**OPIS PRZEDMIOTU ZAMÓWIENIA**

Usługa monitorowania, wykrywania i reagowania na cyberzagrożenia w zakresie realizacji I, II i III linii SOC wraz z dostawą narzędzi (SIEM, SOAR, XDR) do kompleksowego wykrywania, monitorowania, blokowania i usuwania zaawansowanych zagrożeń i ataków cybernetycznych wraz z możliwością wykonania automatycznie oraz manualnie działań naprawczych (ang. remediation).

W ramach usługi mają być dostarczone komercyjny systemy:

1. SIEM z SOAR
2. XDR

(lub systemy), których minimalne wymagania zostały wyspecyfikowane. W ramach świadczonej usługi Dostawca zapewni licencje niezbędne do realizacji usługi dla 100 punktów końcowych (komputerów i serwerów).

I. Przedmiot usługi:

Opis projektu

W związku z realizacją projektu pt. ”Zwiększenie cyberbezpieczeństwa Urzędu Miejskiego w Janikowie”, realizowanego w ramach programu Cyberbezpieczny Samorząd, zwracamy się z zapytaniem ofertowym.

Celem realizowanego projektu jest zwiększenie poziomu bezpieczeństwa informacji Urzędu Miejskiego w Janikowie. Projekt realizuje cel szczegółowy Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, Działanie 2.2 - Wzmocnienie Krajowego Systemu Cyberbezpieczeństwa w zakresie zapewnienia cyberbezpieczeństwa Urzędu poprzez budowę, rozwój oraz wdrożenie narzędzi służących do monitorowania bezpieczeństwa, zbierania, analizy i wymiany informacji o zagrożeniach, podatnościach i incydentach, a także poprzez rozwój kompetencji cyfrowych pracowników Urzędu w obszarze cyberbezpieczeństwa.

Przedmiotem zamówienia jest dostarczenie usługi monitorowania, wykrywania i reagowania na cyberzagrożenia w zakresie realizacji I, II i III linii SOC wraz z dostawą narzędzi (SIEM, SOAR, XDR) do kompleksowego wykrywania, monitorowania, blokowania i usuwania zaawansowanych zagrożeń i ataków cybernetycznych wraz z możliwością wykonania automatycznie oraz manualnie działań naprawczych (ang. remediation).

W ramach usługi ma być dostarczony Komercyjny System SIEM i SOAR oraz XDR (lub systemy), których minimalne wymagania są opisane w poniżej. W ramach świadczonej usługi Dostawca zapewni licencje niezbędne do realizacji usługi dla 100 punktów końcowych (komputerów i serwerów).

Zakres rzeczowy świadczonej usługi

* Realizowanie usługi 24h/7 dni w tygodniu przez 365 dni w roku;
* monitorowanie i analiza zdarzeń (logi systemowe, ruch sieciowy, zdarzenia z systemów bezpieczeństwa, informacje od administratorów);
* wykrywanie incydentów, klasyfikacja incydentów;
* reagowanie na incydenty – zdalnie;
* współpraca z zamawiającym w zakresie implementacji środków zaradczych;
* we współpracy z zamawiającym przywrócenie normalnego działania po ataku;
* wykonywanie skanów podatności – 4 razy w roku;
* monitorowanie sieci DarkWeb o w trybie online.

Słownik użytych pojęć

| Skrót lub Pojęcie | Opis |
| --- | --- |
| Best Effort | W ogólnym podejściu najlepsze możliwe działanie, dążenie do osiągnięcia celu. Stan realizacji usługi, w którym zostały przekroczone ograniczenia SLA ze względu na wystąpienie zwiększonego zapotrzebowania na usługę. W przypadku przekroczenia ograniczeń SLA Wykonawca niezwłocznie poinformuje Zamawiającego o zaistniałej sytuacji. |
| Cyberbezpieczeństwo | Adekwatny do potrzeb stan ochrony zapewniający możliwość wykrycia oraz reagowania na zdarzenia niepożądane oraz wskazane w dokumentacji systemu zarządzania bezpieczeństwem informacji Zamawiającego. |
| Cyberprzestrzeń | Przestrzeń, w której następuje wymiana, gromadzenie i udostępnianie informacji za pośrednictwem komputerów oraz komunikacja między człowiekiem i komputerem. |
| SOC | Security Operations Center – centrum operacji bezpieczeństwa, którego zadaniem jest całodobowe monitorowanie, zapobieganie, wykrywanie, badanie i reagowanie na zagrożenia cybernetyczne. |
| Czas Reakcji | Zagwarantowany przez Wykonawcę czas na podjęcie kroków zmierzających do usunięcia Incydentu |
| Czas Podjęcia | Zagwarantowany przez Wykonawcę czas od momentu zgłoszenia Incydentu do rozpoczęcia działań zmierzających do jego identyfikacji i oceny, poprzedza reakcję na Incydent. |
| Dzień roboczy | Od poniedziałku do piątku od 08.00 – 18.00 z wyłączeniem dni ustawowo wolnych od pracy oraz dni wolnych u Zamawiającego. |
| Praca ciągła | Praca w trybie 24/7/365 dni. |
| On-call | Dostępność konsultanta dyżurującego pod telefonem |
| Incydent Bezpieczeństwa  Informacji (Incydent) | Pojedyncze zdarzenie lub seria zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i/lub zagrażają bezpieczeństwu informacji. |
| Scenariusz Reakcji | Dokument opisujący wymagane czynności w przypadku wykrycia zdarzenia niepożądanego, składający się z:   * opisu możliwości technicznych wykrycia zdarzenia, * warunków wywołania zdarzenia niepożądanego, * opisu identyfikacji zdarzeń zależnych, * instrukcji reakcji na zdarzenie, * instrukcji uruchomienia działań korekcyjnych, * instrukcji wykonywania działań informacyjnych, * ogólnych i szczegółowych ścieżek eskalacyjnych. |
| Scenariusz użycia systemu bezpieczeństwa | * Dokument opisujący zestaw zadań wymaganych do wykonania w ramach Pierwszej i Drugiej Linii Wsparcia, w skład którego wchodzi m.in.: * skonfigurowanie jednego lub kilku źródeł zdarzeń; * opisanie procesu normalizacji; * przygotowanie Scenariuszy Reakcji w zakresie czynności wykonywanych przez Pierwszą Linię Wsparcia. |
| SLA | Zestaw wartości granicznych dla kluczowych wskaźników wydajności, dla których określona realizacja usługi jest wymagana w zakresie jakościowym. |

II.A Wymagania w zakresie świadczenia usługi

1. W zakresie pracy SOC
   1. Monitorowanie poprzez agentów oprogramowania XDR:

i. Stacji roboczych z systemami MS Windows, Linux

ii. Serwerów wirtualnych i fizycznych z systemami MS Windows Server i Linux

* 1. Monitorowanie poprzez zbieranie logów:

i. Urządzeń sieciowych (UTM, routerów, Firewalli, przełączników)

ii. Systemów aplikacyjnych (usługi pocztowej, usługi WWW, usługi AD, DHCP, DNS itp.)

iii. Systemów bezpieczeństwa (systemów AV, DLP, NAC itp.)

* 1. Zbieranie, agregacja, normalizacja i analiza niezbędnych dla świadczenia usługi monitorowania bezpieczeństwa danych, udostępnionych przez Zamawiającego.
  2. Identyfikację odchyleń od standardowego wzorca zachowań, na podstawie czego Wykonawca będzie dokonywał zgłoszeń do Zamawiającego (alertowania) wraz ze wskazaniem miejsca wystąpienia zdarzenia, określenia jak konkretne zdarzenie czy incydent może wpłynąć na Infrastrukturę Teleinformatyczną Zamawiającego.
  3. Identyfikację odchyleń od standardów pracy sieci i urządzeń, określonych dokumentami RFC (<https://pl.wikipedia.org/wiki/Request_for_Comments>).
  4. Działania realizowane podczas monitoringu zdarzeń przez operatorów I linii wsparcia Wykonawcy:

i. Monitorowanie zdarzeń i alertów w systemie monitorującym klasy SIEM;

ii. Wstępna analiza i klasyfikacja incydentów (triage);

iii. Priorytetyzacja incydentów i działań następczych;

iv. Uzupełnianie (Enrichment) zdarzeń o dane dodatkowe, w tym dane z baz danych o zagrożeniach.

