Śląska Sieć
Metropolitalna
Sp. z o.o.

Wstępny Opis Przedmiotu Zamówienia

Dostawa oprogramowania na potrzeby uruchomienia Centrum Nadzoru Bezpieczeństwa Teleinformatycznego (ang. SOC – Security Operations Center) dla Śląskiej Sieci Metropolitalnej Sp. z o. o.

Śląska Sieć Metropolitalna Sp. z o.o. zwraca się z prośbą

o przedstawienie szacunkowej wartości przedmiotu zamówienia na

Dostawę oprogramowania na potrzeby uruchomienia Centrum Nadzoru Bezpieczeństwa Teleinformatycznego (ang. SOC – Security Operations Center) dla Śląskiej Sieci Metropolitalnej Sp. z o. o.

I. ZAMAWIAJĄCY

Śląska Sieć Metropolitalna Sp. z o.o.
ul. Bojkowska 37P, 44-100 Gliwice
NIP: 6312578261, REGON: 241069249
Sąd Rejonowy w Gliwicach KRS: 0000322774

II. WSTĘPNY OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia będzie dostarczenie oprogramowania na potrzeby uruchomienia Centrum Nadzoru Bezpieczeństwa Teleinformatycznego (ang. SOC – Security Operations Center) dla Śląskiej Sieci Metropolitalnej Sp. z o. o. w zakresie:

1. Wdrożenia oprogramowania wykorzystującego co najmniej mechanizmy Active Directory, EDR i/lub XDR, logów urządzeń sieciowych, w tym urządzeń bezpieczeństwa sieci, (w większości marki HUAWEI) kopii informacji o ruchu sieciowym w formie Flowstream lub informacji pochodzących z systemów ADS (Anomaly Detection System) i/lub NDR (Network Detection and Response), logów systemów serwerowych i ich hipernadzorców, oraz informacji pochodzących bezpośrednio ze stacji końcowych użytkowników i serwerów (kolekcja przy użyciu agenta systemowego, lub natywnych mechanizmów kolekcji logów, wbudowanych w system operacyjny).

2. Zamawiający dopuszcza następujące warianty rozwiązania dla środowiska serwerowego:
   a. dostarczone przez Wykonawcę wymaganej platformy sprzętowej wraz ze wszystkimi wymaganymi licencjami,
   b. wymagane środowisko udostępnione przez Zamawiającego (VMWare ESXi) – niezbędne wskazanie przez Wykonawcę minimalnych i zalecanych wymagań technicznych.

3. Zamawiający dla wariantu pkt 2b wymaga oszacowania następujących wariantów licencjonowania:
   a. Wykonawca dostarcza wyłącznie licencje będące przedmiotem niniejszego zapytania, gdzie licencje systemu operacyjnego i baz danych zapewnia Zamawiający (niezbędne wskazanie przez Wykonawcę minimalnych i zalecanych wymagań w tym zakresie)
   b. częściowo udostępnione przez Zamawiającego (system operacyjny), w pozostałym zakresie dostarczone przez Wykonawcę.

4. Zamawiający zakłada etapową realizację zadania.

5. **ETAP 1** - zakłada się następujący zakres źródeł informacji istotnych z punktu widzenia wdrożenia zamawianych systemów nadzoru bezpieczeństwa:

a. Biuro Zamawiającego (definiowane jako strefa bezpieczeństwa przeznaczona głównie dla personelu nieposiadającego wiedzy technicznej na poziomie eksperckim):

