RI.3037.53.2024

Załącznik Nr 6 do Zapytania ofertowego

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest
„Zakup systemu monitorowania i wykrywania zdarzeń w ramach projektu grantowego pn.: „Cyberbezpieczny Samorząd” zgodne poniższą specyfikacją. Rozwiązanie musi spełniać poniższe wymagania lub równoważne.

System klasy XDR (Extended Detection and Response)	
1. Gromadzenie danych	Obsługuje gromadzenie danych o ruchu i danych dziennika z sensorów, terminali, urządzeń zabezpieczających (takich jak NGFW, IDPS, WAF itp.) i urządzeń sieciowych innych firm.
	Obsługuje dane w formatach Syslog, sysmon, netflow, metadanych i linux.
2. Wydajność platformy	Obsługuje do 5 urządzeń w celu utworzenia klastra HA, w celu elastycznej rozbudowy przestrzeni dyskowej i wydajności przetwarzania danych.
	Dostęp do platformy możliwy poprzez adres typu IPv6 oraz IPv4.
	Podczas wdrażania platformy obsługiwane jest używanie adresów IPv6 do konfigurowania powiązanych instancji platformy.
3. Wyświetlanie pełnoekranowe	Obsługa mapy rozkładu ataków, kompleksowych wyników, sytuacji podatności, sytuacji serwerów, sytuacji terminali, najnowszych zagrożeń.
	Możliwość przeglądania statystyk i wyświetlania podziału ataków zewnętrznych na poziomie zdarzeń, 5 najpopularniejszych źródłowych adresów IP ataków, 5 najpopularniejszych lokalizacji geograficznych źródeł ataków, rozkład etapów ataku, sytuację zdarzeń ataku oraz 5 najpopularniejszych zasobów/obszarów objętych atakiem.
	Moduł wyświetlania pełnoekranowego, który obsługuje serwer, rozkład stanu bezpieczeństwa, TOP5 ryzykownych serwerów, TOP5 zagrożeń, tygodniowy trend ryzyka i ranking zagrożeń.
	Moduł wyświetlania pełnoekranowego, który obsługuje terminale, dystrybucję statusu bezpieczeństwa, TOP5 ryzykownych serwerów, TOP5 zagrożeń, tygodniowy trend ryzyka i ranking zagrożeń.

	Moduł wyświetlania pełnoekranowego obsługujący zdarzenia, statystyki zagrożeń, najnowsze zagrożenia, najnowsze informacje o zagrożeniach, tygodniowy trend ryzyka i historyczny ranking zagrożeń.
	Moduł wyświetlania pełnoekranowego, który obsługuje podatności hostów, dystrybucję podatności na zagrożenia, trend podatności i ranking historycznych podatności.
	Obsługa obszarów ryzyka i wyświetlanie serwerów, punktów końcowych, zagrożeń i luk w zabezpieczeniach w ramach każdego obszaru ryzyka.
	Obsługa przeskakiwania z pełnoekranowego wyświetlacza kompleksowej sytuacji bezpieczeństwa do innych wyświetlaczy pełnoekranowych; manualna lub automatyczna.
	Obsługa kontroli filtrów czasowych, wybór wyświetlania informacji z dnia dzisiejszego, 7 dni i 30 dni
4. Monitorowanie sytuacji infrastruktury	Obsługuje powiadamianie o alarmach oraz o zagrożeniach, informacjach alarmowych o działaniu systemu i informacjach alarmowych o licencjach w systemie.
	Obsługuje przegląd sytuacji bezpieczeństwa, w tym kompleksowy status ryzyka całej sieci, porównanie statusu ryzyka w tym samym okresie tygodnia, liczbę zadań i status wykonania zadania, zagrożenia i ich rozkład w tygodniu, status ryzyka i status naruszonych zasobów.
	Obsługuje statystyki i wyświetlanie całkowitej liczby ryzykownych terminali, całkowitej liczby ryzykownych serwerów, całkowitej liczby zadań, ukończonych zadań i niedokończonych zadań
	Obsługa niestandardowych ustawień w celu wyświetlania zagrożeń, którymi zainteresowany jest użytkownik, oraz wsparcie dla drill-down odpowiednich zdarzeń w celu przejścia do strony szczegółowej.
	Obsługa ogólnej oceny stanu zagrożenia całej sieci i porównywanie stanu zagrożenia z jednego tygodnia w tym samym okresie czasu.
	Obsługa statystyk i wyświetlanie 5 najważniejszych zdarzeń związanych z zagrożeniami w danym tygodniu Obsługa statystyk zagrożeń i wyświetlania rozkładu na mapie

