***Załącznik nr 1 do Umowy nr……z dnia…..***

**Opis przedmiotu zamówienia**

Przedmiotem zamówienia jest dostawa, uruchomienie i wdrożenie systemu klasy Security Orchestration, Automation And Response (SOAR) / Security Information and Event Management (SIEM) - System do zarządzania informacją i zdarzeniami, zwany dalej „Systemem” lub „oprogramowaniem”.

Zamawiający na potrzeby wdrożenia udostępni infrastrukturę na serwerach zwirtualizowanych, wg. specyfikacji uzgodnionych z Wykonawcą. Wszystkie czynności związane z wdrożeniem Systemu będącego przedmiotem umowy będzie wykonywał Wykonawca. Instalacja Systemu przez Wykonawcę odbywać się będzie w siedzibie Zamawiającego. Zamawiający może wyrazić zgodę na wykonanie prac zdalnie w całości lub części.

* + 1. WYMAGANIA FUNKCJONALNE

1. System musi zapewnić narzędzia do tworzenia elektronicznej, interaktywnej dokumentacji systemu teleinformatycznego, w tym schematów architektury sieci (tzn. mapy pokazującej urządzenia zabezpieczeń, strefy bezpieczeństwa, zasoby IT, połączenia i topologię sieci), prezentującej informacje nt. bezpieczeństwa w ujęciu technicznym oraz w odniesieniu do procesów działania organizacji.
2. System musi zapewnić narzędzia umożliwiające dokonanie oceny wpływu incydentu bezpieczeństwa IT na działalność organizacji, m.in. po wpisaniu adresu IP zasobu IT związanego z incydentem bezpieczeństwa system wyszukuje i prezentuje informacje nt. procesów organizacji i klasyfikowanych informacji (m.in. danych osobowych), które mogły zostać naruszone w wyniku incydentu oraz wyświetla przewidywane istotne dla organizacji konsekwencje naruszenia bezpieczeństwa.
3. System musi zapewnić narzędzia prezentujące techniczne informacje nt. bezpieczeństwa IT z perspektywy działalności organizacji. Umożliwia zapisywanie, wyszukiwanie i prezentowanie co najmniej następujących informacji: procesy działania organizacji, klasyfikacja zbiorów informacji, ważność zasobu IT dla organizacji, właściciel zasobu IT oraz zespół obsługi.
4. System musi zapewnić narzędzia służące do ustalania wrażliwych zbiorów informacji, jakie są narażone w razie incydentu bezpieczeństwa. Umożliwia definiowanie własnego schematu klasyfikacji danych w organizacji (np. własność intelektualna dane osobowe, dane finansowe) oraz umożliwia wyszukiwanie lokalizacji zasobów IT, gdzie znajdują się dane określonej kategorii oraz wskazywać je na graficznej mapie systemu teleinformatycznego.
5. System musi zapewnić narzędzia do modelowania zagrożeń umożliwiające symulowanie różnych potencjalnych scenariuszy incydentów bezpieczeństwa IT. Dostępne są narzędzia działające na graficznej mapie systemu teleinformatycznego służące m.in. do:
   1. wyznaczania źródła zagrożenia zasobu IT wraz z wynikiem analizy ryzyka dla tego zagrożenia wyliczanym w sposób automatyczny,
   2. wyświetlania zabezpieczeń zasobu IT przed potencjalnymi źródłami zagrożenia,
   3. wyświetlania zabezpieczeń chroniących zasoby IT przed określonym źródłem zagrożenia,
   4. wyświetlania lokalizacji zasobów określonego rodzaju,
   5. wyświetlania najbardziej narażonych zasobów IT,
   6. wyświetlania ważnych zasobów IT narażonych na awarie.
6. System musi zapewnić graficzne narzędzia do definiowania wymagań bezpieczeństwa organizacji (m.in. środków ochrony wymaganych dla określonych elementów i obszarów systemu teleinformatycznego) oraz narzędzia do audytowania bezpieczeństwa względem tych wymagań. Narzędzia Systemu muszą umożliwić m.in.:
   1. zweryfikowanie, czy stan bezpieczeństwa systemu teleinformatycznego odpowiada specyficznym wymaganiom organizacji,
   2. wyznaczenie zasobów IT o wysokim poziomie ryzyka, które nie posiadają wymaganych zabezpieczeń,
   3. wskazywanie zasobów IT o krytycznym znaczeniu dla organizacji, które nie posiadają odpowiednich zabezpieczeń,
7. System powinien zawierać narzędzia graficzne do tworzenia i przeszukiwania elektronicznej dokumentacji, prezentujący wyniki na schemacie mapy logicznej oraz fizycznej. Umożliwić rozbudowę elektronicznej dokumentacji o nowe parametry oraz dołączane dokumenty, odnoszące się m.in. do sfer bezpieczeństwa systemów zabezpieczeń, urządzeń fizycznych oraz zasobów informacyjno usługowych.
8. System musi posiadać możliwość wykrywania topologii sieci fizycznej oraz jej wizualizacji na podstawie następujących protokołów sieciowych: SNMP v2 i v3, LLDP, CDP.
9. System musi posiadać mechanizmy umożliwiające rozpoznanie systemów IT ( Asset Discovery) oraz zapisuje wyniki w module elektronicznej dokumentacji zapewniając:
   1. możliwość wykrywania zasobów oraz ich parametrów na podstawie wyników przynajmniej jednego skanera podatności,
   2. możliwość wykrywania zasobów oraz ich parametrów na podstawie wyników przynajmniej jednego skanera sieciowego,
   3. możliwość wykrywania zasobów oraz ich parametrów przy wykorzystaniu protokołu WMI,
   4. możliwość wykrywania zasobów oraz ich parametrów przy wykorzystaniu skryptów SSH oraz PowerShell,
   5. możliwość wykrywania zasobów oraz ich parametrów na podstawie interpretacji zdarzeń
10. System musi posiadać bazę wiedzy eksperckiej zawierających wiedzę pozwalającą ocenić poprawność projektu zabezpieczeń identyfikując efektywność zastosowanych mechanizmów sieciowych oraz lokalnych w stosunku do potencjalnych wektorów ataków oraz w przypadku ich nie zastosowania zidentyfikować ryzyka, które się z tym wiążą.
11. System musi zapewnić możliwość definiowania procesów organizacji oraz zależności od innych procesów, a także zapewnić możliwość definiowania czasów ich aktywności (np. proces praca biurowa w organizacji jest aktywny od pon do pt od 8:15 do 16:15). Zależności muszą być prezentowane w postaci graficznej.
12. System musi posiadać mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT zdefiniowanego w elektronicznej dokumentacji oraz prezentacji tych informacji w formie graficznej.
13. Elektroniczna dokumentacja zapisana w systemie musi umożliwić automatyczne wyszukiwanie pojedynczych punktów awarii sieci i systemów IT (tzn. elementów bez redundancji), których uszkodzenie spowoduje zablokowanie ważnych procesów organizacji.
14. System powinien umożliwiać automatyczne szacowanie ryzyka dla wszystkich systemów IT zdefiniowany w elektronicznej dokumentacji. Szacowanie ryzyka powinno odbywać się względem zagrożeń natury informatycznej, np. włamanie, infekcja złośliwym programem, podsłuch sieciowy, awaria.
15. System w formie graficznej powinien prezentować podsumowanie aktualnego stanu bezpieczeństwa, m.in. procesy organizacji zagrożone przez pojedyncze punkty awarii.
16. System powinien zapewniać możliwość monitorowania aktywności stron internetowych, portów TCP, ICMP oraz mapowania czasów dostępności/niedostępność bezpośrednią na procesy biznesowe oraz procesy zależne. W przypadku wykrycia niedostępność monitorowanej usługi generować alarm powiadamiając jednocześnie właścicieli procesów biznesowych, których procesy zależą w sposób pośredni lub bezpośredni od tej usługi (np. email, sms, komunikator).

