**Opis przedmiotu zamówienia/ Formularz ofertowy**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| LP. | Przedmiot zamówienia | Jm. | ilość | Wartość całkowita zł brutto |
| 1 | **SUMURI RECON LAB** | szt. | 1 | do uzupełnienia |
| 2 | **IDA PRO ESSENTIAL** | szt. | 1 | do uzupełnienia |
| Łącznie | | | | do uzupełnienia |

**Zakup zestaw narzędzi do informatyki śledczej, który umożliwia zaawansowaną analizę obrazów dysków w systemie macOS- SUMURI RECON LAB – 1 szt.**

|  |  |
| --- | --- |
| **Właściwości** |  **Wspierane systemy operacyjne**:   * **macOS**: Oprogramowanie jest zoptymalizowane do pracy na komputerach Mac, w tym z procesorami Apple Silicon, co pozwala w pełni wykorzystać specyficzne funkcje i zasoby macOS. * **Kompatybilność z innymi systemami**: Obsługa analizy danych z systemów Windows, iOS, Android, Linux, Google Takeout, co czyni oprogramowanie wszechstronnym narzędziem do analizy danych pochodzących z różnych źródeł i platform.    **Funkcje oprogramowania**:   * **Zautomatyzowana analiza danych**:   + Oprogramowanie umożliwia automatyczną analizę tysięcy artefaktów z różnych systemów operacyjnych (Windows, macOS, iOS, Android, Google Takeout), co znacząco przyspiesza proces śledztwa i zmniejsza liczbę spraw do opracowania.   + Obsługuje pełną analizę rozszerzonych metadanych Apple, które mogą być pominięte przez inne narzędzia śledcze. Umożliwia to dokładniejsze badanie, kto, kiedy i jak korzystał z określonych plików, w tym odpowiedzi na pytania, takie jak kto wysłał plik, kiedy został pobrany, czy był otwierany przez użytkownika, itp. * **Trzystopniowe przetwarzanie**:   + **W pełni automatyczne**: Kompleksowe przetwarzanie danych bez potrzeby ręcznego nadzoru.   + **Półautomatyczne**: Umożliwia operatorowi interakcję na wybranych etapach analizy.   + **Manualne**: Umożliwia pełną kontrolę nad każdym aspektem analizy danych, pozwalając użytkownikowi na dogłębną analizę dowodów. * **Zaawansowane filtrowanie i sortowanie**:   + Możliwość tworzenia tysięcy kombinacji filtrów i sortowania danych według wyników automatycznych, metadanych oraz rozszerzonych metadanych Apple. Pozwala to na szybkie i precyzyjne znalezienie kluczowych informacji w dużych zbiorach danych. * **Raportowanie i edycja raportów**:   + **Story Board Mode**: Oprogramowanie oferuje zaawansowane narzędzie do raportowania, które pozwala na edycję zawartości raportów bezpośrednio w programie. Użytkownik może sortować zarejestrowane lub oznaczone dane w kolejności chronologicznej, co umożliwia przedstawienie "historii" od początku do końca w odpowiedniej sekwencji. * **Obsługa analizy pamięci RAM**:   + Umożliwia analizę pamięci RAM dla systemów Windows i macOS, co pozwala na odzyskiwanie haseł użytkowników Apple oraz identyfikację śladów działania złośliwego oprogramowania lub innych aktywności na komputerze. * **Obsługa wielu formatów danych**:   + Zintegrowane przeglądarki dla różnych typów danych, w tym SQLite, plist, tekst, ciągi znaków, EXIF, dane geolokalizacyjne, hex i inne. Oprogramowanie wspiera również wykonywanie zapytań SQL w celu przeprowadzania zaawansowanej analizy baz danych SQLite bezpośrednio w programie.    **Funkcje dodatkowe**:   * **Obsługa zdalnych systemów plików**:   + Głęboka analiza systemów plików na poziomie bajtów, co umożliwia odkrywanie ukrytych lub usuniętych danych. Oprogramowanie może analizować struktury plików systemowych, takie jak rejestry, pliki systemowe, dane aplikacji i dzienniki, w celu uzyskania pełnego obrazu aktywności użytkownika. * **Zaawansowane funkcje przetwarzania i raportowania**:   + Możliwość edycji raportów "na żywo" oraz w pełni zintegrowany edytor raportów, który pozwala na modyfikację każdego aspektu raportu, co pozwala dostosować dokumentację do specyficznych wymagań śledztwa. |
| **Dodatkowe informacje** | * **Wymagania sprzętowe**:   + Oprogramowanie wymaga komputera Mac z procesorem i7 Quad-Core i co najmniej 16 GB RAM, co umożliwia sprawne działanie nawet przy dużych zbiorach danych i zaawansowanej analizie. * **Aktualizacje i wsparcie techniczne**:   + Regularne aktualizacje oprogramowania oraz pełne wsparcie techniczne, co zapewnia, że narzędzie pozostaje na bieżąco z najnowszymi standardami w dziedzinie informatyki śledczej. * **Pełne wykorzystanie mocy komputerów Mac**:   + Oprogramowanie zostało stworzone specjalnie dla komputerów Mac, aby zapewnić bardziej efektywne przetwarzanie danych, szczególnie w przypadku analizy rozszerzonych metadanych Apple, co nie jest możliwe przy użyciu innych narzędzi śledczych. * **Unikalne narzędzie do analizy rozszerzonych metadanych Apple**:   Oprogramowanie oferuje wszechstronną obsługę i interpretację metadanych Apple, umożliwiając wykrywanie dowodów, które mogą zostać pominięte przez inne narzędzia śledcze. Dzięki temu pozwala na bardziej szczegółową analizę danych, zwłaszcza w kontekście urządzeń Apple, takich jak macOS i iOS. |
| **Szkolenie online** |  Szkolenie dla jednej osoby (5 dniowe). Szkolenie można zrealizować w terminie ustalonym przez organizatora szkolenia obejmuje wykonywanie czynności z zakresu informatyki śledczej od zabezpieczenie komputera z system macOS do wykonania szczegółowej analizy i raportowania.   Dostępne jest jako kurs online, prowadzony przez ekspertów producenta oprogramowania. Zapewnieniu uczestnikom dogłębnej wiedzy i praktycznych umiejętności, umożliwiających im przeprowadzenie analizy z wykorzystaniem systemu macOS. Zakres szkolenie obejmuje min.:  - Konfiguracja systemu macOS pod kątem informatyki śledczej  - Podstawy korzystanie z terminala systemu macOS  - Rozszerzone metadane systemu macOS  - wykonywania kopii nośników danych komputerów z system macOS  - Zbieranie danych ulotnych i nieulotnych z systemu macOS  Szkolenia powinny być realizowane online z instruktorem, w terminie wybranym przez Zamawiającego z listy dostępnych terminów wskazanych przez producenta oprogramowania do końca 2025 roku. |

