Opis przedmiotu Zamówienia

Przedmiotem zamówienia jest zakup systemu bezpieczeństwa systemów teleinformatycznych, w skład którego wchodzi:

- Firewall (UTM),

- System ochrony poczty mailowej (bramka antyspam),

- System zarządzania kontami uprzywilejowanymi (PAM),

- system automatyzacji procesów IT (SOAR).

Szczegółowe dane dot. urządzeń opisane są poniżej.

1. Wymagania Ogólne dot. Firewall

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
   - 16 portami Gigabit Ethernet RJ-45.
   - 8 gniazdami SFP 1 Gbps.
   - 4 gniazdami SFP+ 10 Gbps.
   - 4 gniazdami SFP28 25 Gbps.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System jest wyposażony w zasilanie 2xAC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 8 mln. jednoczesnych połączeń oraz 550 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 137 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 32 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 256 nie mniej niż 55 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 14 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 10 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 9 Gbps.

Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.

13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS).
   - Microsoft Azure.
   - Cisco ACI.
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware NSX.
   - Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19, 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
   - Tworzenie nielimitowanych licencją połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
   - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.

- Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
- Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
- Mechanizm „Split tunneling" dla połączeń Client-to-Site.

2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
   - realizację połączeń IPSec VPN lub SSL VPN przy użyciu oprogramowania klienckiego nie wymagającego zakupu dodatkowych licencji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.

3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.

2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Certyfikaty

Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje:

- EAL4 dla funkcji Firewall.

Testy wydajnościowe oraz funkcjonalne

Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.

Gwarancja oraz wsparcie

Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

2. Wymagania ogólne dot. systemu ochrony poczty elektronicznej

System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników.

Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym, na którym będzie instalowane rozwiązanie. Platformy muszą mieć możliwość uruchomienia na co najmniej następujących hypervisorach: VMWare ESX/ESXi, Citrix XenServer, Microsoft Hyper-V Server, KVM qemu, AWS (Amazon Web Services), Nutanix AHV, Microsoft Azure, Google Cloud Platform, Oracle Cloud Infrastructure.

Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń.

Dostarczone rozwiązanie musi mieć możliwość pracy w każdym z trybów:

1. Tryb Gateway.
2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).

Parametry fizyczne systemu antyspamowego

1. System musi obsługiwać co najmniej 6 interfejsów sieciowych oraz wspierać powierzchnię dyskową o pojemności co najmniej 4 TB.

Ogólne funkcje systemu ochrony poczty

Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:

1. Wsparcie dla co najmniej 500 domen pocztowych.
2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 220 tys. wiadomości/godzinę.
3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).

6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie.
7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
11. Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.
12. Ochrona linków URL poprzez ponowne skanowanie w momencie uzyskiwania dostępu do zawartości.
13. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail.
14. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
15. Możliwość przechowywania poczty realizowana lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
16. Możliwość przechowywania kopii zapasowej poczty realizowana na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
17. Listy blokowanych i bezpiecznych adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
18. Listy blokowanych i bezpiecznych adresów mailowych dla poszczególnych użytkowników.
19. Ochrona przed wyciekiem informacji poufnej DLP (Data Loss Prevention).
20. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.

Kontrola antywirusowa i ochrona przed malware

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Skanowanie antywirusowe wiadomości SMTP.
2. Kwarantannę dla zainfekowanych plików.
3. Skanowanie załączników skompresowanych.
4. Definiowanie komunikatów powiadomień w języku polskim.
5. Blokowanie załączników w oparciu o typ pliku.
6. Możliwość zdefiniowania nie mniej niż 400 profili kontroli antywirusowej.
7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.
8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.

9. Ochronę typu wirus outbrake.
10. Ochronę przed zagrożeniami zawartymi wiadomościach pocztowych i w załącznikach (nie mniej niż: pliki MS Office, PDF, HTML, tekstowe) poprzez usuwanie treści będących zagrożeniem (makra, adresy URL zagnieżdżone w plikach, skrypty, ActiveX) i dostarczaniem oczyszczonych w ten sposób wiadomości.

Kontrola antyspamowa

System musi zapewniać poniższe funkcje i metody filtrowania spamu:

1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
3. Szczegółowa kontrola nagłówka wiadomości.
4. Analiza Heurystyczna.
5. Współpraca z zewnętrznymi serwerami RBL, SURBL.
6. Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.
7. Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników.
8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
9. Kontrola w oparciu o Greylisting oraz SPF.
10. Filtrowanie treści wiadomości i załączników.
11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
12. Możliwość zdefiniowania nie mniej niż 400 profili kontroli antyspamowej.
13. Ochrona typu outbrake.
14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malicious websites, hacking).
15. Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata.
16. Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level).
17. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.

Ochrona przed atakami na usługę poczty

System musi zapewniać poniższe funkcje i metody filtrowania:

1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing).
2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
5. Weryfikacja poprawności adresu e-mail nadawcy.

Funkcje logowania i raportowania

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Logowanie do zewnętrznego serwera SYSLOG.
2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.
4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.
5. Możliwość analizy przebiegu sesji SMTP.
6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.

Funkcje pracy w trybie wysokiej dostępności (HA)

System ochrony poczty musi zapewniać poniższe funkcje:

1. Konfigurację HA w każdym z trybów: gateway, transparent.
2. Tryb synchronizacji konfiguracji dla scenariuszy, gdy każde z urządzeń występuje pod innym adresem IP.
3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
4. Monitorowanie stanu pracy klastra.

Aktualizacje sygnatur, dostęp do bazy spamu

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.
2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.

Zarządzanie

System ochrony poczty musi zapewniać poniższe funkcje:

1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
3. Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.

Certyfikaty

Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji:

1. VBSpam, VB100 rated, Common Criteria, FIPS 140-2 Certified.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

1. Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake, Sandbox w chmurze, ochrona typu Click Protect, Content Disarm & Reconstruction, Business Email Compromise na okres 36 miesięcy.

Gwarancja oraz wsparcie

System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy. W ramach tego serwisu producent musi zapewniać dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

2. Wymagania ogólne dot. systemu zarządzania kontami uprzywilejowanymi

Dostępne narzędzia typu PAM (ang: Privileged Access Management) to rozwiązanie zapewniające zarządzanie uprzywilejowanym dostępem do zasobów sieciowych. Wymagania funkcjonalne dla tego typu rozwiązania dla poprawy rozliczalności i bezpieczeństwa budowanej infrastruktury muszą obejmować przede wszystkim:

