Załącznik Nr 2

Urządzenie klasy NDR – rozwiązanie do wykrywania i reagowania na różnego rodzaju ataki sieciowe i zagrożenia

Opis przedmiotu szacowania:

Minimalne parametry techniczne i funkcjonalne:

1. **Elementy systemu bezpieczeństwa**
   1) Wysokość maks. 1U do montażu w szafie rack(elementy mocujące w zestawie).
   2) Posiadać co najmniej dwa porty USB.
   3) Urządzenie musi posiadać dedykowany port do zarządzania.
   4) Urządzenie musi posiadać minimum interfejsów: 2x SFP+, 8x SFP, 8x GE.
   5) Musi obsługiwać co najmniej 1T przestrzeni dyskowej.
   6) Minimum 1 Gb/s przepustowości wykrywania naruszeń w dwukierunkowym ruchu HTTP z włączonymi wszystkimi funkcjami wykrywania zagrożeń.
   7) Proponowane rozwiązanie musi obsługiwać minimum 750 tys . jednoczesnych sesji.
   8) Proponowane rozwiązanie musi obsługiwać 32000 nowych sesji /s w ruchu HTTP.
2. **Usługi sieciowe**
   1) Musi obsługiwać pasywny tryb pracy (TAP), nie ingerując w sieć klienta.
   2) Rozwiązanie musi być w stanie zintegrować się z zaporami ogniowymi tej samej marki w celu ograniczenia zagrożeń.
   3) Musi posiadać możliwość rozwiązywania wiadomości przez protokół MPLS, VXLAN oraz QinQ i wykrywania zagrożeń w tych wiadomościach.
3. **Kontrola aplikacji**
   1) Rozwiązanie musi obsługiwać ponad 6000 aplikacji, musi obsługiwać filtrowanie aplikacji według nazwy, kategorii, podkategorii, technologii i ryzyka oraz wspierać komunikatory internetowe, p2p, pocztę e-mail, przesyłanie plików, gry online, strumieniowe przesyłanie multimediów itp.
   2) Rozwiązanie musi być w stanie zidentyfikować aplikacje mobilne typu iOS lub Android.
   3) Rozwiązanie musi być w stanie identyfikować aplikacje w chmurze, musi zapewniać wielowymiarowe monitorowanie i statystyki dla aplikacji w chmurze, w tym kategorię ryzyka i funkcje.
4. **Wykrywanie zagrożeń**
   1) Rozwiązanie musi obsługiwać co najmniej 16000 sygnatur IPS. Musi obsługiwać niestandardowe sygnatury, ręczne i automatyczne aktualizacje, wyodrębnianie sygnatur oraz wbudowaną encyklopedię zagrożeń.
   2) Rozwiązanie musi obsługiwać ochronę przed atakami SQL injection, XSS, buffer overflow zarówno dla IPv4 jak i IPv6.
   3) Rozwiązanie powinno obsługiwać ochronę przez atakami C&C z limitem żądań, limitem proxy, niestandardowym progiem, Musi obsługiwać wykrywanie co najmniej metod uwierzytelniania: JS Cookie, Redirect, Access confirm, CAPCHA
   4) Rozwiązanie musi obsługiwać wykrywanie anomalii protokołów HTTP, SMTP, IMAP, POP3, VOIP, NETBIOS itp.
   5) Niestandardowe reguły wykrywania włamań muszą obsługiwać konfigurowanie kierunku ruchu ataku w celu poprawy dokładności analizy źródła ataku.
   6) Rozwiązanie powinno umożliwiać tworzenie białych list dla modułu IPS.
   7) Rozwiązanie musi mieć wstępnie zdefiniowane profile IPS.
   8) Rozwiązanie musi mieć opcję przechwytywania pakietów.
   9) Rozwiązanie musi umieć wykrywać reverse-shell.
   10) Rozwiązanie musi potrafić zdefiniować odpowiednie treshholdy chroniące przed atakami Flood, bazując na parametrach dostarczonego ruchu.
   11) System musi mapować wykryte zagrożenia na framework MITRE ATT&CK.
5. **Skanowanie antywirusowe**
   1) Rozwiązanie musi obsługiwać co najmniej 13 milionów sygnatur antywirusowych z ręcznymi lub automatycznymi aktualizacjami sygnatur.
   2) Rozwiązanie musi wspierać antywirus oparty na przepływie dla protokołów min. HTTP, SMTP, POP3, IMAP, FTP/SFTP.
   3) Rozwiązanie powinno obsługiwać wykrywanie wirusów w skompresowanych plikach, takich jak RAR, ZIP, GZIP, BZIP2, TAR oraz wspierać wielowarstwowe wykrywanie skompresowanych plików dla nie mniej niż 5 warstw dekompresji i dostosowanie akcji po wykryciu zagrożenia w tych plikach.
   4) Rozwiązanie musi obsługiwać wykrywanie zaszyfrowanych skompresowanych plików.

