**Formularz wymogów**

**Załącznik nr 2 swz**

Znak Sprawy: **PCM/ZP 07/I/2023**

**Nazwa Wykonawcy...................................................................................................................**

**Adres:..........................................................................................................................................**

**NIP:............................................................................REGON..................................................**

**OPIS PRZEDMIOTU ZAMÓWIENIA – WYMAGANIA SPRZĘTOWE**

**1. Testy penetracyjne i hardening systemów**

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Wymaganie | Wymagane bezwzględnie | Spełnienie przez Oferenta  TAK/NIE |
| 1 | **Testy penetracyjne zewnętrzne:**   * Identyfikacje dostępnych serwisów sieciowych, określenie oraz weryfikacja ich podatności; * Penetracja systemu za pomocą skanerów TCP i UDP; * Bezpieczeństwo aplikacji oraz usług dostępnych z zewnątrz; * Analiza topologii sieci widzianej z zewnątrz; * Możliwość uzyskania nieautoryzowanego dostępu do danych; * Badanie podatności związanych atakami typu DDoS; * Konfiguracja komunikacji z usługami (np. konfiguracja SSL/TSL, IPsec); | TAK |  |
| 2 | **Testy penetracyjne wewnętrzne:**   * Bezpieczeństwo urządzeń sieciowych; * Bezpieczeństwo protokołów trasowania; * Analiza topologii sieci i logiki jej segmentacji; * Bezpieczeństwo maszyn zlokalizowanych w obrębie sieci (serwery, stacje robocze); * Bezpieczeństwo usług zlokalizowanych na każdym z dostępnych w sieci urządzeniu oraz maszynie, Istnienie nieautoryzowanych urządzeń (np. nieautoryzowanego urządzenia bezprzewodowego wpiętego do sieci); * Filtrowanie komunikacji wewnętrznej (np. konfiguracja firewall, IDS/IPS, WAF, separacja pomiędzy kluczowymi podsieciami); * Konfiguracja komunikacji z zasobami (np. konfiguracja SSL/TLS dla kluczowych aplikacji); * Możliwość uzyskania nieautoryzowanego dostępu do danych (np. danych wrażliwych); * Przegląd danych dostępnych na udziałach sieciowych * Podatność na ataki DDoS; | TAK |  |
| 3 | **Hardening systemów:**   * aktualizacje systemowe i oprogramowania, * wyłączenie zbędnych usług, * zablokowanie nieużywanych portów, * odinstalowanie zbędnych programów, * wyłączenie zbędnych protokołów, * zmiana domyślnych poświadczeń, * wdrożenie Microsoft LAPS, * zastosowanie architektury: zero trust (w jak największym możliwym zakresie) | TAK |  |

