Załącznik nr 2

Opis i harmonogram procesu wdrożenia

Szczegółowy harmonogram procesu wdrożenia przedstawia poniższa tabela:
Wdrożenie SIEM/SOAR

Id.	Nazwa	Odpowiedzialność	Rozpoczęcie planowane	Zakończenie planowane	Zakończenie rzeczywiste	Poprzednik	Uwagi
Etap 1			**dd.mm.rrrr**	**dd.mm.rrrr**			
1.	**Analiza przedwdrożeniowa**		**dd.mm.rrrr**	**dd.mm.rrrr**			
1.1.	Ankieta przedwdrożeniowa	**Zamawiający**					
1.2.	Przygotowanie schematu architektury i komunikacji, oraz harmonogramu prac	**Wykonawca**					
1.3.	Zatwierdzenie Harmonogramu prac i schematu architektury	**Zamawiający**				1.2	
1.4.	Przygotowanie dostępu VPN	**Zamawiający**					
1.5.	Przygotowanie maszyn wg zaproponowanej architektury i udrożnienie ruchu	**Zamawiający**				1.3	
1.6.	Weryfikacja przygotowanych maszyn (zasoby, licencje, udrożnienie ruchu)	**Wykonawca**				1.4, 1.5	
1.7.	Określenie źródeł logów	**Zamawiający przy doradztwie Wykonawcy**					
1.8.	Przekazanie klas adresowych wg szablonu	**Zamawiający**					
1.9.	Przekazanie parametrów do integracji z AD	**Zamawiający**					
1.10.	Przekazanie parametrów skrzynek pocztowych do powiadomień i zadań	**Zamawiający**					
1.11.	Przekazanie informacji o grupach/rolach użytkowników (AD)	**Zamawiający**					
1.12.	Przekazanie listy zasobów i procesów krytycznych	**Zamawiający**					

1.13.	Przekazanie danych do integracji ze skanerem podatności	**Zamawiający**					
1.14.	Ustalenie terminów szkoleń	**Zamawiający i Wykonawca**					
2.	**Instalacja systemu**						
2.1.	Instalacja SecureVisio	**Wykonawca**				1.4, 1.5, 1.6	
2.2.	Aktywacja licencji SecureVisio	**Wykonawca**				2.1	
2.3.	Import SVDATA	**Wykonawca**				2.1, 2.2	
2.4.	Przekierowanie źródeł logów	**Zamawiający przy doradztwie Wykonawcy**				1.7	
2.5.	Utworzenie konta lokalnego w SecureVisio	**Wykonawca**				2.1	
3.	**Konfiguracja systemu**		**dd.mm.rrrr**	**dd.mm.rrrr**			
3.1.	Import klas adresowych i utworzenie stref bezpieczeństwa	**Wykonawca**				1.8	
3.2.	Konfiguracja i podłączenie źródeł logów po stronie SV	**Wykonawca**				2.4	
3.3.	Powiązanie polityk bezpieczeństwa ze źródłami logów	**Wykonawca**				3.2	
3.4.	Uruchomienie narzędzi wykrywania	**Wykonawca**				3.1, 3.2, 3.3	
3.5.	Integracja skrzynek email	**Wykonawca**				1.10	
3.6.	Integracja z AD w kontekście użytkowników SecureVisio	**Wykonawca**				1.9	
3.7.	Utworzenie kont użytkowników SecureVisio	**Wykonawca**				1.11	
3.8.	Konfiguracja grup i ról użytkowników	**Wykonawca**				1.1, 3.4	
3.9.	Konfiguracja zespołów obsługi	**Wykonawca**				1.1, 3,4	
3.10.	Integracja z AD w kontekście UEBA	**Wykonawca**				1.9	
3.11.	Dostosowanie słownika procesów biznesowych na podstawie listy procesów krytycznych	**Wykonawca**				1.12	
3.12.	Uzupełnienie bazy CMDB na podstawie listy zasobów i procesów krytycznych	**Wykonawca**				3.11	
3.13.	Integracja ze skanerem podatności	**Wykonawca**				1.13	

