

Wytyczne

określające wymagania cyberbezpieczeństwa w
zakresie wdrażania nowych lub modernizacji
istniejących Systemów OT/SCADA
w Spółce Operator Gazociągów Przesyłowych
GAZ-SYSTEM S.A.

PC-DY-W02

Spis treści

Spis treści	2
Definicje i skróty	4
Cel Wytycznych.....	5
Przedmiot	5
Zakres stosowania	6
Rozdział I Inwentaryzacja komponentów Systemu OT/SCADA	6
Rozdział II Dokumentacja ogólna Systemu OT/SCADA	8
Rozdział III Analiza Ryzyka	9
Rozdział IV Utwardzanie Systemu OT/SCADA.....	10
Podrozdział IVa Blokada zbędnych usług i portów	10
Podrozdział IVb System wykrywania włamań na urządzeniu (ang. HIDS)	12
Podrozdział IVc Ograniczenie uprawnień zmian plików systemowych oraz konfiguracji systemów operacyjnych	13
Podrozdział IVd Konfiguracja sprzętowa	13
Podrozdział IVe Sygnał Heartbeat.....	14
Podrozdział IVf Instalowanie aktualizacji i poprawek systemów operacyjnych, aplikacji i oprogramowania firm trzecich.....	15
Rozdział V Ochrona brzegowa Systemu OT/SCADA	16
Podrozdział Va Zapora ogniowa (ang. Firewall).....	16
Podrozdział Vb System wykrywania włamań w infrastrukturze sieciowej (ang. NIDS)	18
Rozdział VI Zarządzanie użytkownikami	19
Podrozdział VIa Wyłączanie, usuwanie lub modyfikowanie kont domyślnych, testowych lub gości.....	19
Podrozdział VIb Zarządzanie sesjami	20
Podrozdział VIc Polityki haseł oraz uwierzytelniania	21
Podrozdział VId Kontrola użycia kont	22
Podrozdział VIe Kontrola dostępu do aplikacji Systemu OT/SCADA	23
Rozdział VII Praktyki programowania	24
Rozdział VIII Usuwanie podatności w Systemie OT/SCADA	25
Podrozdział VIIa Notyfikacje i powiadomienia ze strony Wykonawcy	25
Podrozdział VIIb Zgłaszanie podatności przez Zamawiającego	26
Rozdział IX Wykrywanie i ochrona przed złośliwym oprogramowaniem	27
Rozdział X Nazwy Hostów oraz adresacja	28

Rozdział XI Urządzenia obiektowe	29
Rozdział XII Zdalny dostęp.....	30
Rozdział XIII Bezpieczeństwo fizyczne	32
Rozdział XIV Segmentacja Systemu OT/SCADA.....	33
Podrozdział XIVa Urządzenia sieciowe	33
Podrozdział XIVb Architektura sieci	35
Przepisy końcowe.....	36
Załączniki.....	36

Definicje i skróty

ACL (Access Control List) – zestaw reguł filtrujących ruch w sieci.

DMZ (Demilitarized Zone) – strefa ograniczonego zaufania czyli wydzielany na zaporze sieciowej (ang. *firewall*) obszar sieci nienależący ani do sieci wewnętrznej (sieć OT), ani do sieci zewnętrznej (sieć IT).

ESD (Emergency Shutdown System) – system bezpieczeństwa w sterowaniu przemysłowym zapewniający bezpieczne zatrzymanie procesu na wypadek awarii oparty o układ blokad.

FAT (Factory Acceptance Test) – fabryczne testy akceptacyjne.

HIDS (host-based intrusion detection system) – system wykrywania i zapobiegania włamaniom działający jako aplikacja w ochranianym systemie operacyjnym poprzez analizę zdarzeń pochodzących z logu systemowego oraz z lokalnych interfejsów sieciowych.

Host – dowolne urządzenie (serwer, komputer, karta sieciowa, modem itp.) uczestniczące w wymianie danych lub udostępniające usługi sieciowe poprzez sieć komputerową za pomocą protokołu komunikacyjnego TCP/IP oraz posiadające własny adres IP.

ID – unikalny identyfikator fizycznego komponentu w zakresie wdrażanego/ modernizowanego systemu OT/SCADA.

NIDS/NIPS – Network Intrusion Detection System/Network Intrusion Prevention System – sieciowe systemy wykrywania i zapobiegania włamaniom.

PC – Jednostka Organizacyjna właściwa ds. cyberbezpieczeństwa w Spółce.

SAT (Site Acceptance Test) – obiektowe testy akceptacyjne.

SCADA (supervisory control and data acquisition) - połączenie sprzętu komputerowego i oprogramowania używanego do wysyłania poleceń i pozyskiwania danych w celu monitorowania i kontrolowania procesu.

SIEM (security information and event management) – narzędzie pozwalające na analizę w czasie rzeczywistym alertów bezpieczeństwa generowanych przez komponenty Systemu OT/SCADA.

SIS (Safety Instrumented System) – przyrządowy system bezpieczeństwa.

SOC (Centrum Operacyjne Cyberbezpieczeństwa Operatora Gazociągów Przesyłowych GAZ-SYSTEM S.A. / SOC GAZ-SYSTEM) – zespół pracowników PC, który wykrywa, analizuje i reaguje na incydenty cyberbezpieczeństwa przy użyciu rozwiązań technologicznych i procesowych.

Spółka/ GAZ-SYSTEM S.A./Spółka GAZ-SYSTEM S.A. – Operator Gazociągów Przesyłowych GAZ-SYSTEM S.A.

Sygnal Heartbeat – okresowy sygnał generowany przez sprzęt lub oprogramowanie do celów diagnostycznych (np. stanu komunikacji pomiędzy komponentami systemu) lub do synchronizacji komponentów systemu.

System OT/SCADA / System – zestaw wzajemnie powiązanych lub współzależnych komponentów tworzących złożoną całość i realizujących funkcje związane z monitorowaniem lub kontrolowaniem procesu.

Środowisko OT/SCADA (Operational Technology) – sprzęt i oprogramowanie przeznaczone do wykrywania lub wprowadzania zmian w procesach fizycznych poprzez bezpośrednie monitorowanie, lub sterowanie fizycznymi urządzeniami takimi jak silniki i sprężarki gazowe, zawory, pompy itp.

Wykonawca – Jednostka Organizacyjna Spółki lub podmiot gospodarczy, który na zlecenie Zamawiającego instaluje, konfiguruje, uruchamia lub utrzymuje System OT/SCADA.

VPN (Virtual Private Network) – wirtualna sieć prywatna oparta na hostach VPN oraz sieci teleinformatycznej, za pomocą której można bezpiecznie przysyłać dane (w sposób zaszyfrowany) przez sieć niezaufaną. Pomiędzy hostami VPN tworzony jest tunel VPN, przez który można przysyłać prywatne dane. Dane są chronione przed niepowołanym odczytem użytkowników sieci przez którą są one przesyłane.

Zamawiający – Spółka/ GAZ-SYSTEM S.A.

Pozostałym określeniom niezdefiniowanym w niniejszych wytycznych nadaje się znaczenie określone w wewnętrznych regulacjach Spółki.

Cel Wytycznych

Wytyczne stanowią uszczegółowienie wymagań dotyczących wdrażania nowych oraz modernizacji istniejących Systemów OT/SCADA zawartych w rozdziale IV Regulaminu Zarządzania Cyberbezpieczeństwem OT/SCADA w Spółce Operator Gazociągów Przesyłowych GAZ-SYSTEM S.A. (PC-DY-R01).

Przedmiot

Przedmiotem wytycznych jest zdefiniowanie minimalnych wymagań technicznych oraz proceduralnych w zakresie cyberbezpieczeństwa Systemów OT/SCADA, które należy uwzględnić na etapie budowy nowych oraz modernizacji istniejących Systemów w Spółce GAZ-SYSTEM S.A. Niniejsze wytyczne zawierają informacje na temat bazowych konfiguracji bezpieczeństwa dla poszczególnych rodzajów komponentów wchodzących w skład Systemów OT/SCADA oraz wymagania proceduralne związane z procesem wdrażania nowych oraz modernizacji istniejących Systemów.

Wymagania zawarte w wytycznych stanowią rekomendacje dotyczące implementacji mechanizmów cyberbezpieczeństwa w Systemach OT/SCADA i nie są podstawą do

zwolnienia Wykonawcy ze stosowania najlepszych praktyk inżynierskich w zakresie cyberbezpieczeństwa.

Implementacja poszczególnych wymagań zawartych w wytycznych powinna być poprzedzona analizą zakresu projektu, oczekiwanych i możliwych do zaimplementowania zabezpieczeń Systemu OT/SCADA.

Zakres stosowania

Wytyczne przeznaczone są do stosowania przez Jednostki Organizacyjne Spółki biorące udział w procesie inwestycji obejmującym budowę lub modernizację Systemów OT/SCADA oraz podmioty zewnętrzne realizujące te inwestycje na rzecz Spółki.

Wytyczne należy dotaczać do warunków technicznych dla zadań inwestycyjnych i modernizacyjnych obejmujących zakresem wdrażanie nowych lub modernizację istniejących Systemów OT/SCADA.

Obowiązek dostosowania projektu Systemów OT/SCADA oraz procedur ich wdrażania do niniejszych wytycznych należy uwzględnić na etapie przygotowywania dokumentacji do postępowania o udzielenie zamówienia oraz na etapie wydawania warunków technicznych dla zadań inwestycyjnych i modernizacyjnych.

Wszystkie wystąpienia sformułowania „Wykonawca powinien [...]” należy rozumieć jako zobowiązanie Wykonawcy do realizacji zawartych po nich zapisów. Jednocześnie implementacja każdego z wymagań zgodnie z zapisem powyżej (w części Przedmiot) powinna być poprzedzona analizą zakresu projektu, oczekiwanych i możliwych do zaimplementowania zabezpieczeń Systemu OT/SCADA. Stąd obligatoryjność poszczególnych wymagań będzie uzależniona od zakresu projektu oraz możliwości technicznych Systemów.

Rozdział I

Inwentaryzacja komponentów Systemu OT/SCADA

1. Wymagania

- 1.1. Wykonawca powinien dostarczyć listę komponentów wchodzących w skład Systemu OT/SCADA wraz z parametrami, zgodnie z zakresem projektu. Wymagane parametry dla komponentów Systemów OT/SCADA zostały zestawione w **Załączniku 1** do niniejszych wytycznych. W tym celu Wykonawca powinien wypełnić rejestr komponentów Systemu OT/SCADA (**Załącznik 2**) dostarczony przez Zamawiającego.

- 1.2. Wykonawca powinien oznakować w sposób widoczny poszczególne komponenty (fizyczne) wchodzące w skład Systemu OT/SCADA poprzez naniesienie ID komponentu, które powinno być unikalne dla każdego komponentu.
- 1.3. Wykonawca powinien ustalić wzorzec oraz zakresy ID komponentów z Zamawiającym.
- 1.4. Wykonawca powinien nanieść oznakowanie na kablach sieciowych do transmisji danych tak, aby można było jednoznacznie zidentyfikować komponent źródłowy, komponent docelowy połączenia oraz numery portów fizycznych na poszczególnych komponentach, do których kabel powinien zostać podłączony.
- 1.5. Wykonawca powinien nanieść oznakowanie na szafach / szafkach zawierających komponenty wdrażanego / modernizowanego Systemu OT/SCADA.
- 1.6. Wykonawca powinien ustalić wzorzec oznakowania kabli sieciowych oraz szaf sterowniczych i przyłączeniowych z Zamawiającym.

2. Weryfikacja wymagań na testach FAT

- 2.1. Wykonawca powinien przekazać wypełniony rejestr komponentów OT/SCADA (**Załącznik 2**) Zamawiającemu.
- 2.2. Wykonawca powinien zweryfikować czy wszystkie komponenty Systemu OT/SCADA używane w trakcie testów FAT zostały oznakowane unikalnym numerem ID w zakresie dostarczanego / modernizowanego Systemu.
- 2.3. Wykonawca powinien zweryfikować czy wszystkie przewody sieciowe oraz szafy / szafki z fizycznymi komponentami Systemu zostały oznakowane wg ustalonego schematu. Wykonawca powinien również porównać oznaczenia przewodów sieciowych i szaf na ustalonej próbce z dokumentacją techniczną Systemu OT/SCADA.