i. do 120 stacji roboczych opartych głównie o systemy operacyjne z rodziny MS Windows, ale także Linux oraz MacOS,
ii. 1 klaster HA (dwie sztuki) urządzeń bezpieczeństwa sieci, z zastosowaniem podziału na wirtualne konteksty, działający jako UTM o głębokiej inspekcji,
iii. 2 klastry HA (po dwie sztuki każdy) urządzeń bezpieczeństwa sieci USG z zastosowaniem podziału na wirtualne konteksty, działające jako UTM,
iv. 1 stos przełączników sieciowych (dwie sztuki), warstwy 3 siedmiowarstwowego modelu ISO/OSI, działających przy wykorzystaniu dynamicznych protokołów routingu,
v. 30 szt. przełączników sieciowych warstwy 2 siedmiowarstwowego modelu ISO/OSI,
vi. System sieci bezprzewodowej, złożony z dedykowanego kontrolera centralnego, serwera autentykacji, oraz 8 systemowych punktów bezprzewodowych, posiadający osobne dedykowane urządzenie bezpieczeństwa na potrzeby sieci gości,
vii. System sieci bezprzewodowej, złożony z dedykowanego kontrolera centralnego, korzystający z zewnętrznego serwera autentykacji, posiadający 38 punktów dostępowych z których jeden zlokalizowano bezpośrednio w przestrzeni Biura SSM,
viii. do 30 systemów informatycznych, opartych o systemy operacyjne z rodzin MS Windows Server oraz Linux, wykorzystywanych na potrzeby wewnętrzne Zamawiającego, przykładowo:

- centralne serwery uwierzytelniania,
- system elektronicznego obiegu dokumentów,
- baza wiedzy,
- centralnie zarządzanie oprogramowaniem antywirusowym.

b. Domena Techniczna Biura Zamawiającego (definiowana jako strefa bezpieczeństwa przeznaczona dla personelu posiadającego wiedzę techniczną na poziomie eksperckim, odseparowana funkcjonalnie jako osobny wirtualny kontekst bezpieczeństwa):

i. 2 komplety zestawów ściany wizyjnej, na potrzeby istniejących systemów nadzoru i operacji sieciowych (ang. NOC - Network Operations Center),
ii. 6 dedykowanych serwerów fizycznych działających pod kontrolą hipernadzorcy marki WMWare ESXi, wraz z dedykowaną macierzą dyskową,
iii. 32 wirtualne serwery działające w oparciu o systemy operacyjne rodziny Linux,
iv. 2 serwery wirtualne działające w oparciu o systemy operacyjne rodziny Windows, (w tym serwery centralnej autentykacji na potrzeby personelu technicznego SSM)
v. 4 routery wirtualne,
vi. 2 systemy akwizycji informacji o całości połączeń północ-południe wykonywanych przez infrastrukturę sieciową, znajdująca się pod bezpośrednią opieką SSM, zgodnie z wymogami art. 180a Ustawy Prawo

Telekomunikacyjne, w tym jeden wyposażony a system detekcji anomalii (ang. ADS – Anomaly Detection System), stanowiący rudymentalna wersję NDR (ang. Network Detection and Response), Ilość zdarzeń, pochodzących z urządzeń sieciowych i dedykowanych systemów nadzoru, wymienionej powyżej strefy Biura SSM oraz Domeny Technicznej Biura SSM, szacować należy na poziomie 1000 MPS (komunikatów na sekundę).

6. **ETAP 2** - zakłada się objęcie aktywnością SOC obszaru Centrum Przetwarzania Danych Zamawiającego (chmura prywatna) w zakresie:

a. 2 środowiska wirtualizacyjne VMWare ESXi składające się z 26 serwerów fizycznych, w oparciu o które działa do 150 maszyn wirtualnych,
b. do 75 systemów operacyjnych z rodziny MS Windows Server,
c. do 75 systemów operacyjnych z rodziny Linux,
d. 2 klastry HA (po dwie sztuki każdy) urządzeń bezpieczeństwa sieci USG z zastosowaniem podziału na wirtualne konteksty działające jako North-facing UTM (duża liczba zdarzeń w związku z szeroką ekspozycją w kierunku publicznych zasobów sieci internet),
e. 8 sztuk przełączników, działających w oparciu o system Commware, połączonych w cztery redundantne stosy,
f. 3 sztuki central telefonicznych VoIP (ang. Voice over IP), połączonych w jeden redundantny system wysokiej dostępności, zbudowanych na bazie standardowych serwerów i stanowiących zamknięte rozwiązanie Producenta,
g. 2 sztuki przełączników innego dostawcy niż w ppkt.e, połączonych w stos redundantny,
h. 2 sztuki urządzeń bezpieczeństwa sieci, połączonych w klaster wysokiej dostępności,
i. 1 przełącznik rdzeniowy,

