Dofinansowanie dla szpitali KPO

– Zakres realizacji przedsięwzięcia –

PUNKT 3. KPO - DZIAŁANIA ZWIĘKSZAJĄCE POZIOM CYBERBEZPIECZEŃSTWA SZPITALA

W ramach trzeciego zakresu możliwe będzie uzyskanie wsparcia finansowego na działania zwiększające poziomu cyberbezpieczeństwa szpitali, co ma służyć bezpiecznemu przetwarzaniu elektronicznej dokumentacji medycznej.
W ramach przedsięwzięcia będzie możliwie sfinansowanie następujących kategorii kosztów (urządzenia, licencje, usługi) w zakresie:

a) systemu kopii zapasowych,
b) zapór sieciowych,
c) ochrony poczty e-mail,
d) segmentacji sieci,
e) ochrony stacji roboczych oraz serwerów (rozwiązania klasy EDR),
f) systemu zarządzania podatnościami,
g) systemu zarządzania bezpieczeństwem informacji,
h) szkolenia dla kadry kierowniczej oraz personelu medycznego i administracyjnego,
i) usługi zarządzane bezpieczeństwa,
j) uwierzytelnienia i autoryzacji do systemów,
k) audytu.

Zakres przedsięwzięcia obejmuje również aktualizację i rozbudowę urządzeń i systemów, przedłużenie posiadanych już licencji, subskrypcji oraz wsparcie dla posiadanych urządzeń lub systemów, zarówno on-premise jak i w chmurze, w okresie trwania przedsięwzięcia.

Testy bezpieczeństwa

☑ Do każdego zakupionego u nas rozwiązania oferujemy bezpłatnie skany podatności z pełnym raportem (mogą być przed i po wdrożeniu).

ARKANET Wojciech Oleś, Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
32 787 48 88
handel@arkanet.pl
www.arkanet.pl

Spis treści

ARKANET Wojciech Oleś, Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
32 787 48 88
handel@arkanet.pl
www.arkanet.pl

Arkanet
Bezpieczeństwo to my

Kategoria A

Zakup lub modernizacja oprogramowania lub urządzeń oferujących co najmniej: tworzenie kopii zapasowych, przywracanie danych, zarządzanie i konfigurację, bezpieczeństwo, monitoring i raportowanie, skalowalność i wydajność, integrację z innymi systemami.

Co możemy zaproponować i jakie są wyróżniki danych rozwiązań?

XOPERO (Xopero Unified Protection – backup Appliance, XOPERO ONE - oprogramowanie)

- ☑ Zintegrowane rozwiązanie sprzętowo-programowe (cyberbunkier) – sprzęt, oprogramowanie i centralne zarządzanie w jednym systemie (dodatkowo jest jeszcze chmura).
- ☑ Nieograniczona ilość licencji – w ramach zakupu urządzenia można backupować co się chce, ogranicza nas jedynie storage (ale można go rozszerzać).
- ☑ WORM – write once, read many – rozwiązanie nie do przejęcia przez oprogramowanie typu ransomware, ponieważ nawet admin ma dostęp tylko do odczytu plików.

NAKIVO (oprogramowanie)

- ☑ Nieskomplikowane rozwiązanie do backupu – podstawowe wdrożenie Nakivo zajmuje naszemu inżynierowi około 30 minut.
- ☑ Genialny backup środowisk wirtualnych (bo od tego de facto Nakivo zaczęło) – obecnie dopieszczają backup środowisk fizycznych.
- ☑ Dobry stosunek jakość/cena – to niedrogie rozwiązanie (w porównaniu do innych, podobnych) i ma licencje wieczyste! 😊

VEEAM (oprogramowanie)

- ☑ Kompleksowy backup – VEEAM potrafi zbackupować niemal wszystko, nie bez kozery jest liderem na naszym rynku.
- ☑ Prosty model licencjonowania – kupujesz paczkę 10 instancji i wykorzystujesz jak chcesz
- ☑ INTEGRACJA – VEEAM ma chyba najbogatszą listę systemów, z którymi się integruje/współpracuje (serwery, NAS, taśmy, chmury).

ACRONIS (oprogramowanie)

- ☑ Backup + zabezpieczenia – Acronis Active Protection wykrywa i blokuje nieautoryzowane szyfrowanie plików/automatycznie przywraca zmodyfikowane dane.
- ☑ Wszechstronność – backupuje zarówno środowiska fizyczne, jak i wirtualne (ponad 20 platform i systemów operacyjnych).

