

OPIS PRZEDMIOTU ZAMÓWIENIA

Ochrona przetwarzania informacji w infrastrukturze IT na poziomie usług sieciowych i aplikacji

1. Część 1 zamówienia - Wdrożenie systemu kontroli dostępu do zasobów i usług sieciowych – system NAC

Podstawowa funkcjonalność i wymagania wobec systemu NAC:

1. System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych.
2. System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor)
3. System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek.
4. System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji.
5. System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji.
6. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych.
7. System musi umożliwiać obsługę co najmniej 300 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 1000 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania.
8. Licencja ma być zwalniana po rozłączeniu urządzenia końcowego.
9. System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia.
10. System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym:
 - VM – min. VMWare ESXi co najmniej w wersji 5.x, Hyper-V w wersji min 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.x, Citrix XenServer w wersji min 4.x
 - Maszyny fizyczne - serwery wspierane przez producenta.
11. System musi posiadać funkcjonalność serwerów:
 - serwera RADIUS dla infrastruktury sieciowej,
 - serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+,
 - serwera SYSLOG,
 - serwera TACACS+,
 - serwera Monitoringu,
 - serwera DHCP,
 - serwera polityk uwierzytelniania i kontroli dostępu 802.1X,
 - serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego.
12. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostęp do sieci i DHCP.
13. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.

14. System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google Workspace, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.
15. System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznymi systemami (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, Radius, OpenLDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC), CheckPoint, Service Now).
16. Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email.
17. System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.
18. System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania.
19. System musi mieć możliwość obsługi wielu PKI dla różnych grup użytkowników.
20. System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie.
21. System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. Login, Hasło, Imię, Nazwisko, Email, Status).
22. System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania.
23. Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim).
24. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.
25. System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP.
26. System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia.
27. System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.
28. System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP.
29. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, Autoryzacji, Statusu, Opisu.
30. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
31. System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP.
32. System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci.
33. System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.
34. System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP, Tacacs+.

35. System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.
36. System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).
37. System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook, Google, LinkedIn.
38. System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS.
39. System musi posiadać funkcję personalizacji strony gościnnej.
40. Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.
41. Captive Portal musi umożliwiać rejestrację gości potwierdzanych przez konta typu sponsor.
42. Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS.
43. Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.
44. Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.
45. Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.
46. Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru.
47. Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).
48. Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.
49. Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni.
50. Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań.
51. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.
52. System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego.
53. System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.
54. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.
55. System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.
56. System musi obsługiwać różne metody profilowania do wykrywania typu urządzenia, systemu operacyjnego, przez co najmniej DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF.
57. System musi umożliwiać integrację z zewnętrznymi rozwiązaniami typu MDM (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc).
58. System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minimum na systemach: FortiGate, Pulse Secure, OpenVPN, Palo Alto, Cisco ASA.
59. System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej:
 - Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności

- Czy włączony jest firewall
 - Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur
 - Czy jest włączone szyfrowanie dysku systemowego
 - Czy urządzenie końcowe jest połączone do domeny Microsoft Active Directory
 - Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora
 - Czy w systemie są uruchomione procesy wskazane przez administratora
 - Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności
 - Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem:
 - Wartości klucza rejestru
 - Typu wartości: Number, String, Version
60. System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal.
61. System musi współpracować z serwerem tokenów.
62. System musi posiadać mechanizm autokonfiguracji sieci (autokonfigurator sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działu IT dla systemów co najmniej:
- Microsoft Windows
 - Mac OS
 - iOS
 - Android
63. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfigurator sieci).
64. System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory.

Mechanizmy uwierzytelniania

1. System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.
2. System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły:
 - MAC,
 - PAP/ASCII,
 - CHAP,
 - SNMP,
 - 802.1X.
3. Wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), TEAP, itp.
4. System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.
5. System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.
6. System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Windows 11, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant).
7. System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:
 - Tożsamość/Urządzenie końcowe,
 - Grupa tożsamości/urządzeń końcowych,
 - Parametry urządzeń końcowych, min: system operacyjny, wersja,
 - Atrybuty Active Directory,
 - Jednostka organizacyjna tożsamości/urządzeń końcowych,
 - Urządzenia sieciowe sieci przewodowej, bezprzewodowej,

- Grupy urządzeń sieciowych,
 - Porty urządzeń sieciowych,
 - Grupy portów urządzeń sieciowych,
 - Jednostka organizacyjna portów,
 - Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),
 - Data, czas ważności polityki,
 - Wewnętrzny Captive Portal,
 - Metoda autoryzacji.
8. System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, Juniper Networks, Ruckus Networks, MicroTik, Ubiquiti Networks.
 9. System musi wspierać funkcjonalność *IP-to-ID Mapping*, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.
 10. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI.
 11. System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.
 12. System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.
 13. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.
 14. System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.
 15. System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal.
 16. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC.
 17. System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.
 18. System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www.
 19. System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.
 20. System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP.

Obsługa serwerów certyfikatów CA

1. System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.
2. Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności:
 - możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych.
 - możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych.
 - Możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol).
 - usługę OCSP (Online Certificate Status Protocol).

Obsługa serwerów DHCP

1. System musi posiadać funkcję zintegrowanego serwera DHCP.
2. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP.
3. System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP:
 - Uruchamianie usługi dla wybranych podsieci,
 - Przypisanie ustalonego adresu IP dla adresu MAC.
 - Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci,
 - Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC,
 - Możliwość określania braku dostępu dla wybranych adresów MAC,
 - Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC,
 - Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP,
 - Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego,
 - Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi,
 - Dokonywanie zmian bez konieczności wyłączania usług.

Obsługa serwerów TACACS+

System musi umożliwiać tworzenie grup uprawnień do kontroli dostępu urządzeń sieciowych:

1. System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów.
2. System musi umożliwiać tworzenia haseł administratorom.
3. System musi umożliwiać tworzenie listy komend uprawnień dla administratorów
4. System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych.
5. System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu.
6. System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory.
7. System musi wspierać logowanie administratorów za pomocą tokenów OTP.
8. System musi umożliwiać przypisywanie atrybutów zwrotnych VSA podczas etapu autoryzacji.

Raportowanie i monitoring

System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:

1. Monitoring autoryzacji.
2. Monitoring dla zdarzeń systemowych.
3. Monitoring dla zdarzeń DHCP.
4. Monitoring dla tożsamości.
5. Monitoring dla urządzeń końcowych.
6. Monitoring dla urządzeń sieciowych.
7. Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email.
8. Raport ze zdarzeń logowania z informacją o nadanym adresie IP.
9. Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług.
10. Raport z logów DHCP z informacją o polityce dostępu logowania do sieci.
11. System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.
12. System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie.

13. System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności VLANów w urządzeniach sieciowych działających w środowisku.
14. System musi wspierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych.
15. System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja.
16. System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi.
17. Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS.
18. Raport zdarzeń Microsoft Active Directory, minimum:
 - Logowania, wylogowania z system w tym błędne logowania
 - Logowania do sieci 802.1X

Alarmy

1. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:
 - wiadomości e-mail,
 - Syslog,
 - notyfikacji systemowych.
2. Alarmy mogą być generowane w sytuacjach, min:
 - Ilości obsługiwanych transakcji RADIUS,
 - Opóźnienie obsługi transakcji RADIUS,
 - Statusu krytycznego modułów.
3. System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:
 - badanie łączności IP za pomocą ping, traceroute,
 - tcpdump protokołów RADIUS, TACACS+,
 - wyszukiwanie zdarzeń RADIUS z uwzględnieniem:
 - nazwy użytkownika,
 - adresu MAC,
 - statusu uwierzytelnienia (udana lub nieudana),
 - powodu, jeżeli uwierzytelnienie nieudane,
 - zakresu czasowego, co do dnia, godziny i minuty,
 - wykonanie zdalnego polecenia na urządzeniu sieciowym.

Wymagania dotyczące wdrożenia i harmonogram ramowy:

- Dostawa, instalacja, konfiguracja wstępna i zalicencjonowanie produktu w środowisku klienta.
- Podstawowa konfiguracja Systemu NAC (integracja z domeną, konfiguracja urzędu certyfikacji, uruchomienie HA).
- Konfiguracja urządzenia firewall (dodatkowo VLAN-u gościnnego, ustawienie polityk, etc.).
- Import urządzeń końcowych i tożsamości (z AD oraz dostarczonych przez Zamawiającego list).
- Integracja dostarczanych urządzeń sieciowych (switche, AP itp.) z Systemem NAC, w ramach funkcjonalności dostępnych na urządzeniach.
- Uruchomienie uwierzytelniania w oparciu o 802.1X (EAP-TLS) na urządzeniach końcowych wzorcowych po jednym z każdej serii, testy.
- Uruchomienie uwierzytelniania w oparciu o adres MAC w korelacji z innymi możliwościami np. DHCP, SNMP, skan portów, testy.
- Przeprowadzenie szkolenia dla administratorów z konfiguracji i administrowania Systemem

NAC. Dwudniowe szkolenie online zdalne dla do 4 osób po 5h dziennie.

- Przygotowanie dokumentacji powykonawczej opisującej wykonane prace oraz sposób konfiguracji poszczególnych urządzeń do 14 dni po zakończeniu wdrożenia.

Szkolenia/warsztaty:

- Wykonawca zapewni 2-dniowe warsztaty (2 dni x 5h) w zakresie użytkowania i administrowania wdrożonym systemem NAC
- Warsztaty zostaną przeprowadzone dla maksymalnie 4 osób i będą uwzględniać informacje z zakresu wdrożonego systemu NAC
- Po zakończeniu warsztatów, uczestnicy otrzymają zaświadczenia potwierdzające uczestnictwo w szkoleniach/warsztatach oraz nabycie umiejętności obsługi systemu NAC
- Warsztaty odbędą się w formie zdalnej.
- Wykonawca dla każdego uczestnika dostarczy materiały szkoleniowe w języku polskim w postaci elektronicznej.
- Szczegółowy plan, zakres i terminy szkoleń/warsztatów zostaną uzgodnione przez Wykonawcę z Zamawiającym

Licencja wsparcia technicznego producenta oprogramowania:

Wykonawca dostarczy wraz z dożywotnią licencją systemu NAC – min. 12 miesięczną licencję na wsparcie producenta oprogramowania (wsparcie producenta zgodne będzie z deklaracją Wykonawcy w ofercie – kryterium oceny ofert). Licencja ta powinna obejmować minimum:

- Kontakt mailowy z działem wsparcia technicznego w celu rozwiązania problemów związanych z wdrożeniem lub obsługą systemu NAC
- Rozwiązywanie powtarzalnych i rozwiązywalnych problemów związanych z oprogramowaniem a także wsparcie przy identyfikacji problemów trudnych do powtórzenia.
- Wsparcie przy rozwiązywaniu problemów oraz pomoc w określaniu parametrów dla konfiguracji oprogramowania oraz wstępne obejścia dla wykrytych problemów.
- Dostęp do dokumentacji i instrukcji na stronie internetowej.
- Dostęp do aktualizacji i poprawek, które powinny być dostępne z poziomu interfejsu oprogramowania.