3. Weryfikacja wymagań na testach SAT

- 3.1. Wykonawca powinien zweryfikować czy wszystkie informacje na temat komponentów Systemu OT/SCADA zainstalowanych na obiekcie są wprowadzone do rejestru komponentów Systemu OT/SCADA.
- 3.2. Wykonawca powinien zweryfikować czy wszystkie komponenty zostały oznakowane zgodnie z wymaganiami.
- 3.3. Wykonawca powinien zweryfikować czy wszystkie kable sieciowe, szafy / szafki z komponentami zostały oznakowane zgodnie z wymaganiami.

4. Utrzymanie w okresie gwarancyjnym

- 4.1. Zmiany fizyczne wprowadzone w Systemach OT/SCADA po odbiorze końcowym powinny być zgłoszone do Zamawiającego w formie wniosku o aktualizację rejestru komponentów OT/SCADA Zamawiającego. Zmiany wprowadzane w Systemach OT/SCADA, powinny być poprzedzone opracowaniem zmian w dokumentacji Systemu OT/SCADA. Również zmiany logiczne / konfiguracyjne, które wpływają na aktualność tego rejestru (np. zmiana firmware'u, adresu MAC lub IP, wersji oprogramowania, itd.) powinny być zgłaszane w ten sam sposób.
- 4.2. Wykonawca powinien zweryfikować czy wszystkie informacje na temat komponentów Systemu OT/SCADA dodanych, usuniętych lub zmodyfikowanych

w okresie gwarancyjnym zostały zaktualizowane w rejestrze komponentów Systemu OT/SCADA zgodnie z Załącznikiem 1.

- 4.3.** W ramach wprowadzania zmian w okresie gwarancyjnym zastosowanie mają postanowienia punktów 2 i 3 powyżej (w tym w zakresie przeprowadzenia testów FAT i SAT).

Rozdział II

Dokumentacja ogólna Systemu OT/SCADA

1. Wymagania

- 1.1.** Wykonawca powinien dostarczyć opis funkcjonalny Systemu OT/SCADA zgodnie z zakresem projektu.
- 1.2.** Wykonawca powinien dostarczyć schematy sieciowe Systemu OT/SCADA z uwzględnieniem sieci Ethernet oraz urządzeń podłączonych po protokołach szeregowych (e.g. Modbus RTU, Profibus, etc.), zgodnie z zakresem projektu. Schematy powykonawcze muszą zawierać wszelkie poprawki wykonawcze, powstałe w czasie wdrożenia, a niewystępujące na schematach projektu wykonawczego. Dodatkowo Wykonawca powinien dostarczyć listę z parametrami transmisji magistral komunikacji szeregowej (prędkość transmisji, bity stopów, sprawdzanie parzystości itp.).
- 1.3.** Wykonawca powinien dostarczyć raport z analizy ryzyka związanego z cyberbezpieczeństwem Systemu OT/SCADA.
- 1.4.** Wykonawca powinien dostarczyć do Zamawiającego plan testów FAT nie później niż 10 dni roboczych przed planowanym rozpoczęciem testów.
- 1.5.** Wykonawca powinien dostarczyć do Zamawiającego plan testów SAT nie później niż 10 dni roboczych przed planowanym rozpoczęciem testów.
- 1.6.** Wykonawca powinien przeprowadzić testy FAT w swojej lokalizacji przed rozpoczęciem wdrożenia komponentów na obiekcie i dostarczyć do Zamawiającego raport z tych testów nie później niż 10 dni roboczych przed rozpoczęciem prac instalacyjnych.
- 1.7.** Wykonawca powinien dostarczyć do Zamawiającego raport z testów SAT nie później niż 15 dni roboczych od zakończenia testów.

2. Weryfikacja wymagań na testach FAT

- 2.1.** Wykonawca powinien zweryfikować kompletność i poprawność dokumentacji projektowej.
- 2.2.** Wykonawca powinien zweryfikować czy wszystkie komponenty Systemu OT/SCADA są zgodne z dokumentacją projektową.

3. Weryfikacja wymagań na testach SAT

- 3.1.** Wykonawca powinien zweryfikować zgodność Systemu OT/SCADA z dokumentacją projektową.

4. Utrzymanie w okresie gwarancyjnym

- 4.1.** Zmiany wprowadzane w Systemach OT/SCADA, powinny być poprzedzone opracowaniem zmian w dokumentacji Systemu OT/SCADA.

Rozdział III Analiza Ryzyka

1. Wymagania

- 1.1.** Wykonawca powinien wykonać analizę ryzyka związanego z cyberbezpieczeństwem Systemu OT/SCADA, zgodnie z zakresem projektu.
- 1.2.** Analiza ryzyka powinna obejmować identyfikację wektorów ataków cybernetycznych na poszczególne komponenty wchodzące w skład Systemu OT/SCADA, w tym wektory związane ze znanymi podatnościami wdrażanych komponentów, identyfikację zastosowanych mechanizmów cyberbezpieczeństwa oraz potencjalne konsekwencje ataku cybernetycznego.
- 1.3.** Wykonawca powinien określić, dla poszczególnych komponentów wchodzących w skład Systemu OT/SCADA, poziom ryzyka związanego z atakiem cybernetycznym na podstawie matrycy ryzyka dostarczonej przez Zamawiającego.
- 1.4.** Analiza powinna obejmować także rekomendacje działań obniżających prawdopodobieństwo wystąpienia lub skutki materializacji ryzyka.
- 1.5.** Przedstawiciele ze strony Zamawiającego powinni uczestniczyć w analizie ryzyka związanego z cyberbezpieczeństwem Systemów OT/SCADA.
- 1.6.** Wykonawca powinien opracować raport z analizy ryzyka związanego z cyberbezpieczeństwem Systemu OT/SCADA.

2. Weryfikacja wymagań na testach FAT

- 2.1.** Wykonawca powinien przekazać Zamawiającemu raport z analizy ryzyka.
- 2.2.** Wykonawca powinien zweryfikować, czy w analizie uwzględniono wszystkie komponenty wchodzące w skład Systemu OT/SCADA.
- 2.3.** Wykonawca powinien zweryfikować, czy dla wszystkich komponentów zidentyfikowano:
 - 2.3.1.** wektory potencjalnego ataku cybernetycznego,
 - 2.3.2.** zaimplementowane mechanizmy bezpieczeństwa,
 - 2.3.3.** konsekwencje potencjalnego ataku cybernetycznego oraz określono poziom ryzyka zgodnie z matrycą ryzyka Zamawiającego.
- 2.4.** Wykonawca powinien wypełnić listę kontrolną potwierdzającą implementację oraz poprawne działanie mechanizmów bezpieczeństwa zidentyfikowanych w analizie ryzyka. Lista kontrolna powinna być przekazana Zamawiającemu.

3. Weryfikacja wymagań na testach SAT

- 3.1.** Wykonawca powinien zweryfikować, czy wszystkie komponenty Systemu OT/SCADA zainstalowane na obiekcie zostały ujęte w analizie ryzyka, zgodnie z zakresem projektu.

- 3.2.** Wykonawca powinien przeprowadzić testy potwierdzające poprawność działania mechanizmów bezpieczeństwa zidentyfikowanych w analizie ryzyka.

4. Utrzymanie w okresie gwarancyjnym

- 4.1.** Zmiany wprowadzane w Systemach OT/SCADA, powinny być poprzedzone wykonaniem analizy ryzyka związanego z cyberbezpieczeństwem, zgodnie z wymaganiami niniejszego rozdziału.

Rozdział IV

Utwarczanie Systemu OT/SCADA

Podrozdział IVa

Blokada zbędnych usług i portów

1. Wymagania

- 1.1.** Wykonawca powinien dostarczyć wykaz z opisem wszystkich aplikacji, narzędzi, usług systemowych, skryptów, plików konfiguracyjnych, baz danych i wszelkiego innego wymaganego oprogramowania oraz wymaganych konfiguracji, w tym wersji i / lub poziomów poprawek dla każdego z systemu komputerowego wchodzącego w skład Systemu OT/SCADA.
- 1.2.** Wykonawca powinien dostarczyć wykaz usług wymaganych dla każdego urządzenia z uruchomionymi aplikacjami systemu sterowania lub wymaganego do połączenia aplikacji systemu sterowania. Wykaz powinien zawierać wszystkie porty i usługi wymagane do normalnego działania, a także wszystkie dodatkowe porty i usługi wymagane do pracy awaryjnej.
- 1.3.** Wykonawca zapewni w ramach okresu wsparcia określonego w umowie (nie krócej niż 2 lata) odpowiednie aktualizacje oprogramowania i usług w celu ograniczenia wszystkich luk bezpieczeństwa i luk funkcjonalnych związanych z produktem i utrzymania wymaganego poziomu bezpieczeństwa Systemu.
- 1.4.** Wykonawca powinien zainstalować najnowsze aktualizacje dostępne dla komponentów wchodzących w skład Systemu OT/SCADA i zatwierdzone przez producenta Systemu w momencie instalacji (w tym poprawki systemu operacyjnego, aplikacji oraz firmware urządzeń).
- 1.5.** Wykonawca, przed testami FAT, powinien usunąć i / lub wyłączyć wszystkie składniki oprogramowania, które nie są wymagane do działania i konserwacji systemu sterowania. Wykonawca powinien dostarczyć listę usuniętych i / lub wyłączonych składników oprogramowania.
Oprogramowanie, które powinno zostać usunięte i / lub wyłączone, obejmuje między innymi:
- 1.5.1.** gry,
 - 1.5.2.** sterowniki urządzeń, które nie zostały fizycznie zainstalowane,
 - 1.5.3.** usługi przesyłania wiadomości (np. MSN, Skype, GG itd.),
 - 1.5.4.** serwery lub klientów nieużywanych usług sieciowych,
 - 1.5.5.** kompilatory oprogramowania na wszystkich stacjach roboczych i serwerach, z wyjątkiem stacji roboczych i serwerów programistycznych,
 - 1.5.6.** kompilatory oprogramowania dla języków, które nie są używane w Systemie OT/SCADA,

- 1.5.7. protokoły sieciowe i komunikacyjne nieużywane przez System OT/SCADA,
- 1.5.8. nieużywane narzędzia administracyjne, diagnostyczne, zarządzania siecią i funkcje zarządzania systemem operacyjnym,
- 1.5.9. kopie zapasowe plików, baz danych i programów używanych tylko podczas tworzenia Systemu OT/SCADA,
- 1.5.10. wszystkie nieużywane dane i pliki konfiguracyjne,
- 1.5.11. programy demonstracyjne i przykładowe skrypty,
- 1.5.12. nieużywane narzędzia do przetwarzania dokumentów (np. Microsoft Word, Excel, PowerPoint, Adobe Acrobat, OpenOffice, Paint, itp.),
- 1.5.13. nieużywane przeglądarki internetowe,
- 1.5.14. programy do wymiany plików, które nie zostały autoryzowane przez Zamawiającego (np. Dropbox, OneDrive),
- 1.5.15. programy zdalnego dostępu, które nie zostały autoryzowane przez Zamawiającego w ramach danego projektu (np. VNC, TeamViewer).

2. Weryfikacja wymagań na testach FAT

- 2.1. Wykonawca powinien przeprowadzić przy użyciu odpowiedniego narzędzia skanowanie bezpieczeństwa dla wdrażanego / modernizowanego Systemu OT / SCADA (przynajmniej jako skanowanie luk w zabezpieczeniach, skanowanie podatności i aktywne skanowanie portów, z najnowszymi plikami sygnatur dla danego urządzenia).
- 2.2. Wyniki skanowania powinny być następnie porównywane z wykazem wymaganych usług, stanem poprawek i dokumentacją, aby potwierdzić, że wymagania w zakresie utwardzania Systemu zostały zaimplementowane.

