Szczegółowy zakres i wytyczne procesu wdrożenia systemu

Etapy wdrożenia Systemu:

Etap 1 – Analiza przedwdrożeniowa - cykl prac analitycznych i organizacyjnych ustalający szczegółowy zakres oraz sposób realizacji wdrożenia oraz harmonogram i zakres szkoleń.

Na podstawie Etapu 1 Wykonawca opracuje i przedstawi do akceptacji Zamawiającemu projekt harmonogramu i metodologii wdrożenia.

Etap 2 - Instalacja i uruchomienie Systemu w środowisku produkcyjnym Zamawiającego – po uzyskaniu akceptacji Etapu 1. Celem tego etapu jest uzyskanie dynamicznego raportu audytowego pokazującego potencjalne możliwości przełamania zabezpieczeń w infrastrukturze Urzędu. Po zakończeniu tego etapu musi zostać sporządzony protokół bez uwag podpisany przez obie strony.

Instalacja i uruchomienie Systemu podzielone zostanie na 4 obszary:

1. **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);
2. **Obszar Detekcji**, zakładający podłączenie i konfigurację narzędzi odpowiedzialnych za wykrywanie zdarzeń i incydentów bezpieczeństwa w ramach zainstalowania modułu SIEM;
3. **Obszar Reakcji**, zakładający podłączenie i konfigurację mechanizmów wspomagających proces automatyzacji reakcji na wykryte zdarzenia, incydenty bezpieczeństwa i podatności w ramach zainstalowania modułu SOAR;
4. **Obszar Danych Osobowych**, zakładający zainstalowanie i skonfigurowanie modułu Ochrony Danych Osobowych i jego integracji z pozostałymi modułami systemu (tj. SIEM i SOAR).

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:
  - ruch z/do serwerów webowych i aplikacyjnych,
  - ruch z/do serwerów baz danych,
  - ruch z/do serwerów pocztowych,
  - ruch z/do kontrolerów domenowych,
  - ruch z/do serwerów usług podstawowych (m.in. DNS/NTP),
  - 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;

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

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 ich dostosowaniem; pomoc przy generowaniu API KEY dla wbudowanych akcji);
b) Konfigurację zespołów obsługi celem właściwej adresacji podatności oraz zdarzeń wymagających obsługi;
c) Konfigurację mechanizmów powiadamiania;

Obszar Danych Osobowych zakłada przeprowadzenie następujących prac wdrożeniowych

w zakresie modułu danych osobowych:

a) Przygotowania rejestru czynności przetwarzania i rejestru kategorii czynności przetwarzania – wprowadzenie min. 10 czynności/ kategorii czynności;
b) Wprowadzenia kluczowych usług przetwarzających dane osobowe – wprowadzenie min. 5 kluczowych usług;
c) Wprowadzenia przykładowych udostępnień - wprowadzenie min. 5 udostępnień;
d) Wprowadzenia przykładowych powierzeń - wprowadzenie min. 5 powierzeń;
e) Wprowadzenia przykładowych upoważnień - wprowadzenie min. 5 upoważnień;
f) Wprowadzenia jednostek organizacyjnych - wprowadzenie min. 10 jednostek;
g) Wprowadzenie stanowisk pracowników - wprowadzenie min. 5 stanowisk.

Etap 3 - Optymalizacja Systemu – Celem tego etapu jest dostrojenie scenariuszy obsługi zaimplementowanych w Etapie 2, w szczególności poprzez przeprowadzenie symulacji i analizy wyników przeprowadzonych symulacji, dotyczących procesów krytycznych (określonych w Etapie 2) Urzędu. Po zakończeniu tego etapu musi zostać sporządzony protokół bez uwag podpisany przez obie strony.

Etap 4 - Przeszkolenie administratorów/użytkowników Systemu z uruchomionych funkcjonalności.

Po zakończeniu tego etapu musi zostać sporządzony protokół bez uwag podpisany przez obie strony obejmujący imienną listę przeszkolonych osób.

Etap 5 – Wsparcie serwisowe - 36 miesięcy od zakończenia prac przewidzianych w Etapie 4.