Moduł Security Information and Event Management (SIEM)

1. System musi zapewnić parsowanie spływających do niego zdarzeń w następujących formach:
   1. Syslog,
   2. Wiadomości email,
   3. Dziennik zdarzeń Windows (WEF)

Przez parsowanie zdarzeń rozumie się proces analizy zdarzenia i rozkład na elementy składowe takie jak np. adres IP źródła, adres IP docelowy, data, czas, użytkownik, treść . zdarzenia itp.

1. System musi umożliwiać zaprojektowanie i wdrożenie przesyłania, parsowania, korelowania i przechowywania logów i innych danych z co najmniej z następujących źródeł:

* Systemy bezpieczeństwa: Check Point, Palo Alto, Juniper SSG, Trend Micro Deep Security, Pulse Connect Secure, Fidelis, Fudo
* Firewalle WAF: F5 Networks, Imperva, Fortinet
* Urządzeń CISCO: przełączniki, routery, firewalle
* Systemu operacyjne: Red Hat, Microsoft Windows
* Usługi serwerowe: DNS, DHCP, WWW (Apache, IIS)
* Bazy danych: Oracle, SQL Server, MySQL, Postgres
* System powinien umożliwiać zbieranie danych netflow o wydajności 200tys fpm
* Systemy wirtualizacji: Vmware vSphere, Red Hat Virtualization
* Logi Windows Events (Logi Application, Security, System I inne)
* Login z systemu kontroli dostępu