1. **Zarządzanie kontami uprzywilejowanymi**: centralne zarządzanie kontami uprzywilejowanymi, takimi jak konta administratorów, konta z dostępem root czy konta serwisowe. Powinno być możliwe tworzenie, usuwanie i modyfikowanie kont, zarządzanie hasłami, a także kontrola dostępu i uprawnień.
2. **Bezpieczne przechowywanie danych uwierzytelniających**: System powinien zapewniać bezpieczne przechowywanie danych uwierzytelniających, takich jak hasła, certyfikaty czy klucze prywatne. Dane te powinny być zaszyfrowane i chronione przed nieuprawnionym dostępem.
3. **Kontrola dostępu**: musi być możliwa kontrola dostępu do zasobów sieciowych na podstawie zasad i polityk. Powinno być możliwe definiowanie reguł i ograniczeń dostępu dla poszczególnych kont uprzywilejowanych, a także monitorowanie i rejestrowanie działań użytkowników.
4. **Audyt i monitorowanie aktywności**: System musi umożliwiać audyt i monitorowanie aktywności użytkowników posiadających uprzywilejowany dostęp. Powinno być możliwe rejestrowanie i analiza logów związanych z operacjami wykonywanymi przez konta uprzywilejowane, w celu identyfikacji potencjalnych zagrożeń i śledzenia działań.
5. **Uwierzytelnianie wieloskładnikowe**: narzędzie powinno wspierać uwierzytelnianie wieloskładnikowe (MFA), takie jak tokeny OTP, certyfikaty czy biometria. Wprowadzenie MFA zwiększa bezpieczeństwo procesu uwierzytelniania i utrudnia atakującym przejęcie kont uprzywilejowanych.
6. **Zarządzanie sesjami uprzywilejowanymi**: System powinien umożliwiać zarządzanie sesjami uprzywilejowanymi, takie jak monitorowanie i kontrola aktywnych sesji, automatyczne wylogowywanie nieaktywnych sesji czy możliwość zdalnego przerwania sesji w przypadku podejrzenia nadużyć.
7. **Integracja z innymi narzędziami i rozwiązaniami**: PAM powinien umożliwiać integrację z innymi narzędziami i rozwiązaniami, takimi jak systemy zarządzania tożsamościami (IAM), narzędzia do zarządzania incydentami czy SIEM (Security Information and Event Management). Integracja ta pozwala na lepszą koordynację działań i wykorzystanie przygotowywanej infrastruktury bezpieczeństwa.

Dostęp uprzywilejowany to dostęp do konta z uprawnieniami wykraczającymi poza uprawnienia kont nieuprzywilejowanych, zwykle ograniczony do menedżerów IT i administratorów systemu. Przykłady dostępu uprzywilejowanego obejmują lokalne konta administracyjne, konta administracyjne domeny, konta usługi Active Directory lub domenowej oraz konta aplikacji. Prawie 100 procent szkodliwych ataków opiera się na wykorzystaniu uprzywilejowanych danych uwierzytelniających.

System kategorii *Privileged Access Management* (PAM) chroni uprzywilejowane konta przed kradzieżą poświadczeń i nadużywaniem uprawnień, zarządzając danymi uwierzytelniającymi, kontrolując dostęp uprzywilejowanych użytkowników i monitorując uprzywilejowaną aktywność

Wymagania funkcjonalne dla systemu PAM

1. Zapewnienie wysokiego poziomu bezpieczeństwa danych i poufności informacji
2. Wsparcie dla szyfrowania danych w transmisji i przechowywaniu haseł i kluczy
3. Elastyczność w zakresie skalowania infrastruktury w celu obsługi zwiększonego obciążenia
4. System musi posiadać Mechanizmy failover i redundancji, aby zapewnić ciągłość działania w przypadku awarii serwera lub innego komponentu
5. System PAM musi posiadać przyjazny interfejs graficzny (GUI) umożliwiający łatwe zarządzanie kontami uprzywilejowanymi i monitorowanie działań użytkowników.
6. Integracja z technologią ZTNA (Zero Trust Network Access) oraz możliwość działania jako punkt wymuszania dla ZTNA
7. Musi istnieć możliwość sprawdzania silnikiem antywirusowym przesyłanych podczas sesji plików. Kontrola musi być realizowana co najmniej dla transferu plików poprzez web (Web SFTP, Web SAMBA) oraz SCP.
8. Automatyczne blokowanie niebezpiecznych poleceń za pomocą profilu filtrowania SSH. System musi monitorować komendy wydawane przez operatora sesji.
9. Rozwiązanie musi być dostępne w formie zarówno urządzeń wirtualnych (*virtual appliance*), jak i sprzętowych. Dla wirtualizacji musi być wspierany co najmniej hypervisor VMWare oraz KVM.
10. Działanie PAM musi pozwalać na obsługę połączeń bezpośrednich jak i proxy.
11. Możliwość obsługi niestandardowych protokołów chociażby poprzez dedykowane wyzwalacze (*custom application launcher*)
12. Możliwość ostrzegania użytkowników o nagrywaniu w celu zapewnienia zgodności z wymaganiami RODO.
13. System PAM w wersji wirtualnej musi obsługiwać moduł vTPM (*Virtual Trusted Platform Module*) dla przechowywania kluczy prywatnych użytkowników.
14. PAM musi obsługiwać mechanizm awaryjnego dostępu do zaszyfrowanych haseł przechowywanych w systemie na zasadzie procedury „glass breaking". Wszystkie działania w tym trybie muszą być logowane celem możliwości przeprowadzenia audytu.
15. System musi automatycznie nagrywać obraz podczas uruchomienia procedury awaryjnej (glass breaking)
16. Automatyczna zmiana hasła konta po poprawnym zalogowaniu
17. Wsparcie dla zaplanowanej zmiany haseł według harmonogramu
18. Możliwość tworzenia procedury żądania dostępu do haseł i zatwierdzania takich żądań poprzez konfigurowalną ilość administratorów
19. Ustawienie dedykowanego dostępu do skonfigurowanego hasła dla jednego administratora. W tym stanie dostęp jest ograniczony tylko dla jednego użytkownika uprzywilejowanego.
20. Wymagane jest wsparcie dla algorytmów szyfrowania SSH o wysokiej sile
21. Zaawansowany protokół uwierzytelniania RDP, w tym CredSSP i TLS
22. Kontrola dostępu oparta na rolach (RBAC)
23. Kontrola uprawnień oparta na użytkownikach oraz grupach użytkowników
24. Kontrola profili dostępowych w formie polityk

25. Wsparcie dla Disaster Recovery
26. Użytkownik uprzywilejowany musi mieć możliwość pracy co najmniej w następujących trybach:
    a. Agentowy – dostępne wszystkie funkcjonalności. Agent musi być dostępny bezpłatnie
    b. Bezagentowo, za pomocą przeglądarki internetowej wraz z dedykowanym rozszerzeniem. Metoda ta musi umożliwiać uzupełnianie haseł przez PAM oraz nagrywanie sesji
    c. Bezagentowo, za pomocą przeglądarki internetowej bez dodatkowych rozszerzeń

Uwierzytelnianie

1. Obsługa uwierzytelniania użytkowników za pomocą certyfikatów
2. Możliwość korzystania z lokalnej bazy danych użytkowników
3. Obsługa uwierzytelniania wieloskładnikowego opartego na SAML
4. Obsługa OIDC (openID Connect), SAML
5. Obsługa wielu połączeń SAML SP
6. Możliwość integracji z istniejącymi usługami uwierzytelniania, w nie mniejszym zakresie niż Active Directory, LDAP, radius.
7. Wsparcie dla integracji z istniejącymi systemami zarządzania tożsamościami
8. Możliwość obsługi większej liczby kont uprzywilejowanych w miarę rozwoju organizacji
9. Dostęp do zasobów użytkowników uprzywilejowanych musi również obejmować możliwości blokady w oparciu o dodatkowe parametry:
    a. Kontrola dostępu oparta na adresie źródłowym IP użytkownika
    b. Ograniczanie dostępu oparte na harmonogramie użytkownika
    c. Kontrola dostępu do docelowego serwera oparta o przypisane tagi ZTNA (stan stacji, z której następuje połączenie jest badany przez mechanizmy ZTNA)

Licencjonowanie

1. Oprogramowanie musi być objęte kompletną licencją producenta na całe rozwiązanie. Nie dopuszcza się dodatkowych wymagań licencyjnych dla systemu operacyjnego, bazy danych, oprogramowania serwera WWW lub podobnych.
2. Nie dopuszcza się licencjonowania ilości zasobów, do których realizowany jest nadzorowany dostęp.
3. Nie dopuszcza się licencjonowania ilości zajętego miejsca na dysku przez nagrania sesji.
4. Licencja systemu musi pozwalać na podłączenie się co najmniej 25 użytkowników do monitorowanych zasobów.