* 1. Działania realizowane podczas monitoringu zdarzeń przez operatorów II linii wsparcia Wykonawcy:

i. Analiza zdarzeń i alertów w systemie monitorującym;

ii. Zaawansowana analiza incydentów;

iii. Wsparcie dotyczące obsługi incydentów przez Klienta;

iv. Analizy dotyczące bezpieczeństwa, źródeł i celów zagrożeń, problemów w infrastrukturze.

* 1. Opracowanie scenariusza mitygacji zagrożenia wynikającego z incydentu oraz wsparcie pracowników zamawiającego przy realizacji przygotowanego scenariusza – usługa realizowana zdalnie.
  2. Przygotowanie scenariusza działań naprawczych mających na celu usunięcie skutków incydentu.
  3. Opracowanie wniosków z incydentu, mających na celu ograniczenie możliwości powtórzenia się danego typu incydentu w przyszłości.
  4. Proponowanie nowych scenariuszy bezpieczeństwa do wdrożenia (nowych zabezpieczeń i działań zabezpieczających systemy) oraz propozycje optymalizacji aktualnie działających scenariuszy mitygacji incydentów.
  5. Proponowanie zabezpieczenia systemu przed przyszłymi podobnymi incydentami, identyfikowanie przyczyn problemu oraz jego ew. autorów, zebranie dowodów i wreszcie ewentualne powiadomienie odpowiednich służb, o ile jest to wskazane lub wymagane.
  6. Automatyczne reagowanie poprzez moduł SOAR systemu SIEM na wykryte zagrożenia i anomalie w zakresie urządzeń sieciowych i serwerów (blokada ruchu, blokada użytkownika, przeniesienie użytkownika/komputera do innej grupy AD itp.).
  7. Organizowanie co kwartalnych spotkań (z wykorzystaniem narzędzi wideokonferencyjnych), mających na celu podsumowanie wydarzeń z ostatniego kwartału oraz określeniu możliwości optymalizacji infrastruktury IT zamawiajacego.

1. W zakresie monitoringu sieci wewnętrznej:
   1. Monitorowanie wskazanych urządzeń w sieci, np. monitoring wielkości ruchu generowanego przez urządzenia i stacje robocze, działania skanujące oraz działania wskazujące na działania złośliwe;
   2. Monitorowanie zagrożeń na podstawie danych o potencjalnych atakujących i intruzach z wykorzystaniem posiadanego urządzenia przez Klienta klasy IDS/IPS/NIDS;
   3. Analiza dostępności (availability) wybranych kluczowych urządzeń.
2. W zakresie monitoringu styku z sieciami publicznymi:
   1. Monitorowanie ruchu przychodzącego z zewnątrz (źródło, cel, kto inicjował czy inicjował) w oparciu o dane z urządzeń brzegowych;
   2. Monitorowanie ruchu wychodzącego na zewnątrz (źródło, cel, kto inicjował czy inicjował) w oparciu o dane z urządzeń brzegowych;
   3. Monitorowanie i wykrywanie udostępnianych do sieci publicznej zasobów (otwarte porty, usługi, adresy i porty, wykrywanie zmian i dostępności);
   4. Monitoring VPN (wykrywanie anomalii – wymagane logi systemów VPN).
3. Monitoring hostów (stacje robocze, serwery, etc.):
   1. Monitorowanie dostępności urządzeń (w tym zgłaszanie braku dostępności oraz potencjalnej przyczyny – przy zapewnieniu logów z urządzeń);
   2. Monitoring kluczowych zdarzeń systemu operacyjnego hosta (wymagane jest ustalenie listy zdarzeń, które mają podlegać monitorowaniu oraz sposób zbierania zdarzeń z hostów);
4. Ocena podatności na ataki

Monitoring podatności (stacje robocze, serwery, urządzenia sieciowe, oprogramowanie na wskazanych hostach w tym oprogramowanie narzędziowe):

* 1. Okresowe skany podatności wskazanych komponentów infrastruktury (autoryzowane i nie autoryzowane – wymagana konfiguracja po stronie urządzeń, oraz konfiguracja dostępów i przepuszczania ruchu sieciowego);
  2. 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).

1. Analiza zachowań użytkowników

Oparta na badaniu działań użytkowników (UBA Verification) analiza zachowań użytkowników zapewnia możliwość upewnienia się, że osoby uzyskujące dostęp do zasobów organizacji są tym, za kogo się podają. Możliwości wykorzystywanego narzędzia pomagają identyfikować nieautoryzowane próby dostępu do sieci Klienta.

1. Raportowanie:
   1. Rodzaj zagrożeń
   2. Incydenty oraz sposoby mitygacji wynikających z nich zagrożeń
   3. Wykryte podatności i rekomendacje w zakresie ich usunięcia lub wprowadzone środki zaradcze, jeżeli podatności nie można wyeliminować
   4. Wykryte zagrożenia w infrastrukturze zamawiającego
   5. Znane podatności i zagrożenia pochodzące od producentów systemów, systemów bezpieczeństwa i jednostek CSIRT
   6. Alerty spływające ze wszystkich opisanych systemów muszą być prezentowane w jednym centralnym dashboardzie.
   7. Raportowanie w cyklach miesięcznych
2. Monitorowanie DarkWeb:
   1. Poszukiwanie i raportowanie wszystkich informacji związanych z UM w Janikowie i mających wpływ na jego bezpieczeństwo cybernetyczne.
   2. Upublicznienia danych związanych z domeną klienta (adresy mailowe, nazwy użytkowników, hasła dostępowe, inne informacje związane z domeną),
   3. Specyficznych informacji związanych z konkretnymi adresami mailowymi (adresami spoza domeny firmowej),
   4. Informacji związanych z publicznymi adresami IP używanymi przez klienta,
   5. Informacjami związanymi z konkretnymi użytkownikami po stronie klienta,
   6. Zdarzeń związanych z upublicznianiem danych związanych z konkretnymi numerami telefonów.
   7. Informacji o podobnych nazwach domen do domeny klienta (zakładanych m.ni. W celu przeprowadzenia akcji phisingowej lub wyłudzania danych, płatności).

II.B Poziom świadczenia usługi

Usługa monitorowania bezpieczeństwa jest świadczona przez SOC z następującymi minimalnymi poziomami SLA dla działań zespołu SOC.

* Pierwsza Linia Wsparcia

czasy dla pierwszych 75 Incydentów każdego dnia, pozostałe zadania realizowane w trybie „Best Effort”:

| Priorytet incydentu | Czas od wykrycia do | |
| --- | --- | --- |
| Podjęcia działania | Realizacji |
| Krytyczny/Wysoki | 15 min | 4 h |
| Średni | 60 min | 6 h |
| Niski | 2 h | 12 h |
| Informacyjny | 4 h | 24 h |

dostępność usługi w trybie 24/7/365.

* Druga Linia Wsparcia

czasy dla pierwszych Incydentów każdego dnia, jednak nie więcej niż 10, pozostałe zadania realizowane w trybie „Best Effort”:

| Priorytet incydentu | Czas od wykrycia do | |
| --- | --- | --- |
| Podjęcia działania | Realizacji |
| Krytyczny/Wysoki | 60 min | 24 h |
| Średni | 90 min | 2 dni |
| Niski | 2 h | 4 dni |
| Informacyjny | 4 h | 7 h |

dostępność usługi w dni robocze pomiędzy godzinami 8:00 a 18:00. Dodatkowo dla incydentów o priorytecie Wysokim - w trybie „on-call” w dni robocze w godzinach 00:00 do 8:00 i 18:00 do 24:00, w pozostałe dni w trybie „on-call” w godzinach 00:00 do 23:59.