1. Zaoferowany System musi umożliwiać pobieranie logów / danych zapisanych w plikach (dziennikach systemowych / aplikacyjnych) jak również w postaci komunikatów przechwytywanych z portów TCP/UDP oraz z wykorzystaniem następujących mechanizmów:
   * Wysyłanie logów / danych ze źródłowego systemu na wskazany port TCP/UDP serwera, będącego częścią wdrażanego rozwiązania (minimalnie syslog)
   * Rozwiązanie musi wspierać zbieranie danych w formacie CEF oraz przyjmowanie logów z Syslog Relay
   * Wskazanie w interfejsie użytkownika wdrażanego rozwiązania Systemu na znajdujący się lokalnie plik / katalog.
   * Wykonywanie przez zaoferowane rozwiązania zapytań SQL w zewnętrznych bazach danych i pobieranie wyników zapytań. Alternatywnie musi istnieć możliwość komunikacji z bazami danych w standardzie JDBC lub ODBC.
   * Windows Management Infrastructure (WMI)
   * Checkpoint OPSEC LEA
2. System musi posiadać predefiniowany zestaw parserów zdarzeń.
3. System musi zapewnić mechanizmy umożliwiające mu na pozyskiwanie zdarzeń z baz danych oraz plików płaskich.
4. System musi posiadać wbudowany interfejs do tworzenia własnych parserów umożliwiający:
   1. parsowanie warunkowe,
   2. wzbogacanie zdarzeń o dodatkowe pola,
   3. mapowanie wartości,
   4. zastosowanie wyrażeń regularnych,
   5. wsparcie dla formatów JSON oraz XML,
   6. wykorzystanie gotowych procesów przy tworzeniu nowych,
   7. mechanizmy wykorzystania w polach zdarzeń
5. System musi zapewnić możliwości zbierania i przetwarzania informacji dot. Przepływów sieciowych (ang. Netflow)
6. System musi umożliwić analizę anomalii, bazując na informacjach zbieranych z przepływów sieciowych, gdzie w zależności od zdefiniowanych reguł buduje dynamiczne linie trendów wykrywając odchylenia związane z procentową zmianą poziomu transmisji.
7. System musi umożliwić zastosowanie filtrów pozwalających na analizę anomalii względem parametrów zdefiniowanych w dokumentacji, tj. rodzaj zasobu, strefa bezpieczeństwa, proces biznesowy.
8. System musi odczytywać alarmy wysłane z innych systemów, w tym systemów zabezpieczeń, dla których na podstawie zawartych w dokumentacji automatycznie oszacowuje konsekwencje incydentów bezpieczeństwa, m.in. jakie procesy organizacji mogą zostać zakłócone, jakie informacje klasyfikowane mogą zostać skradzione przez przestępców.
9. System musi posiadać mechanizm definiowania reguł analizy incydentów dla każdego odbieranego zdarzenia. Reguły musza umożliwiać korelację informacji technicznych wyciągniętych ze zdarzenia przekazanego z innych systemów (m.in. adres IP, kategoria, severity) z parametrami zdefiniowanymi w dokumentacji (m.in. ważność zasobu, klasyfikowane informacje, procesy organizacji) oraz aktualnymi incydentami bezpieczeństwa.
10. System musi umożliwiać detekcję anomalii poprzez osiągnięcie określonej liczby punktów na danym zasobie wyliczonych z sum punktów wszystkich zdarzeń na nim występujących w określonym przedziale czasu. W tym celu wynik działania reguł korelacyjnych jest oceniany w skali punktowej w odniesieniu do rodzaju zasobu oraz jego parametrów.
11. System musi pozwalać na budowanie profili aktywności użytkowników oraz zasobów poprzez wielowartościowe listy referencyjne przykładowo nazwa użytkownika, aplikacja i adres docelowy oraz umożliwiać wykorzystywanie ich w regułach korelacyjnych.
12. Wykryte incydenty muszą być priorytetowe w odniesieniu do ważności oraz organizacji zasobów których dotyczą (tzn. wspomaganie procesów, przetwarzanie informacji klasyfikowanych). System musi udostępnić graficzny edytor pozwalający na dostosowanie reguł wyznaczania priorytetów obsługi względem dowolnych parametrów zawartych w dokumentacji.
13. Dla rejestrowanych incydentów System musi wyznaczać ścieżkę ataku i prezentować ją w formie graficznej na schemacie sieci. Ścieżka ataku musi pokazywać wszystkie urządzenia zabezpieczeń na drodze pomiędzy sprawcą i ofiarą ataku.
14. System w razie wykrycia incydentów o poważnych konsekwencjach dla organizacji musi umożliwić automatyczne powiadomienie o zdarzeniu wskazanych pracowników, m.in. email, sms.
15. System w formie graficznej musi prezentować podsumowanie aktualnego stanu bezpieczeństwa, m.in. procesy organizacji zagrożone przez incydenty bezpieczeństwa.
16. System musi udostępnić możliwość prezentacji danych w postaci tzw. Dashboard, czyli dostosuje zakres i prezentację danych do potrzeb administratora czy też zalogowanego użytkownika.
17. System powinien posiadać predefiniowane widoki dedykowane dla specjalistów odpowiedzialnych za poszczególne domeny bezpieczeństwa, minimalnie.:
    1. wykrywanie i przeciwdziałanie złośliwemu oprogramowaniu;
    2. wykrywanie i obsługa podatności;
    3. analiza ruchu sieciowego;
    4. analiza flow-ów sieciowych w oparciu o wbudowane reguły bezpieczeństwa, które są zintegrowane z ATT&CK MITRE.
    5. analiza oraz śledzenie wykorzystywanych portów i protokołów;
    6. analiza oraz śledzenie aktualizacji oprogramowania w ramach organizacji;
    7. analiza i śledzenie uprawnień dostępu.
    8. Wykrywanie ataków typu brute force na różne usługi, minimum: HTTP(s), FTP, IMAP, SSH, RDP, LDAPS, MS SQL
    9. Wykrywanie aktywności na podejrzanych portach (w oparciu o Black i White-listy)
    10. Wykrywanie nieautoryzowanego dostępu do określonych usług, w tym w szczególności niedozwolony dostęp do sieci Internet
    11. nieautoryzowana komunikacja z usługami DHCP, DNS, Mail Server (wykrywanie komunikacji z serwerami usług, które nie znajdują się na liście dozwolonych serwerów w organizacji, tzw. rogue servers)
    12. wykrywanie anomalii wskazujących na rozprzestrzeniania się złośliwego oprogramowania na podstawie nietypowych komunikacji pomiędzy stacjami roboczymi w organizacji
    13. wykrywanie komunikacji z podejrzanymi adresami IP (minimum: C2, Ransomware, Malware, Botnet) na podstawie zewnętrznych oraz customowych list reputacyjnych
    14. wykrywanie naruszeń polityk bezpieczeństwa poprzez monitorowanie minimum takich aktywności jak:
        1. Wykrywanie ataków typu brute force na różne usługi, minimum: HTTP(s), FTP, IMAP, SSH, RDP, LDAPS, MS SQL
        2. Wykrywanie aktywności na podejrzanych portach (w oparciu o Black i White-listy)
        3. Wykrywanie nieautoryzowanego dostępu do określonych usług:
        4. niedozwolony dostęp do sieci Internet
        5. nieautoryzowana komunikacja z usługami DHCP, DNS, Mail Server (wykrywanie komunikacji z serwerami usług, które nie znajdują się na liście dozwolonych serwerów w organizacji, tzw. rogue servers)
        6. wykrywanie anomalii wskazujących na rozprzestrzeniania się złośliwego oprogramowania na podstawie nietypowych komunikacji pomiędzy stacjami roboczymi w organizacji
        7. wykrywanie komunikacji z podejrzanymi adresami IP (minimum: C2, Ransomware, Malware, Botnet) na podstawie zewnętrznych oraz customowych list reputacyjnych
        8. wykrywanie komunikacji z siecią TOR (na podstawie automatycznie aktualizowanych feedów reputacyjnych)
        9. wykrywanie komunikacji z Open Proxy (na podstawie automatycznie aktualizowanych feedów reputacyjnych)
        10. wykrywanie komunikacji P2P na podstawie monitorowania portów popularnych serwisów P2P
    15. wykrywania prób eksfiltracji danych na podstawie analizy anomalii w protokołach sieciowych, co najmniej:
        1. anomalie w protokole DNS dot. nietypowej wielkości transferu danych czy też nietypowych wskaźników wysłanych/odebranych komunikatów DNS
        2. anomalie w protokole SMTP na wykrywane na podstawie parametru PPF (Packets per Flow)
        3. nietypowe transfery danych, w tym: transakcje powyżej zdefiniowanego progu
        4. anomalie w protokołach icmp, tcp oraz udp na podstawie wykorzystywania nietypowych rozmiarów pakietów
    16. wykrywanie różnych typów ataków DDoS, minimum: ICMP Flood, TCP Flood, UDP Flood, DNS Amplification w oparciu o co najmniej przedstawione parametry parametry: PPM (Packets Per Minute), BPP (Bytes Per Packet), liczba flowów sieciowych, liczba unikalnych adresów IP, liczba unikalnych ASN-ów w kontekście pary docelowy host: docelowy port.
    17. Wszystkie reguły powinny mieć możliwość whitelistowania poprawnych komunikacji poprzez grup adresów sieciowych oraz konfiguracji dopuszczalnych progów wyzwalania alertów bezpieczeństwa.