3. Weryfikacja wymagań na testach SAT

- 3.1. Wykonawca powinien przeprowadzić skanowanie bezpieczeństwa Systemu OT/SCADA (zgodnie z wymaganiami z testów FAT – pkt. 2.1) wraz z inwentaryzacją wymaganych usług, stanem poprawek oprogramowania i weryfikacją kompletności wymaganej dokumentacji. Po zakończeniu testów SAT i przed uruchomieniem Systemu OT/SCADA powyższe skanowanie bezpieczeństwa powinno być przeprowadzone ponownie z najnowszymi plikami sygnatur.
- 3.2. Zamawiający powinien zweryfikować czy urządzenia wchodzące w skład Systemu OT/SCADA mają zablokowany dostęp do sieci niezaufanej.

4. Utrzymanie w okresie gwarancyjnym

- 4.1. Wszelkie aktualizacje systemów operacyjnych i poprawki oprogramowania powinny być udokumentowane przez Wykonawcę.
- 4.2. Po każdej instalacji aktualizacji systemu operacyjnego lub aplikacji Wykonawca zobowiązany jest zweryfikować, czy żadne dodatkowe, zbędne usługi nie zostały zainstalowane lub uruchomione.
- 4.3. Za każdym razem, gdy System jest aktualizowany, wymagane jest, aby Wykonawca ponownie przeprowadził odpowiedni zakres testów FAT przed ich implementacją w Systemie OT/SCADA Zamawiającego.

Podrozdział IVb

System wykrywania włamań na urządzeniu (ang. HIDS)

1. Wymagania

- 1.1. Wykonawca powinien dostarczyć skonfigurowany system HIDS, uzgodniony z Zamawiającym, realizujący takie funkcje, jak analiza logów zdarzeń, sprawdzanie integralności plików, egzekwowanie polityki bezpieczeństwa, wykrywanie rootkitów, monitorowanie wydajności i tworzenie ustawień bazowych w celu wykrywania zmian w konfiguracji Hosta.
- 1.2. Wykonawca powinien skonfigurować HIDS tak, aby wszystkie połączenia z Systemem i kontami użytkowników były rejestrowane. Dziennik zdarzeń powinien być skonfigurowany w taki sposób, aby alarmy mogły być przesłane do SOC w przypadku wystąpienia nieprawidłowej sytuacji.
- 1.3. Wykonawca dostarczy konfigurację bazową dla HIDS, która nie wpływa negatywnie na funkcje Systemu OT/SCADA.
- 1.4. Wykonawca powinien wskazać rekomendowane narzędzia do analizy logów oraz wysyłania powiadomień z HIDS.

2. Weryfikacja wymagań na testach FAT

- 2.1. Wykonawca powinien dostarczyć dokumentację dotyczącą dostarczonego rozwiązania HIDS.
- 2.2. W celu potwierdzenia poprawnego działania systemu HIDS Wykonawca powinien uruchomić HIDS na czas całego testu FAT oraz przeprowadzić testy:
 - 2.2.1. zainfekowania Systemu próbkami złośliwego oprogramowania,
 - 2.2.2. nieautoryzowanego użycia kont systemowych.
- 2.3. Wykonawca powinien przeanalizować pliki dziennika zdarzeń rozwiązania HIDS i zweryfikować je na zgodność z oczekiwanymi wynikami.
- 2.4. W przypadku, jeśli w ramach testów FAT System zostanie zainfekowany złośliwym oprogramowaniem lub okaże się nieodpornym na nieautoryzowane użycie kont systemowych, wówczas Wykonawca musi zaimplementować zmiany eliminujące te podatności i ponownie przeprowadzić testy zgodnie z punktami 2.2-2.3 powyżej.

3. Weryfikacja wymagań na testach SAT

- 3.1. Wykonawca powinien dostarczyć dokumentację dotyczącą dostarczonego rozwiązania HIDS.
- 3.2. W celu potwierdzenia poprawnego działania systemu HIDS Wykonawca powinien uruchomić HIDS na czas całego testu SAT oraz przeprowadzić testy nieautoryzowanego użycia kont systemowych,
- 3.3. Wykonawca powinien przeanalizować pliki dziennika zdarzeń rozwiązania HIDS i zweryfikować je na zgodność z oczekiwanymi wynikami.
- 3.4. W przypadku, jeśli w ramach testów SAT System okaże się nieodpornym na nieautoryzowane użycie kont systemowych, wówczas Wykonawca musi zaimplementować zmiany eliminujące te podatności i ponownie przeprowadzić testy zgodnie z punktami 3.2-3.3 powyżej.
- 3.5. Po zakończeniu testów SAT z wynikiem pozytywnym Wykonawca powinien w uzgodnieniu z Zamawiającym wygenerować obraz Systemu i przekazać go Zamawiającemu.

4. Utrzymanie w okresie gwarancyjnym

- 4.1.** Wykonawca powinien zapewnić w ramach okresu określonego w umowie (jednak nie krócej niż 2 lata) aktualizacje reguł oraz poprawki do HIDS w celu utrzymania wymaganego poziomu bezpieczeństwa Systemu.

Podrozdział IVc

Ograniczenie uprawnień zmian plików systemowych oraz konfiguracji systemów operacyjnych

1. Wymagania

- 1.1.** Wykonawca powinien skonfigurować hosty z ograniczeniem uprawnień poszczególnych kont do niezbędnego minimum, w tym ograniczenia użycia portów fizycznych (np. USB) oraz dostarczyć dokumentację konfiguracji uprawnień dla poszczególnych kont.
- 1.2.** Wykonawca powinien skonfigurować uruchamianie tylko niezbędnych usług systemowych dla poszczególnych kont użytkowników i dostarczyć dokumentację konfiguracji.
- 1.3.** Wykonawca powinien udokumentować, że ograniczenie lub wyłączenie dostępu do plików i funkcji/usług zostało zaimplementowane.

2. Weryfikacja wymagań na testach FAT

- 2.1.** Wykonawca powinien wykonać i udokumentować walidację konfiguracji przyznanych uprawnień.

3. Weryfikacja wymagań na testach SAT

- 3.1.** Wykonawca powinien wykonać i udokumentować walidację konfiguracji przyznanych uprawnień.

4. Utrzymanie w okresie gwarancyjnym

- 4.1.** Wykonawca powinien dokonać ponownej oceny uprawnień i konfiguracji bezpieczeństwa Systemu przed dostarczeniem jakichkolwiek aktualizacji.

Podrozdział IVd

Konfiguracja sprzętowa

1. Wymagania

- 1.1.** Wykonawca powinien wyłączyć, poprzez oprogramowanie (BIOS) lub fizyczne odłączenie, wszystkie nieużywane porty komunikacyjne i napędy wymiennych nośników lub zapewnić odpowiednie bariery techniczne ograniczające dostęp do portów oraz napędów wymiennych nośników.
- 1.2.** Wykonawca powinien zabezpieczyć hasłem dostęp do BIOSu w celu ochrony przed nieautoryzowanymi zmianami. W przypadku gdy zabezpieczenie BIOS hasłem jest technicznie niewykonalne Wykonawca powinien udokumentować taki

przypadek i zapewnić odpowiednie środki kompensujące. Wprowadzone hasła Wykonawca zobowiązany jest dostarczyć Zamawiającemu.

- 1.3. Wykonawca powinien dostarczyć pisemną listę wszystkich wyłączonych lub usuniętych portów komunikacyjnych, napędów CD / DVD i innych urządzeń z wymiennymi nośnikami.
- 1.4. Wykonawca powinien Skonfigurować System tak, aby umożliwić administratorom Systemu, po stronie Zamawiającego, ponowne włączenie portów, napędów oraz urządzeń, jeśli urządzenia są wyłączone przez oprogramowanie oraz powinien dostarczyć dokumentację konfiguracji.

2. Weryfikacja wymagań na testach FAT

- 2.1. Wykonawca powinien, w ramach testów FAT, wykonać walidację ograniczenia dostępu do portów oraz napędów urządzeń wymiennych.

3. Weryfikacja wymagań na testach SAT

- 3.1. Wykonawca powinien, w ramach testów SAT, wykonać walidację ograniczenia dostępu do portów oraz napędów urządzeń wymiennych.

4. Utrzymanie w okresie gwarancyjnym

- 4.1. Wykonawca, w przypadku konieczności wymiany urządzenia, powinien zweryfikować i dostarczyć dokumentację potwierdzającą, że każde wymienione urządzenie jest skonfigurowane tak samo i realizuje funkcje identycznie jak urządzenie zainstalowane pierwotnie.

Podrozdział IVe Sygnał Heartbeat

1. Wymagania

- 1.1. Wykonawca powinien zaimplementować w Systemie OT/SCADA sygnały lub protokoły „Heartbeat” oraz wskazać sposób włączenia ich do monitorowania stanu sieci.
- 1.2. Wykonawca powinien opracować bazową konfigurację ruchu komunikacyjnego „Heartbeat” z uwzględnieniem częstotliwości, rozmiarów pakietów i oczekiwanych konfiguracji pakietów.
- 1.3. Wykonawca powinien udokumentować definicję pakietów sygnałów „Heartbeat” i przykłady ruchu „Heartbeat”.

2. Weryfikacja wymagań na testach FAT

- 2.1. Wykonawca powinien zapewnić dokumentację wymagań w zakresie sygnałów „Heartbeat”.
- 2.2. Wykonawca powinien przeprowadzić testy działania sygnału „Heartbeat” z uwzględnieniem scenariuszy całkowitej utraty lub zakłócenia sygnału „Heartbeat”.

3. Weryfikacja wymagań na testach SAT

- 3.1.** Wykonawca powinien przeprowadzić testy działania sygnału „Heartbeat” z uwzględnieniem scenariuszy całkowitej utraty lub zakłócenia sygnału „Heartbeat”.

4. Utrzymanie w okresie gwarancyjnym

- 4.1.** Wykonawca powinien udokumentować wszelkie zmiany w konfiguracji bazowej ruchu komunikacyjnego „Heartbeat”.

Podrozdział IVf

Instalowanie aktualizacji i poprawek systemów operacyjnych, aplikacji i oprogramowania firm trzecich.

1. Wymagania

- 1.1.** Wykonawca powinien wdrożyć proces zarządzania i aktualizacji Systemu OT/SCADA.
- 1.2.** Wykonawca powinien dostarczyć szczegółowy opis procesu zarządzania i aktualizacji dla wdrażanego / modernizowanego Systemu OT/SCADA.
- 1.3.** Wykonawca powinien powiadamiać Zamawiającego o znanych podatnościach, które dotyczą wdrożonego / zmodernizowanego Systemu OT/SCADA przez Wykonawcę (w tym systemu operacyjnego, aplikacji i innego oprogramowania stron trzecich) w czasie nie dłuższym niż czas określony w umowie (ale nie więcej niż 5 dni) od czasu opublikowania podatności lub wykrycia podatności przez Wykonawcę.
- 1.4.** Komunikacja dotycząca podatności będzie się odbywać wyłącznie po ustalonej ścieżce komunikacyjnej z Zamawiającym.
- 1.5.** Wykonawca musi informować Zamawiającego o poprawkach wpływających na bezpieczeństwo Systemu OT/SCADA przez okres określony w umowie, ale nie krócej niż 2 lata.
- 1.6.** Wykonawca powinien przetestować i zweryfikować odpowiednie aktualizacje lub poprawki we własnym środowisku testowym przed ich implementacją w Systemie Zamawiającego, w celu potwierdzenia, że zainstalowana aktualizacja lub poprawka nie wpłynie negatywnie na poprawne działanie Systemu OT/SCADA Zamawiającego.

2. Weryfikacja wymagań na testach FAT

- 2.1.** Wykonawca powinien zainstalować wszystkie przetestowane i zatwierdzone poprawki zabezpieczeń i aktualizacje przed rozpoczęciem testu FAT.
- 2.2.** Wykonawca powinien dostarczyć dokumentację potwierdzającą, że wszystkie poprawki zabezpieczeń i aktualizacje zostały przetestowane i zainstalowane.
- 2.3.** Wykonawca powinien wykonać skanowanie bezpieczeństwa (z najnowszą bazą sygnatur) w celu sprawdzenia, czy podatności w Systemie zostały wyeliminowane.
- 2.4.** Wykonawca powinien dostarczyć dokumentację wyników skanów bezpieczeństwa.