Monitorowanie i raportowanie

1. Możliwość monitorowania aktywności użytkowników z kontami uprzywilejowanymi.
2. Generowanie szczegółowych raportów audytowych w celu analizy i śledzenia działań użytkowników

Wsparcie techniczne i aktualizacje

1. Gwarancja wsparcia technicznego i dostępności aktualizacji oprogramowania w celu utrzymania systemu w aktualnym i bezpiecznym stanie musi być zapewniona na okres 36 miesięcy .

2. Dostawca rozwiązania musi zapewnić pojedynczy punkt kontaktu z pomocą techniczną dla wszystkich zainstalowanych komponentów w urządzeniu wirtualnym lub sprzętowym.

4. Wymagania ogólne dot. systemu SOAR

Celem niniejszego Zapytania jest przedstawienie wymagań i potrzeb Zamawiającego w zakresie dostarczenia, wdrożenia, integracji i uruchomienia Systemu Security Orchestration Automation And Response (dalej SOAR) w środowisku teleinformatycznym Zamawiającego.

Wymagania techniczne i funkcjonalne opatrzone są wyrażeniami, które mają następujące znaczenie i interpretację:

MUSI, MUSZĄ - oznacza, że wymaganie jest bezwzględnie wymagalne w ramach standardowych właściwości Systemu.

POWINIEN, POWINNY - oznacza, że jest dopuszczalne odstąpienie od danego wymagania przez Zamawiającego. Warunkiem koniecznym do odstąpienia od wymagania jest przedstawienie przez Wykonawcę uzasadnienia i akceptowalnej rekomendacji alternatywnego rozwiązania.

NIE MOŻE, NIE MOGĄ - oznacza, że dana właściwość jest niedopuszczalna.

NIE POWINIEN, NIE POWINNY - oznacza, że jest możliwe dopuszczenie danej właściwości do listy wymagań. Zamawiający może dopuścić daną właściwość do listy wymagań na podstawie przedstawionego przez Wykonawcę uzasadnienia i akceptowalnej rekomendacji.

Słownik pojęć i skrótów

Pojęcie/skrót	Wyjaśnienie
API	Application Programming Interface. Interfejs programistyczny do udostępniania funkcjonalności systemu.
BPMN	Business Process Model and Notation. Format tworzenia schematów postępowania (flowcharts) ze szczególnym uwzględnieniem zastosowania w aspekcie cyberbezpieczeństwa.
CSIRT	Computer Security Incident Response Team. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym wg. Ustawy o Krajowym Systemie Cyberbezpieczeństwa.
CTI	CyberThreatIntelligence. Gromadzenie, analiza i wymiana informacji o cyberzagrożeniach.
Connector action, action	Zdefiniowane wcześniej w ramach konektora akcje, które pozwalają na wykonywanie podstawowych czynności integracyjnych. Przykładem akcji może być: aktualizacja konta użytkownika, sprawdzenie dostępnych informacji o adresie IP, etc.
Konektor	Rozszerzenie systemu SOAR w postaci spójnej biblioteki wraz z akcjami i dokumentacją. Celem konektora jest umożliwienie współdziałania z zewnętrznymi systemami dla uzyskania dodatkowych informacji lub wykonania zmian w zewnętrznym systemie.

GUI	Graficzny interfejs użytkownika, GUI. Sposób komunikowania się człowieka z oprogramowaniem komputera, wykorzystujący obiekty wyświetlane na monitorze w trybie graficznym; do wprowadzania danych korzysta się z klawiatury i myszy.
HTTP	Hypertext Transfer Protocol. Protokół przesyłania danych hipertekstowych.
IoC	Indicator of compromise. Wskaźnik naruszenia bezpieczeństwa, określa cechy charakterystyczne i artefakty związane z incydentem bezpieczeństwa.
Incydent, Incydent bezpieczeństwa, Incydent cyberbezpieczeństwa	Zdarzenie związane z naruszeniem bezpieczeństwa.
Multitenant	Model pracy aplikacji lub systemy w trybie współdzielenia zasobów pomiędzy wielu klientów lub organizacji (tenantów). System pracujący w tym trybie kontroluje prawa każdej organizacji i zapewnia logiczną separację.
VMware	Oprogramowanie do wirtualizacji infrastruktury teleinformatycznej.
Oprogramowanie	Oprogramowanie Systemu SOAR.
Playbook	Procedura programowana w systemie SOAR składająca się z sekwencji działań podejmowanych przez oprogramowanie zgodnie z założonym przepływem.
RBAC	Role-basedaccesscontrol (RBAC), kontrola dostępu oparta na rolach – mechanizm kontroli dostępu w systemach komputerowych.
SDK	SDK to zbiór oprogramowania używanego do programowania aplikacji dla określonego urządzenia lub systemu operacyjnego
SIEM	Security Information and Event Management. System do zarządzania informacją i zdarzeniami cyberbezpieczeństwa.
SOC	Security Operation Center. Zespół wykwalifikowanych specjalistów którego celem jest monitorowanie bezpieczeństwa teleinformatycznego, wykrywanie i reagowanie na Incydenty bezpieczeństwa przy wykorzystaniu zarówno środków technicznych i organizacyjnych.
SOAR, System SOAR, System	Security Orchestration, Automation and Response. System odpowiadający za zarządzanie w obszarze rozwiązywania Incydentów cyberbezpieczeństwa w zakresie reagowania, rozwiązywania oraz raportowania poprzez automatyzację zadań i integrację z innymi narzędziami bezpieczeństwa.
Workflow	Sposób przedstawienia i organizacji przepływu informacji pomiędzy rozmaitymi obiektami biorącymi udział w jej przetwarzaniu
STIX	StructuredThreat Information Expression. Format danych używany do wymiany informacji o cyberzagrożeniach.
Service Desk	System zarządzający zgłoszeniami serwisowymi.
TAXII	Trusted Automated Exchange of Intelligence Information. Protokół warstwy aplikacji służący do przekazywania informacji o cyberzagrożeniach w prosty i skalowalny sposób.
VM	Vulnerability Management. Zarządzanie wykrytymi podatnościami.

Wymagania

System musi zrealizować podstawowe cele stawiane przez Zamawiającego:

A. Udostępnienie jednego interfejsu i platformy pochodzących od tego samego producenta dla zarządzania, orkiestracji bezpieczeństwem informatycznym jak i automatyzacji działań i zadań
B. Zarządzanie incydentami bezpieczeństwa
C. Zautomatyzowanie powtarzalnych zadań w ramach zespołu SOC
D. Identyfikacja i rozróżnienie zagrożeń od fałszywych alarmów
E. Poprawa parametrów działania zespołu SOC
F. Ułatwienie zarządzania pracą zespołu SOC
G. Ustandaryzowanie procesów i procedur postępowania
H. Wprowadzenie parametrów oraz ich pomiaru, służących do raportowania wydajności i skuteczności obsługi zdarzeń bezpieczeństwa zarówno przez zespół jak i mechanizmy automatyzujące
I. Zdecydowaną redukcję powtarzalnych działań pracowników na rzecz automatycznych kroków i całych procesów

Szczegółowe wymagania zebrano w poniżej liście.