	Obsługuje funkcję monitorowania ruchu i wykonuje statystyki, analizę i wyświetlanie informacji o danych NetFlow uzyskanych przez platformę z trendów ruchu, trendów nowych połączeń, aktywności źródłowych adresów IP i docelowych adresów IP.
	Obsługa monitorowania całkowitego trendu ruchu i monitorowania ruchu źródłowego adresu IP / docelowego adresu IP, obsługa wyświetlania adresu IP, typu zasobu, nazwy zasobu, obszaru, ruchu uplink i downlink, nowego połączenia i innych informacji oraz obsługa rankingu TOP.
	Obsługa zliczania liczby serwerów/terminali o różnych poziomach ryzyka zgodnie z poziomem ryzyka: krytycznym, wysokim, średnim i niskim oraz tygodniowy wykres trendu oraz TOP5
	Obsługa statystyk trendów liczby serwerów/terminali o różnych poziomach ryzyka w ciągu tygodnia.
	Obsługa wyświetlania statystyk TOP5 serwerów/terminali o najbardziej krytycznym ryzyku w ciągu tygodnia.
	Obsługa rankingu TOP5 zagrożeń związanych z zasobami i obsługa statystyk ryzyka związanych z zasobami w ciągu tygodnia
	Obsługa pulpitu monitorowania zasobów, zliczanie wszystkich zasobów/ serwerów/terminali o różnych poziomach ryzyka, oraz wyświetlanie 5 najbardziej ryzykownych zasobów/serwerów/terminali.
	Obsługa wyświetlania typu zasobu związanego z pojedynczym adresem IP, nazwy zasobu, zlokalizowanego regionu, liczby nowych połączeń, całkowitego ruchu, rozkładu ruchu i powiązanych z nim działań
	Obsługa statystyk i wyświetlanie całkowitej liczby zasobów, całkowitej liczby serwerów/terminali/sprzętu sieciowego/sprzętu bezpieczeństwa/innego sprzętu, liczby zasobów w stanie naruszenia
	Obsługa statystyk i wyświetlanie rozkładu typu zasobu, rozkładu źródła i systemu operacyjnego, rankingu TOP5 otwartych portów, rankingu TOP5 aplikacji oraz rankingu TOP5 dystrybucji zasobów.
	Obsługa statystyk zagrożeń, tygodniowych statystyk zagrożeń
	Obsługa konfigurowania danych zdarzeń, statystyk i wyświetlania rozkładu danych zagrożeń oraz informacji o zasobach dotkniętych

	danymi zagrożeniami
	Obsługa statystyk luk w zabezpieczeniach, tygodniowego trendu luk w zabezpieczeniach i tygodniowej liczby luk w zabezpieczeniach
	Obsługa statystyk obszaru ryzyka, tygodniowego trendu obszaru ryzyka i tygodniowej liczby statystyk obszaru ryzyka
	Obsługa śledzenia źródła globalnie, obsługa śledzenia źródła poprzez IP/nazwę domeny/MD5 i musi obejmować informacje o zdarzeniach zagrożeń, analizie podatności, monitorowaniu ruchu, powiązanych danych wywiadowczych i innych powiązanych informacjach.
	Obsługuje monitorowanie w czasie rzeczywistym użycia procesora, pamięci i dysku twardego
	Obsługa statystyk stanu czujników, w tym całkowitej liczby czujników, liczby niedziałających czujników i liczby działających czujników,
	Obsługa niestandardowej planszy tematycznej, wielowymiarowe wyświetlanie wykresów zasobów, zagrożeń i luk w zabezpieczeniach
5. Analiza zagrożeń	Obsługa statystyk statusu wszystkich zasobów - statusu serwera, statusu terminala, statusu usługi i zagrożenia.
	Obsługa tygodniowych statystyk trendów zagrożeń, w tym ryzykownych serwerów, ryzykownych terminali i zagrożeń
	Obsługa analizy statystycznej zagrożeń, w tym etapu ataku, typu, informacji o opisie, sugestii usunięcia, informacji o zagrożeniu, informacji o dowodach i informacji o procesie. Można dostosować elementy wyświetlane w nagłówku i sortować według pól nagłówka.
	Obsługuje kompleksowe wyświetlanie sytuacji zagrożenia z perspektywy kompleksowej, zasobów i ataku
	Obsługuje oznaczanie zagrożeń i powiązanych zagrożeń, w tym rozwiązanych lub fałszywie pozytywnych.
	Obsługa zapytań o zagrożeniu z kombinacją wielu warunków, w tym nazwy, typu, poziomu, adresu IP, statusu itp.
	Obsługa zagregowanego wyświetlania i statystyk zagregowanych szczegółów zagrożeń według nazwy zagrożenia
	Obsługuje funkcję przechowywania pakietów informacji o dowodach i obsługuje pobieranie oryginalnego ruchu zebranego przez czujnik
	Obsługa pobierania oryginalnego pakietu danych
	Obsługa narzędzi dekodujących, informacje o zagrożeniach obsługują dekodowanie URL

	i Base64
	Obsługa bezpośredniej obsługi zagrożeń na stronie zdarzeń. Poza normalną konfiguracją polityk, można wydawać polityki bezpieczeństwa hosta, w tym blokowanie IP, kontrolę dostępu, kontrolę procesu, izolowanie plików, ponowne uruchamianie terminala, kontrolę USB itp.
	Obsługa analizy statystycznej serwerów/terminali zagrożeń, w tym etykiet zagrożeń, zagrożeń, poziomów ważności itp.
	Obsługuje powiązanie użytkowników końcowych w celu wyświetlenia najnowszego adresu IP logowania, adresu MAC i czasu ostatniego zdarzenia
	Obsługa uszkodzeń serwera/terminala, ocena aktualnego uszkodzenia hosta, wizualizacja zagrożeń na różnych etapach ataku i dostarczanie sugestii dotyczących usuwania zagrożeń.
	Obsługa perspektywy zagrożenia, relacji zagrożenia, kierunku ataku i wizualizacji zakresu wpływu.
	Obsługa widoku zasobu, który został podejrzany o naruszenie, oraz przeglądanie raportów dotyczących naruszeń, raportów ryzyka, powiązanych zagrożeń i informacji o lukach w zabezpieczeniach.
	Obsługuje statystyki monitorowania usług zagrożeń, które mogą być statystycznie filtrowane według obszaru, czasu, nazwy, poziomu i etykiety ryzyka, a także mogą być sortowane według pola nagłówka.
	Obsługuje szczegółowe statystyki zagrożeń, w tym serwery, obszary, opisy biznesowe, raporty o naruszeniach.
	Obsługa odbierania, przechowywania i wyświetlania dzienników Syslog, w tym dzienników Syslog IPv6
	Obsługa odbierania i przechowywania dzienników Netflow
	Obsługa odbierania i przechowywania metadanych
	Obsługa odbierania i przechowywania dziennika sysmon
	Obsługa odbierania i przechowywania dzienników systemu Linux
	Obsługa statystyk dziennika, w tym ogólnej liczby i statystyk typu dzienników Syslog, netflow, metadanych, sysmon i linux.
	Obsługa analizowania i wyświetlania dzienników IPv6 Netflow.
	Obsługa wyszukiwania zagrożeń, serwerów,