- 2.5. Wykonawca powinien udokumentować konfigurację bazową Systemu po testach FAT, aby stworzyć bazowe środowisko do walidacji przyszłych poprawek i aktualizacji.

3. Weryfikacja wymagań na testach SAT

- 3.1. Wykonawca powinien zainstalować wszystkie przetestowane i zatwierdzone poprawki zabezpieczeń i aktualizacje przed rozpoczęciem testu SAT.
- 3.2. Wykonawca powinien dostarczyć dokumentację potwierdzającą, że wszystkie poprawki zabezpieczeń i aktualizacje zostały przetestowane i zainstalowane.
- 3.3. Wykonawca powinien wykonać skanowanie bezpieczeństwa (z najnowszą bazą sygnatur) w celu sprawdzenia, czy podatności w Systemie zostały wyeliminowane.
- 3.4. Wykonawca powinien dostarczyć dokumentację wyników skanów bezpieczeństwa.
- 3.5. Wykonawca powinien udokumentować konfigurację bazową Systemu po testach SAT.

4. Utrzymanie w okresie gwarancyjnym

- 4.1. Wykonawca powinien wdrożyć proces zarządzania poprawkami dla dostarczonego Systemu po jego instalacji. Proces zarządzania poprawkami powinien uwzględniać alternatywne strategie mitygacji podatności bezpieczeństwa w przypadkach, gdy Wykonawca nie rekomenduje instalowania poprawek w Systemie OT/SCADA.
- 4.2. Wykonawca powinien zapewnić wsparcie w zakresie testowania poprawek oraz aktualizacji.
- 4.3. Wskazane jest, aby administratorzy Systemów OT/SCADA instalowali otrzymane od Wykonawcy poprawki i aktualizacje najpierw w Systemie nieprodukcyjnym w celu testowania i sprawdzania poprawności przed instalacją na docelowym Systemie produkcyjnym.

Rozdział V

Ochrona brzegowa Systemu OT/SCADA

Podrozdział Va

Zapora ogniowa (ang. Firewall)

1. Wymagania

- 1.1. Wykonawca powinien dostarczyć zapory ogniowe, uzgodnione z Zamawiającym, wraz z zestawem reguł zapory w celu ochrony brzegowej Systemu OT/SCADA. W przypadku, jeśli zapory nie są dostarczane przez Wykonawcę wówczas Wykonawca powinien dostarczyć zestaw reguł dla zapór.
- 1.2. Wykonawca powinien dostarczyć zaporę ogniową umożliwiającą analizę ruchu sieciowego w warstwie aplikacyjnej protokołów.
- 1.3. Wykonawca powinien dostarczyć dokumentację zawierającą zestawy reguł zapory z uwzględnieniem adresów źródłowych, docelowych, używanych portów i protokołów. Informacje zawarte w dokumentacji powinny być traktowane jako

wrażliwe dla działalności Zamawiającego i powinny być chronione z należytą starannością.

- 1.4. Podstawową zasadą zestawu reguł powinno być tzw. „deny all”, z wyjątkami wyraźnie określonymi przez Wykonawcę, tzn. domyślne zablokowanie całej komunikacji na zaporze ogniowej i przepuszczanie wyłącznie granularnie określonych wyjątków komunikacji.
- 1.5. Wykonawca powinien dostarczyć szczegółowe informacje na temat ruchu sieciowego wymaganego do pracy Systemu OT/SCADA (w tym używanych protokołów) przechodzącego przez zaporę, zarówno przychodzącego, jak i wychodzącego oraz zidentyfikować każde urządzenie inicjujące komunikację zgodnie z odpowiednimi zestawami reguł.
- 1.6. Zapory ogniowe powinny zapewniać przekazywanie informacji do wskazanego, przez Zamawiającego, systemu nadrzędnego. Zakres informacji przekazywanych do systemu nadrzędnego powinien zostać uzgodniony z Zamawiającym.
- 1.7. Jeżeli zapory ogniowe są dostarczane przez Wykonawcę, to powinny zostać dostarczone z najnowszym dostępnym wbudowanym oprogramowaniem (firmware) zatwierdzonym przez Wykonawcę.

2. Weryfikacja wymagań na testach FAT

- 2.1. Wykonawca powinien uruchomić zaporę ogniową zgodnie ze specyfikacją na czas całego testu FAT.
- 2.2. Wykonawca powinien wykonać testy sprawdzające działanie zapory, sprawdzanie plików dziennika, weryfikację poprawności wyników testu oraz aktualności firmware'u urządzenia.
- 2.3. Wykonawca powinien zweryfikować czy dokumentacja w zakresie reguł zapory jest kompletna.

3. Weryfikacja wymagań na testach SAT

- 3.1. Wykonawca powinien uruchomić zaporę na czas całego testu SAT.
- 3.2. Zamawiający powinien uruchomić zapory ogniowe w ramach zarządzanej przez niego infrastruktury na czas całego procesu SAT.
- 3.3. Wykonawca powinien wykonać testy sprawdzające działanie zapory, sprawdzanie plików dziennika oraz weryfikację poprawności wyników testu.
- 3.4. Wszelkie domyślne konta Wykonawcy, konta testowe lub inne kody zabezpieczeń Wykonawcy dla zapory powinny zostać zmienione przez Zamawiającego.
- 3.5. Zamawiający powinien zweryfikować czy dokumentacja w zakresie reguł zapory jest kompletna.
- 3.6. Zamawiający powinien zweryfikować czy nie występują znane podatności dla wgranej wersji oprogramowania zapory ogniowej. Zamawiający powinien zweryfikować aktualność wgranego oprogramowania dla zapory ogniowej.

4. Utrzymanie w okresie gwarancyjnym

- 4.1. W przypadku wprowadzania zmian w Systemie OT/SCADA reguły zapory powinny być przeanalizowane pod kątem wymaganych modyfikacji.
- 4.2. Wykonawca zobowiązany jest do analizowania uaktualnień wbudowanego oprogramowania (firmware-u) dla zapór ogniowych wchodzących w skład

Systemu i rekomendowania ich implementacji. W uzgodnieniu z Zamawiającym aktualizuje to oprogramowanie i dokumentację powykonawczą.

- 4.3.** Wszelkie modyfikacje reguł lub aktualizacje firmware-u powinny być zakończone testem SAT zgodnie z zakresem modyfikacji.

Podrozdział Vb

System wykrywania włamań w infrastrukturze sieciowej (ang. NIDS)

1. Wymagania

- 1.1.** Wykonawca powinien dostarczyć system NIDS o charakterze sygnaturowym oraz behawioralnym dla Systemu OT/SCADA pozwalający na monitorowanie ruchu sieciowego co najmniej pomiędzy poziomami Level 3 oraz Level 3,5 (tzw. OT DMZ) oraz na urządzeniach sieciowych na granicy Systemu OT/SCADA zgodnie z zakresem projektu.
- 1.2.** Wykonawca powinien dostarczyć system NIDS z najnowszą wersją oprogramowania oraz z najnowszymi dostępnymi sygnaturami.
- 1.3.** Wykonawca powinien dostarczyć NIDS z funkcjonalnością Deep Packet Inspection (analizy protokołu w warstwie 7 modelu ISO/OSI) dla wielu protokołów, które są powszechnie stosowane w sieciach OT/SCADA (DNP3, MODBUS, CIP, PROFINET, etc.)
- 1.4.** Wykonawca powinien dostarczyć profile ruchu z oczekiwanymi ścieżkami komunikacji i oczekiwanymi granicami komunikacji dla NIDS behawioralnego.
- 1.5.** Wykonawca powinien dostarczać aktualizacje bazy sygnatur dla modułu sygnaturowego systemu NIDS oraz poprawki dla samego oprogramowania przez ustalony okres z Zamawiającym (ale nie krócej niż przez 2 lata).
- 1.6.** Wykonawca powinien dostarczyć system NIDS w formie skonfigurowanej i dostrojonej do infrastruktury Zamawiającego.
- 1.7.** Wykonawca powinien dostarczyć dokumentację zawierającą informacje niezbędne do samodzielnego skonfigurowania systemu NIDS, administrowania i użytkowania.
- 1.8.** Wykonawca powinien zapewnić wymianę danych systemu NIDS z nadrzędnym systemem Zamawiającego (np. SIEM) oraz przekazać dokumentację i wytyczne dotyczące połączenia NIDS z tym systemem.

2. Weryfikacja wymagań na testach FAT

- 2.1.** Wykonawca powinien uruchomić system NIDS z dostarczonymi modułami (tj. sygnaturowy, behawioralny) na czas testu FAT.
- 2.2.** Wykonawca powinien wykonać testy sprawdzające działanie NIDS, sprawdzanie plików dziennika oraz weryfikację poprawności wyników testu.
- 2.3.** Wykonawca powinien zweryfikować, czy dokumentacja w zakresie NIDS jest kompletna.

3. Weryfikacja wymagań na testach SAT

- 3.1.** Wykonawca powinien uruchomić NIDS na czas testu SAT z pełną dostarczoną funkcjonalnością. NIDS powinien być zaktualizowany do najnowszej wersji i posiadać aktualne sygnatury.

- 3.2.** Wykonawca powinien wykonać testy sprawdzające działanie NIDS, sprawdzanie plików dziennika oraz weryfikację poprawności wyników testu.
- 3.3.** Zamawiający powinien zweryfikować, czy dokumentacja w zakresie profili ruchu NIDS jest kompletna.
- 3.4.** Wszelkie domyślne konta Wykonawcy, konta testowe lub inne kody zabezpieczeń Wykonawcy dla systemu NIDS powinny zostać zmienione przez Zamawiającego.
- 3.5.** Zamawiający powinien sprawdzić aktualność oprogramowania Systemu oraz sygnatur.

4. Utrzymanie w okresie gwarancyjnym

- 4.1.** W przypadku wprowadzania zmian w Systemie OT/SCADA profile ruchu powinny być przeanalizowane pod kątem wymaganych modyfikacji.
- 4.2.** Wykonawca powinien wdrożyć proces dostrojenia sygnatur oraz profili ruchu, aby zmniejszyć liczbę fałszywych alarmów i zminimalizować ilość fałszywych zdarzeń NIDS.

Rozdział VI

Zarządzanie użytkownikami

Podrozdział VIa

Wyłączanie, usuwanie lub modyfikowanie kont domyślnych, testowych lub gości

1. Wymagania

- 1.1.** Wykonawca powinien opracować i udokumentować listę kont, które muszą być aktywne, wraz z przypisanym poziomem uprawnień oraz listę kont które należy wyłączyć, usunąć lub zmodyfikować.
- 1.2.** Wykonawca powinien wyłączyć, usunąć lub zmodyfikować wszystkie konta zgodnie z opracowaną listą.
- 1.3.** Wykonawca powinien wyłączyć lub usunąć wszystkie konta domyślne Wykonawcy (lub producenta rozwiązania), konta testowe i konta gości przed testami FAT.
- 1.4.** Wykonawca powinien wyłączyć, usunąć lub zmodyfikować po testach SAT wszystkie konta należące do Wykonawcy. Istnieje możliwość pozostawienia kont Wykonawcy, na potrzeby utrzymania Systemu OT/SCADA, za pisemną zgodą Zamawiającego. Konta te w ramach normalnego funkcjonowania Systemu powinny być zablokowane, a aktywowane mogą być jedynie na czas prowadzenia przez Wykonawcę prac serwisowych i usuwania awarii.

2. Weryfikacja wymagań na testach FAT

- 2.1.** Wykonawca powinien zweryfikować czy wszystkie konta gości, konta testowe oraz konta domyślne Wykonawcy (lub producenta rozwiązania) zostały wyłączone, usunięte lub zmodyfikowane zgodnie z dokumentacją.

3. Weryfikacja wymagań na testach SAT

- 3.1.** Zamawiający powinien zweryfikować czy wszystkie konta należące do Wykonawcy, konta domyślne, testowe oraz konta gości zostały wyłączone, usunięte lub zmodyfikowane zgodnie z dokumentacją.

