19. 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.
20. Rozwiązanie musi zawierać mechanizm pasywnej analizy podatności, obejmującej systemy IT uzupełnione o informację zgodne z słownikiem CPE (ang. Common Platform Enumeration), umożliwiającą import wykrytych podatności zasobu do systemu z publicznie dostępnej bazy CVE (ang. Common Vulnerabilities and Exposures) i dalszą obsługę tych podatności w systemie.
21. 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.
22. System w swoim działaniu musi korzystać z wbudowanych algorytmów uczenia maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników i komputerów.
23. 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).
24. 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.
25. 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).
26. 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.

27. 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).
28. System musi zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role.

II. POZYSKIWANIE ZDARZEŃ

1. System musi umożliwić odbieranie logów wygenerowanych przez systemy zabezpieczeń, systemy sieciowe, systemy operacyjne i aplikacje następującymi protokołami: Syslog, TLS syslog, NetFlow, Windows Event Forwarding.
2. Logi pozyskiwane z systemów Microsoft Windows nie mogą wymagać instalowania dedykowanego oprogramowania bezpośrednio na tych systemach.
3. System musi posiadać wbudowane mechanizmy zapewniające możliwość pobierania zdarzeń poprzez wykorzystanie RestFull-API, sterownika ODBC, agenta do czytania plików płaskich, protokołów IMAPS, POP3S, MAPI do pobierania wiadomości ze skrzynek poczty elektronicznej oraz obsługi zapytań WQL w ramach protokołu WMI;
4. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych.

III. NORMALIZACJA (PARSOWANIE) ZDARZEŃ

1. 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.
2. 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.
3. Proces normalizacji musi wspierać następujące typy składni: CEF, LEEF, URI, SYSLOG (zgodny z RFC 3164) i automatycznie tworzyć na ich podstawie pola i ich wartości zgodne z zasadami określonymi przez te składnie. Parsowanie powyższych składni nie może być realizowane za pomocą wyrażeń regularnych.
4. Normalizacja musi umożliwiać automatyczne nadawanie kategorii zdarzeń w formie nowych pól, np.: logowanie, wylogowanie, zmiana uprawnień, błąd konfiguracji, wykryte skanowanie systemu czy zablokowany malware.
5. Normalizacja logów musi posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól o nazwę lub kod kraju korzystając z wbudowanej w produkt bazy.
6. 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.
7. System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) dla zdarzeń z niestandardowych źródeł danych, w oparciu o następujące składnie: CEF, LEEF, URI, XML, JSON, SYSLOG, REGEX. System musi umożliwiać zastosowanie wszystkich typów składni dla pojedynczego zdarzenia, przykładowo pole „msg" znormalizowane automatycznie według standardu CEF powinno mieć możliwość dalszej normalizacji np.: zgodnej z URI lub REGEX.
8. 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.

IV. SKŁADOWANIE ZDARZEŃ

1. System musi rejestrować i przechowywać pozyskane logi w postaci surowej (RAW) oraz znormalizowanej.
2. 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.
3. 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.
4. 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.
5. 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.

6. System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych w postaci skompresowanej.
7. System musi zapewnić mechanizmy bezpieczeństwa dla danych przechowywanych w repozytoriach uniemożliwiające ich nieautoryzowaną modyfikację oraz zapewnić operatorom mechanizmy weryfikacyjne integralność danych.
8. 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.
9. 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.

V. MECHANIZMY DETEKCJI CYBERZAGROŻEŃ

1. Dostarczone rozwiązanie musi umożliwiać gromadzenie i korelacje zdarzeń przesyłanych lub pobieranych z innych systemów. Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł oraz ich agregację.
2. System musi posiadać interfejs graficzny do tworzenie własnych reguł korelacyjnych odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie. Korelacja musi odbywać się na bieżąco na etapie rejestrowania danych w systemie a mechanizm tworzenie reguł musi uwzględniać:
   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®,
3. 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.
4. 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).
5. 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.
6. 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.
7. 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;
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.
14. 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.

VI. OBSŁUGA CYBERZAGROŻEŃ

1. 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.
2. 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.
3. 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. zamianę kolejności realizacji poszczególnych kroków poprzez ich przenoszenie za pomocą myszki komputerowej.
4. System musi potrafić wczytywać informacje z innych systemów bezpieczeństwa i traktować je, jako elementy/dowody dla zdarzeń w obsłudze.
5. 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.
6. 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.
7. 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.
8. 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.
9. 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).