	usług i dzienników w języku naturalnym, języku SPL i kombinacji predefiniowanych warunków.
	Obsługuje zdarzenia oznaczone jako false positive i zapewnia funkcję czyszczenia, którą można ręcznie usunąć pojedyncze zagrożenia lub usunąć zagrożenia partiami
6. Analiza podatności	Obsługa wyświetlania i przeglądania sytuacji podatności z perspektywy hosta, w tym: adres IP hosta, nazwa raportu podatności, czas skanowania, status podatności,
	Obsługa wyświetlania i przeglądania sytuacji podatności z perspektywy podatności, w tym: nazwa podatności, typ podatności, poziom podatności, liczba ustaleń
	Obsługa ręcznego importu raportów o podatnościach, minimum raportów w formacie .nessus z wersji 6.x i 8.x.
	Obsługa instalacji dodatkowych skanerów podatności w celu uzyskania raportów o podatnościach, administratorzy mogą dodawać, przeglądać, modyfikować i usuwać skanery;
	Obsługa wydawania zasad skanowania i konfiguracji skanowania do urządzeń skanujących podatności
	Obsługa okresowego zarządzania zadaniami skanowania (codziennie, co tydzień, co miesiąc), dodawanie, usuwanie, modyfikowanie, otwieranie i zamykanie zadań skanowania
7. Zarządzanie ryzykiem	Wyświetlanie ogólnych informacji o ryzyku wszystkich zasobów/serwerów/usług w formie wykresów, w tym: liczba ryzykownych zasobów, liczba ważnych zagrożonych zasobów, rozkład ryzykownych serwerów, rozkład zagrożeń serwera / trend tygodniowy, rozkład podatności serwera / trend tygodniowy.
	Obsługuje wyświetlanie listy ryzykownych zasobów/serwerów/usług i szczegółów poszczególnych ryzykownych zasobów. Szczegóły ryzykownych zasobów obejmują trzy wymiary: raport ryzyka, podatność serwera i same zagrożenia.
	Obsługa eksportowania 10 000 najważniejszych zagrożeń/informacji o ryzykownych zasobach przechowywanych w systemie w formacie CSV
	Obsługuje funkcję oceny awarii ryzykownych serwerów i ryzykownych terminali.
8. Reagowanie na incydenty	Wspieranie wyznaczonej osoby odpowiedzialnej za przetwarzanie odpowiednich zagrożeń, podatności i obiektów ryzyka za pośrednictwem systemu zleceń pracy.
	Obsługa statystycznego wyświetlania wskaźnika realizacji zleceń, całkowitej liczby zleceń, oczekujących zleceń i innych informacji.

	Obsługuje dodawanie powiązanych podmiotów do platformy XDR w celu scentralizowanego zarządzania, wykonywanie działań na powiązanych podmiotach.
	Obsługa sieciowych urządzeń zabezpieczających NGFW, IPS, WAF tego samego producenta
	Obsługa statystycznego wyświetlania całkowitej liczby playbooków, automatycznych playbooków i potwierdzonych playbooków oraz innych informacji.
	Obsługuje konfigurację warunków wyzwalania, warunków oceny dla automatycznej reakcji i działań odpowiedzi (wydawanie polityk, blokowanie adresów IP lub tworzenie zleceń pracy)
	Wbudowane 5 predefiniowanych playbooków, w tym miningu, wymuszeń i słabych haseł.
	Podczas wydawania polityki obsługuje ustawianie czasu jej działania
	Obsługuje dwa tryby: automatycznych playbooków i potwierdzonych playbooków, tryb potwierdzony obsługuje powiadomienia e-mail do administratora.
	Playbook obsługuje dopasowywanie adresów IPv4 i IPv6 oraz segmentów adresów.
	Gdy playbook wykonuje zadanie, które wymaga ręcznego potwierdzenia, zostanie ono zapisane na liście zadań, na które należy odpowiedzieć.
	Obsługa polityk dostarczanych do firewalla za pośrednictwem playbooków, muszą być sprawdzane przez agregację polityk, aby uniknąć dużej liczby podobnych polityk pojawiających się na urządzeniu firewall i wpływających na wydajność firewalla.
9. Zarządzanie raportami	Centralne wyświetlanie wszystkich wygenerowanych raportów, obsługa przeglądania zawartości raportów online lub eksportowanie i wyświetlanie w formacie PDF; obsługa natychmiastowego ręcznego generowania raportów o określonych wymaganiach
	Obsługa konfiguracji zadań raportowania i regularne generowanie odpowiednich raportów zgodnie z ustalonymi warunkami, w tym raportów dziennych, tygodniowych i miesięcznych, a także raportów krótkich i szczegółowych.
	Obsługa uruchamiania/zatrzymywania zadań raportowania w dowolnym momencie
	Wstępnie ustawione szablony dla ogólnych raportów ryzyka, raportów ryzyka terminali, raportów ryzyka serwerów i raportów reagowania na incydenty, a także obsługa niestandardowych szablonów raportów

