Załącznik nr 1 – 32/2026/Z – opis przedmiotu zamówienia

1.	**Przedmiot zamówienia**	System bezpieczeństwa realizujący wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Klaster urządzeń Unified Threat Management.
2.	**Wymagania ogólne**	• System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. • System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. • System wspiera protokoły IPv4 oraz IPv6 w zakresie: o Firewall, o ochrony w warstwie aplikacji, o protokołów routingu dynamicznego.
3.	**Redundancja, monitoring i wykrywanie awarii**	• W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. • Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. • Monitoring stanu realizowanych połączeń VPN. • System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
4.	**Interfejsy, Dysk, Zasilanie**	• System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: o 8 portami Gigabit Ethernet RJ-45, o 2 gniazdami SFP+ 10 Gbps, • System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB. • System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. • System jest wyposażony w zasilanie AC.

5.	**Parametry wydajnościowe**	• W zakresie Firewall'a obsługa nie mniej niż 1.5 mln jednoczesnych połączeń oraz 120 tys. nowych połączeń na sekundę. • Przepustowość Stateful Firewall: nie mniej niż 28 Gbps dla pakietów 512 B. • Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps. • Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 25 Gbps. • Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side, jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 4 Gbps. • Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2 Gbps. • Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 2.5 Gbps.
6.	**Funkcje Systemu Bezpieczeństwa:** W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych	• Kontrola dostępu - zapora ogniowa klasy Stateful Inspection, • kontrola Aplikacji, • poufność transmisji danych - połączenia szyfrowane IPSec VPN, • ochrona przed malware, • ochrona przed atakami - Intrusion Prevention System, • kontrola stron WWW, • kontrola zawartości poczty – Antyspam dla protokołów SMTP. • zarządzanie pasmem (QoS, Traffic shaping), • dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site, • inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3, • możliwość filtrowania zapytań DNS w ruchu przechodzącym

		przez system, • rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
7.	**Polityki, Firewall**	• Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. • System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: o translację jeden do jeden oraz jeden do wielu, o dedykowany ALG (Application Level Gateway) dla protokołu SIP. • W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. • Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP. • Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. • możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. • Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu: o Amazon Web Services (AWS), o Microsoft Azure, o Cisco ACI, o Google Cloud Platform (GCP), o OpenStack, o VMware NSX, o Kubernetes.
8.	**Połączenia VPN** System umożliwia	• wsparcie dla IKE v1 oraz v2, • obsługę szyfrowania protokołem minimum AES z kluczem 128

	konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:	oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM), • obsługa protokołu Diffie-Hellman grup 19, 20, • wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, • tworzenie połączeń typu Site-to-Site oraz Client-to-Site, • monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności, • możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat, • możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu, • możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu, • obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth, • mechanizm „Split tunneling” dla połączeń Client-to-Site, • producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie VPN jest dostępne jako opcja i nie jest wymagane w implementacji. • autoryzowany i wspierany przez producenta oferowanego rozwiązania mechanizm uwierzytelniania wieloskładnikowego (MFA/2FA) z jednoczesnym dostępem dla 5 dodatkowych kont użytkowników
9.	**W zakresie routingu rozwiązanie zapewnia obsługę:**	• routingu statycznego, • Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego), • protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM, • możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu, • ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu, • BFD (Bidirectional Forwarding Detection).

		• monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
10.	**Funkcje SD-WAN**	• System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. • SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
11.	**Zarządzanie pasmem**	• System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. • System daje możliwość określania pasma dla poszczególnych aplikacji. • System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. • System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
12.	**Ochrona przed malware**	• Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). • Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. • W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum. • System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. • System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). • Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. • System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na

		terenie Unii Europejskiej. • Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. • Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
13.	**Ochrona przed atakami**	• Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. • System chroni przed atakami na aplikacje pracujące na niestandardowych portach. • Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. • Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. • System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. • Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). • Wykrywanie i blokowanie komunikacji C&C do sieci botnet. • Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
14.	**Kontrola aplikacji**	• Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. • Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. • Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. • Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. • Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. • Istnieje możliwość blokowania aplikacji działających na

		niestandardowych portach (np. FTP na porcie 2021). • System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
15.	**Kontrola WWW**	• Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. • W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. • Filtr WWW dostarcza kategorii stron zabronionych prawem, np.: hazard. • Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. • Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). • Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. • Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek, takich jak: Google oraz Yahoo. • Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. • System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
16.	**Uwierzytelnianie użytkowników w ramach sesji**	• System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: o haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu, o haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP, o haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

		• System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego. • System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. • Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP
17.	**Zarządzanie**	• Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. • Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. • Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego. • System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. • System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. • Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. • Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. • Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). • Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
18.	**Logowanie**	• Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

