Ri.271.56.2025

Opis techniczny przedmiotu zamówienia

Informacje o zamawiającym i przedmiocie zakupu.

Osoby upoważnione do kontaktowania się z wykonawcami w sprawie przedmiotu zamówienia:

Robert Kretowicz, tel. (22) 766-40-33;

Maciej Skarżyński, tel. (22) 766-40-94.

Przedmiot zamówienia:

Zakup oprogramowania do zbierania i zaawansowanej analizy logów z możliwością integracji z innymi systemami bezpieczeństwa w ramach realizacji projektu „Wzmocnienie zdolności do przeciwdziałania zagrożeniom informatycznym i reakcji na te zagrożenia w Gminie Miejskiej Legionowo. Program Fundusze Europejskie na Rozwój Cyfrowy (FERC) Priorytet – II. Zaawansowane usługi cyfrowe Działanie - 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa - nr wniosku FERC.02.02-CS.01-001/23/1713 - nr naboru FERC.02.02-CS.01-001/23.”

Opis przedmiotu zamówienia:

1 Oprogramowanie do zbierania i zaawansowanej analizy logów z możliwością integracji z innymi systemami bezpieczeństwa w ramach realizacji projektu „Wzmocnienie zdolności do przeciwdziałania zagrożeniom informatycznym i reakcji na te zagrożenia w Gminie Miejskiej Legionowo. Program Fundusze Europejskie na Rozwój Cyfrowy (FERC) Priorytet – II. Zaawansowane usługi cyfrowe Działanie - 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa - nr wniosku FERC.02.02-CS.01-001/23/1713 - nr naboru FERC.02.02-CS.01-001/23.” o funkcjonalności nie słabszej niż:

1.1 System musi pracować w oparciu o architekturę Linux;

1.2 System musi mieć możliwość centralnego zbierania i zarządzania logami;

1.3 System działać w trybie zbliżonym do rzeczywistego;

1.4 System musi umożliwiać funkcjonowanie bez dostępu do sieci internet;

1.5 System musi zapewniać efektywną obsługę do 100 GB danych dziennie;

1.6 System nie może ograniczać ilości zarejestrowanych lub jednoczesnych użytkowników systemu;

1.7 Licencja na oferowany system nie może ograniczać ilości źródeł danych, z których pobierane są dane i zdarzenia;

1.8 Interfejs musi posiadać angielską lub polską wersję językową;

1.9 System musi zapewniać pełen audyt aktywności jego użytkowników, w tym: udanych/nieudanych logowaniach, pełnej historię operacji, realizowanych zapytań, zmian uprawnień;

1.10 System musi zapewniać mechanizmy umożliwiające pracę w trybie multitenant;

1.11 System musi pozwalać na tworzenie parserów z poziomu GUI;

1.12 System musi umożliwiać predykcję danych w oparciu o dowolne dane historyczne zgromadzone w systemie;

1.13 System musi być wyposażony w zaawansowane metody analizy danych oparte na algorytmach sztucznej inteligencji;\

1.14 Algorytmy sztucznej inteligencji muszą wspierać pracę operatora w wykrywaniu anomalii w danych: pojedynczego parametru liczbowego, wielu parametrów liczbowych, tekstu oraz danych mieszanych. Oczekuje się, że wykrywanie anomalii będzie połączone z obliczaniem punktów, co umożliwi operatorowi skoncentrowanie swojej pracy na zdarzeniach o najwyższych wynikach;

1.15 Algorytmy sztucznej inteligencji muszą umożliwiać nienadzorowane, dynamiczne grupowanie zdarzeń na podstawie ich wspólnych cech. Dodatkową wartością będzie możliwość graficznej wizualizacji zdarzeń tworzących większe lub mniejsze grupy, aby izolowane zdarzenia można było łatwo zidentyfikować;

1.16 Wykrywanie anomalii musi umożliwiać tworzenie reguł detekcji, aby możliwa była szybka reakcja w sytuacjach, które się pojawiają.

1.17 System musi zapewniać wizualizację danych w postaci, oryginalnych logów, list, wykresów i diagramów;

1.18 System musi umożliwiać graficzną wizualizację zidentyfikowanych połączeń sieciowych pomiędzy adresami IP;

1.19 System musi umożliwiać funkcjonalność eksportu danych o Zdarzeniach i Incydentach do formatu CSV i HTML m.in. w celu analizy wyników działania reguł korelacyjnych;

1.20 System musi zapewniać parsowanie spływających do niego wiadomości w formatach:

1.20.1 Syslog;

1.20.2 SNMP trap;

1.20.3 XML;

1.20.4 JSON;

1.20.5 CSV;

1.20.6 system musi pozwalać na implementację innych formatów w przypadku

zaistnienia takiej potrzeby ze strony Zamawiającego;

1.21 System musi zbierać logi z rozwiązań chmurowych opartych minimum o AWS oraz Microsoft Azure;

1.22 System musi umożliwiać gromadzenie danych z baz danych relacyjnych, NoSQL, czasu rzeczywistego, m.in. MSSQL, Oracle, PostgreSQL, SQL Server, MongoDB, Apache Cassandra, InfluxDB i Apache Kafka;

1.23 System 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;

1.24 System musi do przyjmowania zdarzeń wykorzystywać zarówno mechanizmy agentowe jak i bezagentowe;

1.25 System musi posiadać predefiniowany zestaw parserów zdarzeń;

1.26 System musi mieć funkcjonalność Bad IP Reputation tj. porównywania adresów IP z bazami reputacyjnymi dostarczonymi przez producenta;

