Główny Urząd Statystyczny al. Niepodległości 208 00-925 Warszawa	**DIALOG TECHNICZNY** **Nr sprawy 1/ST/KSZBI/DT/2019**

ZAPROSZENIE DO UDZIAŁU W DIALOGU TECHNICZNYM

Wdrożenie systemu do zarządzania informacją i zdarzeniami bezpieczeństwa (SIEM), gromadzącego i korelującego informacje z systemów, aplikacji oraz urządzeń.

I. ZAPRASZAJĄCY

Główny Urząd Statystyczny
al. Niepodległości 208
00-925 Warszawa

II. PODSTAWA PRAWNA

Dialog techniczny prowadzony jest na podstawie art. 31a - 31d ustawy z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych (Dz. U. z 2018 r. poz. 1986 i 2215 oraz z 2019 r. poz. 53 i 730).

III. CEL I PRZEDMIOT DIALOGU TECHNICZNEGO

Celem dialogu technicznego jest doradztwo oraz uzyskanie informacji w zakresie niezbędnym do precyzyjnego przygotowania opisu przedmiotu zamówienia oraz specyfikacji istotnych warunków zamówienia, w tym uzyskanie przez Zapraszającego informacji umożliwiających wybranie najkorzystniejszego technicznie, organizacyjnie i efektywnego ekonomicznie rozwiązania.

Zapraszający będzie oczekiwał uzyskania informacji w szczególności w zakresie:
1) zakres informacji, które Zapraszający chce pozyskać w trakcie dialogu technicznego – **Załącznik nr 1,**
2) opis infrastruktury Zapraszającego – **Załącznik nr 2.**

IV. WARUNKI I ZASADY DIALOGU TECHNICZNEGO

1. Warunkiem udziału w dialogu technicznym jest złożenie wraz z wnioskiem o dopuszczenie do udziału w dialogu technicznym:
   1) dokumentu poświadczającego prowadzenie działalności gospodarczej w zakresie będącym przedmiotem dialogu technicznego (KRS, wpis do ewidencji działalności gospodarczej),
   2) Wykazanie (w formie oświadczenia) wykonania przez Wykonawcę w okresie ostatnich trzech lat co najmniej 1 usługi (umowy) polegającej na pełnym wdrożeniu min. 1 rozwiązania SIEM w organizacji liczącej minimum 2000 użytkowników.
2. Dialog techniczny prowadzony będzie drogą pisemną, elektroniczną oraz w formie indywidualnych spotkań w siedzibie Zapraszającego.
3. Dialog techniczny jest prowadzony w języku polskim.
4. Dialog jest jawny, z zastrzeżeniem że, Zapraszający nie ujawni informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2018 r. poz. 419), jeżeli Uczestnik dialogu technicznego, nie później niż w dniu przekazania informacji zastrzegł, że konkretnie wskazane informacje nie mogą być udostępniane innym podmiotom.
5. Za udział w dialogu technicznym Uczestnik nie otrzymuje wynagrodzenia ani zwrotu kosztów związanych z udziałem w dialogu.
6. Dialog techniczny jest prowadzony w sposób zapewniający przejrzystość, uczciwą konkurencję oraz równe traktowanie Uczestników dialogu technicznego.
7. Dialog techniczny będzie prowadzony do momentu, gdy Zapraszający, na podstawie uzyskanych od Uczestników dialogu technicznego informacji, uzna, że pozyskana wiedza jest wystarczająca do przygotowania dokumentacji postępowania o udzielenie zamówienia publicznego, z zastrzeżeniem pkt 8.

8. Zapraszający zastrzega sobie prawo do zakończenia dialogu technicznego na każdym jego etapie bez podania przyczyn.
9. W przypadku gdy informacje przekazywane Zapraszającemu przez Uczestników dialogu technicznego mają charakter utworu i Uczestnikowi przysługują do nich lub ich części autorskie prawa majątkowe, to powinny one być jednoznacznie wskazane w przekazywanych materiałach.
10. Zapraszający zastrzega sobie prawo do wykorzystania przekazanych przez uczestników dialogu technicznego informacji, opracowań i utworów w całości lub części, a także ich przetwarzania w celu opracowania dokumentacji przetargowej, w tym opisu przedmiotu zamówienia, specyfikacji istotnych warunków zamówienia i warunków umowy.
11. Przystąpienie do dialogu technicznego jest równoznaczne z udzieleniem zgody na wykorzystanie przez Zapraszającego przekazywanych informacji do przygotowania dokumentacji przetargowej, w tym opisu przedmiotu zamówienia, specyfikacji istotnych warunków zamówienia i warunków umowy. W przypadku przekazania Zapraszającemu w toku dialogu technicznego utworu w rozumieniu ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2017 r. poz. 880 i 1089 oraz z 2018 r. poz. 650) Uczestnik dialogu technicznego udziela Zapraszającemu bezwarunkowej zgody na wykorzystanie tego utworu (w całości bądź w części) na potrzeby przygotowania dokumentacji przetargowej, w tym opisu przedmiotu zamówienia, specyfikacji istotnych warunków zamówienia i warunków umowy oraz zezwolenia na wykonywanie praw zależnych do utworu, rozporządzanie i korzystanie z opracowań utworu. Uczestnik dialogu technicznego zapewnia, że wykorzystanie utworu przez Zapraszającego nie będzie naruszało praw osób trzecich.
12. Zapraszający powiadomi Uczestników dialogu technicznego o terminie i miejscu spotkania.
13. Zaproszenie do uczestnictwa w dialogu technicznym będzie wysłane w terminie nie krótszym niż trzy dni robocze przed datą wyznaczonego spotkania.
14. Powołana przez Zapraszającego w celu przeprowadzenia dialogu technicznego Komisja, zobowiązana jest do zapewnienia bieżącego prowadzenia protokołu z dialogu technicznego, a także do udostępnienia protokołu wszystkim zainteresowanym podmiotom, z zastrzeżeniem informacji stanowiących tajemnicę przedsiębiorstwa.

