Załącznik nr 1 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

PAKIET 1

Dostawa i konfiguracja serwerów oraz przełączników

1) Serwer 2 sztuki

Zamawiający przyjmuje oferty równoważne lub lepsze niż zaprezentowane poniżej.

lp.	Element, parametr lub cecha	Opis wymagania
1.	Ilość serwerów	• 2 sztuki.
2.	Obudowa	• Wysokość serwera nie może przekraczać 2U; • Zestaw szyn do mocowania w szafie Rack 19” i wysuwania serwera do celów serwisowych; • Ramie do prowadzenia okablowania.
3.	Liczba procesorów	• Zainstalowany minimum 1 procesor.
4.	Specyfikacja procesora	• Obsługa minimum dwóch procesorów; • ilość rdzeni dla procesora minimum 8; • taktowanie procesora nie niższe niż 2.3GHz.
5.	Płyta główna	• Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje AMD64 lub EM64T (np. AMD Opteron albo Intel Xeon);
6.	Pamięć operacyjna	• Zainstalowane minimum 64GB pamięci RAM. Pamięć musi być zoptymalizowana do działania z serwerem danego producenta; • Możliwość instalacji pamięci typu Persistent Memory.
7.	Zabezpieczenie pamięci	• Minimum (lub równoważne): memory mirroring, demand scrubing, patrol scrubing, memory rank sparing, ECC, SDDC, ADDDC.
8.	Procesor Graficzny	• Zintegrowana karta graficzna;
9.	Rozbudowa dysków	• Możliwość zainstalowania minimum 8 dysków; • Możliwość instalacji dysków SED.
10.	Kontroler dysków	• Serwer powinien posiadać zainstalowany kontroler dyskowego wykorzystującego pamięć flash NAND; • Kontroler powinien posiadać funkcjonalność podtrzymania napięcia w przypadku utraty głównego zasilania; • Kontroler powinien znajdować się w ofercie producenta serwera; • Kontroler powinien obsługiwać następujące poziomy zabezpieczeń raid 0/1/10/5/50/6/60. • Możliwość obsługi następującego formatowania dysków: 512e, 512n, 4K; • Możliwość tworzenia globalnych dysków hot-spare; • Kontroler powinien mieć możliwość odbudowy macierzy raid po awarii zasilania; • Powinna być możliwość zmiany pojemności dysków wirtualnych, jak również typu raid w trybie online.
11.	Zasilacz	• Obsługa zasilania zapasowego.
12.	Interfejsy sieciowe	• Serwer powinien posiadać 4 porty 1Gb RJ45, które będą umiejscowione na płycie głównej lub na dodatkowej karcie rozszerzeń. Użyte złącze PCIe nie może być liczone do ilości złącz, które zostało określone w sekcji Dodatkowe sloty I/O.
13.	Dodatkowe	• Serwer powinien mieć możliwość instalacji 3 kart PCIe.

	sloty I/O	
14.	Dodatkowe porty	• Z przodu obudowy: dodatkowe porty USB 3.0 oraz USB 2.0, opcjonalnie VGA; • Z tyłu obudowy: porty USB 3.0 oraz RS-232, możliwość instalacji portu DB9.
15.	Chłodzenie	• Wentylatory wspierające wymianę Hot-Plug.
16.	Zarządzanie	• Sprzętowy kontroler umożliwiający zdalne zarządzanie niezależnie od zainstalowanego systemu operacyjnego pozwalający na: o Monitoring systemu; o Pozyskanie informacji o zainstalowanych podzespołach oraz wykorzystaniu zasobów przez serwer; o Zbieranie logów ze zdarzeń, działań w systemie oraz zmian w zainstalowanych podzespołach; o Update firmware.
17.	Funkcje zabezpieczeń	• Hasło administratora, moduł TPM 1.2/2.0.
21.	Systemy operacyjne	• Microsoft Windows Server 2016, 2019, Red Hat Enterprise Linux 7 oraz 8, SUSE Linux Enterprise Server 12 oraz 15, VMware vSphere (ESXi) 6.5, 6.7, 7.0.
22.	Gwarancja	• Min. 36 miesięcy wsparcia producenta w trybie pełnego serwisu on-site w trybie NBD świadczonym przez autoryzowany serwis producenta.

2) Przełączniki 10 szt. + konfiguracja

Zamawiający przyjmuje oferty równoważne lub lepsze niż zaprezentowane poniżej.

lp.	Element, parametr lub cecha	Opis wymagania
1.	Porty	• 24 x 10/100/1000 RJ45; • 4 x SFP.
2.	Port zarządzania	• 1 sztuka.
3.	Port konsolowy	• 1 sztuka.
4.	Typ warstwy	• Warstwa 2.
5.	Przepustowości	• Switching Capacity min 56 Gbps; • Forwarding Rate min 41 Mpps.
6.	Pamięć RAM	• Min 128 MB
8.	Pamięć Flash	• Min 64 MB
11.	Ilość adresów MAC	• Min 15 000
12.	Ilość VLAN	• Min 4 000
13.	MTBF (godz.)	• Min 100 000 h
14.	Metody uwierzytelniania	• 802.1X, AAA
15.	Protokoły zdalnego zarządzania	• SNMP, RMON, Telnet, SSH
16.	Wskaźniki stanu	• System, aktywność LINK
17.	Automatyczna negocjacja	• TAK
18.	MDIX	• TAK
23.	Miejsce w szafie Rack	• 1U
24.	Zasilacze	• Min 1 zasilacz - wewnętrzny
25.	Wentylatory	• -
26.	Przepływ powietrza	• Bez wentylatora
30.	Gwarancja	• Min. 24 m-ce

3) Serwer NAS 2 szt.+ konfiguracja

Zamawiający przyjmuje oferty równoważne lub lepsze niż zaprezentowane poniżej.

