OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest dostawa i wdrożenie systemu monitorowania ruchu sieciowego oraz zarządzania bezpieczeństwem Security Information and Event Management (SIEM) i Network Behavior Anomaly Detection (NBAD) zwanego dalej Systemem mającego na celu realizację następujących funkcji:

- agregacja logów zbieranych z wielu źródeł danych, włączając w to urządzenia sieciowe, systemy operacyjne serwerów, oprogramowanie bezpieczeństwa (antywirusowe, firewall, IPS/IDS), aplikacje i bazy danych, polegająca na zgromadzeniu zbieranych do bazy danych Systemu oraz przetworzeniu ich do postaci użytecznej dla Systemu, mająca na celu zapewnienie, iż w procesie monitorowania nie zostaną pominięte zdarzenia bezpieczeństwa,
- korelacja – funkcja Systemu polegająca na łączeniu danych, pochodzących z różnych źródeł danych oraz różnych okresów ich pochodzenia, wyszukująca na podstawie wbudowanych reguł analitycznych cech dla nich wspólnych oraz przekształcająca je do postaci użytecznej dla funkcji detekcji, dzięki czemu funkcja detekcji może zidentyfikować wystąpienie zdarzenia bezpieczeństwa,
- detekcja – informowanie o automatycznie (na podstawie wbudowanych reguł detekcji) zidentyfikowanych w zbiorze danych zgromadzonych w skutek agregacji i korelacji zdarzeniach, mogących świadczyć o wystąpieniu zdarzenia bezpieczeństwa. Alarmowanie to powinno być realizowane poprzez wyświetlanie odpowiednich komunikatów na konsoli użytkownika Systemu i/lub poprzez wysyłanie alarmów, np. za pośrednictwem poczty elektronicznej,
- prezentacja – wyświetlanie wyników działania funkcji detekcji, korelacji i agregacji w postaci konsoli, na której w formie wykresów i grafów widoczne będą informacje o wszelkich zidentyfikowanych zdarzeniach, mogących świadczyć o wystąpieniu zdarzeń bezpieczeństwa oraz odbiegających od wzorca statystycznego zachowania obserwowanego przez System źródła danych,
- badanie zgodności – funkcja Systemu mająca na celu automatyzację gromadzenia danych dotyczących zachowania zgodności monitorowanych systemów z wymaganiami (np. wdrożonym u Zamawiającego Systemem Zarządzania Bezpieczeństwem Informacji) oraz sporządzająca w tym zakresie raporty,
- retencja – zapewnienie przechowywania logów i danych historycznych, mające na celu umożliwienie korelacji zdarzeń z różnych źródeł w różnych okresach, a także zapewnienie dostępu do logów historycznych, w chwili wystąpienia konieczności przeprowadzenia dochodzenia kryminalistycznego dotyczącego zidentyfikowanego naruszenia zasad bezpieczeństwa.

Opis szczegółowy Systemu:

System ma zostać dostarczony w formie urządzenia/urządzeń fizycznych rejestrujących zdarzenia. Pożądane parametry urządzeń przedstawione są w poniższym opisie. Wraz z urządzeniami musi zostać dostarczona konsola zarządzająca, spełniająca wymagania producenta odnośnie pracy i zarządzania urządzeniem/urządzeniami.

Każde z urządzeń rejestrujących ma spełnić poniższe parametry i funkcjonalności:

a. Musi posiadać wydajność co najmniej 300 (EPS) zdarzeń na sekundę oraz 15000 strumieni (Flows) na minutę,
b. Musi posiadać możliwość rozbudowy do 5000 EPS i 100000 Flow/min. poprzez rozszerzenie licencyjne,
c. Musi działać na bazie dostrojonego przez producenta systemu operacyjnego. Cena systemu operacyjnego musi być wliczona w cenę dostarczanego rozwiązania,
d. Musi umożliwiać integrację z zewnętrznymi repozytoriami danych, co najmniej NAS,
e. Musi umożliwiać przechowywanie logów (sparsowanych i surowych) oraz danych z przepływów sieciowych przez okres co najmniej 90 dni.

- System musi utrzymywać centralne repozytorium logów pobieranych z innych urządzeń i systemów oraz realizować funkcje Security Information and Event Management (SIEM) i Network Behavior Anomalny Detection (NBAD).
- W raz z systemem należy dostarczyć platformę sprzętową umożliwiającą płynne korzystanie z Systemu i przechowywanie danych historycznych przez okres co najmniej 90 dni (minimalnie 1 CPU 4core, 24 GB RAM, 2 TB HDD, 2 NIC) oraz niezbędne oprogramowanie .

