

## PAKIET II - Zakup rozwiązania klasy SIEM oraz EDR

### 1. Zakup rozwiązania klasy Security Information and Event Management dla Urzędu Miejskiego Śmigła.

<b>Wymagania dla systemu klasy Security Information and Event Management</b>
System musi być oparty o nowoczesną nierelacyjną bazę danych typu noSQL
System musi pracować w oparciu o architekturę OS w licencji open source.
System musi mieć możliwość centralnego zbierania i zarządzania logami
System działać w trybie zbliżonym do rzeczywistego
System musi umożliwiać funkcjonowanie bez dostępu do sieci internet
System musi mieć możliwość działania jako niezależne instancje zainstalowane w oddziałach Zamawiającego wraz z możliwością centralnego dostępu.
Instancje systemu muszą mieć możliwość działania w przypadku odłączenia scentralizowanego dostępu.
System musi zapewniać efektywną obsługę do 20 GB danych dziennie
System musi zapewniać retencję danych w okresie minimum 30 dni.
Oferowany system nie może ograniczać ilości zarejestrowanych lub jednoczesnych użytkowników systemu.
Licencja na oferowany system nie może ograniczać ilości źródeł danych, z których pobierane są dane i zdarzenia.
System musi umożliwiać rozbudowę bez potrzeby wyłączania lub restartu środowiska.
Architektura rozwiązania musi umożliwiać rozdzielenie ról systemu pomiędzy osobne komponenty (serwery/maszyny wirtualne). Należy przewidzieć rozdzielenie przynajmniej 3 typów ról: Agregacja, Prezentacja, Retencja.
Dołączenie nowego węzła przetwarzania, prezentacji lub przechowywania pozwalającego na skalowanie wydajności. Rozszerzenie takie powinno odbywać się bez konieczności restartu działającego systemu.
Interfejs musi posiadać angielską lub polską wersję językową.

System musi być tworzony zgodnie z zaleceniami standardu OWASP Testing Guide, a w szczególności OWASP - TOP 10 (Open Web Application Security Project). Projektowany System powinna spełniać wymagania standardu OWASP ASVS (Application Security Verification Standard) w wersji 4.0 co najmniej na poziomie pierwszym (L1).

System musi zapewniać pełen audyt aktywności jego użytkowników, w tym: udanych/nieudanych logowaniach, pełnej historię operacji, realizowanych zapytań, zmian uprawnień.

System musi umożliwiać ręczne ustawianie poziomu szczegółowości gromadzonych danych audytowych.

System musi posiadać autoryzowane przez producenta narzędzie/moduł do kontroli wydajności dostarczonego systemu. Wsparcie producenta musi obejmować zakresem również to narzędzie.

System musi zapewniać mechanizmy umożliwiające pracę w trybie multitenant.

System musi pozwalać na tworzenie parserów z poziomu GUI

System musi umożliwiać predykcję danych w oparciu o dowolne dane historyczne zgromadzone w systemie.

System musi zapewniać budowę modeli prognostycznych w oparciu o metody matematyczne i statystyczne tzw. Machine Learning.

System musi być wyposażony w zaawansowane metody analizy danych oparte na algorytmach sztucznej inteligencji.

Algorytmy sztucznej inteligencji muszą umożliwiać przewidywanie zachowań systemu poprzez zrozumienie liczby generowanych zdarzeń oraz wartości liczbowych w tych zdarzeniach, takich jak wysłane bajty (sent\_bytes), rozmiar pliku (file\_size) i czas trwania sesji (session\_duration).

Algorytmy sztucznej inteligencji muszą wspierać pracę operatora w wykrywaniu anomalii w danych: pojedynczego parametru liczbowego, wielu parametrów liczbowych, tekstu oraz danych mieszanych. Oczekuje się, że wykrywanie anomalii będzie połączone z obliczaniem punktów, co umożliwi operatorowi skoncentrowanie swojej pracy na zdarzeniach o najwyższych wynikach.

Algorytmy sztucznej inteligencji muszą umożliwiać nienadzorowane, dynamiczne grupowanie zdarzeń na podstawie ich wspólnych cech. Dodatkową wartością będzie możliwość graficznej wizualizacji zdarzeń tworzących większe lub mniejsze grupy, aby izolowane zdarzenia można było łatwo zidentyfikować.

Wykrywanie anomalii musi umożliwiać tworzenie reguł detekcji, aby możliwa była szybka reakcja w sytuacjach, które się pojawiają.

Algorytmy sztucznej inteligencji musi umożliwiać nienadzorowane, dynamiczne grupowanie zdarzeń na podstawie ich wspólnych cech. Dodatkową wartością będzie możliwość graficznej wizualizacji zdarzeń tworzących większe lub mniejsze grupy, aby izolowane zdarzenia można było łatwo zidentyfikować.

Wykrywanie anomalii musi umożliwiać tworzenie reguł detekcji, aby możliwa była szybka reakcja w sytuacjach, które się pojawiają.

System musi posiadać wbudowaną funkcjonalność badania zachowania użytkowników oraz urządzeń (UEBA), która będzie oparta na danych pochodzących ze zgromadzonych logów oraz analizowanych za pomocą algorytmów sztucznej inteligencji.

