Załącznik nr 2: Opis przedmiotu zamówienia

Znak sprawy: ZP/220/82/22

Przedmiotem zamówienia jest rozwiązanie do identyfikacji i zarządzania podatnościami oraz system typu SIEM (Security Information and Event Management) (zwane dalej „Rozwiązaniami" lub „Systemami"). Zamówienie będzie zrealizowane poprzez dostawę niezbędnych licencji, oprogramowania, pakietów suportowych, wdrożenie oraz świadczenie serwisu dla wdrożonych Rozwiązań.

1. W szczególności przedmiot zamówienia obejmuje:

1.1. Dostawę Rozwiązań wraz z licencjami oraz aktualizacjami, w tym:

1.1.1. Odpowiednich licencji niezbędnych do prawidłowego funkcjonowania Systemu zarządzania podatnościami dla 600 instancji. Możliwe będzie dokupienie dodatkowych licencji w paczkach.

1.1.2. Odpowiednich licencji niezbędnych do prawidłowego funkcjonowania Systemu SIEM dla 600 instancji.

1.1.3. Najnowszej dostępnej wersji oprogramowania oferowanego Rozwiązań.

1.1.4. Niezbędnych pakietów suportowych producenta na okres 24 miesięcy.

1.1.5. Model licencjonowania produktu powinien być modelem subskrypcyjnym. Licencjonowanie powinno odbywać się na podstawie liczby skanowanych instancji (dla system zarządzania podatnościami) oraz liczby podłączonych instancji i ilości przesyłanych danych (dla systemu SIEM).

1.2. Świadczenie serwisu i wsparcia technicznego dla wdrożonego Rozwiązania w okresie 24 miesięcy od daty podpisania Protokołu odbioru końcowego.

1.3. Wdrożenie wymienionych systemów, w zakresie:

1.3.1. Utworzenie dedykowanego konta w systemach i aktywacja licencji

1.3.2. Instalacja konsoli zarządzania z silnikiem skanującym Systemu zarządzania podatnościami.

1.3.3. Podłączenie konsoli zarządzania Systemu zarządzania podatnościami do niezbędnych elementów chmurowych Systemu.

1.3.4. Instruktaż stanowiskowy prezentujący instalację dedykowanego oprogramowania dla jednostek końcowych na wybranych stacjach oraz podłączenie wybranych urządzeń sieciowych do Systemu SIEM (5 komputerów, 2 serwery LINUX, 2 serwery WINDOWS, 2

macierze dyskowe Netapp, 2x switche Extreme, 2x UTM Sophos) – Zamawiający skonfiguruje export logów z wymienionych narzędzi do Systemu.

1.3.5. Instalacja komponentów np. zbierających dane i wykonujących akcje automatyczne współpracujących z Systemami.

1.3.6. Szkolenie stanowiskowe z Systemów.

1.4. Systemy będące przedmiotem zamówienia powinny pochodzić od tego samego producenta.

2. Specyfikacja rozwiązania – System zarządzania podatnościami

2.1. Architektura rozwiązania

2.1.1. Architektura Klient (silniki skanujące) / Serwer zarządzania (magazyn danych, serwer raportowania). Licencja powinna przewidywać możliwość uruchomienia minimum 3 serwerów zarządzających.

2.1.2. Zarządzanie Systemem musi się odbywać przy pomocy przeglądarki, nie dopuszcza się zarządzania za pomocą dodatkowo instalowanej aplikacji na komputerze administratora. Wspierane przeglądarki:

- Google Chrome (latest)
- Mozilla Firefox (latest)
- Mozilla Firefox ESR (latest)
- Microsoft Edge

2.1.3. Rozwiązanie (zarówno silnik jak i serwer zarządzania) powinno dawać możliwość wdrożenia, jako maszyna wirtualna.

2.1.4. Rozwiązanie (silniki skanujące i serwer zarządzania) powinno być możliwe do uruchomienia w architekturze on-premise Zamawiającego. Dopuszcza się możliwości wykorzystania niektórych funkcjonalności z użyciem chmurowej platformy.

