**Załącznik nr 2.7 do PPU - Opis przedmiotu zamówienia dla części 7 postepowania**

**Zakup oprogramowania do zbierania danych oraz analizy stacji końcowych lokalnych oraz zdalnych z system Microsoft Windows XP i nowszych  
w zakresie włamań związanych ze złośliwym oprogramowaniem, oprogramowaniem ransomware i innych incydentów komputerowych – 2 szt.**

|  |  |
| --- | --- |
| Zbieranie danych ze stacji końcowych | **Właściwości**  * **Wspierane systemy operacyjne: Windows XP i nowsze** * **Kolekcja danych w postaci:**   + Dane ulotne (w tym uruchomione procesy, otwarte porty, zalogowani użytkownicy, aktywne połączenia sieciowe i pamięć podręczna DNS)   + Mechanizmy utrwalania złośliwego oprogramowania, w tym elementy startowe i zaplanowane zadania   + Aktywność użytkownika, w tym uruchomione programy, aktywność w sieci i loginy   + Metadane ze wszystkich plików w systemie * Zbieranie danych niestabilnych i danych systemu plików * Zbieranie danych do i z USB * Zbieranie danych przez sieć * Zbieranie danych do kontenera S3 * Importowanie obrazów dysków * Importowanie danych wyjściowych KAPE * Importowanie plików logicznych * Importowanie obrazów pamięci (używa Volatility 2) * Kolejkowanie wielu kolekcji opartych na plikach |
| **Analiza** | * Analiza heurystyczna do identyfikacji podejrzanych plików * Wykrywanie złośliwego oprogramowanie za pomocą ReversingLabs * Skanowanie złośliwego oprogramowanie na bazie min. 40 silnków * Limit skanowania złośliwego oprogramowania min. 4000/dzień * Analiza za pomocą reguł Yara * Automatyczna punktacja artefaktów * Kolejkowanie i analiza wielu hostów w tym samym czasie   **Raportowanie**:   * **Generowanie raportów HTML, Excel i CybOX, JSON**   **Szkolenie:**   * **Roczna dostęp do portalu szkoleniowego producenta oprogramowania obejmujący kwartalne zestawy danych szkoleniowych.** |

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 musi być czasowa** **(subskrypcja) na okres 36 miesięcy począwszy od dnia dostawy**
  + 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.