

Dostawa urządzenia klasy NDR wraz z oprogramowaniem (1 szt.)

Przedmiotem zamówienia jest dostawa urządzenia typu NDR (Network Detection and Response) inteligentnego systemu, który analizuje ruch sieciowy i wykorzystuje techniki takie jak uczenie maszynowe, sztuczna inteligencja (AI) i analiza behawioralna do wykrywania podejrzanej lub złośliwej aktywności w sieci.

Minimalne parametry techniczne i funkcjonalne:

1. Elementy systemu bezpieczeństwa
 - a. Wysokość 1U do montażu w szafie rack.
 - b. Posiadać co najmniej dwa porty USB
 - c. Urządzenie musi posiadać dedykowany port do zarządzania
 - d. Urządzenie musi posiadać minimum interfejsów: 2x SFP+, 8x SFP, 8x GE
 - e. Musi obsługiwać co najmniej 1T przestrzeni dyskowej.
 - f. Minimum 1 Gb/s przepustowości wykrywania naruszeń w dwukierunkowym ruchu HTTP z włączonymi wszystkimi funkcjami wykrywania zagrożeń
 - g. Proponowane rozwiązanie musi obsługiwać minimum 750 tys. jednoczesnych sesji.
 - h. Proponowane rozwiązanie musi obsługiwać 32000 nowych sesji /s w ruchu HTTP.
2. Usługi sieciowe
 - a. Musi obsługiwać pasywny tryb pracy (TAP), nie ingerując w sieć klienta.
 - b. Rozwiązanie musi być w stanie zintegrować się z zaporami ogniowymi tej samej marki w celu ograniczenia zagrożeń
 - c. Musi posiadać możliwość rozwiązywania wiadomości przez protokół MPLS, VXLAN oraz QinQ i wykrywania zagrożeń w tych wiadomościach.
3. Kontrola aplikacji
 - a. 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.
 - b. Rozwiązanie musi być w stanie zidentyfikować aplikacje mobilne typu iOS lub Android.
 - c. 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
 - a. Rozwiązanie musi obsługiwać co najmniej 16000 sygnatur IPS. Musi obsługiwać niestandardowe sygnatury, ręczne i automatyczne aktualizacje, wyodrębnianie sygnatur oraz wbudowaną encyklopedię zagrożeń.
 - b. Rozwiązanie musi obsługiwać ochronę przed atakami SQL injection, XSS, buffer overflow zarówno dla IPv4 jak i IPv6
 - c. Rozwiązanie powinno obsługiwać ochronę przed atakami C&C z limitem żądań, limitem proxy, niestandardowym progiem, Musi obsługiwać wykrywanie co najmniej metod uwierzytelniania: JS Cookie, Redirect, Access confirm, CAPCHA
 - d. Rozwiązanie musi obsługiwać wykrywanie anomalii protokołów HTTP, SMTP, IMAP, POP3, VOIP, NETBIOS itp.
 - e. Niestandardowe reguły wykrywania włamań muszą obsługiwać konfigurowanie kierunku ruchu ataku w celu poprawy dokładności analizy źródła ataku.
 - f. Rozwiązanie powinno umożliwiać tworzenie białych list dla modułu IPS.