lp.	Element, parametr lub cecha	Opis wymagania
1.	Typ	• Serwer typu rack do montażu w szafie rack.
2.	Procesor	• Procesor 64 bit x86 o takowaniu nie mniejszym niż 2.0 GHz; • Min 4 rdzenie.
3.	Pamięć operacyjna	• Min 4 GB SODIMM DDR4; • Min 2 sloty pamięci RAM; • Możliwość rozszerzenia o min 16 GB.
4.	Liczba zatok na dyski	• Min 4.
5.	Pojemność dysków twardych	• Min 18 TB.
6.	Zasilacz	• 300 W PSU (x2), 100–240 V; • Pobór mocy: Tryb uśpienia HDD: 32,19 W.
7.	Obudowa	• Szyny do montażu kompatybilne z serwerem NAS w zestawie: TAK • Rack: min 1U.
8.	Kompatybilność dysków	• 3,5-calowe dyski twarde SATA • 2,5-calowe dyski twarde SATA • 2,5-calowe dyski SSD SATA
9.	Specyfikacja oprogramowania	• Obsługiwane klienckie system operacyjne: o Apple Mac OS 10.10 lub nowszy o Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 lub nowszy Linux o IBM AIX 7, Solaris 10 lub nowszy UNIX o Microsoft Windows 7, 8, 10 i 11 o Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016 i 2019 • Rozszerzenie JBOD: TAK • Usługa ISCSI: TAK • Typ macierzy RAID: o 8-kieszeniowy (i więcej): JBOD, Single, RAID 0, 1, 5, 6, 10, 50, 60 o 6-kieszeniowy: JBOD, pojedynczy, RAID 0, 1, 5, 6, 10, 50 o 4-kieszeniowy: JBOD, Pojedynczy, RAID 0, 1, 5, 6, 10 o 2-kieszeniowy: JBOD, Pojedynczy, RAID 0, 1 • Migracja na poziomie RAID: TAK • Rozszerzenie RAID przez dodanie dysku: TAK • RAID Hot Spare: Globalny, lokalny
10.	Gwarancja	• Min 36 m-cy gwarancji standardowej.
11.	Wymagania dodatkowe	• Koprocesor arytmetyczny FPU: Tak; • Mechanizm szyfrowania: AES-NI; • Transkodowanie wspomagane sprzętowo: Opcjonalne przez kartę graficzną PCIe; • Port 2,5 Gigabit: min 2; • Obsługa przyspieszenia pamięci podręcznej SSD: Tak; • Obsługuje hosty wirtualne: Tak; • Wskaźniki LED: HDD 1–8, stan, LAN, USB, zasilanie; • Port USB 3.2 Gen 2 (10 Gb/s): 4 (2 gniazdka A, 2 typu C); • Gniazdko M.2: 2 x M.2 2280: tak; • Wake on LAN WOL: Tak.
12.	Pamięć flash	• Min 4 Gb.

4) Dyski serwera NAS 16 szt.

Zamawiający przyjmuje oferty równoważne lub lepsze niż zaprezentowane poniżej.

lp.	Element, parametr lub cecha	Opis wymagania
1.	Rozmiar HDD	3,5”
2.	Pojemność HDD	10 TB
3.	Prędkość obrotowa HDD	7200 RPM
4.	Rozmiar buforu dysku pamięci	256 MB
5.	Wydajność:	Szybkość transferu: 273 MB/sec Średnia latencja: 4,16 ms Szybkość transferu interfejsu: 600 MB/s Interfejs: SATA 6GB/s
6.	Gwarancja	Gwarancja producenta min. 36 miesięcy
7.	Niezawodność:	Dostępność: 24/7 Cykl załadunku/rozładunku: 600,000 MTBF: 2 000 000 godziny Odczyt nieodwracalnych bitów o współczynniku błędu: 1 in 10^{15}
8.	Zużycie energii:	8 wat (moc w stanie bezczynności, średnia) 9,2 wat (srednia moc robocza)
9.	Wymagania dodatkowe	Proponowany dysk musi się znajdować na liście kompatybilnych dysków twardych proponowanego serwera NAS

Pakiet 2

Oprogramowanie SIEM + Usługa wdrożenia

Zamawiający przyjmuje oferty równoważne lub lepsze niż zaprezentowane poniżej.

lp.	Wymaganie
1.	System musi zbierać dane z różnych dostępnych źródeł.
2.	System musi umożliwiać pobieranie logów z innych systemów za pomocą wielu metod.
3.	System musi umożliwiać analizowanie logów wielolinijkowych.
4.	System musi udostępniać mechanizmy pozwalające na integracje urządzeń źródłowych, z wykorzystaniem graficznego kreatora reguł parsowania.
5.	Graficzny kreator reguł parsowania musi obsługiwać wiele formatów.
6.	Graficzny kreator reguł parsowania musi umożliwiać tworzenie reguł z wykorzystaniem wyrażeń regularnych.
7.	Graficzny kreator reguł parsowanie musi mieć możliwość podpowiadania użytkownikowi wzorca wyrażenia regularnego dla wskazanego łańcucha w payloadzie.
8.	Mechanizmy integracji źródeł, zarówno tych wskazanych przy wdrożeniu, jak i integrowanych w przyszłości przez Zamawiającego, nie mogą być w żaden sposób ograniczane licencyjnie przez producenta ani wymagać dodatkowych opłat ze strony Zamawiającego.
9.	System musi umożliwiać zmianę sposobu normalizacji danych w trakcie używania systemu i pozwalać na równoległe używanie różnych sposobów normalizacji logów.
10.	System musi posiadać możliwość automatycznego rozpoznawania źródeł logów, które są przekierowane do SIEM (zakładając, że posiada parser dla technologii tego źródła danych). Musi automatycznie rozpoznać typ logu i dobrać odpowiedni parser, tak aby nie była wymagana żadna aktywność ze strony administratora systemu.
11.	System musi posiadać możliwość zainstalowania natywnego komponentu generującego dane o przepływach na podstawie analizy ruchu sieciowego.
12.	System musi mieć możliwość przeprowadzenia bezagentowej akwizycji danych. W uzasadnionych przypadkach dopuszczamy stosowanie agentów.
13.	Zbierane informacje muszą być poddane w systemie korelacji, na podstawie których administratorzy systemu będą informowani o stanie bezpieczeństwa infrastruktury Zamawiającego oraz ostrzegani o ewentualnych incydentach bezpieczeństwa.
14.	System musi zawierać bazę predefiniowanych reguł korelacyjnych, których wykorzystanie przez Zamawiającego nie wymaga ponoszenia dodatkowych nakładów z tym związanych.
15.	System musi umożliwiać budowanie reguł korelacyjnych bazujących na zdarzeniach, przepływach, jednocześnie zdarzeniach i przepływach, a także na innych korelacjach.
16.	System umożliwia wykorzystanie reguł korelacyjnych jako bloków do wykorzystania w nadrzędnych regułach korelacyjnych.
17.	System, oprócz prezentowania informacji o alertach w tablicach, musi posiadać możliwość powiadamiania o zdarzeniach w inny sposób.
18.	System musi umożliwiać zastosowanie w regułach korelacyjnych testów logicznych na wartościach pól bazy danych zdarzeń i przepływów.
19.	System musi umożliwiać zastosowanie w regułach języka zapytań bazy danych zdarzeń i przepływów.
20.	System musi umożliwiać zastosowanie w regułach testów zawartości payloadu zdarzenia.
21.	Rozwiązanie powinno posiadać wbudowane mechanizmy śledzące wydajność reguł korelacyjnych.
22.	System nie może wykorzystywać bazy danych ogólnego zastosowania do