2.1.5. Skanowanie może być wykonywane z poziomu serwera oraz dowolnego silnika skanującego. Rozwiązanie powinno umożliwiać instalację wielu silników skanujących (architektura rozproszona) w ramach dostarczonych licencji. Liczba możliwych do uruchomienia silników skanujących nie powinna być ograniczona licencyjnie.

2.1.6. Rozwiązanie powinno posiadać możliwość wykonania skanowania z zewnętrznego, internetowego/chmurowego silnika skanującego utrzymywanego przez producenta.

2.1.7. Rozwiązanie powinno dawać możliwość instalacji na platformach min.:

- Ubuntu Linux 20.04 LTS
- Ubuntu Linux 18.04 LTS
- Ubuntu Linux 16.04 LTS

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows 8.1
- Red Hat Enterprise Linux Server 8
- Red Hat Enterprise Linux Server 7
- Red Hat Enterprise Linux Server 6
- CentOS 7
- Oracle Linux 8
- Oracle Linux 7
- SUSE Linux Enterprise Server 12

2.1.8. Serwer zarządzania powinien przechowywać wszystkie dane pochodzące z dowolnego, podpiętego silnika skanującego.

2.2. Administracja

2.2.1. Serwer zarządzania powinien udostępniać możliwość tworzenia wielu użytkowników o różnych poziomach dostępu i konfiguracji obiektów. Administrator powinien móc ograniczyć określonym użytkownikom dostęp do np. skanowania i jego wyników dla danych zasobów.

2.2.2. Narzędzie powinno umożliwić ograniczenie możliwości skanowania do określonych instancji/logicznych grup instancji dla danych użytkowników.

2.2.3. Rozwiązanie powinno dawać możliwości zewnętrznego uwierzytelniania co najmniej w narzędziach:

- Microsoft Active Directory
- Kerberos
- SAML 2.0

2.2.4. Rozwiązanie powinno dawać możliwość uwierzytelniania dwuskładnikowego dla użytkowników.

2.2.5. Przekazywanie danych z silników skanujących do serwera zarządzania powinno odbywać się bezpiecznym kanałem szyfrowanym.

2.2.6. Rozwiązanie powinno umożliwiać wykonanie skanów w sposób automatyczny wg zaplanowanego harmonogramu lub w reakcji na skutek określonych sytuacji, np. wykrycia, że dany asset jest online lub nowych podatności, które mogą wpływać na środowisko. Powinna być też możliwość zapewnienia w harmonogramie okresów, kiedy żaden skan nie może być wykonany (tzw. „blackout”).

2.2.7. Rozwiązanie powinno umożliwiać automatyczne wykonywanie kopii zapasowych według harmonogramu.

2.2.8. Rozwiązanie powinno mieć możliwość powiadamiania i alertowania administratora o wybranych zdarzeniach poprzez STMP e-mail, Syslog, SNMP.

2.2.9. System musi umożliwiać automatyczną aktualizację Rozwiązania oraz jego danych (np. sygnatur podatności) z zasobów producenta oraz ręczną aktualizację w tym zakresie w trybie offline.

2.3. Funkcjonalności

2.3.1. Skan podatności powinien być możliwy do wykonania z uwierzytelnieniem do systemu skanowanego i bez uwierzytelnienia.

2.3.2. Metody uwierzytelnienia do systemu wspierane przez rozwiązanie to co najmniej:

- Concurrent Versioning System (CVS)
- File Transfer Protocol (FTP)
- Web Site http Authentication
- IBM AS/400
- Lotus Notes/Domino
- Microsoft SQL Server
- Sybase SQL Server
- Microsoft Windows/Samba (SMB/CIFS)
- Microsoft Windows/Samba LM/NTLM Hash (SMB/CIFS)
- Oracle
- Oracle Service Name
- Post Office Protocol (POP)
- PostgreSQL
- Remote Excecution
- Simple Network Management Protocol v1/v2c
- Simple Network Management Protocol v3
- Secure shell (SSH)
- Secure shell (SSH) Public Keys
- Telnet
- MySQL Server
- DB2
- Kerberos
- SAP HANA

2.3.3. Rozwiązanie powinno mieć możliwość wykonania audytu konfiguracji wybranych urządzeń w odniesieniu do zgodności z uznanymi standardami – co najmniej ze standardem CIS. Skaner konfiguracji powinien być standardową częścią systemu.