1. Wymagania w zakresie licencji.

Zamawiający wymaga, aby oferowany przedmiot zamówienia objęty był:

* + licencja musi być nowa, nie może być używana albo odnawiana,   
    i nieaktywowana nigdy wcześniej na inny urządzeniu,
  + musi istnieć możliwość przenoszenia licencji między stanowiskami,
  + nie dopuszcza się oprogramowania do zastosowań domowych,
  + **licencja wieczysta /wsparcie techniczne na okres 3 lat**
  + licencja musi zostać zarejestrowana na dane Centralnego Biura Zwalczania Cyberprzestępczości – Zarząd we Wrocławiu
  + wersja instalacyjna oprogramowania musi być udostępniona na autoryzowanej stronie producenta oprogramowania,
  + w przypadku licencji elektronicznej, licencja musi zostać wysłana na adres [licencje@cbzc.policja.gov.pl](mailto:licencje@cbzc.policja.gov.pl),
  + aktywacja oprogramowania powinna umożliwiać aktywację na komputerach niepodłączonych do Internetu,
  1. Dostarczone urządzenia powinny być nowe, wolne od wad i zgodne z poziomem technologii istniejącym w momencie podpisania umowy.

………………………………………….

(podpis)

**ZAKUP OPROGRAMOWANIA DO INŻYNIERII WSTECZNEJ DLA CBZC ZARZĄD WE WROCŁAWIU- IDA PRO ESSENTIAL – 1 SZT.**

|  |  |
| --- | --- |
| **Właściwości** | * Wspierane procesory: Oprogramowanie musi wspierać 68 rodzin procesorów, z możliwością dodania własnych poprzez SDK/IDA Python. Obsługiwane architektury to m.in. x86, x64, ARM, ARM64, PPC, PPC64, MIPS, MIPS64, ARC. * Obsługa plików 64-bitowych: Oprogramowanie musi wspierać analizę plików 64-bitowych. * Wspierane systemy operacyjne: Windows 7, Windows 8, Windows 10, Windows 11. * Disassemblery: min. PC (x86 and x64), ARM (32-bit and 64-bit), MIPS (32-bit and 64-bit), PPC (PowerPC, 32-bit and 64-bit) * 2 dekompilatory z tej samej rodziny: PC (x86) 32-bit oraz PC (x64) 64-bit * Typ dekompilatora: tylko chmura * Debuggery: Oprogramowanie musi wspierać debugowanie lokalne i zdalne dla systemów Windows, Linux, macOS, iOS, XNU, Bochs, GDBServer, WinDbg, Intel PIN, oraz Android (Dalvik). * Formaty plików: Oprogramowanie musi obsługiwać analizę ponad 45 formatów plików, z możliwością dodania własnych za pomocą SDK i IDA Python. Obsługiwane formaty to m.in. PE, ELF, Mach-O. * Zastosowanie komercyjne: Oprogramowanie musi umożliwiać komercyjne wykorzystanie. * Skrypty Python: Oprogramowanie musi wspierać skrypty Python. * Interfejs tekstowy (Terminal UI): Oprogramowanie musi oferować interfejs tekstowy dla zaawansowanych użytkowników. * Dostęp do SDK C++ i narzędzi: Oprogramowanie musi zapewniać dostęp do SDK C++ oraz narzędzi deweloperskich. * Zapisywanie postępów analizy: Oprogramowanie musi umożliwiać zapisywanie wyników i postępów analizy. * Licencję przypisaną do komputera * Wsparcie techniczne: Oprogramowanie musi zapewniać wsparcie techniczne poprzez e-mail oraz forum użytkowników. |
| **Analiza** | * Zaawansowana analiza kodu złośliwego: Oprogramowanie musi być standardem w analizie kodu złośliwego, wykorzystywane przez analityków w celu wykrywania i badania nowych zagrożeń w postaci wirusów, spyware i malware, ze szczególnym wsparciem dla analiz na systemie Windows. * Wizualizacja przepływu sterowania: Narzędzie musi umożliwiać wizualizację przepływu sterowania, drzew wywołań oraz zależności w kodzie na platformie Windows. * Tworzenie raportów: Narzędzie musi umożliwiać tworzenie zaawansowanych raportów z możliwością swobodnego dopasowywania ich zawartości, kompatybilnych z systemem Windows. |

1. **Wymagania w zakresie licencji.**

Zamawiający wymaga, aby oferowany przedmiot zamówienia objęty był:

* + Typ licencji: Licencję przypisaną do komputera, z pełnym wsparciem dla instalacji na systemie Windows.
  + Nowa licencja: Licencja musi być nowa, nieużywana, i nigdy wcześniej nieaktywowana na innym urządzeniu.
  + Możliwość przenoszenia licencji między stanowiskami, z pełnym wsparciem dla systemu Windows.
  + Wykluczenie licencji domowych: Nie dopuszcza się oprogramowania do zastosowań domowych, musi być przystosowane do pracy w środowisku Windows w środowiskach profesjonalnych.
  + **Okres licencji: Czasowa (subskrypcja) na okres 12 miesięcy, począwszy od dnia dostawy (podpisania przez Zamawiającego protokołu odbioru).**
  + Rejestracja licencji: Licencja musi zostać zarejestrowana na dane Centralnego Biura Zwalczania Cyberprzestępczości – Zarząd we Wrocławiu.
  + Udostępnienie wersji instalacyjnej: Wersja instalacyjna oprogramowania musi być udostępniona na autoryzowanej stronie producenta oprogramowania, z pełnym wsparciem dla instalacji na systemie Windows.
  + Dostarczenie licencji elektronicznej: Licencja musi zostać wysłana na adres licencje@cbzc.policja.gov.pl.
  + Aktywacja offline: Aktywacja oprogramowania powinna umożliwiać aktywację na komputerach niepodłączonych do Internetu, w tym komputerach z systemem Windows.
  1. Dostarczone urządzenia powinny być nowe, wolne od wad i zgodne z poziomem technologii istniejącym w momencie podpisania umowy.

………………………………………….

(podpis)