	przechowywania zdarzeń i przepływów.
23.	Baza danych musi umożliwiać wydawanie poleceń w języku zapytań bazy danych.
24.	Ze względu na zachowanie integralności danych, język bazy danych zdarzeń i przepływów może pozwalać na wykonanie jedynie polecenia SELECT. Baza danych nie może pozwalać na wykonywanie poleceń UPDATE, INSERT i DELETE.
25.	Dane pochodzące z logów zapisywane są w domyślnie dostępnych polach bazy danych przynajmniej takich jak: nazwa zdarzenia, kategoria zdarzenia, adres IP źródłowy, źródłowy port TCP/IP, adres IP źródłowy przed translacją, adres IP źródłowy po translacji, czas urządzenia, z którego wysłany był log, nazwa protokołu, nazwa użytkownika, nazwa hosta, nazwa grupy, nazwa NetBIOS (o ile zawartość tych pól jest zawarta w logu).
26.	System musi umożliwiać dodanie własnych pól w bazie, które można przywoływać jako kryteria wyszukiwania, określane przy pomocy nowych wzorców.
27.	System musi przechowywać w bazie danych również payloady zdarzeń i przepływów.
28.	System musi umożliwiać wskazanie które pola mają być zapisywane w bazie danych bezpośrednio po otrzymaniu zdarzenia, a które nie. W tym drugim przypadku wartość pola jest każdorazowo wyznaczana z payloadu na podstawie reguł parsera w momencie użycia tego pola (np. przy wyświetleniu lub wykonaniu testu logicznego na polu).
29.	System musi umożliwić zapisanie wzorca wyszukiwania, a także związanych z nim szablonów prezentacji oraz wyników w celu późniejszego przywołania lub też udostępnienia wyszukiwania innym użytkownikom.
30.	System musi umożliwiać umieszczenie zapisanego wzorca w ramach utworzonej grupy wzorców, na tablicach (dashboard) oraz w miejscu umożliwiającym szybki dostęp.
31.	System musi być gotowy na przyjęcie chwilowych gwałtownych przyrostów ilości zdarzeń bez ich utraty.
32.	System musi być w stanie monitorować środowisko conajmniej 25 serwerów.
33.	System musi mieć możliwość budowania profilu stanu i zachowania środowiska IT oraz identyfikowania odchyleń i wykrywania anomalii na podstawie analizy behawioralnej.
34.	System musi mieć możliwość wykrywania anomalii na podstawie odchyłki wartości w ostatnim okresie od wartości w okresie historycznym.
35.	System musi mieć możliwość wykrywania anomalii na podstawie przekroczenia wartości progowej.
36.	System musi mieć możliwość wykrywania anomalii na podstawie odchyłki wartości od zarejestrowanego trendu.
37.	System musi umożliwiać tworzenie szablonów raportów.
38.	Wymagane formaty raportów: co najmniej PDF, HTML, XML, XLS, CSV.
39.	System musi mieć możliwość generowania raportów zgodnie z ustalonym harmonogramem czasowym.
40.	System powinien mieć możliwość wysyłania mailem raportów na wskazane adresy.
41.	System musi mieć możliwość weryfikowania tożsamości użytkowników poprzez wykorzystanie kont lokalnych oraz zewnętrzne systemy uwierzytelnienia – MS Active Directory oraz RADIUS i LDAP.
42.	System musi zawierać funkcjonalność precyzyjnego nadawania uprawnień użytkownikom i administratorom.
43.	System musi posiadać zaimplementowane mechanizmy automatycznej kontroli własnego stanu oraz alarmowania w przypadku wykrytych nieprawidłowości.
44.	System musi posiadać zaimplementowany dedykowany dashboard prezentujący dokładne statystyki związane z wydajnością systemu: utylizacja CPU, utylizacja pamięci RAM, heap usage, disk IO throughtput, disk IOPS, statystyki połączeń sieciowych, ilość wykonywanych zapytań, statystyki dotyczące wywołań API itp.
45.	System musi zapewniać centralne gromadzenie wszystkich logów i zapewniać ich bezpieczne przechowywanie oraz dostępność przez okres 30 dni.