* Trzecia Linia Wsparcia/Linia wsparcia producenta systemów użytych w usłudze MDR

czasy dla pierwszych Incydentów, jednak nie więcej niż 10, pozostałe zadania realizowane w trybie „Best Effort”:

| Priorytet incydentu | Czas od wykrycia do | |
| --- | --- | --- |
| Podjęcia działania | Realizacji |
| Krytyczny/Wysoki | 3h | 7 dni |

Gdzie poziom incydentu zdefiniowany jest następująco:

* Poziom KRYTYCZNY/WYSOKI:
  + Jest stosowany w przypadku wystąpienia na wskazanych zasobach lub zasobie mogącym przetwarzać lub przechowywać rekordy danych objętych definicją rozporządzenia RODO.
  + Jest stosowany w przypadku wystąpienia na wskazanych zasobach lub zasobie mogącym przetwarzać lub przechowywać rekordy danych objętych definicją tajemnicy przedsiębiorstwa.
  + Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadcząc o wystąpieniu co najmniej jednego wskaźnika.
  + Zestawienie zwrotnego kanału komunikacji z serwera dowodzenia i kontroli złośliwego oprogramowania (C&C) aktywnie wykorzystywanego (więcej niż 1kb/min).
  + Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych.
  + Nieautoryzowane dysponowanie uprawnieniami administracyjnymi.
  + Zidentyfikowane oraz potwierdzone naruszenie integralności plików konfiguracyjnych, binariów lub skryptów aplikacji i/lub systemu operacyjnego.
  + Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na ustanowienie tylnej furtki, podsłuchiwanie transmisji lub wykorzystanie podatności.
  + Ujawnienie wycieku danych z chronionego obszaru z wykorzystaniem protokołów mailowych, przesłanie na dyski webowe lub danych z wykorzystaniem nieautoryzowanych nośników przenośnych;
  + Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na utworzenie tylnej furtki, podsłuchu transmisji lub wykorzystania podatności;
  + Ujawnienie nieautoryzowanego kodu służącego jako oprogramowanie administracyjne (tzw. adminware) lub ofensywnych technik przełamywania zabezpieczeń (tzw. grayware);
  + Celowany atak na personel klienta z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym;
  + Wykrycie przez system antywirusowy oprogramowania złośliwego na zasobie realizującym funkcje systemu informacyjnego.
* Poziom ŚREDNI:
  + Zebrane dowody w systemach realizujących monitoring bezpieczeństwa zaświadczą o wystąpieniu co najmniej jednego wskaźnika.
  + Ujawnienie nieznanego przez VirusTotal lub przez inne bazy reputacyjne oprogramowania mającego złośliwe funkcje pozwalające operatorowi na uruchomienie nieautoryzowanych skryptów lub kodu.
  + Ujawnienie podatności systemów lub infrastruktury mających wartość CVSS powyżej 7.
  + Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych w strefie chronionej.
  + Wykrycie przez system antywirusowy oprogramowania złośliwego na zasobie realizującym funkcje systemu informacyjnego.
* Poziom NISKI:
  + Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego wskaźnika na systemie chronionym.
  + Częściowo personalizowany atak na personel klienta z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym.
  + Wszystkie przypadki wystąpienia na chronionych systemach komputerowych złośliwego oprogramowania, które jest rozpoznawane przez system antywirusowy ale nie zostało zatrzymane przez inny system bezpieczeństwa.
  + Wszystkie potwierdzone przypadki z naruszenia poufności, dostępności lub integralności wykryte przez systemy bezpieczeństwa dla których użytkownik wyklucza świadome działanie.
* Poziom INFORMACYJNY:
  + Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego wskaźnika.
  + Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu zdefiniowanego zdarzenia bezpieczeństwa opisanego scenariuszem reakcji, ale udało się potwierdzić, że wywołanie zdarzenia było efektem realizacji autoryzowanych czynności służbowych z pominięciem ustalonych procedur bezpieczeństwa.

II.B Dodatkowe wymagania na realizacje usługi

Z uwagi na fakt, iż, Zamawiający dysponuje zdefiniowanym budżetem na zadanie określone zostały poniższe wymagania:

1. Rozwiązanie XDR akceptowalne jest w modelu onpremis(wariant instalacji lokalnej) jak również z konsolą umieszczoną w chmurze w Europejskiej Przestrzeni Gospodarczej,
2. Rozwiązanie SIEM z SOAR wymagane jest w modelu onpremis.
3. Rozwiązanie XDR musi występować w magic quardrat Gartnera lub raporcie MITRE
4. Rozwiązanie SIEM i SOAR musi występować w raportach Gartnera,
5. Preferowane jest rozwiązanie all in one dla SIEM i SOAR,
6. Parametry świadczenia usługi:
   1. Ilość korelacji – bez ograniczeń,
   2. Ilość podłączonych źródeł danych – bez ograniczeń,
   3. Ilość przetwarzanych zdarzeń i incydentów w miesiącu - bez ograniczeń,
   4. Ilość przetwarzanych danych w systemie SIEM – bez ograniczeń,
   5. Ilość dostępnych w miesiącu godzin inżyniera – bez ograniczeń,
   6. Ilość godzin dla usług III linii SOC w miesiącu – bez ograniczeń,
7. Zakres objęty usługą:
   1. Liczba instytucji objętych usługą – 4 (Urząd Miasta, MGOPS, MGZO, OSiR)
   2. Liczba endpointów odjętych usługą – 100
   3. Liczba urządzeń sieciowych brzegowych – 4

* Styk zamawiającego z Internetem.
* Styk zamawiającego z innymi jednostkami i podmiotami nie korzystającymi z usług SOC.
* Sieć wewnętrzna Zamawiającego.
* Wszystkie urządzenia pracujące w sieci, które są wyposażone w agenta systemów zakupionych w ramach niniejszej usługi (stacje robocze, serwery fizyczne i wirtualne).
* Wszystkie systemy pracujące w sieci (urządzenia sieciowe, drukarki), z których logi mogą posłużyć do korelacji zdarzeń bezpieczeństwa.
* Dla aplikacji kupionych w modelu SaaS - zapewnienie bezpieczeństwa ruchu między aplikacją a infrastrukturą Zamawiającego w oparciu o agentów systemów zakupionych w ramach niniejszej usługi oraz urządzenia brzegowe Zamawiającego.
* Analiza zachowań użytkowników (wykrywanie niepożądanych zachowań użytkowników, podatność na socjotechniki).

**1.** Odpowiedzialność Wykonawcy

* Mitygacja zagrożeń i usunięcie skutków wywołanych przez incydent
* Uszkodzenie/usunięcie danych
* Kradzież danych
* Zaszyfrowanie danych
* Modyfikacja przelewów bankowych prowadząca do przywłaszczenia określonej kwoty
* Modyfikacja zobowiązań wpływająca na zmniejszenie wpływów lub zwiększenie należności
* Naruszenia polityk bezpieczeństwa, kradzież danych i inne incydenty wywołane przez własnych pracowników Wykonawcy

**2.** Wymagania co do harmonogramu wdrożenia:

Proces wdrożenia i uruchomienia usługi powinien ramowo składać się z następujących etapów i trwać nie dłużej niż 30 dni:

* Analiza środowiska Zamawiającego,
* Ustalenie scenariuszy działania i eskalacji dla poszczególnych incydentów,
* Instalacja i uruchomienie niezbędnych systemów,
* Szkolenie Personelu zamawiającego (do 4 osób),
* Uruchomienie produkcyjne.

II.C Minimalne wymagania na narzędzia XDR do świadczenia usługi

1. Wykorzystanie narzędzi posiadanych przez zamawiającego (UTM, WAF, AD, systemy monitorowania zamawiającego) do zwiększenia bezpieczeństwa realizowanej usługi
2. Dostarczenie pozostałych, niezbędnych narzędzi do zapewnienia bezpieczeństwa wraz z zarządzaniem całym cyklem życia tych narzędzi w tym: narzędzia SIEM wraz z modułem SOAR.
3. W obu przypadkach środowiska Sandbox (on-premise, cloud) koszty wszystkich wymaganych licencji winny być wliczone w cenę rozwiązania i nie powinny powodować konieczności ponoszenia dodatkowych opłat.
4. System wykorzystywany winien być licencjonowany jako subskrypcja na liczbę chronionych urządzeń/systemów końcowych bez rozróżnienia na typ chronionego hosta (serwer, stacja końcowa) oraz system operacyjny (Windows, Linux), koszty subskrypcji pokrywa Wykonawca.
5. Dostarczona w ramach usługi subskrypcja zawiera wszystkie opisane elementy funkcjonalne, nieograniczona liczbę instancji serwerów centralnych, wsparcie producenta wraz z usługa SOC producenta 24/7.
6. Minimalne parametry techniczne systemu SIEM i SOAR:

| 1. | w zakresie prewencji i detekcji zagrożeń w oparciu o logi z urządzeń |
| --- | --- |
| 1.2 | System działa w trybie zbliżonym do rzeczywistego |
| 1.3 | · System umożliwia funkcjonowanie bez dostępu do sieci Internet |
| 1.4 | · System ma możliwość działania jako niezależne instancje zainstalowane w oddziałach organizacji wraz z możliwością centralnego dostępu. |
| 1.5 | · Instancje systemu mają możliwość działania w przypadku odłączenia scentralizowanego dostępu. |
| 1.6 | · System zapewnia efektywną obsługę co najmniej 4000 EPS lub 80 GB danych dziennie |
| 1.7 | · System zapewnia retencję danych w okresie minimum 365 dni. |
| 1.8 | · Oferowana licencja nie ogranicza liczby zarejestrowanych lub jednoczesnych użytkowników systemu. |
| 1.9 | · System umożliwia rozbudowę bez potrzeby wyłączania lub restartu środowiska. |
| 1.10 | · Interfejs posiada angielską wersję językową. |
| 1.11 | · System zapewnia pełen audyt aktywności jego użytkowników, w tym: udanych/nieudanych logowań, pełną historię operacji, realizowanych zapytań, zmian uprawnień. |
| 1.12 | · System umożliwia ręczne ustawianie poziomu szczegółowości gromadzonych danych audytowych. |
| 1.13 | · System pozwala na tworzenie parserów z poziomu GUI |
| 1.14 | · System umożliwia predykcję danych w oparciu o dowolne dane historyczne zgromadzone w systemie. |
| 1.15 | · System zapewnia wizualizację danych w postaci, oryginalnych logów, list, wykresów i diagramów. |
| 1.16 | · Wizualizacja danych jest również możliwa dla wartości tekstowych jak i liczbowych przekazywanych w logach. |
| 1.17 | · System umożliwia funkcjonalność eksportu danych o Zdarzeniach i Incydentach do formatu CSV i HTML m.in. w celu analizy wyników działania reguł korelacyjnych. |
| 1.18 | · System zapewnia parsowanie spływających do niego wiadomości w formatach: |
| 1.18.1 | a. Syslog, |
| 1.18.2 | b. WEF, |
| 1.18.3 | c. Flat file, |
| 1.18.4 | d. Event log, |
| 1.18.5 | e. WMI, |
| 1.18.6 | f. XML, |
| 1.18.7 | g. JSON, |
| 1.19 | · System umożliwia prezentację logu o zdarzeniu w interfejsie użytkownika w takiej formie w jakiej ten log został przesłany do Systemu tj. wyświetlenie logu w postaci surowej (RAW) przed parsowaniem. |
| 1.20 | · System do przyjmowania zdarzeń wykorzystuje zarówno mechanizmy agentowe jak i bezagentowe. |
| 1.21 | · System umożliwia definiowanie parserów dla niestandardowych formatów logów w oparciu o składnię wyrażeń regularnych oraz formatów wymiany danych dla wszystkich obsługiwanych formatów. |
| 1.22 | · Interfejs umożliwia parsowanie warunkowe na podstawie dopasowania wartości pól. Po dopasowaniu wzorca dalsze parsowanie jest konfigurowalne w celu wyboru optymalnej metody parsowania, np.: REGEX, JSON, XML oraz umożliwia zastosowanie innego parsera. |
| 1.23 | · System posiada predefiniowany zestaw parserów zdarzeń. |
| 1.24 | · System wspiera geolokalizację zdarzeń na bazie adresów IP. |
| 1.25 | · System umożliwia normalizowanie wiadomości po sparsowanych polach, np. dzięki zmianie wartości tych pól oraz wzbogacaniu tych danych o dodatkowe pola bazując na całych wartościach lub wzorcach wyszukiwania. |
| 1.26 | · System umożliwia przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach. |
| 1.27 | · Proces parsowania umożliwia wzbogacanie treści obieranych Wiadomości poprzez matematyczne operacje wykonywane na innych polach. |
| 1.28 | · Proces parsowania umożliwia anonimizację Danych Wejściowych celem ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzny procedury bezpieczeństwa. |
| 1.29 | · System pozwala na rozpoznanie formatów czasu i daty oraz normalizowanie ich do jednego wspólnego formatu. |
| 1.30 | · System umożliwia łączenie wyników dwóch niezależnych zapytań w postaci jednej odpowiedzi, bez użycia składni SQL |
| 1.31 | · System posiada interfejs umożliwiający zmianę wybranej wartości w zgromadzonych danych. |
| 1.32 | · Incydent, który powstał w wyniku korelacji, daje się wyszukiwać korzystając ze standardowego dostępnego w systemie mechanizmu wyszukiwania. System umożliwia budowanie na jego podstawie kolejnych reguł korelacyjnych lub generowania alarmów. |
| 1.33 | · System posiada funkcjonalność korelacji danych w czasie rzeczywistym. |
| 1.34 | · System umożliwia tworzenie nowych reguł korelacyjnych oraz modyfikowanie istniejących. |
| 1.35 | · System umożliwia tworzenie własnych reguł korelacyjnych na bazie reguł odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie: |
| 1.35.1 | a. Wykrycia dowolnej treści w logach, |
| 1.35.2 | b. Wykrycia wystąpienia wartości pola na wybranej liście, |
| 1.35.3 | c. Wykrycia niewystępowania wartości pola na wybranej liście, |
| 1.35.4 | d. Wykrycia zmiany jednego z kilku pól, |
| 1.35.5 | e. Wykrycia zdarzeń występujących z zadaną częstotliwością, |
| 1.35.6 | f. Wykrycia zdarzeń, których liczba zmienia się w wskazany sposób względem czasu poprzedniego, |
| 1.35.7 | g. Wykrycia zaniku Wiadomości, |
| 1.35.8 | h. Wykrycia nowej wartości pola w zadanym okresie czasu, |
| 1.35.9 | i. Wykrycia incydentu będącego pochodną zdarzeń występujących w określonej kolejności |
| 1.36 | · System pozwala na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym. |
| 1.37 | · System pozwala na realizację zapytań obejmujących całą historię gromadzonych w nim danych |
| 1.38 | · Rozwiązanie posiada funkcjonalność wysyłania powiadomień o Incydentach do innych systemów bądź zdefiniowanych użytkowników (powiadamianie email, opcjonalnie SMS, czat). |
| 1.39 | · System umożliwia testowanie reguł korelacyjnych i alertów na etapie ich tworzenia. Wynik testu nie może tworzyć wpisu o sytuacji alarmowej i ewentualnego incydentu. |
| 1.40 | · Tworzone incydenty będące wynikiem pracy reguł bezpieczeństwa posiadają wbudowany poziom istotności. Jest możliwość modyfikacji poziomu istotności dla każdej reguły. |
| 1.41 | · Oferowana licencja nie ogranicza liczby urządzeń będących źródłem logów. |
| 1.42 | · System umożliwia czasowe przyjęcie zwiększonej ilości danych o minimum 30% bez potrzeby zwiększania zasobów sprzętowych lub licencyjnych. |
| 2. | w zakresie reakcji oraz remediacji |
| 2.1 | · Wykorzystanie posiadanego przez Zamawiającego oprogramowania EDR/XDR w zakresie reakcji i remediacji, w ramach posiadanych możliwości przez ten system, |
| 2.2 | · Wykorzystanie modułu SOAR wbudowanego w narzędzie SIEM do: |
| 2.2.1 | Remediacji związanych z zagrożeniami na urządzeniach sieciowych, |
| 2.2.2 | Remediacji związanych z zagrożeniami w Active Directory, |
| 2.2.3 | Remediacji związanych z innymi systemami bezpieczeństwa które posiada lub nabędzie zamawiający (do których system SIEM posiada interfejsy). |
| 3. | w zakresie raportowania |
| 3.1 | · Umożliwia generowanie raportów na podstawie zebranych danych, takich jak np.: |
| 3.1.1 | a. Alerty otwarte i zamknięte |
| 3.1.2 | b. Szczegółowe raporty związane z wykrytym ryzykiem |
| 3.1.3 | c. Trendy alertów, pokazujące podatne elementy w sieci w funkcji czasu |
| 3.1.4 | d. Najczęstsze typy alertów |
| 3.2 | · Możliwe do wygenerowania z Systemu raporty powinny zawierać informacje o poziomie ryzyka związanego z danym obiektem. |
| 3.3 | · Innego typu raporty uzgodnione z zamawiającym. |