- g. Rozwiązanie musi mieć wstępnie zdefiniowane profile IPS.
- h. Rozwiązanie musi mieć opcję przechwytywania pakietów
- i. Rozwiązanie musi umieć wykrywać reverse-shell
- j. Rozwiązanie potrafi zdefiniować odpowiednie treshholdy chroniące przed atakami Flood, bazując na parametrach dostarczonego ruchu
- k. System musi mapować wykryte zagrożenia na framework MITRE ATT&CK
- 5. Skanowanie antywirusowe
 - a. Rozwiązanie musi obsługiwać co najmniej 13 milionów sygnatur antywirusowych z ręcznymi lub automatycznymi aktualizacjami sygnatur.
 - b. Rozwiązanie musi wspierać antywirus oparty na przepływie dla protokołów min. HTTP, SMTP, POP3, IMAP, FTP/SFTP.
 - c. 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
 - d. Rozwiązanie musi obsługiwać wykrywanie zaszyfrowanych skompresowanych plików
- 6. Wykrywanie botnetów C&C
 - a. Rozwiązanie powinno wspierać skuteczne wykrywanie botów intranetowych i zapobieganie dalszym atakom ze strony zaawansowanych zagrożeń poprzez porównywanie uzyskanych informacji z bazą adresów C&C.
 - b. Rozwiązanie musi obsługiwać automatyczną aktualizację sygnatur botnetów C&C
 - c. Rozwiązanie musi obsługiwać dwa typy bazy adresów C&C: bazę adresów IP i bazę danych domen.
 - d. Rozwiązanie musi obsługiwać wykrywanie C&C protokołów w protokołach TCP, HTTP i DNS.
 - e. Rozwiązanie musi wspierać włączenie wykrywania DGA w celu analizy odpowiedzi DNS i wykrywania, czy urządzenie jest atakowane przez nazwę domeny DGA.
 - f. Musi wspierać wykrywanie tunelowania w protokole DNS w tym analizowanie zapytań DNS a także rejestrować logów zagrożeń wykrytych tuneli DNS.
- 7. Sandbox w chmurze
 - a. Rozwiązanie musi obsługiwać oparte na chmurze wirtualne środowisko analizy złośliwego oprogramowania w celu znalezienia nieznanych zagrożeń
 - b. Rozwiązanie musi obsługiwać przesyłanie złośliwych plików do piaskownicy w chmurze w celu analizy.
 - c. Rozwiązanie powinno obsługiwać przesyłanie złośliwych plików z protokołów, w tym HTTP/HTTPS, POP3, IMAP4, SMTP i FTP.
 - d. Rozwiązanie musi obsługiwać typy plików, w tym PE, ZIP, RAR, Office, PDF, APK, JAR, SWF oraz skrypty
 - e. Rozwiązanie powinno dostarczyć kompletny raport analizy behawioralnej dla złośliwych plików.
 - f. Rozwiązanie musi obsługiwać globalne udostępnianie informacji o zagrożeniach, aby wykryć nowe nieznane zagrożenie.
- 8. Wykrywanie spamu
 - a. Rozwiązanie musi wspierać klasyfikację i wykrywanie spamu w czasie rzeczywistym
 - b. Rozwiązanie musi obsługiwać wykrywanie spamu niezależnie od języka, formatu lub treści wiadomości.
 - c. Rozwiązanie musi obsługiwać protokoły poczty e-mail smtp i pop3
 - d. Rozwiązanie musi obsługiwać białe listy wiadomości e-mail z zaufanych domen.
- 9. Dodatkowe funkcje ochrony
 - a. Rozwiązanie musi obsługiwać wykrywanie DoS / DDoS, SYN Flood, DNS query flood itp.

- b. Rozwiązanie musi obsługiwać wykrywanie ataków ARP w tym spoofing ARP
 - c. Rozwiązanie musi obsługiwać wykrywanie anormalnych ataków protokołu.
 - d. Rozwiązanie powinno obsługiwać rejestrowanie IOC w celu śledzenia zagrożeń, takich jak brute force, tworzenia podejrzanych plików, złośliwych procesów PowerShell itp. w celu pop
10. Inteligentne funkcje bezpieczeństwa
- a. Rozwiązanie powinno obsługiwać analizę korelacji zagrożeń, korelację między nieznanymi zagrożeniami, nietypowym zachowaniem i zachowaniem aplikacji, aby wykryć potencjalne zagrożenia lub ataki.
 - b. Rozwiązanie powinno umożliwiać aktualizację bazy danych modelu zachowania szkodliwego oprogramowania online w czasie rzeczywistym.
 - c. Rozwiązanie powinno obsługiwać wykrywanie ponad 2000 znanych i nieznanych rodzin złośliwego oprogramowania, w tym wirusów, robaków, trojanów itp
 - d. Rozwiązanie musi obsługiwać zaawansowane wykrywanie złośliwego oprogramowania oparte na obserwacji zachowania
 - e. Rozwiązanie musi wspierać wykrycia oprogramowania ransomware i złośliwego oprogramowania do wydobywania kryptowalut.
 - f. 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.
 - g. Rozwiązanie musi obsługiwać wykrywanie DDoS, w tym Flood, Sockstress, zip of death, reflect, dns query, SSL DDos i aplikacyjny DDoS
 - h. Rozwiązanie musi obsługiwać inspekcję zaszyfowanego ruchu tunelowego dla nieznanymi aplikacji
 - i. Rozwiązanie musi obsługiwać aktualizację bazy danych modelu nieprawidłowego zachowania online w czasie rzeczywistym
 - j. Rozwiązanie musi zapewniać analizę kryminalistyczną , w tym analizę zagrożeń, bazę wiedzy, historię i topologię zagrożeń.
 - k. Rozwiązanie musi obsługiwać działania administratora w celu zmiany stanu zagrożenia na false positive, naprawionego, zignorowanego, potwierdzonego zdarzenia
 - l. Rozwiązanie musi obsługiwać czyszczenie zagrożeń serwera jednym kliknięciem i ponowną ocenę bezpieczeństwa hosta
 - m. Rozwiązanie powinno obsługiwać białą listę zagrożeń, w tym nazwę zagrożenia, źródłowy/docelowy adres IP, liczbę odwiedzin itd.
 - n. Rozwiązanie musi obsługiwać przechwytywanie pakietów online
 - o. Rozwiązanie musi obsługiwać lokalną technologię honeypot, aby wychwytywać ataki zagrożeń sieciowych i potwierdzać źródło zagrożenia, typ zagrożenia i częstotliwość występowania
 - p. Rozwiązanie musi obsługiwać wykrywanie oszustw na podstawie behawioralnej dla ftp, HTTP, MYSQL, SSH, TELNET, dokumentów lub baz danych
 - q. Rozwiązanie musi obsługiwać funkcję polowania na zagrożenia (threat hunting), aby zebrać kompleksowe dowody i zapewnić dogłębną analizę
 - r. Rozwiązanie powinno obsługiwać rejestrowanie IOC w celu śledzenia zagrożeń, takich jak brute force remote dektto, tworzenia podejrzanych plików, złośliwych procesów PowerShell itp. w celu poprawy wykrywalności funkcji śledzenia zagrożeń.
11. Widoczność ryzyka/zagrożeń
- a. Rozwiązanie musi obsługiwać wizualizację zagrożeń intranetowych dla serwerów (zasobów krytycznych), a także wykrywanie nietypowego ruchu z nimi związanego.
 - b. Rozwiązanie musi obsługiwać widoczność zagrożeń dla ryzykownych hostów, w tym nazwy hosta, systemu operacyjnego, przeglądarki, typu usługi, aby rejestrować zagrożenia hosta i nietypowy ruch.