	skonfigurowanych przez użytkownika.
	Obsługa logo raportu zdefiniowanego przez użytkownika.
	Wsparcie dla statystyk i archiwizacji dokumentów i raportów.
10. Intelligence Center	Obsługuje odbieranie nowych informacji o zagrożeniach i obsługuje zapytania wywiadowcze na podstawie adresu IP/pliku/domeny/nazwy URL/nazwy/CVEID/etykiety zagrożenia z perspektywy poziomu zagrożenia i zakresu czasu.
	Po otrzymaniu wypchniętych informacji CVE, wsparcie w celu zainicjowania powiązanych zadań skanowania podatności i wysyłania zleceń pracy.
	Obsługa wyświetlania informacji o rodzinie/grupie i obsługa powiązania z modułem śledzenia w celu generowania tagów
	Obsługuje co najmniej 7 typów baz danych wywiadowczych, w tym bazę danych wywiadowczych DNS, bazę danych wywiadowczych złośliwego kodu, bazę danych wywiadowczą URL, bazę danych wywiadowczą IP, bazę danych wywiadowczą podatności, bazę danych wywiadowczą wykrywania włamań i bazę danych geolokalizacyjnych.
	Obsługuje aktualizację offline i aktualizację online bazy danych wywiadowczych. Aktualizacja online obejmuje aktualizację ręczną i zaplanowaną.
	Obsługa zdefiniowanej przez użytkownika białej listy nazw domen, skutecznej dla wszystkich reguł DNS.
	Obsługa zdefiniowanej przez użytkownika białej listy plików, która obowiązuje dla wszystkich reguł klasy plików.
	Obsługa zdefiniowanej przez użytkownika konfiguracji globalnej białej listy
	Obsługa importu/eksportu białych list globalnych, klas DNS i klas plików jako plików CSV
	Obsługa zdefiniowanej przez użytkownika czarnej listy DNS, złośliwego kodu i IP
11. Zarządzanie zasobami	Obsługa wsadowego importu/eksportu informacji o zasobach obszaru, usługi, serwera i terminala w postaci plików CSV.
	Obsługa aktywnego wykrywania i ręcznego importowania w celu wykrywania i wyświetlania zasobów w sieci prywatnej, ale nie na liście zasobów, które mogą być klasyfikowane i aktualizowane przez użytkowników
	Obsługa aktywnego wykrywania i ręcznego

	importowania w celu wykrywania i wyświetlania zasobów w sieci prywatnej, ale nie na liście zasobów, które mogą być klasyfikowane i aktualizowane przez użytkownikówObsługa zaawansowanej klasyfikacji zasobów, w tym etykiet klasyfikacji zasobów w 5 głównych kategoriach i 29 podkategoriach, takich jak terminale, serwery, sprzęt sieciowy, sprzęt bezpieczeństwa, sprzęt IOT i inny sprzęt.
	Obsługa scentralizowanego zarządzania obszarami sieci, w tym zarządzanie konfiguracją ważności, lokalizacji i osób odpowiedzialnych.
	Obsługa statystycznego wyświetlania liczby terminali i serwerów w obszarze sieci.
	Obsługa scentralizowanego zarządzania serwerami i grupami serwerów, w tym zarządzanie konfiguracją adresu IP, obszaru, usługi, systemu operacyjnego, typu usługi itp., obsługa konfiguracji wielu segmentów sieci IP.
	Obsługa scentralizowanego zarządzania terminalami i grupami terminali, w tym zarządzanie konfiguracją adresów IP, obszarów, systemów operacyjnych itp., obsługa konfiguracji wielu segmentów sieci IP.
	Obsługa odbierania pakietów rozliczeniowych Radius wysyłanych przez zewnętrzne serwery uwierzytelniania, analizowanie bieżących informacji o użytkownikach i hostach online oraz wyświetlanie ich w "Statusie użytkownika".
	Obsługa scentralizowanego zarządzania usługami i przeprowadzanie analizy zagrożeń z poziomu usługi poprzez dodawanie serwerów tego samego typu do tej samej usługi.
	Obsługa pasywnej identyfikacji ruchu, wykrywanie i wyświetlanie zasobów sieci prywatnej, które nie znajdują się na liście konfiguracji zasobów, oraz oczekiwanie na potwierdzenie i klasyfikację przez użytkownika.
	Obsługuje konfigurację zasobów serwerowych typu IPv6 i zasobów terminalowych oraz obsługuje identyfikację zasobów typu IPv6 za pomocą informacji Netflow.
12. Rules Engine	Obsługa wykrywania skanowań, w tym skanowanie SYN, skanowanie UDP, atak skanowania adresu IP, atak skanowania portów
	Obsługa silnika plików, w tym wykrywanie podejrzanych plików PE (wykonywalnych), plików z niedopasowanym sufiksem i zawartością, podejrzanych plików z wieloma sufiksami, podejrzanych plików z wieloma sufiksami, plików z podejrzanym rozmiarem, plików z niedopasowanym sufiksem