ARKANET Wojciech Oleś, Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
32 787 48 88
handel@arkanet.pl
www.arkanet.pl

Arkanet
Bezpieczeństwo to my

Kategoria B

Zakup sprzętu i oprogramowania dla zapór sieciowych nowej generacji. Zakup sprzętu, oprogramowania, usług dla zapór sieciowych w warstwie aplikacji (WAF). Zakup sprzętu, oprogramowania, usług dla rozwiązań klasy Sandbox.

Co możemy zaproponować i jakie są wyróżniki danych rozwiązań?

FORTINET – FortiGate

- ☑ Fortinet Security Fabric – ścisła integracja z ekosystemem Fortinet (np. FortiSwitch, FortiClient, FortiAnalyzer, FortiPAM, FortiNAC, FortiAutenticator) – pozwala automatyzować reakcje, współdzielić informacje o zagrożeniach.
- ☑ Mnogość informacji i materiałów – Fortinet jest liderem na polskim rynku, ilość materiałów dla klientów, ale też wątków na forach itp., pozwala na rozwiązywanie nawet najbardziej skomplikowanych tematów.
- ☑ Własny VPN w cenie rozwiązania – Fortinet posiada darmowego FortiClienta (jest też wersja płatna) do zestawiania tuneli VPN z użytkownikami. Po zakupie dodatkowych tokenów można korzystać z 2FA (2 tokeny są w zestawie z urządzeniem).

SOPHOS – XGS FIREWALL

- ☑ Synchronized Security – integracja z endpointami Sophosa – pozwala firewallowi reagować na stan zabezpieczeń stacji roboczych.
- ☑ All in ONE – wszystkie dodatkowe funkcjonalności są w formie dodatkowego pakietu UTM, nie potrzeba do tego dodatkowych rozwiązań (poza switchami czy access pointami, bo to nie do przejścia 😊).
- ☑ Konsola Sophos Central – wszystkie rozwiązania Sophosa są zarządzane poprzez chmurę Sophos Central, co bardzo ułatwia administrowanie tym ekosystemem.

Stormshield

- ☑ Modele dedykowane dla OT/ICS – Posiada dedykowaną linię fxpxpi przemysłowych zaprojektowanych do ochrony sieci OT.
- ☑ Zarządzanie w ojczystym języku – chyba, jako jedyny w naszym zestawieniu posiada konsolę w języku polskim.

FORTINET – FortiWeb (WAF)

- ☑ INTEGRACJA – FortiWeb korzysta z usług FortiGuard np. Feed reputacyjny IP czy skanowanie silnikiem AV. Działa również w ramach Security Fabric.
- ☑ Sztuczna Inteligencja – FortiWeb wykorzystuje modele ML do anomalii zachowań, zaawanasowanej ochrony przed atakami zero-day oraz automatycznej aktualizacji polityk bezpieczeństwa.
- ☑ Brute-Force – dedykowane mechanizmy wykrywania i blokowania prób wielokrotnego logowania na aplikacjach internetowych (limity prób logowania, dynamiczne listy blokad, monitorowanie login/logout).

ARKANET Wojciech Oleś, Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
32 787 48 88
handel@arkanet.pl
www.arkanet.pl

Kategoria C

Ochrona poczty email. Zakup sprzętu, usługi lub oprogramowania.

Co możemy zaproponować i jakie są wyróżniki danych rozwiązań?

FORTINET – FortiMail

- ☑ Wielowarstwowe wdrożenie – dostępny jako sprzęt/VM/SaaS/API dla M365, może działać w trybie serwera pocztowego.
- ☑ Ochrona przed wyciekiem – DLP z szyfrowaniem dla wiadomości wychodzących.

Barracuda – Email Protection

- ☑ Zwalczanie ukierunkowanych ataków – moduł oparty na AI (Sentinel), analizuje historię korespondencji.
- ☑ Automatyzacja reakcji na incydenty – pozwala na przeszukanie skrzynki pod kątem złośliwego maila i usunięcie go u wszystkich adresatów.

SOPHOS EMAIL

- ☑ SPX Encryption – szyfrowanie wiadomości e-mail, dostępne na dowolnym kliencie poczty. Konwertuje wiadomości e-mail oraz ich załączniki do pliku PDF i szyfruje je hasłem.
- ☑ Kompleksowe rozwiązanie – pełna funkcjonalność bramy zabezpieczającej, ale i API Mailflow dla Microsoft 365 (chroni skrzynki bez przekierowywania ruchu).