Moduł Security Orchestration, Automation And Response (SOAR)

1. System musi zawierać mechanizm definiowania scenariuszy obsługi incydentów uruchamianych na podstawie następujących kryteriów:
   1. w przypadku gdy zasób przetwarza zdefiniowane informacje klasyfikowane (np. dane osobowe),
   2. w przypadku gdy zasób jest elementem określonego procesu organizacji,
   3. w przypadku gdy zasób zlokalizowany jest w danej lokalizacji,
   4. w przypadku, gdy na zasobie może dojść do określonego cyber zagrożenia,
   5. w przypadku gdy na zasobie może dojść do określonej konsekwencji naruszenia bezpieczeństwa,
   6. w przypadku gdy na zasobie jest zainstalowany określony system operacyjny lub oprogramowanie
2. W ramach scenariuszy obsługi incydentów System musi umożliwić wykonanie następujących akcji i powiązanie ich z poszczególnymi krokami:
   1. zmianę operatora
   2. zmianę statusu,
   3. zmianę priorytetu,
   4. Przekazywanie i pobieranie parametrów z innych systemów poprzez skrypty SSH/PowerShell oraz REST API.
   5. wysłanie powiadomień,
   6. aktualizację dokumentów wraz z ich automatycznym wersjonowaniem,
   7. gromadzenie informacji na bazie podręcznego schowka oraz dołączenia plików wraz z wyliczaniem dla nich funkcji skrótu.
   8. aktualizację list referencyjnych,
   9. edycję bazy wiedzy zarówno w kontekście określonego wątku jak i definiowania nowych.
   10. założenie zadania.
3. System automatycznie musi proponować odpowiednie scenariusze obsługi incydentów. Scenariusze obsługi muszą zawierać możliwość ich symulacji i weryfikacji, m.in. na przykładowe zasoby IT.
4. Wymagana jest konfiguracja Systemu, w ramach której przebieg scenariusza dostosuje się dynamicznie do pozyskania w ramach jego obsługi informacji umożliwiając następujące funkcjonalności:
   1. automatyzację wykonania wielu kroków nie wymagających reakcji operatora,
   2. warunkowe wykonywanie kroków w zależności od informacji zawartej zarówno w elektronicznej dokumentacji jak i informacji pozyskanej z innych systemów,
   3. warunkowe wykonywanie kroków w zależności od odpowiedzi operatora na zdefiniowane pytanie.
5. System powinien posiadać gotowe integracje z producentami narzędzi do skanowania podatności (tzn. narzędzi Vunreability Assessment).
6. System na podstawie wyników skanowania podatności musi umożliwić identyfikowanie komputerów na podstawie ich nazw pozwalając tym samym na procesowanie podatności danego komputera przy dynamicznym adresie IP pobieranym z serwera DHCP.
7. System musi zawierać mechanizm definiowania scenariuszy obsługi podatności uruchamianych na podstawie następujących kryteriów:
   1. w przypadku gdy na zasób przetwarza zdefiniowane informacje klasyfikowane, np. dane osobowe,
   2. w przypadku gdy zasób jest elementem określonego procesu organizacji,
   3. w przypadku gdy zasób zlokalizowany jest w danej lokalizacji,
   4. w przypadku gdy na zasobie może dojść do określonego cyber zagrożenia,
   5. w przypadku gdy na zasobie może dojść do określonej konsekwencji naruszenia bezpieczeństwa,
   6. w przypadku gdy na zasobie jest zainstalowany określony system operacyjny lub oprogramowanie
8. W ramach scenariuszy obsługi podatności System umożliwia:
   1. zmianę operatora,
   2. zmianę statusu,
   3. zmianę priorytetu,
   4. przekazywanie i pobieranie parametrów z innych systemów poprzez skrypty SSH/PowerShell oraz REST API.
   5. wysłanie powiadomień.
   6. aktualizację dokumentów wraz z ich automatycznym wersjonowaniem,
   7. gromadzenie informacji na bazie podręcznego schowka oraz dołączenia plików wraz z wyliczaniem dla nich funkcji skrótu.
   8. aktualizację list referencyjnych,
   9. edycję bazy wiedzy zarówno w kontekście określonego wątku jak i definiowania nowych.
   10. założenie zadania.
9. System automatycznie musi proponować odpowiednie scenariusze obsługi podatności. Scenariusze obsługi muszą zawierać możliwości ich symulacji i weryfikacji, m.in. na przykładowym zasobie IT.
10. System w razie wykrycia podatności o poważnych konsekwencjach dla organizacji musi umożliwić automatyczne powiadomienie o zdarzeniu wskazanych pracowników, m.in. email/sms.
11. System w razie wykrycia podatności na podstawie informacji wyciągniętej z wyniku skanu musi automatycznie przydzielić odpowiedni zespół obsługi dla danego zdarzenia (np. przydzielenie osób dla podatności dot. Oprogramowania Microsoft, SQL Serwer). Podczas procesu przydzielania podatności dla zespołów obsługi system musi bierać pod uwagę ilość aktualnie obsługiwanych podatności przez członków zespołów (osoby które mają mniejszą ilość podatności będą mieli w pierwszej kolejności przypisywane nowe podatności, następnie będą one rozkładane pomiędzy osobami równomiernie).