2.3.4. System powinien mieć możliwość współdzielenia poświadczeń do skanowanych stacji pomiędzy różnymi definicjami/zakresami skanowania.

2.3.5. System powinien umożliwiać statyczne oraz dynamiczne (automatycznie zmienny zakres) definiowanie zakresu skanowanych instancji. Dynamiczne definiowane może odbywać się za pomocą logicznych grup instancji przypisanych do zakresu skanowania, bazujących na cechach charakterystycznych dla systemu i na tej podstawie umożliwiających kategoryzację.

2.3.6. System powinien umożliwiać skany wykonujące rekonesans: rozpoznające czy instancja jest aktywna, jakie ma dostępne usługi, określająca wersję i typ systemu i inne podobne szczegóły.

2.3.7. Wykryte podatności powinny w formie pozwalającej na szybkie odniesienie do otwartych baz podatności, takich jak: NVD, Bugtraq, MSFT, CERT, SANS.

2.3.8. System powinien mieć możliwość sugerowania rozwiązań (remediacji) wykrytych podatności. System powinien podawać je w sposób inteligentny, wskazując jak najmniejszą ilość poprawek niezbędnych do zainstalowania, w celu załatania podatności. System powinien umożliwiać śledzenie postępu prac remediacyjnych oraz ustalenie terminu zakończenia prac (deadline).

2.3.9. Baza podatności wykrywanych przez Rozwiązanie powinna być aktualizowana przez producenta.

2.3.10. System powinien umożliwiać tworzenie własnych wzorców sygnatur podatności przez użytkownika.

2.3.11. Zakres skanowania powinien być oparty o wzorce predefiniowane lub utworzone przez użytkownika. Każdy wzorzec powinien mieć możliwość definicji co najmniej:

- Metody (np. SYN, SYN-RST scan) i zakresu portów warstwy transportowej w skanie
- Kategorii podatności (np. wszystkie podatności dla konkretnego OS), które mają zostać sprawdzone
- Typu podatności (np. bezpieczne z punktu widzenia ciągłości działania skanowanej instancji lub nie), które mają zostać sprawdzone
- Indywidualnie sprawdzenia pojedynczych podatności (np. w oparciu o CVE-ID)

2.3.12. Podczas skanowania typu „discovery” użytkownik powinien mieć możliwość definiowania parametrów wydajnościowych skanu (np. limit „packets-per-second rate”).

2.3.13. Rozwiązanie powinno mieć możliwość dynamicznego wykrywania instancji bez konieczności wykonywania skanowania („Dynamic Discovery”). Opcja ta powinna być dostępna co najmniej dla:

- AWS Instances
- Microsoft Azure Instances
- VMWare vCenter/ESX/ESXi Instances
- Instancji wykrywanych przez DHCP log queries
- Instancji wykrywanych przez Active Directory

2.3.14. Możliwość śledzenia zmian ryzyka związanego z konkretnym hostem. Powiązanie ryzyka z hostem powinno odbywać się, co najmniej na podstawie:

- Adresu IP.
- Adresu MAC.
- Nazwy hosta (hostname).

2.3.15. Rozwiązanie powinno umożliwiać śledzenie sumarycznego poziomu ryzyka (określanego na podstawie wykrytych podatności) dla organizacji, logicznych grup lub instancji i prezentować je na wykresie w odniesieniu do czasu.

2.3.16. Kontrola baz danych powinna być standardową częścią Rozwiązania. Wspierane bazy danych to, co najmniej: MSSQL, Oracle, DB2, PostgreSQL, MySQL.

2.3.17. Rozwiązanie powinno umożliwiać podstawowe skanowanie aplikacji webowych, w zakresie potencjalnych problemów z kategorii SQL Injection, CSS/XSS, backup script files, odczytywalne CGI Scripts etc.

2.3.18. Raportowanie musi być niezależne od wykonującego skanowanie silnika (raporty muszą umożliwiać konsolidację wszystkich wyników).

2.3.19. Raporty powinny mieć możliwość generowania przy użyciu:

- Przygotowanych przez producenta wzorców.
- Modyfikowanych przez użytkownika standardowych wzorców.

