**Załącznik nr 1.5**

OPIS PRZEDMIOTU ZAMÓWIENIA

**Część 5**

1. **System cyberbezpieczeństwa dostarczany w modelu SaaS, zapewniający kompleksową ochronę infrastruktury IT organizacji**

**Podsumowanie opisu przedmiotu zamówienia**

Przedmiotem zamówienia jest zaawansowany system cyberbezpieczeństwa dostarczany w modelu SaaS, zapewniający kompleksową ochronę infrastruktury IT organizacji. System powinien oferować centralną konsolę zarządzania, wysoką dostępność (co najmniej 99,9%) oraz wsparcie dla szerokiej gamy urządzeń, w tym serwerów, stacji roboczych i urządzeń mobilnych. Wszystkie moduły i funkcje muszą pochodzić od jednego producenta, a dane przetwarzane w systemie muszą być zgodne z regulacjami GDPR oraz standardami bezpieczeństwa, takimi jak ISO/IEC 27001:2022 i SOC 2 Type 2. Wymagane jest także, aby system był sklasyfikowany jako rozwiązanie czołowe w uznanych raportach branżowych, takich jak Gartner Magic Quadrant for Endpoint Protection Platforms oraz Forrester Wave for Extended Detection and Response Platforms.

Oczekiwany system powinien integrować moduły odpowiedzialne za detekcję i odpowiedź na zagrożenia (EDR/XDR), zarządzanie incydentami oraz identyfikację podatności w infrastrukturze IT (ASM). System musi oferować szerokie możliwości automatyzacji, takie jak grupowanie alertów, tworzenie scenariuszy obsługi incydentów oraz integrację z narzędziami zewnętrznymi poprzez interfejs API. Kluczowym elementem funkcjonalności jest również możliwość przeprowadzania szczegółowych analiz incydentów, ułatwiających zrozumienie zakresu i przyczyn ataków.

System powinien być dostarczony z usługami wsparcia technicznego, usługami wdrożeniowymi oraz szybką reakcją na incydenty bezpieczeństwa IT. Ważnym elementem zamówienia jest potwierdzenie skuteczności rozwiązania w praktyce poprzez jego ocenę w niezależnych raportach branżowych. Dodatkowe punkty oceny ofert mogą być przyznane za rozbudowę funkcji systemu, takich jak większa liczba analiz w sandboxie czy rozwinięcie modułów ochrony tożsamości oraz analizy zagrożeń. Zamawiający przewiduje możliwość dalszego rozwoju funkcjonalności systemu, dostosowanego do indywidualnych potrzeb użytkownika.

Przedmiotem zamówienia jest wdrożenie, utrzymanie oraz rozwój zintegrowanego systemu cyberbezpieczeństwa, obejmującego ochronę punktów końcowych, serwerów, urządzeń mobilnych oraz środowisk VDI, z wykorzystaniem rozwiązania SaaS o wysokiej dostępności, wraz z usługami zarządzalnymi oraz możliwością całodobowego wsparcia przez jednostkę Security Operations Center (SOC).

**Usługa MSSP (Managed Security Service Provider) przez cały okres obowiązywania umowy:**

* Wdrożenie i utrzymanie całej platformy bezpieczeństwa EPP (endpoint prtection platform)
* Obsługa zgłoszeń w trybie 8/5
* Wykonywanie wszelkich zleconych zmian konfiguracyjnych w czasie rozumianym jako NBD (next business day)
* Prowadzenie komunikacji z producentem, zgłaszanie wszelkich prac serwisowych, analiza błędów
* Przygotowywanie raportów z działania systemu i wykrytych detekcji
* Współpraca z zespołem SOC przy integracji rozwiązania z systemami klasy SIEM