12. System musi zapewnić możliwość tworzenia własnych wymagań bezpieczeństwa oraz ich weryfikacji względem zasobów IT, w tym serwerów, stacji roboczych oraz urządzeń sieciowych na bazie REST API, skryptów PowerShell/SSH oraz parametrów elektronicznej dokumentacji. System musi umożliwić rozbudowę list zgodności o wyniki działania przynajmniej jednego skanera podatności umożliwiającego przeprowadzenie skanowania typu COMPLIANCE.
13. System musi umożliwić budowanie grupy wymagań dotyczących zgodności z normami czy rozporządzeniami pozwalając wpisać do systemu poszczególne wymagania (np. punkty normy) oraz połączyć te wymagania ze skryptami je weryfikującymi. System pozwala na automatyczne zbudowanie raportu zgodności na podstawie wyników skryptów weryfikujących oraz innych parametrów elektronicznej dokumentacji.
14. System musi zawierać możliwość analizy poprawności konfiguracji poszczególnych elementów systemu teleinformatycznego np. przełączniki, systemu Firewall, serwery.
15. Prace przygotowawcze: narzędzia SOAR muszą zostać uruchomione na odpowiednim adresie IP w segmencie sieci chronionym przez Firewall, dostęp do narzędzi możliwy będzie tylko z komputerów upoważnionych użytkowników, zostaną zdefiniowane konta użytkowników z odpowiednimi uprawnieniami.
16. System musi realizować konfigurację schematu/ów klasyfikacji danych oraz schematu/ów klasyfikacji incydentów.
17. Zaoferowany System musi umożliwiać skonfigurowanie przekierowania alarmów z narzędzi SIEM i NBAD za pomocą protokołu syslog. Zweryfikowanie poprawności parsowania alarmów i w razie potrzeby dostrojenie parserów.
18. Wykonawca zobowiązany jest do wykonania w terminie 10 dni roboczych od podpisania umowy, logicznej architektury bezpieczeństwa teleinformatycznego Systemu. Architektura powinna opisywać urządzenia zabezpieczeń (Firewall, itp.) i ich połączenia sieciowe oraz systemu bezpieczeństwa i adresy IP oraz uzupełnienie architektury o system IT i OT ważne dla organizacji (na podstawie danych przekazanych przez zamawiającego), których incydenty wymagają natychmiastowego działania.
19. Wykonana przez Wykonawcę architektura bezpieczeństwa teleinformatycznego powinna być zaimplementowana w systemie IT oraz w postaci elektronicznej, która zostanie przekazana Zamawiającemu dokonać weryfikacji i dostrojenia scenariuszy obsługi incydentów i podatności bezpieczeństwa (tzn. wbudowanych playbooków) w ramach przyjętego procesu obsługi (tzn. Workflow). Zamawiający wymaga podczas wdrożenia konieczność skonfigurowania do 40 playbooków. Playbooki muszą umożliwiać automatyzację pracy ludzi i integrację z zewnętrznymi źródłami danych, m.in. Threat Inteligence. Przekazywanie i pobieranie parametrów z innych systemów odbywa się m.in. poprzez skrypty SSH/PowerShell oraz REST API.
20. Wymagane jest zapewnienie możliwości zweryfikowania działania wbudowanych w Systemie algorytmów szacowania ryzyka względem różnych wektorów ataków. W razie potrzeby dostrojenie parametrów dotyczących szacowania ryzyka.
21. Wymagane jest zapewnienie możliwości zweryfikowania predefiniowanych statystyk i raportów dotyczących obsługi incydentów i podatności bezpieczeństwa (m.in. kluczowe wskaźniki efektowności KPI oraz kluczowe wskaźniki ryzyka KRI) i w razie potrzeby ich dostrojenie.
22. System musi umożliwiać generowanie raportów (bezpośrednio z systemu lub pośrednio przez eksport danych do formularza raportów) z obsługi incydentu w języku polskim. W przypadku eksportu danych do formularza raportu, wykonawca opracuje i wdroży tę funkcjonalność.
23. Wymagane jest zapewnienie możliwości zweryfikowania predefiniowanej zawartości konsoli Dashboard i w razie potrzeby dostosowanie zakresu i sposobu prezentacji danych do potrzeb użytkownika.
24. Wymagane jest zapewnienie możliwości zweryfikowania predefiniowanych reguł priorytetyzacji incydentów bezpieczeństwa i w razie potrzeby ich dostrojenie.
25. Wymagane jest zapewnienie możliwości zweryfikowania wymagań SLA dla obsługi incydentów i podatności oraz zasad powiadomienia.
26. System musi zapewnić możliwość tworzenia własnych wymagań bezpieczeństwa oraz ich weryfikacji względem zasobów IT w tym (serwerów, stacji roboczych oraz urządzeń sieciowych) na bazie skryptów PowerShell/SSH oraz parametrów elektronicznej dokumentacji.
27. System musi pozwalać na automatyczne zbudowanie raportu zgodności na podstawie wyników skryptów weryfikujących stan faktyczny zasobów informatycznych oraz innych parametrów elektronicznej dokumentacji.
28. System musi umożliwiać rozbudowę raportu wymagań bezpieczeństwa poprzez dodanie nowych typów informacji i uwzględnienie ich w algorytmach oceny.
29. Zaoferowany System nie może posiadać ograniczeń w postaci ilości urządzeń , z których pobierane są logi jak również ilości zdarzeń na sekundę (EPS)