- Funkcjonalności modułów SIEM i NBAD:

  a. Moduł SIEM musi pobierać logi z wielu różnych elementów systemu informatycznego, poddawać je korelacji i na tej podstawie przedstawiać administratorom wiarygodne informacje na temat stanu bezpieczeństwa i wykrytych incydentów.
  b. Moduł NBAD na podstawie statystyk i opisu ruchu (NetFlow, sflow itp.) pobieranych bezpośrednio z urządzeń sieciowych (ruterów, przełączników) musi dokonywać analizy stanu i efektywności pracy sieci, w tym wykrywania sytuacji nieprawidłowych (anomalii).
  c. Moduł NBAD musi dokonywać wykrywania anomalii w systemie informatycznym za pomocą analizy behawioralnej. W tym celu muszą być na bieżąco budowane profile normalnego stanu i zachowania sieci oraz identyfikowane odchylenia (m.in. zmiany stanu, nagłe zwiększenia lub zmniejszenia natężenia ruchu i przekroczenie wartości progowych).
  d. Moduł NBAD musi posiadać możliwość wykrywania nowych obiektów w systemie informatycznym (hostów, aplikacji, protokołów, itd.). Moduł NBAD musi także posiadać możliwość wykrywania awarii systemów, m.in. zablokowanych lub uszkodzonych serwerów i aplikacji.
  e. Moduły SIEM i NBAD muszą być zintegrowane ze sobą tak, aby informacje o naruszeniach bezpieczeństwa były przedstawiane na podstawie analiz obu tych modułów.
  f. Moduł analizy pakietów musi zapewniać głęboką analizę pakietów (deep packet inspection) dostarczając takich informacji jak: rodzaj aplikacji, porty komunikacji, adresy IP, zawartość nagłówków pakietów, kierunki transmisji, właściwości ilościowe transmisji.
  g. Korelacja zdarzeń powinna odbywać się w sposób ciągły w czasie rzeczywistym a także umożliwiać korelację zdarzeń historycznych dla zapewnienia możliwości testowania reguł na zdarzeniach (logi i przepływy) które wystąpiły wcześniej.

- Obsługa incydentów bezpieczeństwa musi odbywać się na podstawie wielu źródeł informacji, nie mniej niż:
  a. Zdarzenia i logi z systemów zabezpieczeń (firewall, VPN, IPS, AV, itd.), systemów operacyjnych (Unix, Microsoft Windows, itd.) oraz aplikacji i baz danych.
  b. Statystyki i opis ruchu sieciowego odbierane z urządzeń za pomocą NetFlow, J-Flow, S-Flow i Packeteer oraz odczytywane bezpośrednio z sieci (span port).

c. Informacje na temat stanu systemów i ich słabości bezpieczeństwa odczytywane za pomocą skanerów Nessus, NMAP.

- Rozwiązanie musi umożliwiać:
  a. Pobieranie logów z innych systemów za pomocą wielu metod, nie mniej niż Syslog (standardowy format logów, protokoły TCP i UDP), SNMP (wiadomości o zdarzeniach przesyłane poprzez SNMP Trap), a także Security Device Event Exchange (SDEE) i Java Database Connectivity API (JDBC).
  b. Odczytywanie logów z systemów operacyjnych Microsoft Windows (stacje robocze i serwery), Linux (nie mniej niż Ubuntu)i Unix (free BSD),, wymagane protokoły WMI, SCP, SFTP, SMB.
  c. W zakresie odczytu logów musi umożliwiać integrację z innymi systemami zarządzania zabezpieczeń.