4. Utrzymanie w okresie gwarancyjnym

- 4.1.** Wykonawca nie może wprowadzać żadnych nowych kont bez pisemnego polecenia Zamawiającego.

Podrozdział VIb Zarządzanie sesjami

1. Wymagania

- 1.1.** Wykonawca powinien zablokować możliwość przesyłania poświadczeń użytkownika w postaci zwykłego (otwartego) tekstu.
- 1.2.** Wykonawca powinien zapewnić, dla każdego rodzaju sesji, najsilniejszą metodę szyfrowania przy uwzględnieniu możliwości technicznych Systemu OT/SCADA i ograniczeń w zakresie wymaganego czasu odpowiedzi.
- 1.3.** Wykonawca powinien ograniczyć ilość jednoczesnych sesji użytkowników. Ilość sesji jednoczesnych powinna zostać uzgodniona z Zamawiającym.
- 1.4.** Wykonawca powinien wyłączyć jakiekolwiek funkcje zapisu poświadczeń użytkownika na urządzeniu oraz automatycznego wypełniania poświadczeń podczas logowania.
- 1.5.** Wykonawca powinien skonfigurować dla każdego konta możliwość ręcznego wylogowania użytkownika oraz rozłączenia sesji zdalnych po okresie bezczynności przekraczającym zdefiniowaną liczbę minut.

2. Weryfikacja wymagań na testach FAT

- 2.1.** Wykonawca powinien przeprowadzić testy z wykorzystaniem narzędzi do podsłuchu ruchu sieciowego w celu potwierdzenia, że poświadczenia dla żadnego konta nie są przysyłane w sposób jawny.
- 2.2.** Wykonawca powinien zweryfikować ustawienia Systemu w celu potwierdzenia, że zostały uruchomione mechanizmy szyfrowania zgodne z dokumentacją.
- 2.3.** Wykonawca powinien przeprowadzić próbę jednoczesnych logowań dla poszczególnych kont (liczba prób połączeń powinna przekraczać wartość dopuszczalną zgodnie z dokumentacją).
- 2.4.** Wykonawca powinien przeprowadzić test rozłączenia sesji zdalnych po skonfigurowanym okresie bezczynności.

3. Weryfikacja wymagań na testach SAT

- 3.1.** Wykonawca powinien zweryfikować ustawienia Systemu w celu potwierdzenia, że zostały uruchomione mechanizmy szyfrowania zgodne z dokumentacją.
- 3.2.** Wykonawca powinien przeprowadzić próbę jednoczesnych logowań dla poszczególnych kont (liczba prób połączeń powinna przekraczać wartość dopuszczalną zgodnie z dokumentacją).
- 3.3.** Wykonawca powinien przeprowadzić test wylogowania kont po skonfigurowanym okresie bezczynności.

4. Utrzymanie w okresie gwarancyjnym

- 4.1.** Wykonawca nie wprowadzi żadnych nowych konfiguracji sesji bez pisemnego polecenia Zamawiającego.
- 4.2.** Wykonawca zapewni zmianę kluczy szyfrujących nie rzadziej niż raz na 1 rok.

Podrozdział VIc

Polityki haseł oraz uwierzytelniania

1. Wymagania

- 1.1.** Wykonawca powinien dostarczyć i skonfigurować system zarządzania hasłami do kont dla stacji komputerowych oraz urządzeń, które mają taką możliwość (np. panele HMI bazujące na systemach MS Windows), który pozwala na:
 - 1.1.1.** wybór długości hasła (co najmniej 8 znaków),
 - 1.1.2.** ustawianie częstotliwości zmian hasła (nie rzadziej niż raz na 6 miesięcy),
 - 1.1.3.** ustawienia wymaganej złożoności hasła (duże i małe litery, cyfry oraz znaki specjalne),
 - 1.1.4.** wylogowanie nieaktywnej sesji (po okresie bezczynności przekraczającym 30 minut),
 - 1.1.5.** odmowę wielokrotnego użycia tego samego hasła (zakaz ponownego używania ostatnich 3 haseł),
 - 1.1.6.** wymuszenie zmiany domyślnych i startowych haseł do kont przy pierwszym logowaniu.
- 1.2.** Hasła nie mogą być przechowywane w systemie zarządzania hasłami ani w innym repozytorium w formie elektronicznej w sposób nieszyfrowany, ani Wykonawca nie może ich przekazać w dostarczonej papierowej dokumentacji w formie zwykłego tekstu, chyba że nośnik jest fizycznie chroniony (np. zabezpieczona koperta).
- 1.3.** Wykonawca powinien zapewnić kontrolę dostępu do interfejsu konfiguracyjnego systemu zarządzania kontami.
- 1.4.** Wykonawca powinien zapewnić mechanizm przywracania zasad uwierzytelniania podczas awaryjnego odzyskiwania Systemu lub odtwarzania Systemu.

2. Weryfikacja wymagań na testach FAT

- 2.1.** Wykonawca powinien wykonać testy wdrożonych polityk uwierzytelniania oraz haseł.
- 2.2.** Wykonawca powinien zweryfikować prawidłowe działanie mechanizmów kontroli dostępu do interfejsu konfiguracyjnego systemu zarządzania kontami.
- 2.3.** Wykonawca powinien przeprowadzić test przywracania zasad uwierzytelniania w ramach odzyskiwania i odtwarzania Systemu po awarii.
- 2.4.** Po wykonaniu testów FAT Wykonawca powinien skonfigurować polityki uwierzytelniania oraz haseł zgodnie z dokumentacją Systemu OT/SCADA oraz wymaganiami Zamawiającego.

3. Weryfikacja wymagań na testach SAT

- 3.1.** Wykonawca powinien wykonać testy wdrożonych polityk uwierzytelniania oraz haseł.

- 3.2.** Wykonawca powinien zweryfikować prawidłowe działanie mechanizmów kontroli dostępu do interfejsu konfiguracyjnego systemu zarządzania kontami.
- 3.3.** Po wykonaniu testów SAT Wykonawca powinien skonfigurować polityki uwierzytelniania oraz haseł zgodnie z dokumentacją Systemu OT/SCADA oraz wymaganiami Zamawiającego.

4. Utrzymanie w okresie gwarancyjnym

- 4.1.** Wykonawca nie powinien wprowadzać zmian w politykach haseł lub zasadach uwierzytelniania bez pisemnej prośby Zamawiającego.

Podrozdział VIa Kontrola użycia kont

1. Wymagania

- 1.1.** Wykonawca powinien dostarczyć system, w którym rejestrowane jest działanie na koncie z możliwością audytowania działań - zarówno z perspektywy zarządzania (polityki), jak i operacyjnej (użycia konta) wraz ze stemplami czasowymi.
- 1.2.** Wykonawca powinien zapewnić szyfrowanie i kontrolę dostępu do ścieżek audytu lub plików dziennika.
- 1.3.** Wykonawca powinien skonfigurować system tak, aby rejestrowanie ścieżek audytu użycia kont nie miało negatywnego wpływu na wydajność Systemu OT/SCADA.
- 1.4.** Wykonawca powinien skonfigurować nośniki w trybie tylko do odczytu dla tworzenia ścieżek audytu oraz dziennika zdarzeń.
- 1.5.** Wykonawca powinien uwzględniać obowiązujące przepisy o ochronie danych osobowych w zakresie zapisu danych identyfikacyjnych, w tym umożliwiać pseudonimizację, anonimizację lub usunięcie wszystkich wpisów z rejestru zdarzeń zawierających określonego użytkownika.

2. Weryfikacja wymagań na testach FAT

- 2.1.** Wykonawca powinien wykonać testy rejestrowania zdarzeń wykonywanych przez użytkowników posiadających uprawnienia do działań administracyjnych oraz przez użytkowników posiadających uprawnienia do działań operacyjnych w Systemie.
- 2.2.** Wykonawca powinien zweryfikować prawidłowe działanie mechanizmów kontroli dostępu oraz szyfrowania ścieżek audytu i plików dziennika zdarzeń.
- 2.3.** Wykonawca powinien przeprowadzić pomiary wydajności Systemu OT/SCADA, aby sprawdzić, czy czynności rejestrowania nie wpływają negatywnie na wydajność Systemu.
- 2.4.** Wykonawca powinien zweryfikować czy nośnik dla ścieżek audytu oraz dziennika zdarzeń jest w trybie tylko do odczytu.

3. Weryfikacja wymagań na testach SAT

- 3.1.** Wykonawca powinien wykonać testy rejestrowania zdarzeń wykonywanych przez użytkowników posiadających uprawnienia do działań administracyjnych oraz

przez użytkowników posiadających uprawnienia do działań operacyjnych w Systemie.

- 3.2.** Wykonawca powinien zweryfikować prawidłowe działanie mechanizmów kontroli dostępu oraz szyfrowania ścieżek audytu i plików dziennika zdarzeń.
- 3.3.** Wykonawca powinien przeprowadzić pomiary wydajności Systemu OT/SCADA, aby sprawdzić, czy czynności rejestrowania nie wpływają negatywnie na wydajność Systemu.
- 3.4.** Wykonawca powinien zweryfikować czy nośnik dla ścieżek audytu oraz dziennika zdarzeń jest w trybie tylko do odczytu.

4. Utrzymanie w okresie gwarancyjnym

- 4.1.** Wykonawca powinien zapewnić archiwizację i przechowywanie ścieżek audytu oraz dziennika zdarzeń przez okres co najmniej 3 lata.
- 4.2.** Wykonawca powinien regularnie przeglądać dane zawarte w ścieżkach audytu oraz dziennikach zdarzeń.

Podrozdział VIe

Kontrola dostępu do aplikacji Systemu OT/SCADA

1. Wymagania

- 1.1.** Wykonawca powinien skonfigurować uwierzytelnianie na poziomie aplikacji Systemu OT/SCADA przy użyciu innych danych uwierzytelniających niż do systemu operacyjnego, zgodnie z wymaganiami Podrozdziału VIc punkt 1.1.
- 1.2.** Wykonawca powinien utworzyć konta użytkowników z konfigurowalnym dostępem i uprawnieniami związanymi ze zdefiniowaną rolą użytkownika w aplikacji Systemu OT/SCADA. Zakres kont oraz uprawnienia powinny być uzgodnione z Zamawiającym.
- 1.3.** Wykonawca powinien skonfigurować konta użytkowników aplikacji z minimalnym zakresem uprawnień dla danej roli.
- 1.4.** Wykonawca powinien zapewnić mechanizm zmiany uprawnień użytkowników oraz przypisania użytkowników do grup o określonych poziomach uprawnień wyłącznie dla administratora Systemu.
- 1.5.** Wykonawca powinien dostarczyć dokumentację określającą poziomy kont użytkowników wraz z opisem poziomu uprawnień oraz opisem powiązanych ról w aplikacji OT/SCADA.

2. Weryfikacja wymagań na testach FAT

- 2.1.** Wykonawca powinien wykonać sprawdzenie poziomu uprawnień dla poszczególnych kont użytkowników.
- 2.2.** Wykonawca powinien zweryfikować, czy użytkownik nie może podnieść uprawnień w aplikacji Systemu OT/SCADA bez zalogowania się na uprawnieniach administratora.
- 2.3.** Wykonawca powinien usunąć wszelkie konta testowe po FAT.

3. Weryfikacja wymagań na testach SAT

- 3.1.** Wykonawca powinien wykonać testy funkcjonalne aplikacji OT/SCADA dla poszczególnych kont w celu sprawdzenia m.in. poziomu uprawnień.
- 3.2.** Zamawiający powinien zweryfikować, czy użytkownik nie może podnieść uprawnień w aplikacji Systemu OT/SCADA bez zalogowania się na uprawnieniach administratora.
- 3.3.** Zamawiający powinien zmienić wszystkie hasła zdefiniowanych kont po zakończeniu testów SAT.

4. Utrzymanie w okresie gwarancyjnym

- 4.1.** Wykonawca nie powinien tworzyć żadnych dodatkowych kont w aplikacji OT/SCADA bez pisemnej prośby Zamawiającego.
- 4.2.** Wykonawca nie powinien wprowadzać zmian w zakresie uprawnień poszczególnych użytkowników aplikacji bez pisemnej zgody Zamawiającego.