	i zawartością oraz wrażliwych plików.
	Obsługa mechanizmów wykrywania HTTP, w tym HTTP Header Contain Abnormal Keywords, HTTP Response Contain X-Sinkhole, Excessive HTTP Response Errors, Suspicious HTTP Request via Tor.
	Obsługa mechanizmów wykrywania podejrzanych protokołów, w tym podejrzanej aktywności IRC, podejrzanej aktywności LDAP, podejrzanej aktywności NetBIOS, podejrzanej aktywności SMB i podejrzanej aktywności SSDP.
	Obsługa mechanizmów brute force, w tym FTP Brute Force Attack, IMAP4 Brute Force Attack, LDAP Brute Force Attack, MYSQL Brute Force Attack, POP3 Brute Force Attack, SMTP Brute Force Attack, SSH Brute Force Attack, TELNET Brute Force Attack, Weak Password Cracking, RDP Brute Force Attack, VNC Brute Force Attack i SMB Brute Force Attack.
	Obsługa silnika domen, w tym DNS Domain is Generated by DGA, Suspicious Amount of DNS NXDOMAIN Responses, Abnormal DNS Response, TTL in DNS Message is 0, IP Mapped Domain is in Blacklist, IP Mapped Domain is Generated by DGA, Suspicious DNS Tunnel Activity, DNS Protocol Abuse i Suspicious DNS Tunnel Data Transfer.
	Obsługa silnika ransomware, analiza i wykrywanie zgodnie z zachowaniem ransomware
	Obsługa miningu, inteligentne wykrywanie cech zachowania miningu
	Obsługuje silnik klasy zachowania USB, taki jak zachowanie podczas podłączania i odłączania urządzeń USB.
	Obsługuje blokowanie dostępu, w tym naruszenie dostępu, tworzenie złośliwych procesów Powershell, naruszenie uprawnień użytkownika do plików lub aplikacji, nieprawidłowe logowanie i naruszenie dostępu do aplikacji.
	Obsługuje regułę "Naruszenie dostępu do aplikacji". Użytkownicy mogą określić czarną listę / białą listę dostępu do aplikacji, konfigurując obiekt ochrony w regule, wykrywać, czy ruch ma złośliwy dostęp do określonych zasobów usługi aplikacji i generować zdarzenia zagrożeń.
	Obsługuje wykrywanie słabych haseł dla 6 protokołów HTTP, TELNET, SMTP, POP3, IMAP i FTP, które przesyłają nazwę użytkownika i hasło w postaci zwykłego tekstu.

	Obsługuje ustawienia personalizacji silnika w oparciu o zebrane dzienniki zagrożeń, ustawienia wstępne: Malware, Spam, Phishing, DoS, Atak sieciowy, Skanowanie, EternalBlue, Próba ataku WebShell, RDP Remote Windows Kernel Release Reuse Vulnerability
	Obsługuje konfigurację analizy korelacji dzienników zagrożeń hostów
	Obsługuje statystyki zagrożeń oparte na polu x-forward
	Wsparcie dla korelacji wielu zagrożeń i konfiguracji silnika kill-chain w celu odkrywania nowych informacji o zagrożeniach i dokładnej identyfikacji zagrożeń.
	Reguła analizy korelacji klas dzienników zagrożeń sieciowych obsługuje konfigurację adresu źródłowego/docelowego IPv6.
	Reguły analizy asocjacji klas nietypowego ruchu obsługują konfigurację segmentów sieci IP typu IPv6.
13. Zarządzanie logami	Obsługa konfiguracji zaufanych źródeł logów w celu zarządzania i kontrolowania źródeł danych oraz zapewnienia bezpieczeństwa systemu.
	Nie ma ograniczeń co do liczby dostępnych źródeł logów.
	Obsługuje zarządzanie i kontrolę źródeł dzienników Syslog/Netflow oraz ustawienia tworzenia kopii zapasowych i przeglądania dzienników.
	Obsługuje analizowanie, prezentowanie i dalszą analizę dzienników Syslog urządzeń innych firm; zapewnia predefiniowane konfiguracje analizowania dzienników i szablony dla popularnych sieciowych urządzeń zabezpieczających innych firm; obsługuje również tworzenie niestandardowych dzienników w oparciu o format konfiguracji i szablonu analizowania dziennika informacji Syslog, reguły parsowania obejmują Grok, klucz-wartość, JSON.
	Obsługa niestandardowych pól mapowania dla dzienników innych firm.
	Obsługa wyświetlania miejsca na dysku oraz tworzenie kopii zapasowych.
	Obsługa przeglądania informacji o hoście, który wysyła dzienniki Sysmon.
	Obsługuje wysyłanie dzienników Syslog odebranych przez iSource i zagrożeń wykrytych przez platformę do innych serwerów ; Obsługuje konfigurację szyfrowanego protokołu TCP i obsługuje użycie szyfrowanego protokołu

	TCP do odbierania i przesyłania informacji dziennika.
14. System zarządzania	Obsługa wyświetlania podstawowych informacji o oprogramowaniu i sprzęcie systemu, takich jak: platforma sprzętowa, wersja oprogramowania, baza reguł, baza geograficzna, wersja bazy danych analizy zagrożeń itp.
	Obsługa dodawania, modyfikowania i usuwania użytkowników systemu.
	Obsługa rozdziału uprawnień dla administratorów, operatorów i audytorów logów.
	Obsługa konfiguracji zaufanych hostów i kontrola praw dostępu każdego hosta do systemu XDR
	Obsługa konfiguracji i zarządzania wszystkimi kontaktami w systemie
	Obsługa rejestrowania dziennika zdarzeń i dziennika operacji samego systemu oraz obsługa ustawiania maksymalnego czasu przechowywania dziennika systemu
	Obsługa aktualizacji wersji offline.
	Obsługa przeglądania licencji systemowych
	Obsługa serwera pocztowego, ustawień konta i odbiorcy.
	Bramka SMS, obsługuje konfigurację modułu SMS.
	Obsługuje ustawianie reguł alarmowych dla zagrożeń i systemów sprzętowych oraz wyzwala alarmy w postaci wiadomości e-mail, wiadomości tekstowych lub dźwięków; obsługuje wyświetlanie informacji alarmowych o zagrożeniach, działaniu systemu i wygaśnięciu licencji w interfejsie.
	Obsługa ustawień systemowego adresu IP i serwera DNS
	Obsługa edycji i usuwania podłączonych urządzeń typu Sensor.
	Obsługa monitorowania podstawowych informacji o podłączonych czujnikach, w tym adresu IP, numeru seryjnego i modelu sprzętu.
	Obsługa monitorowania informacji o stanie podłączonych urządzeń Sensor, w tym stanu online, ruchu w czasie rzeczywistym, wykorzystania procesora i wykorzystania dysku.
	Obsługa ustawień zabezpieczeń systemu, ustawień zasad logowania, ustawień zasad haseł.
	Obsługa ustawień serwera pocztowego, konta i odbiorcy.
	Obsługa funkcji ustawień zabezpieczeń: - W przypadku korzystania z domyślnego administratora systemu do logowania i hasła