1. System MUSI mieć możliwość instalacji w infrastrukturze Zamawiającego bez żadnego elementu wykonawczego, analitycznego lub innego znajdującego się poza infrastrukturą Zamawiającego.
2. System MUSI mieć możliwość domyślnej instalacji w środowisku wirtualizacyjnym i MUSI wspierać co najmniej środowiska producentów VMWare oraz Red Hat KVM.
3. System POWINIEN być dostarczony jako kompletny obraz do instalacji, zarówno systemu operacyjnego jak i oprogramowania.
   MUSI być dostępna opcja instalacji SOAR na własnym systemie operacyjnym Zamawiającego, co najmniej Red Hat.
4. System SOAR MOŻE mieć możliwość licencjonowania w ramach modelu subskrypcyjnego, gdzie licencje będą opłacane na określony czas działania rozwiązania.
   System SOAR MOŻE posiadać opcję licencjonowania w ramach modelu stałej licencji, nieograniczonej czasowo oraz wsparcia technicznego producenta działającego w ustalonym czasie.
5. System MOŻE posiadać licencjonowanie oparte o ilość użytkowników jednocześnie korzystających z systemu – sprawdzanie powinno być realizowane w oparciu jednoczesne aktywne sesje zalogowanych użytkowników.
6. System MOŻE umożliwiać przypisywanie licencji na sesję dla kont imiennych, gdzie jedno konto zużywa jedną licencję oraz tworzenie kont wspólnych, które działają w ramach pozostałej puli dostępnych połączeń. Zmiana trybu licencji dla poszczególnych kont powinna być możliwa w dowolnym momencie.
7. System SOAR NIE MOŻE licencjonować lub ograniczać innych parametrów systemu, jak ilość wykonywanych akcji, liczba podłączonych konektorów, rozmiar dysku, itp.
8. System MUSI mieć możliwość wyboru wielu języków interfejsu graficznego GUI. Wymagana jest obsługa języka angielskiego. MOŻE istnieć możliwość zaimplementowania języka polskiego.
9. System SOAR MUSI mieć możliwość instalacji oraz aktualizacji w trybie offline, tzn. bez dostępu systemu do Internetu. Wymaganie dotyczy również pracy z konektorami.
10. Producent systemu MUSI dostarczać aktualizacje oprogramowanie SOAR.
11. Aktualizacja konektorów NIE MOŻE powodować restartu systemu.

12. Aktualizacja istniejących w systemie konektorów i obsługiwanych przez producenta MUSI być realizowana z poziomu GUI systemu, bez konieczności uruchamiania innego interfejsu. Aktualizacje MUSZĄ być widoczne w interfejsie systemu od momentu ich dostępności (dotyczy pracy w trybie online).
13. Rozwiązanie MUSI zawierać kreator wspomagający tworzenie niestandardowych integracji. Jednocześnie wszystkie istniejące integracje (konektory i ich akcje) muszą być edytowalne za pośrednictwem GUI, wraz z możliwością pracy nad kodem źródłowym, bez konieczności używania zewnętrznego IDE.
14. Konektory MUSZĄ posiadać funkcję automatycznej weryfikacji działania, tzn. muszą weryfikować poprawność ustawień i prawidłową współpracę z systemem integrowanym poprzez wykonywania aktywnych testów połączenia. Wynik weryfikacji MUSI być widoczny, a błędy muszą być logowane.
15. Wszystkie konektory MUSZĄ udostępniać swój kod źródłowy dla administratora Zamawiającego z poziomu systemu. MUSI też być możliwa swobodna modyfikacja kodu oraz wersjonowanie konektora. MUSI być możliwość dodawania własnych akcji w ramach danego pakietu.
16. Tam, gdzie to jest możliwe i zasadne konektory MUSZĄ wykorzystywać szyfrowane połączenia z systemem integrowanym, np. poprzez protokół SSL i weryfikację certyfikatu.
17. MUSI istnieć możliwość pisania własnych konektorów w języku python. Proces tworzenia nowego konektora MUSI być możliwy do realizacji w środowisku zewnętrznym jak i w ramach zainstalowanego systemu. SOAR MUSI posiadać możliwość importu konektorów z przygotowanego wcześniej archiwum.
18. System MUSI posiadać editor kodu wbudowany w swój interfejs. Minimalne funkcje edytora to: podpowiedzi uzupełnienia składni, interaktywna dokumentacja wyświetlana przy tworzonych wyrażeniach, kolorowanie składni, wskazywanie błędów, miniatura strony kodu z możliwością nawigacji.
19. Producent MUSI dostarczyć zestaw bibliotek SDK dla łatwego tworzenia własnych konektorów. Dokumentacja producenta musi wskazywać sposób integracji przynajmniej z jednym środowiskiem programistycznym.
20. Oferowany system MUSI posiadać publicznie dostępne repozytorium dla integracji, konektorów, pakietów rozszerzeń np. github. Repozytorium to MUSI być aktualizowane zarówno przez producenta jak i społeczność użytkowników.
21. Oferowany system MUSI posiadać publicznie dostępną dokumentację co najmniej w zakresie: instalacji i pierwszej konfiguracji, dokumentacji dla dostępnych w systemie konektorów, API, administracji systemem, ścieżki aktualizacji wersji, informacji o wydaniu (release notes), tworzenie konektorów oraz Playbook-ów.
22. Producent oferowanego systemu MUSI utrzymywać dedykowany (odrębny od wspomnianej dokumentacji) portal dla treści związanych z konfiguracją systemu obejmujący co najmniej: konektory, gotowe szablony konfiguracji, elementy interfejsu graficznego. Portal ten musi pozwalać na pobieranie wcześniej wymienionych, gotowych do importu modułów. Portal MUSI być dostępny publicznie i NIE MOŻE wymagać jakichkolwiek opłat za korzystanie z zawartości.
23. Zamawiający wymaga, aby dla oferowanego systemu dostarczona była również wersja testowa. Wersja testowa POWINNA posiadać taką samą funkcjonalność i wersję jak produkcyjna. MUSI być możliwe uruchomienie więcej niż jednej instancji testowej.
24. System SOAR MUSI umożliwiać importowanie części konfiguracji lub interfejsu z innego systemu, np. testowego.