Oferowana funkcjonalność UEBA musi zawierać wbudowane wizualizacje, kokpity oraz zestawy spredefiniowanych modeli analizy opartych na algorytmach sztucznej inteligencji.

System musi zapewniać wizualizację danych w postaci, oryginalnych logów, list, wykresów i diagramów.

System musi umożliwiać graficzną wizualizację zidentyfikowanych połączeń sieciowych pomiędzy adresami IP.

Wizualizacja danych powinna być również możliwa dla wartości tekstowych jak i liczbowych przekazywanych w logach.

System musi umożliwiać funkcjonalność eksportu danych o Zdarzeniach i Incydentach do formatu CSV i HTML m.in. w celu analizy wyników działania reguł korelacyjnych.

System musi zapewniać parsowanie wpływających do niego wiadomości w formatach: Syslog, WEF, Flat file, Event log, WMI, SNMP trap, XML, JSON, JDBC/ODBC, CSV, Email, jak również musi pozwalać na implementację innych formatów w przypadku zaistnienia takiej potrzeby ze strony Zamawiającego.

System musi zbierać logi z rozwiązań chmurowych opartych minimum o AWS oraz Microsoft Azure.

System musi umożliwiać gromadzenie danych z baz danych relacyjnych, NoSQL, czasu rzeczywistego, m.in. MSSQL, Oracle, PostgreSQL, SQL Server, MongoDB, Apache Cassandra, InfluxDB i Apache Kafka

System musi umożliwiać prezentację logu o zdarzeniu w interfejsie użytkownika w takiej formie w jakiej ten log został przesłany do Systemu tj. wyświetlenie logu w postaci surowej (RAW) przed parsowaniem.

System musi do przyjmowania zdarzeń wykorzystywać zarówno mechanizmy agentowe jak i bezagentowe.

Operacja z rekordami bazy danych muszą być wykonywane jedynie za pomocą składni JSON z wykorzystaniem udokumentowanego API.

Wykorzystanie bazy danych musi odbywać się za pomocą REST API z pominięciem wykorzystania klienta typu SQL client.

System musi umożliwiać definiowanie parserów dla niestandardowych formatów logów w oparciu o składnię wyrażeń regularnych oraz formatów wymiany danych dla wszystkich obsługiwanych formatów.

Interfejs musi umożliwić parsowanie warunkowe na podstawie dopasowania wartości pól. Po dopasowaniu wzorca dalsze parsowanie powinno być konfigurowalne w celu wyboru optymalnej metody parsowania, np.: REGEX, JSON, XML oraz umożliwiać zastosowanie innego parsera.

System musi posiadać predefiniowany zestaw parserów zdarzeń.

System musi mieć funkcjonalność Bad IP Reputation tj. porównywania adresów IP z bazami reputacyjnymi dostarczonymi przez producenta.

System musi wspierać geolokalizację zdarzeń na bazie adresów IP.

System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, np. dzięki zmianie wartości tych pól oraz wzbogacaniu tych danych o dodatkowe pola bazując na całych wartościach lub wzorcach wyszukiwania.

System musi umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach.

Proces parsowania musi umożliwiać wzbogacanie treści obieranych Wiadomości poprzez matematyczne operacje wykonywane na innych polach.

Proces parsowania musi umożliwiać anonimizację Danych Wejściowych celem ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzny procedury bezpieczeństwa.

System musi pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych

System musi pozwalać na rozpoznanie formatów czasu i daty oraz normalizowanie ich do jednego wspólnego formatu.

System musi posiadać wbudowany komponent budowania elektronicznej dokumentacji z możliwością ręcznego i automatycznego dodawania treści oraz uzupełniania jej o wartości pochodzące ze zgromadzonych w Systemie danych.

Komponent budowania elektronicznej dokumentacji musi mieć możliwość m.in. tworzenia lub dodawania diagramów architektury zasobów informatycznych, tabel oraz list.

System musi umożliwiać łączenie wyników dwóch niezależnych zapytań w postaci jednej odpowiedzi, bez użycia składni SQL.

System musi posiadać interfejs umożliwiający zmianę wybranej wartości w zgromadzonych danych.

Incydent, który powstał w wyniku korelacji, musi dać się wyszukiwać korzystając ze standardowego dostępnego w systemie mechanizmu wyszukiwania. System musi umożliwiać budowanie na jego podstawie kolejnych reguł korelacyjnych lub generowania alarmów.

System musi umożliwiać budowanie zapytań z wykorzystaniem składni SQL oraz Piped Processing Language (PPL).

System musi posiadać funkcjonalność korelacji danych w czasie rzeczywistym.

System musi umożliwiać tworzenie nowych reguł korelacyjnych oraz modyfikowanie istniejących.

System musi umożliwiać tworzenie własnych reguł korelacyjnych na bazie reguł odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie, w tym:

- Wykrycia dowolnej treści w logach,
- Wykrycia wystąpienia wartości pola na wybranej liście,
- Wykrycia niewystępowania wartości pola na wybranej liście,
- Wykrycia zmiany jednego z kilku pól,
- Wykrycia zdarzeń występujących z zadaną częstotliwością,
- Wykrycia zdarzeń, których liczba zmienia się w wskazany sposób względem czasu poprzedniego,
- Wykrycia zaniku Wiadomości,
- Wykrycia nowej wartości pola w zadanym okresie czasu,
- Wykrycia incydentu będącego pochodną zdarzeń występujących w określonej kolejności

System musi pozwalać na tworzenie własnych algorytmów ewaluacji Incydentów

Reguły korelacji oraz algorytmy ewaluacji incydentów muszą być możliwe do dodawania lub modyfikacji z poziomów zarówno GUI jak i API.