**Wymagania ogólne**

1. System musi posiadać centralną konsolę realizowaną w formie usługi SaaS (ang. Software-as-a-Service) o dostępności co najmniej 99,9% a do ochrony stacji i serwerów wykorzystywać agenta.
2. Wszystkie moduły funkcjonalne systemu muszą być dostarczony od jednego producenta.
3. System musi przechowywać i przetwarzać dane na terenie Europejskiego Obszaru Gospodarczego.
4. System musi być zgodny z regulacjami GDPR (ang. General Data Protection Regulation), posiadać certyfikację ISO/IEC 27001:2022 lub zgodność z SOC 2 Type 2.
5. Dojrzałość i skuteczność systemu musi być poświadczona przez co najmniej następujące niezależne instytucje badające rynek rozwiązań EDR/XDR:
   1. System musi być sklasyfikowany przynajmniej jako “Leader” dla raportu Forrester Wave For Extended Detection and Response Platforms Q2 2024.
   2. System musi być sklasyfikowany przynajmniej jako „Leader” dla raportu Gartner Magic Quadrant for Endpoint Protection Platforms co najmniej za rok 2024 i 2025.
6. **System należy dostarczyć z subskrypcją na okres 24 miesięcy umożliwiającą objęcie ochroną 210 stacji roboczych i/lub serwerów. System ma obowiązywać od 22.10.2026 r**.
7. System musi przechowywać informacje o alarmach i incydentach co najmniej przez 90 dni.
8. Interfejs API systemu musi umożliwiać co najmniej następujące akcje:
   1. Wykonanie kwerendy do danych telemetrycznych z endpointa i z systemów trzecich
   2. Pobranie pliku instalacyjnego agenta
   3. Uruchomienie skryptu na wskazanym hoście
   4. Zarządzenia izolacją sieciową danego hosta
   5. Przywrócenie pliku z kwarantanny
   6. Pobranie informacji o alarmach
   7. Zlecenie skanowania hosta
   8. Pobranie pliku z hosta
9. System musi przechowywać przez 365 dni logi audytowe odnotowujące co najmniej logowanie użytkowników, zmiany wprowadzane w konfiguracji systemu, nawiązywanie zdalnych połączeń do chronionych stacji i wykorzystanie interfejsu API.
10. System musi posiadać możliwość instalacji agenta na co najmniej następujących systemach operacyjnych:
    1. Microsoft:
       1. Windows 11 (x86-64 oraz arm64)
       2. Windows 10 (x86-64 oraz arm64)
       3. Windows Server 2008 R2 SP1
       4. Windows Server 2012 i 2012 R2
       5. Windows Server 2016 i Server Core 2016
       6. Windows Server 2019 i Server Core 2019
       7. Windows Server 2022 i Server Core 2022
       8. Windows Server 2025 i Server Core 2025
    2. Linux
       1. CentOS 8 i nowsze
       2. Debian 9 i nowsze
       3. Oracle Linux 8 i nowsze
       4. Red Hat Enterprise Linux 8 i nowsze
       5. Rocky Linux 8 i nowsze
       6. SUSE 12 i nowsze
       7. Ubuntu 16 i nowsze
    3. Apple macOS
       1. macOS Sonoma 14
       2. macOS Sequoia 15
       3. macOS Tahoe 26
    4. Apple iOS/iPadOS od 17.x
    5. Android od 13.x
11. System musi posiadać możliwość instalacji agenta na systemach Windows 7 SP1 nie objętych rozszerzonym wsparciem producenta. Wersja agenta dla w/w systemu operacyjnego nie może być wycofana ze wsparcia Producenta i otrzymywać bieżące aktualizacje mechanizmów detekcyjno-prewencyjnych.
12. System musi posiadać możliwość instalacji agenta na systemach VDI.
13. System musi umożliwiać wygenerowanie i pobranie pakietu instalacyjnego:
    1. W formacie msi lub exe dla systemów Microsoft
    2. W formacie pakietu rpm i deb dla systemów Linux
    3. W formacie pakietu pkg dla macOS
14. System musi umożliwiać instalację agenta dla systemów iOS/iPadOS i Android za pośrednictwem systemu MDM lub odpowiednio ze sklepu Apple Store i Google Play.
15. Wymagana jest ocena na poziomie min „A+” dla wszystkich serwisów, z których korzysta oferowane rozwiązanie. Ocena będzie weryfikowana przy pomocy ogólnodostępnego narzędzia <https://www.ssllabs.com>
16. Komunikacja między agentem a konsolą systemu musi być realizowana z wykorzystaniem protokołu HTTPS w wariancie co najmniej z TLS1.2 i odbywać się:
    1. Bezpośrednio
    2. Pośrednio przez proxy systemowe
    3. Pośrednio przez proxy wskazane w trakcie instalacji
17. Dokumentacja systemu musi wskazywać adresy IP oraz adresy URL, z którymi komunikuje się agent nawiązując komunikację z konsolą systemu, aby umożliwić udrożnienie komunikacji sieciowej.
18. System musi posiadać możliwość zarządzania przez przeglądarkę internetową. Komunikacja musi być zabezpieczona HTTPS w wariancie co najmniej z TLS1.2.
19. Interfejs webowy systemu nie może korzystać z komponentów typu Flash, Silverlight, applet Java, ActiveX, wtyczek NPAPI.
20. System musi posiadać możliwość zarządzania przez interfejs API. Uwierzytelnienie do interfejsu API platformy musi być realizowane w oparciu o OAuth2 i musi oferować możliwość granularnej autoryzacji dostępu klienta OAuth2 do poszczególnych obszarów funkcjonalnych Systemu.
21. System musi posiadać możliwość wskazania listy publicznych adresów IP, z których będzie istniała możliwość zalogowania się do konsoli systemu oraz nawiązania połączenia do interfejsu API.
22. System musi umożliwiać integrację z zewnętrznymi katalogami użytkowników z wykorzystaniem SAML 2.0.
23. System musi posiadać wbudowany katalog użytkowników oraz obsługiwać drugi czynnik uwierzytelniający wykorzystujący tokeny TOTP (ang. Time Based One-Time Password).
24. System podczas tworzenia haseł dla lokalnych kont administracyjnych musi wymuszać minimalnie następujące wymagania złożoności hasła: co najmniej 11 znaków, musi zawierać małe i duże litery, cyfry i znaki specjalne.
25. System nie może posiadać ograniczenia licencyjnego na liczbę użytkowników (administratorów, analityków, inżynierów bezpieczeństwa) zdefiniowanych w systemie ani ograniczenia na równocześnie zalogowanych w systemie użytkowników. Wszyscy użytkownicy muszą posiadać własne konta imienne. Nie dopuszcza się wykorzystania współdzielonych kont użytkowników.
26. System musi umożliwiać określenie zakresu dostępu z wykorzystaniem matrycy ról i ich przypisania do użytkownika lub do grupy użytkowników. Rola musi definiować dostęp do określonego obszaru administracyjnego systemu, jego rodzaj (tylko do odczytu, pełen dostęp) oraz jego zakresu (wszystkie lub wybrane hosty).
27. System musi obsługiwać co najmniej 5 poziomów ważności alarmów, np: informacyjny, niski, średni, wysoki i krytyczny.
28. System musi automatycznie grupować powiązane alerty w celu przyspieszenia i ułatwienia triażu i analizy incydentu.
29. System musi umożliwiać tworzenie wyjątków dla reguł prewencyjnych na podstawie certyfikatu producenta oprogramowania.
30. System dla alarmów zgrupowanych w ramach incydentu musi automatycznie tworzyć łańcuchy przyczynowo skutkowe reprezentujące zależności pomiędzy procesami wykorzystywanymi w trakcie ataku i powiązane dane telemetryczne, celem ułatwienia przeanalizowania wykorzystywanych technik, określenia zakres ataku, ustalenia celu i zakresu ataku oraz zweryfikowania, czy atak się powiódł.
31. System musi umożliwiać zarządzanie incydentami co najmniej w następującym zakresie:
    1. Przypisanie incydentu do analityka
    2. Zmianę stanu incydentu np: badany, false positive, true positive, duplikat, testy
    3. Dodawanie notatek
32. System musi mapować alarmy do frameworku MITRE ATT&CK.