6. **Wykrywanie botnetów C&C**
   1) Rozwiązanie powinno wspierać skuteczne wykrywanie botów intranetowych i zapobieganie dalszym atakom ze strony zaawansowanych zagrożeń poprzez porównywanie uzyskanych informacji z bazą adresów C&C.
   2) Rozwiązanie musi obsługiwać automatyczną aktualizację sygnatur botnetów C&C.
   3) Rozwiązanie musi obsługiwać dwa typy bazy adresów C&C: bazę adresów IP i bazę danych domen.
   4) Rozwiązanie musi obsługiwać wykrywanie C&C protokołów w protokołach TCP, HTTP i DNS.
   5) Rozwiązanie musi wspierać włączenie wykrywania DGA w celu analizy odpowiedzi DNS i wykrywania, czy urządzenie jest atakowane przez nazwę domeny DGA.
   6) Musi wspierać wykrywanie tunelowania w protokole DNS w tym analizowanie zapytań DNS, a także rejestrować logów zagrożeń wykrytych tuneli DNS.
7. **Sandbox w chmurze**
   1) Rozwiązanie musi obsługiwać oparte na chmurze wirtualne środowisko analizy złośliwego oprogramowania w celu znalezienia nieznanych zagrożeń.
   2) Rozwiązanie musi obsługiwać przesyłanie złośliwych plików do piaskownicy w chmurze w celu analizy.
   3) Rozwiązanie powinno obsługiwać przesyłanie złośliwych plików z protokołów, w tym HTTP/HTTPS, POP3, IMAP4, SMTP i FTP.
   4) Rozwiązanie musi obsługiwać typy plików, w tym PE, ZIP, RAR, Office, PDF, APK, JAR , SWF oraz skrypty.
   5) Rozwiązanie powinno dostarczać kompletny raport analizy behawioralnej dla złośliwych plików.
   6) Rozwiązanie musi obsługiwać globalne udostępnianie informacji o zagrożeniach, aby wykryć nowe nieznane zagrożenie.
8. **Wykrywanie spamu**
   1) Rozwiązanie musi wspierać klasyfikację i wykrywanie spamu w czasie rzeczywistym.
   2) Rozwiązanie musi obsługiwać wykrywanie spamu niezależnie od języka, formatu lub treści wiadomości.
   3) Rozwiązanie musi obsługiwać protokoły poczty e-mail smtp i pop3.
   4) Rozwiązanie musi obsługiwać białe listy wiadomości e-mail z zaufanych domen.
9. **Dodatkowe funkcje ochrony**
   1) Rozwiązanie musi obsługiwać wykrywanie DoS / DDoS, SYN Flood, DNS query flood itp.
   2) Rozwiązanie musi obsługiwać wykrywanie ataków ARP w tym spoofing ARP.
   3) Rozwiązanie musi obsługiwać wykrywanie anormalnych ataków protokołu.
   4) Rozwiązanie powinno obsługiwać rejestrowanie IOC w celu śledzenia zagrożeń, takich jak brute force, tworzenia podejrzanych plików, złośliwych procesów PowerShell itp.
10. **Inteligentne funkcje bezpieczeństwa**
    1) Rozwiązanie powinno obsługiwać analizę korelacji zagrożeń, korelację między nieznanymi zagrożeniami, nietypowym zachowaniem i zachowaniem aplikacji, aby wykryć potencjalne zagrożenia lub ataki.
    2) Rozwiązanie powinno umożliwiać aktualizację bazy danych modelu zachowania szkodliwego oprogramowania online w czasie rzeczywistym.
    3) Rozwiązanie powinno obsługiwać wykrywanie ponad 2000 znanych i nieznanych rodzin złośliwego oprogramowania, w tym wirusów, robaków, trojanów itp.
    4) Rozwiązanie musi obsługiwać zaawansowane wykrywanie złośliwego oprogramowania oparte na obserwacji zachowania.
    5) Rozwiązanie musi wspierać wykrycia oprogramowania ransomware i złośliwego oprogramowania do wydobywania kryptowalut.
    6) Rozwiązanie powinno obsługiwać modelowanie zachowania w oparciu o ruch bazowy L3-L7, aby ujawnić nietypowe zachowanie sieci, takie jak skanowanie HTTP, Spider, SPAM, słabe hasła SSH / FTP dla serwerów i hostów.
    7) Rozwiązanie musi obsługiwać wykrywanie DDoS, w tym Flood, Sockstress, zip of death, reflect, dns query, SSL DDos i aplikacyjny DdoS.
    8) Rozwiązanie musi obsługiwać inspekcję zaszyfrowanego ruchu tunelowego dla nieznanych aplikacji.
    9) Rozwiązanie musi obsługiwać aktualizację bazy danych modelu nieprawidłowego zachowania online w czasie rzeczywistym.
    10) Rozwiązanie musi zapewniać analizę kryminalistyczną, w tym analizę zagrożeń, bazę wiedzy, historię i topologię zagrożeń.
    11) Rozwiązanie musi obsługiwać działania administratora w celu zmiany stanu zagrożenia na false positive, naprawionego, zignorowanego, potwierdzonego zdarzenia.
    12) Rozwiązanie musi obsługiwać czyszczenie zagrożeń serwera jednym kliknięciem i ponowną ocenę bezpieczeństwa hosta.
    13) Rozwiązanie powinno obsługiwać białą listę zagrożeń, w tym nazwę zagrożenia, źródłowy/docelowy adres IP, liczbę odwiedzin itd.
    14) Rozwiązanie musi obsługiwać przechwytywanie pakietów online.
    15) Rozwiązanie musi obsługiwać lokalną technologię honeypot, aby wychwytywać ataki zagrożeń