System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.

System musi pozwalać na realizację zapytań obejmujących całą historię gromadzonych w nim danych.

System musi umożliwić korelację zdarzeń pochodzących z różnych źródeł informacji z anomaliami wykrywanymi m.in. w. Netflow oraz wykrytymi podatnościami zidentyfikowanymi przez skaner podatności

System musi umożliwiać analizę ruchu sieciowego poprzez przechwytywanie i inspekcję pakietów w czasie rzeczywistym, w tym minimum protokołów HTTP DNS, FTP oraz SSH.

System na bazie gromadzonej kopii ruchu sieciowego musi identyfikować i klasyfikować ataki w oparciu o sygnatury oraz zachowanie użytkowników.

System musi umożliwiać zapisywanie pakietów ruchu sieciowego w formacie PCAP.

System musi umożliwiać gromadzenie i analizowanie danych Netflow, w tym: IPFIX, sFlow, J-Flow, Netflow v9.

System musi zapewnić mechanizmy obsługi incydentów i wymiany informacji pomiędzy operatorami systemu w tym przypisanie incyduentu do operatora i zmiana jego statusu.

System musi posiadać funkcjonalność tworzenia scenariuszy obsługi incyduentu tzw. Playbook

System musi automatycznie podpowiadać odpowiednie scenariusze obsługi incyduentów.

Scenariusze muszą mieć możliwość ich symulacji i weryfikacji, m.in. na przykładowym zasobie IT.

System musi pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących.

Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień o Incydentach do innych systemów bądź zdefiniowanych użytkowników (co najmniej: powiadamianie email, opcjonalnie SMS, czat).

System musi umożliwiać testowanie reguł korelacyjnych i alertów na etapie ich tworzenia. Wynik testu nie może tworzyć wpisu o sytuacji alarmowej i ewentualnego incyduentu.

System musi pozwalać na zautomatyzowane szacowanie ryzyka dla dowolnych kryteriów w ramach przetwarzanych zdarzeń. W rozwiązaniu musi być obecna funkcjonalność. kategoryzacji obiektów (adresy IP, loginy i inne pola), dla których mechanizm szacowania ryzyka uwzględni podane wagi.

System umożliwia konfigurację automatycznych akcji, które są wykonywane na monitorowanych systemach w przypadku detekcji zagrożenia wskazanego w regule

Tworzone incydenty będące wynikiem pracy reguł bezpieczeństwa muszą posiadać wbudowany poziom istotności. Musi istnieć możliwość modyfikacji poziomu istotności dla każdej reguły.

System musi posiadać wbudowany, dostępny z poziomu GUI moduł tworzenia i edycji elektronicznej dokumentacji bazującej oraz wzbogacającej dane gromadzone ze środowiska informatycznego.

System musi umożliwiać zakup licencji wieczystych wraz ze wsparciem producenta na okres 5 lat.

Oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów.

System musi umożliwiać czasowe przyjęcie zwiększonej ilości danych o minimum 30% bez potrzeby zwiększania zasobów sprzętowych lub licencyjnych.

Wykonawca wraz z licencją produkcyjną Wykonawca zobligowany jest dostarczyć licencję na potrzeby środowiska testowego, która umożliwi przetwarzanie minimum 1 000 EPS.

Licencja testowa musi być objęta supportem producenta na takich samych zasadach jak licencja produkcyjna.

### **Dostęp do systemu**

Komunikacja pomiędzy komponentami systemu odpowiadającymi za agregacji, retencję i wizualizację danych musi odbywać się w sposób szyfrowany z wykorzystaniem protokołu TLS w wersji minimum 1.3.

Szyfrowanie komunikacji z przeglądarką internetową użytkownika musi wykorzystywać protokół TLS w wersji minimum 1.3.

System musi posiadać interfejs graficzny dostępny z poziomu przeglądarki internetowej min. Firefox, Chrome, Internet Explorer.

Dostęp do systemu musi być zabezpieczany hasłem lub certyfikatem.

Autoryzacja do systemu musi być zintegrowana z: Microsoft AD, LDAP, Radius

Hasła typu Windows AD bind muszą być przechowywane w postaci zaszyfrowanej.

System musi wspierać mechanizm logowania typu Single Sign On.

System musi umożliwiać zarządzanie czasem automatycznego wygasania sesji użytkowników.

System musi posiadać dedykowany widok zarządzania użytkownikami i rolami.

System powinien umożliwiać zarządzanie uprawnieniami do modyfikacji wytworzonych w systemie obiektów tj. wyszukiwania, wizualizacje, dashboardy. Dla utworzonych ról musi istnieć możliwość przypisania wspomnianych obiektów w podziale na dostęp typu „read only” oraz „pełny”. Obiekty, do których grupa nie ma dostępu, nie mogą być widoczne dla użytkownika.

