Zakres monitorowania: Zapytanie dotyczy - 17 serwerów z systemem operacyjnym Windows Server 2019-2025, 3 serwerów Linux, 3 urządzeń UTM fortigate i 1 Platformy MS Azure. Poniżej Państwo wypisują jednak również usługi poczty, czy usługi WWW – czy możemy prosić o doprecyzowanie zakresu?

Odp: na serwerach mogą być usługi poczty takie jak SMTP, usługi WWW czy np. IIS na której jest portal internetowy wewnętrzny lub zewnętrzny. Nie chodzi tutaj o monitorowanie exchange online i ruchu pocztowego

Czy mają Państwa zdefiniowany standardowy wzorzec zachowań, czy będą wykorzystywane mechanizmy cyberbezpieczeństwa?

Odp: nie mamy, wzorzec powinien być opracowany w ramach współpracy

Czy mają Państwo zdefiniowane dokumenty RFC, których dotyczy identyfikacja odchyleń od standardów sieci?

Odp: Nie

Jakie posiadają Państwo urządzenia do monitorowania wskazanych urządzeń w sieci, np. monitoringu wielkości ruchu generowanego przez urządzenia i stacje robocze, działania skanujące oraz działania wskazujące na działania złośliwe?

Odp: posiadamy antywirus Forticlient EMS nic po za tym

Czy posiadają Państwo urządzenie do monitoringu dostępności np. ZABIX?

Odp: tak, posiadamy zabbix

Jaki zakres monitoringu zdarzeń związanych z upublicznianiem danych związanych z konkretnymi numerami telefonów? Oraz o jakiej ilości numerów do monitoringu się spodziewamy?

Odp: do 150

Jaką liczbę domen chcą Państwo monitorować?

Odp: jedną

Co Państwo rozumią pod pojęciem wyodrębniania prawdziwych incydentów od false positive na podstawie Threat Intelligence?

Odp: false – fałszywe incydenty, true – prawdziwe incydenty. Chodzi o odróżnienie fałszywych od prawdziwych za pomocą mechanizmów sztucznej inteligencji

Czy implementacja pułapek wewnątrz sieci w celu wykrywania wewnętrznych zagrożeń oraz zbierania informacji o atakujących jest dla Państwa wymogiem, z którego możemy zrezygnować?

Odp: proszę przedstawić rozwiązanie alternatywne, jest to funkcja z której nie chcemy rezygnować

Monitorowanie dostępności urządzeń (w tym zgłaszanie braku dostępności oraz potencjalnej przyczyny – przy zapewnieniu logów z urządzeń) – czy zamawiający przewiduje wykorzystanie usługi NOC – network operations center

Odp: NOC nie jest przedmiotem zapytania, monitorujemy styk z sieciami publicznymi a nie urządzenia wewnątrz organizacji od tego jest dział informatyki

Czy monitoring kluczowych zdarzeń systemu operacyjnego hosta (wymagane jest ustalenie listy zdarzeń, które mają podlegać monitorowaniu oraz sposób zbierania zdarzeń z hostów) będzie realizowany przez XDR?

Odp: może być realizowany przez dowolne narzędzie, nie ograniczamy się do konkretnego narzędzia, proszę zaproponować

Okresowe skany inwentaryzacyjne oraz oceny podatności w wynikach skanów dla hostów końcowych (stacje robocze, serwery – wymaga instalacji agenta, konfiguracji urządzeń oraz konfiguracji dostępów i przepuszczania ruchu sieciowego). – Czy wymagają Państwo obligatoryjnie skanowania, którego wynikiem będzie inwentaryzacja sprzętu i oprogramowania, czy tylko podatności przeskanowanego środowiska?

Odp: w przedmiocie jest tylko 20 serwerów na których zakładamy że będzie zainstalowany agent który od czasu do czasu przeskanuje podatności, nie wymagamy inwentaryzacji

Czy mogą Państwa wytłumaczyć dlaczego monitoring w DarkWeb firmy Paged Morąg i jego Spółek zależnych znajduje się w wymaganiach?