2. Część 2 zamówienia - Wdrożenie systemu detekcji i monitorowania sieci oraz narzędzi automatycznej analizy logów – system SIEM/SOAR

Podstawowa funkcjonalność i wymagania wobec systemu SIEM/SOAR:

1. Zaproponowany system SIEM/SOAR musi stanowić platformę do przeciwdziałania cyberzagrożeniom, oferującą możliwości wykrywania i obsługi zdarzeń, incydentów oraz podatności. Dostarczony system musi być wdrożony w środowisku informatycznym Zamawiającego w celu przeciwdziałania cyberzagrożeniom i umożliwiającą ich wykrywanie przy wsparciu mechanizmów uczenia maszynowego oraz zapewniającą automatyzację i orkiestrację ich obsługi.
2. System musi umożliwić odbieranie logów wygenerowanych przez systemy zabezpieczeń, systemy sieciowe, systemy operacyjne i aplikacje następującymi protokołami: Syslog, TLS syslog, NetFlow, Windows Event Forwarding.
3. Logi pozyskiwane z systemów Microsoft Windows nie mogą wymagać instalowania dedykowanego oprogramowania bezpośrednio na tych systemach.
4. System musi posiadać wbudowane mechanizmy zapewniające możliwość pobierania zdarzeń poprzez wykorzystanie RestFull-API, sterownika ODBC, agenta do czytania plików płaskich, protokołów IMAPS, POP3S, MAPI do pobierania wiadomości ze skrzynek poczty elektronicznej oraz obsługi zapytań WQL w ramach protokołu WMI;
5. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych.
6. System musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych zdarzeń umożliwiające ich podział na poszczególne pola, na podstawie których może odbywać się dalsze przetwarzanie oraz wyszukiwanie ich w systemie.
7. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, obejmującą zmianie wartości tych pól lub dodanie nowych w oparciu o ich wartości lub wzorzec wyszukiwania. Cały proces musi odbywać się na bieżąco na etapie rejestrowania danych w systemie.
8. Proces normalizacji musi wspierać następujące typy składni: CEF, LEEF, URI, SYSLOG (zgodny z RFC 3164) i automatycznie tworzyć na ich podstawie pola i ich wartości zgodne z zasadami określonymi przez te składnie. Parsowanie powyższych składni nie może być realizowane za pomocą wyrażeń regularnych.
9. Normalizacja musi umożliwiać automatyczne nadawanie kategorii zdarzeń w formie nowych pól, np.: logowanie, wylogowanie, zmiana uprawnień, błąd konfiguracji, wykryte skanowanie systemu czy zablokowany malware.
10. Normalizacja logów musi posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól o nazwę lub kod kraju korzystając z wbudowanej w produkt bazy.
11. System musi posiadać predefiniowany zestaw parserów oraz umożliwiać ich wersjonowanie, aby po wgraniu nowej wersji parsera, w razie przypadku gdy będzie to konieczne przywrócić jedną z poprzednich wersji.
12. System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) dla zdarzeń z niestandardowych źródeł danych, w oparciu o następujące składnie: CEF, LEEF, URI, XML, JSON, SYSLOG, REGEX. System musi umożliwiać zastosowanie wszystkich typów składni dla pojedynczego zdarzenia, przykładowo pole „msg” znormalizowane automatycznie według standardu CEF powinno mieć możliwość dalszej normalizacji np.: zgodnej z URI lub REGEX.
13. Proces normalizacji musi posiadać możliwość optymalizacji, poprzez automatyczny dobór odpowiedniego parsera dla źródła logów w zależności od składni w której te logi są przesyłane. Przykładowo jeżeli logi są przesyłane w standardzie CEF system dobierze odpowiedni parser, w przypadku gdy źródło zmieni format generowania zdarzeń na LEEF system musi automatycznie zmienić parser bez ingerencji operatora.
14. System musi rejestrować i przechowywać pozyskane logi w postaci surowej (RAW) oraz znormalizowanej.
15. System musi być wyposażony w graficzny interfejs umożliwiający określenie miejsca składowania logów (wskazania właściwego repozytorium logów) w zależności od zawartości tych logów, gdzie reguły przekierowania muszą umożliwiać definiowanie warunków po wszystkich sparsowanych polach. Przykładowo jeżeli w zdarzeniu znajduje się informacja o danych poufnych to zdarzenie to zostanie przekierowane do repozytorium A, natomiast w przypadku gdy tej informacji nie będzie to zdarzenie zostanie przekierowane do repozytorium B.

16. Każde z repozytorium logów musi mieć możliwość definiowania własnych zasad retencji uwzględniających zdefiniowanie okresu przechowywania lub ilości miejsca przeznaczonego na dane repozytorium. Dla każdego z repozytorium w przypadku jego zapelnienia musi być możliwa konfiguracja, która zapewni automatyczne przeniesienie logów do archiwum lub umożliwi ich nadpisanie.

17. System musi umożliwiać fizyczne rozdzielanie repozytoriów logów pobieranych z systemów informatycznych od repozytoriów zdarzeń generowanych w ramach systemu, w tym m.in. odseparowanie zdarzeń korelacyjnych na oddzielne repozytoria danych składowane na osobnych serwerach i dedykowanych do tego celu zasobów dyskowych od wszelkich repozytoriów logów.

18. Ze względu na możliwość wygenerowania dużej ilości danych przez algorytmy uczenia maszynowego system musi mieć możliwość rozdzielania ich składowania na osobny serwer i dedykowane zasoby dyskowe.

19. System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych w postaci skompresowanej.

20. System musi zapewnić mechanizmy bezpieczeństwa dla danych przechowywanych w repozytoriach uniemożliwiające ich nieautoryzowaną modyfikację oraz zapewnić operatorom mechanizmy weryfikacyjne integralności danych.

21. System musi udostępniać możliwość konfiguracji automatycznego odrzucenia logów niezawierających istotnych dla zamawiającego informacji. Definiowanie, które logi mają zostać odrzucone i niezapisane w repozytorium logów musi być realizowane za pomocą reguł, które pozwolą zdefiniować warunki po wszystkich sparsowanych polach.

22. System musi być wyposażony w graficzny interfejs umożliwiający przeglądanie i przeszukiwanie zarejestrowanych zdarzeń w formie znormalizowanej i pierwotnej. Interfejs musi prezentować wyniki wyszukiwania z zastosowaniem filtrów opartych na wartościach pól, złożonych wyrażeniach logicznych, wskazaniach zakresu czasowego i źródła danych. Interfejs wyszukiwania musi umożliwiać zapisywanie zapytań z możliwością ich ponownego wykorzystania w przyszłości. Tworzenie zapytań musi być możliwe poprzez bezpośrednie wskazanie pola zdarzenia za pomocą wskaźnika myszy i dodanie tego pola do filtra wyszukiwania, wraz z określeniem warunków wyszukiwania przez wyrażenie logiczne.

23. System musi zapewniać możliwość utrzymywania dokumentacji sieci, systemów oraz usług, umożliwiającej na gromadzenie i edycję danych istotnych w kontekście oceny generowanych przez system zdarzeń bezpieczeństwa.

24. Elektroniczna dokumentacja musi posiadać możliwość wizualizacji w formie interaktywnej mapy sieci, gdzie na pierwszym planie będą widoczne urządzenia zabezpieczeń, strefy bezpieczeństwa oraz połączenia sieciowe wskazujące jakie mechanizmy zabezpieczeń chronią poszczególne strefy bezpieczeństwa. „Kliknięcie” na dowolny z obiektów na pierwszym planie musi pozwolić na podgląd oraz edycję parametrów tego obiektu. Przykładowo po kliknięciu na strefę bezpieczeństwa musi istnieć możliwość definiowania komputerów należących do tej strefy, ich adresacji oraz innych z nimi związanych parametrów.

25. System musi umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji również w formie tabelarycznej.

26. System musi pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci, np.: poziom krytyczności systemów oraz usług.

27. System musi umożliwiać generowanie elektronicznej dokumentacji sieci i systemów w sposób automatyczny na podstawie dostarczonych przez producenta reguł wykrywania oraz edytora graficznego pozwalającego utworzyć dodatkowe reguły.

28. System musi zawierać narzędzia służące do ustalania wrażliwych zbiorów informacji, jakie są narażone w razie incydentu bezpieczeństwa. Ma umożliwiać definiowanie własnego schematu klasyfikacji danych w organizacji (np. własność intelektualna, dane osobowe, dane finansowe) oraz zapewnić wyszukiwanie lokalizacji zasobów teleinformatycznych, gdzie znajdują się dane określonej kategorii ze wskazaniem ich na graficznej mapie systemu teleinformatycznego.

29. Definiowanie reguł wykrywania musi bazować na sparsowanych polach oraz wyszukanych zależnościach między różnymi zdarzeniami z wielu źródeł oraz po aktywacji automatycznie uzupełnić elektroniczną dokumentację o następujące informacje:

- nowe zasoby wykryte w sieci,
- typy wykrytych zasobów (np.: serwer lub stacja robocza),
- zastosowane na nich zabezpieczenia,

- usługi z którymi się komunikują,
- nowe usługi wykryte na zasobie
- komunikację do usług wykrytych na zasobie.

30. System musi umożliwiać uwiarygodnianie uzyskiwanych informacji na bazie wartości progowych osiągniętych w zadanej jednostce czasu i dopiero po ich uwiarygodnieniu uzupełniać automatycznie elektroniczną dokumentację.

31. System powinien posiadać zestaw predefiniowanych reguł do automatycznego uzupełniania elektronicznej dokumentacji, których uruchomienie będzie automatycznie aktualizować elektroniczną dokumentację bez ingerencji operatora.

32. Interfejs interaktywnej mapy sieci musi posiadać mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT który został zdefiniowany w elektronicznej dokumentacji oraz nazwę usługi której ta komunikacja dotyczy.

33. System musi posiadać wbudowaną bazę wskaźników kompromitacji, która umożliwi zbieranie, przechowywanie oraz przypisywanie wskaźników kompromitacji (IoC) do incydentów. Baza powinna obsługiwać protokół TLP w wersji 2.0 oraz obsługiwać następujące typy wskaźników:

- fqdn,
- e-mail,
- nazwa pliku,
- ścieżka do pliku,
- hash,
- adres IP,
- klucz rejestru,
- cmd.

34. System musi umożliwiać synchronizację wskaźników kompromitacji (IOC) z platformami dostępnymi publicznie. Wymagane jest aby produkt posiadał gotowy mechanizm pobierania wskaźników z platformy MISP (<https://www.misp-project.org/>).

