Załącznik nr 1 do umowy Nr ……..

Szczegółowy opis przedmiotu zamówienia

System kolekcji logów, wyszukiwania pełno tekstowego oraz analizy zagrożeń.

Szczegółowe wymagania.

1. System kolekcji logów:

- musi być oparty o silnik wyszukiwania logów Elasticsearch Lucene oraz wizualizację danych Kibana
- musi być oparty o nowoczesną nierelacyjną bazę danych typu noSQL
- musi działać w trybie zbliżonym do rzeczywistego
- musi zapewniać efektywną obsługę do 100 GB danych dziennie
- architektura rozwiązania musi umożliwiać rozdzielenie ról systemu pomiędzy osobne komponenty (serwery/maszyny wirtualne). Należy przewidzieć rozdzielenie przynajmniej 3 typów ról: Agregacja, Prezentacja, Retencja.
- Interfejs musi posiadać angielską lub polską wersję językową,
- musi zapewniać pełen audyt aktywności jego użytkowników, w tym: udanych/nieudanych logowaniach, pełnej historię operacji, realizowanych zapytań, zmian uprawnień,
- musi pozwalać na tworzenie parserów z poziomu GUI
- musi umożliwiać predykcję danych w oparciu o dowolne dane historyczne zgromadzone w systemie.
- musi zapewniać wizualizację danych w postaci, oryginalnych logów, list, wykresów i diagramów.
- musi umożliwiać funkcjonalność eksportu danych o Zdarzeniach i Incydentach do formatu CSV i HTML m.in. w celu analizy wyników działania reguł korelacyjnych.
- musi zapewniać parsowanie spływających do niego wiadomości w formatach: Syslog, WEF, Flat file, Event log, WMI, SNMP trap, XML, JSON, JDBC/ODBC CSV, Email,
- musi umożliwiać prezentację logu o zdarzeniu w interfejsie użytkownika w takiej formie w jakiej ten log został przesłany do Systemu tj. wyświetlenie logu w postaci surowej (RAW) przed parsowaniem.
- musi umożliwiać definiowanie parserów dla niestandardowych formatów logów w oparciu o składnię wyrażeń regularnych oraz formatów wymiany danych dla wszystkich obsługiwanych formatów.
- musi mieć funkcjonalność Bad IP Reputation tj. porównywania adresów IP z bazami reputacyjnymi dostarczonymi przez producenta
- musi wspierać geolokalizację zdarzeń na bazie adresów IP.
- musi umożliwiać normalizowanie wiadomości po sparsowanych polach, np. dzięki zmianie wartości tych pól oraz wzbogacaniu tych danych o dodatkowe pola bazując na całych wartościach lub wzorcach wyszukiwania.
- musi umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach.
- proces parsowania musi umożliwiać wzbogacanie treści obieranych Wiadomości poprzez matematyczne operacje wykonywane na innych polach.

- proces parsowania musi umożliwiać anonimizację Danych Wejściowych celem ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzny procedury bezpieczeństwa.
- powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych
- powinien pozwalać na rozpoznanie formatów czasu i daty oraz normalizowanie ich do jednego wspólnego formatu.
- musi posiadać wbudowany komponent budowania elektronicznej dokumentacji z możliwością ręcznego i automatycznego dodawania treści oraz uzupełniania jej o wartości pochodzące ze zgromadzonych w Systemie danych.
- komponent budowania elektronicznej dokumentacji musi mieć możliwość m.in. tworzenia lub dodawania diagramów architektury zasobów informatycznych, tabel oraz list.
- musi umożliwiać łączenie wyników dwóch niezależnych zapytań w postaci jednej odpowiedzi, bez użycia składni SQL
- musi posiadać interfejs umożliwiający zmianę wybranej wartości w zgromadzonych danych.
- incydent, który powstał w wyniku korelacji, musi dać się wyszukiwać korzystając ze standardowego dostępnego w systemie mechanizmu wyszukiwania. System musi umożliwiać budowanie na jego podstawie kolejnych reguł korelacyjnych lub generowania alarmów.
- musi posiadać funkcjonalność korelacji danych w czasie rzeczywistym.
- musi umożliwiać tworzenie nowych reguł korelacyjnych oraz modyfikowanie istniejących.
- musi umożliwiać tworzenie własnych reguł korelacyjnych na bazie reguł odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie, w tym: Wykrycia dowolnej treści w logach, Wykrycia wystąpienia wartości pola na wybranej liście, Wykrycia niewystępowania wartości pola na wybranej liście, Wykrycia zmiany jednego z kilku pól, Wykrycia zdarzeń występujących z zadaną częstotliwością, Wykrycia zdarzeń, których liczba zmienia się w wskazany sposób względem czasu poprzedniego, Wykrycia zaniku Wiadomości, Wykrycia nowej wartości pola w zadanym okresie czasu, Wykrycia incydentu będącego pochodną zdarzeń występujących w określonej kolejności
- musi pozwalać na tworzenie własnych algorytmów ewaluacji Incydentów
- reguły korelacji oraz algorytmy ewaluacji incydentów muszą być możliwe do dodawania lub modyfikacji z poziomów zarówno GUI jak i API.
- musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.
- musi pozwalać na realizację zapytań obejmujących całą historię gromadzonych w nim danych
- musi umożliwić korelację Zdarzeń pochodzących z różnych źródeł informacji z anomaliami wykrywanymi m.in. w. Netflow oraz wykrytymi podatnościami zidentyfikowanymi przez skaner podatności
- musi zapewnić mechanizmy obsługi incydentów i wymiany informacji pomiędzy, operatorami systemu w tym przypisanie incydentu do operatora i zmiana jego statusu.
- musi posiadać funkcjonalność tworzenia scenariuszy obsługi incydentu tzw. Playbook
- musi automatycznie podpowiadać odpowiednie scenariusze obsługi incydentów.
- scenariusze muszą mieć możliwość ich symulacji i weryfikacji, m.in. na przykładowym zasobie IT.
- musi pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących.
- musi posiadać funkcjonalność wysyłania powiadomień o Incydentach do innych systemów bądź zdefiniowanych użytkowników (co najmniej: powiadamianie email, opcjonalnie SMS, czat).