1. Minimalne parametry techniczne systemu XDR:

| 1. | Wymagania w zakresie prewencji i detekcji zagrożeń: |
| --- | --- |
| 1.1. | Monitoruje i wizualizuje zagrożenia cybernetyczne w czasie rzeczywistym zarówno na fizycznych jak i wirtualnych komputerach użytkowników końcowych oraz serwerach. |
| 1.2. | Zapewnia ochronę przed znanym złośliwym oprogramowaniem na podstawie sygnatur. |
| 1.3. | Identyfikuje złośliwe oprogramowanie w oparciu o analizę zachowania aplikacji w czasie rzeczywistym. |
| 1.4. | Zapewnia ochronę przy wykorzystaniu statycznych mechanizmów uczenia maszynowego. |
| 1.5. | Wykorzystuje metadane (IOC) dostarczone przez producenta rozwiązania do analizy i wykrywania zagrożeń |
| 1.6. | Wykorzystuje metadane (IOC) dostarczone przez dział SOC do analizy i wykrywania zagrożeń. |
| 1.7. | Zapewnia możliwość prewencyjnego blokowania ataków oraz zagrożeń typu Memory Injection i Ransomware. |
| 1.8. | Umożliwia wykrywanie zdarzeń dotyczących bezpieczeństwa, pochodzących przynajmniej z niżej wymienionych obszarów w infrastrukturze informatycznej: |
| 1.8.1. | ruchu sieciowego, |
| 1.8.2. | urządzeń końcowych (stacje robocze oraz serwery), |
| 1.8.3. | zachowanie plików na urządzeniach końcowych, |
| 1.9. | Zachowanie użytkowników na urządzeniach końcowych. Zapewnia wykrywanie zagrożeń m.in. typu: |
| 1.9.1. | Malware |
| 1.9.2. | Trojan |
| 1.9.3. | Rootkit |
| 1.9.4. | MITM (Man in the Middle) |
| 1.9.5. | DLL Injection |
| 1.9.6. | Ransomware |
| 1.9.7. | Port Scanner Detection |
| 1.9.8. | Reflective DLL injection |
| 1.9.9. | Authentication spoofing (Pass the Hash/SMB Relay) |
| 1.9.10. | Mimikatz |
| 1.9.11. | Powershell Empire |
| 1.9.12. | Meterpreter |
| 1.9.13. | DNS Tunneling |
| 1.9.14. | ICMP Tunneling |
| 1.9.15. | Brute Force |
| 1.9.16. | Powersploit |
| 1.9.17. | ARP Poisoning |
| 1.9.18. | Raw Disk Writing |
| 1.10. | Ogranicza generowanie fałszywych alarmów z wykorzystaniem co najmniej poniższych metod: |
| 1.10.1. | Automatycznej weryfikacji wskaźników wykrytych zagrożeń w odniesieniu do wbudowanej bazy znanych zagrożeń, która jest na bieżąco uaktualniana za pośrednictwem dostępnego w chmurze producenta zestawu narzędzi, zawierających |
| 1.10.2. | Meta-skanowanie antywirusowe, wykorzystujące wszystkie silniki dostępne w bazie VirusTotal. |
| 1.10.3. | Wzorce schematów działania malware oraz bazy przykładowych kodów źródłowych (ang. Post Ex Sources) |
| 1.10.4. | Manualne oznaczanie poziomu ważności wykrytego zagrożenia na podstawie analizy przez zespół SOC. |
| 1.11. | Wykrywa nietypowe zachowania urządzeń, użytkowników oraz plików w sieci. |
| 1.12. | Zbiera wskaźniki kompromitacji (IOC) i zachowania z obszaru stacji końcowych, zachowania użytkowników, połączeń sieciowych oraz aktywności w systemie plików. |
| 1.13. | Posiada funkcjonalność samodzielnego „uczenia się” zachowań typowych w organizacji poprzez zbieranie i ustalenie wskaźników dotyczących zachowania monitorowanych elementów w lokalnej oraz rozległej sieci komputerowej. |
| 1.14. | Profilowanie typowych zachowań i odstępstw od nich |
| 1.15. | Umożliwia stworzenie tzw. „białych listy” (ang. White list) znanych i zaufanych plików na każdym monitorowanym urządzeniu w celu obniżenia poziomu fałszywych alarmów i poprawy wydajności działania całego rozwiązania. |
| 1.16. | Rozwiązanie posiada funkcjonalność szczegółowego skanowania zachowania konkretnego wykonywalnego pliku (\*.exe) na chronionej stacji. (bez udziału sandbox) |
| 1.17. | Rozwiązanie posiada funkcjonalność nadzoru pamięci zewnętrznych USB w zakresie: |
| 1.17.1. | Rozpoznania i blokowania urządzeń pamięci zewnętrznej USB |
| 1.17.2. | Tworzenia dopuszczonych w organizacji urządzeń USB (tzw. White List), które będą monitorowane i dopuszczone do użytkowania |
| 2. | Wymagania w zakresie mylenia atakującego (technologii Decoy): |
| 2.1. | Posiada wbudowany mechanizm pułapek (ang. Decoys) wspomagający wczesne wykrywanie nieznanych ataków oraz źródeł zagrożeń a także aktywności szpiegowskiej w infrastrukturze informatycznej w oparciu o obiekty: |
| 2.1.1. | Hostów (fałszywe usługi sieciowe, serwery i stacje końcowe) |
| 2.1.2. | Użytkowników |
| 2.1.3. | Plików |
| 3. | Wymagania w zakresie reakcji oraz remediacji: |
| 3.1. | Posiada możliwość wykonania manualnych i automatycznych działań naprawczych (ang. Remediation), niwelujących skutki ataków oraz zapobiegających podobnym zdarzeniom w przyszłości. |
| 3.2. | Wykrywanie w czasie rzeczywistym i automatyczne blokowanie na chronionych stacjach końcowych i serwerach poprzez analizę behawioralną m.in. zagrożeń typu: |
| 3.2.1. | Ransomware |
| 3.2.2. | Memory Injection |
| 3.3. | Rozwiązanie ma możliwość automatycznego zabicia (ang. kill) procesu, jeśli wykryje metodę ataku typu Memory Injection |
| 3.4. | Powiadamia o wykryciu zagrożenia na stacji końcowej poprzez wyświetlony komunikat, w panelu zarządzania (na konsoli zarządzającej) oraz drogą mailową oraz SMS na wskazaną skrzynkę pocztową lub nr telefonu i ma możliwość wysyłania logów do zewnętrznego systemu SIEM. |
| 3.5. | Posiada możliwość wykonania predefiniowanych akcji naprawczych (ang. Remediation) bezpośrednio na chronionych komputerach i serwerach, polegających na możliwości utworzenia reguł, które umożliwią usuwanie w sposób automatyczny każdego kolejnego zagrożenia o podobnym charakterze, z możliwością indywidualnego dostosowania sposobu reakcji systemu. |
| 3.6. | System umożliwia podjęcie automatycznej lub ręcznej akcji na minimum poniższych obiektach: |
| 3.6.1. | Plik (usuń plik, poddaj plik kwarantannie, zabij powiązany proces) |
| 3.6.2. | Host (zrestartuj hosta, wyłącz hosta, wyłącz wszystkie karty sieciowe, izoluj – zablokuj komunikację sieciową poza komunikacją związaną z działaniem Systemu, uruchom komendę) |
| 3.6.3. | Użytkownik (zablokuj użytkownika) |
| 3.6.4. | Sieci (blokuj ruch, przekieruj adres domenowy) |
| 3.7. | Rozwiązanie posiada możliwość konfiguracji automatycznego wysyłania nieznanych plików wykonywalnych do analizy w środowisku Sandbox. |
| 4. | Wymagania w zakresie badań poincydentowych oraz wyszukiwania zagrożeń: |
| 4.1. | Posiada możliwość przeprowadzania szczegółowych analiz po włamaniowych. Wspiera działania takie jak przeszukiwanie drzew procesów biorących udział w incydencie. Wspiera wyszukiwanie w organizacji plików biorących udział w incydencie np. poprzez wynik funkcji skrótu MD5. |
| 4.2. | Posiada możliwość wysłania podejrzanych plików do wykonania w sandbox producenta lub w infrastrukturze lokalnej. |