33. System musi posiadać możliwość kontroli urządzeń podłączanych do portów USB co najmniej na systemach windows i macOS w następującym zakresie:
    1. Określenia jakie urządzenia USB można podłączyć
    2. Określenia zakresu dostępu do pamięci masowej USB:
       1. Brak dostępu
       2. Tylko odczyt
       3. Odczyt i zapis
       4. Odczyt, zapis i uruchamianie
34. System musi posiadać możliwość kontroli host firewalla co najmniej na systemach Windows i MacOS.
35. System musi posiadać możliwość skonfigurowania manualnej i automatycznej aktualizacji agenta dla wskazanych grup hostów. Polityka automatycznej konfiguracji agenta musi umożliwiać określenie:
    1. Dnia tygodnia i zakresu czasu, w którym aktualizacja nie będzie wykonywana
    2. Tempa propagacji aktualizacji
    3. Możliwość wersji: względnie wobec najnowszych wydanych lub bezwzględnie (konkretna wersja)
36. System musi posiadać możliwość kontroli w jaki sposób agent będzie pobierał aktualizacje mechanizmów detekcyjno-prewencyjnych co najmniej w następującym zakresie:
    1. Agent pobiera aktualizację natychmiast po opublikowaniu przez producenta
    2. Agent pobiera aktualizację z określonym opóźnieniem od momentu publikacji przez producenta
37. System musi umożliwiać dynamiczne grupowanie hostów z wykorzystaniem co najmniej następujących atrybutów: nazwa hosta, domena Active Directory, pojemnik Organizational Unit wewnątrz Active Directory, system operacyjny, adres ip, podsieć ip, znacznik.
38. System musi umożliwiać nawiązanie zdalnego połączenia konsolowego do hosta chronionego agentem oferując co najmniej następujące funkcje:
    1. Podgląd uruchomionych procesów
    2. Podgląd systemów plików
    3. Podgląd stanu socketów sieciowych
    4. Wyłączenie wskazanego procesu
    5. Uruchomienie skryptu z biblioteki
    6. Pobranie pliku z hosta
    7. Wgranie pliku na hosta
    8. Zrzut pamięci procesu
    9. Zrzut pamięci systemu operacyjnego
    10. Wyłączenie i restart systemu
39. System musi umożliwiać zdalną izolację sieciową hosta. W trakcie trwania izolacji sieciowej cały ruch sieciowy z wyjątkiem połączenia do systemu oraz protokołu DHCP musi zostać zablokowany.
40. System musi umożliwiać tworzenie biblioteki skryptów oraz ich zdalne uruchamianie na pojedynczym hoście i na grupie hostów. Wymagana jest obsługa co najmniej następujących języków skryptowych:
    1. Systemy windows: powershell
    2. Systemy Linux: skrypty bash lub python
    3. Systemy MacOS: skrypty zsh lub python
41. System musi posiadać możliwość uruchomienia pełnego skanowania hosta na żądanie i w odpowiedzi na zarejestrowany alarm.
42. System musi umożliwiać bezpośrednią integrację z usługą VirusTotal, DomainTools oraz Security Scorecard. Wraz z Systemem nie jest wymagane dostarczenie licencji do żadnego z w/w narzędzi.
43. System musi umożliwiać globalne oraz per grupa hostów blokowanie uruchamiania plików binarnych poprzez wskazanie ich hasha.
44. System musi posiadać możliwość budowania własnych reguł detekcyjno-prewencyjnych bazujących co najmniej na określeniu łańcucha przyczynowo-skutkowego procesów wraz z określeniem parametrów linii poleceń.
45. System musi posiadać możliwość budowania własnych list indykatorów (ang. Indicator Of Compromise) w formie nazw domenowych, adresów IPv4 i IPv6 oraz hashy SHA256 i MD5 poprzez:
    1. Import indykatorów z pliku
    2. Manualne dodanie indykatorów
    3. Programowe dodanie indykatorów przez interfejs API
46. System musi umożliwiać definiowanie własnych dashboardów (konsol) z wykorzystaniem predefiniowanych widgetów (kontrolek) oraz kontrolek definiowanych samodzielnie poprzez kwerendy do danych telemetrycznych.
47. System musi umożliwiać przeszukiwanie wszystkich danych telemetrycznych przy pomocy kreatorów lub manualnie z wykorzystaniem kwerend. Kwerendy muszą umożliwiać łączenie danych telemetrycznych z różnych źródeł, ich filtrowanie, przekształcanie wyników i obsługiwać free text search (wyszukiwanie dowolnego ciągu znaków bez wskazywania konkretnego pola). Reguły tworzenia kwerend muszą być opisane w dokumentacji systemu.
48. System musi umożliwiać zapisanie kwerendy do danych telemetrycznych do biblioteki.
49. System musi umożliwiać zrealizowanie kwerendy do danych telemetrycznych i odczytanie jej wyników via interfejs API.
50. System musi umożliwiać eksport wyników kwerendy do danych telemetrycznych w formie pliku tekstowego.
51. System musi umożliwiać przekształcenie kwerendy do danych telemetrycznych w uruchamianą zgodnie z podanym harmonogramem regułę korelacyjną generującą alarmy, jeśli kwerenda zwróciła więcej niż jeden rekord.
52. System musi umożliwiać wykrywanie zasobów podłączonych w sieci wewnętrznej w sposób pasywny (analiza tablicy ARP) oraz umożliwiać skonfigurowanie aktywnego skanowania sieci.
53. System musi umożliwiać eksport danych telemetrycznych z agenta i danych telemetrycznych z systemów trzecich.
54. System musi posiadać wbudowany moduł raportowania o podatnościach systemu operacyjnego i o podatnościach zainstalowanych aplikacji na systemach operacyjnych Windows, macOS i Linux oraz tworzyć inwenturę zainstalowanych aplikacji i dodatków do przeglądarek. Dopuszcza się rozwiązanie, w którym inwentura aplikacji i dodatków do przeglądarek będzie wykonywana ad-hoc na żądanie z wykorzystaniem customowych skryptów (np. python).
55. System musi posiadać wbudowany moduł SOAR (ang. Security Orchestration, Automation and Response) umożliwiający automatyczną obsługę alarmów w tym m.in. możliwość zmiany konfiguracji (orkiestracji) innych systemów bezpieczeństwa i rozszerzenie kontekstu alarmu poprzez integrację z systemami trzecimi. Wbudowany moduł SOAR musi umożliwiać budowanie spersonalizowanych scenariuszy obsługi (ang. playbooki) z wykorzystaniem graficznego narzędzia bez potrzeby pisania kodu.
56. Wbudowany moduł SOAR musi posiadać możliwość orkiestracji systemów bezpieczeństwa wewnątrz sieci Zamawiającego (systemów on-prem) oraz systemów bezpieczeństwa dostarczanych w formie usługi chmurowej (systemy SaaS).
57. Wbudowany moduł SOAR musi umożliwiać zrealizowanie co najmniej następujących scenariuszy:
    1. Wysłanie powiadomienia mailowego i via Microsoft Teams w przypadku, gdy mechanizmy detekcyjno-prewencyjne agenta przestały funkcjonować poprawnie
    2. Włączenie skanowania hosta w odpowiedzi na alarm o wskazanej istotności
    3. Wysłanie maila do wskazanych adresatów w odpowiedzi na alarm o wskazanej istotności celem potwierdzenia załączenia izolacji sieciowej hosta.
    4. Założenie zgłoszenia w systemie Jira w odpowiedzi na alarm o wskazanej istotności lub alternatywnie wywołanie konfigurowalnego webhooka w odpowiedzi na alarm o wskazanej istotności celem integracji z systemem do śledzenia zgłoszeń.
    5. Raz na dobę wysyłanie powiadomienia mailowego o serwerach, na których agent jest offline.
    6. W odpowiedzi na alarm o zadanej wartości, w którym zidentyfikowano komunikację z groźnymi publicznymi adresami IP musi nastąpić dodanie w/w adresów IP do listy blokowanych adresów IP firewallu Palo Alto Networks. Zgodę na dodanie adresów IP musi wyrazić wskazany operator otrzymując powiadomienie o konieczności podjęcia decyzji w formie powiadomienia wysłanego na wskazany kanał Microsoft Teams lub drogą mailową.