### **Przyjmowanie, identyfikacja i wizualizacja danych**

Musi istnieć możliwość automatycznego importu informacji IoC (ang. Indicator Of Compromise), a następnie automatyczne przeszukiwanie wśród zgromadzonych zdarzeń w wyznaczonym czasie.

System musi posiadać natywną integrację z bazą MISP min. Adresy IP, hash zainfekowanych plików, adresy domen, adresy URL.

System musi być dostarczony z repozytorium danych IoC utrzymywanym i rozwijanym przez producenta.

System posiada natywną integrację z Mitre ATT@CK.

### **Reguły korelacyjne, alerty i obsługa incydentów**

System musi posiadać bazę minimum 700 predefiniowanych reguł korelacyjnych



System musi dostarczać funkcjonalność badania integralności plików i rejestrach na monitorowanych hostach, w tym: monitorowanie zmian na zawartości plików i katalogów, zmiany uprawnień dostępu do pliku, zmiany w atrybutach plików oraz zmian na sumach kontrolnych MD5 i SHA1.

System musi posiadać funkcjonalność monitorowania konfiguracji systemów oraz aplikacji w celu zapewnienia zgodności z politykami i standardami bezpieczeństwa oraz praktykami dotyczącymi hardeningu, takimi jak CIS Benchmark.

System musi posiadać gotowe wizualizacje i polityki zgodności z GDPR, PCI-DSS, NIST, ISO 27001

System musi posiadać możliwość skanowania środowiska pod kątem detekcji rootkit'u i wykrywania ukrytych procesów, plików, portów

System musi posiadać funkcjonalności skanowania podatności dla aplikacji oraz systemów operacyjnych Linux i Windows

System musi posiadać funkcjonalność ciągłego śledzenia polityk OpenSCAP

### **Raportowanie i Archiwizacja danych**

System musi zapewniać wbudowany mechanizm archiwizacji danych w postaci plików płaskich oraz ich zarządzaniem z poziomu konsoli użytkownika.

Mechanizm archiwizacji musi posiadać funkcjonalność przesyłania danych online do archiwum według zadanych kryteriów w sposób automatyczny lub ręczny.

Mechanizm archiwizacji musi umożliwiać pozwalając na przywracanie danych do systemu celem analizy online.

Mechanizm archiwizacji musi zapewniać funkcjonalność wyszukiwania w spakowanych danych bez potrzeby ich wcześniejszego rozpakowania.

System musi zapewniać funkcjonalność generowania raportów z dowolnych danych gromadzonych w systemie.

Raporty muszą być generowane ręcznie oraz automatycznie według zdefiniowanego harmonogramu.

System musi generować raporty do formatów minimum PDF, docx oraz JPEG z jednoczesną możliwością opatrywania dokumentu logo Zamawiającego oraz komentarzami.

### **Lista źródeł**

**Zależnie od chęci Zamawiającego można podać listę systemów źródłowych objętych wdrożeniem.**

### **Wdrożenie**



Zakres oczekiwanych prac związanych z wdrożeniem systemu:
Opracowanie harmonogramu wdrożenia systemu.
Przeprowadzenie przez Wykonawcę analizy przedwdrożeniowej oraz projektu technicznego wdrożenia.
Przeprowadzenie instalacji i konfiguracji systemu.
Podłączenie do systemu wskazanych przez Zamawiającego w OPZ źródeł danych.
Do podłączonych źródeł Wykonawca musi skonfigurować reguły korelacyjne, raporty oraz dashboards z wykorzystaniem gotowych komponentów dostarczonych wraz z systemem.
Jeżeli oferowany system nie posiada predefiniowanych parserów, wizualizacji, dashboardów oraz reguł korelacyjnych Wykonawca jest zobligowany do ich implementacji na etapie wdrożenia.
Wykonawca na etapie analizy przedwdrożeniowej przedstawi do akceptacji Zamawiającego listę proponowanych reguł korelacyjnych, wizualizacji oraz dashboardów odnoszących się do zidentyfikowanych źródeł danych.
Przygotowanie i przeprowadzenie scenariuszy testowych weryfikujących wydajność i poprawność wdrożonego systemu w środowisku Zamawiającego.
Proponowane scenariusze będą przedłożone Zamawiającemu do akceptacji.
<b>Szkolenia</b>
Wykonawca przeprowadzi szkolenia z zakresu użytkowania oraz administrowania systemem dla pracowników zamawiającego w wymiarze 2 dni roboczych (min. 16h roboczych).
Grupa szkoleniowa będzie miała nie więcej niż 10 słuchaczy.
Szkolenie odbędzie się w siedzibie Zamawiającego.
Szkolenie musi być prowadzone w języku polskim.
Każdy uczestnik szkolenia otrzyma materiały szkoleniowe przygotowane w języku polskim lub angielskim.
Osoby prowadzące szkolenie muszą posiadać certyfikat wystawiony przez producenta oferowanego rozwiązania potwierdzające ich kompetencje w zakresie użytkowania i administrowania systemem.
<b>Utrzymanie systemu</b>
Dokumentacja techniczna i baza wiedzy dotycząca oferowanego systemu musi być opublikowana na ogólnodostępnej stronie internetowej producenta.

Producent musi zapewnić dostęp do oficjalnego portalu społeczności użytkowników systemu, który umożliwia wymianę informacji, zadawanie pytań, zgłaszanie problemów oraz komunikację z inżynierami producenta i innymi użytkownikami.

