*Załącznik nr 1a*

***Szczegółowy zakres i wytyczne procesu wdrożenia systemu***

1. Proces wdrożenia systemu określony w Etapie I powinien zostać zrealizowany zgodnie z opisanymi niżej wytycznymi, umożliwiając efektywne wdrożenie rozwiązania.

2. Proces wdrożeniowy podzielony zostanie są na 3 obszary:

 a. Obszar Analizy, zakładający stworzenie elektronicznej dokumentacji organizacji wraz z podłączeniem i skonfigurowaniem mechanizmów szacowania ryzyka pod kątem kluczowych zasobów IT i procesów organizacji (budowa kontekstu organizacji);

 b. Obszar Detekcji, zakładający podłączenie i konfigurację narzędzi odpowiedzialnych za wykrywanie zdarzeń i incydentów bezpieczeństwa w ramach zainstalowania modułu SIEM;

 c. Obszar Reakcji, zakładający podłączenie i konfigurację mechanizmów wspomagających proces automatyzacji reakcji na wykryte zdarzenia, incydenty bezpieczeństwa i podatności w ramach zainstalowania modułu SOAR.

3. Obszar Analizy ma na celu identyfikację potencjalnych cyber zagrożeń oraz możliwych konsekwencji na jakie narażona jest organizacja. Zakres prac powinien uwzględniać kolejno:

 a. Pracę z konsultantem (w zakresie m.in. wprowadzenia do metodyki oraz uzupełnienia ankiety przedwdrożeniowej);

 b. Uruchomienie systemu w infrastrukturze zamawiającego, w tym:

 • konsultacje w przygotowaniu infrastruktury zamawiającego do instalacji systemu,

 • instalację lub import maszyny wirtualnej typu „software appliance”,

 • zestawienie połączenia zdalnego,

 • aktywację licencji,

 • wstępną konfigurację,

 • import/wprowadzenie tabeli adresacji znaczących stref bezpieczeństwa, wymaganych przez mechanizmy wykrywania (np.: sieci serwerów, sieci DMZ, sieci LAN);

 c. Podłączenie głównego źródła zdarzeń opisującego komunikację sieciową, w tym:

 • przekierowanie logów opisujących transmisje sieciową (traffic) z zapór sieciowych (Firewall) na kolektor systemu,

 • uruchomienie reguł wykrywania;

 d. Prace audytowe, w tym:

 • pasywną analizę transmisji sieciowej:

 o ruch z/do serwerów webowych i aplikacyjnych,

 o ruch z/do serwerów baz danych,

 o ruch z/do serwerów pocztowych,

 o ruch z/do kontrolerów domenowych,

 o ruch z/do serwerów usług podstawowych (m.in. DNS/NTP),

 o ruch z/do zasobów zidentyfikowanych na bazie charakterystyki i wolumenu ruchu oraz możliwości identyfikacji aplikacji,

 • konsultacje w ramach otrzymanych wyników;

 • zebranie danych audytowych wymaganych do sporządzenia raportu;

 e. Analizę podatności, w zakresie:

 • integracji po API ze wskazanym przez zamawiającego komercyjnym skanerem/ skanerami podatności lub zainstalowanie skanera podatności typu open source;

 • przygotowanie reguł priorytetów i importu krytycznych podatności;

 f. Przygotowanie dynamicznego raportu audytowego w oparciu o dostępne w systemie narzędzia elektronicznej dokumentacji i szacowania ryzyka obejmującego analizę prawdopodobieństwa przełamania zabezpieczeń organizacji. Raport powinien zawierać:

 • zidentyfikowane zagrożenia oraz prawdopodobieństwo ich wystąpienia;

 • potencjalne wektory ataków dla wykrytych zagrożeń;

 • wizualizacja graficzna wykrytych źródeł zagrożeń oraz wektorów ataków;

 • rekomendacja zabezpieczeń;

 • zidentyfikowane zagrożenia związane z podatnościami oraz prawdopodobieństwo wykorzystania ich do przełamania zabezpieczeń;

 g. Transfer wiedzy w formie spotkania podsumowującego, obejmujący interpretację przez analityka wyników analizy ujętej w raporcie z systemu;

4. Obszar Detekcji ma na celu uruchomienie i dostrojenie mechanizmów wykrywania zagrożeń. Zakres prac powinien uwzględniać kolejno:

 a. Podłączenie (przekierowanie do systemu) źródeł zdarzeń i ich dalszą konfigurację. Kluczowe źródła zdarzeń obejmują:

 • zapory sieciowe w punkach styku z siecią Internet (Firewall brzegowy);

 • sieciowe systemy bezpieczeństwa dedykowane do wykrywania incydentów bezpieczeństwa (np.: Sandbox, IDP/IPS, AntySpam)

 • centralne systemy, dedykowane do kontroli złośliwego oprogramowania na stacjach końcowych/Serwerach, umożliwiające wykrywanie aktywności złośliwego oprogramowania (np.: AntyWirus, EDR);

 • kontroler domenowy oraz system zarządzania dostępem uprzywilejowanym;

 • systemy detekcji anomalii w przepływach lub zdarzeniach (np.: NBA);

 • system SIEM

 • w przypadku niestandardowych źródeł, muszą zostać przygotowane odpowiednie parsery, pozwalające na detekcję zgodną z wbudowanymi w system regułami korelacji;

 b. Adaptację reguł profilowych, pozwalających na dostosowanie zdarzeń do zasobów, których dotyczą;

 c. Podłączenie reguł detekcji;

 d. Podłączenie i konfiguracja mechanizmów UEBA:

 • integracja z Active Directory

 • utworzenie profili użytkowników UBA

 • utworzenie profili hostów EBA

 • import reguł bezpieczeństwa UEBA, utworzenie customowych reguł bezpieczeństwa UEBA, uruchomienie procesu uczenia

 • obserwacja i doprecyzowanie postępu uczenia maszynowego, wykluczenie/ dodanie nowych reguł zdarzeń użytkowników/ hostów.

 d. Dostrojenie systemu, w tym reguł priorytetyzacji zdarzeń i incydentów, mające na celu dopasowanie czułości systemu do możliwości operacyjnych organizacji;

5. Obszar Reakcji ma na celu uruchomienie i dostrojenie mechanizmów automatyzacji w działaniach reagowania na wykryte zagrożenia bezpieczeństwa. Zakres prac powinien uwzględniać kolejno:

 a. Pracę z konsultantem (m.in wprowadzenie do scenariuszy wbudowanych w systemie, analizę wymaganych zmian związanych z dostosowaniem scenariuszy, pomoc przy generowaniu API KEY dla wbudowanych akcji);

 b. Konfigurację zespołów obsługi, celem właściwej adresacji podatności oraz zdarzeń wymagających obsługi;

 c. Konfigurację mechanizmów powiadamiania.