**Wymagania dla agenta**

1. Agent nie może wykorzystywać Oracle Java JRE/JDK.
2. Instalacja agenta nie może wymagać restartu systemu operacyjnego.
3. Agent musi weryfikować poprawność certyfikatu w trakcie nawiązywania połączenia z systemem w celu ochrony przed atakami man-in-the-middle z wykorzystaniem mechanizmu certificate pinning lub podobnego.
4. Agent musi posiadać mechanizmy ochronne uniemożliwiające wyłączenie agenta lub wpłynięcie na jego poprawne funkcjonowanie nawet przez użytkowników z podwyższonymi uprawnieniami (ang. anti-tampering) na systemach Windows, macOS i Linux.
5. Odinstalowanie agenta musi być chronione unikalnym hasłem dla każdej chronionej stacji, tak aby uniemożliwić odinstalowanie agenta nawet użytkowników z podwyższonymi uprawnieniami na systemach Windows, macOS i Linux.
6. W trakcie instalacji agenta musi istnieć możliwość nadania agentowi nieusuwalnego bezpośrednio z konsoli systemu znacznika, który może zostać wykorzystany jako atrybut do grupowanie hostów.
7. W trakcie instalacji agenta musi istnieć możliwość wskazania dedykowanego serwera proxy, z którego agent będzie korzystał nawiązując połączenie z systemem.
8. Agent musi wykrywać i blokować próby wyłączenia usługi Volume Shadow Copy Service (VSS) oraz inne próby uszkodzenia migawek VSS.
9. Agent musi realizować ochronę przed atakami klasy Bring Your Own Vulnerable Driver poprzez wykrywanie i blokowanie prób ładowania podatnych sterowników.
10. Agent musi bezpośrednio na chronionym hoście zapewniać ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi co najmniej w następujący sposób:
    1. Weryfikacja reputacji pliku w bazie threat intelligence producenta systemu
    2. Lokalna analiza statyczna bazująca na uczeniu maszynowym (ang. Machine learning)
11. Agent musi zapewnić ochronę przed znanymi i nieznanymi złośliwymi makrami w plikach Microsoft Word i Microsoft Excel co najmniej w następujący sposób:
    1. Weryfikacja reputacji makra w bazie threat intelligence producenta
    2. Lokalna analiza statyczna bazująca na uczeniu maszynowymi (ang. Machine learning)
12. Agent musi posiadać możliwość usuwania złośliwych makr wykrytych w plikach Microsoft Word i Microsoft Excel.
13. Agent musi realizować ochronę przed zaszyfrowaniem dysku i plików przez złośliwe oprogramowanie (aka ochrona anty-ransomware’owa).
14. Agent musi wykonywać analizę plików binarnych po tym jak zostały zapisane w systemie plików.
15. Musi zapewniać ochronę przed znanymi i nieznanymi exploitami wykorzystującymi znane i nieznane luki bezpieczeństwa w oprogramowaniu.
16. Agent musi posiadać konfigurowalną opcję umieszczania złośliwych plików w kwarantannie.
17. Agent musi automatycznie wykonywać skanowanie pamięci masowej natychmiast po jej podłączeniu do portu USB lub musi blokować próby intencjonalnego i automatycznego uruchomienia plików wykonywalnych z pamięci masowej.
18. Agent musi posiadać mechanizm skanowania pamięci RAM w celu wykrywania złośliwego kodu.
19. Agent, poprzez analizę złożonych łańcuchów przyczynowo skutkowych i wykrywanie technik i taktyk stosowanych przez cyberprzestępców, musi zapewnić ochronę przed atakami klasy Living of The Land wykorzystującymi legalne narzędzia systemowe w groźny sposób.
20. Agent musi zapewniać ochronę przed atakami mającymi na celu kradzież poświadczeń użytkowników.
21. Agent musi posiadać możliwość automatycznej remediacji złożonych ataków co najmniej poprzez wyłączenie złośliwych procesów, umieszczenie plików w kwarantannie, usunięcie zadań z harmonogramu i wpisów z rejestru.
22. Agent musi integrować się z Windows Security Center.
23. Agent musi umożliwiać kwarantannę groźnych plików.
24. Agent musi działać:
    1. W jądrze systemu (używać sterownika) na systemach Windows
    2. W jądrze systemu (aka kernel space) lub poza jądrem systemu (aka user space) na systemach Linux
    3. Poza jądrem systemu na systemach MacOS
25. Agent na systemy Linux musi posiadać możliwość automatycznego przełączenia się do pracy w trybie bez sterownika (aka user space), jeśli sterownik nie został poprawnie załadowany.
26. Agent dla systemów Windows, MacOS i Linux musi zbierać i wysyłać do systemu co najmniej następujące dane telemetryczne:
    1. Utworzenie nowego procesu i zakończenie procesu
    2. Operacje na socketach sieciowych dla TCP i UDP
    3. Operacje na plikach
    4. Zdarzenia z event logu dotyczące uwierzytelnienia.
    5. Operacje na rejestrze (tylko systemy Windows)
27. W przypadku braku łączności z systemem agent musi lokalnie przechować dane telemetryczne i wysłać je do systemu po przywróceniu łączności sieciowej.
28. **Usługa SOC**

Usługa musi być świadczona przez cały okres 36 miesięcy.