ARKANET Wojciech Oleś, Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
32 787 48 88
handel@arkanet.pl
www.arkanet.pl

Arkanet
Bezpieczeństwo to my

Kategoria D

Segmentacja sieci. Zakup lub modernizacja urządzeń i/lub oprogramowania: przełączniki wielowarstwowe, oprogramowanie klasy NAC.

Co możemy zaproponować i jakie są wyróżniki danych rozwiązań?

FORTINET – FortiSwitch:

- ☑ Zarządzanie – FortiSwitche są zarządzane z poziomu FortiGate'a i działają jak rozszerzenie firewalla, stosując polityki bezpośrednio na portach przełącznika.
- ☑ Prosty NAC – używanie FortiSwitchy pozwala na stworzenie bardzo prostego NAC-a (profilowanie i segmentacja nowych urządzeń).

FORTINET – FortiNAC

- ☑ Integracja – na tle innych rozwiązań NAC oferuje lepszą integrację z systemami bezpieczeństwa – jest częścią Fortinet Security Fabric, do tego jest rozwiązaniem, które odnajdzie się w większości sieci ze sprzętem różnych producentów.
- ☑ Głęboka widoczność – ma aż 21 metod profilowania, wykorzystuje AI/ML do identyfikacji nietypowych urządzeń.
- ☑ Kompatybilność – można go wdrożyć jako appliance fizyczny lub maszynę wirtualną.

NACVIEW

- ☑ Niezależność – NACVIEW jest niezależny od dostawców sprzętu, działa z istniejącą infrastrukturą i integruje się praktycznie z każdym systemem dzięki otwartości producenta na zmiany i ulepszenia.
- ☑ Proste licencjonowanie – jedna licencja dostosowana tylko do ilości IP.
- ☑ Lokalny patriotyzm – NACVIEW to polskie rozwiązanie i samo to może nie być plusem, ale polski support i dostosowanie produktu do naszego rynku jak najbardziej.

ARKANET Wojciech Oleś, Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
32 787 48 88
handel@arkanet.pl
www.arkanet.pl

Arkanet
Bezpieczeństwo to my

Kategoria E

Ochrona stacji roboczych oraz serwerów (rozwiązania klasy EDR).

Co możemy zaproponować i jakie są wyróżniki danych rozwiązań?

ESET – Inspect

- ☑ LiveGrid – podejście do wykrywania oparte na reputacji i występowaniu w innych urządzeniach.
- ☑ Integracja z rozwiązaniami ESET – od antywirusa, przez szyfrowanie, sandbox.
- ☑ Lekki klient – dobrze zoptymalizowany, dzięki czemu wpływ na wydajność maszyn jest minimalny.

WithSecure Elements EDR

- ☑ Całościowy obraz ataku – funkcja Broad Context Detection buduje całą ścieżkę ataku, łączy wydarzenia z wielu urządzeń, nadaje im wspólny identyfikator incydentu i przedstawia na interaktywnej osi czasu.
- ☑ Co-security – współpraca z klientem. Dodatkowa usługa producenta polegająca na obsłudze incydentu, przez wewnętrzny zespół threat hunterów - otrzymują stosowne dane i dostarczają zwrotnie spersonalizowane zalecenia.
- ☑ Wsparcie AI – już w podstawowej wersji, producent wykorzystuje AI do pomocy przy zarządzaniu produktem (Luminen). Dodatkowo jest ona wykorzystywana przy kontekstowym modelu wykrywania, ucząc się historii (pomocne przy false-positivach).

CrowdStrike Falcon Insight

- ☑ Cloud-native – chmurowe rozwiązanie o ogromnej skalowalności, potrafi przeszukać bazę zdarzeń z 100 000 endpointów w ciągu kilku sekund lub skorelować bieżący atak z incydentami u innych klientów.
- ☑ Jakość wykrywania zagrożeń – producent skupia się na zachowaniach i sekwencji działań intruza, dzięki czemu jakość wykrywanych zagrożeń jest na bardzo wysokim poziomie i wykrywa rzeczy niesygnaturowe.
- ☑ Rozbudowa – można dokupić moduł Falcon Spotlight do skanowania podatności, Logscale do analizy logów czy Forensics do zbierania śladów po incydencie.

ARKANET Wojciech Oleś, Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
32 787 48 88
handel@arkanet.pl
www.arkanet.pl

Arkanet
Bezpieczeństwo to my

Kategoria F

System zarządzania podatnościami. Zakup lub modernizacja systemu zarządzania podatnościami.

