Załącznik nr 1c do SWZ

**Opis przedmiotu zamówienia na część nr 3**

**Opis funkcjonalności oprogramowania** **SIEM oferowanego**

**przez Wykonawcę**

…………………………….…………………………………………..

(producent, pełna nazwa oprogramowania oferowanego przez Wykonawcę)

|  |  |  |
| --- | --- | --- |
| **Opis funkcjonalności oprogramowania SIEM wymaganej przez Zamawiającego** | | |
|  | **TAK\*** | **NIE** |
| \*należy potwierdzić spełnianie funkcji poprzez wpisanie „TAK” lub „NIE” w przypadku niespełniania funkcji) | |
| Rozwiązanie musi być system klasy SIEM / SOAR w chmurze producenta z miejscem  przechowywania logów na terenie UE |  |  |
| Logowanie do instancji chmurowej rozwiązania, powinno umożliwiać wykorzystanie 2FA |  |  |
| Rozwiązanie musi umożliwiać przesyłania nieograniczonej ilości oraz wielkości logów, bez wpływu na konieczną do wykupienia licencję |  |  |
| Rozwiązanie musi posiadać katalog minimum 140 gotowych integracji (przygotowane parsery) zdarzeń ze źródeł takich jak systemy, aplikacje i urządzenia bezpieczeństwa, ale także posiadać możliwość integracji źródeł z wykorzystaniem narzędzi wbudowanych do tworzenia paserów |  |  |
| Rozwiązanie musi umożliwiać generowanie powiadomień o braku otrzymywania logów per pojedyncze źródło oraz zdefiniowany czas niedostępności logów |  |  |
| Rozwiązanie musi posiadać możliwość dzielenia instancji głównej na pod instancje dla których mogą być zaimplementowane inne źródła logów oraz inne reguły bezpieczeństwa wyzwalające alerty w konsoli |  |  |
| Rozwiązanie musi udostępniać możliwość instalacji przekaźnika logów instalowanego lokalnie na systemie Linux Debian i musi być to już gotowy kontener dostarczony przez producenta. |  |  |
| Rozwiązanie musi posiadać możliwość implementacji agenta na systemy Linux oraz Windows który bezpośrednio będzie komunikował się z instancja chmurową oraz będzie monitorował system na którym zostanie zainstalowany. Agent musi być dostępny w ramach licencji podstawowej. |  |  |
| Systemy na których musi być możliwość instalacji agenta:  • Windows 8  • Windows 10  • Windows 11  • Windows Server 2016  • Windows Server 2019  • Windows Server 2022  • Ubuntu 14.04 i nowszy  • Debian 8 i nowszy  • CentOS 7 i nowszy  • Redhat 7 i nowszy |  |  |
| W ramach integracji Agenta na systemie operacyjnym, minimum poniższe źródła danych oraz zdarzenia powinny być dostępne:  • Access tokens  • Authentication logs  • DLL monitoring  • File monitoring  • Host network interface  • Loaded DLLs  • PowerShell logs  • Process command-line parameters  • Process monitoring  • Process use of network  • Windows event logs  • Windows Registry  • WMI Objects |  |  |
| Rozwiązanie powinno mieć możliwość napisania własnych reguł na podstawie wzorca STIX lub SIGMA, wzorzec powinien być oparty na formacie wartość. Rozwiązanie powinno także umożliwiać budowania reguł na podstawie zasilania informacjami CTI oraz na bazie anomalii |  |  |
| Rozwiązanie musi posiadać listę minimum 830 gotowych reguł bezpieczeństwa dostarczane przez producenta. |  |  |
| Katalog gotowych reguł musi być ciągle rozbudowywany przez producenta |  |  |
| Rozwiązanie musi umożliwiać automatyczne powiadomienie o pojawieniu się nowej reguły przygotowanej przez producenta |  |  |
| mplementacja nowych reguł bezpieczeństwa dostarczona przez producenta musi być możliwa w dwóch trybach :  • W trybie automatycznym , gdzie nowa reguła jest automatycznie włączana do zestawu aktywnych reguł w momencie jej pojawienia się.  • W trybie manualnym w którym administrator decyduje o jej włączeniu. |  |  |
| Rozwiązanie musi umożliwiać podział reguł na co najmniej 4 poziomy ze względu na ryzyko generowania przez nie fałszywych alarmów. |  |  |
| Uruchomione reguły muszą być wizualizowane w rozwiązaniu na bazie matrycy MITRE ATT&CK i pokrycia przez nie poszczególnych punktów w tej matrycy |  |  |
| Rozwiązanie powinno umożliwiać wykorzystanie wskaźników naruszenia bezpieczeństwa (IoC) dostarczone przez producenta rozwiązania. |  |  |
| Rozwiązanie w karcie Alertu powinno wskazywać takie informacje jak :  • Typ alertu,  • Instancja której dotyczy alert,  • Ważność alertu obliczane na bazie wagi (severity) reguły oraz krytyczności zasobu  którego dotyka alert  • Typu detekcji (np. SIGMA)  • Inormacje jakiego zasobu dotknął atak  • Fazy ataku (w ramach Cyber Kill Chain)  • Treść wzorca reguły który wyzwolił alarm |  |  |
| Rozwiązanie w panelu analityka musi umożliwiać podgląd listy zasobów (Assets) wykrywanych automatycznie przez system dzięki analizie zdarzeń oraz mapę ciepła aktywności zasobów na osi czasu. |  |  |
| Lista zasobów powinna zawierać minimum takie informacje jak:  • Nazwa  • Typ zasobu  • Ilośc zdarzeń dotyczących danego zasobu  • Ilośc alertów dotyczących danego zasobu  • Poziom Krytyczności zasobu |  |  |
| Karta zasobu (Asset) powinna umożliwiać:  • Wpisanie Tagu dla zasobu  • Opisanie instancji do którego należy zasób  • Manualne określenie krytyczności zasobu  • W przypadku użytkownika wpisanie maila  • W przypadku hosta wpisanie FQDN i dodatkowych adresów IP  • W przypadku hosta powinna umożliwić zmianę/opis typu systemu operacyjnego  • Dodanie własnego opisu kontekstowego, odnoszącego się do zasobu np. numer seryjny urządzenia itp |  |  |
| Rozwiązanie musi umożliwiać tworzenie playbooków w zakresie obsługi incydentów oraz delegowanie zadań do zdefiniowanych użytkowników |  |  |
| Rozwiązanie musi umożliwiać przekazywanie notyfikacji z wykorzystaniem webhooks do Slack i Teams |  |  |
| W ramach obsługi playbooków rozwiązanie powinno umożliwiać wewnątrz platformy stworzenie kont do systemów zewnętrznych z wykorzystaniem Api w celu wzbogacania informacji ułatwiających analitykę . Platformy które powinny być gotowe do integracji w rozwiązaniu to:  • Binary Edge  • Virus Total  • Glimps  • Censys  • Shodan  • RiskIQ  • Iknowwhatyoudownload |  |  |
| Rozwiązanie w ramach playbooków powinno umożliwiać komunikacje z wykorzystaniem Api do systemów zewnętrznych. |  |  |
| Rozwiązanie musi udostępniać modułu możliwy do instalacji w lokalnej infrastrukturze w celu wyzwalania zadań automatyzacji reagowania z poziomu sieci lokalnej w której znajdują się urządzenia, systemy docelowe. |  |  |

*(****podpis elektroniczny*** *osoby/osób upoważnionej do reprezentowania Wykonawcy)*