7. **ETAP 3** - zakłada się objęcie aktywnością SOC infrastruktury teleinformatycznej Miejskich Jednostek Organizacyjnych Miasta Gliwice (do 80 MJO) w zakresie:

a. do 100 urządzeń bezpieczeństwa sieci, zlokalizowanych na terenie Miejskich Jednostek Organizacyjnych, pełniących rolę UTM, routerów brzegowych oraz koncentratorów połączeń zdalnego dostępu pracowniczego, na potrzeby konkretnej Miejskiej Jendnostki Organizacyjnej,
b. do 1100 urządzeń sieciowych, z czego większość stanowią zarządzalne przełączniki sieciowe warstwy 2 siedmiowarstwowego modelu ISO/OSI.
c. do 400 punktów dostępowych sieci bezprzewodowej, rozlokowanych na ternie MJO, z czego część pod kontrolą centralnego systemu zarządzania a część kontrolowane lokalnie, w ramach danej Miejskiej Jednostki Organizacyjnej,
d. do 1900 stacji roboczych opartych głównie o systemy operacyjne z rodziny MS Windows, z czego 70% stanowią systemy Windows 10 Pro, a pozostałe to Windows 11 Pro i inne (np. MacOS),
e. do 50 maszyn wirtualnych opartych o systemy operacyjne MS Windows Server.

Przyjąć należy, szacunkowo, iż ilość zdarzeń pochodzących z każdej z wymienionych powyżej Miejskich Jednostek Organizacyjnych to, średnio, 500 MPS (komunikatów na sekundę) per Jednostka, przy czym osobnym szacunkiem objąć należy wiadomości

pochodzące z centralnych kontrolerów domeny Active Directory, obejmującej wszystkie MJO, uwzględniając fakt, iż zamawiający szacuje liczbę kont użytkowników Active Directory na 2900 pracowników.

8. Dostarczone oprogramowanie musi posiadać możliwość współpracy/integracji z systemem NDR, lub bezpośredniej analizy informacji netflow, przy czym obecny wolumen ruchu wschód-zachód szacować należy jako 700 TB rocznie dla infrastruktury własnej SSM, 400 TB rocznie dla najistotniejszych usług Centrum Przetwarzania Danych na użytek MJO, oraz 500 TB rocznie, średnio, dla każdej z Miejskich Jednostek Organizacyjnych.

9. Wypis podstawowych wymogów funkcjonalno - użytkowych dla dostarczanego systemu klasy SIEM

1.) Rozwiązanie SIEM (ang. Security Information and Event Management) musi zapewniać skalowalną architekturę spełniającą następujące wymagania:

a.) wszystkie elementy składowe wdrożonego rozwiązania mogą być dostarczone jedynie w postaci rozwiązań wirtualnych, opartych na jednej platformie wirtualizacji lub platform sprzętowych pochodzących od tego samego producenta (wymaga się zachowania zasady jednolitości technologicznej rozwiązania),

b.) zasoby odpowiedzialne za akwizycję informacji muszą mieć możliwość buforowania otrzymanych danych. Wszystkie buforowane informacje muszą zostać przetworzone przez system SIEM. Nie dopuszcza się automatycznego odrzucania danych bez ich przetworzenia, o ile czynność takowa nie wynika ze świadomej decyzji podjętej przez analityka obsługującego system,

c.) system SIEM powinien powiadamiać użytkowników o opóźnieniu w przetwarzaniu danych wynikającym z obciążenia bufora i wysycenia licencji w przypadku wykorzystania w systemie SIEM modelu licencyjnego mogącego powodować takie opóźnienia.
W przypadku wystąpienia cytowanych opóźnień, istnieć powinna możliwość awaryjnego przywrócenia funkcjonowania systemu w czasie rzeczywistym, poprzez przetworzenie kolejki danych w trybie wyjątku typu burst (chwilowe zwiększenie zasobów licencyjnych i/lub sprzętowych, związanych z przetwarzaniem danych), lub poprzez selektywne odrzucenie informacji najmniej istotnych na bazie reguł filtracji wyznaczonych przez analityka bezpieczeństwa, obsługującego system,

d.) komunikacja pomiędzy modułami wchodzącymi w skład systemu SIEM, musi odbywać się z wykorzystaniem bezpiecznych, szyfrowanych metod komunikacji, gwarantujących poufność informacji.