W ramach wykupionego wsparcia producenta, Zamawiający powinien mieć zapewniony dostęp do nowych wersji oprogramowania, aktualizacji (patchy) oraz repozytorium danych wskaźników kompromitacji (IoC).

### **Infrastruktura**

Zamawiający zapewnia niezbędną infrastrukturę techniczną wymaganą do uruchomienia systemu. Strony określają wymagania dotyczące niezbędnego środowiska produkcyjnego na etapie tworzenia projektu technicznego.

### **Integracja z SOAR**

Dodatkowo Zamawiający w ramach kryterium oceny ofert będzie oceniać możliwość rozbudowy oferowanego rozwiązania o moduł funkcjonalny SOAR lub zapewnienie gotowej integracji z systemem SOAR tego samego producenta.

## **2. Zakup systemu Endpoint Protection Platform (EPP) i Endpoint Detection & Response (EDR) dla Urzędu Miejskiego Śmigła**

### **Wymagania EPP:**

1. Rozwiązanie musi opierać się wyłącznie na sztucznej inteligencji i uczeniu maszynowym jako podstawowych funkcjach zapobiegania złośliwemu oprogramowaniu.
2. EPP zastosuje analizę algorytmiczną kodu w celu zidentyfikowania złośliwego oprogramowania przed jego wykonaniem.
3. Rozwiązanie musi mieć możliwość raportowania niechronionych urządzeń w Active Directory.
4. Rozwiązanie nie może polegać na piaskownicy, wyszukiwaniu sygnatur ani heurystyce w celu zapobiegania złośliwemu oprogramowaniu.
5. Agentem należy zarządzać za pośrednictwem centralnej konsoli administracyjnej dostępnej w architekturze chmurowej, hybrydowej, lub on-prem, także w środowisku pozbawionym dostępu do Internetu.
6. Uwierzytelnianie w konsoli zarządzania powinno być kontrolowane i audytowane.
7. Konsola musi zapewniać dashboard, który będzie agregował alerty z różnych rozwiązań: EPP, oraz EDR i ZTNA tego samego producenta, oraz grupował je z uwzględnieniem różnych priorytetów, minimum 5 poziomów od najniższego do najbardziej krytycznego.
8. Rozwiązanie musi obsługiwać zarządzanie dostępem w oparciu o role, ograniczając kontrolę konsoli do określonych administratorów.
9. Rozwiązanie musi umożliwiać zarządzanie segmentowe w oparciu o różne grupy urządzeń (każdy Administrator zarządza tylko grupą urządzeń).
10. Komunikacja pomiędzy agentami a konsolą zarządzającą powinna być szyfrowana.
11. Rozwiązanie musi zostać wyróżnione tytułem Customers' Choice for Endpoint Protection Platforms for Large Enterprise przez Gartner Peer Insights co najmniej raz w ciągu ostatnich 2 lat.
12. Agent EPP na urządzeniach musi mieć możliwość statycznego skanowania plików przed wykonaniem i wykrywania wszelkich niebezpiecznych plików.

13. Rozwiązanie powinno mieć sprawdzoną historię blokowania ataków Zero-Day i oprogramowania ransomware poprzez analizę plików statycznych.
14. Rozwiązanie musi zawierać moduł blokujący ataki Fileless i wykrywający szkodliwe procesy w pamięci RAM na punktach końcowych.
15. EPP nie zezwala na uruchomienie oprogramowania uznanego za złośliwe.
16. EPP zapewnia ochronę przed uruchomieniem złośliwego oprogramowania w różnych formatach PE (rozszerzenia: exe, dll, sys, ocx, oraz scr) dla systemu Windows, formatu ELF dla systemu Linux, oraz Mach-O dla systemu MacOS.
17. Rozwiązanie musi być w stanie wykryć i zakończyć ataki i exploity oparte na pamięci, takie jak odczyty LSASS, przesunięcia stosu itp.
18. Rozwiązanie musi zapewniać szczegółową kontrolę złośliwych skryptów, w tym Powershell, Active Script, Python, skryptów .NET i makr XLM.
19. Identyfikacja potencjalnie niechcianych programów (PUP), takich jak oprogramowanie reklamowe, paski narzędzi, generatory kluczy, cracki i toolbary
20. EPP musi obsługiwać instalację pojedynczego agenta na serwerach, laptopach, urządzeniach mobilnych i stacjach roboczych.
21. EPP musi wspierać zabezpieczanie środowisk VDI (trwałe i nietrwałe)
22. Agent EPP powinien wspierać platformy Windows, MacOS i Linux, w tym starsze systemy operacyjne (takie jak Windows XP, Windows Vista i Windows 2003 Server), także w środowiskach pozbawionych stałego dostępu do sieci
23. EPP musi obejmować mobilną ochroną przed zagrożeniami systemy iOS i Android.
24. Rozwiązanie EPP powinno wykorzystywać na 4-rdzeniowym urządzeniu z 4 GB pamięci RAM z systemem Windows w stanie bezczynności mniej niż 100 MB pamięci RAM i 5% procesora.
25. Rozwiązanie EPP powinno wykorzystywać 4-rdzeniowe, 4 GB pamięci RAM, urządzenie z systemem Windows w stanie aktywnym, na którym znajduje się ponad 200 złośliwych programów, mniej niż 200 MB pamięci RAM i 20% procesora.
26. Rozwiązanie EPP powinno chronić przed dezinstalacją/zamknięciem usługi na punkcie końcowym. Nawet lokalni administratorzy nie powinni mieć możliwości odinstalowania agenta.
27. EPP musi umożliwiać automatyczne przypisywanie zasad w oparciu o charakterystykę urządzenia (taką jak IPv4, członkostwo w grupie, wersja systemu operacyjnego).
28. EPP musi dostarczać szczegółowych informacji na temat blokowanych zagrożeń.
29. EPP będzie identyfikować i blokować działania zarówno złośliwego kodu wykonywalnego, jak i złośliwych skryptów lub poleceń.
30. EPP wykrywa i zapobiega nieautoryzowanym lub złośliwym zmianom w kodzie programów działających w pamięci systemowej.
31. EPP będzie działać równie dobrze zarówno w sieciach podłączonych do Internetu, jak i w sieciach izolowanych/odłączonych.
32. EPP zapewni szczegółowe opcje umieszczania na białej liście według skrótu pliku, katalogu folderów lub certyfikatu.
33. EPP zapewni szczegółowe opcje wykluczeń, które można zastosować dla każdego urządzenia, zasady lub globalnie.
34. EPP NIE może wymagać połączenia z Internetem lub siecią w celu wykrycia znanych lub nieznanych zagrożeń.
35. Rozwiązanie będzie obsługiwać opcję wdrażania hybrydowego, aby obsłużyć maszyny odłączone/ z przerwami w dostępie do Internetu.
36. EPP NIE może wymagać częstych aktualizacji (minimum co 6 miesięcy).
37. EPP NIE może polegać na analizie zachowań ani analizie heurystycznej w celu identyfikacji złośliwego oprogramowania.
38. EPP NIE może polegać na „białych listach” znanego, dobrego oprogramowania w celu zezwolenia lub odmowy wykonania.