- System musi posiadać możliwość:
  a. Powiadamiania administratorów o zdarzeniach za pomocą co najmniej email, SNMP oraz Syslog.
  b. Nawiązania połączenia z urządzeniami zabezpieczeń sieci w celu zablokowania niedozwolonej komunikacji.
  c. Przypisywanie zidentyfikowanych incydentów bezpieczeństwa do obsługi określonym administratorom.
  d. Wdrożenia poszczególnych urządzeń w architekturze scentralizowanej (wszystkie funkcje na jednym appliance) oraz rozproszonej, złożonej z wielu urządzeń. W przypadku rozproszonej struktury zarządzanie całości Systemu musi odbywać się z jednej konsoli. W przypadku rozproszonej struktury musi być możliwość kryptograficznej ochrony (szyfrowanie) komunikacji sieciowej pomiędzy komponentami Systemu.
  e. Definiowania precyzyjnych uprawnień administratorów w zakresie monitorowanego obszaru systemu informatycznego oraz dostępnych operacji w Systemie. Tożsamość administratorów musi być weryfikowana poprzez lokalne konto oraz zewnętrzne systemy uwierzytelniania - co najmniej RADIUS, LDAP i Active Directory.
  f. Do celów obsługi zdarzeń musi utrzymywać centralne repozytorium logów z możliwością ich przeglądania w formie rzeczywistej (raw) oraz znormalizowanej. Dla logów System musi utrzymywać wskaźniki czasu (timestamp). Starsze logi muszą być poddawane kompresji.
  g. Składowanie informacje w bazie danych zaprojektowanej w sposób zoptymalizowany pod proponowany System do obsługi zdarzeń i ich korelacji. Baza danych powinna zapewniać dostęp do danych bieżących i archiwalnych bez konieczności przywracania ich z kopii zapasowych. Składowane w systemie zarządzania informacje muszą być zabezpieczone kryptograficznie za pomocą sum kontrolnych - dostępne są minimum funkcje MD5, SHA-1 oraz SHA-2 (NIST FIPS 180-2).
  h. Wykonywania operacji backup i restore, uruchamianych z graficznej konsoli. System musi mieć możliwość wykonywania archiwizacji informacji do zewnętrznych repozytoriów danych – nie mniej niż NAS.
  i. Utworzenie wielu zaawansowanych reguł korelacyjnych w tym możliwość tworzenia korelacji na danych historycznych. Poniżej w tabeli zawarto przykładowe reguły, które powinny być móc utworzone celem generowania alarmów/incydentów.

Lp.	Przykładowe reguły korelacyjne, generowanie zdarzeń i alarmów
1	2
I.	**Funkcje detekcji** Detekcja następujących incydentów:
A	Wszystkie systemy:
1.	Logowanie i próby logowania na konta root/administrator. Incydent powinien być generowany dla przypadków: logowanie się na konto administrator/root na wielu systemach z jednego komputera, logowanie z wielu komputerów na konto administrator/root w jednym systemie, próby nieudanego logowania na konto root/administrator – priorytet wysoki
2.	Nieudane próby logowania. Odnotowywanie nieudanych prób logowania się na dowolne konta w dowolnych systemach, po przekroczeniu określonego progu dla konta lub systemu powinien być generowany incydent – priorytet wysoki
3.	Dodanie konta administratora. Incydent generowany w przypadku utworzenia konta z podniesionymi uprawnieniami w systemie – priorytet wysoki
4.	Zarządzanie użytkownikami. Incydent powinien być generowany w przypadku wystąpienia zdarzenia – priorytet niski
5.	Zmiana hasła administratora (członków grup administratorów). Incydent powinien być generowany w przypadku wystąpienia zdarzenia zmiany hasła dla dowolnego konta ze wskazanej listy kont administracyjnych – priorytet średni
6.	Wykorzystanie uprawnień administratora (przejęcie zasobów na własność, reset hasła użytkownika). Incydent powinien być wygenerowany w przypadku wystąpienia zdarzenia polegającego na przejęciu uprawnień do zasobów użytkownika przez administratora – priorytet wysoki
7.	Restarty serwerów. Incydent powinien być generowany w przypadku wystąpienia restartu serwera – priorytet niski
8.	Instalacja nowego oprogramowania. Incydent powinien być generowany w przypadku zarejestrowania instalacji nowego oprogramowania na serwerze – priorytet niski
9.	Zmiana polityki haseł. Incydent powinien być generowany w przypadku zarejestrowania zmiany polityki haseł w domenie, serwerze, komputerze – priorytet wysoki

