Warunki równoważności dotyczące znaków towarowych wskazanych w treści Umowy i załączników

I. Cisco Certified Network Professional - za certyfikat równoważny do Cisco Certified Network Professional Zamawiający uzna certyfikat potwierdzający poniższe umiejętności:

1) Instalacja i konfiguracja routerów
2) Konfiguracja VLAN
3) Konfiguracja Spanning-Tree
4) Konfiguracja BGP
5) Konfiguracja ISIS
6) Konfiguracja HSRP

II. Brocade Certified Network Professional - za certyfikat równoważny do Brocade Certified Network Professional Zamawiający uzna certyfikat potwierdzający poniższe umiejętności:

1) Instalacja i konfiguracja przełączników LAN
2) Konfiguracja VLAN
3) Konfiguracja Spanning-Tree
4) Konfiguracja OSPF
5) Konfiguracja MCT
6) Konfiguracja VRRP-E
7) Konfiguracja stosów przełączników
8) Konfiguracja MRP

III. Technologia Cisco – technologia równoważna do technologii Cisco to urządzenia sieciowe typu router pracujące w trzeciej warstwie modelu OSI. Służące do łączenia różnych sieci komputerowych, pełniące rolę węzła komunikacyjnego. Na podstawie informacji zawartych w pakietach TCP/IP mogące przekazać pakiety z dołączonej do siebie sieci źródłowej do docelowej, rozróżniając ją spośród wielu dołączonych do siebie sieci.

IV. Technologia Brocade – technologia równoważna do technologii Brocade to urządzenia typu switch łączące segmenty sieci komputerowej, pracujące głównie w drugiej warstwie modelu ISO/OSI. Urządzenia przekazujące ramki między segmentami sieci z doborem portu przełącznika, na który jest przekazywana.

V. System Zabbix – technologia równoważna do systemu Zabbix to system umożliwiający monitorowanie różnych komponentów IT, w tym sieci, serwerów, maszyn wirtualnych (VM) i usług w chmurze.

1. System musi zapewnić monitorowanie metryk, między innymi wykorzystania sieci, obciążenia procesora i zużycia miejsca na dysku. Konfiguracja monitorowania może być wykonana za pomocą szablonów opartych na XML, które zawierają elementy do monitorowania. Oprogramowanie monitoruje operacje na systemach Linux, Hewlett Packard Unix (HP-UX), Mac OS X, Solaris i innych systemach operacyjnych.
2. System musi posiadać następujące opcje monitorowania:
   1) Proste kontrole mogą zweryfikować dostępność i czas reakcji standardowych usług, takich jak SMTP lub HTTP, bez instalowania żadnego oprogramowania na monitorowanym hoście.
   2) Musi zawierać obsługę monitorowania poprzez kontrole SNMP, TCP i ICMP, a także przez IPMI, JMX, SSH, Telnet i używanie niestandardowych parametrów.

VI. SIEM – technologia równoważna do rozwiązania SIEM posiadanego przez Zamawiającego musi spełniać następujące wymagania:

1. Funkcjonalność Systemu

1) zapewnienie funkcji: pobierania, normalizacji danych, przechowywania, wyszukiwania i zarządzania bazą zebranych zdarzeń, warstwy analitycznej i interfejsu użytkownika;
2) skalowalność oraz dodawanie kolejnych komponentów Systemu, które zapewniać będą rozwój możliwości operacyjnych rozwiązania (zwiększenie wydajności, widoczności źródeł oraz przestrzeni dyskowej);
3) aktualizowane na bieżąco rozwiązania reguły korelacyjne;
4) dokonywanie analizy stanu i efektywności pracy sieci, w tym wykrywanie sytuacji nieprawidłowych, anomalii, na podstawie statystyk oraz opisu ruchu pobieranych bezpośrednio z urządzeń sieciowych oraz urządzeń bezpieczeństwa;
5) budowanie profilu stanu i zachowania sieci oraz identyfikowanie odchyleń i wykrywanie anomalii na podstawie analizy behawioralnej;
6) wykrywanie nowych urządzeń w infrastrukturze informatycznej;
7) graficzny interfejs użytkownika dostępny przez przeglądarkę internetową, w którym dostępne będą wszystkie funkcjonalności niezbędne do zarządzania incydentami bezpieczeństwa;
8) wizualizacja danych na raportach i dashboardach z wykorzystaniem tabel, listy zdarzeń, wykresów, map oraz map kolorowanych;