V. ZGŁOSZENIE DO UDZIAŁU W DIALOGU TECHNICZNYM

1. Podmioty zainteresowane udziałem w dialogu technicznym, spełniające wymagania określone w zaproszeniu do udziału w dialogi technicznym, proszone są o złożenie wypełnionego i podpisanego przez osobę uprawnioną do występowania w imieniu podmiotu „Wniosku o dopuszczenie do udziału w dialogu technicznym", którego wzór stanowi **Załącznik nr 3** do Regulaminu prowadzenia dialogu technicznego w Głównym Urzędzie Statystycznym.
2. Wnioski można składać:
   1) pisemnie (osobiście, pocztą lub za pośrednictwem kuriera) pod adresem: Główny Urząd Statystyczny, al. Niepodległości 208, 00-925 Warszawa, pok. nr 210;
   2) elektronicznie na adres e-mail: b.pluta2@stat.gov.pl lub d.lewkiewicz@stat.gov.pl
3. Wniosek o dopuszczenie do udziału w dialogu technicznym należy złożyć do dnia: 18.10.2019 r., godz. 10:00. Decyduje data wpływu wniosku do Zapraszającego.

VI. KONTAKT

Osoby wyznaczone do kontaktów:
1. Beata Pluta tel.: +48 22 608 36 64, e-mail: b.pluta2@stat.gov.pl
2. Dariusz Lewkiewicz tel.: +48 22 608 34 39; e-mail: d.lewkiewicz@stat.gov.pl

VII. ZAŁĄCZNIKI

Załącznik nr 1 - Zakres informacji, które Zapraszający chce pozyskać w trakcie dialogu technicznego;
Załącznik nr 2 - Opis infrastruktury Zapraszającego;
Załącznik nr 3 - Wniosek o dopuszczenie do udziału w dialogu technicznym.

DYREKTOR GENERALNY
Anna Borowska
8.10.2019 r.

Załącznik nr 1

Zakres informacji, które Zapraszający chce pozyskać w trakcie dialogu technicznego dotyczącego Dostawy i wdrożenia systemu do zarządzania informacją i zdarzeniami bezpieczeństwa (SIEM), gromadzącego i korelującego informacje z systemów, aplikacji oraz urządzeń.

Zapraszający chce w ramach dialogu technicznego pozyskać zakres informacji dotyczący:
1) opracowania koncepcji w układzie zawierającym informacje zgodne z założeniami w zakładanym terminie,
2) potwierdzenia zgodności proponowanego rozwiązania z obowiązującymi przepisami prawa,
3) wskazania dodatkowych zaleceń dla warunków technicznych, organizacyjnych i realizacyjnych związanych z realizacją projektu.

Koncepcja powinna być sporządzona z uwzględnieniem niniejszych założeń oraz założeń określonych w załącznikach. W przypadku wątpliwości co do słuszności założeń Wykonawca w ostatnim punkcie koncepcji przedstawi opis swoich założeń wraz z kosztorysem i uzasadnieniem. Niniejsza uwaga dotyczy również załączników do założeń.

Lista wymagań funkcjonalnych i niefunkcjonalnych dla systemu SIEM
Wymagania funkcjonalne, jak i nie funkcjonalne dla systemu SIEM należy rozpatrywać w trzech obszarach: usług, dostępności oraz jakości.
Do wymagań funkcjonalnych należy zaliczyć katalog usług systemu, które bezpośrednio wpływają na pracę SIEM. Należy tu uwzględnić parametry wydajnościowe, funkcje uzupełniające jak również parametry bezpieczeństwa.
Wyspecyfikowanie katalogu usług bez określenia warunków ich dostępności nie gwarantuje bez problemowego korzystania z możliwości systemu. Tym samym niezbędne staje się również sparametryzowanie wymagań nie-funkcjonalnych w zakresie dostępności serwisu i licencji.
Konfiguracja programowo-sprzętowa elementów systemu musi zapewniać pełną współpracę nowo dołączanych rozwiązań do systemu – w taki sposób, aby zagwarantować realizację wyspecyfikowanych w niniejszym dokumencie usług w oparciu o spójną sieć.