Co możemy zaproponować i jakie są wyróżniki danych rozwiązań?

WithSecure Exposure Management (XM)

- ☑ Integracja z ekosystemem bezpieczeństwa – XM jest częścią platformy WithSecure Elements, ściśle integruje się z ich rozwiązaniami EPP i EDR. Jeden agent odpowiada za ochronę endpointa i wykrywanie luk w oprogramowaniu.
- ☑ Korzystne licencjonowanie – produkt jest licencjonowany per użytkownik, a nie per IP jak bywa w większości przypadków co znacząco obniża koszty użytkowania.
- ☑ Rekomendacje AI i wskazanie wektorów ataku – XM używa sztucznej inteligencji do priorytetyzacji i workflow. System podpowiada, którymi podatnościami zająć się najpierw, aby obniżyć globalne ryzyko. Dodatkowo system wskazuje potencjalne wektory ataku, rekomendując jednocześnie działania zapobiegawcze.

Holm Security VMP

- ☑ Pełne pokrycie wektorów ataku – platforma jednym rozwiązaniem obejmuje infrastrukturę IT, aplikacje webowe, OT/IOT, a także element ludzki w postaci ataków socjotechnicznych (phishing).
- ☑ Dodatkowe dane o podatnościach – kontekst zagrożeń w procesie oceny ryzyka jest wzbogacony dodatkowymi danymi: czy luka jest wykorzystywana przez atakujących, ilu urządzeń dotyczy, czy może prowadzić do ransomware itp.
- ☑ Zgodność z regulacjami – HOM posiada gotowe rozwiązania wspierające zgodność z regulacjami – dedykowane raporty pod NIS2, ISO 27001, GDPR, DORA itp.

SECPOINT (Penetrator)

- ☑ Kompleksowość – SecPoint dostępny jest jako urządzenie fizyczne lub wirtualne, lub usługa chmurowa. Posiada również moduł Portable Penetrator, który umożliwia przeprowadzenie audytów w terenie.
- ☑ Funkcje specjalne – wbudowany moduł testowania zabezpieczeń wi-fi, dark web search, realtime blackhole list.
- ☑ System ticketingowy – do śledzenia znalezionych podatności i tworzenia użytkowników z odrębnymi uprawnieniami.

ARKANET Wojciech Oleś, Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
32 787 48 88
handel@arkanet.pl
www.arkanet.pl

Kategoria G

Wdrożenie lub modyfikacja systemu zarządzania bezpieczeństwem informacji.

Co możemy zaproponować?

Specyfika

☑ Przygotowanie lub przegląd/modyfikację istniejącego Systemu Zarządzania Bezpieczeństwem informacji, zgodnego z posiadanymi wdrożonymi już rozwiązaniami i tymi, które są planowane w ramach dofinansowania z KPO.

ARKANET Wojciech Oleś, Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
32 787 48 88
handel@arkanet.pl
www.arkanet.pl

Kategoria H

Szkolenia z zakresu podnoszenia świadomości w obszarze Cyberbezpieczeństwa (Cyberhigieny).

Co możemy zaproponować i jakie są wyróżniki danych rozwiązań?

EDUHEZO

- ☑ Dostosowanie do polskiego rynku – szkolenia są opracowane z uwzględnieniem specyfiki polskiego środowiska biznesowego i administracyjnego.
- ☑ Przystępność – kursy są dostępne w języku polskim, co ułatwia zrozumienie materiału przez uczestników.
- ☑ Testy phishingowe – platforma posiada możliwość przeprowadzenia testów phishingowych na użytkownikach. Testy są personalizowane pod danego klienta, więc nie ma mowy o tzw. szablonowym mailu dla każdego.

ProofPoint

- ☑ Zróżnicowane formaty nauki – oferuje szkolenia online, na żywo oraz w formie samodzielnej nauki, co pozwala dostosować proces edukacyjny do indywidualnych potrzeb uczestników.
- ☑ Dostosowanie do ról zawodowych – programy szkoleniowe są zaprojektowane z myślą o różnych stanowiskach i poziomach zaawansowania, co umożliwia skuteczne przekazywanie wiedzy odpowiedniej dla danego użytkownika. Można również implementować własne szkolenia np. dla BHP.
- ☑ Zaawansowane narzędzia analityczne – platforma umożliwia monitorowanie postępów uczestników oraz identyfikację obszarów wymagających dodatkowego szkolenia.