35. System musi umożliwiać definiowanie list referencyjnych zarówno z jedną wartością jak i łączących unikalne wartości w pojedynczym wierszu (np: obraz pliku, hash, nazwa procesu).

36. Listy referencyjne muszą mieć możliwość synchronizacji z listami publikowanymi publicznie (np.: „Malicious IPs”, „Malicious domain” czy „Tor Exit Nodes”).

37. System musi być zintegrowany z usługą katalogową Microsoft Active Directory celem pobrania informacji o poświadczeniach oraz atrybutach użytkowników i komputerów zarejestrowanych w domenie. Minimum to: nazwa komputera wraz z systemem operacyjnym, nazwa użytkownika, login, e-mail, przynależność do grup, przełożonego, jednostkę organizacyjną oraz listę kont uprzywilejowanych.

38. System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać możliwość jej synchronizacji z usługą katalogową Microsoft Active Directory.

39. System musi umożliwiać analizę konfiguracji systemów IT poprzez ich skanowanie bezpośrednio w ramach mechanizmów dostępnych w samym rozwiązaniu oraz poprzez integrację ze skanerami podatności. Oczekiwanym wynikiem analizy jest lista niezgodności, (np: czy na zasobie jest ustawione wymuszanie zmiany haseł w zadanym okresie czasu).

40. System powinien posiadać zestaw predefiniowanych reguł weryfikacji konfiguracji zasobów IT.

41. System musi zawierać mechanizm integracji ze skanerami podatności co najmniej trzech producentów. W ramach integracji system musi mieć możliwość uruchamiania skanowania podatności, importowania jego wyników zawierających listę podatności i ich atrybuty oraz możliwość kasowania ze skanera zaimportowanych wcześniej skanów. Wszystkie powyższe operacje muszą być konfigurowalne z poziomu graficznego interfejsu systemu.

42. Rozwiązanie musi zawierać mechanizm pasywnej analizy podatności, obejmującej systemy IT uzupełnione o informację zgodne z słownikiem CPE (ang. Common Platform Enumeration), umożliwiającą import wykrytych podatności zasobu do systemu z publicznie dostępnej bazy CVE (ang. Common Vulnerabilities and Exposures) i dalszą obsługę tych podatności w systemie.

43. System musi umożliwiać mapowanie zdarzeń bezpieczeństwa na poszczególne techniki z bazy wiedzy

MITRE ATT&CK® oraz zapewniać mechanizmy filtrowania zdarzeń po tych technikach oraz wyświetlania szczegółów związanych z daną techniką, w szczególności:

- id techniki,
- taktykę,
- platformy których dotyczy,
- potencjalne źródła,
- opis zagrożenia,
- mityzację,
- sposób detekcji,
- referencje.

44. System w swoim działaniu musi korzystać z wbudowanych algorytmów uczenia maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników i komputerów.

45. Modele zachowania użytkowników (UBA) i komputerów (EBA) muszą być tworzone automatycznie na bazie zdarzeń historycznych ze skonfigurowanego (wskazanego) okresu lub zdefiniowanej ilości zdarzeń wymaganych do ukończenia procesu nauczania. Algorytm nauczania musi mieć możliwość konfiguracji sposobu odrzucania wartości skrajnych mogących wpłynąć negatywnie na wyniki procesu nauczania oraz umożliwić odrębne uczenie w ramach zdefiniowanych zakresów czasowych (np.: rozdzielenie zdarzeń do nauczania w godzinach pracy od zdarzeń po godzinach pracy).

46. System musi posiadać zestaw predefiniowanych i konfigurowalnych reguł do automatycznego przyporządkowania użytkowników i zasobów do właściwych profili nauczania, reguły te muszą zapewnić minimum:

- rozdzielenie procesu nauczania zachowania użytkowników uprzywilejowanych od użytkowników nieuprzywilejowanych,
- rozdzielenie procesu nauczania zachowania stacji roboczych od serwerów,
- rozdzielenie serwerów świadczących usługi w sieci Internet od serwerów świadczących usługi lokalnie w organizacji,
- rozdzielenie procesu nauczania serwerów należących do domeny od pozostałych serwerów.

47. System uczenia maszynowego musi posiadać wbudowane mechanizmy nie wymagające żadnej dodatkowej konfiguracji, które po zakończeniu procesu nauki umożliwią detekcję anomalii zachowania użytkowników oraz zasobów (UEBA).

48. Wykryte przez mechanizmy uczenia maszynowego anomalie muszą generować zdarzenia, zawierające minimum informację o użytkowniku lub adresie IP na którym została wykryta anomalia oraz wykorzystany algorytm. System musi umożliwiać wykorzystanie tych zdarzeń w celu dalszej korelacji.

49. System musi pozwalać na zautomatyzowaną ocenę wpływu incydentu bezpieczeństwa IT na działalność organizacji względem zagrożeń natury informatycznej (np: utrata wizerunku, związana z zagrożeniem przełamania zabezpieczeń serwera webowego organizacji dostępnego z sieci Internet).

50. System musi zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role.

51. Dostarczone rozwiązanie musi umożliwiać gromadzenie i korelację zdarzeń przesyłanych lub pobieranych z innych systemów. Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł oraz ich agregację.

52. System musi posiadać interfejs graficzny do tworzenia własnych reguł korelacyjnych odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie. Korelacja musi odbywać się na bieżąco na etapie rejestrowania danych w systemie a mechanizm tworzenia reguł musi uwzględniać:

- sparsowane pola oraz ich wartości,
- listy referencyjne,
- atrybuty użytkowników z Active Directory,
- atrybuty komputerów z Active Directory,
- bazę wskaźników kompromitacji (IOC),
- informacje z elektronicznej dokumentacji,
- anomalie w zachowaniu użytkowników (UBA),
- anomalie w zachowaniu zasobów (EBA),
- podatności na zasobach,
- wyniki analizy konfiguracji,
- techniki MITRE ATT&CK®.

53. Reguły korelacyjne bazujące na sparsowanych polach i ich wartościach muszą umożliwić:

- wykrycie dowolnej treści w logach,
- wykrycie zmiany jednego z kilku pól,
- wykrycie zaniku wiadomości,
- wykrycie nowej wartości pola w zadanym okresie czasu,
- wykrycie incydentu będącego pochodną zdarzeń występujących w określonej kolejności,
- wykrycie zdefiniowanej ilości przesłanych danych w zadanym okresie czasu,
- wykrycie chwilowego wzrostu ilości przesłanych danych (tzw. peek) w stosunku do całkowitej ilości przesłanych danych w zadanym okresie czasu,
- wykrycie sumarycznego wzrostu przesłanych danych w zdefiniowanej strefie bezpieczeństwa,
- wykrycie zdefiniowanej ilości przesyłanych pakietów w zadanym okresie czasu,
- wykrycie chwilowego wzrostu (tzw. peek) w stosunku do ilości przesyłanych pakietów w zadanym okresie czasu,
- wykrycie sumarycznego wzrostu ilości pakietów przesyłanych w zdefiniowanej strefie bezpieczeństwa,
- wykrycie ilości uruchomionych procesów w zadanym okresie czasu,
- wykrycie skanowania portów.

54. Reguły korelacyjne bazujące na listach referencyjnych muszą umożliwić:

- wykrycie wystąpienia wartości pola na wybranej liście,
- wykrycie niewystępowania wartości pola na wybranej liście,
- wykrycie wystąpienia pary wartości na wybranej liście (np.: proces i obraz pliku z którego został uruchomiony),
- wykrycie niewystąpienia pary wartości na wybranej liście
- (np.: nazwa użytkownika wraz aplikacją z którą się wcześniej nie łączył).

55. Reguły korelacyjne wykorzystujące atrybuty użytkowników z Active Directory muszą umożliwić:

- wykrycie czy zdarzenie pochodzi od użytkownika posiadającego konto w Active Directory,
- wykrycie czy zdarzenie pochodzi od użytkownika posiadającego uprzywilejowane konto w Active Directory,
- wykrycie czy zdarzenie pochodzi od użytkownika podszywającego się pod konto użytkownika Active Directory (np.: którego e-mail zdefiniowany w Active Directory różni się od e-maila ze zdarzenia mimo, zgodności pozostałych atrybutów konta).
- wykrycie czy zdarzenie pochodzi od użytkownika należącego do wybranej grupy w Active Directory (np.: Domain Admins),
- wykrycie czy zdarzenie pochodzi od użytkownika nie należącego do wybranej jednostki organizacyjnej.

56. Reguły korelacyjne wykorzystujące atrybuty komputerów z Active Directory muszą umożliwić:

- wykrycia czy zdarzenie pochodzi z komputera należącego do domeny Active Directory,
- wykrycia czy zdarzenie pochodzi z komputera z systemem operacyjnym zdefiniowanym w Active Directory,
- wykrycia czy zdarzenie pochodzi z komputera z wybranej jednostki organizacyjnej.

57. Reguły korelacyjne wykorzystujące bazę wskaźników kompromitacji (IOC) muszą umożliwić:

- wykrycie czy źródłowy adres IP nie jest oznaczony w systemie jako wskaźnik kompromitacji;
- wykrycie czy HASH występujący w zdarzeniu nie jest oznaczony w systemie jako wskaźnik kompromitacji;
- wykrycie czy docelowa nazwa hosta (FQDN) nie jest oznaczona w systemie jako wskaźnik kompromitacji;

58. Reguły korelacyjne wykorzystujące informacje z elektronicznej dokumentacji muszą umożliwić:

- wykrycie połączenia z serwera do stacji roboczej w przypadku braku informacji o rodzajach zasobu w korelowanym zdarzeniu,
- wykrycie połączenia do usługi przez nieautoryzowanego użytkownika,
- wykrycie nieautoryzowanej usługi na serwerze,
- wykrycie nieautoryzowanego połączenia do usługi na serwerze,
- wykrycie nieautoryzowanego połączenia z serwera usług,
- wykrycie nieautoryzowanego połączenia do sieci Internet.

59. Reguły korelacyjne wykorzystujące anomalie w zachowaniu użytkowników (UBA) muszą umożliwić:

- wykrycie anomalii ilościowej związanej z kontem użytkownika wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania,
- wykrycie anomalii związanej ze zmianą zachowania na koncie użytkownika, wskazującej na potencjalny atak APT/Ransomware,
- wykrycie różnych typów anomalii na koncie użytkownika wskazujących na możliwe przejęcie konta użytkownika przez cyberprzestępcę lub złośliwe oprogramowanie,
- wykrycie anomalii związanych z logowaniami użytkowników w ramach sesji VPN.