46.	System musi samodzielnie zarządzać retencją danych.
47.	System musi umożliwiać wyspecyfikowanie różnego czasu retencji danych dla różnych zdarzeń i przepływów - na podstawie zawartości pól bazy danych.
48.	System musi posiadać mechanizm automatycznego archiwizowania danych i konfiguracji systemu do katalogu w lokalnym systemie plików i określenia retencji dla przechowywanych w ten sposób danych.
49.	System musi umożliwiać włączenie lub wyłączenie indeksacji pola bazy danych z interfejsu graficznego.
50.	Zdarzenia i przepływy muszą być przechowywane w postaci skompresowanej.
51.	System musi zapewniać możliwość obsługi poprzez przeglądarkę.
52.	System musi udostępniać możliwość prezentacji statystyk i wyników działania w postaci tablic (dashboard), których wygląd i rozkład poszczególnych składowych daje się dostosować do potrzeb administratora i użytkownika. Widoczność stworzonych i domyślnie dostępnych tablic można przełączać przy pomocy łatwo dostępnej listy rozwijanych pozycji.
53.	Informacje prezentowane w poszczególnych tablicach są wynikiem stworzonych przez producenta predefiniowanych korelacji, a także wyników wyszukiwania stworzonych przez użytkownika lub udostępnionych mu przez innych użytkowników i administratorów.
54.	System nie może wymagać instalacji dedykowanego oprogramowania klienckiego do jego obsługi.
55.	System musi umożliwiać prezentację zdarzeń i przepływów na podstawie filtrów tworzonych przy pomocy pól wyboru.
56.	System musi umożliwiać prezentację zdarzeń i przepływów na podstawie filtru wyspecyfikowanego w języku bazy danych.
57.	System musi umożliwiać prezentację zdarzeń i przepływów na podstawie filtru specyfikującego słowo występujące w payloadzie.
58.	System musi mieć możliwość tworzenia clustra wysokodostępnego dla każdego z komponentów (za wyjątkiem agentów instalowanych na innym serwerze/stacji oraz analizatora ruchu sieciowego). Awaria pojedynczego komponentu nie może spowodować utraty funkcjonalności i wydajności systemu.
59.	Każda z reguł korelacyjnych musi mieć możliwość korelowania zdarzeń i przepływów z wszystkich serwerów przetwarzających dane, bądź z jednego serwera - zależnie od decyzji projektanta reguły.
60.	System musi umożliwiać prezentację zdarzeń i przepływów w postaci tabelarycznej, z możliwością wyboru okresu lub w czasie rzeczywistym.
61.	System musi posiadać dashboard prezentujący mapę, na której w czasie rzeczywistym są prezentowane incydenty lub dowolnie zdefiniowane zdarzenia.
62.	System musi umożliwiać automatyczne łączenie wielu incydentów w jeden.
63.	System musi posiadać aplikację monitorującą charakterystykę zachowania użytkowników (user behavior analysis), która pozwala na ocenę ryzykownych czynności podejmowanych przez wewnętrznych użytkowników na infrastrukturze.
64.	Aplikacja analizująca zachowania użytkowników musi przypisywać użytkownikom tzw. punkty ryzyka i generować alarm po przekroczeniu wartości progowej sumarycznych punktów ryzyka. Wartość progowa może być ustalana statycznie (bezwzględna wartość liczbowa) lub dynamicznie (na podstawie rozkładu wartości punktów ryzyka dla całej populacji użytkowników).
65.	Aplikacja musi wyświetlać kształtowanie się poziomu ryzyka dla użytkownika w czasie.
66.	System analizy zachowania użytkowników musi mieć możliwość wykorzystania uczenia maszynowego.

67.	Wbudowane modele uczenia maszynowego mają analizować trendy zachowania w czasie oraz porównywać zachowanie użytkownika z grupą innych użytkowników o podobnych parametrach charakteryzujących danego użytkownika - przykładowo ulokowanie w konkretnym kontenerze Active Directory lub posiadających konkretny atrybut (np. nazwa stanowiska).
68.	Użytkownik musi mieć możliwość tworzenia własnych modeli uczenia maszynowego analizujących trendy zmian wartości w czasie.
69.	W przypadku braku zdefiniowanych grup użytkowników, system sam wykonuje grupowanie użytkowników na podstawie podobnych wzorców zachowania.
70.	System ma możliwość wyspecyfikowania grup użytkowników, dla których punkty ryzyka są modyfikowane o wyspecyfikowany mnożnik.
71.	System musi mieć możliwość tworzenia szczegółowego logu audytowego zawierającego informacje przynajmniej o logowaniu do systemu i zmianach w jego konfiguracji.
72.	Licencja systemu SIEM oraz system SIEM nie mogą ograniczać liczby równocześnie zalogowanych użytkowników.
73.	System musi posiadać możliwość automatycznego wykrywania nowych elementów infrastruktury poprzez analizę zdarzeń i/lub ruchu sieciowego. SIEM musi wykryć pojawienie się nowego adresu IP, adresu MAC i opcjonalnie zgłosić to operatorowi.
74.	System musi posiadać możliwość automatycznego grupowania elementów infrastruktury poprzez ich cechy charakterystyczne. Przykładowo, system SIEM powinien być w stanie dokonać klasyfikacji elementów posiadających otwarte porty charakterystyczne dla baz danych jako "serwery bazodanowe".
75.	System musi umożliwiać tworzenie własnego schematu opisu i oznaczania (tzw. tagowania) assetów.
76.	System musi umożliwiać filtrowanie assetów w oparciu o dowolne pole charakteryzujące dany element infastruktury.
77.	System musi zapewniać automatyczny mechanizm aplikacji poprawek do systemu.
78.	System musi umożliwiać utworzenie struktury adresacji IP używanej w poszczególnych miejscach sieci i w ten sposób określić adresacje obce. Ta struktura używana jest następnie do określenia kierunków rejestrowanych zdarzeń komunikacji i przepływów
79.	System musi umożliwić konfigurację serwera poczty, przez który wysyłane są wiadomości pocztowe. Musi być możliwość konfiguracji innych serwerów poczty dla różnych serwerów przetwarzających zdarzenia i przepływy.
80.	System pozwala na integrację z systemami zarządzania podatnościami w celu uzupełnienia informacji o zasobach o bardziej szczegółowe dane.
81.	System pozwala na integrację z co najmniej tymi systemami zarządzania podatnościami: eEye, BigFix, Juniper NSM, nmap, Qualys, Rapid7, Tenable
82.	System musi posiadać własną bazę reputacji IP
83.	System musi posiadać możliwość przeprowadzenia korelacji historycznej, czyli symulacji działania reguły dla zdarzeń historycznych
84.	System musi posiadać udokumentowany interfejs API
85.	System musi posiadać narzędzie graficzne umożliwiające testowanie różnych zapytań API i weryfikację otrzymywanych danych
86.	System musi umożliwiać rozdzielenie plików bazy danych na wiele "domen", z możliwością tworzenia oddzielnych reguł korelacyjnych dla domen
87.	Licencja nie może bezpośrednio ograniczać wielkości przetwarzanych danych w bajtach.
88.	System musi umożliwiać obfuskację (ukrywanie) danych wrażliwych zdarzeń i przepływów przed operatorem
89.	System musi umożliwiać kontrolę integralności bazy danych przez zastosowanie hashowania
90.	Producent systemu musi udostępniać zestawy dodatkowych reguł, ponad podstawowy zbiór reguł dostępny w produkcie po instalacji
91.	System musi tworzyć indeks słów znajdujących się w payloadzie, w celu szybszego wyszukiwania zdarzeń.
92.	System musi umożliwiać detekcję nadużycia protokołu DNS typu: DGA, squatting,