Dagma – „Wydział”

- ☑ Narracyjna forma nauki – szkolenie wykorzystuje fabularną opowieść, co zwiększa zaangażowanie uczestników i ułatwia przyswajanie wiedzy.
- ☑ Praktyczne scenariusze – kurs zawiera realistyczne sytuacje, takie jak próby phishingu czy ataki socjotechniczne, pozwala to uczestnikom na praktyczne zastosowanie zdobytej wiedzy.
- ☑ Dostępność – szkolenie jest dostępne online, co umożliwia naukę w dowolnym miejscu i czasie.

ARKANET Wojciech Oleś, Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
32 787 48 88
handel@arkanet.pl
www.arkanet.pl

Kategoria I

Usługi zarządzania bezpieczeństwem.

Co możemy zaproponować i jakie są wyróżniki danych rozwiązań?

Dagma – SOC jako usługa

- ☑ Elastyczne podejście – firma Dagma podchodzi bardzo indywidualnie do każdego projektu. Od monitorowania zdarzeń w trybie 8x5, do pełnego monitoringu 24x7 wraz z pakietem godzin do wykorzystania (na szkolenia, testy phishingowe, pentesty, usługi IT itp.)
- ☑ Duży, zróżnicowany zespół – SOC DAGMA tworzy zespół specjalistów z wieloletnim doświadczeniem w dziedzinie cyberbezpieczeństwa, w tym analitycy na poziomach L1–L3, architekci, inżynierowie systemowi, pentesterzy oraz audytorzy. Ich wiedza i umiejętności gwarantują wysoką jakość świadczonych usług.
- ☑ Raporty i rekomendacje – klienci otrzymują cotygodniowe raporty ogólne oraz comiesięczne raporty szczegółowe dotyczące stanu bezpieczeństwa, wykrytych incydentów oraz rekomendowanych działań naprawczych.

ARKANET Wojciech Oleś, Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
32 787 48 88
handel@arkanet.pl
www.arkanet.pl

Kategoria J

Uwierzytelnianie i autoryzacja systemów.

Co możemy zaproponować i jakie są wyróżniki danych rozwiązań?

FORTINET – FortiToken, FortiAutenticator, FortiSase

- ☑ Centralizacja tożsamości – połączenie tokenów i autentykatora (współpracuje również z SASE) pozwala zachować jedno źródło uwierzytelniania dla całej organizacji (LDAP, AD, Radius itp).
- ☑ Polityki dostępu – szczegółowa kontrola kto i w jakich warunkach może uzyskać dostęp do zasobów.
- ☑ ZTNA (SASE) – dostęp przyznawany dynamicznie na podstawie tożsamości użytkownika i stanu urządzenia, nie tylko po IP.

SEGURA (SENHASEGURA)

- ☑ Nagrywanie – pełne rejestrowanie i odtwarzanie sesji (wideo + metadane komend).
- ☑ Automatyczna rotacja haseł – dynamiczna zmiana haseł i kluczy SSH/SSL po każdej sesji lub zgodnie z harmonogramem.

WALLIX BASTION

- ☑ Dostęp przez pośrednika – użytkownik nigdy nie zna hasła, loguje się wyłącznie przez PAM-a.
- ☑ Workflow Approval – zatwierdzanie dostępu z automatycznym nadawaniem i odbieraniem uprawnień na żądanie.

FUDO Security PAM

- ☑ Detekcja AI - analiza zachowania uczestnika podczas sesji, poprzez zachowania myszy, czy stosowanie nietypowych komend (możliwość przerwania w momencie wykrycia anomalii).
- ☑ Bezagentowe wdrożenie – brak agentów na serwerach i urządzeniach docelowych.

ARKANET Wojciech Oleś, Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
32 787 48 88
handel@arkanet.pl
www.arkanet.pl

Kategoria K

Audyt końcowy w obszarze Cyberbezpieczeństwa.

Co możemy zaproponować?

Specyfika

☑ Pełny audyt, zgodny z obszarami wskazanymi przez zamawiającego.

ARKANET Wojciech Oleś, Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
32 787 48 88
handel@arkanet.pl
www.arkanet.pl

Arkanet
Bezpieczeństwo to my

Masz pytania?
Chcesz porozmawiać?

Skontaktuj się ze swoim opiekunem handlowym w Arkanet

Napisz: handel@arkanet.pl

Zadzwoń: 32 787 48 88

ARKANET Wojciech Oleś, Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
32 787 48 88
handel@arkanet.pl
www.arkanet.pl