- musi umożliwiać testowanie reguł korelacyjnych i alertów na etapie ich tworzenia. Wynik testu nie może tworzyć wpisu o sytuacji alarmowej i ewentualnego incydentu.
- musi umożliwiać konfiguracje automatycznych akcji, które są wykonywane na monitorowanych systemach w przypadku detekcji zagrożenia wskazanego w regule
- musi posiadać wbudowany, dostepny z poziomu GUI moduł tworzenia i edycji elektronicznej dokumentacji bazującej oraz wzbogacającej dane gromadzone ze środowiska informatycznego.
- musi być dostarczony z licencją wieczystą wraz ze wsparciem na okres 12 miesięcy.
- Wykonawca zapewni aktualizacje systemu przez okres 12 miesięcy.
- oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów. Oferowana licencja nie może ograniczać ilości logów.
- wsparcie systemu musi być realizowane w języku polskim przez dedykowanych inżynierów.
- wsparcie nie może być limitowane ilością zgłoszeń i musi być realizowane zdalnie oraz w siedzibie Zamawiającego.
- dokumentacja techniczna i baza wiedzy dotycząca oferowanego systemu musi być opublikowana na ogólnodostępnej stronie internetowej producenta.

2. Dostęp do systemu

- komunikacja pomiędzy komponentami systemu odpowiadającymi za agregacji, retencję i wizualizację danych musi odbywac się w sposób szyfrowany z wykorzystaniem protokołu TLS w wersji minimum 1.3.
- szyfrowanie komunikacji z przeglądarką internetową użytkownika musi wykorzystywać protoków TLS w wersji minimum 1.3.
- system musi posiadać interfejs graficzny dostępny z poziomu przeglądarki internetowej min. Firefox, Chrome, Internet Explorer.
- dostęp do systemu musi być zabezpieczany hasłem lub certyfikatem.
- autoryzacja do systemu musi być zintegrowana z: Microsoft AD, LDAP
- hasła typu Windows AD bind muszą być przechowywane w postaci zaszyfrowanej.
- system musi wspierać mechanizm logowania typu Single Sign On.
- system musi umożliwiać zarządzanie czasem automatycznego wygasania sesji użytkowników.
- system musi posiadać dedykowany widok zarządzania użytkownikami i rolami.
- system powinien umożliwiać zarządzenie uprawnieniami do modyfikacji wytworzonych w systemie obiektów tj. wyszukiwania, wizualizacje, dashboardy. Dla utworzonych ról musi istnieć możliwość przypisania wspomnianych obiektów w podziale na dostęp typu „read only” oraz „pełny”. Obiekty, do których grupa nie ma dostępu, nie mogą być widoczne dla użytkownika.

3. Przyjmowanie, identyfikacja i wizualizacja danych

- musi istnieć możliwość automatycznego importu informacji IoC (ang. Indicator Of Compromise), a następnie automatyczne przeszukiwanie wśród zgromadzonych zdarzeń w wyznaczonym czasie.
- system musi posiadać natywną integrację z bazą MISP min. Adresy IP, hash zainfekowanych plików, adresy domen, adresy URL.

4. Reguły korelacyjne, alerty i obsługa incydentów

- system musi posiadać bazę minimum 700 predefiniowanych reguł korelacyjnych

- system musi dostarczać funkcjonalność badania integralności plików i rejestrach na monitorowanych hostach, w tym: monitorowanie zmian na zawartości plików i katalogów, zmiany uprawnień dostępu do pliku, zmiany w atrybutach plików oraz zmian na sumach kontrolnych MD5 i SHA1.
- system musi posiadać funkcjonalność monitorowania konfiguracji systemów oraz aplikacji w celu zapewnienia zgodności z politykami i standardami bezpieczeństwa oraz praktykami dotyczącymi hardeningu, takimi jak CIS Benchmark.
- system musi posiadać gotowe wizualizacje i polityki zgodności z GDPR, PCI-DSS, NIST, ISO 27001
- system musi posiadać możliwość skanowania środowiska pod kątem detekcji rootkit'u i wykrywania ukrytych procesów, plików, portów
- system musi posiadać funkcjonalności skanowania podatności dla aplikacji oraz systemów operacyjnych Linux i Windows
- system musi posiadać funkcjonalność ciągłego śledzenia polityk OpenSCAP