Security Operation Center (SOC) powinien obejmować kompleksową usługę w zakresie monitorowania, analizy, reagowania i raportowania na incydenty cyberbezpieczeństwa w trybie całodobowym (24/7/365), realizowaną w modelu usługowym z wykorzystaniem kompetencji oraz własnej infrastruktury.

**Zakres usługi**

Usługa SOC obejmuje:

* **Monitorowanie infrastruktury IT** pod kątem wykrywania i analizy zdarzeń bezpieczeństwa oraz identyfikacji nietypowych i podejrzanych aktywności.
* **Reagowanie na incydenty** – klasyfikacja incydentów, analiza i weryfikacja zdarzeń oraz podejmowanie działań ograniczających ich skutki.
* **Zarządzanie podatnościami** – cykliczne skany podatności oraz współpraca w zakresie eliminacji zagrożeń.
* **Raportowanie i rekomendacje prewencyjne** mające na celu minimalizację ryzyka przyszłych incydentów.

**Technologie i kompetencje**

Usługa jest realizowana przez zespół certyfikowanych specjalistów posiadający akredytację ‘Trusted Introducer’ status minimum Accredited oraz zgodność z normami: ISO 27001 i ISO 22301 potwierdzona certyfikatami wystawionymi przez jednostkę posiadającą akredytację Polskiego Centrum Akredytacji (PCA) albo jednostkę uznawaną przez PCA.

Dodatkowo zespół SOC powinien posiadać certyfikaty osobowe min.:

- CEH – Certified Ethical Hacker;

- CISSP – Certified Information System Security Professional

- SC-200 – Microsoft Security Operations Analyst

- OSCP - Offensive Security Certified Professional

- CySA+ - CompTIA Cybersecurity Analyst

**Kluczowe wymagania organizacyjne**

* Stały monitoring i obsługa incydentów 24/7/365.
* Wsparcie konsultacyjne z zakresu cyberbezpieczeństwa.
* Dostarczenie oraz utrzymanie technologii i infrastruktury niezbędnej do świadczenia usługi.
* Bieżąca komunikacja i współpraca z zespołem bezpieczeństwa organizacji zamawiającej.
* Raportowanie bieżące i okresowe oraz rekomendacje w zakresie poprawy bezpieczeństwa.

**Standardy realizacji usługi**

Jednostka Security Operation Center powinna spełniać w całości **Rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo.**

**Linie wsparcia SOC i czasy reakcji**

* **Pierwsza linia wsparcia (Tier 1):**
  + Odpowiada za natychmiastowe przyjęcie zgłoszenia, wstępną analizę i triage incydentu. Analiza ma na celu kwalifikację zdarzeń na potencjalne incydenty lub fałszywe alarmy (tzw. false-positives)
  + Czas reakcji: natychmiast po otrzymaniu zgłoszenia lub automatycznym wykryciu przez system monitoringu **do 30 min**. Działanie w trybie **24/7.**
  + Call Center – przyjmowanie i rejestracja zgłoszeń, informowanie w nagłych wypadkach
  + Mapowanie sieci
* **Druga linia wsparcia (Tier 2):**
  + Prowadzi zaawansowaną analizę incydentu, podejmuje działania naprawcze i koordynuje reakcję eliminującą zagrożenie.
  + Czas reakcji: uruchamiana **w ciągu 1 godziny** od eskalacji przez pierwszą linię; godziny od potwierdzenia incydentu wymagającego specjalistycznej interwencji. Działanie w trybie **24/7.**
  + Koordynacja działań związanych z reakcją na incydent
  + Zdalna reakcja na incydenty
  + Raportowanie – raportowanie ustalonych KPI w zakresie obsługi i reakcji na incydenty
  + Inżynieria detekcji - budowanie, modyfikowanie i rozwijanie w trybie ciągłym obszaru telemetrii i reguł detekcji, w oparciu o wiedzę ze źródeł CTI, znajomości monitorowanego środowiska, jego ryzyk, kontekstu działania.
  + Skanowanie podatności – badanie hostów sieciowych opiera się na weryfikacji poziomu aktualizacji oprogramowania i zgodności konfiguracji z zaleceniami bezpieczeństwa
* **Trzecia linia wsparcia (Tier 3):**
  + Czas reakcji: podejmuje działania w ciągu 4 godzin od eskalacji incydentu przez drugą linię; w przypadku skomplikowanych zdarzeń, prace uruchamiane są natychmiast po potwierdzeniu potrzeby przez Tier 2, z gwarancją rozpoczęcia działań **do 4 godzin**. Tryb pracy **8/5**. Dostęp do 3 linii wsparcia w modelu Time&Materials zapewniający przynajmniej takie usługi jak:
  + Pozyskiwanie i analiza Threat Intelligence oraz aktywny Threat Hunting
  + Forensic wraz z możliwością reakcji na incydenty w miejscu ich wystąpienia
  + Pentesty – symulowanie ataków hakerskich
  + Reverse Engineering – analiza nieznanego malware’u

1. **Platforma przeciwdziałania cyberzagrożeniom, oferująca możliwości wykrywania i obsługi zdarzeń, incydentów oraz podatności.**

Wymagana obsługa minimum 250 urządzeń

Przedmiotem zamówienia jest zakup, dostarczenie i wdrożenie w środowisku informatycznym Zamawiającego systemu przeciwdziałającemu cyberzagrożeniom, umożliwiającego ich wykrywanie przy wsparciu mechanizmów uczenia maszynowego oraz zapewniającego 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 umożliwiający 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 zwartości 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 zapełnienia musi być możliwa konfiguracja, która zapewni automatyczne przeniesienie logów do archiwum lub umożliwi ich nadpisanie.