sieciowych i potwierdzać źródło zagrożenia, typ zagrożenia i częstość występowania.
16) Rozwiązanie musi obsługiwać wykrywanie oszustw na podstawie behawioralnej dla ftp, HTTP, MYSQL, SSH, TELNET, dokumentów lub baz danych.
17) Rozwiązanie musi obsługiwać funkcję polowania na zagrożenia (threat hunting), aby zebrać kompleksowe dowody i zapewnić dogłębną analizę.
18) Rozwiązanie powinno obsługiwać rejestrowanie IOC w celu śledzenia zagrożeń, takich jak brute force remote dekto, tworzenia podejrzanych plików, złośliwych procesów PowerShell itp. w celu poprawy wykrywalność funkcji śledzenia zagrożeń.

11. **Widoczność ryzyka/zagrożeń**
    1) Rozwiązanie musi obsługiwać wizualizację zagrożeń intranetowych dla serwerów (zasobów krytycznych), a także wykrywanie nietypowego ruchu z nimi związanego.
    2) Rozwiązanie musi obsługiwać widoczność zagrożeń dla ryzykownych hostów, w tym nazwy hosta, systemu operacyjnego, przeglądarki, typu usługi, aby rejestrować zagrożenia hosta i nietypowy ruch.
    3) Rozwiązanie musi obsługiwać widoczność podstawowych informacji opartych na hoście, indeksu ryzyka, zagrożeń i nietypowego ruchu.
    4) Rozwiązanie powinno wspierać widoczność zagrożeń, w tym nazwę zagrożenia, typ zagrożenia, poziom ryzyka, bazę wiedzy, pakiet kryminalistyczny itp.
    5) Rozwiązanie powinno dostarczyć wszystkie statystyki klasyfikacji zdarzeń zagrożeń w oparciu o IOC i trend zdarzeń zagrożeń w ciągu co najmniej 2 tygodni.
    6) Rozwiązanie musi wspierać wskazanie ścieżki ataku.
12. **Analiza i odpowiedzi na incydenty**
    1) Rozwiązanie musi obsługiwać aktualizację w czasie rzeczywistym najpoważniejszych informacji o zagrożeniach znalezionych w branży do urządzenia z chmury.
    2) Obsługa wyświetlania najnowszych informacji o zagrożeniach w wyskakujących okienkach.
    3) Obsługa rejestrowania i sprawdzania, czy w sieci wystąpiło odpowiednie zagrożenie.
    4) Pomoc techniczna w celu dostarczenia szczegółowych informacji o zagrożeniach i sugestii dotyczących rozwiązania.
    5) Wsparcie konfigurowania reguł ostrzegania o zagrożeniach, w tym warunków zagrożenia i metody działania, które w przypadku wystąpienia zdarzenia stanowiącego zagrożenie, system powiadomi użytkownika lub podejmie odpwiedź w odpowiednim czasie zgodnie z metodą działania określoną w regule (np. połączenie z firewall, przypomnienie głosowe lub wysłanie pocztą e-mail.