	tunelowanie
93.	System musi umożliwiać tworzenie aplikacji osadzanych w interfejsie graficznym systemu
94.	System musi mieć możliwość uniemożliwienia użytkownikom wykonywanie zapytań które mogą trwać zbyt długo lub wyszukiwań które będą zwracały dużą ilość danych co może mieć negatywny wpływ na wydajność systemu. Takie polityki muszą mieć możliwość definiowania na poziomie użytkownika, roli lub tenantów.
95.	System oprócz podstawowego interfejsu przeglądania danych z funkcjonalnością administracyjną musi mieć dodatkowo odseparowany interfejs przeznaczony do pracy dla operatorów SOC. Interfejs ten musi być pozbawiony funkcjonalności administracyjnych i powinien w pełni być skoncentrowany na analizie incydentów bezpieczeństwa.
96.	System musi zawierać funkcjonalność wsparcia przy tuningu reguł. System powinien raportować reguły które najczęściej inicjują incydenty bezpieczeństwa oraz reguły które są najmniej efektywne.
97.	System musi automatycznie informować o nowych dodatkowych funkcjonalnościach dostępnych do ściągnięcia z dedykowanego repozytorium aplikacji.
98.	System musi zawierać dedykowany dashboard który prezentuje przydatne artykuły, wiadomości, przypadku użycia, podcasty oraz odnośniki do szkoleń. Zawartość musi być dostosowana automatycznie do charakterystyki obsługiwanej infrastruktury
99.	System musi umożliwiać wykorzystanie tzw. zapytań federacyjnych do różnych niezależnych instancji systemów SIEM w oparciu o format STIX
100.	System musi umożliwiać prostą integrację z systemem klasy SOAR bez konieczności prowadzenia prac integracyjnych - przykładowo za pomocą gotowej aplikacji
101.	Licencje na system nie mogą być dostarczane w modelu subskrypcyjnym (ograniczone czasowo)
102.	Dodanie od system kolejnego komponentu analizującego/przechowującego zdarzenia/przepływy nie może wymagać dokupienia dodatkowej licencji
103.	Utworzenie clustra HA komponentu poprzez dodanie serwera zapasowego nie może wymagać dokupienia dodatkowej licencji
104.	System musi znajdować się w "ćwiartce liderów" w najnowszym opracowaniu tzw. magicznego kwadrata systemów SIEM wg. Gartnera.
105.	Zwiększenie strumienia EPS (zdarzeń na sekundę) monitorowanego przez SIEM nie może wymagać dokupienia dodatkowej licencji

Pakiet 3

Oprogramowanie do tworzenia kopii zapasowych + Usługa wdrożenia

lp.	Wymaganie
1.	● Oprogramowanie może być dostarczane w dwóch scenariuszach: ○ Cloud(Software as Service); ○ On-premise.
2.	● Istnieje możliwość migracji w obie strony pomiędzy środowiskiem on-premise oraz cloud.
3.	● Oprogramowanie nie preferuje platformy sprzętowej, nie jest profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych; ● Oprogramowanie może być uruchomione w kontenerze docker.
4.	● Możliwość instalacji oraz uruchomienia serwera zarządzania na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy: ○ Debian: 9+; ○ Ubuntu: 16.04+; ○ Fedora: 29+; ○ centOS: 7+; ○ RHEL: 6+; ○ openSUSE: 15+; ○ SUSE Enterprise Linux (SLES): 12 SP2+; ○ Windows Client: 7, 8.1, 10 (1607+); ○ Windows Server: 2008 R2+.
5.	● System wykonuje kopię własnej bazy danych, która umożliwia odtworzenie wszystkich ustawień i całej konfiguracji.
6.	● Oprogramowanie działa w architekturze wykluczającej pojedynczy punkt awarii(awaria jednego z komponentów nie spowoduje przestoju).
7.	● Pomoc techniczna w językach: ○ Polskim; ○ angielskim.
8.	● Materiały samopomocowe: ○ Baza wiedzy: ■ Polski; ■ angielski.
9.	● Zarządzanie całością działania systemu (backup, przywracanie)z poziomu jednej konsoli webowej.
10.	● Zarządzanie całym systemem poprzez dashboardy.
11.	● Gradacja uprawnień kont administratorów z poziomu panelu zarządzającego.
12.	● System posiada wbudowane predefiniowane zadania backupowe.
13.	● System umożliwia tworzenie zadań backupowych w oparciu o kalendarz.
14.	● Automatyczne oraz ręczne uruchamianie kopii zapasowych zgodnie z ustalonym harmonogramem.
15.	● Automatyczne oraz ręczne uruchamianie procesu przywracania zgodnie z ustalonym harmonogramem.
16.	● Monitorowanie postępu działania zadania.
17.	● Posiada system powiadamiania poprzez e-mail o zdarzeniach w następujących przypadkach: ○ Zadanie zostało zakończone pomyślnie; ○ Zadanie zostało zakończone z ostrzeżeniami; ○ Zadanie zostało zakończone z błędem; ○ Zadanie zostało anulowane; ○ Zadanie nie zostało uruchomione.