60. Reguły korelacyjne wykorzystujące anomalie w zachowaniu zasobów (EBA) muszą umożliwić:

- wykrycie anomalii ilościowej związanej z komputerem wskazującej na potencjalny atak (D)DoS lub próbę

- propagacji złośliwego oprogramowania,
- wykrycie anomalii związanej ze zmianą zachowania komputera, wskazującej na potencjalny atak APT/Ransomware,
- wykrycie różnych typów anomalii na komputerze, wskazujących na możliwe przejęcie komputera przez cyberprzestępcę lub złośliwe oprogramowanie,
- wykrycie anomalii związanych z procesami uruchamianymi na serwerach.

61. Reguły korelacyjne wykorzystujące podatności na zasobach muszą umożliwić:

- wykrycie skanowania portów z zasobu posiadającego krytyczne podatności,
- wykrycie wielokrotnych prób połączeń do zasobu posiadającego krytyczne podatności,
- wykrycie zdarzeń o wysokim „severity” na zasobach posiadających krytyczne podatności,
- wykrycie zdarzeń o wysokim „severity” do zasobów posiadających krytyczne podatności.

62. Reguły korelacyjne wykorzystujące wyniki analizy konfiguracji muszą pozwalać na:

- wykrycie wielokrotnych prób nieudanego logowania do komputera, umożliwiające ustawienie hasła zawierającego mniej niż 14 znaków,
- wykrycie wielokrotnych prób nieudanego logowania do komputera, który umożliwia tworzenie haseł nie spełniających następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny.

63. Reguły korelacyjne wykorzystujące technikach MITRE ATT&CK® muszą umożliwić:

- wykrycie zdefiniowanej ilości technik w zdarzeniach dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP,
- wykrycie zdefiniowanej ilości zdarzeń w ramach jednej techniki dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP,
- wykrycie incydentu będącego pochodną zdarzeń z technik występujących w określonej kolejności na wybranym adresie IP lub zasobie identyfikowanym po nazwie.

64. Pojedyncza reguła korelacyjna musi mieć możliwość wzajemnej korelacji wszystkich powyższych mechanizmów umożliwiając, m.in.:

- wykrycie anomalii na koncie uprzywilejowanym użytkownika,
- wykrycie ruchu z serwera domenowego do skompromitowanej domeny wykazanej w liście referencyjnej,
- wykrycie wielu typów anomalii na komputerze z krytyczną podatnością,
- wykrycie złośliwego oprogramowania na bazie wskaźnika kompromitacji stanowiącego HASH procesu, z którego następuje nieautoryzowana próba dostępu do usługi,
- wykrycie wielokrotnych prób nieudanego logowania na konto uprzywilejowane, którego hasło nie spełnia następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny.

65. System przy wykorzystaniu reguł kwalifikacyjnych musi automatycznie selekcjonować zdarzenia wygenerowane przez reguły korelacyjne, wybierając do obsługi tylko zdarzenia spełniające zdefiniowane warunki (tzw. zdarzenia w obsłudze). Pozostałe zdarzenia powinny być wykluczone z obsługi, ale równocześnie pozostać w systemie, zachowując możliwość ich obsługi na żądanie operatora. Zastosowane reguły selekcji zdarzeń do obsługi muszą równocześnie umożliwiać wyliczenie właściwego dla nich priorytetu. Reguły selekcji i priorytetyzacji zdarzeń w obsłudze muszą uwzględniać:

- sparsowane pola oraz ich wartości,
- atrybuty użytkowników z Active Directory,
- atrybuty komputerów z Active Directory,
- informacje z elektronicznej dokumentacji.

66. Zdarzenia w obsłudze, muszą obsługiwać opcje grupowania polegającą na tym, iż każde kolejne zdarzenie wynikające z reguł korelacyjnych, spełniających tą samą regułę w zdefiniowanym okresie czasu będzie automatycznie dodawane do tego samego zdarzenia w obsłudze. Grupowanie musi odbywać się po:

- a. adresie IP,
- b. koncie domenowym użytkownika,
- c. strefie bezpieczeństwa,
- d. zakresie adresów IP.

67. Obsługiwane zdarzenia muszą posiadać zestaw predefiniowanych scenariuszy obsługi (ang. Playbook) oraz pozwalać na tworzenie własnych scenariuszy obsługi oraz ich edycję z poziomu interfejsu graficznego. System musi wspierać funkcję „Drag and Drop” umożliwiającą m.in. na zmianę kolejności realizacji poszczególnych kroków poprzez ich przenoszenie za pomocą myszki komputerowej.

68. System musi potrafić wczytywać informacje z innych systemów bezpieczeństwa i traktować je, jako elementy/dowody dla zdarzeń w obsłudze.

69. Zdarzenia w obsłudze muszą umożliwiać gromadzenie dodatkowych informacji wygenerowanych podczas ich

obsługi oraz umożliwiać do nich dostęp bezpośrednio z poziomu tych zdarzeń, obejmujących m.in.

- a. wszystkie skorelowane zdarzenia,
- b. korespondencja pocztowa,
- c. załączniki z próbkami lub dowodami,
- d. wskaźniki kompromitacji (IoC),
- e. informacje pozyskane z innych systemów.

70. System powinien posiadać możliwość rejestracji zgłoszeń przez stronę webową udostępnianą przez system dla użytkowników z innych jednostek organizacyjnych oraz umożliwić ich przekształcenie w zdarzenia w obsłudze z możliwością rozdzielania uprawnień dla obu tych czynności. System musi umożliwiać scenariusz, gdzie użytkownik zgłasza incydent, który zanim zostanie zakwalifikowany do dalszej obsługi musi zostać autoryzowany przez uprawnionego do tego celu operatora.

71. Dla obsługiwanych zdarzeń system powinien umożliwiać automatyczne pozyskanie informacji z innych systemów oraz bazując na uzyskanej od nich odpowiedzi automatycznie zmieniać ich status, np.: na podstawie pozyskanego wskaźnika kompromitacji (IoC) zmienić status zdarzenia na incydent bezpieczeństwa.

72. Dla zdarzeń w obsłudze dotyczących ruchu sieciowego pomiędzy źródłem a celem transmisji, system musi automatycznie wyznaczyć wektor zagrożenia i zaprezentować go w formie graficznej, na której będą zwizualizowane następujące dane:

- a. identyfikację celu i źródła zagrożenia,
- b. nazwę oraz adres IP źródła zagrożenia,
- c. rodzaj zasobu będący źródłem zagrożenia np.: urządzenie mobilne, stacja robocza,
- d. lokalizację z której pochodzi zagrożenie np.: Internet,
- e. strefę bezpieczeństwa z której pochodzi zagrożenie,
- f. prawdopodobieństwo zagrożenia ze strefy stanowiącej jego źródło,
- g. wszystkie urządzenia sieciowe chroniące cel zagrożenia i zastosowane na nich mechanizmy zabezpieczeń (np.: Application Control, Network Firewall, User Identification),
- h. nazwę oraz adres IP celu zagrożenia,
- i. zabezpieczenia lokalne chroniące cel zagrożenia,
- j. strefę bezpieczeństwa w której znajduje się cel zagrożenia.

73. Dla każdego wektora zagrożenia system musi automatycznie wyliczać efektywność zastosowanych mechanizmów zabezpieczeń, pozwalającą w ramach wbudowanych w system edytowalnych reguł ocenić prawdopodobieństwo materializacji się cyberzagrożeń. Na przykład: dla serwera webowego dostępnego ze strefy Internet zagrożenie przełamania zabezpieczeń ma niskie prawdopodobieństwo w przypadku gdy jest on zabezpieczony przez rozwiązanie klasy WAF (Web Application Firewall).

74. Dla wyznaczonych w czasie obsługi wektorów zagrożeń przedstawiane wyniki szacowania prawdopodobieństwa muszą być zwizualizowane operatorowi w formie listy zagrożeń z oszacowanymi dla nich poziomami. Przykładowe wartości z listy to: wysoki poziom prawdopodobieństwa włamania na serwer oraz średni poziom prawdopodobieństwa infekcji złośliwym oprogramowaniem.

75. Dla zdarzeń w obsłudze zarówno w odniesieniu do adresów źródłowych jak i docelowych system musi umożliwiać operatorowi uzupełnianie pozyskanych informacji, dotyczących zarówno źródła jak i celu zagrożenia w następującym zakresie:

- a. nazwy zasobu,
- b. rodzaju zasobu,
- c. ważności zasobu dla organizacji,
- d. rodzaj przetwarzanych informacji,
- e. usług, które ten zasób świadczy,
- f. lokalizację użytkowników, którzy z niego korzystają,
- g. usługi z których zasób korzysta.

76. System powinien mieć logikę automatycznego przypisywania zdarzeń zakwalifikowanych do obsługi wraz z powiadomieniem operatora, któremu zostało ono przydzielone (min. e-mail, SMS). Kwalifikacja musi uwzględniać m.in. dostępność operatora, jego obciążenia oraz parametry zasobu którego dotyczy zdarzenie, typ zasobu (np.: serwer lub stacja robocza), jego krytyczność oraz realizowane z jego udziałem usługi z katalogu usług. Na przykład: zdarzenie przypisane do krytycznego serwera realizującego usługę DNS powinny trafić do innego operatora niż zdarzenia dotyczące pozostałych serwerów usług sieciowych.

77. Zdarzenia w obsłudze muszą obejmować statusy właściwe dla procesu obsługi zdarzeń, minimum to:

- a. nowe zdarzenie – jako zdarzenie zarejestrowane w systemie,
- b. segregacja – segregacja i kwalifikacja zdarzeń,
- c. incydent bezpieczeństwa – zdarzenie zakwalifikowane jako incydent bezpieczeństwa,
- d. fałszywy alarm – zdarzenie zakwalifikowane jako fałszywy alarm,

e. zdarzenie obsługowane – zdarzenie, które zostało obsługowane w systemie.

System musi także zapewniać możliwość ich edycji w zakresie dodawania (np.: wydzielenie z segregacji statusu kwalifikacji) lub usuwania statusów oraz konfiguracji przejść pomiędzy nimi. Przykładowo: umożliwiać przejście ze statusu „incydent bezpieczeństwa” do statusu „zdarzenie zamknięte”, ale zablokować zmianę ze statusu „incydent bezpieczeństwa” na status „fałszywy alarm”.

78. System powinien umożliwiać definiowanie parametrów SLA dla wszystkich statusów obsługi zdarzeń oraz dokonywać automatycznego pomiaru tych czasów i ich weryfikacji względem zdefiniowanych wartości. Wyniki pomiarów czasów SLA powinny być stale aktualizowane i prezentowane na liście zdarzeń zakwalifikowanych do obsługi.

79. System musi umożliwiać grupowanie manualne dla zdarzeń w obsłudze, których powiązanie zostanie wykryte przez operatorów w trakcie obsługi i umożliwiać zgrupowanie ich do jednego zdarzenia. Zgrupowane zdarzenia muszą być podrzędne w stosunku do zdarzenia z którym są grupowane oraz synchronizować z nim statusy. Dla zdarzeń przetwarzanych przez operatora, zmiana statusu głównego zdarzenia musi wymusić zmianę statusu pozostałych. Na przykład: zamknięcie nadrzędnego zdarzenia musi zamykać też wszystkie podrzędne. Na liście zdarzeń oraz w podglądzie każdego zdarzenia powinna się pojawić informacja o zdarzeniach z nim powiązanych.