- c. Rozwiązanie musi obsługiwać widoczność podstawowych informacji opartych na hoście, indeksu ryzyka, zagrożeń i nietypowego ruchu.
 - d. Rozwiązanie powinno wspierać widoczność zagrożeń, w tym nazwę zagrożenia, typ zagrożenia, poziom ryzyka, bazę wiedzy, pakiet kryminalistyczny itp.
 - e. Rozwiązanie powinno dostarczyć wszystkie statystyki klasyfikacji zdarzeń zagrożeń w oparciu o IOC i trend zdarzeń zagrożeń w ciągu co najmniej 2 tygodni.
 - f. Rozwiązanie musi wspierać wskazanie ścieżki ataku.
12. Analiza i odpowiedzi na incydenty
- a. Rozwiązanie musi obsługiwać aktualizację w czasie rzeczywistym najpoważniejszych informacji o zagrożeniach znalezionych w branży do urządzenia z chmury
 - b. Obsługa wyświetlania najnowszych informacji o zagrożeniach w wyskakujących okienkach.
 - c. Obsługa rejestrowania i sprawdzania, czy w sieci wystąpiło odpowiednie zagrożenie.
 - d. Pomoc techniczna w celu dostarczenia szczegółowych informacji o zagrożeniach i sugestii dotyczących rozwiązania.
 - e. 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 odpowiedź w odpowiednim czasie zgodnie z metodą działania określoną w regule (np. połączenie z firewall, przypomnienie głosowe lub wysłanie pocztą e-mail).
13. Administracja
- a. Rozwiązanie musi mieć zintegrowany sieciowy interfejs użytkownika (WebUI) i interfejs wiersza poleceń (CLI)
 - b. Rozwiązanie powinno obsługiwać zarządzanie dostępem z HTTP/HTTPS, SSH, telnet, konsoli
 - c. Rozwiązanie musi być w stanie chronić system przed atakami brute-force na nazwę użytkownika i hasło
 - d. Rozwiązanie musi obsługiwać zasady zabezpieczeń haseł dla kont administratorów.
 - e. Rozwiązanie musi obsługiwać monitorowanie hostów i serwerów w sieci wewnętrznej, identyfikując nazwę, system operacyjny, przeglądarkę, typ i rejestr statystyk zagrożeń sieciowych
 - f. Oferowany zestaw urządzeń musi pochodzić o jednego producenta i być w pełni kompatybilny
 - g. Oferowany zestaw urządzeń musi posiadać aplikację mobilną pozwalającą na monitoring pracy urządzeń i analizę zdarzeń
14. Logowanie i raportowanie
- a. Rozwiązanie musi obsługiwać raportowanie zdefiniowane przez użytkownika. Raport można wyeksportować co najmniej w formacie PDF i/lub wysłać na adres e-mail lub FTP.
 - b. Rozwiązanie powinno obsługiwać ustawianie alarmów dotyczących wykorzystania procesora, wykorzystania pamięci, wykorzystania miejsca na dysku, nowych połączeń itp.
 - c. Rozwiązanie powinno obsługiwać wysyłanie alarmów przez e-mail, SMS.
 - d. Alerty powinny być generowane na podstawie przepustowości aplikacji i nowych połączeń.
 - e. Logi powinny być możliwe do eksportu za pośrednictwem Syslog lub poczty e-mail i zawierać minimum logi zdarzeń, sieci, zagrożenia, konfigurację i sesje
 - f. Wstępnie zdefiniowane zadania raportowania
 - g. 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.
 - h. Rozwiązanie musi wspierać restAPI

15. Gwarancja – Dostawa musi zawierać również
- a. 24-miesięczną gwarancję producenta na dostarczone elementy systemu
 - b. Licencje na wszystkie funkcje bezpieczeństwa producentów na okres minimum 24 miesięcy (IPS, AV, AS, QoS, Cloud-Sandbox, URL, IP Reputation, Botnet C&C)
 - c. Wsparcie techniczne dystrybutora rozwiązań w języku polskim
 - d. Gwarancja musi być zapewniona przez autoryzowanego partnera