Rozdział VII

Praktyki programowania

1. Wymagania

- 1.1.** Wykonawca powinien dostarczyć dokumentację dotyczącą standardów oraz praktyk stosowanych przy opracowaniu oprogramowania Systemu OT/SCADA napisanego przez Wykonawcę, w tym oprogramowania sterowników PLC.
- 1.2.** Wykonawca przy tworzeniu oprogramowania powinien:
 - 1.2.1.** zaimplementować mechanizmy kontroli wartości zmiennych wejściowych oraz wyjściowych,
 - 1.2.2.** zaimplementować mechanizmy zapobiegające przepiętnieniu buforów danych,
 - 1.2.3.** zaimplementować mechanizmy uwierzytelniania i sprawdzania integralności przesyłanych danych,
 - 1.2.4.** upewnić się, że systemy operacyjne oraz biblioteki firm trzecich użyte do opracowania oprogramowania mają wdrożony proces aktualizacji oraz łatania podatności,
 - 1.2.5.** nie przechowywać otwartym tekstem w kodzie programu haseł oraz kluczy szyfrowania,
 - 1.2.6.** nie przysyłać otwartym tekstem haseł oraz kluczy szyfrowania.
- 1.3.** Wykonawca powinien zaimplementować mechanizmy przeglądu kodu oprogramowania z wykorzystaniem automatycznych narzędzi pozwalających na wykrycie luk bezpieczeństwa.
- 1.4.** Wykonawca powinien dostarczyć wyniki przeglądu kodu oprogramowania.
- 1.5.** Prawa autorskie do oprogramowania i własność kodu źródłowego powinny zostać przeniesione na Zamawiającego.

2. Weryfikacja wymagań na testach FAT

- 2.1.** Wykonawca powinien zweryfikować kompletność dokumentacji oprogramowania.

- 2.2.** Wykonawca powinien wykonać testy potwierdzające zastosowanie odpowiednich praktyk programowania zgodnie z dokumentacją oraz przekazać Zamawiającemu protokół z testów.
- 2.3.** Wykonawca powinien przekazać Zamawiającemu raport z przeglądu kodu źródłowego.
- 2.4.** Wykonawca powinien przekazać Zamawiającemu kod źródłowy oprogramowania wraz z wszelkimi hasłami zabezpieczającymi oprogramowanie lub jego biblioteki. Kod źródłowy powinien zawierać komentarze a zmienne powinny posiadać nazwy symboliczne wraz z opisem ich roli w kodzie.

3. Weryfikacja wymagań na testach SAT

- 3.1.** Wykonawca powinien wykonać testy potwierdzające, że kod użyty w testach SAT jest tym samym, który był używany podczas testów FAT (porównanie odnosi się do wersji, która została zapisana po zakończeniu testów FAT). W przypadku konieczności wprowadzenia modyfikacji w kodzie po testach FAT Wykonawca musi uzyskać najpierw zgodę Zamawiającego.
- 3.2.** Wykonawca powinien zabezpieczyć hasłem dostęp do kodu źródłowego oprogramowania jeśli kod może zostać odczytany bezpośrednio z urządzenia oraz przekazać Zamawiającemu to hasło.

4. Utrzymanie w okresie gwarancyjnym

- 4.1.** Wszystkie aktualizacje oprogramowania i poprawki powinny być sprawdzone w środowisku testowym Wykonawcy przed wprowadzeniem do wersji produkcyjnej i powinny być wprowadzone zgodnie ze standardami oraz najlepszymi praktykami użytymi przy tworzeniu oprogramowania.

Rozdział VIII

Usuwanie podatności w Systemie OT/SCADA

Podrozdział VIIIa

Notyfikacje i powiadomienia ze strony Wykonawcy

1. Wymagania

- 1.1.** Wykonawca powinien wdrożyć i dostarczyć dokumentację procesu usuwania podatności w Systemie OT/SCADA.
- 1.2.** Wykonawca powinien zapewnić odpowiednie aktualizacje oprogramowania mające na celu załatanie wykrytych podatności przez okres zapisany w umowie, ale nie krócej niż 2 lata.
- 1.3.** W przypadku gdy Wykonawca uzyskał informację lub wykrył podatności związane z bezpieczeństwem w Systemie OT/SCADA powinien powiadomić o takiej sytuacji Zamawiającego w ciągu 5 dni od jej wykrycia lub pozyskania informacji.
- 1.4.** Powiadomienie powinno zawierać, ale nie ograniczać się do, szczegółowego opisu podatności wraz z opisem jej potencjalnego wpływu na bezpieczeństwo Systemu OT/SCADA, oceną ryzyka zmaterializowania się podatności oraz do rekomendacji wraz z opisem działań naprawczych.

2. Weryfikacja wymagań na testach FAT

- 2.1.** Wykonawca powinien zweryfikować czy wszystkie znane Wykonawcy podatności zostały usunięte.
- 2.2.** Wykonawca powinien przekazać Zamawiającemu oświadczenie o usunięciu wszystkich znanych Wykonawcy lub opublikowanych podatności w Systemie OT/SCADA.
- 2.3.** Wykonawca powinien sprawdzić kompletność oraz poprawność dokumentacji opisującej proces usuwania podatności w Systemie OT/SCADA.

3. Weryfikacja wymagań na testach SAT

- 3.1.** Wykonawca powinien zweryfikować czy wszystkie znane Wykonawcy podatności zostały usunięte.
- 3.2.** Wykonawca powinien przekazać Zamawiającemu oświadczenie o usunięciu wszystkich znanych Wykonawcy lub opublikowanych podatności w Systemie OT/SCADA.

4. Utrzymanie w okresie gwarancyjnym

- 4.1.** W przypadku ujawnienia podatności w ramach utrzymania Systemu Wykonawca jest zobowiązany do obsługi podatności zgodnie z punktami 1, 2 i 3 powyżej przy zastrzeżeniu, że usunięcie podatności wymaga uprzednich ustaleń szczegółów i uzyskania zgody Zamawiającego.
- 4.2.** Wykonawca powinien przechowywać, przez okres zapisany w umowie (ale nie krócej niż 5 lat) listę wszystkich podatności oraz działań naprawczych w celach audytowych.

Podrozdział VIIIb

Zgłaszanie podatności przez Zamawiającego

1. Wymagania

- 1.1.** Wykonawca powinien zapewnić obsługę procesu zgłaszania przez Zamawiającego luk bezpieczeństwa oraz przesyłania raportów o problemach i żądania działań naprawczych przez okres zapisany w umowie, ale nie krócej niż 2 lata.
- 1.2.** Proces powinien umożliwiać Zamawiającemu śledzenie historii zgłoszeń oraz raportowanie stanu działań naprawczych.
- 1.3.** Wykonawca powinien podjąć zgłoszenie oraz przedstawić wstępny plan działania w ciągu 24 godzin od zgłoszenia problemu.
- 1.4.** Wykonawca powinien zapewnić odpowiednią ochronę procesu zgłaszania problemów dotyczących luk w zabezpieczeniach przed publicznym ujawnieniem zarówno w trakcie przesyłania jak również w trakcie przechowywania zgłoszeń.
- 1.5.** Wykonawca powinien dostarczyć Zamawiającemu raport z analizy zgłoszonej luki w Systemie OT/SCADA w czasie nie dłuższym niż 10 dni roboczych i zapewnić działania naprawcze, poprawki lub wskazówki dotyczące monitorowania luki w zabezpieczeniach.

- 1.6. Wykonawca powinien przechowywać do celów audytu historię zgłoszonych podatności bezpieczeństwa w systemach zabezpieczeń, w tym kroki zaradcze podjęte dla każdej z nich przez okres co najmniej 5 lat.
- 1.7. Wykonawca powinien udostępnić historię zgłaszanych luk bezpieczeństwa na żądanie Zamawiającego.

2. Weryfikacja wymagań na testach FAT

- 2.1. Wykonawca powinien przetestować kanały zgłaszania luk w Systemach OT/SCADA.

3. Weryfikacja wymagań na testach SAT

- 3.1. Zamawiający powinien przetestować kanały zgłaszania luk w Systemach OT/SCADA.

4. Utrzymanie w okresie gwarancyjnym

- 4.1. W przypadku zgłoszenia przez Zamawiającego podatności w ramach utrzymania Systemu, Wykonawca jest zobowiązany do obsługi podatności zgodnie z Podrozdziałem VIIIa, punkty 1, 2 i 3 przy zastrzeżeniu, że usunięcie podatności wymaga uprzednich ustaleń szczegółów i uzyskania zgody Zamawiającego.
- 4.2. Wykonawca powinien przetestować wszelkie poprawki w środowisku testowym przed wgraniem ich do środowiska produkcyjnego Zamawiającego.

Rozdział IX

Wykrywanie i ochrona przed złośliwym oprogramowaniem

1. Wymagania

- 1.1. Wykonawca powinien ujawnić Zamawiającemu istnienie wszelkich znanych lub zidentyfikowanych luk bezpieczeństwa w Systemie OT/SCADA utworzonych umyślnie w celu późniejszego wykorzystania, tzw. „backdoor”.
- 1.2. Wykonawca musi wdrożyć co najmniej jedno z następujących rozwiązań:
 - 1.2.1. Wykonawca zapewni możliwość wykrywania złośliwego oprogramowania poprzez monitorowanie Hostów. Wykonawca skonfiguruje narzędzie do wykrywania złośliwego oprogramowania tak, aby wysyłało powiadomienie o wykryciu podejrzanych plików zamiast automatycznego usuwania ich. Wykonawca zapewni proces aktualizacji sygnatur narzędzia do wykrywania złośliwego oprogramowania. Wykonawca powinien przetestować i potwierdzić poprawność działania poprawek i uaktualnień aplikacji do wykrywania złośliwego oprogramowania przed przekazaniem do Zamawiającego.
 - 1.2.2. Jeśli Wykonawca nie dostarcza narzędzia do wykrywania złośliwego oprogramowania w oparciu o monitorowanie Hostów wówczas powinien zaproponować Zamawiającemu listę produktów do wykrywania złośliwego oprogramowania, które mogą zostać zainstalowane przez Zamawiającego. Wykonawca powinien również dostarczyć przewodnik do

konfiguracji tych narzędzi w celu zapewnienia niezakłóconej pracy Systemu przez te narzędzia.

- 1.3. Działanie narzędzia do wykrywania złośliwego oprogramowania nie powinno wpływać na wydajność pracy Systemu OT/SCADA.
- 1.4. Narzędzie do wykrywania złośliwego oprogramowania powinno być skonfigurowane tak, aby pobranie i zainstalowanie nowych sygnatur było akceptowane przez użytkownika lub administratora Systemu.
- 1.5. Narzędzie do wykrywania złośliwego oprogramowania powinno być skonfigurowane tak, aby rozpoczęcie skanowania wymagało uzyskania akceptacji użytkownika Systemu.

2. Weryfikacja wymagań na testach FAT

- 2.1. Wykonawca powinien wykonać oraz udokumentować pomiary wydajności Systemu OT/SCADA obejmujące System OT/SCADA z uruchomionym oraz wyłączonym systemem wykrywania złośliwego oprogramowania.
- 2.2. Wykonawca powinien przeprowadzić test aktualizacji narzędzia do wykrywania złośliwego oprogramowania.
- 2.3. Wykonawca powinien przetestować działanie narzędzia do wykrywania złośliwego oprogramowania na różnych próbkach.
- 2.4. Wykonawca powinien udokumentować wszystkie znane na dzień testów luki „backdoors” w Systemie OT/SCADA.

3. Weryfikacja wymagań na testach SAT

- 3.1. Wykonawca powinien wykonać oraz udokumentować pomiary wydajności Systemu OT/SCADA obejmujące System OT/SCADA z uruchomionym oraz wyłączonym systemem wykrywania złośliwego oprogramowania.
- 3.2. Wykonawca powinien przeskanować wszystkie nośniki danych oraz urządzenia wchodzące w skład Systemu przy użyciu najbardziej aktualnych wersji narzędzia oraz sygnatur do wykrywania złośliwego oprogramowania.