80. Obsługiwane zdarzenia muszą zapewniać historyczność, obejmującą wszystkie aktywności realizowane w ramach poszczególnych statusów. Aktywności muszą uwzględniać zarówno akcje realizowane w ramach samego systemu (m.in. zmiana priorytetu czy przekazanie zdarzenia innemu operatorowi). Dodatkowo historia musi też zawierać wszelkie komentarze wpisywane przez operatorów.

81. Dla każdego obsługiwanego zdarzenia system powinien udostępniać automatyczny raport obejmujący wszystkie podjęte działania wraz z komentarzami operatorów.

82. W ramach obsługi zdarzeń system musi automatycznie porównywać wskaźniki kompromitacji zidentyfikowane w bieżącym zdarzeniu względem wszystkich wskaźników pozyskanych do tej pory w ramach dotychczasowej obsługi. Na przykład: jeżeli w obsługiwanej zdarzeniu znajduje się FQDN oraz HASH to system musi automatycznie porównać je ze wszystkimi wskaźnikami typu FQDN oraz HASH, zebranymi do tej pory w obsługiwanych zdarzeniach bez względu na to czy wskaźniki te zostały wpisane ręcznie czy zostały pozyskane automatycznie z innych systemów.

83. System powinien pozwalać, przy użyciu języków skryptowych ogólnie dostępnych (np. Python lub PowerShell), na skonfigurowanie nowych integracji z zewnętrznymi systemami oraz zapewnić dla tych systemów mechanizmy bezpiecznego zarządzania i przechowywania danych związanych z tymi integracjami, m.in. loginy, hasła oraz klucze API.

84. W ramach obsługi zdarzenia dla operatora powinien być dostępny dedykowany panel analityczny pozwalający mu na:

- a. podgląd aktywności zagrożonego zasobu na linii czasu,
- b. w przypadku zagrożenia sieciowego podgląd aktywności zarówno ofiary jak i celu ataku,
- c. w przypadku identyfikacji użytkownika podgląd jego aktywności na linii czasu,
- d. podgląd reguły korelacyjnej, która wygenerowała zdarzenie,
- e. w przypadku wykrytej techniki MITRE ATT&CK® jej szczegółowy opis,
- f. listowanie podpiętych zdarzeń wraz z mechanizmami filtrowania po nich,
- g. gotowe i proste w użyciu filtry rozszerzające analizę zdarzeń o:
 - listę wszystkich zdarzeń pomiędzy celem a źródłem ataku w zadanym okresie czasowym, np.: godzinę przed oraz 2 godziny po,
 - listę wszystkich zdarzeń dotyczących źródła lub celu ataku w zadanym okresie czasowym,
- a. gotowe i proste w użyciu filtry rozszerzające analizę logów o:
 - listę wszystkich logów pomiędzy celem a źródłem ataku w zadanym okresie czasowym,
 - listę wszystkich logów dotyczących źródła lub celu ataku w zadanym okresie czasowym.

85. Dla zdarzeń w obsłudze system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących:

- a. warunki powiadomień,
 - zdarzeń o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi,
 - zdarzeń o przekroczonych czasach SLA o definiowalny okres,
 - zdarzeń ze zbliżającym się i definiowalnym terminem przekroczenia SLA,
 - zdarzeń, których priorytet osiągnął określoną wartość,
 - zdarzeń zakwalifikowanych jako incydent bezpieczeństwa,
 - zdarzeń na których doszło do naruszenia bezpieczeństwa,
 - zdarzeń powstałych poprzez zdefiniowaną regułę korelacyjną,
 - zdarzeń realizujących zdefiniowaną usługę,

- zdarzeń przetwarzających sklasyfikowane informację,
- zdarzeń przetwarzanych na krytycznych zasobach,
- b. odbiorców powiadomień, w tym:
 - operatora, któremu zostało przydzielone zdarzenie,
 - właściciela zasobu na którym wystąpiło zdarzenie,
 - zespół obsługi, który odpowiada za obsługę zdarzeń,
 - właściciela usługi która jest realizowana na zasobie na którym wystąpiło zdarzenie,
 - podmiot zewnętrzny, jeżeli zdarzenie dotyczy zasobu obsługiwanego przez firmę zewnętrzną.
- c. kanały powiadomień, m.in. e-mail, sms, komunikator,
- d. zastosowanie mechanizmów grupowania:
 - grupowanie wielu powiadomień w jednej wiadomości,
 - ograniczenie liczby wierszy powiadomienia do określonej wartości.

86. System powinien posiadać gotowe szablony powiadomień pozwalające na wysyłanie powiadomień jego operatorom w przypadku gdy system przydzieli im zdarzenia do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach:

- a. utworzenia nowego zdarzenia z określonym priorytetem,
- b. utworzenia nowego zdarzenia na zasobie krytycznym,
- c. utworzenia nowego zdarzenia na zasobie realizującym zdefiniowaną usługę,
- d. utworzenie nowego zdarzenia na zasobie przetwarzającym dane osobowe,
- e. utworzenie nowego zdarzenia na podstawie zdefiniowanej reguły korelacyjnej,
- f. modyfikacji przydzielonego operatorowi zdarzenia przez innego operatora,
- g. zamknięcia przydzielonego operatorowi zdarzenia przez innego operatora,
- h. przejęcia przydzielonego operatorowi zdarzenia przez innego operatora.

87. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora umożliwiającego:

- a. wybór raportu, który ma zostać wysłany,
- b. zdefiniowanie jego tytułu,
- c. zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny,
- d. możliwość ograniczenia cyklu do dni powszednich,
- e. określenie daty przesłania pierwszego raportu,
- f. możliwości ograniczenia okresu przez jaki raport będzie przesyłany, do:
 - zdefiniowanej daty końcowej,
 - określonej liczby raportów,
- g. określenie odbiorców raportu.

88. System musi umożliwiać obsługę podatności w ramach scenariuszy obsługi (Playbook).

89. Importowane do systemu podatności muszą być przeanalizowane pod względem ryzyka jakie mogą wygenerować dla organizacji. W tym celu musi być dostępny mechanizm ich automatycznej priorytetyzacji bazujący na regułach, które wyznaczą dla podatności wymagających obsługi priorytet w oparciu o następujące parametry:

- a. strefę bezpieczeństwa w której została wykryta podatność,
- b. prawdopodobieństwo obecności intruza lub złośliwego oprogramowania w tej strefie,
- c. rodzaj zasobu którego dotyczy ta podatność,
- d. ważność tego zasobu dla organizacji,
- e. przetwarzane na tym zasobie informacje, np.: dane osobowe,
- f. usługi realizowane przez ten zasób, np.: DNS,
- g. wartość parametrów CVSS dla podatności, np.: „Confidentiality Impact” = High,
- h. poprawność konfiguracji zasobu na którym została wykryta podatność, np.: brak reguł wymuszenia złożoności haseł,
- i. szacowane prawdopodobieństwo przełamania zabezpieczeń ze zdefiniowanej strefy, która jest autoryzowana do dostępu do tego zasobu, np.: wysokie prawdopodobieństwa zagrożenia ze strefy Internet dla zasobu z wykrytą podatnością, który świadczy usługę w strefie Internet.

90. W systemie musi być dostępny predefiniowany zestaw reguł automatycznej priorytetyzacji wszystkich importowanych podatności oraz interfejs umożliwiający definiowanie własnych reguł umożliwiających zarówno zakwalifikowanie podatności do obsługi jaki i możliwość ich wyłączenia z obsługi w przypadku znikomego zagrożenia dla organizacji.

91. Obsługiwane w systemie podatności muszą być dostępne w formie listy umożliwiającej ich filtrowanie po następujących wartościach:

- a. wyliczonym priorytecie podatności,
- b. aktualnym statusie obsługi,

- c. ważności zasobu na którym została wykryta,
- d. adresie IP tego systemu,
- e. parametrów SLA związanych z tym statusem,
- f. przetwarzanych na zasobach informacji, np.: lista podatności dotycząca tylko systemów przetwarzających dane osobowe,
- g. parametrach CVSS, np.: lista podatności których „Access Complexity (AC)” = „low” oraz „Access Vector (AV)” = „Network”.

92. System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień dla kadry zarządzającej, obejmujących eskalacje oraz monitorowanie SLA. Szablony powinny uwzględniać powiadomienia kierowników jednostek organizacyjnych w następujących sytuacjach:

- a. przekroczenia czasu reakcji o określony czas np.: o godzinę,
- b. możliwości przekroczenia czasu reakcji, np.: została godzina aby rozpocząć obsługę zdarzenia i uchronić się przed przekroczeniem czasu reakcji,
- c. przekroczenia czasu reakcji dla zdarzenia na zasobie przetwarzającym dane osobowe,
- d. przekroczenia czasu reakcji dla zdarzenia na zasobie krytycznym,
- e. przekroczenia czasu reakcji dla zdarzenia na zasobie realizującym krytyczną usługę,
- f. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów przetwarzających dane osobowe,
- g. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów krytycznych,
- h. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów realizujących krytyczną usługę,
- i. przekroczenia czasu reakcji dla podatności na zasobie przetwarzającym dane osobowe,
- j. przekroczenia czasu reakcji dla podatności na zasobie krytycznym,
- k. przekroczenia czasu reakcji dla podatności na zasobie realizującym krytyczną usługę,

93. Dla obsługiwanych podatności system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących:

- a. warunki powiadomień,
 - podatności o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi,
 - podatności o przekroczonych czasach SLA o definiowalny okres,
 - podatności ze zbliżającym się i definiowalnym terminem przekroczenia SLA,
 - podatności, których priorytet osiągnął określoną wartość,
 - zdarzeń realizujących zdefiniowaną usługę,
 - zdarzeń przetwarzających sklasyfikowane informacje,
 - zdarzeń przetwarzanych na krytycznych zasobach,
- b. odbiorców powiadomień, w tym:
 - operatora, któremu została przydzielona podatność,
 - właściciela zasobu na którym wystąpiła podatność,
 - zespół obsługi, który odpowiada za obsługę podatności,
 - właściciela usługi na która jest realizowana na zasobie na którym wystąpiła podatność,
 - podmiot zewnętrzny, jeżeli zdarzenie dotyczy podatności na zasobie obsługiwany przez firmę zewnętrzną.
- c. kanały powiadomień, m.in. e-mail, sms, komunikator,
- d. zastosowanie mechanizmów grupowania:
 - grupowanie wielu powiadomień w jednej wiadomości,
 - ograniczenie liczby wierszy powiadomienia do określonej wartości.