5. Integracja z systemem Splunk Enterprise

- w ramach wdrożenia systemu wykonawca dostarczy aplikację integrującą rozwiązanie Splunk Enterprise z oferowanym rozwiązaniem.
- aplikacja musi być zainstalowana na obecnie funkcjonującej u Zamawiającego instalacji systemu Splunk Enterprise oraz funkcjonować zgodnie ze standardem Splunk App.
- integracja musi umożliwiać odczyt danych zgromadzonych w zaoferowanym rozwiązaniu bezpośrednio z interfejsu użytkownika systemu Splunk.
- aplikacja musi umożliwiać przegląd logów gromadzonych w ofertowanym rozwiązaniu bezpośrednio z konsoli Splunk, bez potrzeby ich indeksowania w systemie Splunk.
- aplikacja utworzona dla Splunk musi wspierać tworzenie szczegółowych zapytań kierowanych do oferowanego rozwiązania oraz ich opcjonalne dalsze przetwarzanie potokowe z wykorzystaniem skład języka Splunk Programming Language.
- aplikacja musi być oficjalnie wspierana przez producenta rozwiązania Splunk lub producenta oferowanego rozwiązania centralnego gromadzenia zdarzeń.

6. Raportowanie i Archiwizacja danych

- system musi zapewniać wbudowany mechanizm archiwizacji danych w postaci plików płaskich oraz ich zarządzaniem z poziomu konsoli użytkownika.
- mechanizm archiwizacji musi posiadać funkcjonalność przesyłania danych online do archiwum według zadanych kryteriów w sposób automatyczny lub ręczny.
- mechanizm archiwizacji musi umożliwiać pozwalać na przywracanie danych do systemu celem analizy online.
- mechanizm archiwizacji musi zapewniać funkcjonalność wyszukiwania w spakowanych danych bez potrzeby ich wcześniejszego rozpakowania.
- system musi zapewniać funkcjonalność generowania raportów z dowolnych danych gromadzonych w systemie.
- raporty muszą być generowane ręcznie oraz automatycznie według zdefiniowanego harmonogramu.
- system musi generować raporty do formatów minimum PDF oraz JPEG z jednoczesną możliwością opatrywania dokumentu logo Zamawiającego oraz komentarzami.
- lista źródeł
- zależnie od chęci Zamawiającego można podać listę systemów źródłowych objętych wdrożeniem.

7. Wdrożenie

Zamawiający zapewni infrastrukturę serwerową opartą o wirtualizację Vmware niezbędną do uruchomienia systemu oraz zasoby dyskowe przeznaczone na przechowywanie logów.

Zakres oczekiwanych prac związanych z wdrożeniem systemu:

- opracowanie harmonogramu wdrożenia systemu.
- przeprowadzenie przez Wykonawcę analizy przedwdrożeniowej oraz projektu technicznego wdrożenia.
- przeprowadzenie instalacji i konfiguracji systemu.
- podłączenie do systemu wskazanych przez Zamawiającego źródeł danych:
  - kontrolery Active Directory (6 kontrolery AD)
  - Firewall Paloalto Networks (2 urządzenia fizyczne + 1 wirtualne)
  - poczta elektroniczna Zimbra
  - serwery plików
  - przełączniki sieciowe Cisco
  - serwery Microsoft Application Request Routing
  - serwery WWW (apache, ngnix, IIS)
- do podłączonych źródeł Wykonawca musi skonfigurować reguły korelacyjne, raporty oraz dashboardy z wykorzystaniem gotowych komponentów dostarczonych wraz z systemem.
- Jeżeli oferowany system nie posiada predefiniowanych parserów, wizualizacji, dashboardów oraz reguł korelacyjnych Wykonawca jest zobligowany do ich implementacji na etapie wdrożenia.
- wykonawca na etapie analizy przedwdrożeniowej przedstawi do akceptacji Zamawiającego listę proponowanych reguł korelacyjnych, wizualizacji oraz dashboardów odnoszących się do zidentyfikowanych źródeł danych.
- przygotowanie i przeprowadzenie scenariuszy testowych weryfikujących wydajność i poprawność wdrożonego systemu w środowisku Zamawiającego.
- proponowane scenariusze będą przedłożone Zamawiającemu do akceptacji.

Szkolenie

- Wykonawca przeprowadzi szkolenia z zakresu użytkowania oraz administrowania systemem dla min 4 pracowników Zamawiającego w wymiarze 2 dni roboczych (min. 16h roboczych).
- szkolenie odbędzie się w siedzibie Zamawiającego.
- szkolenie musi być prowadzone w języku polskim.
- każdy uczestnik szkolenia otrzyma materiały szkoleniowe przygotowane w języku polskim lub angielskim.
- osoby prowadzące szkolenie muszą posiadać certyfikat wystawiony przez producenta oferowanego rozwiązania potwierdzające ich kompetencje w zakresie użytkowania i administrowania systemem.