| 4.3. | Posiada możliwość wysłania podejrzanych plików do SOC producenta w trybie 24/7 celem analizy, oceny ryzyka oraz zalecanych działań naprawczych. |
| 4.4. | Umożliwia badanie zdarzeń dotyczących bezpieczeństwa, pochodzących przynajmniej z niżej wymienionych obszarów w infrastruktury informatycznej: |
| 4.4.1. | ruchu sieciowego, |
| 4.4.2. | urządzeń końcowych (stacje robocze oraz serwery), |
| 4.4.3. | zachowanie plików na urządzeniach końcowych, |
| 4.4.4. | zachowanie użytkowników. |
| 4.5. | Zbiera wskaźniki kompromitacji (IOC) i zachowania z obszaru stacji końcowych, zachowania użytkowników, połączeń sieciowych oraz aktywności w systemie plików. |
| 4.6. | W zakresie wsparcia analiz po włamaniowych i prowadzenia dochodzeń (and. Forensics) system umożliwia przeszukiwanie IOC w powiązaniu z minimum poniższymi obiektami: |
| 4.6.1. | Pliki, |
| 4.6.2. | Hosty, |
| 4.6.3. | Użytkownicy, |
| 4.6.4. | Połączenia sieciowe (zarówno w oparciu o adresy domenowe jak i adresy IP), |
| 4.7. | Rozwiązanie w obszarze wsparcia zaawansowanych analiz i przeszukiwania danych powinno umożliwiać przeszukiwanie zdarzeń dotyczących obiektów plikowych poprzez minimum: |
| 4.7.1. | nazwa pliku z poniższymi parametrami: |
| 4.7.1.1. | Rozpoczyna się od |
| 4.7.1.2. | Kończy się na |
| 4.7.1.3. | Zawiera |
| 4.7.1.4. | Nie Zawiera |
| 4.7.1.5. | Jest równy |
| 4.7.1.6. | Nie równa się |
| 4.7.2. | Poziom przypisanego ryzyka w postaci liczbowej: |
| 4.7.2.1. | większy niż |
| 4.7.2.2. | mniejszy niż |
| 4.7.2.3. | równy |
| 4.7.3. | wystąpienia pliku: |
| 4.7.3.1. | mniej niż |
| 4.7.3.2. | więcej niż |
| 4.7.3.3. | równe |
| 4.7.4. | pierwsze zarejestrowanie pliku: |
| 4.7.4.1. | Od data |
| 4.7.4.2. | Do data |
| 4.7.4.3. | Dnia (określony dzień) |
| 4.7.4.4. | W ciągu ostatnich (minut) |
| 4.7.5. | ostatnie zarejestrowanie pliku: |
| 4.7.5.1. | Od data |
| 4.7.5.2. | Do data |
| 4.7.5.3. | Dnia (określony dzień) |
| 4.7.5.4. | W ciągu ostatnich (minut) |
| 4.7.6. | Binarny atrybut (tak/nie) czy plik jest uruchamiany automatycznie (autostart) |
| 4.7.7. | Binarny atrybut (tak/nie) czy plik ukrywa swoje okno |
| 4.7.8. | Binarny atrybut (tak/nie) czy plik występuje w folderze typu „program files” |
| 4.7.9. | Binarny atrybut (tak/nie) czy plik otwiera połączenia sieciowe |
| 4.7.10. | Binarny atrybut (tak/nie) czy plik uruchamia się także w nocy |
| 4.7.11. | Binarny atrybut (tak/nie) czy plik występuje w folderze System32 |
| 4.7.12. | Binarny atrybut (tak/nie) czy plik występuje w folderach tymczasowych |
| 4.7.13. | Adres IP z którym się komunikuje ( poprzez podanie adresu IP ) |
| 4.7.14. | Rozmiar pliku |
| 4.7.15. | Funkcję skrótu MD5 |
| 4.7.16. | Funkcję skrótu SHA256 |
| 4.8. | Informacje o zebranych plikach zawiera minimum korelację dotyczące powiązanych obiektów: |
| 4.8.1. | Procesy potomne, |
| 4.8.2. | Typ procesu (np. usługa, proces, załadowany moduł), |
| 4.8.3. | Użytkownicy, w których kontekście był uruchamiany plik, |
| 4.8.4. | Powiązany ruch sieciowy (zarówno w kontekście adresów IP oraz portów jak i nazw domenowych), |
| 4.8.5. | Załadowanych bibliotek dll, |
| 4.8.6. | Powiązanych operacjach w systemie plików, przynajmniej utworzenie pliku, uruchomienie pliku, usunięcie lub zmiana nazwy, |
| 4.9. | Rozwiązanie umożliwia przeszukiwanie oraz wyświetlanie szczegółowych danych dotyczących hostów, które obejmują minimum: |
| 4.9.1. | Nazwa hosta z filtrowaniem z poniższymi parametrami: |
| 4.9.1.1. | Rozpoczyna się od |
| 4.9.1.2. | Kończy się na |
| 4.9.1.3. | Zawiera |
| 4.9.1.4. | Nie Zawiera |
| 4.9.1.5. | Jest równy |
| 4.9.1.6. | Nie równa się |
| 4.9.2. | Poziom przypisanego ryzyka w postaci liczbowej z poniższymi parametrami: |
| 4.9.2.1. | większy niż |
| 4.9.2.2. | mniejszy niż |
| 4.9.2.3. | równy |
| 4.9.3. | Data ostatniego skanowania hosta, |
| 4.9.4. | Adres IP hosta, |
| 4.9.5. | Wersja systemu operacyjnego, |
| 4.9.6. | Liczba procesów wykrytych na hoście, |
| 4.9.7. | Liczba i dane użytkowników, którzy logowali się na hoście, |
| 4.9.8. | Liczba i szczegóły połączeń sieciowych wykrytych na hoście, |
| 4.9.9. | Informacje o bieżącym obciążeniu hosta minimum w zakresie: |
| 4.9.9.1. | CPU, |
| 4.9.9.2. | Pamięć (całkowita, wolna), |
| 4.9.9.3. | Dysk systemowy (rozmiar całkowity, wolna przestrzeń), |
| 4.9.10. | Informacje o wykorzystywanych portach, |
| 4.9.11. | Zainstalowane certyfikaty, |
| 4.9.12. | Zainstalowane aktualizacje systemu (preferowane wskazanie KBxxxxxxxx), |
| 4.9.13. | Zainstalowane oprogramowanie wraz z wersją, |
| 4.9.14. | Udziały sieciowe. |
| 4.10. | System wspiera przeszukiwanie użytkowników wykrytych na hostach, poprzez minimum poniższe atrybuty: |
| 4.10.1. | Nazwa użytkownika |
| 4.10.2. | Poziom ryzyka związany z danym użytkownikiem |
| 4.10.3. | Status blokady konta (zablokowane/nie zablokowane) |
| 4.10.4. | Status konta (włączone/wyłączone) |
| 4.10.5. | Ilość otwartych plików przez użytkownika |
| 4.10.6. | Wiek hasła użytkownika |
| 4.10.7. | Data ostatniego logowania |
| 4.10.8. | Data pierwszego logowania (zarejestrowanego przez system) |
| 4.10.9. | Ilość komputerów, do których logował się użytkownik w ostatnim czasie (dzień wcześniej, w ostatnim tygodniu, w ostatnim miesiącu, w ostatnich 3 miesiącach, całkowita ilość). |
| 4.10.10. | Ilość prawidłowych logowań |
| 4.10.11. | Ilość błędnych logowań |
| 4.10.12. | Nazwa hosta na którego jest zalogowany |
| 4.11. | Narzędzie umożliwia zapisanie filtrów wyszukiwania do późniejszych analiz. |
| 4.12. | System zawiera informacje o otwartych portach i połączeniach sieciowych realizowanych na monitorowanych hostach oraz umożliwiać przeszukiwanie ich minimum poprzez: |
| 4.12.1. | Adres IP hosta |
| 4.12.2. | Port Lokalny |
| 4.12.3. | Adres IP zdalny (publiczny/prywatny) |
| 4.12.4. | Port Zdalny |
| 4.12.5. | Data i czas pierwszego wystąpienia |
| 4.12.6. | Data i czas ostatniego wystąpienia |
| 4.13. | Rozwiązanie posiada możliwość ręcznego wysyłania nieznanych plików wykonywalnych do analizy w środowisku Sandbox. |
| 4.14. | System posiada możliwość wyszukania dowolnej frazy w pamięci operacyjnej chronionych systemów. |
| 5. | Wymagania w zakresie zapewnienia wysokiej dostępności, skalowalności oraz wsparcia infrastruktury rozproszonej oraz architektury: |
| 5.1. | Umożliwia instalowanie hierarchicznych instancji serwerów zarządzania systemem w układzie Master-Slave, które zapewniają również separację wielu domen administracyjnych (tzw. multitenant). |