**2. Wdrożenie systemu XDR, SIEM, SOAR, SIRP**

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Wymaganie | Wymagane bezwzględnie | Spełnienie przez Oferenta  TAK/NIE |
|  | **XDR (Extended Detection and Response)** | TAK |  |
|  | Rozpoznawanie Zagrożeń: System powinien monitorować i rozpoznawać znane oraz nieznane zagrożenia w czasie rzeczywistym. | TAK |  |
|  | Integracja Z Narzędziami: Zdolność integracji z różnymi narzędziami bezpieczeństwa, takimi jak systemy IDS/IPS, antywirusy, firewall i inne. | TAK |  |
|  | Analiza Zachowań: System powinien analizować zachowania użytkowników i urządzeń w celu wykrywania nieprawidłowości. | TAK |  |
|  | Inteligencja Zagrożeń: System wykorzystuje informacje związane z inteligencją zagrożeń, takie jak bazy danych IOCs (Indicators of Compromise), aby identyfikować znane wzorce ataków i zagrożeń. | TAK |  |
|  | Skalowalność: System ten jest skalowalny i może obsługiwać duże ilości danych oraz liczne źródła informacji, co jest istotne w dużych organizacjach | TAK |  |
|  | **SIEM (System Information and Event Management)** | TAK |  |
|  | Monitorowanie Logów: Zbieranie, normalizacja i analiza logów z różnych źródeł, w tym logów systemowych, zabezpieczeń i aplikacji. | TAK |  |
|  | Korelacja Zdarzeń: Możliwość korelacji zdarzeń w celu wykrycia bardziej zaawansowanych zagrożeń. | TAK |  |
|  | Alertowanie: Generowanie alertów w czasie rzeczywistym w przypadku wykrycia podejrzanych lub złośliwych aktywności. | TAK |  |
|  | Analiza bezpieczeństwa: w czasie rzeczywistym zbieranie, agregowanie, indeksowanie i analizowanie danych dotyczących bezpieczeństwa. Pomaga wykryć włamania, zagrożenia oraz wszelkie anomalie | TAK |  |
|  | Wykrywanie włamań: skanuje system w poszukiwaniu złośliwego oprogramowania, rootkitów | TAK |  |
|  | Monitorowanie integralności plików: monitoruje system plików, identyfikuje zmiany w treści | TAK |  |
|  | Zarządzanie podatnościami: pobieranie danych inwentaryzujących oprogramowanie i bieżące korelowanie ich z aktualizowanymi bazami danych CVE (Common Vulnerabilities and Exposures) | TAK |  |
|  | Ocena konfiguracji: monitorowanie ustawień konfiguracji systemu i aplikacji, aby upewnić się, że są one zgodne z przyjętymi zasadami, alerty mogą zawierać wytyczne dotyczące utwardzenia konfiguracji | TAK |  |
|  | Reakcja na incydent: podjęcie reakcji na wykryty incydent bezpieczeństwa | TAK |  |
|  | Zgodność z przepisami: badanie zgodności technicznej z regulacjami NIST 800-53, GPG13, TSC SOC2 i HIPAA | TAK |  |
|  | Bezpieczeństwo w chmurze: integracja z infrastrukturą chmury na poziomie API (AWS, Azure, GC) i zapewnienie reguł oceny konfiguracji środowiska chmurowego | TAK |  |
|  | Bezpieczeństwo kontenerów: wgląd w bezpieczeństwo kontenerów Dockera | TAK |  |
|  | **SOAR (Security Orchestration, Automation, and Response)** | TAK |  |
|  | Automatyzacja Zadań: Możliwość definiowania i automatyzacji zadań związanych z reakcją na incydenty | TAK |  |
|  | Integracja Skryptów: Wsparcie dla używania skryptów do automatycznego reagowania na zagrożenia | TAK |  |
|  | Koordynacja Działań: Koordynacja działań w zespole ds. bezpieczeństwa w celu skutecznego zarządzania incydentami | TAK |  |
|  | SIRP (Security Incident Response Platform) | TAK |  |
|  | Zarządzanie Incydentami: Kompleksowe zarządzanie incydentami od ich zgłoszenia po ich rozwiązanie i dokumentację. | TAK |  |
|  | Kategoryzacja Incydentów: Możliwość kategoryzacji incydentów na podstawie ich rodzaju, priorytetu i skomplikowania. | TAK |  |
|  | Raportowanie: Generowanie raportów dotyczących incydentów, działań reakcji i zgodności z regulacjami. | TAK |  |
|  | **Rozwiązanie powinno składać się z:** | TAK | --- |
|  | Agent: Agent wdrożony na endpointach (serwery, komputery, urządzenia chmurowe itp.) w celu monitorowania i reagowania na zagrożenia. | TAK |  |
|  | Serwer: Serwer, który zbiera, analizuje i zarządza danymi od agentów. Odpowiada za detekcję zagrożeń i koordynację działań reakcji. | TAK |  |
|  | Silnik wyszukiwania/analizy: Komponent przetwarzający i indeksujący alerty generowane przez system. | TAK |  |
|  | Dashboard: Interfejsu użytkownika dla danych wizualizacji, analizy oraz zarządzania konfiguracją i incydentami. | TAK |  |