2.3.20. Użytkownik powinien mieć możliwość wykonania dowolnego zapytania SQL do bazy danych serwera zarządzania. Wynik takiego zapytania powinien być prezentowany, jako raport w formacie CSV.

2.3.21. Raporty powinny mieć możliwość automatycznego generowania według harmonogramu.

2.3.22. Moduł raportujący powinien mieć możliwość automatycznego przesyłania raportów do dedykowanych użytkowników.

2.3.23. Raporty powinno dać się generować do następujących formatów (formaty wyjściowe mogą się różnić w zależności od typu raportu): PDF, , XML, CSV.

2.3.24. System powinien zapewniać wzorce wykresów dostępnych w przygotowanej dla użytkownika bazie w celu przeglądania informacji statystycznych. Wykresy powinny być dostępne w ramach samej platformy, a nie jako osobne narzędzie.

2.3.25. Ocena ryzyka powinna być możliwa w oparciu o:

- CVSS
- CVSSv3
- Dedykowany, dynamiczny „Risk Score".

2.3.26. Użytkownik Rozwiązania powinien mieć możliwość wyboru strategii obliczania wskaźnika ryzyka oraz jego granularność. System powinien zapewniać możliwość obliczenia wskaźnika w oparciu o metryki CVSSv2, uwzględniając:

- Wpływ podatności na poufność, integralność i dostępność danych.
- Wektor dostępu, Złożoność dostępu, Wymóg uwierzytelniania
- Wiek podatności, ekspozycję na exploit, narażenie na złośliwe oprogramowanie

Dodatkowo Rozwiązanie może uwzględniać w wyliczeniach wskaźnika wytyczne standardu PCI-DSS v 2.0 *(PCI ASV 2.0)* lub stosować algorytmy nie określające górnego limitu wskaźnika podatności (większa granularność). – *(TemporalPlus strategy)*

2.3.27. Rozwiązanie powinno dawać możliwość uwzględniania w obliczaniu wskaźnika ryzyka dla danej instancji lub grupy także kontekst biznesowy związany z czynnikami zewnętrznymi (np. krytyczność aplikacji). Odpowiednio poziom „Risk Score" dla instancji krytycznej powinien być wyższy niż instancji mniej istotnej z punku widzenia biznesu przy tych samych podatnościach wykrytych na instancji.

2.3.28. Rozwiązanie powinno umożliwiać dodawanie znaczników („tag'ów") do instancji/grup związanych z np. krytycznością, lokalizacją, opisem.

2.3.29. Rozwiązanie powinno samo informować o gotowych modułach exploitacji danej podatności dostępnych w Internecie oraz sugerować akcje naprawcze, np. wskazywać poprawki dla systemu operacyjnego, które łatają wskazane podatności. Powinno także prezentować linki do pobrania aktualizacji/patch'y.

2.3.30. Rozwiązanie powinno wspierać skanowanie obrazów kontenerów.

2.3.31. Rozwiązanie powinno umożliwiać analizę konfiguracji wybranych zasobów chmurowych pod kątem zgodności ze standardem CIS.

2.3.32. System musi dawać możliwość dodawania wyjątków z listy podatności.

2.3.33. System musi dawać możliwość przeszukania wyników w oparciu o:

- CVE-ID
- CVSS Score
- CVSSv3 Score
- Poziom ryzyka
- Vulnerability Category
- Vulnerability Title

2.4. Integracje

2.4.1. Rozwiązanie musi integrować się z systemem umożliwiającym wykonywanie testów penetracyjnych. Integracja powinna zakładać automatyczne wykorzystywanie przez system penetracyjny podatności wykrytych przez Rozwiązanie, z uwzględnieniem gotowych modułów exploitacji. Także skanowanie powinno być możliwe na skutek wyzwolenia go, przez wspomniane narzędzie pentestingowe. (np. Metasploit PRO)

2.4.2. Rozwiązanie musi zapewniać dwukierunkowy interfejs API. Korzystanie z interfejsu API nie powinno wymagać dodatkowych licencji.