94. System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień jego operatorom w przypadku gdy system przydzieli im podatności do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach:

- a. przydzielenia nowej podatności do obsługi z określonym priorytetem,
- b. przydzielenia nowej podatności do obsługi na zasobie krytycznym,
- c. przydzielenia nowej podatności do obsługi na zasobie realizującym zdefiniowaną usługę,
- d. przydzielenia nowej podatności do obsługi na zasobie przetwarzającym dane osobowe,
- e. modyfikacji przydzielonej operatorowi podatności przez innego operatora,
- f. zamknięcia przydzielonej operatorowi podatności przez innego operatora,
- g. przejęcia przydzielonej operatorowi podatności przez innego operatora.

95. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora pozwalającego na:

- a. wybór raportu który ma zostać wysłany,
- b. zdefiniowanie jego tytułu,
- c. zdefiniowanie cyklu w jakim ma zostać wysłany, np.: tygodniowy lub miesięczny,
- d. możliwość ograniczenia cyklu do dni powszednich,

- e. określenie daty przesłania pierwszego raportu,
- f. określenie okresu przez jaki będą one przysyłane, poprzez:
 - zdefiniowanie daty końcowej,
 - bez daty końcowej,
 - określenie liczby raportów,
- g. określenie odbiorców raportu.

96. System powinien w formie graficznej prezentować podsumowanie aktualnego stanu bezpieczeństwa organizacji w postaci tzw. „Dashboard’u”, tj. dostosowywać zakres i prezentację danych do potrzeb zalogowanego użytkownika.

97. System musi pozwalać na tworzenie dedykowanych dashboard’ów obejmujących:

- a. zestaw wykresów dla bieżącego użytkownika,
- b. zestaw wykresów dla wybranego użytkownika,
- c. zestaw wykresów dla roli zdefiniowanej w systemie, np.: administratorzy systemu,
- d. zestaw wykresów dla wybranego zespołu obsługi, np.: operatorzy SOC (Security Operations Center).

98. System musi zapewniać zestaw predefiniowanych dashboard’ów obejmujących następujące wykresy:

- a. wykres przedstawiający status klasyfikacji zdarzeń, który uwzględnia:
 - ilość zdarzeń nowych i niesklasyfikowanych,
 - ilość zdarzeń sklasyfikowanych jako incydenty bezpieczeństwa,
 - ilość zdarzeń sklasyfikowanych jako fałszywe alarmy,
- b. wykres przedstawiający skalę zagrożeń, który uwzględnia:
 - ilość zasobów krytycznych na których są obsługiwane zdarzenia,
 - ilość zasobów niekrytycznych na których są obsługiwane zdarzenia,
- c. wykres przedstawiający źródła zagrożeń, który uwzględnia:
 - ilość nowych zdarzeń dotyczących użytkowników,
 - ilość podjętych zdarzeń dotyczących użytkowników,
 - ilość nowych zdarzeń dotyczących zasobów,
 - ilość podjętych zdarzeń dotyczących zasobów,
- d. wykres przedstawiający poziom zagrożeń, który uwzględnia:
 - ilość nowych zdarzeń w podziale na priorytety,
 - ilość podjętych zdarzeń w podziale na priorytety,
- e. wykres przedstawiający czas obsługi zagrożeń, który uwzględnia:
 - ilość zdarzeń zarejestrowanych w bieżącym dniu,
 - ilość zdarzeń zarejestrowanych w ostatnim tygodniu,
 - ilość zdarzeń zarejestrowanych w ostatnim miesiącu,
 - ilość zdarzeń zarejestrowanych wcześniej niż w ostatnim miesiącu,
- f. wykres przedstawiający zagrożone usługi, który uwzględnia:
 - ilość usług krytycznych zagrożonych przez obsługiwane zdarzenia,
 - ilość pozostałych usług zagrożonych przez obsługiwane zdarzenia,
- g. wykres przedstawiający zagrożone dane, który uwzględnia:
 - ilość nowych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje,
 - ilość podjętych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje,
 - ilość nowych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje,
 - ilość podjętych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje,
- h. wykres przedstawiający skalę podatności, który uwzględnia:
 - ilość zasobów krytycznych na których są obsługiwane podatności,
 - ilość zasobów niekrytycznych na których są obsługiwane podatności,
- i. wykres przedstawiający czas obsługi podatności, który uwzględnia:
 - ilość podatności zarejestrowanych w bieżącym dniu,
 - ilość podatności zarejestrowanych w ostatnim tygodniu,
 - ilość podatności zarejestrowanych w ostatnim miesiącu,
 - ilość podatności zarejestrowanych wcześniej niż w ostatnim miesiącu,
- j. wykres przedstawiający wagę podatności, który uwzględnia:
 - ilość nowych podatności w podziale na priorytety,
 - ilość podjętych podatności w podziale na priorytety,

99. Nawigacja w ramach „Dashboard’u” musi wspierać opcję typu „Drill down” w następującym zakresie:

- a. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej zdarzeń w obsłudze musi przenieść operatora systemu do listy tych zdarzeń z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
- b. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej podatności musi przenieść operatora systemu do listy tych podatności z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości

- których dotyczy wykres,
- c. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej użytkowników (UBA) musi przenieść operatora systemu do listy tych użytkowników z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
 - d. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej zasobów (EBA) musi przenieść operatora systemu do listy tych zasobów z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
 - e. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej wybranych zdarzeń korelacyjnych musi przenieść operatora systemu do listy prezentującej te zdarzenia z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
 - f. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej wybranych logów musi przenieść operatora systemu do listy prezentującej te logi z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres.

100. Rozwiązanie może być dostarczone w ramach odrębnych rozwiązań, jednakże muszą być one zintegrowane w sposób umożliwiający spełnienie wszystkich wymagań z poziomu jednej konsoli.

101. Rozwiązanie musi zapewniać elastyczną i skalowalną architekturę, której rozbudowa nie będzie wymagała zakupu dodatkowych licencji, zapewniając tym samym możliwość wydzielania następujących warstw funkcjonalnych zwanych dalej kolektorami, do instalacji na osobnych serwerach bądź maszynach wirtualnych:

- a. kolektor parsujący;
- b. kolektor logów;
- c. kolektor korelacyjny;
- d. kolektor zdarzeń;
- e. kolektor sztucznej inteligencji;
- f. kolektor reakcyjny;
- g. kolektor kontrolujący.

102. Kolektor parsujący powinien być odpowiedzialny za odbieranie i parsowanie logów a następnie ich przesyłanie zarówno postaci surowej jak i sparsowanej do odpowiednich kolektorów logów, zgodnie z regułami ich przekierowania zdefiniowanymi w jednym miejscu dla wszystkich kolektorów w interfejsie graficznym. Pojedynczy kolektor parsujący musi zapewniać wydajność co najmniej 20 tysięcy zdarzeń na sekundę w trybie ciągłym oraz posiadać bufor do obsługi natłoku w rozmiarze miliona zdarzeń.

103. Kolektor logów powinien być odpowiedzialny za przechowywanie logów zarówno w postaci surowej jak i sparsowanej oraz przechowywać pliki indeksów. Logi muszą być przechowywane w postaci skompresowanej oraz kolektor musi zapewnić mechanizmy zabezpieczające je przed nieautoryzowaną modyfikacją (np.: Certyfikat cyfrowy czy funkcja skrótu). Pojedynczy kolektor logów powinien mieć wydajność co najmniej 10 tys zdarzeń na sekundę w trybie ciągłym oraz posiadać bufor do obsługi natłoku w rozmiarze miliona zdarzeń.

104. Kolektor korelujący powinien umożliwiać korelację logów oraz ich agregację zgodnie z regułami korelacyjnymi zdefiniowanymi w jednym miejscu dla wszystkich kolektorów w interfejsie graficznym.

105. Kolektor zdarzeń powinien umożliwiać składowanie zdarzeń stanowiących wyniki korelacji oraz umożliwiać ponowne wykorzystanie tych zdarzeń w kolejnych regułach umożliwiając tym korelację zależności pomiędzy nimi. Zdarzenia muszą być przechowywane w postaci skompresowanej oraz kolektor musi zapewnić mechanizmy zabezpieczające je przed nieautoryzowaną modyfikacją (np.: Certyfikat cyfrowy czy funkcja skrótu).

106. Kolektor sztucznej inteligencji powinien zawierać wiedzę pozyskaną ze środowiska obejmującą zarówno linię trendu zachowania użytkowników oraz zasobów obejmujące mechanizmy uczenia maszynowego jak i algorytmy sztucznej inteligencji pozwalające na wypracowanie nowej wiedzy wynikającej z korelacji wyników wiedzy wypracowanej poprzez inne metody.

107. Kolektor reakcyjny musi umożliwiać automatyczną reakcję na wykryte zagrożenia, która nie będzie wymagała żadnej interakcji ze strony użytkownika, chyba że taka będzie dodatkowo zdefiniowana. W celu automatyzacji reakcji musi posiadać funkcjonalność systemu PAM lub być z nim dostarczony w celu przechowywania danych uwierzytelniających oraz kluczy API potrzebnych do automatyzacji reakcji.

108. Architektura rozwiązania musi w pełni wspierać konfigurację niezawodnościową, zapewniającą zarówno pełną redundancję w zakresie, odbierania logów i ich przechowywania, korelacji oraz reakcji na zagrożenia jak i możliwość zastosowania konfiguracji o ograniczonej redundancji do najważniejszych dla zamawiającego źródeł danych.

109. Konfiguracja niezawodnościowa musi wspierać możliwość zastosowania stosu kolektorów zastępczych które zostaną uruchomione w przypadku awarii stosu podstawowego, przy czym wszystkie one muszą być zarządzane centralnie z poziomu tej samej konsoli co kolektory podstawowe.

110. Kolektory muszą mieć zapewnione mechanizmy automatycznej aktualizacji zarówno w zakresie parserów czy reguł korelacyjnych jak i wersji oprogramowania, przy czym aktualizacja musi odbywać się z poziomu centralnego systemu zarządzania.

111. Rozwiązanie musi zapewnić konsole do aktualizacji pozwalającą na wybór dodatkowych pakietów reguł czy parserów udostępnianych w ramach aktywnego wsparcia producenta w formie usługi, każda aktualizacja musi wspierać mechanizm wersjonowania pozwalający zarówno aktualizację jaki i przywracanie poprzednich wersji reguł i parserów.

112. Rozwiązanie musi mieć możliwość skalowania się poprzez dodawanie kolejnych maszyn wirtualnych lub maszyn fizycznych z nowymi typami kolektorów, przy czym dodawanie nowych komponentów nie może wiązać się z koniecznością zakupu nowej licencji, ani posiadać ograniczeń licencyjnych związanych z ilością lub rozmiarem przechowywanych zdarzeń i/lub danych. Jedynym ograniczeniem w tym zakresie (dotyczącym przechowywanych danych) może być rozmiar przestrzeni dyskowej.