10. 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.
11. 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.
12. 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.
13. 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.
14. 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".
15. System powinien umożliwiać definiowanie parametrów SLA dla wszystkich statusów obsługi zdarzeń oraz dokonywać automatycznego pomiaru tych czasów i ich weryfikacji względem zdefiniowanych wartości. Wyniki pomiarów czasów SLA powinny być stale aktualizowane i prezentowane na liście zdarzeń zakwalifikowanych do obsługi.
16. 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.
17. 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.
18. Dla każdego obsługiwanego zdarzenia system powinien udostępniać automatyczny raport obejmujący wszystkie podjęte działania wraz z komentarzami operatorów.
19. 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.
20. System powinien pozwalać, przy użyciu języków skryptowych ogólnie dostępnych (np. Python lub PowerShell), na skonfigurowanie nowych integracji z zewnętrznymi systemami oraz zapewnić dla tych systemów mechanizmy bezpiecznego zarządzania i przechowywania danych związanych z tymi integracjami, m.in. loginy, hasła oraz klucze API.
21. W ramach obsługi zdarzenia dla operatora powinien być dostępny dedykowany panel analityczny pozwalający 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:
   a) listę wszystkich zdarzeń pomiędzy celem a źródłem ataku w zadanym okresie czasowym, np.: godzinę przed oraz 2 godziny po,
   b) listę wszystkich zdarzeń dotyczących źródła lub celu ataku w zadanym okresie czasowym,
8) gotowe i proste w użyciu filtry rozszerzajcie analizę logów o:
   a) listę wszystkich logów pomiędzy celem a źródłem ataku w zadanym okresie czasowym,
   b) listę wszystkich logów dotyczących źródła lub celu ataku w zadanym okresie czasowym.

22. Dla zdarzeń w obsłudze system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących:
    1) warunki powiadomień,
       a) zdarzeń o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi,
       b) zdarzeń o przekroczonych czasach SLA o definiowalny okres,
       c) zdarzeń ze zbliżającym się i definiowalnym terminem przekroczenia SLA,
       d) zdarzeń, których priorytet osiągnął określoną wartość,
       e) zdarzeń zakwalifikowanych jako incydent bezpieczeństwa,
       f) zdarzeń na których doszło do naruszenia bezpieczeństwa,
       g) zdarzeń powstałych poprzez zdefiniowaną regułę korelacyjną,
       h) zdarzeń realizujących zdefiniowaną usługę,
       i) zdarzeń przetwarzających sklasyfikowane informację,
       j) zdarzeń przetwarzanych na krytycznych zasobach,
    2) odbiorców powiadomień, w tym:
       a) operatora, któremu zostało przydzielone zdarzenie,
       b) właściciela zasobu na którym wystąpiło zdarzenie,
       c) zespół obsługi, który odpowiada za obsługę zdarzeń,
       d) właściciela usługi która jest realizowana na zasobie na którym wystąpiło zdarzenie,
       e) podmiot zewnętrzny, jeżeli zdarzenie dotyczy zasobu obsługiwanego przez firmę zewnętrzną.
    3) kanały powiadomień, m.in. e-mail, sms, komunikator,
    4) zastosowanie mechanizmów grupowania:
       a) grupowanie wielu powiadomień w jednej wiadomości,
       b) ograniczenie liczby wierszy powiadomienia do określonej wartości.
23. 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.
24. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora umożliwiającego:
    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) możliwości ograniczenia okresu przez jaki raport będzie przesyłany, do:
       a) zdefiniowanej daty końcowej,
       b) określonej liczby raportów,
    7) określenie odbiorców raportu.
25. System musi umożliwiać obsługę podatności w ramach scenariuszy obsługi (Playbook).
26. 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.

27. 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.
28. 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".
29. 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,
30. Dla obsługiwanych podatności system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących:
    1) warunki powiadomień,
        a) podatności o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi,
        b) podatności o przekroczonych czasach SLA o definiowalny okres,
        c) podatności ze zbliżającym się i definiowalnym terminem przekroczenia SLA,
        d) podatności, których priorytet osiągnął określoną wartość,
        e) zdarzeń realizujących zdefiniowaną usługę,
        f) zdarzeń przetwarzających sklasyfikowane informację,
        g) zdarzeń przetwarzanych na krytycznych zasobach,
    2) odbiorców powiadomień, w tym:
        a) operatora, któremu została przydzielona podatność,
        b) właściciela zasobu na którym wystąpiła podatność,
        c) zespół obsługi, który odpowiada za obsługę podatności,
        d) właściciela usługi na która jest realizowana na zasobie na którym wystąpiła podatność,
        e) podmiot zewnętrzny, jeżeli zdarzenie dotyczy podatności na zasobie obsługiwanym przez firmę zewnętrzną.
    3) kanały powiadomień, m.in. e-mail, sms, komunikator,
    4) zastosowanie mechanizmów grupowania:

a) grupowanie wielu powiadomień w jednej wiadomości,
b) ograniczenie liczby wierszy powiadomienia do określonej wartości.