17. System musi umożliwiać fizyczne rozdzielenie 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 rozdzielenia 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 integralność 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:

1. nowe zasoby wykryte w sieci,
2. typy wykrytych zasobów (np.: serwer lub stacja robocza),
3. zastosowane na nich zabezpieczenia,
4. usługi z którymi się komunikują,
5. nowe usługi wykryte na zasobie
6. 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:

1. fqdn,
2. e-mail,
3. nazwa pliku,
4. ścieżka do pliku,
5. hash,
6. adres IP,
7. klucz rejestru,
8. 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:

1. id techniki,
2. taktykę,
3. platformy których dotyczy,
4. potencjalne źródła,
5. opis zagrożenia,
6. mityzację,
7. sposób detekcji,
8. 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:

1. rozdzielenie procesu nauczania zachowania użytkowników uprzywilejowanych od użytkowników nieuprzywilejowanych,
2. rozdzielenie procesu nauczania zachowania stacji roboczych od serwerów,
3. rozdzielenie serwerów świadczących usługi w sieci Internet od serwerów świadczących usługi lokalnie w organizacji,
4. 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 korelacje 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 tworzenie 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 tworzenie reguł musi uwzględniać:

1. sparsowane pola oraz ich wartości,
2. listy referencyjne,
3. atrybuty użytkowników z Active Directory,
4. atrybuty komputerów z Active Directory,
5. bazę wskaźników kompromitacji (IOC),
6. informacje z elektronicznej dokumentacji,
7. anomalie w zachowaniu użytkowników (UBA),
8. anomalie w zachowaniu zasobów (EBA),
9. podatności na zasobach,
10. wyniki analizy konfiguracji,
11. techniki MITRE ATT&CK®,

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

1. wykrycie dowolnej treści w logach,
2. wykrycie zmiany jednego z kilku pól,
3. wykrycie zaniku wiadomości,
4. wykrycie nowej wartości pola w zadanym okresie czasu,
5. wykrycie incydentu będącego pochodną zdarzeń występujących w określonej kolejności,
6. wykrycie zdefiniowanej ilości przesłanych danych w zadanym okresie czasu,
7. wykrycie chwilowego wzrostu ilości przesłanych danych (tzw. peek) w stosunku do całkowitej ilości przesłanych danych w zadanym okresie czasu,
8. wykrycie sumarycznego wzrostu przesłanych danych w zdefiniowanej strefie bezpieczeństwa,
9. wykrycie zdefiniowanej ilości przesyłanych pakietów w zadanym okresie czasu,
10. wykrycie chwilowego wzrostu (tzw. peek) w stosunku do ilości przesyłanych pakietów w zadanym okresie czasu,
11. wykrycie sumarycznego wzrostu ilości pakietów przesyłanych w zdefiniowanej strefie bezpieczeństwa,
12. wykrycie ilości uruchomionych procesów w zadanym okresie czasu,
13. wykrycie skanowania portów.

54. Reguły korelacyjne bazujące na listach referencyjnych muszą umożliwić:

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

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

1. wykrycie czy zdarzenie pochodzi od użytkownika posiadającego konto w Active Directory,
2. wykrycie czy zdarzenie pochodzi od użytkownika posiadającego uprzywilejowane konto w Active Directory,
3. 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).
4. wykrycie czy zdarzenie pochodzi od użytkownika należącego do wybranej grupy w Active Directory (np.: Domain Admins),
5. wykrycie czy zdarzenie pochodzi od użytkownika nie należącego do wybranej jednostki organizacyjnej.

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

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

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

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

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

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

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

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

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

1. wykrycie anomalii ilościowej związanej z komputerem wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania,
2. wykrycie anomalii związanej ze zmianą zachowania komputera, wskazującej na potencjalny atak APT/Ransomware,
3. wykrycie różnych typów anomalii na komputerze, wskazujących na możliwe przejecie komputera przez cyberprzestępcę lub złośliwe oprogramowanie,
4. wykrycie anomalii związanych z procesami uruchamianymi na serwerach.

61. Reguły korelacyjne wykorzystujące podatności na zasobach muszą umożliwić:

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

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

1. wykrycie wielokrotnych prób nieudanego logowania do komputera, umożliwiającego ustawienie hasła zawierającego mniej niż 14 znaków,
2. 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:

1. wykrycie zdefiniowanej ilości technik w zdarzeniach dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP,
2. wykrycie zdefiniowanej ilości zdarzeń w ramach jednej techniki dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP,
3. 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.:

1. wykrycie anomalii na koncie uprzywilejowanym użytkownika,
2. wykrycie ruchu z serwera domenowego do skompromitowanej domeny wykazanej w liście referencyjnej,
3. wykrycie wielu typów anomalii na komputerze z krytyczną podatnością,
4. wykrycie złośliwego oprogramowania na bazie wskaźnika kompromitacji stanowiącego HASH procesu, z którego następuje nieautoryzowana próba dostępu do usługi,
5. 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:

1. sparsowane pola oraz ich wartości,
2. atrybuty użytkowników z Active Directory,
3. atrybuty komputerów z Active Directory,
4. 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:

1. adresie IP,
2. koncie domenowym użytkownika,
3. strefie bezpieczeństwa,
4. 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 zamianę 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.

1. wszystkie skorelowane zdarzenia,
2. korespondencja pocztowa,
3. załączniki z próbkami lub dowodami,
4. wskaźniki kompromitacji (IoC),
5. 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 rozdzielenia 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:

1. identyfikację celu i źródła zagrożenia,
2. nazwę oraz adres IP źródła zagrożenia,
3. rodzaj zasobu będący źródłem zagrożenia np.: urządzenie mobilne, stacja robocza,
4. lokalizację z które pochodzi zagrożenie np.: Internet,
5. strefę bezpieczeństwa z której pochodzi zagrożenie,
6. prawdopodobieństwo zagrożenia ze strefy stanowiącej jego źródło,
7. wszystkie urządzenia sieciowe chroniące cel zagrożenia i zastosowane na nich mechanizmy zabezpieczeń (np.: Application Control, Network Firewall, User Identification),
8. nazwę oraz adres IP celu zagrożenia,
9. zabezpieczenia lokalne chroniące cel zagrożenia,
10. 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:

1. nazwy zasobu,
2. rodzaju zasobu,
3. ważności zasobu dla organizacji,
4. rodzaj przetwarzanych informacji,
5. usług, które ten zasób świadczy,
6. lokalizację użytkowników, którzy z niego korzystają,
7. 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:

1. nowe zdarzenie – jako zdarzenie zarejestrowane w systemie,
2. segregacja – segregacja i kwalifikacja zdarzeń,
3. incydent bezpieczeństwa – zdarzenie zakwalifikowane jako incydent bezpieczeństwa,
4. fałszywy alarm – zdarzenie zakwalifikowane jako fałszywy alarm,
5. zdarzanie obsłużone – zdarzenie, które zostało obsłużone 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 obsługiwanym 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:

1. podgląd aktywności zagrożonego zasobu na linii czasu,
2. w przypadku zagrożenia sieciowego podgląd aktywności zarówno ofiary jak i celu ataku,
3. w przypadku identyfikacji użytkownika podgląd jego aktywności na linii czasu,
4. podgląd reguły korelacyjnej, która wygenerowała zdarzenie,
5. w przypadku wykrytej techniki MITRE ATT&CK® jej szczegółowy opis,
6. listowanie podpiętych zdarzeń wraz z mechanizmami filtrowania po nich,
7. gotowe i proste w użyciu filtry rozszerzajcie 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,
8. gotowe i proste w użyciu filtry rozszerzajcie 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:

1. 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,
2. 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.
3. kanały powiadomień, m.in. e-mail, sms, komunikator,
4. 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:

1. utworzenia nowego zdarzenia z określonym priorytetem,
2. utworzenia nowego zdarzenia na zasobie krytycznym,
3. utworzenia nowego zdarzenia na zasobie realizującym zdefiniowaną usługę,
4. utworzenie nowego zdarzenia na zasobie przetwarzającym dane osobowe,
5. utworzenie nowego zdarzenia na podstawie zdefiniowanej reguły korelacyjnej,
6. modyfikacji przydzielonego operatorowi zdarzania przez innego operatora,
7. zamknięcia przydzielonego operatorowi zdarzania przez innego operatora,
8. przejęcia przydzielonego operatorowi zdarzania przez innego operatora.

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

1. wybór raportu, który ma zostać wysłany,
2. zdefiniowanie jego tytułu,
3. zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny,
4. możliwość ograniczenia cyklu do dni powszednich,
5. określenie daty przesłania pierwszego raportu,
6. możliwości ograniczenia okresu przez jaki raport będzie przesyłany, do:
   * zdefiniowanej daty końcowej,
   * określnej liczby raportów,
7. 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:

1. strefę bezpieczeństwa w której została wykryta podatność,
2. prawdopodobieństwo obecności intruza lub złośliwego oprogramowania w tej strefie,
3. rodzaj zasobu którego dotyczy ta podatność,
4. ważność tego zasobu dla organizacji,
5. przetwarzane na tym zasobie informacje, np.: dane osobowe,
6. usługi realizowane przez ten zasób, np.: DNS,
7. wartość parametrów CVSS dla podatności, np.: „Confidentiality Impact” = High,
8. poprawność konfiguracji zasobu na którym została wykryta podatność, np.: brak reguł wymuszenia złożoności haseł,
9. 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:

1. wyliczonym priorytecie podatności,
2. aktualnym statusie obsługi,
3. ważności zasobu na którym została wykryta,
4. adresie IP tego systemu,
5. parametrów SLA związanych z tym statusem,
6. przetwarzanych na zasobach informacji, np.: lista podatności dotycząca tylko systemów przetwarzających dane osobowe,
7. 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:

1. przekroczenia czasu reakcji o określony czas np.: o godzinę,
2. możliwości przekroczenia czasu reakcji, np.: została godzina aby rozpocząć obsługę zdarzenia i uchronić się przed przekroczeniem czasu reakcji,
3. przekroczenia czasu reakcji dla zdarzenia na zasobie przetwarzającym dane osobowe,
4. przekroczenia czasu reakcji dla zdarzenia na zasobie krytycznym,
5. przekroczenia czasu reakcji dla zdarzenia na zasobie realizującym krytyczną usługę,
6. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów przetwarzających dane osobowe,
7. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów krytycznych,
8. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów realizujących krytyczną usługę,
9. przekroczenia czasu reakcji dla podatności na zasobie przetwarzającym dane osobowe,
10. przekroczenia czasu reakcji dla podatności na zasobie krytycznym,
11. 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:

1. 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 informację,
   * zdarzeń przetwarzanych na krytycznych zasobach,
2. 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 obsługiwanym przez firmę zewnętrzną.
3. kanały powiadomień, m.in. e-mail, sms, komunikator,
4. 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:

1. przydzielenia nowej podatności do obsługi z określonym priorytetem,
2. przydzielenia nowej podatności do obsługi na zasobie krytycznym,
3. przydzielenia nowej podatności do obsługi na zasobie realizującym zdefiniowaną usługę,
4. przydzielenia nowej podatności do obsługi na zasobie przetwarzającym dane osobowe,
5. modyfikacji przydzielonej operatorowi podatności przez innego operatora,
6. zamknięcia przydzielonej operatorowi podatności przez innego operatora,
7. 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:

1. wybór raportu który ma zostać wysłany,
2. zdefiniowanie jego tytułu,
3. zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny,
4. możliwość ograniczenia cyklu do dni powszednich,
5. określenie daty przesłania pierwszego raportu,
6. określenie okresu przez jaki będą one przesyłane, poprzez:
   * zdefiniowanie daty końcowej,
   * bez daty końcowej,
   * określenie liczby raportów,
7. określenie odbiorców raportu.

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

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

1. zestaw wykresów dla bieżącego użytkownika,
2. zestaw wykresów dla wybranego użytkownika,
3. zestaw wykresów dla roli zdefiniowanej w systemie, np.: administratorzy systemu,
4. zestaw wykresów dla wybranego zespołu obsługi, np.: operatorzy SOC (Security Operations Center).