| 5.2. | System nie ogranicza licencyjnie liczby instancji serwerów zarządzania zarówno głównych (Master) jak i zależnych (Slave), które mogą być wdrażane w infrastrukturze zarówno lokalnej jak i rozproszonej. |
| 5.3. | Rozwiązanie winno posiadać możliwość konfiguracji lokalnego środowiska Sandbox oraz wykorzystania środowiska. |
| 6. | Wymagania w zakresie wspieranych platform: |
| 6.1. | Oprogramowanie systemu umożliwia instalację na serwerach fizycznych oraz wirtualnych w środowisku Windows Server 2012 R2 (wersja angielska) lub nowszych oraz mechanizmów wirtualizacji Hyper-V, VMware. |
| 6.2. | System umożliwia monitorowanie i ochronę m.in. następujących systemów operacyjnych: |
| 6.2.1. | Windows – od wersji XP SP3 |
| 6.2.2. | Windows Server – od wersji Windows 2008 R2 |
| 6.2.3. | Linux – co najmniej Fedora, CentOS, RedHat, Suse, Debian, Ubuntu, OracleLinux |
| 6.2.4. | MacOSX – co najmniej El Capitan |
| 7 | Wymagania w zakresie ochrony nadmiernego wykorzystania zasobów na ochranianych hostach: |
| 7.1. | Rozwiązaniu umożliwia wybranie predefiniowanego maksymalnego poziomu obciążania CPU na monitorowanej i chronionej stacji, co najmniej w zakresie zajętości pamięci operacyjnej. Ustawienie maksymalnej zajętości pamięci operacyjnej powinno być definiowane procentach. |
| 8. | Wymagania w zakresie instalacji i wdrażania Systemu: |
| 8.9. | System umożliwia zdefiniowanie hostów do automatycznej instalacji agenta minimum poprzez: |
| 8.9.1. | Adres IP, |
| 8.9.2. | Zakres adresów IP, |
| 8.9.3. | OU hosta z Active Directory. |
| 8.10. | Instalacja agenta powinna wymagać jedynie uprawnień na poziomie lokalnego administratora stacji końcowej. |
| 8.11. | Monitorowanie stacji powinno działać minimum w 3ch trybach: |
| 8.11.1. | Interwałowym – połączenie w celu przeskanowania monitorowanego hosta jest inicjowane przez serwer centralny w określonych interwałach czasowych i nie wymaga instalacji na stałe żadnego oprogramowania na systemie końcowym. Po przeskanowaniu proces jest usuwany z pamięci operacyjnej. |
| 8.11.2. | Agenta ulotnego – po każdorazowym uruchomieniu hosta serwer centralny implementuje oprogramowanie agenta monitorującego w pamięci operacyjnej. Agent działa do momentu restartu chronionego systemu. |
| 8.11.3. | Normalnego Agenta – oprogramowanie monitorujące jest instalowane jako usługa uruchomiona w postaci rezydentnego procesu w pamięci operacyjnej urządzenia końcowego. |
| 8.12. | Agent na hoście działa z uprawnieniami „LocalSystem” w celu minimalizacji ew. konfliktów z innymi systemami zainstalowanymi na tym samym systemie operacyjnym w obszarach takich jak sterowniki, itp. |
| 8.13. | System umożliwia dystrybucję agentów służących do ochrony stacji końcowych przynajmniej za pomocą następujących mechanizmów: |
| 8.13.1. | Wbudowane mechanizmy Microsoft – TCP 445 |
| 8.13.2. | SSH – port 22 |
| 8.13.3. | Scheduled Tasks dla systemów Windows |
| 8.13.4. | RPC |
| 8.13.5. | Poprzez pliki .msi |
| 9. | Wymagania w zakresie współpracy z innymi platformami: |
| 9.1. | Zapewnia możliwość przyjęcia kopii ruchu sieciowego przy wykorzystania SPAN portu lub TAP-a. |
| 9.2. | Umożliwia wysyłanie informacji do narzędzi klasy SIEM przy użyciu szyfrowanego protokołu UDP lub TCP |
| 9.3. | Umożliwia wysyłanie do narzędzia klasy SIEM zdarzeń z urządzeń końcowych (alarmów) oraz zdarzeń audytowych serwera Cynet. |
| 9.4. | Umożliwia integrację z zewnętrznymi systemami i narzędziami za pośrednictwem pełnego REST API. |
| 9.5. | System umożliwia zdalną w pełni automatyczną instalację agenta monitorującego stacje końcowe. |
| 9.6. | System umożliwia korelowanie i parsowanie danych z zewnętrznych systemów (np. firewall, proxy, inne komponenty sieci IP) w celu wzbogacenia zebranych danych. |
| 10. | Wymagania w zakresie raportowania: |
| 10.1. | Koreluje minimum następujące elementy aktywności na hoście w celu oceny poziomu zagrożenia w postaci liczbowej odrębnie dla każdego hosta, pliku, użytkownika oraz zewnętrznych adresów IP: |
| 10.1.1. | wskaźniki kompromitacji (IOC) |
| 10.1.2. | zachowania w zakresie połączeń sieciowych |
| 10.1.3. | aktywności procesów |
| 10.1.4. | aktywności użytkownika |
| 10.1.5. | aktywności w ramach systemu plików |
| 10.2. | Umożliwia generowanie raportów na podstawie zebranych danych, takich jak np.: |
| 10.2.1. | Alerty otwarte i zamknięte |
| 10.2.2. | Szczegółowe raporty związane z wykrytym ryzykiem |
| 10.2.3. | Trendy alertów, pokazujące podatne elementy w sieci w funkcji czasu |
| 10.2.4. | Najczęstsze typy alertów |
| 10.3. | Możliwe do wygenerowania z Systemu raporty powinny zawierać informacje o poziomie ryzyka związanego z danym obiektem. |
| 10.4. | Rozwiązanie powinno umożliwiać generowanie raportów w postaci plików (csv lub excel) oraz widoków dla obiektów plikowych, zawierających minimum: |
| 10.4.1. | Nazwę pliku |
| 10.4.2. | Powiązaną ocenę ryzyka w postaci liczbowej |
| 10.4.3. | Nazwę twórcy (publisher) |
| 10.4.4. | Liczba stacji roboczych na których dany plik występuje |
| 10.4.5. | Nazwa produktu |
| 10.4.6. | Binarny atrybut (tak/nie) czy plik jest uruchamiany automatycznie (autostart) |
| 10.4.7. | Binarny atrybut (tak/nie) czy plik ukrywa swoje okno |
| 10.4.8. | Binarny atrybut (tak/nie) czy plik występuje w folderze typu „program files” |
| 10.4.9. | Binarny atrybut (tak/nie) czy plik otwiera połączenia sieciowe |
| 10.4.10. | Binarny atrybut (tak/nie) czy plik uruchamia się także w nocy |
| 10.4.11. | Binarny atrybut (tak/nie) czy plik występuje w folderze System32 |
| 10.4.12. | Binarny atrybut (tak/nie) czy plik występuje w folderach tymczasowych |
| 10.4.13. | Adres IP z którym się komunikuje |
| 10.4.14. | Rozmiar pliku |
| 10.4.15. | Funkcję skrótu MD5 |
| 10.4.16. | Funkcję skrótu SHA256 |
| 10.5. | Koreluje w centralnej konsoli minimun następujące elementy: informacje z agentów dostarczonych systemów, logów ze stacji roboczych i serwerów logów z urządzeń sieciowych (przełączniki, firewalle, umt, itp.) |
| 11. | Wymagania w zakresie interfejsu użytkownika/administratora: |
| 11.1. | Zapewnia dostęp do panelu operatorskiego przez zwykłą przeglądarkę (GUI webowe). |
| 11.2. | Wyświetla dodatkowe informacje związane z alertami, m.in.: opis zdarzenia, zalecenia dotyczące usunięcia przyczyn alertu oraz wszystkie powiązane ze zdarzeniem obiekty (hosty, użytkowników, pliki i adresy IP). |
| 11.3. | Posiada panel informacyjny, w którym są wyświetlane informacje o statusie podatności monitorowanych urządzeń końcowego, alertach, skanowaniach i przeprowadzonych analizach. |
| 11.4. | Na konsoli operatorskiej wyświetlane są wygenerowane przez system aktywne alerty oraz status skompromitowania poszczególnych urządzeń końcowych. |