Lp.	Przykładowe reguły korelacyjne, generowanie zdarzeń i alarmów
1	**2**
10.	Zmiana polityk inspekcji zabezpieczeń. Incydent powinien być generowany w przypadku zmiany w politykach inspekcji zabezpieczeń – priorytet wysoki
11.	Zmiana konfiguracji interfejsów sieciowych. Incydent powinien być generowany w przypadku zarejestrowania dodania nowego interfejsu sieciowego (LAN, modem) na serwerach – priorytet średni
12.	Dodanie lub usunięcie nowego dysku. Incydent powinien być generowany w przypadku dodania nowego dysku na serwerach – priorytet średni
13.	Skasowanie lub przepełnienie dziennika logów. Incydent powinien być generowany w przypadku wystąpienia przepełnienia lub skasowania dziennika logów (inspekcji, aplikacji lub systemu) – priorytet wysoki
14.	Zmiana czasu. Incydent powinien być generowany, jeżeli w zdarzeniach zarejestrowano zmianę czasu systemowego lub czas pobrania logu z maszyny różni się znacznie od czasu w logu
15.	Deaktywacja lub zmiana konfiguracji zapory sieciowej. Incydent powinien być generowany, jeżeli nastąpi zmiana konfiguracji zapory sieciowej lub jej wyłączenie
16.	Deaktywacja lub odinstalowanie oprogramowania antywirusowego. Incydent powinien być generowany, jeżeli nastąpi deaktywacja lub odinstalowanie oprogramowania antywirusowego
17.	Błąd wykonania zadania kopii zapasowych. Incydent powinien być generowany, jeżeli zadanie wykonania kopii zapasowej serwera zwróci błąd
18.	Zmiana sum kontrolnych plików. Incydent powinien być generowany dla tych serwerów, dla których uruchomiono usługę weryfikacji sum kontrolnych plików w przypadku ich zmiany
19.	Skanowanie adresów IP i portów. Incydent powinien być generowany w przypadku wykrycia próby skanowania adresów IP
20.	Infekcja złośliwym oprogramowaniem. Incydent powinien być generowany w przypadku zarejestrowania infekcji złośliwym oprogramowaniem
21.	Próba infekcji złośliwym oprogramowaniem.

Lp.	Przykładowe reguły korelacyjne, generowanie zdarzeń i alarmów
1	2
	Incydent powinien być generowany w przypadku wykrycia próby infekcji złośliwym oprogramowaniem
B	Sieć:
22.	Podłączenie nieznanego urządzenia do sieci. Incydent powinien być generowany w przypadku podłączenia do sieci nieznanego urządzenia
23.	Wykrycie anomalii w ruchu sieciowym na podstawie informacji statystycznych o (w zależności od licencji systemu i możliwości zebrania danych): • adresie źródłowym i docelowym, • cechach charakterystycznych dla danego protokołu (adresy portów, flagi, itp.), • zawartości przesyłanych danych, • wolumenie danych, sekwencji przesyłanych danych, • czasie, w jakim dane są przesyłane
24.	Próby nawiązania sesji administracyjnej do urządzenia sieciowego. Incydent powinien być generowany w przypadku wykonania nieudanej próby wykonania sesji administracyjnej do urządzenia sieciowego bazując na logach uwierzytelnienia oraz potwierdzenia ruchu na bazie transmisji sieciowej
25.	Wykonanie zmiany konfiguracji urządzenia sieciowego. Incydent powinien być generowany w przypadku zarejestrowania zmiany konfiguracji urządzenia sieciowego
26.	Awaria urządzenia firewall. Incydent powinien być generowany w przypadku awarii urządzenia firewall
27.	Zmiana konfiguracji serwera zarządzania i monitorowania sieci. Incydent powinien być generowany w przypadku zarejestrowania zmiany konfiguracji serwera zarządzania i monitorowania sieci
C	Serwery proxy:
28.	Wykrycie anomalii proxy, np.: próby komunikacji do C&C z wielu hostów w sieci wewnętrznej, wysyłanie dużej ilości pakietów danych do sieci zewnętrznej z jednego hosta, próby komunikacji do sieci IRC, próby komunikacji do sieci TOR.
29.	Zmiana konfiguracji usługi proxy. Incydent powinien być generowany w przypadku zarejestrowania zmiany konfiguracji usługi proxy (dodanie lub modyfikacja udostępnianych usług, zmiana zasad przechowywania logów inspekcji, dodanie użytkownika)
30.	Nawiązanie sesji administracyjnej do proxy.
D	Stacje robocze:
31.	Nieudane próby logowania do stacji roboczej.

