DOLKOM

www.dolkom.pl
e-mail: dolkom@dolkom.pl

Dolnośląskie Przedsiębiorstwo Napraw Infrastruktury Komunikacyjnej DOLKOM spółka z ograniczoną odpowiedzialnością
50-502 Wrocław, ul. Hubska 6

PN-EN ISO 9001
ISOCERT CERTYFIKAT
ISO 45001
ISOCERT CERTYFIKAT

Prezes Zarządu Sekretariat : tel. (71) 717 5630 tel. (71) 717 5942 fax. (71) 717 5164	Członek Zarządu Dyrektor ds. Techniczno-Handlowych: tel. (71) 717 3419	Członek Zarządu Dyrektor ds. Ekonomiczno-Finansowych: tel. (71) 717 1124	DTI Tel. +48 799 074 103 t.gudowski@dolkom.pl

Wrocław, 04.09.2024.

Zapytanie ofertowe

Dolnośląskie Przedsiębiorstwo Napraw Infrastruktury Komunikacyjnej DOLKOM spółka z ograniczoną odpowiedzialnością, z siedzibą we Wrocławiu przy ul. Hubskiej 6, 50-502 Wrocław, prosi o złożenie oferty cenowej na zakup usługi SOC (Security Operations Center).

Opis przedmiotu zamówienia:

Przedmiotem niniejszego zamówienia jest zakup usługi Security Operations Center wg poniższej specyfikacji:

1) monitorowanie bezpieczeństwa w ramach SOC w trybie ciągłym: 24/7/365,
2) obsługa środowiska SIEM (Security Information and Event Management), zalecana jest znajomość środowiska używanego przez odbiorcę – w tym celu prosimy w ofercie wypisać obsługiwane dotychczas przez oferenta systemy SIEM/SOAR lub dostarczenie własnego środowiska SIEM na serwerach zlokalizowanych w Polsce (zaleca się prezentację rozwiązania w czasie do tygodnia od złożenia oferty w formie zdalnej lub wideoprezentacji)
3) obsługa minimum 500 EPS (event per second),
4) ilość źródeł: minimum 500, w tym serwery, urządzenia sieciowe oraz urządzenia końcowe,
5) realizowanie zadań w ramach opłaty abonamentowej 1 linii wsparcia SOC, a w szczególności:
   5.1) reagowanie na podejrzenia i obsługa zidentyfikowanych incydentów,
   5.2) analiza incydentów i ich klasyfikowanie,
   5.3) zarządzanie incydentami,
   5.4) raportowania incydentów – dzienny raport w tym szczegółowy raport z incydentów,
   5.5) opracowanie i obsługa minimum 10 scenariuszy,
   5.6) SLA o notyfikacji – do 60 min. od zidentyfikowania incydentu,
   5.7) minimalny gwarantowany poziom incydentu a czas reakcji:
      a) krytyczny – do 60 min,
      b) średni – do 120 min,
      c) niski – do 240 min,
      d) klasyfikacja (poziomy) incydentów uzgadniane będą w ramach wdrożenia i opracowywania scenariuszy monitorowania i reagowania,
   5.8) kanały komunikacji obejmujące notyfikację: e-mail i kontakt telefoniczny,
   5.9) raportowanie incydentów poważnych w rozumieniu ustawy o Krajowym Systemie Bezpieczeństwa (Dz.U. z 2018 r. poz. 1560) do wskazanego CSIRT do 24h,

5.10) skanowanie podatności,
6) składowanie logów i dostęp w ramach zasobów dostawcy usługi, zlokalizowane w Polsce. Okres przechowania – minimum 6 miesięcy (dotyczy rozwiązania zewnętrznego),
7) przedstawienie analizy przedwdrożeniowej i harmonogramu realizacji,
8) wdrożenie (dotyczy rozwiązania zewnętrznego),
9) uruchomienie i przekazanie systemu do eksploatacji (dotyczy rozwiązania zewnętrznego),
10) przekazanie dokumentacji powykonawczej (dotyczy rozwiązania zewnętrznego),
11) uruchomienie usługi – w czasie zadeklarowanym przez usługodawcę, maksymalnie do 60 dni od zawarcia umowy,
12) zapewnienie wsparcia grupy projektowej i dedykowanego kierownika projektu,
13) niezbędne licencje na uruchomienie systemu bezpieczeństwa.
14) Zadania realizowane w ramach 2 linii wsparcia SOC:
14.1) obsługa incydentów przekazanych z 1 linii w szczególności incydentów krytycznych,
14.2) zaawansowane wdrożenia,
14.3) troubleshooting,
14.4) strojenie systemów,
14.5) tworzenie reguł,
14.6) pisanie scenariuszy,
14.7) zaawansowanie skanowanie podatności,
14.8) kontakt z dostawcą - zgłaszanie znalezionych błędów i zakładania ticket'ów,
14.9) threat intelligence.
15) Zadania realizowane w ramach 3 linii wsparcia SOC:
15.1) analiza złożonych incydentów,
15.2) działania forensic,
15.3) analizy powłamaniowe,
15.4) analizy malware,
15.5) zaawansowane testy penetracyjne,
15.6) threat hunting,
15.7) pisanie polityk bezpieczeństwa.

Dodatkowe informacje:
Wszelkie dodatkowe informacje odnośnie ilości urządzeń końcowych, sieciowych, serwerów – zostaną udzielone telefonicznie.

Termin i miejsce składania ofert:

Oferty cenowe należy dostarczyć mailowo na adres t.gudowski@dolkom.pl lub o.falkowski@dolkom.pl do dnia 13.09.2024 do godziny 14:00.

Opis kryterium, którymi zamawiający będzie się kierował przy wyborze ofert:

Oferty zostaną ocenione przez Zamawiającego w oparciu o kryterium cenowe 25%, zgodność ze specyfikacją 50%, oraz termin uruchomienia usługi 25%.

Informacje o negocjacjach handlowych po złożeniu ofert:

Zamawiający po złożeniu ofert przeprowadzi dodatkowe negocjacje handlowe z Oferentami, którzy złożyli najkorzystniejsze oferty cenowe.

Płatność:

Płatność nastąpi w formie przelewu w ciągu 14 dni od uruchomienia usługi.

Sprawę prowadzi Dział Teleinformatyki

Kontakt:

Tomasz Gudowski, tel.: 799-074-103, e-mail: t.gudowski@dolkom.pl
lub
Oskar Falkowski, tel.: 697-047-616, e-mail: o.falkowski@dolkom.pl

Od poniedziałku do piątku w godz. 8:00 – 14:00.