39. EPP powinien zapewniać odpowiednią klasyfikację zidentyfikowanych zagrożeń, takich jak złośliwe oprogramowanie, oprogramowanie ransomware, generator kluczy, PUP, bot, trojan, narzędzie hakerskie itp.
40. Rozwiązanie EPP powinno umożliwiać integrację z dowolnymi komercyjnymi rozwiązaniami SIEM dostępnymi na rynku.
41. EPP powinien obsługiwać kontrolę USB z białą/czarną listą USB na podstawie numerów seryjnych i producenta USB.
42. EPP powinien obsługiwać kontrolę USB z białą/czarną listą USB w oparciu o mobilny system operacyjny, taki jak iOS i Android.
43. EPP powinien być w stanie utwardzać urządzenia w oparciu o dodatkowy tryb kontroli aplikacji. Po utwardzeniu komputera nie należy zezwalać na uruchamianie żadnych plików wykonywalnych a także na dodawanie nowych czy modyfikację już istniejących.
44. EPP powinien być w oparciu o tryb kontroli aplikacji, zapewnić opcję tymczasowego okna serwisowego w celu umożliwienia, edytowania i uruchamiania nowych aplikacji lub wykonywania aktualizacji.
45. EPP powinien być w stanie zatrzymać złośliwe kody osadzone w dokumentach pakietu Office (Word, Excel i PowerPoint).
46. EPP powinien być w stanie dostarczać raporty w oparciu o zagrożenia, zdarzenia, urządzenia, zdarzenia zapobiegające wyzyskowi.
47. EPP powinien być w stanie bezpiecznie wyświetlić listę dowolnych plików według podpisanego certyfikatu, umożliwiając dowolnemu niestandardowemu oprogramowaniu, które jest prawidłowo podpisane, działać bez zakłóceń.
48. EPP powinien mieć możliwość dodania dowolnego pliku do białej listy, dodając wartość skrótu tego pliku w zasadach.
49. Agent EPP powinien obsługiwać wdrażanie za pośrednictwem SCCM, Altiris, Group Policy Objects lub innych standardowych narzędzi do dystrybucji oprogramowania.
50. EPP powinien wykorzystywać uczenie maszynowe do identyfikowania i zapobiegania uruchamianiu złośliwych plików wykonywalnych w punkcie końcowym przed wykonaniem, korzystając ze statycznej analizy plików, jednocześnie stosując uczenie maszynowe do identyfikowania zachowań wskazujących na konkretny wektor ataku, aby uniemożliwić podmiotowi zagrażającemu pomyślną realizację swoich celów po wykonaniu.
51. EPP powinien korzystać z modułów wykrywania zagrożeń opartych na uczeniu maszynowym, ukierunkowanych na ataki bezplikowe, złośliwe/podejrzane polecenia jednowierszowe i zachowanie złośliwych aplikacji.
52. EPP powinien umożliwiać niestandardową kontrolę danych/metadanych wysyłanych poza firmę, zgodnie z przepisami dotyczącymi ochrony danych i RODO. Tj. możliwość kontrolowania adresu IP, FQDN, nazwy komputera i nazw użytkowników jako minimum wysłanego na zewnątrz lub do chmury dostawcy.
53. Dostawca EPP musi zapewnić funkcjonalność API umożliwiającą integrację z istniejącymi rozwiązaniami w zakresie bezpieczeństwa i orkiestracji.
54. Rozwiązanie EPP musi zapewniać możliwość audytu umożliwiające śledzenie dostępu analityków i działań w konsoli zarządzania EPP.
55. Rozwiązanie EPP powinno posiadać wbudowaną funkcjonalność pozwalającą na automatyczną inwentaryzację oprogramowania w systemie Windows. Zestaw informacji zebranych i dostępnych w konsoli administracyjnej systemu powinien obejmować minimalnie: nazwę aplikacji, wersję i nazwę producenta.