Przez źródło danych należy rozumieć zasób IT / zasób sieciowy, który zostanie zdefiniowany w systemie oraz będzie objęty jego logiką działania. Przykładowym źródłem danych może być serwer fizyczny, serwer w postaci maszyny wirtualnej, stacja robocza, urządzenie mobilne, switch , router, urządzenia bezpieczeństwa takie jak firewall, IPS, system ochrony anti-malware, strefa sieci obejmująca stacje robocze i inne.

1. System ma gwarantować możliwość elastycznej rozbudowy o dalsze zasoby, które w przyszłości zostaną objęte jego działaniem.
2. System musi zapewniać wydajność parsowania logów, których wielkość dochodzi do 100 GB dziennie.
3. Rozwiązanie musi być zaoferowane w konfiguracji wysokiej dostępności eliminującej wystąpienie Single Point of Failure.
4. Zaoferowany System nie może blokować / odrzucać logów / danych w przypadku przekroczenia dziennego limitu danych (w odniesieniu do wykorzystywanych w danym momencie licencji).
5. W przypadku problemów wydajnościowych któregokolwiek komponentu zaoferowanego Systemu musi istnieć możliwość jego rozbudowy (przynajmniej zwielokrotnienia ilości węzłów) bez konieczności zakupu dodatkowych modułów czy licencji.
6. System powinien umożliwiać co najmniej półroczne przechowywanie gromadzonych logów oraz ich wydajną analizę dla co najmniej 20 TB .
7. Rozwiązanie powinno wspierać mechanizm przenoszenia danych na pamięci masowe niższego poziomu na podstawie czasu lub okresu.
8. System musi umożliwiać integrację danych gromadzonych z różnych źródeł. Dane powinny być dostępna jako spójna informacja na poziomie interfejsu analitycznego systemu.
9. System musi zapewnić kontrolę dostępu na poziomie Role Based Access Control w granulacji określonej na poziomie wartości poszczególnych, identyfikowanych danych.
10. Zaoferowany System powinien pozwalać na podłączenie dodatkowej przestrzeni dyskowej CIFS/NFS w celu przechowywania danych archiwalnych. Dane archiwalne powinny być dostępne w systemie w ten sam sposób jak dane dostępne on-line.
11. Mechanizm przechowywania logów / danych / zdarzeń wdrożonego rozwiązania musi uniemożliwiać nieupoważnione usunięcie całości lub części logów, danych, raportów i innych informacji oraz zapewniać dostęp do nich tylko dla uprawnionych, uwierzytelnionych użytkowników.
12. System musi umożliwiać parsowanie logów o długości co najmniej 10 000 znaków oraz zawierających więcej niż jedną linię.
13. System musi umożliwiać tworzenie bazy definicji formatów logów.