31. 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.
32. 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:
        a) zdefiniowanie daty końcowej,
        b) bez daty końcowej,
        c) określenie liczby raportów,
    7) określenie odbiorców raportu.
33. System powinien w formie graficznej prezentować podsumowanie aktualnego stanu bezpieczeństwa organizacji w postaci tzw. „Dashboard'u", tj. dostosowywać zakres i prezentacje danych do potrzeb zalogowanego użytkownika.
34. 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).
35. System musi zapewniać zestaw predefiniowanych dashboard'ów obejmujących następujące wykresy:
    1) wykres przedstawiający status klasyfikacji zdarzeń, który uwzględnia:
        a) ilość zdarzeń nowych i niesklasyfikowanych,
        b) ilość zdarzeń sklasyfikowanych jako incydenty bezpieczeństwa,
        c) ilość zdarzeń sklasyfikowanych jako fałszywe alarmy,
    2) wykres przedstawiający skale zagrożeń, który uwzględnia:
        a) ilość zasobów krytycznych na których są obsługiwane zdarzenia,
        b) ilość zasobów niekrytycznych na których są obsługiwane zdarzenia,
    3) wykres przedstawiający źródła zagrożeń, który uwzględnia:
        a) ilość nowych zdarzeń dotyczących użytkowników,
        b) ilość podjętych zdarzeń dotyczących użytkowników,
        c) ilość nowych zdarzeń dotyczących zasobów,
        d) ilość podjętych zdarzeń dotyczących zasobów,
    4) wykres przedstawiający poziom zagrożeń, który uwzględnia:
        a) ilość nowych zdarzeń w podziale na priorytety,
        b) ilość podjętych zdarzeń w podziale na priorytety,
    5) wykres przedstawiający czas obsługi zagrożeń, który uwzględnia:
        a) ilość zdarzeń zarejestrowanych w bieżącym dniu,
        b) ilość zdarzeń zarejestrowanych w ostatnim tygodniu,
        c) ilość zdarzeń zarejestrowanych w ostatnim miesiącu,
        d) ilość zdarzeń zarejestrowanych wcześniej niż w ostatnim miesiącu,
    6) wykres przedstawiający zagrożone usługi, który uwzględnia:
        a) ilość usług krytycznych zagrożonych przez obsługiwane zdarzenia,
        b) ilość pozostałych usług zagrożonych przez obsługiwane zdarzenia,
    7) wykres przedstawiający zagrożone dane, który uwzględnia:
        a) ilość nowych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje,
        b) ilość podjętych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje,
        c) ilość nowych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane

informacje,
   d) ilość podjętych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje,
8) wykres przedstawiający skale podatności, który uwzględnia:
   a) ilość zasobów krytycznych na których są obsługiwane podatności,
   b) ilość zasobów niekrytycznych na których są obsługiwane podatności,
9) wykres przedstawiający czas obsługi podatności, który uwzględnia:
   a) ilość podatności zarejestrowanych w bieżącym dniu,
   b) ilość podatności zarejestrowanych w ostatnim tygodniu,
   c) ilość podatności zarejestrowanych w ostatnim miesiącu,
   d) ilość podatności zarejestrowanych wcześniej niż w ostatnim miesiącu,
10) wykres przedstawiający wagę podatności, który uwzględnia:
   a) ilość nowych podatności w podziale na priorytety,
   b) ilość podjętych podatności w podziale na priorytety,

36. 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.

VII. WYMAGANIA OGÓLNE

1. Rozwiązanie może być dostarczone w ramach odrębnych rozwiązań, jednakże muszą być one zintegrowane w sposób umożliwiający spełnienie wszystkich wymagań z poziomu jednej konsoli.
2. 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.
3. 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.
4. 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.
5. Kolektor korelujący powinien umożliwiać korelację logów oraz ich agregację zgodnie z regułami korelacyjnymi zdefiniowanymi w jednym miejscu dla wszystkich kolektorów w interfejsie graficznym.
6. 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).

7. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.
14. 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.
15. 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.)
16. Poszczególne kolektory zdarzeń oraz logów muszą zapewniać przechowywanie danych zarówno na maszynach wirtualnych jak i na dyskach sieciowych.
17. 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.
18. Rozwiązanie nie może Przechowywanie logów oraz zdarzeń nie może wykorzystywać klasycznej relacyjnej bazy danych (w tym, choć nie tylko: MS SQL, Postgresql, MySQL, Oracle, itp.) celem gromadzenia i przechowywania danych związanych ze zbieranymi zdarzeniami. Rozwiązanie musi wykorzystywać w tym celu nowoczesną bazę taką jak na przykład noSQL lub OLAP lub autorskie rozwiązanie producenta.
19. Rozwiązanie musi zapewniać możliwość zbudowania większej ilości replik danych, aby zapewnić niezawodność przechowywania oraz możliwość zbudowania struktury rozproszonej, zapewniającej większą wydajność zapisu i wyszukiwania.
20. Klasyczne relacyjne bazy danych mogą być wykorzystywane jedynie do przechowywania szablonów, raportów, konfiguracji, bazy CMDB oraz innych ustrukturyzowanych informacji.
21. Rozwiązanie musi zapewniać możliwość automatycznego budowania kontekstu poprzez wykrywanie urządzeń oraz komputerów mających swoją reprezentację w bazie urządzeń (Configuration Management Database - CMDB).
22. Wymagane jest, aby kolektor odpowiedzialny za parsowanie pozwalał na odrzucanie danych, które uznane są za nieistotne lub niepotrzebne. Mechanizm ten nie może mieć żadnego wpływu na model licencjonowania.
23. Musi istnieć możliwość samodzielnej modyfikacji i poprawiania wszystkich parserów.
24. Tworzenie własnych parserów musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI)
25. 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).
26. 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.

27. 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.
28. 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.
29. Rozwiązanie musi zapewniać wsparcie dla zarządzania w oparciu o role (Role Based Administration) celem ograniczania dostępu do danych oraz do GUI
30. 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.
31. 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).
32. System musi mieć możliwość korelacji informacji z baz zagrożeń z danymi historycznymi
33. System musi mieć możliwość odpytywania (ręcznego lub automatycznego) zewnętrznych źródeł reputacji takich jak np.VirusTotal.
34. System musi mieć możliwość wizualizacji informacji w oparciu o kategorie MITRE ATT&CK dla standardowego zbioru wbudowanych reguł.
35. Pulpity administracyjne (dashboards) muszą mieć możliwość wspólnej prezentacji.
36. 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.
37. System musi wpierać mechanizmy typu Machine Learning w oparciu o zgromadzone zdarzenia. Musi być możliwe użycie przynajmniej 4 różnych rodzajów mechanizmów Machine Learning wraz z możliwością ich ręcznego wybrania oraz działania w trybie automatycznym. W wyniku działania opisanych mechanizmów Machine Learning system SIEM ma tworzyć model bazowy zachowania oraz umożliwiać wykrycie odchyleń i anomalii od niego. Zadania Machine Learning mają mieć możliwość dystrybuowania ich pomiędzy elementy warstwy korelującej i/lub zarządzającej. Mechanizmy Machine Learning mają również umożliwiać wsparcie dla podejmowania decyzji przy rozwiązywaniu incydentów w systemie SIEM.
38. 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.
39. 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.
40. W związku z tym, że obsługa systemu ma objąć także użytkowników nieposługujących się biegle językiem angielskim, interfejs użytkownika musi umożliwiać obsługę w języku polskim lub posiadać możliwość wgrania plików językowych tłumaczących interfejs na język polski. Pliki tłumaczące interfejs na język polski muszą zostać wgrane w trakcie wdrożenia systemu, przed jego zakończeniem.
41. 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.

42. Produkt musi umożliwiać równoczesną pracę co najmniej 2 operatorów oraz obsługiwać do 100 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.
43. System musi gwarantować możliwość elastycznej rozbudowy o kolejne źródła logów.
44. 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.
45. System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows (minimum Server 2016), Redhat/Oracle Linux (minimum 7.x).
46. Dostarczone rozwiązanie musi być objęte 24 miesięcznym wsparciem producenta lub producentów. Wsparcie musi obejmować bezpłatne dostarczanie aktualizacji oprogramowania, reagowanie na zgłaszane błędy systemowe oraz usługę konsultacji 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).
47. 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.
48. Wykonawca zapewni szkolenie w zakresie użytkowania i administrowania wdrożonego systemu lub systemów. Szkolenie ma zostać przeprowadzone dla 1 osoby i musi być zakończone przyznaniem certyfikatu, potwierdzającego wspomniane umiejętności wydanym przez producenta systemu/ systemów. Szkolenia mogą odbyć się w formie zdalnej.