Załącznik nr 3
Producent: .....
Model: .....

1	2	3
Lp.	**Opis wymagań minimalnych**	**Parametry oferowane (należy podać opis sposobu spełnienia wymagań opisanych w kolumnie 2.)**
1	Rozwiązanie na platformie sprzętowej z możliwością montażu w szafie RACK 19".	
2	Platforma sprzętowa musi posiadać co najmniej 4 interfejsy Gigabit w pełni konfigurowalne. System musi pozwalać na konfigurację pracy urządzenia w co najmniej 40 sieciach VLAN.	
3	System musi obsługiwać sieci z minimum 500 hostów.	
4	Urządzenie musi zapewniać możliwość skanowania urządzeń w infrastrukturze sieciowej.	
5	Produkt musi być autoryzowanym produktem korzystającym z bazy CVE (zarówno bazy głównej jak i bazy kandydatów) oraz bazy NVD (National Vulnerability Database).	
6	Możliwość wykrywania luk bezpieczeństwa w dowolnych systemach sieciowych bez instalowania dodatkowych aplikacji na tych systemach.	
7	Możliwość tworzenia polityk bezpieczeństwa sieci w oparciu o wbudowany system polityk bezpieczeństwa sieciowego.	
8	Możliwość weryfikacji bezpieczeństwa sieci w oparciu o normy bezpieczeństwa minimum: ISO27001/ISO17799.	
9	Rozwiązanie musi posiadać wbudowany system zarządzania zagrożeniami, przydzielania zleceń naprawy systemów wybranym pracownikom z możliwością nadzorowania postępu prac.	
10	Urządzenie musi oferować szczegółowe raporty zawierające opisy wykrytych luk bezpieczeństwa wraz z informacją o możliwości ich wyeliminowania z danego systemu.	
11	System musi posiadać wbudowany system raportowania z możliwością tworzenia podsumowań dla wskazanych systemów. System raportowania musi umożliwiać tworzenie raportów dla administratorów a także ogólnych raportów podsumowujących poziom bezpieczeństwa. Raporty muszą być dostępne minimum w formatach PDF oraz xml.	
12	System musi posiadać mechanizm wykrywania aktywnego malware oraz aktywacji linków phishingowych przez użytkowników sieci. Na bazie zintegrowanych mechanizmów system musi blokować	

	hosty zainfekowane malware lub aktywujące linki phishingowe.	
13	System musi umożliwiać wykrywanie i automatyczne blokowanie nieautoryzowanego dostępu do infrastruktury sieciowej w oparciu o zintegrowany, bezagentowy system Network Access Control.	
14	System musi umożliwiać wykrywanie i klasyfikowanie wszystkich urządzeń pracujących w infrastrukturze.	
15	Rozwiązanie musi posiadać system wykrywania zmian w obrębie infrastruktury sieciowej i powiadamiania administratorów o każdej zanotowanej zmianie.	
16	System musi posiadać mechanizm automatycznego skanowania pod kątem występowania podatności i luk bezpieczeństwa zaufanych systemów podłączających się do infrastruktury sieciowej.	
17	System musi wykrywać wszelkie anomalie sieciowe związane z MAC spoofing.	
18	Możliwość integracji z przełącznikami posiadanymi przez Zamawiającego (HP, Aruba, Cisco)	
19	System musi umożliwiać automatyczne przełączanie hostów niezaufanych do nowopowstałego VLANu (tzw. Blackhole) lub do wskazanego przez administratora VLAN o niskim priorytecie dostępu.	
20	Możliwość wykrywania i powiadamiania o pojawieniu się w sieci hostów z danej puli adresów IP.	
21	Możliwość monitorowania aktywności hostów i powiadamianie w przypadku braku łączności z monitorowanymi systemami/urządzeniami.	
22	Zarządzanie przez interfejs webowy, bez konieczności używania maszyny Javy ani dodatkowego oprogramowania instalowanego na maszynie zarządzającej.	
23	Praca urządzenia powinna być możliwa w sieciach z adresacją statyczną oraz w środowisku DHCP.	
24	Urządzenie powinno umożliwiać określenie wykrytych luk bezpieczeństwa jako tzw. false positive dodatkowo powinna być możliwość generowania raportów podsumowujących a także zbiorczych raportów dla osób zarządzających.	
25	Awaria systemu nie może powodować przestojów w dostępie hostów do sieci wewnętrznej.	
26	Minimum 36 miesięczna subskrypcja aktualizacji baz zagrożeń oraz firmware i 36 miesięczna gwarancja na urządzenie i wsparcie techniczne producenta rozwiązania. W ramach gwarancji i wsparcia serwisowego Zamawiający wymaga: - możliwości zgłaszania problemów w dni robocze w godzinach 8:00 – 16:00, - czas reakcji na zgłoszenie nie dłuższy niż 4 godziny, - dostęp do najnowszych wersji oprogramowania, patchy,	

	hotfix, - wysyłka sprawnej części lub całego urządzenia nie później niż w następnym dniu roboczym od potwierdzenia usterki.	

.....
data i miejscowość

.....
podpis i pieczęć osoby upoważnionej
do reprezentacji Wykonawcy