		• W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. • Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. • Możliwość włączenia logowania per reguła w polityce firewall. • System zapewnia możliwość logowania do serwera SYSLOG. • Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
19.	**Testy wydajnościowe oraz funkcjonalne**	• Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta, lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni).
20.	**Serwisy i licencje** Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje	• Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen, Weryfikacja zgodności konfiguracji z dobrymi praktykami producenta (audyt konfiguracji i polityk urządzenia) na okres na okres 36 miesięcy.
21.	**Wymagania ogólne**	• Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.), oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością, tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

		• Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

Wykonawca zapewni dostawę, instalację i konfigurację dwóch sztuk urządzeń Unified Threat Management w trybie klastra oraz migrację dotychczasowej konfiguracji z eksploatowanego systemu firewall WatchGuard Firebox do nowego rozwiązania.

Zakres obejmuje:

a) konfiguracja ogólna systemu - adresów IP, DNS, DHCP, routing, NTP,

b) konfiguracja interfejsów sieciowych - WAN, LAN, DMZ. Konfiguracja dodatkowego łącza zapasowego, łącznie z ustawieniem routingu oraz przygotowanie odpowiednich polityk,

c) przeniesienie całej konfiguracji z istniejącego urządzenia Firewall na nowy system UTM z najnowszą stabilną wersją oprogramowania,

d) inwentaryzacja reguł i ustawień, weryfikacja i poprawienie reguł oraz ustawień, optymalizacja używanych dotychczas reguł, zgodnie z dobrymi praktykami,

e) konfiguracja QoS oraz kształtowania pasma,

f) konfiguracja i uruchomienie mechanizmów IDS/IPS w celu wykrywania i zapobiegania włamaniom, identyfikacji podejrzanego ruchu sieciowego oraz blokowania prób wykorzystania znanych podatności, wraz z dostosowaniem reguł detekcji i prewencji do środowiska Zamawiającego.

g) przeniesienie istniejących obiektów sieciowych,

h) przeniesienie istniejących reguł firewall oraz NAT,

i) przeniesienie konfiguracji IPSec VPN,

j) przeniesienie filtrów URL oraz SSL,

k) konfiguracja inspekcji SSL,

l) konfiguracja przesyłania logów do posiadanych przez Zamawiającego instancji zbierających i przechowujących logi,

m) konfiguracja klastra zapewniającego ciągłość działania usług sieciowych w przypadku awarii jednego z urządzeń, wraz z weryfikacją poprawności przełączania awaryjnego

n) wykonanie podstawowej segmentacji sieci poprzez wydzielenie odrębnych stref bezpieczeństwa zgodnie z zasadą minimalnych uprawnień i dobrymi praktykami bezpieczeństwa,

o) przeprowadzenie szkolenia dla administratorów Zamawiającego z obsługi i administracji wdrożonym systemem UTM,

p) przekazanie kompletnej dokumentacji powykonawczej.

Dostawa i wdrożenie platformy do wielopoziomowej ochrony urządzeń końcowych wraz z licencją i wsparciem technicznym producenta na okres 36 miesięcy

Wymagania platformy:

1. musi zapewniać centralne zarządzanie ochroną wszystkich typów urządzeń końcowych (stacje robocze, serwery) i automatyzację reakcji na incydenty;
2. musi umożliwiać wdrożenie we wszystkich trzech modelach: cloud (SaaS), on-premise, hybrydowo;
3. musi zapewniać centralną konsolę zarządzającą, dostępna przez przeglądarkę, wspierać autentykację wieloskładnikową (MFA) i mechanizm pojedynczego logowania (SSO) oraz granularne role i uprawnienia, jak również integrację z Active Directory;
4. musi obsługiwać automatyczne wykrywanie i instalowanie agentów na nowych urządzeniach oraz zapewniać szybkie, bezobsługowe wdrożenie aktualizacji (bez potrzeby restartów);
5. musi zapewniać możliwość komunikacji przez publiczne API;
6. musi zapewniać integrację z narzędziami do monitorowania, analizowania i reagowania na zagrożenia w czasie rzeczywistym klasy SIEM;
7. musi zapewniać możliwość zdalnego monitorowania i zarządzania Remote Monitoring and Management (RMM);
8. musi zapewniać możliwość integracji z platformami certyfikacji bezpieczeństwa dla sprzętu, oprogramowania i urządzeń Internetu Rzeczy (IoT) Platform Security Architecture (PSA);
9. musi natywnie oferować, bez konieczności dokupywania modułów zewnętrznych:

a) możliwość instalacji agenta ochrony na następujących systemach operacyjnych: Windows XP, Windows 7 i nowsze, Windows Server od 2008 R2 i nowsze, każda wiodąca dystrybucja Linux (wg. W3Techs), macOS (Intel & Apple Silicon);

b) kompleksową ochronę przed szeroką gamą zagrożeń, obejmującą: wirusy, ransomware, oprogramowanie szpiegujące (spyware), oprogramowanie typu rootkit, cryptominers, ataki typu fileless, exploity (w tym ataki na krytyczne komponenty OS), narzędzia hakerskie, phishing;

c) wsparcie zaawansowanej heurystyki oraz uczenia maszynowego do analizy zachowania, a także dynamiczną analizę podejrzanych plików w czasie rzeczywistym (sandbox), umożliwiającą wykrywanie także zagrożeń typu zero-day;

d) rozbudowane mechanizmy analizy zachowań użytkowników (User & Behavioral Analytics), wykrywania ruchu lateralnego (lateral movement), automatycznej detekcji anomalii oraz pełną widoczność ruchu procesów, plików, rejestru, systemu i sieci (detection living-off-the-land);

e) wbudowane mechanizmy automatycznej reakcji na incydenty, w tym: izolacja stacji lub hosta, blokowanie kont użytkowników, natychmiastowe zamykanie procesów, kwarantanna plików, przywrócenie stanu systemu sprzed incydentu (rollback);

f) możliwość blokowania urządzeń (device control) podłączanych za pomocą USB;

g) zaawansowany threat hunting, możliwość eksportu i importu wskaźników kompromitacji IoC, integrację z syslog, SIEM oraz publiczne API dla zarządzania i automatyzacji;

h) natywne mechanizmy deception, czyli: fałszywe pliki, pułapki na hostach i endpointach, pułapki w sieci lokalnej, honeypoty;

i) pełną kompatybilność i koegzystencję z innym legalnie wykorzystywanym w organizacji oprogramowaniem antywirusowym lub zabezpieczającym;

1. musi umożliwiać wykrywanie, blokowanie i automatyczną reakcję na poniższe techniki, bazując na MITRE ATT&CK, musi umożliwiać korelację poniższych technik, ich wizualizację, automatyzację reakcji oraz pełną dokumentację incydentów z poziomu jednej konsoli:
2. wykrywanie oraz blokowanie prób pozyskania credentiali przy nieszyfrowanych poświadczeniach (Unsecured Credentials);
3. pełne monitorowanie procesów, wykrywanie prób enumeracji i blokowanie nieautoryzowanego dostępu do informacji o uruchomionych procesach (Process Discovery;.
4. blokowanie prób wyłączania kluczowych usług i komponentów systemowych (Service Stop);
5. wykrywanie i blokowanie interpretatorów komend/skryptów (np. PowerShell, WMI, Bash, CMD) i ich szkodliwego użycia (Command and Scripting Interpreter);
6. wykrywanie prób automatycznego zbierania danych na stacjach (Automated Collection);
7. detekcja prób automatyzowanej eksfiltracji danych (Automated Exfiltration);
8. wykrywanie i blokowanie prób wycieku danych przez kanały Command & Control np. HTTP/S, DNS, ICMP (Exfiltration Over C2 Channel);
9. analiza i alertowanie obfuskacji plików, kodu, informacji (Obfuscated Files or Information);
10. detekcja prób obejścia narzędzi bezpieczeństwa (Debugger Evasion);
11. monitoring i detekcja prób enumeracji użytkowników systemowych (System Owner/User Discovery);
12. kontrola oraz widoczność zmian i zapytań do konfiguracji sieciowej systemów (System Network Configuration Discovery);
13. detekcja prób zbierania informacji o systemie/hostach (System Information Discovery);
14. identyfikacja i blokowanie niestandardowych mechanizmów uruchamiania, blokada rozwiązań typu guardrail (Execution Guardrails);
15. monitoring kluczy rejestru przechowujących dane uwierzytelniające (Credentials in Registry);
16. alertowanie przy enumeracji plików i folderów (File and Directory Discovery);
17. wykrywanie i blokowanie prób wyłączania/omijania zabezpieczeń (Impair Defenses);
18. analiza, wykrywanie i blokowanie nadużycia legalnych (valid) kont (Valid Accounts);
19. wykrywanie oraz blokowanie destrukcji danych (Data Destruction);
20. detekcja i blokowanie działania ransomware oraz szyfrowania masowego plików (Data Encrypted for Impact);

21. monitoring i zapobieganie czyszczeniu śladów/logów przez atakujących (Indicator Removal on Host);

22. Wymaga się, aby oferowane rozwiązanie bezpieczeństwa wykazało skuteczność potwierdzoną w niezależnych badaniach MITRE ATT&CK Evaluations (Enterprise) z roku 2024 lub nowszym, na poziomie co najmniej:

a) 98% skuteczności w zakresie Detection Visibility (widoczność/detekcja wszystkich kroków ataku),

b) 98% skuteczności w zakresie Protection Rate (blokowanie złośliwych kroków ataku),

c) 98% skuteczności w zakresie Prevention (blokowanie ataków na etapie pierwszych kroków).