25. Interfejs graficzny POWINIEN udostępniać szatę kolorystyczną GUI co najmniej w jasnych barwach i ciemnych (darkmode).
26. System SOAR MUSI posiadać elastyczną możliwość integracji z zewnętrznymi systemami, najlepiej w formie konektorów, za pomocą dostępnych protokołów, nie mniej niż: API, SSH, Syslog, TAXII, SMTP, SOAP, IMAP, bazy danych, pliki w formatach XML, HTML i JSON, SMB, LDAP, SSL. Dla każdego integrowanego producenta MUSZĄ być dostępne akcje charakterystyczne dla danego rozwiązania. MUSI być możliwość instalacji tylko niezbędnych do działania konektorów.
27. SOAR MUSI posiadać graficzny interfejs budowania i symulacji Playbook-ów.
28. Edytor Playbook-ów MUSI udostępniać co najmniej następujące typy elementów wykonawczych:
    1. Wykonanie zadania przez użytkownika technicznego SOAR (personel SOC/CSIRT)
    2. Wykonanie zadania przez użytkownika biznesowego
    3. Wykonanie automatycznego zadania w zintegrowanym z SOAR systemie bezpieczeństwa Zamawiającego
    4. Wykonanie automatycznego zadania w elemencie infrastruktury teleinformatycznej Zamawiającego
29. Projektowanie i wykonywanie Playbook-ów MUSI udostępniać możliwość złożonych ścieżek postępowania, w tym co najmniej:
    1. Ścieżek równoległych
    2. Ścieżek alternatywnych
    3. Ścieżek warunkowych
30. Playbook MUSI udostępniać możliwość budowania rozdzielnych ścieżek postępowania na każdym jego etapie w zależności od parametrów wejściowych dodanego elementu.
31. Wykonywanie Playbook-ów MUSI udostępniać możliwość:
    1. Rozwidlania na wiele ścieżek
    2. Zbieżności wielu ścieżek w jednym elemencie
32. SOAR MUSI udostępniać możliwość budowania nowych Playbook-ów na bazie już istniejących poprzez kopiowanie i edycję.
33. SOAR MUSI udostępniać możliwość wersjonowania Playbook-ów.
34. System SOAR MUSI posiadać możliwość importu do Playbook-ów workflow z narzędzia BPMN. MUSI być obsługiwany format pliku źródłowego XML i JSON.
35. SOAR MUSI udostępniać możliwość tworzenia Playbook-ów zagnieżdżonych tzn .korzystających z już istniejących, gdzie istniejący Playbook jest częścią utworzonego nowego playbook-a.
36. SOAR MUSI posiadać mechanizmy wyboru ścieżki/ścieżek w Playbook-ach na podstawie kontekstu danych/parametrów.
37. SOAR MUSI się integrować z zewnętrznymi systemami CTI (Cyber Threat Intelligence).
38. System MUSI posiadać warstwowy mechanizm przetwarzania obsługiwanych alarmów. Minimalny zakres to: stopień 1: przetwarzanie odebranych rekordów z zewnątrz zanim zostanie on zapisany w systemowych bazach danych (możliwe jest na przykład odrzucenie rekordu do dalszego przetwarzania); stopień 2: właściwe przetwarzanie procedur; stopień 3: działania po wykonaniu procedur (playbook), przez co możliwe jest na przykład zaawansowane łączenie podobnych rekordów z nowo utworzonym.
39. Producent SOAR MUSI dostarczać własną bazę CTI (Cyber Threat Intelligence) możliwą do uruchomienia i wykorzystania w systemie.

40. System MUSI posiadać interfejsy pozwalające na integrację z rozwiązaniami CyberThreatIntelligence (STIX, TAXII).
41. Integracja z CTI MUSI umożliwiać pobieranie przez System SOAR informacji o aktualnych danych związanych z zagrożeniami występujących w cyberprzestrzeni (listy reputacyjne adresów IP, adresów DNS, skróty (sumy kontrolne) złośliwego oprogramowania oraz złośliwych plików, itp.).
42. SOAR MUSI posiadać możliwość wprowadzania informacji o Incydentach różnymi interfejsami w tym co najmniej:
    1. Poprzez Operatora manualnie
    2. Poprzez integracje z systemem ServiceDesk (zdarzenie zakwalifikowane jako Incydent cyberbezpieczeństwa)
    3. Poprzez integracje z systemami bezpieczeństwa
    4. Przez SIEM co najmniej Energy Logserver posiadany przez Zamawiającego
    5. Porzez pocztę elektroniczną – dedykowane konto dla powiadomień
43. System SOAR MUSI posiadać możliwość definiowania w sposób ustrukturyzowany danych o Incydencie w postaci artefaktów. Co najmniej MUSZĄ być wspierane domyślnie następujące rodzaje:
    - pliki
    - skróty danych w postaci SHA1, SHA256, MD5
    - adresy IP
    - adresy URL
    - nazwy DNS
    - Hostname
    - Port
    - Rejestr
    - użytkownik
    - proces
    - adres email
44. System SOAR MUSI mieć możliwość dowolnego definiowania nowych typów artefaktów.
45. SOAR POWINIEN mieć możliwość tworzenia skryptów w co najmniej języku programowania PYTHON.
46. SOAR MUSI mieć domyślnie zdefiniowane co najmniej 5 stopni istotności Incydentów. Ilość stopni jak i ich nazwy POWINNY udostępniać możliwość definiowania.
47. SOAR MUSI mieć możliwość TAG-owania zdarzeń przekazywanych do SOAR, alertów, zadań i incydentów.
48. SOAR MUSI mieć możliwość definiowania SLA na poziomie:
    1. Alarmów
    2. Incydentów
49. SOAR MUSI mieć możliwość definiowania ról w zakresie rozwiązywania, zarządzania i raportowania incydentów bezpieczeństwa.
50. SOAR MUSI mieć możliwość definiowania co najmniej pięciu rodzajów ról ze względu na uprawnienia:
    1. Menadżer Incydentów
    2. Pracownik I linii SOC
    3. Pracownik II linii SOC
    4. Pracownik III linii SOC
    5. Użytkownik biznesowy

51. SOAR MUSI posiadać możliwość integracji z systemami SIEM w zakresie przekazywania informacji o Incydentach.
52. SOAR MUSI mieć możliwość załączania plików.
53. SOAR MUSI mieć możliwość zamieszczania komentarzy w zadaniach.
54. SOAR MUSI mieć możliwość cyklicznego uruchamiania Playbook-ów według ustalonego harmonogramu.
55. SOAR MUSI umożliwiać przechowywanie danych o Incydentach z pełną informacją o operacjach wykonanych w systemie w zadanym okresie czasu.
    a. MUSI zawierać moduł zarządzania kryzysowego w postaci tzw. War Room, aby umożliwić współpracę między zespołami w wypadku wystąpienia krytycznych incydentów. War Room MUSI być tworzony ręcznie lub poprzez eskalację istniejącego incydentu.
56. SOAR Moduł War Room zapewniać interfejs agregujący całościową informację o rozwiązywanym incydencie szczególnej wagi w tym:
    1. Status incydentu
    2. Listę aktualnie wykonywanych zadań
    3. Wyniki wykonanych zadań
    4. Raport aktualnej sytuacji oraz plan kolejnych działań
57. SOAR MUSI mieć możliwość personalizowania widoków w interfejsach dla użytkowników.
58. SOAR MUSI posiadać mechanizmy integracji z systemami bezpieczeństwa oraz infrastrukturą teleinformatyczną w zakresie:
    Wymienione w punkcie „Sposób integracji z zewnętrznymi systemami – konektory"
59. SOAR MUSI mieć możliwość definiowania cyklicznego generowania raportów..
60. SOAR MUSI posiadać mechanizmy logowania zdarzeń i operacji wykonywanych przez użytkownika.
61. SOAR MUSI posiadać mechanizmy uwierzytelniania w oparciu o Active Directory i protokół SAML.
62. Zarządzanie uprawnieniami do elementów interfejsu MUSI być oparte o role. Dla każdego pola danych w systemie musi być możliwość indywidualnej konfiguracji dla roli co najmniej w zakresie: tylko do odczytu (read), tworzenie (create), zmiany (update), kasowania (delete), brak dostępu.
63. SOAR MUSI posiadać mechanizmy uwierzytelnia wieloskładnikowego.
64. SOAR MUSI posiadać mechanizmy integracji co najmniej z dostarczanym systemem PAM.
65. SOAR MUSI posiadać interfejs użytkownika udostępniany poprzez https.
66. SOAR MUSI mieć możliwość automatycznego powiązania i grupowania podobnych incydentów (np. ten sam docelowy adres IP, usługa itp.)
67. System SOAR MUSI posiadać wbudowaną funkcjonalność tworzenia i zarządzania zadaniami.
68. Wszystkie atrybuty widoku alarmów, takie jak nazwa, ważność, itp. MUSZĄ być konfigurowalne, aby użytkownicy mogli je dodawać lub usuwać z interfejsu. Ponadto MUSI istnieć możliwość tworzenia, modyfikowania i usuwania własnych niestandardowych atrybutów w dowolnym module systemu.
69. Rozwiązanie MUSI umożliwiać skorelowanie i powiązanie rekordu typu alert, incydent, IoC z innym rekordem w systemie, w tym z niestandardowymi typami rekordów, które użytkownicy sami definiują. Relacje MUSZĄ obejmować co najmniej modele:
    1. Wiele-do-wiele
    2. Wiele-do-jednego
70. Rozwiązanie MUSI mieć silnik przewidywania oparty na uczeniu maszynowym, który przewiduje wartości pól na podstawie danych historycznych. Zakres przewidywania uczenia maszynowego MUSI

obejmować wszystkie moduły produktu: wbudowane (takie jak alerty, incydenty, wskaźniki,itd.) jak i niestandardowe.