2.4.3. Rozwiązanie powinno mieć możliwość integracji z systemem CI/CD, np. Jenkins.

3. Specyfikacja rozwiązania – System klasy SIEM

3.1. Architektura rozwiązania

3.1.1. Konsola systemu musi być dostarczona w postaci SaaS z funkcjonalnością multi-tenant.

3.1.2. System musi mieć możliwość zbierania danych z środowisk chmurowych oraz on-premise.

3.1.3. System musi wspierać możliwość zbierania danych z co najmniej wymienionych poniżej technologii:

- Active Directory
- LDAP
- Firewall
- Antivirus
- IDS/IPS
- DHCP

- DNS
- Web proxy

3.1.4. Konsola rozwiązania musi być hostowana na platformie Amazon Web Services lub Microsoft Azure.

3.1.5. Rozwiązanie musi mieć możliwość zbierania danych poprzez dostarczone przez producenta kolektory danych.

3.1.6. Komunikacja pomiędzy konsolą a kolektorami i agentami musi być zabezpieczona z wykorzystaniem protokołu TLS.

3.1.7. System musi mieć możliwość zbierania danych z punktów końcowych za pośrednictwem dostarczonego przez producenta oprogramowania instalowanego na stacji końcowej.

3.1.8. Oprogramowanie agentów instalowanych na stacjach końcowych musi mieć możliwość wysyłania danych do kolektora lub bezpośrednio do konsoli osadzonej w chmurze.

3.1.9. System musi dostarczyć możliwości analizy incydentów poprzez konsolę chmurową.

3.1.10. System powinien zapewniać możliwość integracji API z co najmniej wymienionymi poniżej technologiami:

- AWS Cloud Trials
- Box.com
- Duo Security
- Google Apps
- Office 365
- Okta
- Saleforce.com

3.2. Monitorowanie zdarzeń

3.2.1. System musi mieć możliwość śledzenia i analizowania zagrożeń w postaci zunifikowanych incydentów.

3.2.2. System musi mieć możliwość wizualizacji incydentów na osi czasu.

3.2.3. System musi mieć możliwość dostarczania w incydencie co najmniej informacji o hostach, kontach, użytkownikach i dokładnym czasie wystąpienia zdarzenia.

3.2.4. System musi mieć możliwość mapowania taktyk oraz technik atakującego na matrycę MITRE ATT&CK.

3.2.5. System musi mieć możliwość analizy zachowania atakującego poprzez reguły behawioralne zawierające różnorodne możliwości detekcji.

3.2.6. Alerty behawioralne muszą być domyślnie włączone.

3.2.7. System musi obsługiwać co najmniej wymienione poniżej formaty przesyłania danych:

- STIX XML
- CSV

3.2.8. Rozwiązanie musi zbierać dane co najmniej z technologii wymienionych poniżej:

- Firewall
  - Barracuda Firewall
  - Cisco ASA Firewall + VPN
  - Cisco Meraki
  - Check Point
  - Clavister W20
  - Fortinet Firewall
  - Juniper Netscreen
  - Juniper Junos OS
  - Palo Alto
  - Palo Alto Networks WildFire
  - pfSense Firewall
  - SonicWALL
  - Sophos Firewall
  - Stonesoft Firewall
  - WatchGuard XTM
- IDS/IPS
  - Corero IPS
  - Dell iSensor
  - HP TippingPoint
  - McAfee IDS
  - Metaflows IDS
  - Security Onion
  - Snort IDS
  - Sourcefire 3D

3.2.9. System musi wspierać technologie „deception" służącą do wykrywania złośliwych użytkowników i działań poprzez rozwiązania typu Honeypot.

3.2.10. Producent rozwiązania musi udostępnić maszynę Honeypot mogącą integrować się z konsolą zarządzania i w bezpieczny sposób przesyłać do niej dane o incydentach.

3.2.11. System musi dostarczać gotowe reguły analizy zachowania użytkowników UBA oraz zachowania atakującego.

3.2.12. Reguły UBA i zachowań atakującego muszą być automatycznie aktualizowane przez producenta, częstotliwość aktualizacji powinna opierać się na identyfikacji nowych zagrożeń, testowaniu ich wykrywalności, a następnie wypychaniu do platformy.

3.2.13. System musi dodatkowo obsługiwać reguły out-of-the-box, reguły powinny mieć możliwość modyfikacji w oparciu o znane zachowania atakujących.