13. **Administracja**
    1) Rozwiązanie musi mieć zintegrowany sieciowy interfejs użytkownika (WebUI) i interfejs wiersza poleceń (CLI).
    2) Rozwiązanie powinno obsługiwać zarządzanie dostępem z HTTP/HTTPS, SSH, telnet, konsoli.
    3) Rozwiązanie musi być w stanie chronić system przed atakami brute-force na nazwę użytkownika i hasło.
    4) Rozwiązanie musi obsługiwać zasady zabezpieczeń haseł dla kont administratorów.
    5) Rozwiązanie musi obsługiwać monitorowanie hostów i serwerów w sieci wewnętrznej, identyfikując nazwę, system operacyjny, przeglądarkę, typ i rejestr statystyk zagrożeń sieciowych.
    6) Rozwiązanie powinno posiadać aplikację mobilną pozwalającą na monitoring pracy i analizę zdarzeń.
14. **Logowanie i raportowanie**
    1) Rozwiązanie musi obsługiwać raportowanie zdefiniowane przez użytkownika. Raport można wyeksportować co najmniej w formacie PDF i/lub wysłać na adres e-mail lub FTP.
    2) Rozwiązanie powinno obsługiwać ustawianie alarmów dotyczących wykorzystania procesora, wykorzystania pamięci, wykorzystania miejsca na dysku, nowych połączeń itp.
    3) Rozwiązanie powinno obsługiwać wysyłanie alarmów przez e-mail, SMS.
    4) Alerty powinny być generowane na podstawie przepustowości aplikacji i nowych połączeń.
    5) Logi powinny być możliwe do eksportu za pośrednictwem Syslog lub poczty e-mail i zawierać minimum logi zdarzeń, sieci, zagrożenia, konfigurację i sesje.
    6) Rozwiązanie powinno posiadać wstępnie zdefiniowane zadania raportowania.
    7) Rozwiązanie powinno mieć scentralizowane monitorowanie wielu urządzeń, w tym procesora, pamięci, ruchu, sesji, aplikacji, użytkowników, zagrożeń itp. za pośrednictwem aplikacji mobilnej z danymi z ostatnich 7 dni.
    8) Rozwiązanie musi wspierać restAPI.
15. **Gwarancja**
    1) 24-miesięczna gwarancja producenta na dostarczone elementy systemu.
    2) Licencja na wszystkie funkcje bezpieczeństwa oraz wsparcie techniczne producenta na oprogramowanie na okres minimum 24 miesięcy.
    3) Wsparcie techniczne dystrybutora rozwiązań w języku polskim.
16. **Szkolenie**
    1) Wykonawca zapewni szkolenie w zakresie użytkowania i administrowania urządzeniem. Szkolenie musi zostać przeprowadzone dla 1 osoby i musi być zakończone przyznaniem certyfikatu, potwierdzającego

wspomniane umiejętności wydanym przez producenta urządzenia. Szkolenie może odbyć się w formie zdalnej.