	początkowego do urządzenia, system obsługuje funkcję wymuszania zmiany hasła początkowego; - Obsługuje konfigurację funkcji limitu czasu logowania. Po zalogowaniu się użytkownika do urządzenia, jeśli żadna operacja nie zostanie wykonana po upływie określonego limitu czasu, użytkownik musi ponownie zalogować się do urządzenia; - Obsługa funkcji blokady użytkownika, jeśli użytkownik wprowadzi nieprawidłową nazwę użytkownika i hasło określoną liczbę razy. System zablokuje konto użytkownika lub adres IP zgodnie z określonym czasem blokady; - Obsługuje konfigurację reguł haseł, z którymi muszą być zgodne hasła użytkowników; - Obsługa konfiguracji funkcji wymuszonej zmiany hasła dla nowych użytkowników.
	Obsługa konfiguracji funkcji wymuszonej modyfikacji hasła. Jeśli hasło do konta użytkownika przekroczy określoną datę wygaśnięcia, system wymusi na użytkowniku użycie hasła przy ponownym logowaniu.
	Obsługuje generowanie niezależnych reguł alarmowych dla zasobów/zdarzeń, aby spełnić zróżnicowane wymagania alarmów w różnych scenariuszach.
15. Zarządzanie hierarchiczne	Obsługuje hierarchiczne wdrażanie zarządzania, wykorzystuje kanał kaskadowy oparty na transmisji TCP i dwukierunkowym uwierzytelnianiu SSL do realizacji połączenia między platformą wyższego poziomu a platformą niższego poziomu.
	Platforma wyższego poziomu obsługuje pełnoekranowe zarządzanie hierarchiczne, prezentując sytuację ryzyka całej platformy.
	Platforma wyższego poziomu obsługuje przełączanie do widoku innych platform, obsługuje przeglądanie ryzykownych aktywów, słabych punktów, zagrożeń i innych informacji
16. Wydajność	Proponowane rozwiązanie musi obsługiwać przepustowość 3 Gb/s
	Proponowane rozwiązanie musi obsługiwać 5000 EPS
17. Licencjonowanie	Licencja oprogramowania powinna być bezterminowa wraz ze wsparciem na okres 36 miesięcy
18. Wsparcie techniczne	Dystrybutora na terenie Polski, świadczone w języku polskim
19. Funkcje Next Generation Firewall	
20. Elementy systemu bezpieczeństwa	Urządzenie musi mieć możliwość jednoczesnej pracy w trybie Layer 3 (routing), transparentnym

	(most) i Layer 2 (port mirroring) bez konieczności wirtualizacji sprzętu
	Możliwość stworzenia minimum 128 wirtualnych interfejsów zdefiniowanych jako VLAN w oparciu o standard 802.1Q.
	W zakresie Firewall, obsługa nie mniej niż 2 200 000 jednoczesnych połączeń i 130 000 nowych połączeń na sekundę.
	System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o minimalnej pojemności 8 GB do celów logowania i raportowania.
	Możliwość rozszerzenia pamięci do 1.92 TB
	System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zgromadzonych na urządzeniu.
	System musi mieć możliwość włączenia min 1 systemu wirtualnego bez dodatkowej licencji i możliwości rozszerzenia do minimum 5 poprzez dodatkową licencję w przyszłości
	Systemy wirtualne muszą obsługiwać QOS
	System pełniący funkcję zapory musi posiadać nie mniej niż: 2x SFP+, 8x SFP, 8xGigabitEthernet, Dedykowany port do zarządzania
21. Funkcjonalności	Kontrola dostępu — zapora sieciowa Stateful Inspection
	Ochrona przed wirusami - komercyjny antywirus [AV]
	Poufność danych - IPSec VPN i SSL VPN
	Kontrola witryn sieci Web — filtr URL
	Kontrola zawartości poczty - antyspam (dla protokołów SMTP, POP3)
	Kontrola przepustowości i ruchu [QoS i kształtowanie ruchu] z alokacją Tunnel w oparciu o strefę bezpieczeństwa, interfejs, adres, użytkownika/grupę użytkowników, serwera/ grupę serwerów, aplikację/grupę aplikacji, TOS, VLAN
	Kontrola aplikacji i rozpoznawanie ruchu P2P (wideo, gry itp.) oraz ograniczanie nowych połączeń i jednoczesnych sesji
	Reputacja IP
	Cloud Sandbox
	API – możliwość wgrywania i wyciągania informacji z systemu dedykowanym interfejsem Rest API
22. Wydajność	Analiza ruchu szyfrowanego protokołem SSL
	Wydajność Firewall co najmniej 10 Gb/s
	Wydajność skanowania strumienia danych z włączonymi funkcjami: NGFW z włączonym