113. Skalowanie przez dodawanie nowych kolektorów musi zwiększać wydajność rozwiązania zgodnie z wartościami zadeklarowanymi przez producenta, przykładowo dwa kolektory logów muszą zapewnić dwukrotną wydajność rozwiązania czyli minimum 20 tys zdarzeń na sekundę. Przy czym całe rozwiązanie nie może ograniczać ilość zastosowanych kolektorów.

114. Rozwiązanie nie może posiadać ograniczeń licencyjnych związanych z rozmiarem gromadzonych danych w jednostce czasu. Przykładowo nie może być limitowana licencyjnie ilość bajtów danych w jednostce czasu (KB, GB, etc.)

115. Poszczególne kolektory zdarzeń oraz logów muszą zapewniać przechowywanie danych zarówno na maszynach wirtualnych jak i na dyskach sieciowych.

116. Kolektor logów musi mieć możliwość składowania zbieranych danych zarówno w formie surowej (raw event log) jak i w formie sparsowanych danych (parsed event log)/danych znormalizowanych.

117. Rozwiązanie nie może Przechowywanie logów oraz zdarzeń nie może wykorzystywać klasycznej relacyjnej bazy danych (w tym, choć nie tylko: MS SQL, Postgresql, MySQL, Oracle, itp.) celem gromadzenia i przechowywania danych związanych ze zbieranymi zdarzeniami. Rozwiązanie musi wykorzystywać w tym celu nowoczesną bazę taką jak na przykład noSQL lub OLAP lub autorskie rozwiązanie producenta.

118. Rozwiązanie musi zapewniać możliwość zbudowania większej ilości replik danych, aby zapewnić niezawodność przechowywania oraz możliwość zbudowania struktury rozproszonej, zapewniającej większą wydajność zapisu i wyszukiwania.

119. Klasyczne relacyjne bazy danych mogą być wykorzystywane jedynie do przechowywania szablonów, raportów, konfiguracji, bazy CMDB oraz innych ustrukturyzowanych informacji.

120. Rozwiązanie musi zapewniać możliwość automatycznego budowania kontekstu poprzez wykrywanie urządzeń oraz komputerów mających swoją reprezentację w bazie urządzeń (Configuration Management Database - CMDB).

121. Wymagane jest, aby kolektor odpowiedzialny za parsowanie pozwalał na odrzucanie danych, które uznane są za nieistotne lub niepotrzebne. Mechanizm ten nie może mieć żadnego wpływu na model licencjonowania.

122. Musi istnieć możliwość samodzielnej modyfikacji i poprawiania wszystkich parserów

123. Tworzenie własnych parserów musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI)

124. Tworzenie nowych atrybutów (sparsowanych zmiennych), urządzeń oraz rodzajów zdarzeń (events) musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI).

125. Parsery mają być tworzone z wykorzystaniem narzędzi wspierających dla XML (XML framework) i jednocześnie zapewniać następujące właściwości:

- a. zdolność do definiowania wzorców które powtarzają się jako zmienne;
- b. zdolność do definiowania funkcji pozwalających na identyfikację par wartości kluczowych;
- c. zdolność do testowania poszczególnych funkcji;
- d. zdolność do przekształcania danych w trakcie ich parsowania.

126. Rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Windows (Windows Agent), które

posiadają nie mniej niż następujące możliwości:

- a. centralne zarządzanie i możliwość aktualizacji z głównej konsoli zarządzającej;
- b. możliwość zbierania logów z plików tekstowych na urządzeniach z zainstalowanym systemem z rodziny Windows;
- c. możliwość zbierania logów dotyczących zdarzeń rodzajów innych niż: Security, System, Application;
- d. zdolność do monitorowania integralności plików;
- e. zdolność do monitorowania rejestru systemowego;
- f. zdolność do monitorowania urządzeń zewnętrznych (removable devices);
- g. agent instalowany na systemach z rodziny Windows musi komunikować się z poszczególnymi komponentami rozwiązania SIEM w sposób zaszyfrowany z wykorzystaniem protokołu HTTPS;
- h. musi istnieć możliwość monitorowania stanu agentów w konsoli zarządzającej systemu;
- i. musi istnieć możliwość przygotowania różnych zestawów konfiguracji agenta, a następnie przypisywania ich niezależnie do dowolnej ilości (jeden lub więcej) systemów źródłowych. Np. inne konfiguracje dla kontrolerów domeny, a inne dla serwerów DNS;
- j. musi umożliwiać automatyzację reakcji na zagrożenie, jak blokowanie zdefiniowanego ruchu sieciowego czy blokada procesu.

127. System musi mieć możliwość realizacji funkcjonalności UEBA (User Entity Behaviour Analysis) zarówno w oparciu o dedykowanego Agenta na systemy Windows oraz w oparciu o logi z systemu Windows. Metadane lub logi dotyczące funkcji UEBA nie mogą podlegać licencjonowaniu ze względu na EPS lub rozmiar.

128. Rozwiązanie musi zapewniać wsparcie dla zarządzania w oparciu o role (Role Based Administration) celem ograniczania dostępu do danych oraz do GUI

129. System musi być zintegrowany z zewnętrznymi bazami o zagrożeniach (Threat Intelligence Feeds - TI) oraz zawierać już zintegrowany zestaw niekomercyjnych (open source) lub komercyjnych baz zagrożeń.

130. Rozwiązanie musi mieć możliwość korelacji informacji z baz zagrożeń z danymi otrzymywanymi w czasie rzeczywistym. Korelacja ta ma odbywać się w pamięci systemu względem otrzymywanych danych o zdarzeniach (event data).

131. System musi mieć możliwość korelacji informacji z baz zagrożeń z danymi historycznymi

132. System musi mieć możliwość odpytywania (ręcznego lub automatycznego) zewnętrznych źródeł reputacji takich jak np. VirusTotal.

133. System musi mieć możliwość wizualizacji informacji w oparciu o kategorie MITRE ATT&CK dla standardowego zbioru wbudowanych reguł.

134. Pulpity administracyjne (dashboards) muszą mieć możliwość wspólnej prezentacji.

135. Rozwiązanie musi mieć możliwość integracji z innymi systemami do obsługi zgłoszeń poprzez API (ticketing system) oraz mieć wbudowany mechanizm obsługi zgłoszeń (ticketing system) niezależny od obsługi alarmów/incydentów.

136. System musi wspierać mechanizmy typu Machine Learning w oparciu o zgromadzone zdarzenia. Musi być możliwe użycie przynajmniej 4 różnych rodzajów mechanizmów Machine Learning wraz z możliwością ich ręcznego wybrania oraz działania w trybie automatycznym. W wyniku działania opisanych mechanizmów Machine Learning system SIEM ma tworzyć model bazowy zachowania oraz umożliwiać wykrycie odchyleń i anomalii od niego. Zadania Machine Learning mają mieć możliwość dystrybuowania ich pomiędzy elementy warstwy korelującej i/lub zarządzającej. Mechanizmy Machine Learning mają również umożliwiać wsparcie dla podejmowania decyzji przy rozwiązywaniu incydentów w systemie SIEM.

137. Dostarczone rozwiązanie nie może działać w oparciu o oprogramowanie otwarte (ang: open source) w następującym zakresie funkcjonalnym: składowanie, parsowanie, korelacja logów, algorytmy uczenia maszynowego, analiza zachowania użytkowników i zasobów, mechanizmy reakcji/ scenariusze reakcji. Zamawiający nie akceptuje systemu, który wykorzystuje mechanizmy typu open source np.: Elastic Search, OSSIM, Snort, The Hive, AlienVault itd. lub został stworzony przez modyfikację oprogramowania otwartego.

138. W celach weryfikacji zgodności produktu z wymaganiami, musi być on dodatkowo oferowany przez autoryzowanego dystrybutora, dostarczającego produkty z obszaru cyberbezpieczeństwa na rynku polskim, który w przypadku jakichkolwiek wątpliwości Zamawiającego, związanych z wymaganymi funkcjonalnościami będzie mógł je potwierdzić lub im zaprzeczyć.

139. W związku z tym, że obsługa systemu ma objąć także użytkowników nieposługujących się biegle językiem angielskim, interfejs użytkownika musi umożliwiać obsługę w języku polskim lub posiadać możliwość wgrania

plików językowych tłumaczących interfejs na język polski. Pliki tłumaczące interfejs na język polski muszą zostać wgrane w trakcie wdrożenia systemu, przed jego zakończeniem.

140. Zamawiający na obecnym etapie nie jest w stanie zmierzyć ilości danych przekazywanych do systemu, tj. EPS (Events Per Second) oraz nie zna wymagań związanych z architekturą proponowanego rozwiązania, dlatego oferowana licencja nie może nakładać limitów w tym zakresie.

141. Produkt musi umożliwiać równoczesną pracę co najmniej 10 operatorów oraz obsługiwać 250 źródeł logów dotyczących wszystkich zdarzeń związanych z komputerami oraz serwerami wykorzystywanymi w organizacji oraz zapewnić dla tych źródeł detekcję i obsługę cyberzagrożeń w ramach wszystkich oferowanych w tym postępowaniu funkcjonalności.

142. System ma gwarantować możliwość elastycznej rozbudowy o kolejne źródła logów.

143. Funkcjonowanie rozwiązania musi umożliwiać konfigurację „on-premise”, w której wszystkie funkcjonalności oraz przetwarzanie danych będzie się odbywać całkowicie w infrastrukturze zamawiającego, zapewniając tym samym możliwość konfiguracji systemu w strefie odseparowanej od sieci Internet.

144. System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows (minimum Server 2016), Redhat/Oracle Linux (minimum 7.x).

145. Dostarczone rozwiązanie musi być objęte min. 12 miesięcznym wsparciem producenta (wsparcie producenta zgodne będzie z deklaracją Wykonawcy w ofercie – kryterium oceny ofert) . Wsparcie musi obejmować bezpłatne dostarczanie aktualizacji oprogramowania, reagowanie na zgłaszane błędy systemowe oraz usługę konsultacji powdrożeniowej w formie spotkań z dedykowanym inżynierem, certyfikowanym z procesu konfiguracji i obsługi oferowanego systemu. Przez błąd systemowy Zamawiający rozumie błędy krytyczne (zakłócenie uniemożliwiające działanie rozwiązania), błędy poważne (zakłócenie uniemożliwiające działanie części rozwiązania), błędy zwykłe (inne zakłócenia nie stanowiące błędów krytycznych lub poważnych).