18.	● System generuje alerty na konsoli WEB w przypadku zaistnienia określonego zdarzenia systemowego.
19.	● Możliwość zdefiniowania okna backupowego dla każdego z zadań.
20.	● Oprogramowanie posiada wbudowany menadżer haseł do przechowywania kluczy szyfrujących oraz poświadczeń do magazynów.
21.	● System pozwala na klonowanie planów kopii zapasowych.
22.	● System umożliwia reset hasła administratora w przypadku jego utraty.
23.	● Oprogramowanie umożliwia definiowanie retencji według schematów: ○ GFS(Grandfather-Father-Son); ○ FIFO(First-In, First-Out).
24.	● Oprogramowanie umożliwia tworzenie kont użytkowników nie będących administratorami.
25.	● Konta użytkowników mogą być tworzone poprzez import pliku CSV.
26.	● Oprogramowanie umożliwia tworzenie grup urządzeń.
27.	● Oprogramowanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera(urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera(urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).
28.	● System pozwala na zarządzanie multi-tenantowe - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: ○ System Administrator; ○ Backup operator; ○ Restore operator; ○ Viewer.
29.	● Oprogramowanie jest systemem multi-storageowym i umożliwia tworzenie wielu repozytoriów danych jednocześnie,
	● System umożliwia składowanie danych: ○ Lokalnie: ■ Zasób SMB; ■ Zasób NFS; ■ Zasób ISCSI; ■ Zasób S3; ■ Katalog zabezpieczonego urządzenia. ○ W chmurze: ■ Amazon Web Service; ■ Magazyn zgodny z S3; ■ Dostarczanej przez producenta.
30.	● System pozwala na zdefiniowanie zapasowej ścieżki repozytorium, na wypadek niedostępności głównej lokalizacji.
31.	● System oferuje mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.
32.	● System umożliwia replikacje danych między magazynami.
33.	● Odtwarzanie granularne: ○ Pojedynczych plików z kopii obrazu dysku; ○ Pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365.
34.	● Wykorzystanie funkcjonalności Bare Metal Restore(kopii zapasowej całego dysku - łącznie z partycjami i danymi startowymi) dla odtwarzania systemu po awarii, wsparcie dostępne jest dla systemów: ○ Windows: 7+; ○ Windows Server: 2008 R2+.
35.	● Odtwarzanie Bare metal Restore może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.

36.	● Uruchamianie procesu Bare Metal Restore odbywa się z bootowalnej płyty CD lub pendrive'a.
37.	● Oprogramowanie umożliwia odtwarzanie systemu w scenariuszach: P2P, P2V, V2P, V2V.
38.	● Oprogramowanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie(VHD, VHDX, VMDK),
39.	● Odtwarzanie zasobów plikowych bez praw dostępu(tzw. ACL),
40.	● Odtwarzanie zasobów plikowych z prawami dostępu,
41.	● Przywracanie plików pomiędzy systemami operacyjnymi(np. odtwarzanie danych plikowych Linux na systemie Windows),
42.	● Odtwarzanie danych według harmonogramu,
43.	● Przywracanie danych z określonego urządzenia/użytkownika,
44.	● Przywracanie kopii z wybranego magazynu.
45.	● Przywracanie danych Microsoft 365: ○ do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku: ■ pst; ■ mbox. ○ do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji).
46.	● System posiada możliwość nieodwracalnego kasowania danych. ● Wykonywanie pełnych, różnicowych, przyrostowych kopii zapasowych, a także backupu syntetycznego dla: ○ Systemów operacyjnych: ■ Ubuntu; ■ Windows; ■ Windows Server. ○ Środowisk wirtualnych: ■ Hyper-V; ■ Vmware.
47.	● Szyfrowanie danych wykonywana po stronie stacji roboczej za pomocą algorytmu AES w trybie CBC z kluczem szyfrującym o długości: ○ 128 bit; ○ 192 bit; ○ 256 bit.
48.	● Kompresja danych wykonywana po stronie stacji roboczej za pomocą algorytmów: ○ ZStandard; ○ LZ4.
49.	● Oprogramowanie umożliwia zarządzanie poziomem kompresji.
50.	● Wykonywanie kopii zapasowej otwartych plików(VSS).
51.	● System umożliwia uruchamianie skryptów przed i po backupie.
52.	● System umożliwia uruchamianie skryptów po wykonaniu migawki VSS.
53.	● System umożliwia automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku błędów.
54.	● Backup jednego oraz wielu dysków/całego systemu operacyjnego(Windows) ze wsparciem dla partycji MBR oraz GPT.
55.	● Backup plikowy.
56.	● Oprogramowanie realizuje funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie dyskowe.
57.	● Oprogramowanie umożliwia konsolidację wersji kopii zapasowych.
58.	● Oprogramowanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.
59.	● Oprogramowanie pozwala na automatyczne uruchomienie kopii zapasowej podczas zamykania systemu operacyjnego.

60.	● Oprogramowanie pozwala na backup zaszyfrowanych partycji.
61.	● Sposób licencjonowania opiera się na: ○ Ilości serwerów/endpointów- dla fizycznych urządzeń; ○ Ilości fizycznych hostów - dla środowisk wirtualnych.
62.	● Licencje powinny pozwalać na zabezpieczenie w opcji wieczystej: ○ 100 stacji roboczych; ○ 3 serwerów fizycznych bez wirtualizacji.
63.	• Wsparcie techniczne Obowiązuje przez okres minimum **12 miesięcy.**
64.	• Świadczone jest w języku polskim, bezpośrednio przez główną siedzibę producenta.
65.	• Zapewnia dostęp do aktualizacji oprogramowania.