1. Usługi

1.1 Wymagania funkcjonalne

1.	Administrowanie systemem umożliwia przechodzenie od ogólnych danych do szczegółów	Widok poszczególnych pakietów otrzymanych przez system SIEM. SIEM posiada wbudowany edytor do tworzenia reguł korelacyjnych.
2.	Dostęp do informacji w czasie bieżącym	System SIEM umożliwia uzyskiwanie wyników z analizy danych bez zbędnych opóźnień. Możliwa jest nie tylko statystyczna analiza danych, ale także korelacja informacji zgodnie ze zdefiniowanymi regułami wyszukiwania incydentów.
3.	Dostęp do szczegółów zdarzenia w czasie rzeczywistym	System SIEM umożliwia zarówno dostęp do ogólnych statystyk, jak i wgląd w konkretne logi i zdarzenia.
4.	Zaawansowana korelacja danych.	Wyszukiwanie wzorców i odchyleń od linii bazowych w zgromadzonych zdarzeniach, aktywnościach sieciowych i bazach danych, a nawet w treściach przenoszonych przez rozmaite aplikacje działające w sieci. Funkcjonalność ta, zapewnia lepsze i szybsze wyszukiwanie śladów zagrożeń, ataków, utraty danych oraz oszustw związanych z chronionymi zasobami organizacji.
5.	Analiza przepływów sieciowych	
6.	Analiza ruchu aplikacyjnego	Uwzględnienie danych aplikacyjnych w korelacji zdarzeń.
7.	Min. 300 predefiniowanych źródeł danych i gotowe do wykorzystania reguły korelacyjne oraz szablony raportów	Dla źródeł, które nie posiadają gotowych parserów, możliwe jest tworzenie reguł obsługujących zdarzenia.

8.	Skalowalność	Możliwość obsługi milionów zdarzeń na sekundę z rozproszonych źródeł, bez utraty przetwarzanych informacji
9.	Dokładność raportowania	Szczegółowe raportowanie w oparciu o dane pochodzące z dowolnych źródeł informacji: logów, zdarzeń generowanych przez systemy operacyjne i aplikacje, agentów działających na serwerach i stacjach, przepływów sieciowych (flows), baz danych, systemów identyfikacji użytkowników, itd.
10.	Zapewnienie niezmienności i nienaruszalności zbieranych zdarzeń.	System umożliwia zapisywanie i zarządzanie oryginalnymi zdarzeniami przekazywanymi ze źródeł, zapewnia ich kontekstowe przeszukiwanie oraz kompresję.
11.	Zarządzanie oryginalnymi logami.	
12.	Długoterminowa dostępność danych	System SIEM umożliwia wgląd zarówno w napływające dane, jak i zgromadzone wcześniej informacje historyczne.
13.	Kontekst zdarzeń	System SIEM analizuje zgromadzone dane również w odniesieniu do kontekstu w jakim powstały. Jest to możliwe, poprzez wzbogacanie gromadzonych zdarzeń o informacje dotyczące podatności, danych użytkowników, lokalizacji, reputacji, poziomu ryzyka, itd.
14.	Elastyczne raportowanie	System generuje raporty w oparciu o wbudowane szablony i definicje, a także na podstawie kryteriów samodzielnie określonych przez administratorów SIEM.
15.	Predefiniowane alarmy, raporty, dashboard'y	
16.	Możliwość integracji SIEM z innymi rozwiązaniami bezpieczeństwa.	
17.	Powiązanie korelacji z systemem reputacji GTI	Funkcjonalność umożliwiająca uwzględnienie w korelacji kontekstu, wynikającego z oceny ryzyka źródła lub odbiorcy połączenia. Baza GTI gromadzi i przetwarza dane pozyskane zarówno z pasywnych systemów typu honey pot, jak i z informacji o wykrytych atakach przekazywanych przez setki tysięcy źródeł rozsianych po całym świecie. Są one niezwykle cennym uzupełnieniem analizy zdarzeń przeprowadzanej przez system SIEM.