| 11.5. | Wyświetla informacje potrzebne podczas analizy dokonywanej po incydentach w zakresie informacji o plikach, użytkownikach, stacjach i ruchu sieciowym. |
| 11.6. | Wyświetla informacje o wykonanych akcjach naprawczych. |
| 11.7. | Wskazuje listę chronionych hostów z informacją o aktualnym stanie ich ochrony. Przypisuje poziom ryzyka hostom wyrażony w postaci liczbowej na podstawie powiązanych z danym hostem zdarzeniami/anomaliami. |
| 11.8. | Zapewnia ogólny widok z poziomu panelu konsoli do zarządzania (ang. dashboard), pokazujący aktualny pogląd sytuacyjny, zawierający przynajmniej liczbę otwartych alertów w podziale na monitorowane obszary takie jak: pliki, użytkownicy, stacje i komunikacja sieciowa. |
| 11.9. | Wykryte alerty powinny być dodatkowo opisywane kolorem wskazującym na ich ważność za pomocą zróżnicowania kolorystycznego, przy czym alerty krytyczne powinny być wyświetlane zgodnie z branżowymi standardami na czerwono, a alerty o średnim poziomie krytyczności w kolorze pomarańczowo/żółtym. Zdarzenia o niższym poziomie mają być wyświetlane w odcieniach zieleni lub niebieskiego. |
| 11.10. | Umożliwia umieszczenie i prezentację systemów wg ich lokalizacji geograficznej i odpowiadających im alertów na mapie. |
| 11.11. | Umożliwia dynamiczne wyświetlanie poziomu alertów dla każdej z lokalizacji wyświetlonych na mapie. Alerty są wyświetlane dynamicznie w zależności od poziomu zagrożenia/kompromitacji. Dostęp do szczegółów alertów powinien być możliwy bezpośrednio po kliknięciu na alert umieszczony na wyświetlanej mapie. |
| 11.12. | Posiada widok prezentujący liczbę alertów na wykresie czasowym, zawierającym liczbę alertów wygenerowanych w poszczególnych dniach w podziale na monitorowane obszary w tym minimum na: hosty, pliki, użytkowników oraz ruch sieciowy. |
| 11.13. | Dostępne w systemie widoki powinny pozwalać zarządzać alertami i posiadać listy alertów w podziale minimum na: otwarte, zamknięte, oznaczone do ignorowania przez operatora systemu. |
| 11.14. | Użytkownik administrator może tworzyć nowe reguły oceny ryzyka w oparciu o metadane na hostach. |
| 11.15. | W ramach działań forensic system powinien prezentować powiązane obiekty do aktualnie wybranego w postaci przynajmniej uproszczonej (zminimalizowanej) linii czasowej z listą informacji dystynktywnych dla danego typu obiektu. |
| 11.16. | System zapewnia graficzną wizualizację informacji o użytkowniku, ułożoną na linii czasowej, która zawiera informacje o wykrytych zdarzeniach związane z zachowaniem danego użytkownika. |
| 11.17. | System zawiera graficzną reprezentację powiązań użytkownika z innymi obiektami w środowisku. Powiązania hosta z innymi obiektami obejmują m.in. wykaz plików na danym hoście, połączenia z zewnętrznymi adresami IP, innymi hostami w sieci wewnętrznej oraz użytkowników logujący się do danego hosta. |
| 11.18. | System zapewnia informacje o domenach, do których były zapytania z monitorowanych hostów. |
| 11.19. | System powinien generować automatycznie listę domen z którymi występowała komunikacja, która zawiera przynajmniej poniższe informacje: |
| 11.19.1. | Nazwa Internetowa domeny |
| 11.19.2. | Poziom ryzyka związany z domeną |
| 11.19.3. | Klasyfikacja domeny (biała lista, brak klasyfikacji) |
| 11.19.4. | Data i czas, kiedy po raz pierwszy wystąpiła komunikacja z domeną |
| 11.19.5. | Data i czas, kiedy po raz ostatni wystąpiła komunikacja z domeną |
| 11.19.6. | Liczba hostów komunikujących się z daną domeną |
| 11.19.7. | Liczba adresów IP rozwiązywanych pod daną domeną |
| 11.19.8. | Liczba lokalnych adresów IP łączących się z daną domeną |
| 11.19.9. | Liczba użytkowników łączących się z daną domeną |
| 11.20. | Dla listy inwentaryzacyjnej połączeń monitorowane są m. in. pola: |
| 11.20.1. | Nazwy hostów związanych z ruchem sieciowym |
| 11.20.2. | Poziom ryzyka związany z danym połączeniem |
| 11.20.3. | Lokalny adres IP związany z ruchem sieciowym |
| 11.20.4. | Lokalny port źródłowy |
| 11.20.5. | Docelowe IP związane z ruchem sieciowym |
| 11.20.6. | Port docelowy związany z ruchem sieciowym |
| 11.20.7. | Data i czas, kiedy po raz pierwszy dany ruch sieciowy był widoczny |
| 11.20.8. | Data o czas, kiedy po raz ostatni dany ruch sieciowy był widoczny |
| 11.21. | Rozwiązanie z interfejsu administratora winno umożliwiać automatyczne tworzenie na urządzeniach końcowych fałszywych obiektów, tzw. pułapek (ang. Decoy), których zadaniem jest wprowadzanie atakujących w błąd. Zestaw pułapek winien być automatycznie generowany z poziomu serwera centralnego i nie wymaga manualnego przygotowania na hostach. Włączanie i wyłączanie funkcjonalności Decoy winno być dostępne z poziomu konsoli administratora systemu. |
| 11.22. | System winien posiadać możliwość gradacji poziomu dostępu do konsoli administracyjnej w sposób granularny wraz z możliwością tworzenia własnych poziomów dostępu. |
| 11.23. | Rozwiązanie winno posiadać możliwość włączenia i wyłączenia określonych reguł korelacyjnych (alertów) minimum dla poniższych typów zdarzeń: |
| 11.23.1. | Skanowanie portów |
| 11.23.2. | Zatruwanie tablic ARP |
| 11.23.3. | Atak typu Pass the Hash |
| 11.23.4. | Wykrycie Mimikatz |
| 11.23.5. | Wykrycie Powershell Empire |
| 11.23.6. | Zdarzenia administracyjne związane z VSS |
| 11.23.7. | Tunelowanie DNS |
| 11.23.8. | Tunelowanie ICMP |
| 11.23.9. | Atak Brute Force |
| 11.23.10. | Wykrycie narzędzi Hackerskich |
| 11.23.11. | Wykrycie narzędzi do zdalnego dostępu |
| 11.23.12. | Wykrycie Trojana |
| 11.23.13. | Wykrycie tunelowania Http |
| 11.23.14. | Alerty związane wykorzystaniem NetBIOS (np. atak LLMNR) |
| 11.24. | System winien umożliwiać wyświetlanie w konsoli operatorskiej także tych alertów, które zostały przejrzane i zostały zamknięte przez operatora systemu. |
| 11.25. | Lista alertów winna być możliwa do wyeksportowania m.in. w formacie Excel (\*.xlsx). |
| 11.26. | System winien umożliwiać integrację z Active Directory w celu autoryzacji użytkowników konsoli administracyjnej/operatorskiej. |
| 11.27. | System winien posiadać widoki dostarczające informacje z zakresu Vulnerability Management tj. Minimum: |
| 11.27.1. | Listę zainstalowanych poprawek Windows |
| 11.27.2. | Lista nieautoryzowanych Aplikacji |
| 11.27.3. | Walidacja wersji wybranych Aplikacji |
| 11.27.4. | Walidacja wersji Agenta Systemu |
| 11.28. | System powinien posiadać możliwość anonimizacji minimalnie nazwy Hosta i nazwy użytkownika dla danych wysyłanych do SOC |