9) automatyczne tworzenie kopii zapasowej konfiguracji Systemu;
10) generowanie raportów oraz zapisywanie raportów do pliku w formacie min. pdf oraz csv;
11) mechanizm automatycznej kontroli własnego stanu oraz alarmowanie w przypadku wykrytych nieprawidłowości;
12) samodzielne zarządzanie retencją danych;
13) budowanie dedykowanych widoków oraz dashboard'ów, które mogą zawierać konfigurowalne elementy prezentacji danych (wykresy, listy, tabele, statystyki, etc.);
14) możliwość integracji z zewnętrznymi skanerami podatności;
15) integracja ze wskazaną usługą serwera czasu;
16) korelowanie zdarzeń w celu identyfikacji naruszeń bezpieczeństwa;
17) normalizacja danych źródłowych, w tym prezentowanie istotnych pozycji informacyjnych tj. data i czas zdarzenia, adres źródłowy, adres docelowy, port źródłowy, port docelowy, użytkownik;
18) określanie krytyczności oraz priorytetu źródła danych;
19) przeglądanie (w jednej konsoli systemu) logów pobieranych/dostarczanych do Systemu w celu uniknięcia konieczności logowania się do każdego monitorowanego systemu osobno. Filtrowanie w czasie rzeczywistym będzie dopuszczać wyszukiwanie informacji za pomocą wyrażeń regularnych (REGEX) lub gotowych wzorców np: adres IP źródłowy/docelowy, port, protokół;
20) wyszukiwanie zdarzeń w oparciu o definiowane wzorce zapytań (np: srcip, dstip, srcport, dstport adres IP źródłowy/docelowy, port, protokół, nazwa DNS, nazwa użytkownika, zakres dat, lokalizacja sieciowa, słowa kluczowe);
21) wyszukiwanie zdarzeń w oparciu o wyrażenia regularne (REGEX) lub dedykowany, spójny dla rozwiązania język zapytań;
22) centralne gromadzenie danych źródłowych i ich bezpieczne przechowywanie oraz dostępność przez okres minimum 30 dni;
23) zawierać funkcjonalność precyzyjnego nadawania uprawnień użytkownikom i administratorom. Zarówno, jeśli chodzi o określenie zakresu monitorowania obszaru infrastruktury informatycznej, jak i dostępności do informacji z poszczególnych korelacji.

2. System musi zapewnić obsługę źródeł danych:

1) platformy wirtualizacji;
2) ruch sieciowy w postaci kopii pakietów (span port);
3) ruch sieciowy w postaci netflow;
4) serwery aplikacyjne (serwery www takie jak IIS, Apache, serwery FTP, ect.);
5) serwery bazodanowe (Oracle, MS SQL, MySQL, PostgreSQL);

6) system protekcji poczty elektronicznej;
7) system protekcji urządzeń mobilnych;
8) systemy operacyjne (Microsoft Windows, Unix / Linux, Apple OSX);
9) urządzenia i systemy bezpieczeństwa (zapory sieciowe, aplikacyjne zapory sieciowe, systemy antywirusowe, systemy EDR, IDM, DAM, IPS/IDS);
10) urządzenia infrastruktury sieciowej (routery i przełączniki zlokalizowane w sieci IT);
11) usługa poczty elektronicznej Microsoft 365;
12) usługi katalogowe;
13) usługi sieciowe (serwery DNS, serwery DHCP, serwery RADIUS).

3. System musi umożliwiać:

1) pozyskanie danych źródłowych za pomocą protokołu Windows Management Infrastructure (WMI);
2) pozyskanie wskazanych danych źródłowych z systemu źródłowego w postaci np. pliku płaskiego określonego ścieżką z wykorzystaniem dedykowanego rozwiązania agentowego;
3) pozyskanie danych źródłowych z nasłuchu sieci dla minimum protokołów DHCP, DNS, HTTP, IMAP, SIP, SMB, SMTP, MySQL;
4) przyjęcie danych z systemu źródłowego na wskazanym interfejsie sieciowym oraz porcie tego interfejsu sieciowego (TCP/UDP) min. z wykorzystaniem protokołu syslog oraz formatów takich jak Extended Log Format, Common Log Format, Common Event Format, Log Event Extended Format czy JSON.
5) System podczas normalizacji danych będzie klasyfikować zdarzenia w oparciu o kategorię zdarzeń (np. uwierzytelnienie użytkownika, anomalia w ruchu sieciowym, malware, itp.).
6) Silnik korelacji uwzględni występowanie identyfikatorów naruszeń bezpieczeństwa (IoC) dostarczanych przez bazy danych agregujące złośliwe identyfikatory.
7) Silnik korelacji umożliwi konfigurację zdarzeń reakcyjnych w postaci min. wysłania wiadomości e-mail.
8) System na podstawie korelacji zdarzeń dostarcza informację o incydentach bezpieczeństwa do operatorów systemu w postaci czytelnego zestawienia.
9) System umożliwi integrację z systemami obsługi zgłoszeń, tzw. systemy ticketowe, umożliwiające obsługę incydentów bezpieczeństwa oraz jej rozliczalność.
10) System ma możliwość tworzenia szczegółowego logu audytowego zawierającego informacje przynajmniej o logowaniu do systemu i zmianach w jego konfiguracji.