1.2 Wymagania niefunkcjonalne

a) Proponowane rozwiązanie powinno być zbudowane w oparciu, o co najmniej:
   - Centralny Moduł Zarządzający, zwany dalej CMZ – zapewniający centralne zarządzanie rozwiązaniem SIEM, zarządzanie konfiguracją systemu, konfiguracją źródeł zdarzeń, użytkowników i ich uprawnień, zbieranie danych z kolektorów zdarzeń, tworzenie i wdrażanie mechanizmów korelacyjnych, tworzenie i dostosowywanie widoków (tzw. dashboard) i raportów oraz udostępniać graficzną konsolę webową, pozwalającą na centralne zarządzanie oraz pracę z systemem SIEM;
   - Kolektor Zdarzeń, zwany dalej KZ - umożliwiający zbieranie i przechowywanie przetworzonych zdarzeń oraz przepływów sieciowych pozyskanych z podłączonych do systemu SIEM źródeł oraz ich analizę na podstawie wbudowanych lub skonfigurowanych przez użytkownika systemu reguł;
   - Centralny Moduł Zarządzania Logami, zwany dalej CMZL - zapewniający zbieranie zdarzeń w postaci surowej (przez surowe logi Zamawiający rozumie logi w oryginalnej postaci, zapisane w płaskim pliku tekstowym, opatrzonym podpisem cyfrowym w celu zapewnienia ich niezaprzeczalności) i zarządzany z poziomu CMZ;

b) Oferowane rozwiązanie powinno posiadać pojedynczy, webowy interfejs użytkownika obsługiwany przez standardowe przeglądarki, w tym:
   - Microsoft Internet Explorer i Edge;
   - Mozilla Firefox;

- Google Chrome.

Interfejs ten powinien być dostępy przez CMZ.

c) Silnik bazodanowy powinien być specjalistycznym silnikiem stworzonym celowo do zastosowania w danym systemie SIEM. Nie dopuszcza się możliwości, zastosowania w zamawianym systemie baz ogólnego przeznaczenia.
d) Silnik bazodanowy nie może narzucać na system SIEM innych ograniczeń pod względem ilości przechowywanych zdarzeń niż objętość dołączonych do systemu przestrzeni dyskowych.
e) Oferowane rozwiązanie powinno zapewniać możliwość dołączenia w celu długoterminowego przechowywania zbieranych informacji zewnętrznych pamięci masowych typu DAS, NAS (NFS, CIFS) i SAN (iSCSI, FC). Zapisywanie danych na zewnętrznych pamięciach powinno być automatyczne. Zapisane dane na zewnętrznych pamięciach masowych powinny być możliwe do przeglądania online za pomocą konsoli webowej CMZ.
f) Niedopuszczalne jest zastosowanie zautomatyzowanych rozwiązań do przechowywania danych w chmurach publicznych.
g) Oferowane rozwiązanie powinno zapewniać przetwarzanie w trybie ciągłym 40 000 zdarzeń (EPS) na sekundę. Urządzenie musi posiadać fizyczną możliwość zwiększenia ilości przetwarzanych zdarzeń do poziomu (x3) EPS bez konieczności instalacji dodatkowych urządzeń zewnętrznych.
h) Oferowane rozwiązanie powinno zbierać dane przy użyciu co najmniej następujących metod:
   - zbieranie logów pasywnych (SYSLOG);
   - zbieranie logów z uwierzytelnianiem (CIFS, SCP);
   - CEF;
   - OPSEC;
   - SDEE;
   - XML;
   - ODBC.
i) Oferowane rozwiązanie powinno mieć możliwość zbierania informacji o przepływach sieciowych co najmniej w formacie:
   - Netflow;
   - Jflow;
   - IPFIX.
j) Oferowane rozwiązanie powinno zapewniać możliwość zbierania logów audytowych z aplikacji bazodanowych dla co najmniej:
   - IBM DB2;
   - Microsoft SQL.
k) Oferowane rozwiązanie powinno umożliwiać wzbogacanie kontekstu zdarzenia o dane referencyjne niezawarte w samym zdarzeniu (np. uprawnienia użytkownika w domenie), pochodzące ze wskazanych źródeł (baz) danych. Wśród źródeł wzbogacania kontekstu, muszą być co najmniej dostępne:
   - RESTful API;
   - LDAP;
   - MSSQL;
   - pliki dostępne przez FTP, CIFS czy SCP.
l) Oferowane rozwiązanie powinno umożliwiać w przyszłości (w następnym etapie wdrożenia) możliwość rozbudowy systemu SIEM o dostarczenie funkcjonalności pracy w trybie analizowania danych historycznych - zapewniający możliwość wykrycia wstecznie, czy nowoodkryte zagrożenie nie występowało lub nie zostało wykorzystane w przeszłości.
m) Oferowane rozwiązanie powinno umożliwiać integrację z systemem Microsoft Active Directory (AD) i mapowanie grup użytkowników wraz z ich uprawnieniami.
n) Obsługa IPv6.

1.3. Wymagania dodatkowe

a) sposoby i rodzaje licencjonowania;
b) wymagania techniczne dot. lokalizacji;
c) przewidywany czas wdrożenia.

2. Dostępność

2.1 Pojemność

Pojemność systemu wiąże się ze zdolnością do obsłużenia z określonym poziomem jakości usług określonej ilości zdarzeń.