#### **Wymagania EDR:**

1. Rozwiązanie musi działać w architekturze klient – serwer.

2. Rozwiązanie w swoim działaniu musi wykorzystywać informacje spływające od agenta systemu ochrony antymalware tego samego producenta.
3. Ochrona antymalware nie może opierać się na sygnaturach, ani na heurystyce. Nie może także wymagać użycia sandboxa.
4. Rozwiązanie musi wspierać co najmniej systemy Windows 7, Windows 8, Windows 10, Windows 365 (Business, Enterprise), Windows Server 2022 (Standard, Data Center & Server Core), Windows Server 2019, Windows Server 2016, Windows Server 2012, MAC OS 10.15, MAC OS 11, MAC OS 12, MAC OS 13, MAC OS 14, Linux UBUNTU, SUSE Linux Enterprise, Red Hat Enterprise Linux, CentOS, Oracle Linux Server, Debian, Amazon Linux 2
5. Konsola administracji zdalnej systemu EDR, służąca zarządzaniu rozwiązaniem musi być rozwiązaniem chmurowym lub hybrydowym, nie dopuszczalne jest rozwiązanie „on premis” (lokalna instalacja systemu centralnej administracji).
6. Logowanie do konsoli centralnej administracji musi odbywać się za pośrednictwem przeglądarki internetowej – do logowania nie może być wykorzystana konsola w postaci dedykowanego rozwiązania wymagającego instalacji dodatkowej aplikacji.
7. Do swojego działania konsola administracji zdalnej nie może wymagać lokalnej instalacji takich komponentów jak baza danych czy serwer http.
8. Ta sama konsola musi umożliwiać zarządzanie systemem EPP (Endpoint Protection Platform) jak i systemem EDR (Endpoint Detection and Response) pochodzącymi od tego samego producenta.
9. Administrator musi mieć możliwość pobrania plików instalacyjnych agenta systemu EDR bezpośrednio z poziomu konsoli zarządzającej.
10. Dopuszcza się istnienie maksymalnie dwóch instalatorów zawierających w sobie agenta ochrony antymalware i systemu EDR.
11. System EDR musi w swoim działaniu wykorzystywać mechanizmy sztucznej inteligencji (AI).
12. System EDR musi posiadać możliwość wykorzystania w swoim działaniu gotowych reguł utworzonych przez producenta rozwiązania.
13. Musi istnieć możliwość tworzenia własnych zestawów reguł i przypisania ich do wybranych polityk konfiguracyjnych zarządzających rozwiązaniem.
14. Dany zestaw reguł może być jednocześnie przypisany do wielu polityk.
15. Administrator musi posiadać możliwość edycji zestawów reguł, ich klonowania lub usunięcia – wszystkie opcje muszą być dostępne z poziomu webowego interfejsu konsoli zarządzającej rozwiązaniem.
16. Administrator musi mieć możliwość włączenia konkretnej reguły, jej wyłączenia oraz aktywacji powiadomienia od strony endpointa w momencie wykrycia anomalii objętej daną regułą.
17. Administrator musi mieć możliwość tworzenia wykluczeń dla danej reguły.
18. Rozwiązanie musi umożliwiać podjęcie automatycznego działania w momencie wykrycia anomalii w oparciu o regułę, w tym co najmniej: usunięcia pliku, wylogowania wszystkich użytkowników, wylogowania zdalnych użytkowników, zawieszenia pojedynczych procesów jak i jego pochodnych procesów, zakończenia procesów oraz jego pochodnych, wyświetlenie powiadomienia, utworzenia zrzutu danych zebranych podczas wystąpienia incydentu objętego regułą.
19. Wykryte przez system EDR zdarzenia muszą być widoczne w postaci graficznych wykresów w konsoli zarządzającej.
20. Administrator musi mieć możliwość określenia jakie typy incydentów będą widoczne w tym co najmniej: Informacyjne, o niskim, średnim lub wysokim priorytecie.
21. Administrator musi mieć możliwość określenia zakresu czasu, z jakiego będą wyświetlane informacje dotyczące wykrytych incydentów w tym co najmniej z ostatnich 7 dni, 30 dni lub ostatnich 24 godzin.