Wykonawca musi przedłożyć oficjalne materiały producenta lub raporty z MITRE ATT&CK Evaluations potwierdzające spełnienie powyższych progów.;

1. musi zapewnić ochronę offline, czyli zachowanie kluczowych funkcji nawet bez stałego połączenia z serwerem zarządzającym;

2. ma posiadać funkcjonalności deception w zakresie:

a) możliwość automatycznego generowania pułapek będących imitacją endpointów i serwerów i automatyczny sygnał ostrzegawczy po wejściu lub aktywności atakującego na takim deceptive node;

b) możliwość umieszczania plików-pułapek zachęcających do kradzieży, z funkcją monitorowania akcji i generowania alertów;

c) system powiadomień i automatycznej reakcji po każdej nieuprawnionej próbie dostępu;

d) tworzenie kont użytkowników-pułapek, monitorowanie prób logowania oraz wszelkich interakcji z tymi kontami;

e) wykorzystanie deception do szybkiej identyfikacji lateral movement i prób eskalacji uprawnień przez atakującego;

1. musi zapewniać File Integrity Monitoring (FIM) – egzekwowanie polityk w zakresie zmiany plików/zasobów;

2. musi zapewniać wykrywanie skanowania sieci: detekcja aktywności skanowania na poziomie segmentu sieci oraz hosta, wykrywanie prób identyfikacji usług, portów oraz rozpoznawanie różnych technik skanowania (szybkie, wolne, rozproszone);

3. musi zapewniać wykrywanie zatruwania sieci: monitoring prób zatruwania tablic ARP, wykrywanie ataków typu DNS spoofing, technik man-in-the-middle, identyfikacja podszywania się pod urządzenia lub serwery w sieci;

4. musi zapewniać wykrywanie tunelowania eksfiltracji: dentyfikacja nietypowego, tunelowanego ruchu mającego na celu eksfiltrację (DNS tunneling, ICMP tunneling, HTTP/S tunneling), alertowanie przy transferze danych do nieautoryzowanych lokalizacji oraz detekcja długotrwałych i ukrytych połączeń;

5. musi zapewniać zarządzanie i reagowanie poprzez moduł NDR dostępny z poziomu tej samej konsoli zarządzającej;

6. musi zapewniać zaawansowane zarządzanie zasobami sprzętowymi i programowymi (asset management), risk scoring (ocena ryzyka każdego składnika);
7. musi zapewniać pełny logging oraz retencje danych zgodnie z wymogami Zamawiającego (integracja z SIEM, IoC, threat hunting);
8. musi zapewniać możliwość zaawansowanej i personalizowanej automatyzacji reakcji na incydenty (predefiniowane oraz własne playbooki);
9. musi oferować tzw. lekkiego agenta - agent na endpointy nie powinien zużywać więcej niż 250MB RAM oraz 5% CPU;
10. musi zapewniać granularne role/uprawnienia administracyjne, możliwość blokowania zmian ustawień przez użytkowników;

W przypadku wdrożenia w modelu SaaS wszystkie metadane, telemetria, logi i dane użytkownika muszą być przechowywane wyłącznie na terytorium Unii Europejskiej – zgodnie z RODO i normami UE.

Platforma musi obejmować ochroną:

a) do 100 stacji roboczych/serwerów/urządzeń mobilnych

W ramach prac wdrożeniowych Wykonawca zobowiązany jest do:

a) do przeprowadzenia analizy przedwdrożeniowej
b) identyfikacji urządzeń końcowych (stacji roboczych, serwerów, urządzeń mobilnych)
c) zainstalowania i skonfigurowania na zidentyfikowanych urządzeniach końcowych dostarczanego oprogramowania
d) przeniesienia wszystkich polityk bezpieczeństwa z obecnie użytkowanego oprogramowania antywirusowego na nowe oprogramowanie
e) przeprowadzenia 8 godzinnego szkolenia z dostarczonego oprogramowania dla pracowników działu IT

Wykonawca dostarczy pełną dokumentację licencyjną i wdrożeniową w języku polskim lub angielskim.