4. Utrzymanie w okresie gwarancyjnym

- 4.1. Wykonawca powinien zapewnić przechowywanie dziennika zdarzeń narzędzia wykrywającego złośliwe oprogramowanie przez okres co najmniej 2 lat.
- 4.2. Wykonawca powinien aktualizować narzędzie do wykrywania złośliwego oprogramowania zgodnie z wymaganiami.

Rozdział X Nazwy Hostów oraz adresacja

1. Wymagania

- 1.1. Wykonawca powinien uzgodnić z Zamawiającym zakresy adresów sieciowych oraz metodę rozwiązywania nazw Hostów.
- 1.2. Wykonawca powinien dostarczyć skonfigurowany serwer (serwery) DNS lub informacje do skonfigurowania serwera (serwerów) DNS.

- 1.3. Wykonawca powinien zapewnić środki do weryfikacji integralności plików konfiguracyjnych, danych strefowych i innych plików DNS.
- 1.4. Informacje o adresacji powinny być traktowane jako wrażliwe i powinny być odpowiednio chronione.

2. Weryfikacja wymagań na testach FAT

- 2.1. Wykonawca powinien zainstalować i uruchomić serwery DNS na potrzeby przeprowadzenia testów FAT.
- 2.2. Wykonawca powinien zweryfikować czy nazwy wszystkich serwerów oraz Hostów w domenie biorącej udział w testowaniu są odpowiednio rozwiązywane.
- 2.3. Wykonawca powinien zweryfikować rozwiązywanie nazw zarówno do przodu (nazwa Hosta na adres IP), jak i odwrotne (adres IP do nazwy Hosta).

3. Weryfikacja wymagań na testach SAT

- 3.1. Serwery DNS powinny być uruchomione podczas trwania całego testu SAT.
- 3.2. Wykonawca powinien zweryfikować czy nazwy wszystkich serwerów oraz Hostów w domenie biorącej udział w testowaniu są odpowiednio rozwiązywane przez wszystkie systemy klienckie i serwerowe podłączone do sieci Systemu OT/SCADA.

4. Utrzymanie w okresie gwarancyjnym

- 4.1. Wykonawca powinien zapewnić proces zarządzania poprawkami dla DNS oraz powiązanych usług.

Rozdział XI

Urządzenia obiektowe

1. Wymagania

- 1.1. Wykonawca powinien zapewnić bezpieczeństwo cybernetyczne urządzeń obiektowych, w tym między innymi poprzez kontrolę dostępu i uwierzytelnianie, użycie połączeń szyfrowanych, rejestrowanie zdarzeń na urządzeniach i zdarzeń w komunikacji z nimi, monitorowanie i alarmowanie w celu ochrony urządzenia przed nieautoryzowaną modyfikacją lub użyciem.
- 1.2. Wykonawca powinien udokumentować zaimplementowane fizyczne i cybernetyczne funkcje bezpieczeństwa oraz dostarczyć instrukcję utrzymania funkcji bezpieczeństwa, w tym opis metod zmiany konfiguracji.
- 1.3. Wykonawca powinien zweryfikować czy implementacja funkcji bezpieczeństwa nie wpływa niekorzystnie na jakość komunikacji (opóźnienia, przepustowość, czas odpowiedzi).
- 1.4. Wykonawca powinien usunąć lub wyłączyć wszystkie funkcje, które nie są wymagane do działania lub konserwacji urządzenia. Wykonawca powinien udokumentować wszystkie wyłączone lub usunięte funkcje.
- 1.5. Wykonawca powinien zapewnić odpowiednie aktualizacje dla urządzeń obiektowych przez okres zapisany w umowie, ale nie krótszy niż 2 lata.

2. Weryfikacja wymagań na testach FAT

- 2.1.** Wykonawca powinien zweryfikować i potwierdzić implementację wszystkich funkcji bezpieczeństwa zgodnie z dokumentacją Systemu OT/SCADA.
- 2.2.** Wykonawca powinien sprawdzić i potwierdzić, że wszystkie zatwierdzone aktualizacje zabezpieczeń i poprawki są zainstalowane.
- 2.3.** Wykonawca powinien sprawdzić i potwierdzić, że wszystkie nieużywane funkcje i usługi zostały usunięte lub wyłączone.
- 2.4.** Wykonawca powinien, po zakończeniu testów FAT, udokumentować bazową konfigurację urządzeń, w tym między innymi zaimplementowane funkcje zabezpieczeń cybernetycznych, listy oprogramowania, listy używanych protokołów, portów i usług.
- 2.5.** Wykonawca powinien przeprowadzić testy wydajności pracy Systemu OT/SCADA w celu potwierdzenia, że implementacja funkcji bezpieczeństwa nie wpływa niekorzystnie na jakość komunikacji (opóźnienia, przepustowość, czas odpowiedzi).

3. Weryfikacja wymagań na testach SAT

- 3.1.** Wykonawca powinien, po zakończeniu testów SAT, udokumentować bazową konfigurację urządzeń, w tym między innymi zaimplementowane funkcje zabezpieczeń cybernetycznych, listy oprogramowania, listy używanych protokołów, portów i usług.
- 3.2.** Wykonawca powinien zweryfikować i dostarczyć dokumentację potwierdzającą, że wszelkie skonfigurowane przez Wykonawcę, domyślne oraz testowe konta producenta, nazwy użytkowników, hasła, ustawienia zabezpieczeń, kody bezpieczeństwa i inne metody dostępu zostały zmienione, wyłączone lub usunięte.
- 3.3.** Zamawiający powinien skonfigurować własne konta dostępu do urządzeń obiektowych.

4. Utrzymanie w okresie gwarancyjnym

- 4.1.** Wykonawca powinien zapewnić uaktualnienia i poprawki dla urządzeń obiektowych w celu utrzymania ustalonego poziomu bezpieczeństwa Systemu przez okres zawarty w umowie, ale nie krócej niż 2 lata. Aktualizacje powinny być instalowane tylko wówczas, gdy dotyczą funkcji, które nie zostały wyłączone.
- 4.2.** Wykonawca powinien przetestować uaktualnienie oraz poprawki przed wgraniem ich do środowiska produkcyjnego Zamawiającego.
- 4.3.** Wykonawca powinien udokumentować wszystkie zmiany w Systemie OT/SCADA w okresie gwarancji / utrzymania.

Rozdział XII

Zdalny dostęp

1. Wymagania

- 1.1.** Wykonawca powinien udokumentować wszystkie ścieżki zdalnego dostępu i zapewnić możliwość ich włączenia lub wyłączenia przez Zamawiającego w razie potrzeby.

- 1.2. Zdalny dostęp do Systemu OT/SCADA powinien być realizowany z wykorzystaniem infrastruktury zdalnego dostępu Zamawiającego.
- 1.3. Zdalny dostęp do Systemu OT/SCADA powinien być realizowany poprzez tunel VPN z wykorzystaniem uwierzytelniania dwuskładnikowego.
- 1.4. Zdalny dostęp do Systemów OT/SCADA może być zestawiony tylko przez Zamawiającego na czas niezbędny do wykonania prac przez Wykonawcę.
- 1.5. Wykonawca powinien dostarczyć lub wykorzystać istniejące wyizolowane środowisko pod względem bezpieczeństwa poza siecią Systemu OT/SCADA (np. wykorzystując strefę zdemilitaryzowaną OT DMZ) w celu zestawienia komunikacji z urządzeniami w sieci OT/SCADA.
- 1.6. Wykonawca powinien skonfigurować komponenty tunelowania komunikacyjnego, aby zapewnić ochronę typu end-to-end (np. szyfrowanie typu end-to-end) przesyłanych danych.
- 1.7. Wszystkie komputery Wykonawcy łączące się z siecią wewnętrzną Zamawiającego za pomocą technologii zdalnego dostępu muszą korzystać z aktualnego oprogramowania antywirusowego, zaktualizowanego systemu operacyjnego oraz nie powinny być wykorzystywane do innej pracy niż ta związana bezpośrednio ze wsparciem inżynierskim w zakresie Systemu OT/SCADA.
- 1.8. Zdalny dostęp może zostać przydzielony Wykonawcy na okres realizacji inwestycji oraz/lub w trakcie trwania okresu gwarancyjnego / serwisu utrzymania.
- 1.9. O wszelkich połączeniach zdalnych Wykonawca powinien wcześniej poinformować Zamawiającego. Wykonawca powinien informować również o zakończeniu prac, (wyłączenie dostępu).
- 1.10. Podczas zdalnego połączenia do Systemu OT/SCADA Wykonawca musi zapewnić, że komputer użyty do zdalnego połączenia jest podłączony tylko do sieci dostępowej połączenia zdalnego.
- 1.11. Jeżeli istnieje konieczność ciągłego przesyłania danych do Wykonawcy (np. do celów monitorowania parametrów pracy urządzeń przez Wykonawcę), Zamawiający dopuszcza możliwość przesyłania danych przez tunel VPN z szyfrowaniem end-to-end oraz zastosowaniem fizycznej diody danych w strefie DMZ.

2. Weryfikacja wymagań na testach FAT

- 2.1. Wykonawca powinien zweryfikować działanie wszystkich ścieżek zdalnego dostępu do Systemów OT/SCADA.
- 2.2. Wykonawca powinien przeprowadzić skanowanie portów Systemu OT/SCADA w celu potwierdzenia, że w Systemie OT/SCADA nie zostały zaimplementowane inne ścieżki dostępu zdalnego niż te ujęte w dokumentacji.

3. Weryfikacja wymagań na testach SAT

- 3.1. Wykonawca powinien przeprowadzić próby działania wszystkich ścieżek zdalnego dostępu do Systemu OT/SCADA.
- 3.2. Wykonawca powinien przeprowadzić skanowanie portów Systemu OT/SCADA w celu potwierdzenia, że w Systemie OT/SCADA nie zostały zaimplementowane inne ścieżki zdalnego dostępu niż te ujęte w dokumentacji.
- 3.3. Wykonawca powinien zweryfikować i dostarczyć dokumentację potwierdzającą, że wszystkie konta skonfigurowane przez Wykonawcę, konta domyślne

producenta lub konta testowe, nazwy użytkowników, hasła, ustawienia zabezpieczeń, kody bezpieczeństwa i inne metody dostępu zostały zmienione, wyłączone lub usunięte.

4. Utrzymanie w okresie gwarancyjnym

- 4.1.** Wykonawca nie powinien bez zgody Zamawiającego tworzyć innych ścieżek dostępu zdalnego do Systemu OT/SCADA niż te przewidziane w projekcie powykonawczym.
- 4.2.** Wykonawca powinien przeprowadzić przed testami SAT oraz okresowo raz na rok począwszy od testów SAT skanowanie bezpieczeństwa urządzeń używanych przez Wykonawcę do połączeń zdalnych oraz dostarczać wyniki skanowania Zamawiającemu.
- 4.3.** Wykonawca powinien poinformować Zamawiającego o konieczności zmian haseł, kodów dostępu np. w przypadku zmian kadrowych po stronie Wykonawcy.
- 4.4.** Wykonawca powinien udokumentować wszystkie zmiany w Systemie OT/SCADA w okresie gwarancji / utrzymania po uprzedniej akceptacji zmian przez Zamawiającego.

Rozdział XIII

Bezpieczeństwo fizyczne

1. Wymagania

- 1.1.** Wykonawca powinien opracować szczegółowy plan implementacji odpowiednich mechanizmów bezpieczeństwa fizycznego.
- 1.2.** Wykonawca powinien dostarczyć zamykane obudowy z urządzeniami blokującymi dla elementów systemu sterowania (np. Serwerów, sterowników PLC, sprzętu sieciowego, itp.).
- 1.3.** Wykonawca powinien zapewnić urządzenia blokujące z co najmniej dwoma kluczami dla każdego zamka, które można jednoznacznie zidentyfikować dla poszczególnych zamków.
- 1.4.** Wykonawca powinien zainstalować urządzenia blokujące dostęp do pomieszczenia, w którym znajdują się urządzenia Systemu OT/SCADA lub je zarekomendować, jeśli nie są w zakresie zamówienia Wykonawcy.
- 1.5.** Wykonawca powinien zweryfikować i dostarczyć dokumentację potwierdzającą, że nieautoryzowane urządzenia rejestrujące nie są zainstalowane (np. rejestratory kluczy, kamery i mikrofony).
- 1.6.** Wykonawca powinien zapewnić uwierzytelnianie dwuwarstwowe dla fizycznej kontroli dostępu.