Odp: błąd pisarki, chodzi o Zamawiającego

O jakiej liczbie domen Państwo myślą w kontekście monitorowania Dark Web?

Odp: jedna, nasza główna domena

O jakiej liczbie publicznych adresów IP Państwo myślą w kontekście monitorowania Dark Web?

Odp: 3

O jakiej liczbie konkretnych użytkowników Państwo myślą w kontekście monitorowania Dark Web?

Odp: do 150

Czy posiadają Państwo moduł SOAR?

Odp: nie

Informatyka śledcza, po incydencie pogłębiona analiza, mająca na celu ustalenie przyczyny, zasięgu i wpływu zagrożenia jest możliwa, ale wyceniania jest w trybie „time per material” – oznacza to, że nie jesteśmy wstanie jej wycenić nie znając potrzebnego czasu oraz narzędzi potrzebnych do oceny incydentu.

Odp: Zamawiający nie rozumie w jaki sposób Wykonawca zamierza świadczyć usługę bez narzędzi potrzebnych do oceny incydentu, w ofercie powinno być zawarte narzędzie które pozwala pogłębić analizę i ocenić wpływ zagrożenia

Czy szkolenie phisingowe musi zostać przeprowadzone przy pomocy platformy e-learningowej?

Odp: nie musi

Przygotowanie min. 6 szkoleń związanych z cyberbezpieczeństwem – czy posiadają państwo bardziej

szczegółowy zakres tych szkoleń?

Odp: nie posiadamy, każdy podmiot ma swój sposóļ na szkolenie z incydentów, prosimy w ofercie zawrzeć szczegóły szkoleń

Czy obligatoryjne jest aby treści szkoleniowe były w języku niemieckim?

Odp: nie, wymagany jest jezyk polski i angielski

Jaki ma być zakres czasowy usługi SOC?

Odp: czas określony 12miesięcy z przejściem na czas nie określony

Jaki ma być zakres czasowy ważności licencji XDR?

Odp: czas określony 12miesięcy z przejściem na czas nie określony

Czy wszystkie szkolenia mają być szkoleniami e-learningowymi?

Odp: nie

Ilu pracowników ma mieć dostęp do platformy e-learningowej?

Odp: 150

Czy dobrze rozumiem, że raz w roku ma być przeprowadzony phishing (1 scenariusz) i szkolenie elearningowe, a dodatkowo do przygotowania jest jeszcze jeden phishing wykorzystujący podszywający się pod prawdziwą www Zamawiającego portal?

Odp: tak

Czy dobrze rozumiem, że przygotowanie min. 6 szkoleń odnosi się do szkoleń dodatkowych, oprócz tego w póz. 1 - raz na rok?

Odp: w punkcie pierwszy nie ma określonej liczby szkoeń, jest jedna akcja phishingowe połączona ze szkoleniami w liczbie minimum 6 szkoleń, czyli każdy użytkownik dostaje dostęp do platformy w której ma 6 ścieżek szkoleniowych

Przygotowanie na żądanie treści wielojęzycznej szkoleń i phishingów - czy chodzi o wszystkie 6 lub 7

Odp: tak

szkoleń e-learningowych i 2 phishing oraz o cały serwis? Czy chodzi tylko o treści, czy również rozwiązania (e-platforma, www, maile)?

Odp: Zamawiający nie rozumie pytania, proszę doprecyzować, być może pozostałe pytania pozwolą uzyskać odpowiedź na pytanie Wykonawcy

Platforma nie pozwala na ceny opcjonalne, jak potraktować tę część z treściami po angielsku i niemiecku - czy wycenić w cenie głównej

Odp: niemiecki nie musi być, proszę dołączyć oddzielną ofertę jako załącznik