11) System umożliwi współprace z urządzeniami obsługującymi protokół netflow oraz tworzenie r aportów obrazujących ruch sieciowy, wraz z możliwością zdefiniowania własnych raportów m.in.:

a) Przedstawiających ruch sieciowy dla określonego interwału czasowego

b) Przedstawiający ruch sieciowy dla określonego hosta lub określonego portu urządzenia sieciowego lub określonego protokołu czy też portu TCP/IP. Możliwe ma być tworzenie złożonych zapytań operujących logicznymi korelatorami przedstawionych wyróżników (Adres IP , port protokół)

c) Przedstawiających komunikację zachodzącą dla par source i destination dla ruchu sieciowego, czyli generowania raportów określających precyzyjnie komunikację wymienianą między dwoma hostami , hostem a siecią IP , dwoma sieciami IP

d) Obrazujących komunikację dla innych parametrów , które mogą być wysyłane przez protokół Netflow takich jak przykładowo adres URL połączenia http, stan sesji TCP wynikający z przesyłanej flagi protokołu TCP .

12) Wykrywanie malware ransomware, komunikacji typu command and control przy współpracy z zastosowanymi w sieci systemami AV/EDR;

13) Wykrywanie komunikacji do serwerów klasyfikowanych jako źródła ataków phishingowych;

14) Wykrywanie skanowań wykonywanych w sieci wewnętrznej, skanowanie portów przy użyciu skanerów typu nmap , nessus, openvas;

15) Wykrywanie w sieci narzędzi i oprogramowania wykorzystywanego do ataków : Kali Linux, Metasploit;

16) Wykrywanie ataków na warstwę druga modelu OSI/ISO (typu arp spoofing, mac flooding, ataki na infrastrukturę DHCP, wykrywanie zmian topologii warstwy 2);

17) Wykrywanie ataków aplikacyjnych typu cross site scripting, web path traversal , sql injection;

18) Wykrywanie ataków na sieć WLAN typu denial of service: deauthentication, podstawienie rogue ap, pojawienie się nowych sieci w pobliżu (przy współpracy z istniejącą infrastrukturą WLAN);

19) Wykrywanie komunikacji o parametrach odmiennych od standardowych dla danej sieci : tj. ruchu o znaczącym wolumenie, sesji o długim czasie trwania, komunikacji z zasobami na podstawie geolokalizacji odmiennymi od standardowych;

20) Wykrywanie działań związanych z zagrożeniami haseł i kont, takich jak: utworzenie nowego administratora, podniesienie uprawnień, użycie konta administratora w godzinach nocnych, ataki typu brute force, konta blokujące się;

21) Wykrywanie ruchu do domen typu DGA oraz do domen o niskiej reputacji;

22) Monitorowanie spójności i zmian dokonywanych na zasobach takich jak pliki lub klucze rejestru;
23) Wykrywanie ataków typu denial of service i distributed denial of service;
24) Wykrywanie wycieków danych typu DLP (również użycie urządzeń USB na stacjach roboczych);
25) Wykrywanie instalacji nowych urządzeń na stacjach roboczych;
26) Wykrywanie użycia zdefiniowanych przez administratora protokołów komunikacyjnych;
27) Wykrywanie ruchu administracyjnego (SSH, telnet, RDP) lub ruchu typu VNC, teamviewer (również w zdefiniowanym przez administratora przedziale godzinowym);
28) Wykrywanie ruchu typu reverse shell.

VII. System Greenbone -– technologia równoważna do systemu Greenbone to system wykrywania, identyfikacji i oceny podatności oraz systemu zarządzania wiedzą o wykrytych lukach.

Skaner podatności musi wykrywać i identyfikować hosty i usługi w sieci a następnie wykonywać testy w celu wykrycia podatności i luk bezpieczeństwa wynikających z konfiguracji. Testy powinny dzielić się na zewnętrzne oparte na skanowaniu sieciowym lub wykonywane na hostach z wykorzystaniem uwierzytelnień.