3.14.	Konfiguracja harmonogramu skanera podatności	**Wykonawca przy współpracy z Zamawiającym**				3.13	
3.15.	Dostosowanie czasów remediacji, zasad i kanałów powiadamiania	**Zamawiający przy doradztwie Wykonawcy**					
3.16.	Ustawienie macierzy remediacji dla incydentów	**Wykonawca**					
3.17.	Ustawienie powiadomień według wytycznych dla incydentów	**Wykonawca**					
3.18.	Ustawienie macierzy remediacji dla podatności	**Wykonawca**					
3.19.	Ustawienie powiadomień według wytycznych dla podatności	**Wykonawca**					
3.20.	Utworzenie priorytetów zdarzeń	**Wykonawca**					
3.21.	Utworzenie priorytetów podatności	**Wykonawca**					
3.22.	Konfiguracja dostepu do SVCenter	**Wykonawca**					

Id.	Nazwa	Odpowiedzialność	Rozpoczęcie planowane	Zakończenie planowane	Zakończenie rzeczywiste	Poprzednik	Uwagi
Etap 2			**dd.mm.rrrr**	**dd.mm.rrrr**			
4.	**Dostrojenie systemu**		**dd.mm.rrrr**	**dd.mm.rrrr**			
4.1.	Konfiguracja reguł bezpieczeństwa	**Wykonawca**					
4.2.	Dostrojenie profili użytkowników i zasobów w przypadku niestandardowych struktur	**Wykonawca**					
4.3.	Uruchomienie procesu uczenia UEBA	**Wykonawca**				3.17, 3.18	
4.4.	Konfiguracja procesów biznesowych na podstawie wykrywania	**Wykonawca**				3.4	
4.5.	Uzupełnienie bazy CMDB	**Wykonawca**				3.4, 3.12	
4.6.	Zatwierdzenie bazy CMDB	**Zamawiający**				4.5	
4.7.	Doprecyzowywanie reguł bezpieczeństwa	**Wykonawca**					

4.8.	Doprecyzowanie wbudowanych scenariuszy obsługi	**Wykonawca**					
4.9.	Doprecyzowywanie dashboardów	**Wykonawca**					
5.	**Szkolenia**		**dd.mm.rrrr**	**dd.mm.rrrr**	**dd.mm.rrrr**		
5.1.	Szkolenie operatorów Szkolenie SIEM/SOAR (3 dni) PDP (2 dni) – do ustalenia	**Wykonawca**					
6.	**Zamknięcie projektu**		**dd.mm.rrrr**	**dd.mm.rrrr**	**dd.mm.rrrr**		
6.1.	Zgłoszenie gotowości do odbioru	**Wykonawca**					
6.2.	Zamknięcie i odbiór	**Wykonawca i Zamawiający**					
7.	**Przekazanie dokumentacji powdrożeniowej, dokumentacji obsługi i konfiguracji**	**Wykonawca**	**dd.mm.rrrr**	**dd.mm.rrrr**	**dd.mm.rrrr**		
8.	**Uruchomienie usługi wsparcia**	**Wykonawca**	**dd.mm.rrrr**	**dd.mm.rrrr**	**dd.mm.rrrr**		
9.	**Uruchomienie usługi konsultacji i przydzielenie konsultanta**	**Wykonawca**	**dd.mm.rrrr**	**dd.mm.rrrr**	**dd.mm.rrrr**		

Uwaga! Wdrożenie opiera się na wprowadzeniu do systemu danych / informacji przekazanych od Zamawiającego w momencie wdrożenia wg zatwierdzonego harmonogramu. W przypadku braku wymaganych informacji Zamawiający w późniejszym czasie ma możliwość samodzielnego uzupełnienia danych / informacji w systemie SecureVisio.