**Załącznik nr 2.3 do PPU - Opis przedmiotu zamówienia dla części 3 postepowania**

**Zakup oprogramowania do pasywnej analizy ruchu sieciowego, które jest szeroko stosowane w dziedzinie informatyki śledczej i bezpieczeństwa sieciowego. Program umożliwia analizę przechwyconych pakietów sieciowych (PCAP) w celu wyodrębnienia i rekonstrukcji danych, takich jak pliki, obrazy oraz inne artefakty sieciowe – 2 szt.**

|  |  |
| --- | --- |
| Właściwości | * **Wspierane systemy operacyjne**:   + **Windows**: Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2008 R2, Windows Server 2012   + **Linux**: Wspierane poprzez użycie Mono * **Wspierane formaty plików**:   + **Pliki zrzutów sieciowych**: PCAP, PCAP-NG   + **Formaty dzienników**: CSV, JSON * **Funkcje związane z analizą sieci**:   + **Pasujący ruch sieciowy**: Analiza pasywna ruchu sieciowego bez wpływu na jego przepływ.   + **Rekonstrukcja sesji**: Odtwarzanie sesji HTTP, FTP, SMTP, POP3, IMAP, SMB.   + **Eksport artefaktów**: Wyodrębnianie plików, certyfikatów, obrazów, loginów, hasła i innych danych z ruchu sieciowego.   + **Identyfikacja urządzeń**: Rozpoznawanie urządzeń na podstawie ich sygnatur ruchu sieciowego.   + **Geolokalizacja IP**: Przypisywanie lokalizacji geograficznych do adresów IP.   + **Analiza danych DNS**: Odkrywanie domen, serwerów i relacji na podstawie danych DNS. * **Funkcje związane z bezpieczeństwem**:   + **Wykrywanie zagrożeń**: Identyfikacja znanych ataków i exploitów poprzez analizę ruchu.   + **Dekodowanie SSL/TLS**: Rozszyfrowanie zaszyfrowanych połączeń przy użyciu odpowiednich kluczy prywatnych.   + **Wykrywanie złośliwego oprogramowania**: Identyfikacja ruchu związanego z malware na podstawie sygnatur i podejrzanych zachowań. * **Obsługiwane protokoły**:   + **Protokóły warstwy aplikacji**: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, SMB, DNS   + **Protokóły warstwy transportowej**: TCP, UDP * **Integracja z innymi narzędziami**:   + **Możliwość eksportu danych**: CSV, JSON, PCAP   + **Wsparcie dla narzędzi zewnętrznych**: Integracja z narzędziami do analizy logów i SIEM poprzez eksport danych. * **Wspierane funkcje analityczne**:   + **Rekonstrukcja plików i sesji**: Możliwość odzyskiwania plików i sesji na podstawie przechwyconego ruchu sieciowego.   + **Analiza ruchu z urządzeń mobilnych**: Możliwość identyfikacji i analizy ruchu pochodzącego z urządzeń mobilnych.   + **Tworzenie raportów**: Automatyczne generowanie raportów zawierających kluczowe dane i wyniki analizy.   + **Monitorowanie w czasie rzeczywistym**: Pasywne monitorowanie sieci w czasie rzeczywistym. * **Dodatkowe moduły i funkcje**:   + **Analiza artefaktów z plików PCAP**: Automatyczne wydobywanie i analiza artefaktów z przechwyconych pakietów.   + **Wyszukiwanie danych na podstawie słów kluczowych**: Możliwość definiowania i wyszukiwania danych na podstawie słów kluczowych.   + **Obsługa wielodostępu**: Możliwość pracy z wieloma plikami zrzutów jednocześnie. |
| **Analiza** | * **Automatyczna wizualizacja**:   + Wizualizacja relacji pomiędzy artefaktami, plikami i urządzeniami przedstawiona na osi czasu. * **Analiza tekstu**:   + Wyszukiwanie treści o zabarwieniu zdefiniowanym przez użytkownika, np. erotycznym lub złośliwym. * **Raportowanie**:   + Szczegółowe podsumowanie analizy z możliwością eksportu do różnych formatów.   + Tworzenie szablonów raportów dostosowanych do potrzeb użytkownika. * **Optyczne rozpoznawanie znaków (OCR)**:   + Wyodrębnianie tekstu z plików PDF, zeskanowanych dokumentów, oraz obrazów dokumentów. * **Wykrywanie zagrożeń przy użyciu technologii uczenia maszynowego**:   + Użycie algorytmów do identyfikacji potencjalnych zagrożeń i korelacji danych. |

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 (subskrypcja) na okres 3 lat i rejestrowana indywidualnie do pracownika. Bezpłatne aktualizacje i wsparcie przez cały okres licencji.**
  + 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)