2.2 Zasilanie
System musi być zaprojektowany i wykonany z uwzględnieniem zasad bezpieczeństwa użytkowania, ograniczenia zakłóceń i szkodliwego promieniowania elektromagnetycznego oraz ochrony środowiska.

2.3 Nieuszkadzalność
Wymaga się, aby dostarczony system wspierał pracę w układzie zdublowanym elementów systemu mających bezpośredni wpływ na realizację usług. Dostawca musi dostarczyć listę powyższych elementów.

2.4 Obsługiwalność
Wymaga się, aby dostarczony system umożliwiał zdalną konfigurację.

2.5 Skalowalność

2.6 Dołączalność

3. **Jakość usług**
Badania funkcjonalne i jakości usług.

4. **Retencja danych**
Okres przechowywania danych dotyczących aktywności oraz ruchu w sieci GUS – min. 36 miesięcy.

5. **Zakres informacyjny do ujęcia w koncepcji:**

1) Zagadnienia organizacyjne:

- założenia projektowe – należy zamieścić przyjęte założenia projektowe oraz zalety i ograniczenia przyjętego rozwiązania; ponadto można wskazać producentów sprzętu, nazwy wersje przyjętych rozwiązań; punkt powinien też zawierać odniesienia do niezbędnego potencjału technicznego i zasobów ludzkich do budowy systemu.
- proponowany harmonogram realizacji projektu – należy zaproponować harmonogram realizacji projektu, uwzględniający okres począwszy od podpisania umowy do oddania systemu do eksploatacji (jednostką czasu jest tydzień); harmonogram powinien uwzględniać podstawowe etapy realizacji projektu, w tym: opracowanie dokumentacji projektowej, szkolenia i testy akceptacyjne, okres przejściowy oraz opracowanie dokumentacji powykonawczej; ponadto w tym zakresie należy się odnieść do możliwości etapowej budowy (lata budżetowe, inne projekty, podział na ośrodki).
- Szacunkowy koszt realizacji projektu – informacje zawarte w tym punkcie mają dać Zamawiającemu możliwość oszacowania potrzeb finansowych dla realizacji projektu; szacowanie powinno zawierać także zasady i koszty licencjonowania, w tym dla rozbudowy systemu w zakresie infrastruktury, integracji i usług; ponadto punkt powinien zawierać propozycje w zakresie etapowego rozliczenia projektu, kosztach wprowadzenia modyfikacji systemu pod względem organizacji projektu; ceny powinny być cenami brutto w złotych polskich.
- Zakres dla wstępnej dokumentacji projektowej – należy wskazać jaki zakres informacji w zakresie organizacyjnym i technicznym Zamawiający mógłby opracować przed podpisaniem umowy oraz przed sporządzeniem OPZ.
- Szkolenia – należy przedstawić proponowany zakres szkoleń a także przewidywany czas przeprowadzenia i koszty oraz formułę realizacji szkoleń.
- Wdrożenie systemu z uwzględnieniem ciągłości działania GUS – należy zamieścić opis w zakresie proponowanego modelu wdrożenia systemu, w tym: etapy realizacji, sposobu realizacji testów i odbioru.
- Serwis – materiał musi zawierać opis głównych możliwości i ogólne zasady funkcjonowania serwisu gwarancyjnego i pogwarancyjnego oraz uwarunkowania dla linii wsparcia, a także możliwe do zdefiniowania koszty serwisu.

2) Zagadnienia techniczne

- Architektura systemu – należy zamieścić opis architektury systemu wraz ze schematami (opis fizyczny i logiczny), proponowaną topologię połączeń poszczególnych elementów infrastruktury,
- Niezawodność systemu – należy odnieść się do niezawodności pracy systemu; w szczególności należy przedstawić przyjęte w rozwiązaniu sposoby zapewnienia jego niezawodności.
- Lokalizacja i zarządzanie systemem – należy zamieścić co najmniej:
  - Ogólne wymagania dla pomieszczeń do instalacji elementów infrastruktury centralnej proponowanego systemu (wymagana powierzchnia, zasilanie, system klimatyzacji, sieć),
  - Gabaryty, masa głównych elementów proponowanego systemu,
  - Narzędzia do zarządzania i monitorowania poszczególnych modułów systemu

- Możliwości raportowania systemu i ruchu, w tym raporty dostępne w systemie oraz możliwości w zakresie ich definiowania,
- Zalecenia w zakresie kadry administracyjnej,

- Funkcjonalność użytkowa systemu – należy wymienić, wraz z krótkim opisem, listę funkcjonalności Systemu możliwych do osiągnięcia.
- Rejestracja czynności Administratorów, logi z dostępu do oprogramowania i dzienniki zdarzeń,
- Sieć teleinformatyczna – należy wskazać co najmniej:
  - ✓ Wymagania dotyczące sieci dla łączenia elementów infrastruktury systemu;
  - ✓ Protokoły komunikacyjne, warstwy sieciowe i adresacja;
  - ✓ Możliwość odseparowania sieci zarządzania systemem od sieci usługowej;
  - ✓ Zmienność parametrów łącz wraz ze wzrostem ilości i możliwości funkcjonalnych elementów systemu;
  - ✓ Możliwość podłączenia nowych elementów spoza infrastruktury sieciowej Zapraszającego.