71. Widok każdego modułu GUI MUSI być dowolnie konfigurowalny za pomocą szablonu widoku, który definiuje położenie każdego pola i widżetu.
72. System MUSI zapewniać funkcję globalnego wyszukiwania, która umożliwia analitykowi wyszukiwanie poprzez słowa kluczowe w całym systemie i we wszystkich modułach.
73. Interfejs użytkownika GUI MUSI oferować możliwość łączenia różnych rekordów razem (linkowanie). Rekordy mogą być między innymi: artefakty, zadania, War Room, użytkownicy, kampanie, assety, alarmy, załączniki, wiadomości e-mail, incydenty.
74. MUSI być możliwa eskalacja zgłoszenia ręcznie przez operatora lub automatycznie za pośrednictwem automatycznie uruchamianego Playbook-a, który może zastosować dowolną logikę jako warunek przed wykonaniem eskalacji zgłoszenia.
75. Incydenty, alarmy, artefakty, załączniki i moduły niestandardowe MUSZĄ udostępniać analitykom możliwość komunikowania się za pomocą komentarzy. Każda wiadomość wpisana przez analityka lub Playbook MUSI pozostać atrybutem rekordu, w którym został utworzony. Dodatkowo komentarze muszą umożliwiać:
    1. tworzenie ich prostym tekstem lub tekstem sformatowanym
    2. oznaczanie analityków w samym komentarzu, celem zwrócenia ich uwagi poprzez sposób typowy dla komunikatorów: @<nazwa konta>
    3. uruchamianie akcji
    4. obsługę tag-ów
    5. obsługę załączania plików
    6. zarządzanie dostępem do nich w oparciu o RBAC
76. System MUSI umożliwiać analitykowi analizę graficzną powiązań pomiędzy Incydentami i IOC. Graficzna korelacja MUSI być dostępna dla różnych typów rekordów np. assety, podatności, alarmy, incydenty.
77. Rozwiązanie MUSI być zintegrowane z MITRE ATTACK, przez którą to możliwe będzie wzbogacenie analizy incydentów o informacje takie jak: taktyki, analiza zagrożenia i sugestie dotyczące środków zaradczych.
78. System MUSI umożliwiać skonfigurowanie obowiązkowego uzupełnienia notatek przez operatora przed zamknięciem dochodzenia, dla incydentu obejmującego co najmniej sekcje:
    - informacja podsumowująca
    - następne kroki
    - opis sposobu rozwiązania problemu

Każde pole MUSI mieć możliwość wyboru konfiguracji: nieobowiązkowe, obowiązkowe, warunkowo obowiązkowe.

79. Obsługa incydentów MUSI wspierać oznaczanie fazy analizowanego ataku (kill chain phase). MUSI być możliwa zmiana definicji faz jak i ich ilości. Ustawiona faza w ramach incydentu POWINNA być reprezentowana graficznie.
80. 8Rozwiązanie MUSI mieć konfigurowalną funkcję zarządzania kolejkami obsługującą automatyczne przypisywanie alertów/incydentów/zadań do różnych grup obsługujących.

81. Rozwiązanie MUSI wyodrębnić artefakty (IP, URL, Domena, itp) z ponad 1500 typów plików takich jak MS Office, PDF, itd. Wyodrębnione artefakty muszą być połączone z rekordem pliku, z którego zostały wyodrębnione.

MUSI być możliwe wstępne przeglądanie wyniku analizy (preview) w postaci tekstu lub HTML.

82. Rozwiązanie MUSI umożliwiać operatorowi edycję dostępnych pól bezpośrednio w interfejsie WebUI zgodnie z przydzielonymi uprawnieniami. Uprawnienia MUSZĄ być konfigurowalne indywidualnie dla każdego pola. Minimalny zakres uprawnień to: brak, odczyt, odczyt-zapis. Zmiany w polach MUSZĄ być widoczne w logu audytowym systemu.
83. Playbook- i MUSZĄ być pogrupowane w foldery z możliwością eksportowania lub importowania całego folderu bezpośrednio z WebUI. Dzięki temu możliwa będzie migracja schematów pomiędzy systemem testowym a produkcyjnym.
84. Playbook-i MUSZĄ mieć co najmniej 3 priorytety wykonywania, pozwalające na wykonanie niektórych przed innymi w kolejce w zależności od ich ważności.
85. Playbook-i MUSZĄ mieć wyzwalanie warunkowe. Nie będą się uruchamiać, chyba że spełnione są określone warunki. Poniższe operatory warunków muszą być obsługiwane:
    1. Równy
    2. nie równa się
    3. mniej niż/mniej niż lub równa się
    4. większe niż/większe niż lub równe
    5. jest na liście
    6. nie ma na liście
    7. Pusty
    8. jest zgodny z zadanym wzorcem (pattern)
    9. nie jest zgodny z zadanym wzorcem (pattern)

Warunki MUSZĄ obsługiwać sumę logiczną (dowolny warunek spełniony) oraz iloczyn logiczny (wszystkie warunki muszą być spełnione).

86. Playbook-i MUSZĄ obsługiwać następujące sposoby uruchomienia:
    - analityk może ręcznie uruchomić w GUI systemowym
    - automatycznie przy zmianie rekordu (Alert, wskaźnik, incydent... itd.): utworzony/zmieniony/usunięty
    - przez API: gdy SOAR otrzymał żądanie API z określonymi parametrami to uruchamia określonego Playbook-a
    - referencja: playbook ma możliwość wykonania innego playbook-a z zadanymi parametrami
87. System MUSI zapewniać graficzny edytor Playbook-ów, w którym użytkownicy mogą używać myszy do przeciągania i upuszczania operacji lub kolejnych kroków. Ponadto edytor playbook MUSI zawierać panele pomocnicze do pobierania wszystkich dostępnych zmiennych, wybierania wszystkich typów operacji, tworzenia wyrażeń złożonych. Tworzenie Playbook-a lub jego edycja NIE MOŻE wymagać uruchamiania jakiegokolwiek innego interfejsu.
88. Graficzny edytor Playbook-ów MUSI mieć możliwość cofania kroków edycji jak i ich ponawiania. Przykładowo możliwe jest przywrócenie wcześniej usuniętej operacji.