146. Wykonawca musi zapewnić usługę obejmującą proces aktualizacji oprogramowania oraz kontekstu systemu (dotyczy to zwłaszcza bazy reguł korelacyjnych, bazy parserów, bazy dostępnych aktualizacji). Dostęp do centralnej usługi aktualizacyjnej ma pozwalać na automatycznie wyświetlanie i pobieranie z poziomu interfejsu systemu dostępnych aktualizacji. Dla pobranych w procesie aktualizacji reguł oraz parserów musi być dostępne wersjonowanie, pozwalające uruchomić nową wersję reguły korelacyjnej oraz parsera z poziomu interfejsu systemu. Automatyczne wersjonowanie ma umożliwiać wczytanie starszej wersji reguły lub parsera, a zmiana reguł i parserów musi być możliwa z poziomu graficznego systemu.

147. Wykonawca zapewni bezpłatne szkolenia w zakresie użytkowania i administrowania wdrożonego systemu lub systemów. Szkolenie ma zostać przeprowadzone dla maksymalnie 6 osób i muszą być zakończone przyznaniem certyfikatu, potwierdzającego wspomniane umiejętności wydany przez producenta systemu/systemów. Szkolenia mogą odbyć się w formie zdalnej.

148. Zamawiający wymaga by wraz ofertą Wykonawca dostarczył próbkę systemu (np. w postaci przekierowania do wersji demonstracyjnej systemu) z odpowiednią dokumentacją (np. w postaci karty produktu oraz niezbędnych instrukcji). Zamawiający maksymalnie w ciągu dwóch dni roboczych, zweryfikuje zgodność oferowanego systemu na podstawie próbki systemu i dostarczonej dokumentacji, porównując je ze wszystkimi wymaganiami określonymi w powyższych punktach OPZ. W przypadku gdy Zamawiający uzna niezgodność próbki i dokumentacji z wymaganiami OPZ, lub gdy Zamawiający nie odnajdzie określonego wymagania w próbce systemu i dokumentacji, oferta Wykonawcy zostanie odrzucona. W przypadku gdy Wykonawca nie dołączy do oferty próbki systemu wraz z dokumentacją, oferta zostanie odrzucona.



149. Wykonawca jest zobowiązany do wykazania w treści oferty, że oferowane oprogramowanie spełnia wymagane przez Zamawiającego parametry, tj. Wykonawca musi wraz z ofertą (tj. do terminu składania ofert) wypełnić tabelę w formularzu oferty (tabela spełnia/ nie spełnia) oraz złożyć próbki oferowanego oprogramowania (nieodpłatnie, w celu weryfikacji wymaganych przez Zamawiającego parametrów technicznych), pozwalające na ocenę spełniania wymogów wskazanych przez Zamawiającego. Próbką systemu zostanie dostarczona w postaci obrazu maszyny wirtualnej VMware na nośniku zewnętrznym np.: pendrive, dysk zewnętrzny. Na próbkę składają się: nośnik zewnętrzny, hasła (jeżeli są konieczne do uruchomienia próbki demonstracyjnej) oraz instrukcje uruchomienia środowiska umożliwiające samodzielne uruchomienie systemu. Jeżeli złożona próbka jest niekompletna, Zamawiający wezwie do jej uzupełnienia.

Próbka oferowanego oprogramowania powinna być dostarczona w formie demonstracyjnej aby umożliwić weryfikację przez Zamawiającego 10 wymagań określonych w tabeli wymagań załączonej do OPZ. Oprogramowanie musi być skonfigurowane w sposób umożliwiający jego weryfikację z wskazanymi powyżej wymaganiami OPZ. W ramach dostępu do rozwiązania, Wykonawca musi przygotować odpowiednią instrukcję w języku polskim opisującą czynności realizowane w celu uzyskania pożądanego stanu (mogą to być opracowane

dokumenty zawierające zrzuty z ekranu wraz ze szczegółowymi opisami każdego z pól lub/i czynnościami (krok po kroku) jakie należy zrealizować aby osiągnąć opisany efekt/stan). Instrukcja i hasło mogą być dostarczona wraz z próbką demonstracyjną lub wraz z ofertą.

W przypadku gdy Zamawiający na podstawie analizy próbki uzna system za niezgodny z wymaganiami OPZ lub gdy Zamawiający nie będzie miał możliwości zweryfikowania określonego wymagania na podstawie przekazanej próbki systemu, oferta Wykonawcy zostanie odrzucona. W przypadku gdy Wykonawca nie dołączy do oferty próbki systemu, zostanie wezwany do jej złożenia.

Próbki oceniane będą pod względem spełniania wymogów wskazanych poniżej.

Tabela wymagań		
I.p	Poz. z OPZ	Opis parametrów technicznych
1	27	System musi umożliwiać generowanie elektronicznej dokumentacji sieci i systemów w sposób automatyczny na podstawie dostarczonych przez producenta reguł wykrywania oraz edytora graficznego pozwalającego utworzyć dodatkowe reguły.
2	47	System musi posiadać zestaw predefiniowanych i konfigurowalnych reguł do automatycznego przyporządkowania użytkowników i zasobów do właściwych profili nauczania, reguły te muszą zapewnić minimum: a. rozdzielenie procesu nauczania zachowania użytkowników uprzywilejowanych od użytkowników nieuprzywilejowanych, b. rozdzielenie procesu nauczania zachowania stacji roboczych od serwerów, c. rozdzielenie serwerów świadczących usługi w sieci Internet od serwerów świadczących usługi lokalnie w organizacji, d. rozdzielenie procesu nauczania serwerów należących do domeny od pozostałych serwerów.
3	49	System musi pozwalać na zautomatyzowaną ocenę wpływu incydentu bezpieczeństwa IT na działalność organizacji względem zagrożeń natury informatycznej (np: utrata wizerunku, związana z zagrożeniem przełamania zabezpieczeń serwera webowego organizacji dostępnego z sieci Internet).
4	72	Dla zdarzeń w obsłudze dotyczących ruchu sieciowego pomiędzy źródłem a celem transmisji, system musi automatycznie wyznaczyć wektor zagrożenia i zaprezentować go w formie graficznej, na której będą zwizualizowane następujące dane: a. identyfikację celu i źródła zagrożenia, b. nazwę oraz adres IP źródła zagrożenia, c. rodzaj zasobu będący źródłem zagrożenia np.: urządzenie mobilne, stacja robocza, d. lokalizację z której pochodzi zagrożenie np.: Internet, e. strefę bezpieczeństwa z której pochodzi zagrożenie, f. prawdopodobieństwo zagrożenia ze strefy stanowiącej jego źródło, g. wszystkie urządzenia sieciowe chroniące cel zagrożenia i zastosowane na nich mechanizmy zabezpieczeń (np.: Application Control, Network Firewall, User Identification), h. nazwę oraz adres IP celu zagrożenia, i. zabezpieczenia lokalne chroniące cel zagrożenia, j. strefę bezpieczeństwa w której znajduje się cel zagrożenia.
5	73	Dla każdego wektora zagrożenia system musi automatycznie wyliczać efektywność zastosowanych mechanizmów zabezpieczeń, pozwalającą w ramach wbudowanych w system edytowalnych reguł ocenić prawdopodobieństwo materializacji się cyberzagrożeń. Na przykład: dla serwera webowego dostępnego ze strefy Internet zagrożenie przełamania zabezpieczeń ma niskie prawdopodobieństwo w przypadku gdy jest on zabezpieczony przez rozwiązanie klasy WAF (Web Application Firewall).
6	74	Dla wyznaczonych w czasie obsługi wektorów zagrożeń przedstawiane wyniki szacowania prawdopodobieństwa muszą być zwizualizowane operatorowi w formie listy zagrożeń z oszacowanymi dla nich poziomami. Przykładowe wartości z listy to: wysoki poziom prawdopodobieństwa włamania na serwer oraz średni poziom prawdopodobieństwa infekcji złośliwym oprogramowaniem.
7	84	W ramach obsługi zdarzenia dla operatora powinien być dostępny dedykowany panel analityczny pozwalający mu na: a. podgląd aktywności zagrożonego zasobu na linii czasu, b. w przypadku zagrożenia sieciowego podgląd aktywności zarówno ofiary jak i celu ataku, c. w przypadku identyfikacji użytkownika podgląd jego aktywności na linii czasu, d. podgląd reguły korelacyjnej, która wygenerowała zdarzenie, e. w przypadku wykrytej techniki MITRE ATT&CK® jej szczegółowy opis,

		f. listowanie podpiętych zdarzeń wraz z mechanizmami filtrowania po nich, g. gotowe i proste w użyciu filtry rozszerzające analizę zdarzeń o: - listę wszystkich zdarzeń pomiędzy celem a źródłem ataku w zadanym okresie czasowym, np.: godzinę przed oraz 2 godziny po, - listę wszystkich zdarzeń dotyczących źródła lub celu ataku w zadanym okresie czasowym, a. gotowe i proste w użyciu filtry rozszerzające analizę logów o: - listę wszystkich logów pomiędzy celem a źródłem ataku w zadanym okresie czasowym, - listę wszystkich logów dotyczących źródła lub celu ataku w zadanym okresie czasowym.
8	85	Dla zdarzeń w obsłudze system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących: a. warunki powiadomień, - zdarzeń o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi, - zdarzeń o przekroczonych czasach SLA o definiowalny okres, - zdarzeń ze zbliżającym się i definiowalnym terminem przekroczenia SLA, - zdarzeń, których priorytet osiągnął określoną wartość, - zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, - zdarzeń na których doszło do naruszenia bezpieczeństwa, - zdarzeń powstałych poprzez zdefiniowaną regułę korelacyjną, - zdarzeń realizujących zdefiniowaną usługę, - zdarzeń przetwarzających sklasyfikowane informacje, - zdarzeń przetwarzanych na krytycznych zasobach, b. odbiorców powiadomień, w tym: - operatora, któremu zostało przydzielone zdarzenie, - właściciela zasobu na którym wystąpiło zdarzenie, - zespół obsługi, który odpowiada za obsługę zdarzeń, - właściciela usługi która jest realizowana na zasobie na którym wystąpiło zdarzenie, - podmiot zewnętrzny, jeżeli zdarzenie dotyczy zasobu obsługiwanego przez firmę zewnętrzną. c. kanały powiadomień, m.in. e-mail, sms, komunikator, d. zastosowanie mechanizmów grupowania: - grupowanie wielu powiadomień w jednej wiadomości, - ograniczenie liczby wierszy powiadomienia do określonej wartości.
9	90	W systemie musi być dostępny predefiniowany zestaw reguł automatycznej priorytetyzacji wszystkich importowanych podatności oraz interfejs umożliwiający definiowanie własnych reguł umożliwiających zarówno zakwalifikowanie podatności do obsługi jak i możliwość ich wyłączenia z obsługi w przypadku znikomego zagrożenia dla organizacji.
10	111	Rozwiązanie musi zapewnić konsolę do aktualizacji pozwalającą na wybór dodatkowych pakietów reguł czy parserów udostępnianych w ramach aktywnego wsparcia producenta w formie usługi, każda aktualizacja musi wspierać mechanizm wersjonowania pozwalający zarówno aktualizację jak i przywracanie poprzednich wersji reguł i parserów.