	IPS i kontrolą aplikacji 4 Gb/s
	Wydajność ochrony przed atakami (IPS) minimum 8 Gb/s
	Wydajność AV nie mniej niż 4.5 Gb/s
	Wydajność skanowania z włączoną kontrolą aplikacji, AV, IPS, filtrem URL nie mniejsza niż 2.5Gbps.
23. Funkcjonalności VPN	Wydajność IPSec VPN, nie mniej niż 5 Gb/s
	Tworzenie połączenia lokalizacja-lokalizacja i oraz klient-lokalizacja
	Producent oferowanego rozwiązania VPN powinien zapewnić klienta VPN współpracującego z proponowanym rozwiązaniem
	Praca w topologiach Hub and Spoke i Mesh
	Wspierane mechanizmy : IPSec NAT Traversal, DPD, Replay Detection, Xauth, DHCP over IPsec
	Wsparcie grup DH dla IKEv1: 1,2,5,19,20,21,24
	Wsparcie grup DH dla IKEv2: 1,2,5,14,15,16,19,20,21,24
	Wsparcie dla SSL VPN z możliwością testowania zgodności hosta (compliance) co najmniej w zakresie: - Wersji systemu operacyjnego - Zaaplikowanych patchy - Ustawień internetowych - Zainstalowanego oprogramowania antywirusowego - Włączonego Firewalla - Walidacji kluczy rejestru - Walidacji istnienia plików - Walidacji uruchomionych procesów - Walidacji uruchomionych lub zainstalowanych serwisów
	Możliwość rozszerzania ilości użytkowników VPN odpowiednią licencją
	Obsługa PnPVPN (Plug and Play VPN)
24. Routing	Rozwiązanie musi zapewniać: obsługę Policy Routing, routingu statycznego i dynamicznego w oparciu o protokoły: RIPv2, OSPF, BGP, IS-IS
	Obsługa Policy Based Routing
	Funkcjonalność Virtual Wire
25. Translacja adresów NAT	Tłumaczenie adresu NAT adresu źródłowego i adresu NAT adresu docelowego.
	Obsługa NAT46, NAT64, DNS64
	Wsparcie dla STUN
26. Polityka bezpieczeństwa systemu	Polityka bezpieczeństwa systemu bezpieczeństwa musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje bezpieczeństwa, rejestrowanie zdarzeń i

	zarządzanie pasmem sieci (w tym gwarantowaną i maksymalną przepustowość, priorytety).
	Możliwość budowania min. 12000 polityk
	Musi posiadać funkcjonalność asystenta polityk, dzięki której możliwe jest generowanie reguł bezpieczeństwa w oparciu o przepływ ruchu sieciowego
	Musi być w stanie skonfigurować agregowane polityki
	Musi być w stanie ograniczyć sesje na podstawie źródłowego adresu IP, docelowego adresu IP, harmonogramu, protokołu aplikacji (mysql, ms-sql, sqlnet, pobieranie P2P)
27. Wydzielenie stref bezpieczeństwa	Możliwość tworzenia osobnych stref bezpieczeństwa Firewall, np. DMZ, LAN, VPN
	Musi mieć możliwość konfiguracji oddzielnych wirtualnych routerów
	Musi mieć możliwość konfigurowania oddzielnych wirtualnych przełączników
28. Ochrona antywirusowa	Silnik antywirusowy musi być oparty na przepływie tzw. flow-based
	Musi umożliwiać skanowanie protokołów HTTP, SMTP, POP3, IMAP, FTP / SFTP, SMB
	Możliwość ręcznego dodawania lub usuwania sygnatury MD5 do bazy danych AV
	Musi obsługiwać wykrywanie wirusów w plikach skompresowanych, takich jak RAR, ZIP, GZIP, BZIP2, TAR, a także wykrywać wielowarstwowe pliki skompresowane dla nie mniej niż 5 warstw dekompresji
29. Równoważenie obciążenia	Obsługa redundantnego równoważenia obciążenia ISP i ISP z wykrywaniem łącza dla określonej nazwy domeny oraz monitorowanie stanu łącza poprzez aktywną metodę wykrywania
	Obsługa równoważenia obciążenia serwerów w oparciu o weighted hashing, weighted leastconnection i weighted round-robin
	Kontrola stanu serwera, monitorowanie sesji i ochrona sesji
30. Ochrona IPS	Ochrona IPS musi opierać się przynajmniej na analizie protokołu i sygnatury.
	Baza danych wykrytych ataków musi zawierać co najmniej 16000 sygnatur. Dodatkowo musi być w stanie wykrywać anomalie protokołów i ruchu, które stanowią podstawową ochronę przed atakami DoS i Ddos.
	Funkcjonalność zapobiegania atakom SQL injection, XSS injection
	Możliwość budowania własnych niestandardowych reguł IPS
31. Obrona przed atakiem	Ochrona przed nieprawidłowym działaniem

	protokołu
	Anti-DoS/DDoS, zawierający ochronę przed SYN flood, UDP flood, DNS reply flood, DNS query flood defense, TCP fragment, ICMP fragment itp.
	Wsparcie IPv4 jak i IPv6 dla ochrony przed DNS query flood i DNS reply flood
	Biała lista docelowych adresów IP
32. Ochrona antyspam	Rozwiązanie musi zapewniać ochronę przed spamem w czasie rzeczywistym
	Wspieranymi protokołami są minimum SMTP, SMTPS, POP3, POP3S
	Skanowanie antyspamowe musi odbywać się w ruchu w obu kierunkach
	Musi istnieć możliwość dodawania wyjątków w zakresie skanowania antyspamowego, minimum białych list domen
33. Kontrola aplikacji	Kontrola aplikacji musi być w stanie kontrolować ruch w oparciu o głęboką analizę pakietów, a nie tylko w oparciu o wartości portów TCP/UDP
	Baza danych aplikacji zawierająca ponad 6000 aplikacji, które można filtrować według nazwy, kategorii, podkategorii, technologii i ryzyka
34. Filtr adresów URL	Baza filtrów URL pogrupowana w co najmniej 64 kategorie tematyczne. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków.
	Możliwość zdefiniowania własnej bazy kategorii www.
	Automatyczne pobieranie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy danych dostarczającej filtr URL.
	Kategoria takie jak hazard, malware, spam, botnety
	Obsługa Safe Search
	Blokowanie i logowanie stron URL z określonymi słowami, które można budować przez wyrażenia regularne
	Dostosowanie strony ostrzeżenia
35. Ochrona danych	Kontrola transferu plików na podstawie typu pliku, rozmiaru i nazwy
	Identyfikacja protokołu pliku, w tym HTTP,FTP、SMTP, POP3、IMAP
	Obsługa deszyfracji SSL do filtrowania plików przesyłanych przez HTTPS, SMTPS, POP3S, IMAPS
	Filtrowanie plików przesyłanych przez SMB
36. Reputacja IP	Identyfikacja i filtrowanie ruchu z ryzykownych adresów IP, takich jak hosty botnet, spamerzy, węzły Tor, podejrzane hosty i adresy IP atakujące metodą brute force