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

1. wykres przedstawiający status klasyfikacji zdarzeń, który uwzględnia:
   * ilość zdarzeń nowych i niesklasyfikowanych,
   * ilość zdarzeń sklasyfikowanych jako incydenty bezpieczeństwa,
   * ilość zdarzeń sklasyfikowanych jako fałszywe alarmy,
2. wykres przedstawiający skale zagrożeń, który uwzględnia:
   * ilość zasobów krytycznych na których są obsługiwane zdarzenia,
   * ilość zasobów niekrytycznych na których są obsługiwane zdarzenia,
3. 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,
4. wykres przedstawiający poziom zagrożeń, który uwzględnia:
   * ilość nowych zdarzeń w podziale na priorytety,
   * ilość podjętych zdarzeń w podziale na priorytety,
5. 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,
6. wykres przedstawiający zagrożone usługi, który uwzględnia:
   * ilość usług krytycznych zagrożonych przez obsługiwane zdarzenia,
   * ilość pozostałych usług zagrożonych przez obsługiwane zdarzenia,
7. 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,
8. wykres przedstawiający skale podatności, który uwzględnia:
   * ilość zasobów krytycznych na których są obsługiwane podatności,
   * ilość zasobów niekrytycznych na których są obsługiwane podatności,
9. 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,
10. 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:

1. „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,
2. „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,
3. „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,
4. „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,
5. „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,
6. „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 zintegrowanej platformy 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 tyś 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 muszę 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 tyś 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 Inteligence 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 wpierać 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) lub być oprogramowaniem hybrydowym (tj. zbudowanym na bazie otwartoźródłowego) w następującym zakresie funkcjonalnym: zbieranie, przesyłanie, składowanie, parsowanie (przetwarzanie), korelacja i zarządzanie logami, wykresy danych (dashboard), algorytmy uczenia maszynowego, analiza zachowania użytkowników i zasobów, mechanizmy reakcji/ scenariusze reakcji. Zamawiający nie zaakceptuje systemu, który wykorzystuje mechanizmy typu open source np.: Elastic Search, Kibana, Logstash, OSSIM, Snort, The Hive, AlienVault itd. lub został stworzony przez modyfikację oprogramowania otwartego. Dostarczone rozwiązanie musi być oprogramowaniem własnościowym (proprietary), opracowanym i rozwijanym przez zespół techniczny producenta oraz oferowanym w sprzedaży na rynku polskim od co najmniej 10 lat.

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 funkcjonalności 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 licencje 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 wsparciem producenta na okres trwałości projektu tj. 36 miesięcy. 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 błędu krytycznego lub poważnego).

146. Zamawiający oczekuje, że w ramach dostarczonego systemu Wykonawca zrealizuje - po zakończonym wdrożeniu - na rzecz Zamawiającego dodatkową usługę wsparcia powdrożeniowego w łącznym zakresie 5 roboczodni (MD). W ramach dodatkowego wsparcia powdrożeniowego Wykonawca jest zobowiązany dostroić oferowaną platformę w 3 obszarach:

a) Modelowania zagrożeń w oparciu o MITRE ATT&CK Matrix, z wykorzystaniem mechanizmów szacowania ryzyka i z uwzględnieniem TTPs (tactics, techniques, procedures) stosowanych przez cyberprzestępców wraz z mapowaniem zagrożeń do istniejących zabezpieczeń organizacji (wykonanie dokumentacji analizy w systemie);

b) Stworzenia dodatkowych reguł korelacyjnych o charakterze kontekstowym  (osadzone w rzeczywistych procesach i architekturze organizacji) w oparciu o wykonane wcześniej modelowanie zagrożeń - opracowanie do 10 nowych reguł korelacyjnych;

c) Przygotowania nowych playbooków (scenariuszy reakcji), dostosowanych do potrzeb operacyjnych Zamawiającego i jego wewnętrznych procedur reagowania na incydenty. Scenariusze zostaną projektowane z uwzględnieniem architektury systemów, procesów oraz klasyfikacji incydentów - opracowanie do 2 nowych playbooków.

Celem zachowania wysokiej jakości usługi, Zamawiający wymaga by dodatkowe wsparcie powdrożeniowe w opisanym wyżej zakresie zostało zrealizowane przez osoby zatrudnione w firmie Wykonawcy, posiadające co najmniej następujące, ważne certyfikaty:

a) CISM - Certified Information Security Manager:

b) CISA - Certified Information Systems Auditor;

c) CRISC - Certified in Risk and Information Systems Control;

d) BCMS Business Continuity Management Systems Auditor;

e) ITIL Foundation Certificate in IT Service Management.

147. 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.

148. Wykonawca zapewni bezpłatne szkolenia w zakresie użytkowania i administrowania wdrożonego systemu lub systemów. Szkolenie ma zostać przeprowadzone dla maksymalnie 10 osób i muszą być zakończone przyznaniem certyfikatu, potwierdzającego wspomniane umiejętności wydanym przez producenta systemu/ systemów. Szkolenia mogą odbyć się w formie zdalnej.

149. Zmawiający 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 ciagu 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.

150. 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. Próbka 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 9 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 | |  | |
| l.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 które 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 rozszerzajcie 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 rozszerzajcie 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 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. | |
| 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 jaki i możliwość ich wyłączenia z obsługi w przypadku znikomego zagrożenia dla organizacji. | |
|  |  |  |

1. **Dodatkowe wymagania dla Wykonawcy**

Wykonawca jest zobowiązany zapewnić w ramach oferty pełne, prawidłowe i zgodne z przeznaczeniem działanie oferowanego oprogramowania.

W przypadku, gdy uruchomienie, eksploatacja lub prawidłowe funkcjonowanie oferowanego oprogramowania wymaga posiadania dodatkowych licencji na inne składniki programowe, w szczególności systemy operacyjne, bazy danych, platformy serwerowe, lub inne oprogramowanie pośredniczące – wykonawca jest zobowiązany do ujęcia tych elementów w ofercie wraz z odpowiednimi licencjami.

Wykonawca ponosi pełną odpowiedzialność za kompletność środowiska uruchomieniowego i zapewnienie niezbędnych licencji wymaganych do poprawnego działania oferowanego produktu.

W ofercie należy przedstawić wykaz wszystkich składników programowych oraz licencji niezbędnych do uruchomienia rozwiązania z wyszczególnieniem producenta, wersji oraz liczby wymaganych licencji.

Brak ujęcia w ofercie dodatkowych licencji wymaganych do uruchomienia lub działania oprogramowania nie zwalnia wykonawcy z obowiązku ich dostarczenia w ramach ceny oferty.