3) **Integracja z istniejącymi i planowanymi rozwiązaniami**
Integracja z istniejącymi i planowanymi rozwiązaniami IT w GUS.

4) **Inne istotne informacje**
Należy zawrzeć inne istotne informacje, których obszar nie wpisuje się w zakresy tematyczne zdefiniowane niniejszym dokumentem oraz w tym odniesieniu do treści Załącznika nr 1. Załącznikami do koncepcji mogą być min:
a) Dokumentacja produktowa (preferowana w jęz. polskim),
b) Dokumentacja filmowa lub/i prezentacje (w jęz. polskim),
c) Materiały uzupełniające (preferowane w jęz. polskim).

Załącznik nr 2

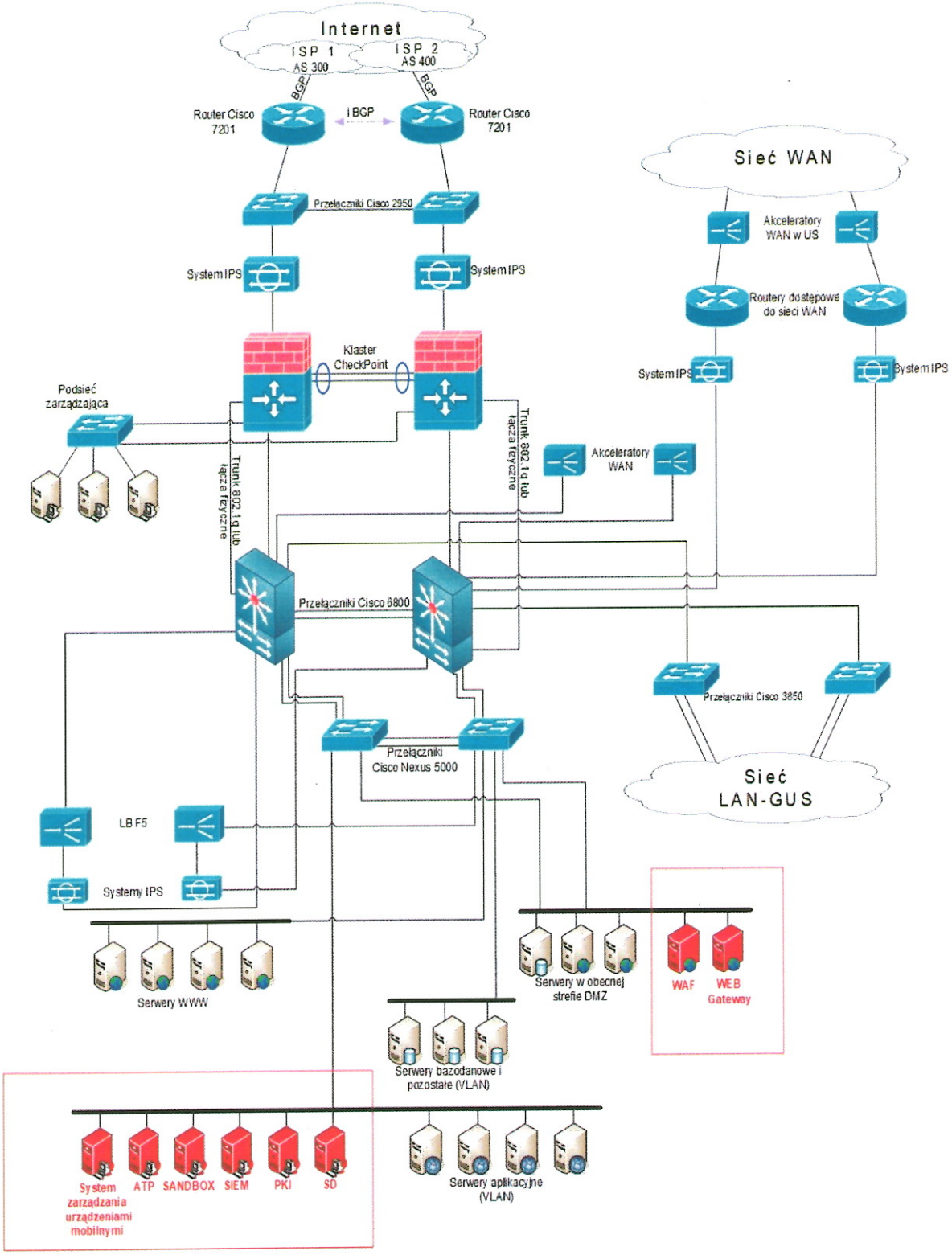
Opis infrastruktury Zapraszającego

I. Opis środowiska

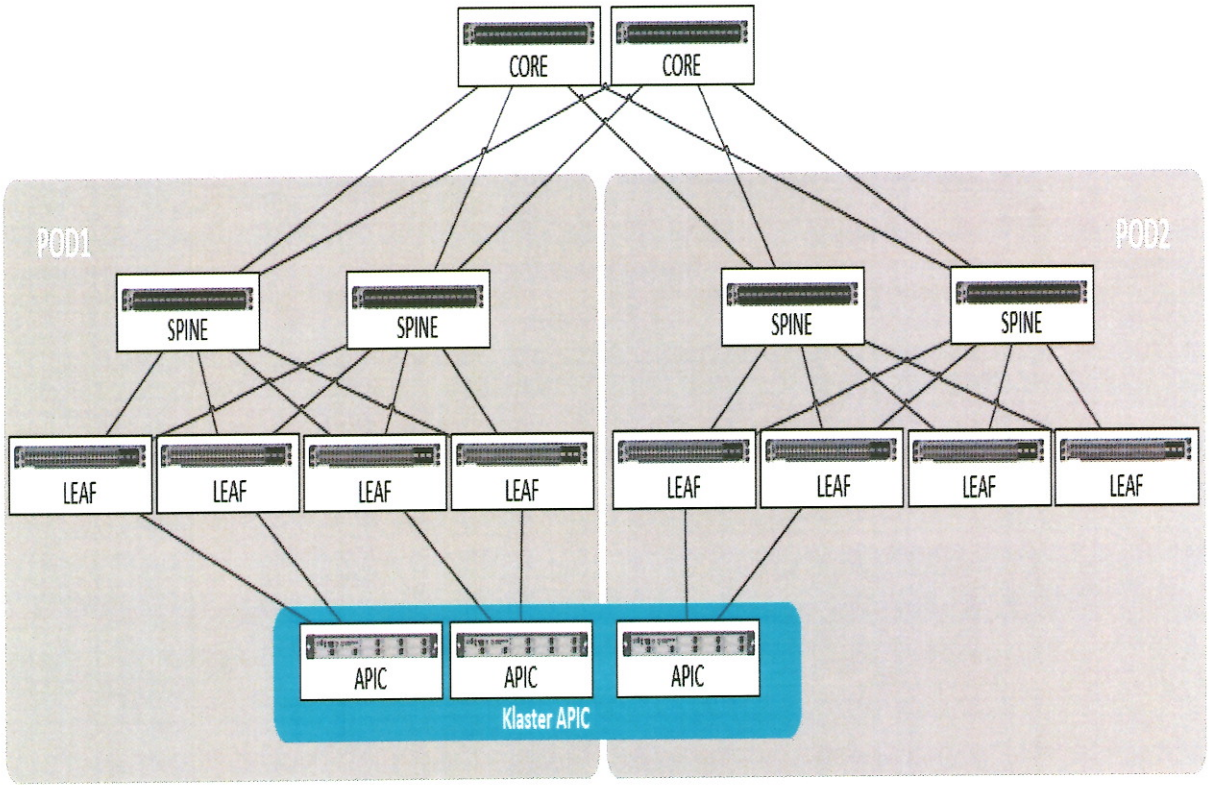
Sieć teleinformatyczna w siedzibie Głównego Urzędu Statystycznego zbudowania jest z przełączników warstwy 3 oraz warstwy 2 i podzielona jest na następujące segmenty:

1. Dostępu do Internetu.
   Strefa ta składa się z dwóch łączy do niezależnych operatorów oraz dwóch routerów, dwóch przełączników warstwy drugiej.
2. Sieci WAN.
   W skład tej strefy wchodzą dwa łącza do sieci WAN, dwa routery oraz dwa akceleratory.
3. Sieci LAN GUS.
   Do strefy należą wszystkie zasoby znajdujące się w sieci LAN GUS: 70 przełączników dostępowych, 7 przełączników agregacyjnych z wbudowanymi kontrolerami sieci bezprzewodowej, punkty dostępowe oraz komputery, laptopy, drukarki, urządzenia wielofunkcyjne.
4. Data Center obecnie – 09/2019.
   W skład strefy wchodzi sześć stref DMZ, serwery aplikacyjne, serwery bazodanowe, serwery BackOffice oraz urządzenia balansujące ruch. Logicznie strefa ta jest podzielona na kilkadziesiąt podsieci, a komunikacja ze strefami DMZ jest kontrolowana przez zaporę ogniową. Przełącznikami szkieletowymi są dwa urządzenia Cisco Catalyst 6807. Przełącznikami agregującymi są urządzenia Cisco Catalyst 6504, Cisco Nexus 5148 oraz Nexus 5548, warstwę dostępową dla serwerów stanowią moduły rozszerzającej FEX oraz przełączniki Cisco Catalyst 2960G.
   Schemat sieci w GUS.