e.) system SIEM powinien posiadać możliwość zarządzania aktualizacjami swoich składników w sposób scentralizowany, za pomocą jednego wspólnego panelu. Składniki systemu SIEM powinny posiadać możliwość aktualizacji online, to znaczy proces aktualizacji komponentów nie może mieć istotnego wpływu na zachowanie bezprzerwowej ciągłości działania systemu, w szczególności pod kątem akwizycji informacji źródłowych. Wymóg powyższy pozostaje w mocy także w przypadku konieczności dokonania aktualizacji systemów operacyjnych stanowiących podstawę dla funkcjonowania komponentów systemu.

2.) Warstwa przechowywania i korelacji danych musi spełniać następujące wymagania minimalne:

a.) implementacja zrealizowana w oparciu o rozwiązania wirtualne lub platformy sprzętowe pochodzące od tego samego producenta, w celu zachowania jednolitości technologicznej systemu, przy czym wszystkie komponenty i licencje

niezbędne w celu prawidłowego uruchomienia i wdrożenia w pełni sprawnego i funkcjonalnego systemu dostarczone być muszą przez Wykonawcę i Integratora w ramach tego samego zlecenia
i objęte wspólną gwarancją oraz wsparciem Wykonawcy lub producenta rozwiązania. Jedynym wyjątkiem od cytowanej reguły są przypadki w których do realizacji zadania wykorzystano, częściowo, infrastrukturę i licencje znajdujące się uprzednio w posiadaniu Zamawiającego,
b.) przedmiotowe rozwiązanie musi wspierać co najmniej poniżej wymienione środowiska wirtualizacji: VMWare, Hyper-V, KVM, Proxmox,
c.) system SIEM musi mieć możliwość skalowania wertykalnego oraz horyzontalnego poprzez dodawanie kolejnych analogicznych modułów lub rozbudowę podzespołów maszyn wirtualnych. W przypadku środowiska wirtualnego, zwiększenie parametrów maszyn lub dodanie nowych modułów środowiska wirtualizacji, nie może wpływać na koszty licencji produktu,
d.) system SIEM musi być wolny od wszelkich ograniczeń licencyjnych dotyczących liczby lub wielkości zdarzeń i danych, które przechowuje. Jedyną dopuszczalną barierą w kontekście przechowywanych danych może być pojemność dysku twardego.
e.) system SIEM powinien umożliwiać wskazanie minimalnego i maksymalnego okresu retencji pozyskanych informacji, przy czym wskazanie okresu minimalnego wiązać musi się z gwarancją braku utraty informacji przed jego upływem, wskazanie okresu maksymalnego musi natomiast gwarantować usunięcie danych po jego upływie w sposób skuteczny i bezpieczny,
f.) system SIEM powinien umożliwiać archiwizację danych i zarządzanie konfiguracją archiwizacji danych. W szczególności system powinien posiadać możliwość konfiguracji automatycznej archiwizacji danych po określonym czasie lub na podstawie kryteriów związanych z dostępnością przestrzeni dyskowej. Dopuszczalne jest by dane poddane archiwizacji dostępne były z mniejszą wydajnością jednak mechanizm dostępu nie może być uciążliwy dla użytkownika końcowego,
g.) system SIEM powinien posiadać możliwość wsparcia Zamawiającego w zarządzaniu zgodnością na podstawie regulacji prawnych co najmniej w zakresie GDPR (RODO), NIS2 (KSC), ISO 27001,
h.) zebrane dane muszą być przechowywane w sposób mający na uwadze optymalizację wykorzystania przestrzeni dyskowej. Zaleca się zastosowanie kompresji i/lub normalizacji danych do formy binarnej,
i.) system SIEM musi mieć możliwość anonimizacji zebranych danych, na bazie reguł określonych przez obsługującego go analityka, w szczególności pod kątem wszystkich informacji eksportowanych poza obręb systemu, w tym raportów stanowiących podstawę lub załącznik na potrzeby dalszych postępowań formalno-prawnych.