22. Administrator musi mieć możliwość wglądu w szczegóły danego incydentu, bezpośrednio z panelu kontrolnego.
23. Administrator musi mieć możliwość utworzenia wykluczenia z wykrywania danego incydentu wykluczenie musi być tworzone w oparciu o informacje widoczne w szczegółach zdarzenia.
24. Administrator musi mieć możliwość usunięcia danego zdarzenia, wyeksportowania danych związanych ze zdarzeniem do formatu .json oraz zablokowania urządzenia na którym incydent miał miejsce.
25. Administrator musi mieć możliwość wysłania zapytania na stację klienckie z zainstalowanym agentem systemu EDR, w którym może uwzględnić co najmniej nazwy plików, skróty (hashe) wyszukiwanych obiektów, nazwy procesów, wartości rejestru.
26. Administrator musi posiadać możliwość wskazania artefaktu podczas wyszukiwania, co najmniej pliku, połączenia sieciowego, klucza rejestru, procesu. Administrator musi mieć możliwość połączenia wyszukiwanego artefaktu z konkretnym aspektem – np. w przypadku wyszukiwania konkretnego pliku musi istnieć możliwość określenia jego sumy kontrolnej SHA256 lub MD5
27. Wyszukiwanie musi być możliwe dla konkretnej grupy hostów lub wszystkich hostów objętych ochroną systemem EDR.
28. Wyniki wyszukiwania muszą być dostępne do wglądu z poziomu konsoli administracyjnej.
29. W momencie wykrycia obiektu spełniającego założenia wyszukiwania Administrator musi mieć możliwość pobrania obiektu.
30. Administrator w momencie przeglądania wyników wyszukiwania musi mieć możliwość wykonania analizy danego obiektu pod kątem jego zachowania – wynik takiej analizy musi być dostępny w postaci graficznej.
31. Graficzny wynik analizy danego obiektu lub incydentu musi przedstawiać ścieżkę aktywności obiektu w systemie.
32. Informacje dotyczące analizy incydentu muszą zawierać informacje o tworzeniu plików, uruchamianiu procesów, operacjach zmian i tworzenia nowych wpisów.
33. Administrator musi mieć możliwość wglądu w incydent w postaci wykresu lub w postaci listy operacji jakie miały miejsce podczas incydentu.
34. Musi istnieć możliwość eksportu informacji dotyczących incydentu do pliku CSV.
35. Administrator musi mieć możliwość uzyskania informacji dotyczących hosta w tym co najmniej jego nazwy, wersji zainstalowanego agenta systemu EDR, grupy do jakiej dany host jest przypisany, jego adresu IP.
36. Rozwiązanie musi umożliwiać automatyczne przesyłanie do konsoli administracyjnej, szczegółowych danych dotyczących incydentów co najmniej dla zablokowanych zagrożeń i mechanizmów ochrony pamięci.
37. Administrator musi mieć możliwość włączenia dodatkowych mechanizmów zbierających dane z systemu, na którym jest zainstalowany agent, w tym co najmniej: zapytań i odpowiedzi DNS, lokalnych połączeń IP, dziennika zdarzeń systemu Windows, dodatkowych atrybutów i parametrów dla poleceń wykonywanych za pomocą Powershell, dodatkowych atrybutów i parametrów dla Windows Management Instrumentation (WMI), dodatkowych informacji powiązanych z Portable Executable (PE), dodatkowych informacji uzyskiwanych z Win32 API i kernela. Rozwiązanie powinno także monitorować i móc reagować na zdarzenia związane z obiektami typu COM, śledzić transakcje Windows http, oraz monitorować ładowanie modułów systemu Windows.
38. Administrator musi mieć możliwość określenia maksymalnej ilości miejsca na dysku od strony chronionej końcówki, które zostanie wykorzystane do przechowywania zebranych logów.

39. Po wykorzystaniu zarezerwowanej do przetrzymywania zebranych logów przestrzeni, musi następować automatyczne nadpisywanie najstarszych elementów i zastępowanie ich nowymi.
40. System EDR musi pozwalać na kontrolę klienta poprzez zdalny wiersz poleceń. Uruchomienie zdalnego połączenia musi być dostępne na żądanie administratora z konsoli zarządzającej.
41. System EDR musi pozwalać na tworzenie i uruchamianie na żądanie oraz automatycznie zadań w formie paczek i zbioru kilku paczek (playbooks), które pozwolą administratorowi na podejmowanie dodatkowych zadań takich jak zabezpieczeń logów ze stacji końcowej, pobranie historii z przeglądarki internetowej oraz uruchamianych aplikacji, zabezpieczenie rejestru oraz MFT czy odinstalowanie wskazanej aplikacji. System powinien być w stanie tak zebrane pliki automatycznie wysyłać na dowolny udział SMB, SFTP oraz AWS S3.
42. Wymagane jest by paczki mogły być tworzone w języku python.
43. System EDR musi umożliwiać zdalną opcję pełnej izolacji sieciowej wskazanego hosta z możliwością automatycznego odblokowania stacji po upływie maksymalnie 96 godzin oraz ręcznego odblokowania poprzez unikalny klucz wprowadzany bezpośrednio na hoście.
44. System EDR musi umożliwiać zdalną opcję częściowej izolacji sieciowej wskazanego hosta, podczas której możliwe jest tylko połączenie z konsolą zarządzającą.
45. System EDR musi posiadać opcję rozszerzenia o wbudowanego asystenta opartego na generatywnej sztucznej inteligencji AI, który pomoże operatorowi w dogłębnym zrozumieniu danego alertu, szczególnie opartego na detekcji wywołanej przez wbudowane reguły.

### **Wymagania dot. montażu, instalacji i konfiguracji sprzętu**

Dostarczone urządzenie zostanie podłączone i skonfigurowane z najlepszą wiedzą techniczną i zaleceniami producenta.