3.2.14. System powinien mieć możliwość wykrywania zagrożeń w oparciu o reguły oraz algorytmy sztucznej inteligencji.

3.2.15. System musi mieć możliwość analizy i profilowania środowiska klienta oraz wykrywania anomalii w środowisku.

3.2.16. Oprogramowanie agenta instalowane na stacjach końcowych musi zapewniać wgląd w aktywność procesów na punktach końcowych – klienckich jak i serwerowych.

3.2.17. Oprogramowanie agenta musi przechwytywać zdarzenia o aktywności procesów na stacji w czasie rzeczywistym.

3.2.18. System musi mieć możliwość identyfikacji unikalnych i rzadkich procesów uruchamianych w środowisku klienta.

3.2.19. System musi wspierać możliwość tworzenia niestandardowych alertów.

3.2.20. System musi mieć możliwość tworzenia własnych sygnatur w formatach – YARA, Snort oraz STIX/TAXII.

3.2.21. System musi mieć możliwość integracji z systemami Enterprise Cloud Serices w celu zbierania informacji na temat uwierzytelniania użytkowników i aktywności administracyjnej w środowiskach chmurowych. System musi wspierać pobieranie danych z następujących środowisk:

- AWS CloudTrail
- Box.com
- Duo Security
- Google Apps
- Office 365
- Okta.com
- Salesforce.com
- Centrify
- OneLogin
- Microsoft Azure

3.2.22. System musi umożliwiać wyszukiwanie danych poprzez Regex, String, KeyValue oraz Keyword.

3.2.23. System musi wspierać możliwości wyszukiwania danych w logach z wykorzystaniem języka LEQL.

3.3. Zaawansowana analiza

3.3.1. System musi koncentrować się na zachowaniu, a nie statycznych wskaźnikach zagrożeń dostarczając kontekst incydentu.

3.3.2. Zakres wykrywania musi obejmować również ataki typu phishing, lateral movement i naruszenie poświadczeń.

3.3.3. Silnik UBA musi mieć możliwości automatycznego korelowania adresów IP z logów typu „raw data" wraz z powiązanymi z nimi nazwami hostów i użytkownikami.

3.3.4. System musi dostarczać możliwości sprawdzania geolokacji IP oraz flagowania anomalii wykrytych w sieci.

3.3.5. Producent musi dostarczać do systemu dane Threat Intelligence stale aktualizowane i analizowane przez grupy badawcze producenta. Producent musi dostarczać co najmniej dane o złośliwych procesach, adresach IP, domenach i adresach URL.

3.3.6. System musi umożliwiać automatyczne generowanie alertu jeśli w środowisku klienta wykryje parametr zgodny z dostarczonymi przez producenta IoC.

3.3.7. Rozwiązanie musi pozwalać na wysyłanie raportów o alertach do wszystkich subskrybowanych w systemie kont.

3.3.8. System musi umożliwiać eksportowanie poszczególnych raportów w formacie PDF.

3.3.9. System musi wspierać analizę ruchu sieciowego (NTA) pozwalając na przechwytywanie i ocenę ruchu end-to-end w środowiskach fizycznych i wirtualnych.

3.3.10. Do analizy ruchu sieciowego system nie może wymagać urządzeń obsługujących przepływy typu NetFlow, sFlow, jFlow.

3.3.11. System musi umożliwiać głęboką analizę pakietów z wykorzystaniem silników Deep Packet Inspection.

3.3.12. System musi mieć możliwość pobierania z ruchu sieciowego informacji takich jak adresy IP, porty i rozpoznane aplikacje.

3.3.13. System musi mieć możliwość wykrywania złośliwego oprogramowania zarówno przed jak i po jego uruchomieniu.

3.3.14. System musi zawierać gotowe szablony Workflow, które zapewniają poszczególne scenariusze automatyzacji środowiska.

3.3.15. Automatyczne akcje muszą być dostępne z wykorzystaniem oprogramowania agenta działającego na stacjach końcowych lub specjalnej maszyny orchestratora, która musi być dostępna do pobrania z konsoli rozwiązania.

3.3.16. System musi wspierać funkcjonalność File Integrity Monitoring, musi mieć możliwość audytowania plików na stacjach końcowych oraz wykrywania modyfikacji krytycznych plików i folderów.