3.) Rozwiązanie SIEM musi mieć możliwość zbierania danych z monitorowanych urządzeń, również w formatach innych niż standardowe logi typu syslog/cef. Zamawiający wymaga co najmniej możliwości pozyskania logów typu Tomcat Catalina, oraz dzienników zdarzeń natywnych dla systemów operacyjnych rodzin Ms Windows oraz linux, w tym binarnych logów systemowych dziennika systemd. Powyższa funkcjonalność może być realizowana przez dedykowanego agenta systemu SIEM, instalowanego w ramach obserwowanego systemu. Powinna istnieć możliwość ręcznego importu wiadomości wyeksportowanych w formie zserializowanych plików statycznych.

4.) Wymaga się, aby system SIEM umożliwiał eliminację danych uznanych za nieistotne lub zbędne przez obsługujących go analityków bezpieczeństwa.

5.) Przedmiotowe rozwiązanie musi umożliwiać samodzielną modyfikację i duplikację istniejących, predefiniowanych parserów, tworzenie własnych parserów, oraz normalizację pozyskiwanych informacji za pomocą reguł tworzonych przez użytkownika końcowego. Tworzenie własnych parserów musi być możliwe w całości zarówno z wykorzystaniem interfejsu graficznego, jak i poleceń typowych dla języków skryptów i/lub wyrażeń regularnych.

6.) Tworzenie nowych atrybutów (sparsowanych zmiennych), urządzeń oraz rodzajów zdarzeń (events) musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) jak i poleceń typowych dla języków skryptów i/lub wyrażeń regularnych. Dodawanie wyżej wymienionych elementów nie może wpływać negatywnie na kompatybilność z dotychczas zapisanymi danymi.

7.) System SIEM musi być w stanie obsłużyć wolumen zdarzeń generowanych przez urządzenia w infrastrukturze Zamawiającego z uwzględnieniem typowych zmian (przyrostów i spadków) w wolumenie generowanych zdarzeń wynikających np. z pory dnia, dnia tygodnia, okresu roku. Zamawiający zaznacza jednocześnie, iż w związku z charakterem pracy Administracji Publicznej, oraz podległych jej Jednostek Oświatowych przewiduje piki danych występujące w związku z synchronizacją zachowań pracowników Administracji Publicznej w chwili rozpoczęcia godzin urzędowych dnia roboczego, rozpoczęcia semestru szkolnego, oraz powrotu do pracy kończącego święta państwowe. Jednocześnie przewiduje się zauważalny spadek ilości generowanych zdarzeń w godzinach nocnych i w trakcie przerwy weekendowej.

8.) Rozwiązanie SIEM musi mieć możliwość zbierania zdarzeń (event) z systemów Windows oraz Linux w oparciu aplikacje typu agent lub bez ich użycia z wykorzystaniem rozwiązań natywnych dla danego systemu np. Windows Event Log, WMI, Syslog.

9.) Aplikacja typu agent wdrożonego rozwiązania, w wersji przeznaczonej dla systemów rodziny Ms Windows, (Windows Agent) musi posiadać możliwości zbierania danych nie mniejsze od istniejących w przypadku obserwacji systemu bez wykorzystania aplikacji typu agent, przy czym wymaga się by komunikacja pomiędzy procesem agenta i centralną częścią systemu odbywała się w sposób bezpieczny, gwarantujący poufność przesyłanych informacji.

10.) Aplikacja typu agent wdrożonego rozwiązania, w wersji przeznaczonej dla systemów rodziny Linux (Linux Agent) , musi posiadać możliwości zbierania danych nie mniejsze od istniejących w przypadku obserwacji systemu bez wykorzystania aplikacji typu agent, przy czym wymaga się dodatkowo możliwości akwizycji logów binarnych dziennika systemd, oraz zagwarantowania by komunikacja pomiędzy procesem agenta i centralną częścią systemu odbywała się w sposób bezpieczny, zapewniających poufność przesyłanych informacji.