2. Weryfikacja wymagań na testach FAT

- 2.1.** Wykonawca powinien wykonać testy działania poszczególnych mechanizmów bezpieczeństwa fizycznego.
- 2.2.** Wykonawca powinien przeprowadzić test dopasowania kluczy do poszczególnych zamków oraz zweryfikować ich oznakowanie.

3. Weryfikacja wymagań na testach SAT

- 3.1.** Wykonawca powinien wykonać testy działania poszczególnych mechanizmów bezpieczeństwa fizycznego.
- 3.2.** Wykonawca powinien przeprowadzić test dopasowania kluczy do poszczególnych zamków oraz zweryfikować ich oznakowanie.

4. Utrzymanie w okresie gwarancyjnym

- 4.1.** W razie konieczności wymiany środków bezpieczeństwa fizycznego wykonawca powinien utrzymać ich konfigurację i standard zgodnie z projektem powykonawczym.

Rozdział XIV

Segmentacja Systemu OT/SCADA

Podrozdział XIVa

Urządzenia sieciowe

1. Wymagania

- 1.1.** Wykonawca powinien skonfigurować urządzenia sieciowe tak, aby umożliwić podłączenie ich do scentralizowanego systemu zarządzania urządzeniami sieciowymi Zamawiającego.
- 1.2.** Wykonawca powinien opracować dokumentację zabezpieczeń interfejsów zarządzania konfiguracją sieci.
- 1.3.** Wykonawca powinien udokumentować listy kontroli dostępu (ACL) z uwzględnieniem docelowych i źródłowych adresów IP oraz potrzebnych do komunikacji portów.
- 1.4.** Wykonawca powinien usunąć lub wyłączyć wszystkie nieużywane funkcje konfiguracji sieci i zarządzania urządzeniami sieciowymi.
- 1.5.** Wykonawca powinien zapewnić architekturę NIPS, która będzie działać w warstwie aplikacyjnej protokołów komunikacyjnych.
- 1.6.** Wykonawca powinien zaimplementować reguły zapory ogniowej segmentów dla ruchu przychodzącego i wychodzącego bazując co do zasady na zestawie reguł tzw. „deny all”, z wyjątkami wyraźnie określonymi przez Wykonawcę, tzn. domyślne zablokowanie całej komunikacji na zaporze ogniowej i przepuszczanie wyłącznie granularnie określonych wyjątków komunikacji.
- 1.7.** Wykonawca powinien dostarczyć reguły NIDS i narzędzia do przeglądania dziennika, które weryfikują działanie zapór sieciowych i wykrywają nieautoryzowany ruch.
- 1.8.** Wykonawca powinien dostarczyć koncentratory VPN Systemu OT/SCADA uzgodnione z Zamawiającym ze skonfigurowanym filtrowaniem ruchu sieciowego na poziomie co najmniej adresów IP oraz portów sieciowych.
- 1.9.** Wykonawca powinien dostarczyć dokumentację dotyczącą zainstalowanych urządzeń sieciowych z wraz z ich konfiguracjami bezpieczeństwa.

2. Weryfikacja wymagań na testach FAT

- 2.1.** Wykonawca przed rozpoczęciem testów FAT powinien zainstalować najnowsze dostępne aktualizacje i poprawki urządzeń wchodzących w skład Systemu OT/SCADA oraz sprawdzić, czy dla tych wersji nadal istnieją podatności. Jeżeli tak, to powinien przekazać Zamawiającemu informacje nt. urządzeń i występujących na nich podatnościach pomimo wgrania najnowszego dostępnego oprogramowania oraz rekomendacje minimalizacji prawdopodobieństwa wystąpienia zdarzenia związanego z podatnością lub minimalizacji jego skutków.
- 2.2.** Wykonawca powinien wykonać testy funkcjonalne narzędzia do scentralizowanego zarządzania urządzeniami sieciowymi Systemu OT/SCADA.
- 2.3.** Wykonawca powinien przeprowadzić test działania ACL na urządzeniach sieciowych.
- 2.4.** Wykonawca powinien przeprowadzić i udokumentować wynik skanowania portów sieciowych w celu potwierdzenia, że wszystkie zbędne usługi zostały wyłączone lub usunięte.
- 2.5.** Wykonawca powinien przeprowadzić i udokumentować testy poprawności działania NIPS podczas normalnej i awaryjnej komunikacji Systemu OT/SCADA.
- 2.6.** Wykonawca powinien dostarczyć dokumentację reguł zapór ogniowych i reguł NIDS.
- 2.7.** Wykonawca powinien przeprowadzić testy działania NIDS wraz z przeglądaniem dziennika.
- 2.8.** Wykonawca powinien dostarczyć dokumentację architektury VPN Systemu OT/SCADA wraz z konfiguracją bezpieczeństwa.

3. Weryfikacja wymagań na testach SAT

- 3.1.** Wykonawca przed rozpoczęciem testów SAT w porozumieniu z Zamawiającym powinien zainstalować aktualizacje i poprawki urządzeń wchodzących w skład Systemu OT/SCADA.
- 3.2.** Wykonawca powinien wykonać testy funkcjonalne narzędzia do scentralizowanego zarządzania siecią Systemu OT/SCADA.
- 3.3.** Wykonawca powinien przeprowadzić test działania ACL.
- 3.4.** Wykonawca powinien przeprowadzić i udokumentować wynik skanowania portów sieciowych w celu potwierdzenia, że wszystkie zbędne usługi zostały wyłączone lub usunięte.
- 3.5.** Wykonawca powinien przeprowadzić i udokumentować testy poprawności działania NIPS podczas normalnej i awaryjnej komunikacji Systemu OT/SCADA.
- 3.6.** Wykonawca powinien dostarczyć dokumentację reguł zapór i reguł NIDS.
- 3.7.** Wykonawca powinien przeprowadzić testy działania NIDS wraz z przeglądaniem dziennika.
- 3.8.** Wykonawca powinien dostarczyć dokumentację architektury VPN Systemu OT/SCADA wraz z konfiguracją bezpieczeństwa.

4. Utrzymanie w okresie gwarancyjnym

- 4.1.** Wykonawca powinien zapewnić aktualizacje i poprawki w celu utrzymania ustalonego poziomu bezpieczeństwa Systemu OT/SCADA przez ustalony okres wsparcia (ale nie krócej niż przez 2 lata).

- 4.2.** Wykonawca powinien przeprowadzić testy aktualizacji i poprawek w środowisku testowym Wykonawcy przed dostarczeniem aktualizacji i poprawek Zamawiającemu.

Podrozdział XIVb

Architektura sieci

1. Wymagania

- 1.1.** Wykonawca powinien przestrzegać wymagań norm ISA/IEC 62443 dotyczących projektowania i konfiguracji segmentów sieci Systemu OT/SCADA.
- 1.2.** Wykonawca powinien zapewnić redundancję na poziomie połączeń i urządzeń.
- 1.3.** Wykonawca powinien podzielić sieci Systemu OT/SCADA na segmenty i wprowadzić techniczne zabezpieczenia (np. zapory ogniowe, jednokierunkowe urządzenia komunikacyjne lub koncentratory VPN) między segmentami sieci.
- 1.4.** Systemy krytyczne (np. ESD, SIS) powinny być umieszczone w dedykowanych segmentach Systemu OT/SCADA.
- 1.5.** Wykonawca powinien udokumentować wszystkie ścieżki komunikacji między poszczególnymi segmentami Systemu OT/SCADA.
- 1.6.** Wykonawca powinien przeprowadzić i udokumentować analizę krytyczności poszczególnych segmentów Systemu OT/SCADA.
- 1.7.** Wykonawca powinien zaimplementować bezpieczną architekturę sieci Systemu OT/SCADA, w której strefy o wyższym poziomie bezpieczeństwa inicjują komunikację do stref o niższym poziomie bezpieczeństwa.
- 1.8.** Wykonawca powinien zaimplementować punkty rozłączenia pomiędzy segmentami oraz udostępnić metody izolowania podsieci, aby w razie potrzeby kontynuować pracę Systemu w trybie awaryjnym.
- 1.9.** Wykonawca powinien zaimplementować reguły filtrowania i monitorowania ruchu sieciowego dla wszystkich segmentów Systemu OT/SCADA wraz z alarmowaniem w przypadku wystąpienia nieautoryzowanego ruchu sieciowego.
- 1.10.** Wykonawca powinien przekazać Zamawiającemu wytyczne dotyczące włączenia monitorowania ruchu sieciowego Systemu OT/SCADA do urządzenia nadrzędnego Zamawiającego typu SIEM.
- 1.11.** Wykonawca powinien dostarczyć dokumentację architektury sieci zawierającą schematy architektury oraz jej opis.

2. Weryfikacja wymagań na testach FAT

- 2.1.** Wykonawca powinien przeprowadzić i udokumentować wyniki testów komunikacji w celu potwierdzenia, że segmenty o wyższym poziomie bezpieczeństwa nawiązują komunikację z segmentami o niższym poziomie bezpieczeństwa.
- 2.2.** Wykonawca powinien wykonać testy działania Systemu OT/SCADA w trybie awaryjnym po całkowitym odizolowaniu podsieci Systemu OT/SCADA.
- 2.3.** Wykonawca powinien przeprowadzić oraz udokumentować wyniki testów działania reguł filtrowania i monitorowania ruchu sieciowego pomiędzy poszczególnymi segmentami dla wszystkich rodzajów pracy Systemu OT/SCADA (rozruch, normalna praca, zatrzymanie, zatrzymanie awaryjne, itp.).

- 2.4.** Wykonawca powinien przeprowadzić test poprawności alarmowania z wywołaniem nieautoryzowanego ruchu sieciowego pomiędzy segmentami.

3. Weryfikacja wymagań na testach SAT

- 3.1.** Wykonawca powinien przeprowadzić i udokumentować wyniki testów komunikacji w celu potwierdzenia, że segmenty o wyższym poziomie bezpieczeństwa nawiązują komunikację z segmentami o niższym poziomie bezpieczeństwa.
- 3.2.** Wykonawca powinien wykonać testy działania Systemu OT/SCADA w trybie awaryjnym po odizolowaniu podsieci Systemu OT/SCADA.
- 3.3.** Wykonawca powinien przeprowadzić oraz udokumentować wyniki testów działania reguł filtrowania i monitorowania ruchu sieciowego pomiędzy poszczególnymi segmentami dla wszystkich rodzajów pracy Systemu OT/SCADA (rozruch, normalna praca, zatrzymanie, zatrzymanie awaryjne, itp.).
- 3.4.** Wykonawca powinien przeprowadzić test poprawności alarmowania z wywołaniem nieautoryzowanego ruchu sieciowego pomiędzy segmentami.

4. Utrzymanie w okresie gwarancyjnym

- 4.1.** Wykonawca powinien prowadzić analizę ruchu sieciowego pomiędzy segmentami Systemu OT/SCADA w celu lepszej kalibracji reguł filtrowania ruchu sieciowego.
- 4.2.** Wykonawca nie powinien wprowadzać zmian w architekturze sieci Systemu OT/SCADA bez zgody Zamawiającego.

Przepisy końcowe

1. Niniejsza regulacja wchodzi w życie z dniem 30 października 2019r.
2. Ewentualne uwagi do niniejszej regulacji należy zgłaszać do jej Właściciela, którym jest Dyrektor PC.
3. Zmiana treści załączników nie jest traktowana jako zmiana treści regulacji.

Załączniki

Załącznik nr 1 – Matryca parametrów wymaganych do aktualizacji rejestru komponentów Systemów OT/SCADA

Załącznik nr 2 – Rejestr komponentów Systemu OT/SCADA (plik MS Excel)