Pakiet 4

Szkolenia w zakresie cyberbezpieczeństwa oraz przygotowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.

lp.	Wymaganie
1.	Szkoleniu będą podlegać wszyscy pracownicy zatrudnieni u Zamawiającego (łącznie ok.580 osób). Zamawiający wymaga aby szkolenie odbyło się w siedzibie Zamawiającego.
2.	Zamawiający udostępni miejsce oraz rzutnik do wyświetlania prezentacji.
3.	Szkolenie może trwać nie dłużej niż 4h dla jednej grupy, w dni robocze od 7:25 do 15:00.
4.	Wykonawca zapewni: • Nieodpłatne materiały w formie elektronicznej, które każdy pracownik będzie mógł wydrukować; • Zaświadczenia dla uczestników o ukończeniu kursu.
5.	Szkolenie zostanie przeprowadzone w taki sam sposób dla wszystkich grup.
6.	Dokumentacja wymagana podczas prowadzenia szkolenia: • Lista obecności; • Lista potwierdzająca odbiór zaświadczenia o ukończeniu szkolenia; • Ankieta.
7.	Szkolenie powinno obejmować swoim zakresem zasady dotyczące cyberbezpieczeństwa oraz powinno poruszać problematykę najczęściej występujących zagrożeń (phising, ransomware, malware).
8.	Osoby szkolone powinny zostać zapoznane ze sposobami przeciwdziałania oraz w sposoby zabezpieczania się przed wspomnianymi zagrożeniami.
9.	• Dokumentacja powinna zostać przygotowana zgodnie z normą PN/EN ISO 27001. • Zakres przedmiotowy dokumentacji SZBI: • Zakres dokumentu. • Powołania normatywne. • Terminy i definicje. • Kontekst organizacji: o Organizacja i jej kontekst; ▪ Czynniki zewnętrzne i wewnętrzne istotne dla działania organizacji. o Potrzeby i oczekiwania stron zainteresowanych: ▪ Strony zainteresowane dla SZBI; ▪ Wymagania stron zainteresowanych, istotne dla bezpieczeństwa informacji. o Zakres Systemu Zarządzania Bezpieczeństwem Informacji (dalej SZBI); o Ustanowienie SZBI. • Przywództwo: o Przywództwo i zaangażowanie: ▪ Ustanowienie Polityki Bezpieczeństwa Informacji (dalej PBI); ▪ Integracja SZBI z procesami organizacji; ▪ Dostępność zasobów potrzebnych w SZBI; ▪ Komunikowanie znaczenia i zgodności z wymaganiami SZBI; ▪ Opomiarowanie i mierzenie wyników SZBI; ▪ Kierowanie i wspieranie osób dla celów skuteczności SZBI; ▪ Promowanie ciągłego doskonalenia; ▪ Wspieranie innych członków kierownictwa w przywództwie w obszarach ich odpowiedzialności. o Polityka: ▪ Cele utworzenia PBI; ▪ Ramy dla ustanowienia PBI; ▪ Zobowiązanie spełnienia założeń PBI; ▪ Zobowiązanie do ciągłego doskonalenia PBI; ▪ Sposoby dokumentowania PBI; ▪ Komunikowanie o PBI; ▪ Dostępność PBI. o Role, odpowiedzialność i uprawnienia ▪ Inspektor Ochrony Danych (IOD);

	▪ Zespół ds. Bezpieczeństwa Informacji (ZBI); ▪ Administrator Systemu Informatycznego (ASI); ▪ Sekretarz Urzędu; ▪ Kierownicy Komórek Organizacyjnych (KKO) i Samodzielne Stanowiska (SS); ▪ Pracownicy (PI). • Planowanie: o Działania odnoszące się do ryzyk i szans: ▪ Postanowienia ogólne; ▪ Szacowanie ryzyka w bezpieczeństwie informacji; ▪ Postępowanie z ryzykiem w bezpieczeństwie informacji. o Cele bezpieczeństwa informacji i planowanie ich osiągnięcia. • Wsparcie: o Zasoby; o Kompetencje; o Uświadamianie; o Komunikacja; o Udokumentowane informacje: ▪ Postanowienia ogólne; ▪ Opracowanie i aktualizowanie; ▪ Nadzór nad udokumentowanymi informacjami. • Działania operacyjne: o Planowanie i nadzór nad działaniami operacyjnymi; o Szacowanie ryzyka w bezpieczeństwie informacji; o Postępowanie z ryzykiem w bezpieczeństwie informacji: ▪ Właściciel ryzyka; ▪ Rejestr ryzyka; ▪ Ryzyka Krytyczne; ▪ Sposób reakcji na ryzyko. • Ocena wyników o Monitorowanie, pomiary, analiza i ocena (MPAO): ▪ Monitorowanie bezpieczeństwa informacji; ▪ MPAO zmian prawnych; ▪ MPAO zmian organizacyjnych; ▪ MPAO zmian w systemach teleinformatycznych; ▪ MPAO zmian w otoczeniu zewnętrznym. o Audyt wewnętrzny; o Przegląd zarządzania; • Doskonalenie: o Niezgodność i działania korygujące; o Ciągłe doskonalenie. • Załącznik A (normatywny) – Wykaz celów stosowania zabezpieczeń. • Polityki bezpieczeństwa informacji: o Kierunki bezpieczeństwa informacji określane przez kierownictwo: ▪ Polityki bezpieczeństwa informacji; ▪ Przegląd polityk bezpieczeństwa informacji. • Organizacja bezpieczeństwa informacji: o Organizacja wewnętrzna: ▪ Role i odpowiedzialność za bezpieczeństwo informacji; ▪ Rozdzielenie obowiązków; ▪ Kontakty z organami władzy; ▪ Kontakty z grupami zainteresowanych specjalistów; ▪ Bezpieczeństwo informacji w zarządzaniu projektami. o Urządzenia mobilne i telepraca: ▪ Polityka stosowania urządzeń mobilnych; ▪ Telepraca. • Bezpieczeństwo zasobów ludzkich: o Przed zatrudnieniem: ▪ Postępowanie sprawdzające; ▪ Warunki zatrudnienia.

- Podczas zatrudnienia:
  - Odpowiedzialność kierownictwa;
  - Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji;
  - Postępowanie dyscyplinarne.
- Zakończenie i zmiana zatrudnienia:
  - Zakończenie zatrudnienia lub zmiana obowiązków.