Architektura fizyczna IT w GUS



Nowa architektura sieciowa Data Center – 12/2019.
Zapraszający planuje wdrożenie nowej architektury Cisco ACI (Application Centric Infrastructure), która będzie służyła do tworzenia architektury sieci programowalnych. W ramach realizowanej umowy zainstalowane będą urządzenia Cisco Nexus 9336C-FX2, Cisco Nexus 9332C, Cisco Nexus 3108TC-FX, Cisco Nexus 93180YC-FX, Cisco Catalyst 9300 48-port, Cisco Catalyst 9300 24-port, APIC-SERVER-L3. Poniżej schemat planowanej architektury.



II. Parametry infrastruktury GUS

1	Liczba fizycznych lokalizacji organizacji	68 szt.
2	Technologie połączeń lokalizacji	MPLS
3	Zarządzanie WAN	Cisco Prime
4	Gromadzenie informacji z sieci WAN	NetFlow
5	Liczba użytkowników sieci	6000 szt.
6	Liczba stacji roboczych	8000 szt.
7	Środowisko domenowe liczba instacji Active Directory	1
8	Liczba i rodzaj urządzeń sieciowych znajdujących się w sieci	430
9	Rodzaj i liczba DataCenter (własne/wynajmowane):	2
10	Liczba serwerów fizycznych we własnej infrastrukturze	600 szt.
11	Liczba serwerów wirtualnych we własnej infrastrukturze	600 szt.
12	Rodzaj i wersja hypervisora	*VmWare v5.5 Hyper-V v*
13	Liczba krytycznych aplikacji dla działania organizacji	30

14	Liczba styków z siecią Internet dla całej organizacji	2
15	Strefy DMZ	tak
16	Liczba użytkowników uprzywilejowanych (administratorów IT)	60
17	Zdalne połączenia do sieci dla zewnętrznych administratorów	tak
20	Mechanizmy ograniczenia dostępu do zasobów użytkownikom uprzywilejowanym	tak
21	Ochrona serwerów i maszyn wirtualnych: rodzaj,producent i wersja	*Symantec*
22	Ochrona punktów styku (rodzaj i model urządzeń)	
23	Firewall/ NGFV	CheckPoint
25	Web Gateway	Netscaler
26	E-mail Gateway	Netscaler
27	NAC	brak
28	SSL encryptor	CheckPoint
29	Remote Access VPN	Netscaler
30	Network Access Control	brak
31	Web Application Controll	brak
32	Proxy	Netscaler
33	Sandbox	brak
34	Monitorowanie urządzeń końcowych/ ruchu sieciowego w celu zapobiegania wyciekowi istotnych danych	brak
35	Cykliczne skanowanie sieci automatycznymi skanerami podatności	tak
36	Systemy pozwalające na identyfikację prób wycieku istotnych danych (DLP)	brak
37	Rodzaj i typ systemu poczty elektronicznej	Exchange
38	Usługi chmurowe	brak
39	Forma wymiany plików pomiędzy użytkownikami	mail. SharePoint, FTP

Załącznik 3

Główny Urząd Statystyczny 00-925 Warszawa al. Niepodległości 208	**WNIOSEK O DOPUSZCZENIE DO UDZIAŁU W DIALOGU TECHNICZNYM** **Nr sprawy: 1/ST/KSZBI/DT/2019**

NAZWA DIALOGU TECHNICZNEGO

Wdrożenie systemu do zarządzania informacją i zdarzeniami bezpieczeństwa (SIEM), gromadzącego i korelującego informacje z systemów, aplikacji oraz urządzeń.

WNIOSKODAWCA:
Niniejszy wniosek zostaje złożony przez:

L.p.	Nazwa Wnioskodawcy	Adres

KONTAKT Wnioskodawcy (pełnomocnik):

Nazwa i adres	
Nr telefonu	
Nr faksu	
Adres e-mail	
Imię i nazwisko osoby uprawnionej do kontaktów	

Będąc uprawnionym do reprezentowania Wnioskodawcy:

1) składam wniosek o dopuszczenie do udziału w dialogu technicznym mającym na celu uzyskanie informacji technicznych w zakresie:
   .....
   .....
2) udzielam zgody na wykorzystanie wszelkich przekazanych informacji oraz utworów stanowiących przedmiot praw autorskich na potrzeby przygotowania i realizacji postępowania o udzielenie ww. zamówienia, zezwalam na rozporządzanie i korzystanie z opracowań tych utworów, jak również zapewniam, że wykorzystanie utworu przez Zapraszającego nie będzie naruszało praw osób trzecich,
3) bez zastrzeżeń przyjmuję przedstawione w ogłoszeniu warunki prowadzenia dialogu technicznego,
4) oświadczam, że Wnioskodawca spełnia warunki udziału w dialogu technicznym, tj.:
   .....
   .....

Załączniki:

1. .....
2. .....

.....
(data i podpis osoby uprawnionej do reprezentowania Wnioskodawcy)