Lp.	Przykładowe reguły korelacyjne, generowanie zdarzeń i alarmów
1	**2**
	Incydent powinien być generowany w przypadku zarejestrowania próby logowania do stacji roboczej (nie do domeny)
32.	Użycie uprawnień administratora lokalnego. Incydent powinien być generowany w przypadku zarejestrowania użycia uprawnień administratora (lokalnego lub domenowego) polegającej na przejęciu własności obiektów w systemie
33.	Zmiana poziomu uprawnień usługi lub procesu na stacji roboczej (np. zmiana właściciela usługi na SYSTEM). Incydent powinien być generowany w przypadku zarejestrowania faktu wystąpienia zmiany poziomu usługi uruchomionej na stacji roboczej
34.	Zmiana uprawnień użytkownika lokalnego.
35.	Wysyłanie dużej ilości (np. pow. 10 plików/3 dni z jednej stacji roboczej) plików do sieci publicznej.
E	Domena MS Active Directory:
36.	Blokada konta użytkownika.
37.	Wpisanie hasła użytkownika w polu nazwy użytkownika (w zależności od jakości logów i danych referencyjnych)
38.	Brak logowania użytkownika przez okres co najmniej 1-go miesiąca.
39.	Zmiana uprawnień użytkownika.

j. Tworzenia wielu typów raportów generowanych zgodnie z kryteriami ustalonymi przez administratorów oraz na podstawie predefiniowanych wzorców (raportów). Raporty muszą być tworzone są w wielu formatach - minimum PDF, HTML, CSV, RTF i XML. System musi posiadać predefiniowane raporty.

Wymagane raporty:

Raport dobowy zbiorczy z incydentów.
Raport dobowy zbiorczy z incydentów ze źródła danych dla administratora źródła danych.
Raport miesięczny zbiorczy z incydentów.
Raport miesięczny zbiorczy z incydentów ze źródła danych dla administratora źródła danych.
Raporty incydentów wg. ISO27001 Możliwości generowania następujących raportów wg. ISO27001:

restarty serwerów,
blokady kont,
zmiany kont administracyjnych,
wszystkie logowania,
wszystkie błędne logowania,
błędy logowania na konta administracyjne,
zmiany kont w domenie,
zmiany w grupach,
zmiany polityk bezpieczeństwa,
zmiany polityk audytu,
zmiany relacji zaufania w domenie,
przepełnienie dzienników logów,
restarty,
resety haseł,
wyczyszczenie dzienników bezpieczeństwa,
użytkownicy nie logujący się od zadanego okresu,
Konsole Możliwość definiowania przykładowych konsol:
incydenty z podziałem na priorytet (ilość w danym priorytecie w okresie predefiniowanym: ostatnia godzina, doba)
incydenty z podziałem na priorytet dla wybranego źródła danych,
bieżące zdarzenia,
zdarzenia o najwyższym priorytecie,
Alarmy,
komputery z największą liczbą alarmów,
użytkownicy z największą liczbą alarmów,
Top 10 użytkowników z błędnymi logowaniami,
Top 10 komputerów zablokowanych na proxy/firewall,
komputery zainfekowane złośliwym oprogramowaniem,
status pracy systemu SIEM (zajętość dysków, pamięci, procesora, błędy i zawieszenia się),
Top 10 alarmów z firewall,
Top 10 alarmów z IPS,

W celu sprawnego przeszukiwania predefiniowanych raportów muszą być one pogrupowane - co najmniej według typu urządzeń i zdarzeń bezpieczeństwa.

k. Utrzymywać szczegółowy log audytowy rejestrujący co najmniej następujące operacje administratorów - logowanie/wylogowanie i zmiany konfiguracji Systemu.
l. Weryfikacji poprawności swojego działania i powiadamiania administratorów o nieprawidłowościach - co najmniej za pomocą wpisu do logów systemowych oraz SNMP Trap.

- Administratorzy Systemu muszą mieć do dyspozycji dedykowane, graficzne narzędzia, uruchamiane z wykorzystaniem standardowej przeglądarki Web.
- Realizacja przeglądania zdarzeń (logów i przepływów) powinna być zapewniona w sposób graficzny nie wymagający znajomości jakiegokolwiek języka skryptowego, bazodanowego lecz poprzez wybieranie odpowiednich pól na temat wybranych fragmentów opisujących logi.

Wymagania dodatkowe:

- Wykonawca dokona wdrożenia systemu – instalacji i konfiguracji w siedzibie Zamawiającego oraz przeszkolenia jego personelu – do 3 administratorów.
- System musi posiadać wsparcie przez okres co najmniej 1 roku obejmujące pomoc techniczną, prawo do nowych wersji systemu oraz dostęp do dodatkowych źródeł informacji (nowe zagrożenia, botnet, sygnatury, reguły korelacyjne).
- Dostarczone elementy sprzętowe muszą być objęte gwarancją przez okres co najmniej 3 lat.