**3. Wdrożenie systemu IDS wraz z integracją z systemem SIEM**

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Wymaganie | Wymagane bezwzględnie | Spełnienie przez Oferenta  TAK/NIE |
|  | Monitorowanie Ruchu Sieciowego: Ciągłe monitorowanie ruchu sieciowego w czasie rzeczywistym. Analiza i identyfikacja ruchu sieciowego na różnych poziomach, w tym na poziomie protokołów, portów i aplikacji. | TAK |  |
|  | Wykrywanie Zagrożeń: Wykrywanie i identyfikacja znanych i nieznanych zagrożeń, w tym ataków typu zero-day. Analiza zachowań sieciowych w poszukiwaniu podejrzanych aktywności. | TAK |  |
|  | Korelacja Zdarzeń: Korelacja zdarzeń sieciowych w celu identyfikacji zaawansowanych ataków i skomplikowanych scenariuszy. | TAK |  |
|  | Reagowanie na Incydenty: Automatyczne działania reakcji na wykryte zagrożenia, takie jak blokowanie adresów IP, wyłączanie usług i alarmowanie personelu bezpieczeństwa. Możliwość konfiguracji zasad reakcji na różne rodzaje zagrożeń. | TAK |  |
|  | Zapisywanie Danych: Rejestracja danych ruchu sieciowego i zdarzeń w celu utworzenia audytu i analizy incydentów. | TAK |  |
|  | Raportowanie: Generowanie raportów dotyczących wykrytych zagrożeń, analizy ruchu sieciowego i zgodności z politykami bezpieczeństwa. | TAK |  |
|  | Integracja: Integracja z innymi narzędziami i systemami bezpieczeństwa, takimi jak systemy SIEM i systemy zarządzania incydentami. | TAK |  |
|  | Wydajność: System powinien być zoptymalizowany pod kątem wydajności i być w stanie obsłużyć duże ilości ruchu sieciowego. | TAK |  |
|  | Aktywna społeczność i wsparcie: System powinien posiadać, poza wsparciem dostawcy/producenta również dużą i aktywną społeczność użytkowników oraz deweloperów. | TAK |  |
|  | Możliwość dostosowania: System powinien umożliwiać konfigurację i dostosowanie reguł wykrywania ataków, na specyficzne potrzeby organizacji. | TAK |  |
|  | Wykrywanie wielu typów ataków: Ataki na podstawie sygnatur (Signature-based attacks), Ataki typu Zero-Day, Ataki typu Denial of Service (DoS), Ataki typu Distributed Denial of Service (DDoS), Ataki na protokoły sieciowe, Ataki na serwery i aplikacje webowe, Ataki na systemy operacyjne, Ataki na protokoły VPN, Ataki na protokoły VoIP, Ataki na protokoły IoT, Ataki typu Brute Force, Ataki na protokoły sieciowe niskiego poziomu. | TAK |  |
|  | Rozszerzalność: System powinien posiadać wiele dostępnych rozszerzeń i dodatków, które pozwalają na rozszerzenie funkcjonalności i umożliwiać bardziej zaawansowane monitorowanie i ochronę sieci względem zmieniającego się otoczenia. | TAK |  |

**4. Wdrożenie posiadanego systemu NACVIEW**

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Wymaganie | Wymagane bezwzględnie | Spełnienie przez Oferenta  TAK/NIE |
| 1. | * Instalacja, konfiguracja wstępna i za licencjonowanie produktu w środowisku wirtualizacyjnym klienta. * Podstawowa konfiguracja NACVIEW (integracja z domeną, konfiguracja urzędu certyfikacji, uruchomienie HA). * Konfiguracja urządzenia firewall (dodatnie VLAN-u gościnnego, ustawienie polityk, etc.). * Import urządzeń końcowych i tożsamości (z AD oraz dostarczonych przez Zamawiającego list). * Integracja dostarczanych urządzeń sieciowych Zamawiającego (switche, AP) z NACVIEW, w ramach funkcjonalności dostępnych na urządzeniach. * Uruchomienie uwierzytelniania w oparciu o 802.1X (EAP-TLS) na urządzeniach końcowych wzorcowych po jednym z każdej serii * Uruchomienie uwierzytelniania w oparciu o adres MAC | TAK |  |

**5. Certyfikowane szkolenie z wdrożonego systemu XDR/SIEM**

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Wymaganie | Wymagane bezwzględnie | Spełnienie przez Oferenta  TAK/NIE |
| 1. | Szkolenie stacjonarne/online dla dwóch osób. | TAK |  |

**6. Szkolenie z pozostałych wdrożonych systemów SOAR/SIRP/IDS**

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Wymagania | Wymagane bezwzględnie | Spełnienie przez Oferenta  TAK/NIE |
| 1. | Szkolenie stacjonarne/online dla dwóch osób. | TAK |  |

**7. Odnowienie licencji na posiadane oprogramowanie antywirusowe**

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Wymagania | Wymagane bezwzględnie | Spełnienie przez Oferenta  TAK/NIE |
| 1. | * Nazwa używanego oprogramowania:  Bitdefender Business Security Premium Elite, * ilość licencji: 100, * okres: 3 lata. | TAK |  |

.................................., dnia ............................