11.) System musi posiadać bazę gotowych reguł korelacyjnych predefiniowanych przez producenta i utworzonych z myślą o typowym środowisku średniej wielkości centrum przetwarzania danych, oraz środowisku Operatora Telekomunikacyjnego świadczącego usługi ISP (ang. Internet Service Provider).

12.) Aktualizacja reguł korelacyjnych przygotowywanych przez producenta musi być wykonywana gotowym i wygodnym mechanizmem, przy wykorzystaniu interfejsu graficznego.

13.) System SIEM musi zapewniać wsparcie dla zarządzania w oparciu o role (Role Based Administration) celem ograniczania dostępu do danych oraz do GUI wyłącznie do zakresu niezbędnego na danym stanowisku pracy (w szczególności: separacji roli administratora systemu i analityka bezpieczeństwa).

14.) Dostarczone rozwiązania powinieno być w stanie wygenerować raporty w oparciu o strukturę systemów wykorzystujących technologię LDAP np. Active Directory.

15.) System SIEM musi posiadać integrację z zewnętrznymi bazami informacji o zagrożeniach (Threat Inteligence Feeds - TI). Musi istnieć możliwość pozyskania informacji z baz nie znajdujących się pod bezpośrednią, wyłączną kontrolą producenta rozwiązania, za pomocą powszechnie stosowanych protokołów.

16.) Przedmiotowe rozwiązanie musi pozwolić na integrację z systemami uzupełniającymi, obecnie użytkowanymi przez Zamawiającego, co najmniej w zakresie pozyskania generowanych przez nie zdarzeń, przy czym do systemów tych należą: AD Audit+, ESET Inspect XDR/EDR, Progress (dawniej Flowmon) ADS (Anomaly Detection System). Za dodatkowy atut systemu Zamawiający uzna integrację z rozwiązaniem ESET Inspect EDR na poziomie pozwalającym na monitorowanie ruchu sieciowego wschód-zachód, oraz północ-południe, oraz ocenę wolumenu ruchu sieciowego w kontekście analizy behawioralnej obserwowanej stacji końcowej, lub wdrożenie równoważnej funkcjonalnie możliwości za pomocą agenta systemu SIEM w sposób nie powodujący konfliktu z agentem systemu marki ESET.

17.) Zamawiający dysponuje oprogramowaniem antywirusowym, wykorzystującym konsole zarządzania ESET Remote Administration. System SIEM powinien posiadać możliwość wykorzystania danych pochodzących z systemu ESET Remo te Administration przy użyciu dostępnych mechanizmów eksportu danych w szczególności poprzez Syslog, LEEF, JSON oraz mechanizmy API.

18.) Zamawiający wymaga kategorycznie, by dostarczone rozwiązanie posiadało możliwość akwizycji, parsowania i normalizacji wiadomości syslog pochodzących z przełączników sieciowych marki Huawei Secospace, HPE serii pod kontrolą systemu Commware, Zyxel, Netgear, D-Link, TP-Link, DCN, Cisco, urządzeń bezpieczeństwa sieci marki Huawei USG, Fortinet Fortigate, MikroTik, Checkpoint. Zamawiający informuje jednocześnie, iż większość jego infrastruktury teletechnicznej oparto na rozwiązaniach marki Huawei, co oznacza, iż prawidłowa i bezproblemowa obsługa urządzeń tej marki jest zagadnieniem kategorycznie istotnym.

19.) Dane prezentowane przez system muszą pozwalać na wykorzystanie popularnych form prezentacji danych takich jak tabela, wykresy, elementy korelujące dane, liczniki, mapy, wyświetlacze wartości.