	Logowanie, odrzucanie pakietów lub blokowanie dla różnych rodzajów ryzykownego ruchu IP
37. Zapobieganie botnetom	Wykrywanie intranetowych hostów botnetu, monitorując połączenia C&C i blokowanie dalszych zaawansowanych zagrożeń takich jak botnet i oprogramowanie ransomware
	Wsparcie DNS sinkhole
	Wsparcie wykrywania tunelowania DNS
	Wyrywanie i blokowanie DGA
38. Cloud Sandbox	Złośliwe oprogramowanie emulowane w wirtualnym środowisku oparte na architekturze chmury w celu wykrywania nieznanych zagrożeń
	Obsługa protokołów, takich jak HTTP/HTTPS, POP3, IMAP, SMTP, FTP i SMB
	Obsługa typów plików : PE, ZIP, RAR, Office, PDF, APK, JAR, SWF i skryptów
	Obsługa blokowania wyników wykrywania w celu szybkiego blokowania nieznanych zagrożeń
39. Uwierzytelnianie użytkownika	System bezpieczeństwa musi być w stanie przeprowadzić uwierzytelnianie tożsamości użytkownika z nie mniej niż: - Statyczne hasła i definicje użytkowników przechowywane w lokalnej bazie danych systemu - Statyczne hasła i definicje użytkowników przechowywane w bazach danych zgodnych z LDAP - Hasła dynamiczne (RADIUS) oparte o zewnętrzne bazach danych - Dynamiczna autoryzacja przez RADIUS na podstawie komunikatów CoA
	Musi umożliwiać budowę architektury uwierzytelniania pojedynczego logowania w środowisku Active Directory
	Wsparcie usług terminalowych
	Uwierzytelnianie użytkownika przez Web przed dostępem do internetu
	Obsługa dwuskładnikowego uwierzytelniania, SMSy, certyfikaty i tokeny
40. Raportowanie i przeglądanie logów:	Wbudowany w system bezpieczeństwa system raportowania i przeglądania logów nie może wymagać dodatkowej licencji na jego działanie
	W zakresie zaimplementowanych funkcjonalności systemu raportowania i przeglądania logów nie mniej niż: - Posiadanie predefiniowanych raportów dla ruchu internetowego, modułu IPS, skanera antywirusowego i antyspamowego - Generowanie co najmniej 10 rodzajów raportów
41. Wysoka dostępność	Rozwiązanie musi obsługiwać tryby

	Active/Active i Active/Passive
	Rozwiązanie musi obsługiwać następujące opcje wdrażania HA: - HA z agregacją linków - Full mesh HA - Geograficznie rozproszony HA
42. System logowania	Wraz z systemem musi być zapewniony system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy chmurowej, do której dostęp jest cały czas z dowolnego urządzenia oraz dedykowanej aplikacji mobilnej.
43. Certyfikaty	Rozwiązanie musi posiadać certyfikat Common Criteria EAL4+ lub posiadać certyfikat ICSA Labs dla funkcji Firewall
44. Zarządzanie	Elementy systemu muszą mieć możliwość zarządzania lokalnie (HTTPS, SSH) oraz współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. Komunikacja między systemami bezpieczeństwa a platformami zarządzania musi odbywać się za pomocą protokołów szyfrowanych.
	Zarządzanie urządzeniem i konfiguracja musi odbywać się za pośrednictwem WebUI bez instalowania oddzielnego oprogramowania, takiego jak dedykowana konsola.
45. Licencjonowanie	Licencja oprogramowania powinna być bezterminowa wraz ze wsparciem na okres 36 miesięcy
	Licencje na wszystkie funkcje bezpieczeństwa producentów na okres minimum 36 miesięcy (IPS, AV, AS, QoS, Cloud-Sandbox, URL, IP Reputation, Botnet C&C)
46. Wsparcie techniczne	Dystrybutora na terenie Polski, świadczone w języku polskim

2. Dostarczone rozwiązanie musi być połączone z wdrożeniem i siedzibie i infrastrukturze Zamawiającego. Wdrożenie może odbywać się zdalnie lub stacjonarnie w siedzibie Zamawiającego. Forma zdalna wdrożenia obejmuje przesłanie wstępnie skonfigurowanego fizycznego urządzenia na adres Zamawiającego i dalszą zdalną jego konfigurację. Wdrożenie rozwiązania programowego (maszyny wirtualnej) może obywać się zdalne lub stacjonarnie w siedzibie Zamawiającego
3. Szkolenie dla administratorów. Wymagane jest przeszkolenie co najmniej dwóch administratorów wskazanych przez Zamawiającego. Szkolenie musi odbywać się stacjonarnie w siedzibie Zamawiającego. Minimalny czas trwania szkolenia to 8 godzin zegarowych.
4. Możliwość skorzystania z konsultacji z inżynierem do 1 miesiąca po odbytym

szkoleniu w formie e-mail lub kontaktu telefonicznego

5. Szkolenie prowadzone przez inżyniera posiadającego certyfikat wystawiony przez producenta wdrażanego rozwiązania
6. Oferowane rozwiązanie musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski.
7. Oferowane urządzenia muszą być objęte co najmniej 36-miesięczną gwarancją producenta, a naprawy muszą być realizowane w serwisie na terenie Polski.