3.3.17. System musi monitorować co najmniej wymienione poniżej typy plików:

- .bat
- .cfg
- .conf
- .config
- .dll
- .exe
- .ini
- .sys

3.4. Zarządzanie i zabezpieczenia

3.4.1. System musi umożliwiać przechowywanie danych w konsoli co najmniej przez okres 13 miesięcy. W tym czasie logi muszą być dostępne do przeszukiwania, analizowania i wizualizowania.

3.4.2. System musi umożliwiać opcjonalnie dłuższe przechowywanie danych.

3.4.3. System musi umożliwiać przechowywanie danych bez konieczności używania sprzętu zewnętrznego.

3.4.4. Rozwiązanie musi dostarczać możliwości tworzenia kopii zapasowych danych klientów, dane te nie mogą być replikowane poza region wybierany podczas aktywowania konsoli chmurowej.

3.4.5. Dane każdego z klientów muszą być izolowane wewnątrz jego własnej instancji w indywidualnej bazie danych uniemożliwiając innym klientom dostęp do bazy użytkowników.

3.4.6. System musi dostarczać co najmniej następujące uprawnienia administratorów:

- Platform Admin Product
- Admin Read/Write
- Read Only

3.4.7. Użytkownicy muszą uwierzytelniać się bezpośrednio w konsoli systemowej, system musi zapewniać funkcjonalność uwierzytelniania wieloskładnikowego poprzez:

- Okta
- SMS
- Google Authenticator

3.4.8. System musi mieć możliwość automatycznego powiadamiania użytkowników o znaczących zagrożeniach za pośrednictwem wiadomości email.

3.4.9. Rozwiązanie musi wspierać integrację z ServiceNow.

3.4.10. Administrator musi mieć możliwość tworzenia notatek dotyczących danego incydentu, notatki muszą być tworzone i przechowywane w ramach konsoli systemu.

3.4.11. System musi mieć możliwość przetwarzania danych strukturalnych w formatach STIX i CSV.

3.4.12. System musi mieć możliwość zbierania danych ze stacji końcowych poprzez oprogramowanie agenta działającego co najmniej na systemach z rodzin:

- Microsoft Windows Desktop
- Microsoft Windows Server
- macOS
- Linux

3.4.13. System musi mieć możliwość okresowego skanowania punktów końcowych w celu zbierania danych o stacjach końcowych.

3.4.14. Rozwiązanie musi być zgodne co najmniej ze standardami GDPR, PCI oraz HIPAA.

3.4.15. Producent musi z powodzeniem uzyskać raport SOC2.

3.5. Wizualizacja i raportowanie

3.5.1. System musi mieć możliwości wizualizacji danych w specjalnej sekcji „Dashboard". Musi mieć możliwość wyświetlania co najmniej informacji o statystykach, użytkownikach, incydentach i hostach.

3.5.2. System musi dostarczać gotowe pulpity do wizualizacji danych jak i umożliwiać klientowi tworzenie własnych niestandardowych pulpitów.

3.5.3. Rozwiązanie musi pozwalać na tworzenie raportów z niestandardowych pulpitów zbudowanych z prekonfigurowanych kart które można dopasowywać wedle potrzeb klienta.

3.5.4. System musi pozwalać na tworzenie raportów jednorazowo jak i wg. skonfigurowanego harmonogramu.

3.5.5. System musi dostarczyć możliwość eksportowania danych na temat użytkowników, hostów i logów bezpośrednio z konsoli rozwiązania.

4. Zakres wsparcia technicznego i serwisu Rozwiązań oraz zakupu pakietów suportowych:

4.1. Wsparcie techniczne jest realizowane bezpośrednio przez producenta Rozwiązań.

4.2. Użytkownik komunikuje się z producentem za pomocą portalu wsparcia.

4.3. Czas inicjalnej reakcji producenta na założenie zgłoszenia w systemie dla zgłoszeń:

4.3.1. Krytycznych – powinien wynosić do 2 godzin (24h/7dni)

4.3.2. Innych priorytetów – powinien wynosić od 4 biznes godzin do 24 biznes godzin.

5. **Gwarancja na oprogramowanie obejmująca aktualizacje do najnowszej wersji przez okres 24** miesięcy od daty zakupu.