89. Rozwiązanie MUSI umożliwiać użytkownikowi uruchomienie Playbook-a z poziomu edytora graficznego i przetestowanie jego wykonania z zmiennymi wybranego rekordu istniejącego w systemie lub ostatnim rekordem, z którym Playbook został wykonany.
90. Administratorzy muszą mieć możliwość indywidualnego eksportowania i importowania Playbook-ów, w tym dowolnie wybranej wersji (podobnie jak SVN / GIT).
91. Rozwiązanie MUSI obsługiwać tworzenie, modyfikowanie i usuwanie zmiennych globalnych dostępnych dla wszystkich Playbook-ów. Zmienne globalne muszą być edytowalne za pomocą Playbook-ów lub GUI.
92. System MUSI dostarczyć wizualną historię wykonania Playbook-ów, która identyfikuje dane wyjściowe, wejściowe i konfigurację każdego kroku.
93. Poziom logowania wykonywania Playbook-ów MUSI być konfigurowalny zarówno globalnie (w całym systemie) jak i lokalnie dla każdego Playbook-a indywidualnie. Muszą być wspierane co najmniej dwa poziomy logowania: informacyjny i debug.
94. Narzędzia do debugowania muszą być dostępne z poziomu edytora Playbook-ów. Debugger MUSI być w stanie korzystać z danych z poprzedniego wykonania Playbook-a lub danych dostarczonych przez analityka.
95. Kontrola praw dostępu (RBAC) MUSI obejmować Playbook-i w zakresie zapisu i uruchamiania.
96. Rozwiązanie MUSI zawierać szczegółowe komunikaty o błędach, gdy wykonanie Playbook -a nie powiedzie się i zezwalać na ponowne uruchomienie Playbook-a od kroku, w którym wykonanie nie powiodło się.
97. Kroki warunkowe w wykonywaniu Playbook-ów muszą być wystarczająco elastyczne, aby móc stosować złożone warunki. Wymagane możliwości budowania warunków:
    - równy porównuje dwa obiekty i wykonuje operację, gdy równe
    - nierówna się porównuje dwa obiekty i wykonuje operację, gdy nie równe
    - większy niż prawda, jeśli lewa strona jest większa niż prawa strona
    - większy niż lub równy prawda, jeśli lewa strona jest większa lub równa prawej stronie
    - mniejsze niż prawda, jeśli lewa strona jest mniejsza niż prawa strona
    - mniejsze lub równe prawda, jeśli lewa strona jest mniejsza lub równa prawej stronie
    - i zwróć wartość „prawda", jeśli lewe i prawe wyrażenie są prawdziwe
    - lub zwróć wartość „prawda", jeśli lewe lub prawe wyraże nie jest prawdziwe
    - nie negacja
    - dodawanie dodaje do siebie dwa obiekty
    - odejmowanie odejmij drugą liczbę od pierwszej
    - dzielenie dzielenie dwóch liczb
    - modulo obliczanie reszty z dzielenia liczby całkowitej
    - mnożenie mnożenie dwóch wartości
    - potęga podnieś lewy operand do potęgi prawego operandu

Warunki takie jak:

(zmienna_X + zmienna_Y)/2 > 3

((zmienna_X + zmienna_Y)/2 >zmienna_Z) OR (zmienna_A / zmienna_B) < 2

muszą być możliwe bez użycia języka programowania .Etap podejmowania decyzji MUSI mieć opcję ustawienia domyślnego następnego kroku, jeśli wszystkie warunki zawiodą.

98. Operatorzy muszą mieć możliwość zastosowania języka programowania, co najmniej Python bezpośrednio w Playbook-ach. Administrator SOAR MUSI być w stanie ograniczyć dostęp i możliwość wykorzystania bibliotek języka python (z dokładnością do pojedynczych bibliotek).
99. Kroki Playbook-ów muszą być konfigurowalne na wypadek wystąpienia błędu. Jeśli wystąpi błąd na poziomie kroku to MUSI być możliwy wybór co najmniej przekazania komunikatu o błędzie do następnego kroku i kontynuowanie lub zaprzestanie dalszego wykonywania.
100. Zarządzanie Playbook-ami MUSI umożliwiać analitykom zbiorczą ich edycję z możliwością wykonywania poniższych funkcji:
    1. Zmiana statusu (Playbook aktywny lub nieaktywowany)
    2. Klonowanie wybranych Playbook-ów
    3. Przenoszenie wybranych Playbook-ów do innej grupy
    4. Zmiana poziomu logowania dla wybranych Playbook-ów
    5. Eksportowanie wybranych Playbook-ów
101. Każdy Playbook w ramach proponowanego rozwiązania MUSI mieć możliwość automatycznego uruchomienia w określonych odstępach czasu z możliwością zapobieżenia jego wykonaniu, jeśli poprzednie wystąpienie jest nadal uruchomione.
102. W ramach edytora Playbook-ów analitycy muszą być w stanie wykonać operacje:
    - sklonuj krok
    - kopiuj i wklej krok lub grupę kroków do tego samego Playbook-a lub innego
    - wyrównaj wizualnie kroki na diagramie do układu pionowego lub poziomego

- wybierz krok lub grupę kroków i usuń je

103. Playbook-i MUSZĄ mieć możliwość wykonania kroku, gdzie konfigurowalne będzie uzyskanie danych i/lub potwierdzenia za pośrednictwem wiadomości e-mail zawierającej link do decyzji z opcją podjęcia określonej akcji w przypadku przekroczenia limitu czasu. Przykładem może być wysłanie wiadomości z prośbą o zgodę na restart urządzenia wraz z informacją zwrotną o dogodnym terminie.
104. System MUSI zapewniać przyjazny dla użytkownika kreator pozyskiwania danych zewnętrznych (np. informacje o użytkownikach, podatnościach) w celu stworzenia mechanizmu integracji pozwalającego na ciągłe i automatyczne pobierania wymaganych informacji.
105. System MUSI zapewnić pulpit (dashboard) z informacją o kondycji konektorów, który wskazuje, czy wszystkie integracje z systemami zewnętrznymi działają prawidłowo.
106. Akcje konektorów muszą podlegać prawom dostępu RBAC tak aby tylko zdefiniowane role mogły używać zdefiniowanych akcji z dokładnością do pojedynczej akcji.
107. System MUSI umożliwiać analitykowi uruchamianie dowolnej akcji konektora do której ma prawo, za pośrednictwem interfejsu GUI bez użycia Playbook-a.
108. Musi istnieć możliwość zbiorczego importu i eksportu wskaźników IOC bezpośrednio z GUI.
109. Rozwiązanie MUSI być na tyle elastyczne, aby umożliwić generowanie reputacji wskaźników na podstawie danych z różnych źródeł Threat Intelligence jednocześnie.
110. Rozwiązanie MUSI umożliwiać tworzenie kopii zapasowych i przywracanie zarówno konfiguracji systemu, jak i zebranych danych.
111. Rozwiązanie MUSI mieć możliwość tworzenia niestandardowych modułów funkcjonalnych z poziomu interfejsu GUI. Moduł jest podsystemem do zarządzania nowym typem rekordów, takich jak: Alerty, Incydenty, wskaźniki, itp.