II. WDROŻENIE SYSTEMU

1. Wykonawca w terminie do **30 dni kalendarzowych od daty podpisania umowy,** będzie odpowiedzialny za dostarczenie, instalację i konfigurację oraz optymalizację środowiska Systemu w infrastrukturze Zamawiającego.
2. Wykonawca przedstawi Zamawiającemu w terminie do 14 dni kalendarzowych po podpisaniu umowy projekt techniczny zawierający w szczególności:
3. Plan i opis architektury logicznej Systemu
4. Opis funkcji Systemu SOAR/SIEM do zaimplementowania w infrastrukturze Zamawiającego. Szczegółowy opis zakresu integracji Systemu SIEM z innymi systemami eksploatowanymi w infrastrukturze Zamawiającego.
5. Opis zakresu prac, ich sekwencji oraz wskazania, kto ma je realizować (Zamawiający, Wykonawca) niezbędnych do dostosowania Systemu do potrzeb Zamawiającego   
   i konfiguracji środowiska produkcyjnego.
6. Szczegółowy opis koniecznych zmian w konfiguracji urządzeń sieciowych i serwerów Zamawiającego.
7. Wykonawca przeprowadzi instruktaż stanowiskowy dla Administratorów (zarządzających systemem), co najmniej w n/w zakresie:
8. przedstawienie architektury Systemu
9. omówienie procedur obsługi administracyjnej Systemu
10. omówienie możliwości funkcjonalnych, zakresu dostępnych funkcji oraz ograniczeń Systemu
11. przekazanie informacji na temat konfiguracji i zarządzania Systemem
12. instruktaż stanowiskowy musi obejmować część teoretyczną i praktyczną
13. Zasady realizacji instruktażu stanowiskowego:
14. dla maksimum 8 osób wskazanych przez Zamawiającego
15. wymiar instruktażu stanowiskowego: 3 dni robocze Zamawiającego.
16. instruktaż stanowiskowy będzie prowadzony w siedzibie Zamawiającego lub innym miejscu wskazanym przez Wykonawcę i zaakceptowanym przez Zamawiającego
17. instruktaż stanowiskowy będzie realizowany minimum w oparciu o zakres wykonywanych prac wdrożeniowych Systemu,
18. instruktaż stanowiskowy powinien zostać przeprowadzony w dniach roboczych Zamawiającego, tj. pn – pt, w godzinach 8:15 – 16:15
19. Instruktaż stanowiskowy musi zakończyć się nie później niż do **28 dni kalendarzowych, liczonych od daty odbioru wdrożonego Systemu**. Osoby prowadzące instruktaż stanowiskowy muszą posiadać wiedzę oraz odpowiednie przygotowanie merytoryczne w zakresie wdrażanego Systemu, a także brać bezpośredni udział we wdrożeniu tego Systemu.
20. W ramach realizacji instruktażu stanowiskowego Wykonawca zapewni każdemu uczestnikowi materiały dydaktyczne w języku polskim (w formie elektronicznej), co najmniej:
21. podręcznik administratora i użytkownika w formie elektronicznej,
22. szczegółowy plan zajęć,
23. opis możliwych do zastosowania rozwiązań: przypadków omawianych w czasie prowadzenia instruktażu oraz najczęściej występujących przypadków przy eksploatacji systemu.

III. DOKUMENTACJA POWYKONAWCZA

1. Wykonawca opracuje i dostarczy Zamawiającemu w terminie do **28 dni kalendarzowych, liczonych od daty odbioru wdrożonego Systemu**, w formie elektronicznej i papierowej dokument „Dokumentacja powykonawcza".
2. Dokumentacja powykonawcza powinna zawierać następujące elementy:
3. Ogólny opis Systemu SOAR/SIEM
4. Wykaz całościowy oprogramowania oraz licencji wykorzystywanych w ramach wdrożonego Systemu SOAR/SIEM
5. Architektura logiczna systemu (graficzna prezentacja systemu i jego połączeń wraz z opisem)
6. Przepływ danych w systemie (koncepcja obiegu informacji w systemie pomiędzy poszczególnymi komponentami, warstwami systemu)
7. Szczegółowa konfiguracja poszczególnych elementów systemu (np. serwery zarządzające, serwery baz danych, systemy operacyjne, serwery aplikacyjne, serwery www - zrzuty ekranów, pliki konfiguracyjne, opisy konfiguracji, opisy uruchomionych usług, opisy poszczególnych funkcji systemu)
8. Politykę aktualizacji systemu i testowania zmian
9. Systemy zależne (np. agenci na innych serwerach, dodatkowe oprogramowanie na innych stacjach roboczych i serwerach współpracujące z systemem, opis integracji z innymi usługami w tym w szczególności z MS Active Directory oraz MS Exchange)
10. Specyfikację i konfiguracja serwerów wirtualnych
11. Architektura sieciowa systemu (opis połączeń sieciowych pomiędzy poszczególnymi elementami, adresacja IP, umiejscowienie elementów systemu w poszczególnych strefach - DMZ, LAN, Internet)
12. Opis portów komunikacyjnych (opis powinien zawierać informacje o otwartych portach oraz sposób zabezpieczenia zbędnych/nieużywanych portów)
13. Rodzaje kont systemowych i ich uprawnienia (określenie standardowych profili uprawnień, sposobu zarządzania użytkownikami oraz uprawnieniami w systemie)
14. Zarządzanie hasłami (opis sposobu przechowywania haseł w systemie, mechanizmów kryptograficznych wykorzystywanych do ich zabezpieczenia, informacje o przechowywaniu haseł w kodzie programu)
15. Uprawnienia kont serwisowych
16. Role administracyjne
17. Ustawienia polityki haseł
18. Procedury zmiany haseł serwisowych, administracyjnych i użytkownika
19. Procedury weryfikacji uprawnień
20. Konfiguracja reguł firewall
21. Bezpieczeństwo transmisji (opis rozwiązań w zakresie zapewnienia poufności transmisji danych zarówno w sieci LAN/DMZ jak i Internet)
22. Ochrona konfiguracji systemu (ochrona krytycznych plików konfiguracyjnych)
23. Opis rozwiązań w zakresie logowania zdarzeń (wskazanie rodzajów oraz lokalizacji dzienników w systemie, opis logowanych zdarzeń, w przypadku niestandardowych logów opis ich struktury)
24. Ochrona dzienników (opis sposobu zabezpieczenia zapisów w logach przed ich utratą oraz nieuprawnioną zmianą, informacja o czasie przechowywania logów, możliwości przekazania logów do systemów zewnętrznych)
25. Procedura odtwarzania systemu (opisanie procedury backupu i odtworzenia całego systemu i jego poszczególnych elementów, określenie czasu potrzebnego na odtworzenie całego systemu oraz jego poszczególnych elementów, opis procedur przywracania systemu do pełnej funkcjonalności po awarii)
26. Procedura instalacji systemu (opis procedury instalacji systemu „od początku - krok po kroku", opis wszystkich kroków instalacji i konfiguracji systemu w postaci zrzutów ekranu z opisami),
27. Procedury wykonywania krytycznych operacji w systemie (migracja, aktualizacja, itp.)
28. Instrukcje obsługi systemu dla Administratorów.