1.27 System musi wspierać geolokalizację zdarzeń na bazie adresów IP;

1.28 Proces parsowania musi umożliwiać anonimizację Danych Wejściowych celem ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzny procedury bezpieczeństwa;

1.29 System powinien pozwalać na rozpoznanie formatów czasu i daty oraz normalizowanie ich do jednego wspólnego formatu;

1.30 System 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;

1.31 Komponent budowania elektronicznej dokumentacji musi mieć możliwość m.in. tworzenia lub dodawania diagramów architektury zasobów informatycznych, tabel oraz list;

1.32 System musi posiadać interfejs umożliwiający zmianę wybranej wartości w zgromadzonych danych;

1.33 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;

1.34 System musi umożliwiać tworzenie własnych reguł korelacyjnych na bazie reguł odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie, w tym;

1.34.1 Wykrycia dowolnej treści w logach;

1.34.2 Wykrycia wystąpienia wartości pola na wybranej liście;

1.34.3 Wykrycia niewystępowania wartości pola na wybranej liście;

1.34.4 Wykrycia zmiany jednego z kilku pól;

1.34.5 Wykrycia zdarzeń występujących z zadaną częstotliwością;

1.34.6 Wykrycia zdarzeń, których liczba zmienia się w wskazany sposób względem czasu poprzedniego;

1.34.7 Wykrycia zaniku Wiadomości;

1.35 System musi umożliwić korelację zdarzeń pochodzących z różnych źródeł informacji z anomaliami wykrywanymi m.in. w. Netflow oraz wykrytymi podatnościami zidentyfikowanymi przez skaner podatności;

1.36 System musi umożliwiać analizę ruchu sieciowego poprzez przechwytywanie i inspekcję pakietów w czasie rzeczywistym, w tym minimum protokołów HTTP DNS, FTP oraz SSH;

1.37 System na bazie gromadzonej kopii ruchu sieciowego musi identyfikować i klasyfikować ataki w oparciu o sygnatury oraz zachowanie użytkowników;

1.38 System musi umożliwiać zapisywanie pakietów ruchu sieciowego w formacie PCAP;

1.39 Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień o Incydentach do innych systemów bądź zdefiniowanych użytkowników (co najmniej: powiadamianie email, opcjonalnie SMS, czat);

1.40 System musi pozwalać na zautomatyzowane szacowanie ryzyka dla dowolnych kryteriów w ramach przetwarzanych zdarzeń. W rozwiązaniu musi być obecna funkcjonalność. kategoryzacji obiektów (adresy IP, loginy i inne pola), dla których mechanizm szacowania ryzyka uwzględni podane wagi;

1.41 System umożliwia konfiguracje automatycznych akcji, które są wykonywane na monitorowanych systemach w przypadku detekcji zagrożenia wskazanego w regule;

1.42 System musi posiadać wbudowany, dostepny z poziomu GUI moduł tworzenia i edycji elektronicznej dokumentacji bazującej oraz wzbogacającej dane gromadzone ze środowiska informatycznego;

1.43 Oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów;

1.44 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.;

1.45 Szyfrowanie komunikacji z przeglądarką internetową użytkownika musi wykorzystywać protoków TLS w wersji minimum 1.3.;

1.46 System musi posiadać interfejs graficzny dostępny z poziomu przeglądarki

internetowej min. Firefox, Chrome, Internet Explorer;

1.47 Dostęp do systemu musi być zabezpieczany hasłem lub certyfikatem;

1.48 Hasła typu Windows AD bind muszą być przechowywane w postaci zaszyfrowanej;

1.49 System musi umożliwiać zarządzanie czasem automatycznego wygasania sesji użytkowników;

1.50 System musi posiadać dedykowany widok zarządzania użytkownikami i rolami;

1.51 System posiada natywną integrację z Mitre ATT@CK;

1.52 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;

1.53 System musi posiadać możliwość skanowania środowiska pod kątem detekcji rootkit'u i wykrywania ukrytych procesów, plików, portów;

1.54 System musi posiadać funkcjonalności skanowania podatności dla aplikacji oraz systemów operacyjnych Linux i Windows;

1.55 Mechanizm archiwizacji musi umożliwiać pozwalać na przywracanie danych do systemu celem analizy online;

1.56 Mechanizm archiwizacji musi zapewniać funkcjonalność wyszukiwania w spakowanych danych bez potrzeby ich wcześniejszego rozpakowania;

1.57 System musi zapewniać funkcjonalność generowania raportów z dowolnych danych gromadzonych w systemie;

1.58 Raporty muszą być generowane ręcznie oraz automatycznie według zdefiniowanego harmonogramu;

2 Wykonawca w ramach przedmiotu zamówienia zapewni 36 miesięcy wsparcia od dnia dostarczenia oprogramowania, potwierdzonego podpisanym protokołu odbioru.

3 Wsparcie producenta musi być realizowane w języku polskim przez dedykowanych inżynierów.

4 Wsparcie nie może być limitowane ilością zgłoszeń i musi być realizowane zdalnie oraz z siedzibie Zamawiającego.

5 Support producenta musi być świadczony w formule minimum 8/5.

6 Wykonawca w ramach przedmiotu zamówienia przeprowadzi w pełni wdrożenie oprogramowania oraz wprowadzi administratorów Zamawiającego udzielając wszystkich niezbędnych informacji z zakresu użytkowania oraz administrowania systemem.