20.) W ramach powiadamiania (notyfikacji) oraz zarządzanie incydentami, system SIEM musi:

a.) posiadać narzędzia pozwalające na samodzielne tworzenie polityk informujących o wykrytych, potencjalnych incydentach,

b.) posiadać możliwość tworzenia wpisów zawierających historię obsługi incydentu/alarmu od momentu wystąpienia incydentu/alarmu do czasu

zakończenia jego obsługi. Takie wpisy powinny być przechowywane przez okres czasu wskazany przez Zamawiającego. Musi istnieć możliwość zmiany okresu czasu przez który zdarzenia są przechowywane (zabezpieczenia materiału powiązanego z incydentem na potrzeby przyszłego postępowania, poza zakres czasu zwykłej retencji danych).

21.) W ramach funkcjonalności związanej z pracą analityka bezpieczeństwa, system SIEM musi mieć możliwość:

a.) wyszukiwania zdarzeń (events) w trybie bieżącym oraz historycznym,

b.) wyszukiwania w oparciu o słowa kluczowe oraz w oparciu o sparsowane atrybuty zdarzeń względem analizowanych danych,

c.) wyszukiwania historycznego z zastosowaniem kwerend zagnieżdżonych, ze wsparciem dla filtrowania typu Boolean, grupowaniem w oparciu o agregację danych, filtry czasowe, wyrażenia regularne, wyrażenia matematyczne,

d.) wyszukiwania w oparciu o nie mniej niż następujące operatory: include =,!=, <,>, IS NULL, IS NOT NULL, contains, not contains, contains regex, not contains regex,

e.) tworzenia harmonogramu raportów i dostarczania ich pocztą elektroniczną,

f.) eksportowania raportów do formatów CSV (w przypadku danych podlegających serializacji), PDF,

g.) wyszukiwania zdarzeń i generowanie raportów dla całej organizacji lub w ujęciu fizycznego lub logicznego obszaru infrastruktury Zamawiającego,

h.) automatycznego korelowania użytkownika z jego lokalizacją i adresem IP, oraz łączenia różnych kont takich jak login w Active Directory, adres e-mail, nazwa konta w usługach chmurowych dla jednego użytkownika w ramach funkcji tzw. Aliasu,

i.) system powinien zapewniać moduł raportowania pozwalający na tworzenie czytelnych raportów dotyczących gromadzonych logów, generowanych zdarzeń, alarmów, użycie w raportach manualnie wskazanego zakresu danych źródłowych pochodzących z odseparowanego logicznie lub fizycznie obszaru infrastruktury Zamawiającego i czasookresu (w tym obejmującego dane archiwalne), oraz użycie gotowych schematów raportów pozwalających na przedstawienie informacji z wbudowanych zdarzeń i alarmów.

10. Producent oferowanego systemu musi utrzymywać publicznie dostępną dokumentację techniczną, dotyczącą jego obsługi. Ponadto, jeżeli producent utrzymuje dokumentację dostępną niepublicznie, Zamawiający powinien posiadać dostęp do niej w zakresie obejmującym dostarczone produkty oraz technologie, przez cały okres wsparcia systemu.

11. Przedmiotowy system musi pozwalać na przyszłą, skuteczną integrację z przynajmniej jednym rozwiązaniem typu SOAR, które umożliwiać musi co najmniej:

a.) uruchamianie procedur wykonawczych SOAR (tzw. Playbook) z poziomu SIEM, także warunkowo na podstawie predefiniowanych reguł korelacyjnych,

b.) wykonywanie operacji na systemach zintegrowanych z SOAR, np. pobranie listy zablokowanych adresów IP na firewall, dodanie do blokady adresu URL, zweryfikowanie reputacji IP w serwisie internetowym.

12. System SIEM musi mieć możliwość przyszłej, skutecznej integracji z przynajmniej jednym rozwiązaniem realizującym funkcjonalności UEBA (ang. User Entity Behaviour Analysis).