VI. INNE WARUNKI REALIZACJI ZAMÓWIENIA I GWARANCJA

1. System ma być dostarczony z licencją na wskazany pozniżej adres mailowy ………………………..i z wsparciem technicznym obejmującym okres 36 miesięcy od daty podpisania protokołu odbioru wdrożenia Systemu. Wsparcie techniczne obejmuje pomoc przy instalacji systemu oraz przy jego późniejszej eksploatacji. Tj. W ramach wsparcia technicznego Zamawiający ma otrzymać:
   1. bezpłatny dostęp do aktualizacji, poprawek i nowych wersji/kompilacji programu,
   2. wsparcie online 24x7,
   3. wsparcie telefoniczne w godzinach pracy suportu,
   4. dostęp do bazy wiedzy oraz dokumentacji Systemu,
2. Wykonawca udziela gwarancji na wykonane przez Wykonawcę w ramach umowy prace, do dnia upływu terminu umowy. W ramach usług gwarancyjnych Wykonawca ma zagwarantować następujące czasy naprawy Systemu licząc od momentu zgłoszenia przez Zamawiającego:
   1. 12 godzin w przypadku Awarii Systemu SOAR/SIEM (jako Awarię Zamawiający definiuje niedostępność systemu lub awarię Systemu, która uniemożliwia jego wykorzystanie)
   2. 48 godzin w przypadku Błędu w Systemie SOAR/SIEM (jako Błąd w systemie Zamawiający definiuje nieprawidłowe działanie systemu lub jego komponentów, które uniemożliwia lub ogranicza prawidłowe działanie Systemu)
3. Problemy z funkcjonowaniem Systemu SOAR/SIEM w ramach gwarancji zgłaszane będą drogą telefoniczną lub mailową lub za pomocą systemu udostępnionego przez Wykonawcę. Wykonawca określi drogę dokonywania zgłoszeń serwisowych oraz przygotuje niezbędne dostępy pozwalające na dokonanie zgłoszenia przez pracowników Zamawiającego. Wykonawca będzie prowadził całą historię złożonych zleceń oraz zapewni Zamawiającemu wgląd do systemu zawierający opis wszystkich zgłoszeń w całym okresie realizacji umowy. Wykonawca zapewni Zamawiającemu możliwość dokonywania zgłoszeń w trybie 24/7. Każde zgłoszenie złożone przez Zamawiającego powinno zawierać:
   1. datę i godzinę zgłoszenia
   2. opis Awarii lub Błędu
   3. sposób naprawy oraz czas realizacji zlecenia.
4. W okresie gwarancji Wykonawca zobowiązany jest do nanoszenia zmian w Dokumentacji powykonawczej związanych z realizacją zadań określonych w pkt. 5. w terminie nie dłuższym niż 10 dni roboczych od dnia dokonania przez Wykonawcę zmian w Systemie. Poprawiona Dokumentacja powinna być dostarczona Zamawiającemu w formie elektronicznej.
5. Wykonawca w ramach asysty zagwarantuje usługi konfiguracji, modernizacji oraz optymalizacji środowiska w liczbie do 500 roboczogodzin. W szczególności usługa w tym zakresie obejmuje :
   1. konsultacje w zakresie źródeł danych i procesów związanych z wykrywaniem i reakcją na incydenty
   2. konsultacje w zakresie wdrożenia systemu zarządzania bezpieczeństwem w oparciu o wdrożony System
   3. konsultacje w zakresie listy zakresu informacji i danych wymaganych do rozbudowy systemu
   4. instalacja i konfiguracja dodatkowych kolektorów
   5. aktualizacje topologii mapy logicznej (np. wykorzystanie narzędzi: Nmap, WMI, analiza ruchu/logów)
   6. aktualizacje zasobów informacyjno-usługowych
   7. uzupełnienie parametrów zasobów informacyjno-usługowych (mechanizmy zabezpieczeń, rodzaje zasobów)
   8. zmiany w schemacie komunikacji międzystrefowej w ramach kluczowych usług IT (bazy danych, serwery WEB, serwery aplikacyjne, serwery plików, DNS)
   9. dostrojenie reguł domyślnych oceny ryzyka zaimplementowanych w systemie do organizacji zamawiającego
   10. dostrojenie reguł zaawansowanych oceny ryzyka zaimplementowanych w systemie do organizacji zamawiającego na podstawie danych przekazanych przez Zamawiającego.
   11. dostrojenie reguł korelacyjnych zaimplementowanych w systemie do organizacji zamawiającego
   12. przygotowanie nowych reguł korelacyjnych
   13. przygotowanie nowych scenariuszy obsługi
   14. przygotowanie nowych skryptów PowerShell/SSH
6. Zadania realizowane będą każdorazowo na zlecenie Zamawiającego i sumowane na podstawie zrealizowanych godzin (strony wspólnie ustalą każdorazowo ilość godzin koniecznych do zrealizowania zleconego zadania). W ramach zleconego zadania Wykonawca dokona aktualizacji dokumentacji technicznej Systemu, która nie będzie wliczana do ilości godzin poświęconych na zrealizowanie zleconego zadania.