112. Architektura systemu MUSI pozwalać na skalowanie rozwiązania jak i tworzenie wysokiej dostępności. Musi istnieć możliwość klastrowania wielu węzłów (minimum 3) w konfiguracji Aktywny/Aktywny.
113. Rozwiązanie MUSI oferować skalowalną geograficznie, rozproszoną architekturę z możliwością separacji części zasobów dla podległych jednostek lub innych użytkowników (model pracy MSSP).
114. Rozwiązanie MUSI umożliwiać uruchamianie Playbook-ów i kolekcję danych w zdalnych segmentach sieci za pośrednictwem agenta SOAR wdrożonego w segmencie sieci zdalnej. Agenty muszą obsługiwać automatyczne aktualizacje.
115. System MUSI umożliwiać korzystanie zarówno z wewnętrznej, jak i zewnętrznej bazy danych.
116. Rozwiązanie POWINIEN oferować aplikację mobilną co najmniej dla systemu Android do zdalnego zarządzania i monitorowania w ramach SOAR.
117. System MUSI zapewniać globalne logowanie aktywności (audyt) obejmujące zarówno działania użytkowników (takie jak logowanie, wylogowanie, instalacje, itp.) jak i zdarzenia związane z danymi (np tworzenie rekordów, aktualizowanie, usuwanie...)
118. System MUSI mieć możliwość przesyłania zdarzeń audytu i aplikacji do serwera zewnętrznego lub rozwiązania SIEM. Następujące protokoły muszą być obsługiwane z konfigurowalnym poziomem dziennika:
    1. UDP
    2. TCP, TCP/TLS
    3. RELP, RELP/TLS
119. System MUSI posiadać skonfigurowany widżet osi czasu dziennika inspekcji śledzący każde zdarzenie dla rekordu w alarmach, incydentach ze szczegółami każdej zmiany. Przykłady: uruchomienie Playbook-a, dodanie komentarza, zmiana wartości, etc.
120. System MUSI zapewniać szczegółową i elastyczną kontrolę dostępu opartą na rolach (RBAC). Administratorzy muszą mieć możliwość ustawienia praw dostępu dla każdego typu rekordu do poziomu pola. Na przykład pole „źródłowy adres IP".
121. SOAR MUSI obsługiwać hierarchię grup użytkowników. Grupa MUSI mieć możliwość dziedziczenia zakresu dostępu z innej grupy lub grup według poziomów:
    - grupa nadrzędna (parent) – ma dostęp do danych niższych grup i swojej
    - grupa równoważna (sibling) – ma dostęp do danych grup w ramach ustawionego połączenia
    - grupa podrzędna (child) – brak możliwości dostępu do danych z nadrzędnych grup
122. System powinien zapewniać wiele konfigurowalnych pulpitów nawigacyjnych (dashboard), które działają zgodnie z prawami dostępu RBAC.
123. System powinien zapewniać mechanizm wyróżniania alertów, które zbliżają się do naruszeń SLA.
124. Pulpit nawigacyjny powinien móc wyświetlać informacje specyficzne dla analityka, takie jak alerty i zadania przypisane do niego.
125. SOAR powinien obliczać szacowany zwrot z inwestycji i wyświetlenie go na pulpicie (dashboard).
126. Powinno być możliwe importowanie i eksportowanie szablonów pulpitu nawigacyjnego.
127. System powinien posiadać skonfigurowane pulpity nawigacyjne dedykowane dla ról, takich jak: analityk linii 1, analityk linii 2, menedżer SOC.
128. SOAR MUSI mierzyć wskaźniki SOC dla incydentów, takie jak średni czas dla poszczególnych faz ataku wg. killchain. Powinno być możliwe wyświetlanie tych danych na pulpicie nawigacyjnym.
129. Rozwiązanie MUSI mieć dedykowany pulpit nawigacyjny do monitorowania stanu/dostępności każdej integracji, a także kondycji systemu SOAR.

130. Rozwiązanie MUSI obsługiwać dostosowanie znaków graficznych (branding) interfejsu użytkownika dla różnych domen MSSP.
131. Rozwiązanie MUSI zapewniać framework dla przygotowana własnego pulpitu nawigacyjnego zgodny z HTML/JSON/JS, aby umożliwić tworzenie niestandardowych widżetów pulpitu nawigacyjnego i importowanie ich do rozwiązania SOAR.
132. System MUSI zapewniać konfigurowany moduł raportowania w GUI.
133. Raporty MUSZĄ mieć możliwość zaplanowania uruchamiania w czasie zdefiniowanym przez użytkownika.
134. Raporty MUSZĄ być generowane w co najmniej formatach CSV i PDF.
135. Wygenerowane raporty MUSZĄ mieć opcję wysłania pocztą elektroniczną.
136. MUSI być możliwe uruchamianie raportów z poziomu playbook.
137. Dostęp do raportów MUSI być ograniczany prawami dostępu RBAC.
138. System MUSI posiadać logi audytu, które dostarczą informacji o aktywności modułu raportowego, włączając akcję pobrania raportu.
139. MUSI istnieć możliwość dołączania do raportu grafik i wykresów.
140. System MUSI posiadać moduł zarządzania zmianą operatorów, w szczególności MUSZĄ być obsługiwane funkcje:
    1. generowanie kalendarza zmiany wg założonego wzoru, np. 8 godzin od 6:00 na tydzień do przodu, dni robocze dla wybranych użytkowników
    2. przekazywanie zmiany: przydzielanie niezamkniętych dochodzeń zmiany kończącej do zmiany rozpoczynającej pracę
    3. przypisywanie musi być możliwe dla wszystkich niezamkniętych spraw, które rozpoczęły się w zadanym przedziale czasu, np. ostatnie 7 dni
    4. przypisywane rekordy muszą mieć możliwość filtrowania:
    o filtrowanie na podstawie zawartości pól charakterystycznych rekordu i operacje na nich (zawiera, nie zawiera, istnieje, nie istnieje, jest na liście, spełnia wyrażenie regularne)
    o poszczególne filtry podlegają sumie logicznej (dowolny spełniony) lub iloczynowi logicznemu (wszystkie spełnione)
    5. musi być możliwe przypisanie rekordu:
    o nie przypisany
    o przypisany kierownikowi zmiany
    o wg. metody round robin w ramach członków zmiany
141. System MUSI posiadać moduł zarządzania kolejkami nadchodzących zdarzeń. Domyślnie musi być możliwe tworzenie dedykowanych kolejek dla rekordów typu zadanie, alarm i incydent. Każda kolejka musi się charakteryzować funkcjami co najmniej:
    1. wybór typu rekordu – dowolny zestaw (jeden typ, wszystkie typy)
    2. musi być możliwe dodawanie nowych typów rekordów do kolejek
    3. kolejka musi obsługiwać filtry wejściowe dla rekordów, minimalny zakres to:
    o utworzenie lub aktualizacja rekordu
    o filtrowanie na podstawie zawartości pól charakterystycznych rekordu i operacje na nich (zawiera, nie zawiera, istnieje, nie istnieje, jest na liście, spełnia wyrażenie regularne
    o poszczególne filtry podlegają sumie logicznej (dowolny spełniony) lub iloczynowi logicznemu (wszystkie spełnione)
    4. musi być możliwe ustawienie priorytetu rekordu w ramach kolei

5. musi być możliwe przypisanie rekordu:
- o nie przypisany
- o przypisany kierownikowi grupy
- o wg. metody roundrobin w ramach członków grupy

Wymiarowanie systemu

Dostarczony system SOAR musi spełniać następujące wymagania licencyjne:

1. Licencja musi być dostarczona w formie subskrypcji na okres co najmniej 36 miesięcy od daty końcowego odbioru
2. Licencja nie może w żaden sposób ograniczać ilości wykonywanych akcji przez system, ilości integracji, rozmiaru dysku, skonfigurowanych kont użytkowników.
3. System musi mieć umożliwiać pracę co najmniej jednego administratora lub operatora w danym momencie.

Sposób integracji z zewnętrznymi systemami - konektory

System SOAR musi być zaoferowany łącznie z integracją z poniższymi systemami posiadanymi przez Zamawiającego:

1. Microsoft Active Directory. Windows 2016
2. Energy Logserver
3. System pocztowy Zimbra
4.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Oferowane rozwiązania muszą pochodzić od jednego producenta.
3. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.