13. Dla wdrożonego systemu SIEM musi istnieć możliwość przeprowadzenia szkoleń certyfikowanych przez producenta dostarczonego rozwiązania, zakończonych wydaniem dokumentu, stanowiącego jednoznaczny i odtwarzalny dowód uzyskanych kompetencji. Wdrożenie systemu musi zawierać szkolenie kadry Zamawiającego z obsługi systemu zarówno pod kątem administrowania systemem jak i obsługi jego funkcjonalności. Szkolenia powinny odbywać się m.in. w formie „On-the-job training". Ukończenie szkolenia powinno zakończyć się możliwością uzyskania certyfikatu przez pracowników Zamawiającego. W ramach wdrożenia Zamawiający oczekuje przeszkolenia administratorów systemu i osób odpowiedzialnych za jego funkcjonalne wykorzystanie, w tym analityków bezpieczeństwa.

14. Zamawiający wymaga przedstawienia możliwych wariantów wsparcia dla wdrożonego systemu.

15. Zamawiający wymaga przedstawienia progów/przedziałów cenowych wynikających z ilości sprzętu/licencji/wolumenu dla poszczególnych Etapów.

16. System powinien mieć ciągły/stały dostęp do internetu, bardzo silnie ograniczony i musi istnieć możliwość podzielenia go na kolektory (które można umieścić w innej podsieci, całkowicie od internetu odseparowanej) zdolne do przechowania pozyskiwanych danych przez pewien czas, w razie chwilowej utraty komunikacji z głównym jego rdzeniem.

17. System powinien posiadać funkcjonalność umożliwiającą pozyskiwanie danych na potrzeby statystyki i określania wskaźników np.:

a. odsetek wyników fałszywie dodatnich,
b. średni czas analizy,
c. poziom gotowości,
d. średni czas do wykrycia,
e. ekspozycja na luki w zabezpieczeniach,
f. czas do wykrycia luki w zabezpieczeniach,
g. dotkliwość luki w zabezpieczeniach,
h. incydenty spowodowane znanymi i nieznanymi lukami w zabezpieczeniach,
i. czas badania alertu,
j. wskaźnik generowania alertów,
k. liczba alertów, które nie zostały przeanalizowane,
l. itp.

18. Dane ilościowe

Typ/funkcja systemu	Liczba – ETAP I	Liczba – ETAP II	Liczba – ETAP III	Uwagi / Informacje dodatkowe
Serwery Windows Active Directory	2	2	2	Maszyny wirtualne, 3 domeny
Maszyny pełniące funkcje serwerowe	6	26	-	Pod kontrolą 3 hipernadzorców VMWare ESXi
Serwery UNIX / Linux / Windows	60	70	50	Procentowy udział typów systemów operacyjnych: Windows 45% RHEL: 25% Debian 20% Other Linux: 15%
Stacje robocze Windows	120	-	2900	Windows 10 68% Windows 11 31% Pozostałe 1%
Serwery DNS	-	5	-	
Serwery Bazodanowe	3	-	7	Do 30 instancji baz danych
Konsole zarządzania systemem AV (Antivirus)	1	-	1	Minimum w zakresie ESET Endpoint Security
EDR/XDR	1	-	1	ESET Inspect Do 120 licencji w lipcu 2024 roku
Urządzenia bezpieczeństwa sieci	6	6	100	UTM'y następujących producentów: Fortinet Juniper Huawei Checkpoint Zyxel StormShield MikroTik PFSense
Urządzenia sieciowe	32	11	1100	Przełączniki sieciowe warstwy 2 i 3, głównie następujących producentów: Huawei HPE NetGear Zyxel MikroTik DCN Aruba

Elementy sieci bezprzewodowych	46	-	400	Rozwiązania systemowe następujących producentów: Ubiquiti MikroTik Aruba TP-Link
Istniejące systemy nadzoru	-	15	-	
Serwery na potrzeby oprogramowania Backup	-	5	-	Commvault

III. OPIS PRZYGOTOWANIA

1. Oferty szacunkowe składane są za pomocą formularza aktywnego na platformie zakupowej.
2. Oferty złożone po terminie nie będą rozpatrywane.

IV. DODATKOWE INFORMACJE

Dodatkowych informacji można uzyskać pod numerem telefonu +48 32 441 90 00.

Złożenie oferty szacunkowej nie stanowi zobowiązania po stronie pytającego ani nie stwarza jakichkolwiek roszczeń ze strony oferenta względem pytającego bądź jego następców prawnych.