- Zarządzanie aktywami:
  - Odpowiedzialność za aktywa:
    - Inwentaryzacja aktywów;
    - Własność aktywów;
    - Akceptowalne użycie aktywów;
    - Zwrot aktywów.
  - Klasyfikacja informacji:
    - Klasyfikowanie informacji;
    - Oznaczanie informacji;
    - Postępowanie z aktywami.
  - Postępowanie z nośnikami:
    - Zarządzanie nośnikami wymiennymi;
    - Wycofywanie nośników;
    - Przekazywanie nośników.
- Kontrola dostępu:
  - Wymagania biznesowe wobec kontroli dostępu:
    - Polityka kontroli dostępu;
    - Dostęp do sieci i usług sieciowych.
  - Zarządzanie dostępem użytkowników:
    - Rejestrowanie i wyrejestrowanie użytkowników;
    - Przydzielanie dostępu użytkownikom;
    - Zarządzanie prawami uprzywilejowanego dostępu;
    - Zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników;
    - Przegląd praw dostępu użytkowników;
    - Odbieranie lub dostosowanie praw dostępu;
  - Odpowiedzialność użytkowników:
    - Stosowanie poufnych informacji uwierzytelniających.
  - 9.4 Kontrola dostępu do systemów i aplikacji:
    - Ograniczenie dostępu do informacji;
    - Procedury bezpiecznego logowania;
    - System zarządzania hasłami;
    - Użycie uprzywilejowanych programów narzędziowych;
    - Kontrola dostępu do kodów źródłowych programów.
- Kryptografia:
  - Zabezpieczenia kryptograficzne:
    - Polityka stosowania zabezpieczeń kryptograficznych;
    - Zarządzanie kluczami.
- Bezpieczeństwo fizyczne i środowiskowe:
  - Obszary bezpieczne:
    - Fizyczna granica obszaru bezpiecznego;
    - Fizyczne zabezpieczenie wejść;
    - Zabezpieczenie biur, pomieszczeń i obiektów;
    - Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi;
    - Praca w obszarach bezpiecznych;
    - Obszary dostaw i załadunku.
  - Sprzęt:
    - Lokalizacja i ochrona sprzętu;
    - Systemy wspomagające;
    - Bezpieczeństwo okablowania;
    - Konserwacja sprzętu;
    - Wynoszenie aktywów;
    - Bezpieczeństwo sprzętu i aktywów poza siedzibą;

- Bezpieczne zbywanie lub przekazywanie do ponownego użycia;
- Pozostawianie sprzętu użytkownika bez opieki;
- Polityka czystego biurka i czystego ekranu.

- Bezpieczna eksploatacja:
  - Procedury eksploatacyjne i odpowiedzialność:
    - Zarządzanie zmianami;
    - Zarządzanie pojemnością;
    - Oddzielanie środowisk rozwojowych, testowych i produkcyjnych.
  - Ochrona przed szkodliwym oprogramowaniem:
    - Zabezpieczenie przed szkodliwym oprogramowaniem.
  - Kopie zapasowe:
    - Zapasowe kopie informacji.
  - Rejestrowanie zdarzeń i monitorowanie:
    - Rejestrowanie zdarzeń;
    - Ochrona informacji w dziennikach zdarzeń;
    - Rejestrowanie działań administratorów i operatorów;
    - Synchronizacja zegarów.
  - Nadzór nad oprogramowaniem produkcyjnym:
    - Instalacja oprogramowania w systemach produkcyjnych.
  - Zarządzanie podatnościami technicznymi:
    - Zarządzanie podatnościami technicznymi;
    - Ograniczenia w instalowaniu oprogramowania.
  - Rozważania dotyczące audytów systemów informacyjnych:
    - Zabezpieczenia audytu systemów informacyjnych.
- Bezpieczeństwo komunikacji:
  - Zarządzanie bezpieczeństwem sieci:
    - Zabezpieczenia sieci;
    - Bezpieczeństwo usług sieciowych;
    - Rozdzielenie sieci.
  - Przesyłanie informacji:
    - Polityki i procedury przekazywania informacji;
    - Porozumienia dotyczące przesyłania informacji;
    - Wiadomości elektroniczne;
    - Umowy o zachowaniu poufności.
- 14 Pozyskiwanie rozwój i utrzymanie systemów:
  - Wymagania związane z bezpieczeństwem systemów informacyjnych:
    - Analiza i specyfikacja wymagań bezpieczeństwa informacji
    - Zabezpieczanie usług aplikacyjnych w sieciach publicznych
    - Ochrona transakcji usług aplikacyjnych
  - Bezpieczeństwo w procesach rozwoju i wsparcia:
    - Polityka bezpieczeństwa prac rozwojowych;
    - Procedury kontroli zmian w systemach;
    - Przegląda techniczny aplikacji po zmianach w platformie produkcyjnej;
    - Ograniczenia dotyczące zmian w pakietach oprogramowania;
    - Zasady projektowania bezpiecznych systemów;
    - Bezpieczne środowisko rozwojowe;
    - Prace rozwojowe zlecane podmiotom zewnętrznym;
    - Testowanie bezpieczeństwa systemów;
    - Testy akceptacyjne systemów.
  - Dane testowe:
    - Ochrona danych testowych.
- Relacje z dostawcami:
  - Bezpieczeństwo informacji w relacji z dostawcami:
    - Polityka bezpieczeństwa informacji w relacjach z dostawcami;
    - Uwzględnianie bezpieczeństwa w porozumieniu z dostawcami;
    - Łańcuch dostaw technologii informacyjnych i telekomunikacyjnych.
  - Zarządzanie usługami świadczonymi przez dostawców:
    - Monitorowanie i przegląd usług świadczonych przez dostawców;
    - Zarządzanie zmianami w usługach świadczonych przez

	dostawców. • Zarządzanie incydentami związanymi z bezpieczeństwem informacji: o Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami: ▪ Odpowiedzialność i procedury; ▪ Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji; ▪ Zgłaszanie słabości związanych z bezpieczeństwem informacji; ▪ Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji; ▪ Reagowanie na incydenty związane z bezpieczeństwem informacji; ▪ Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji; ▪ Gromadzenie materiału dowodowego. • Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania: o Ciągłość bezpieczeństwa informacji: ▪ Planowanie ciągłości bezpieczeństwa informacji; ▪ Wdrożenie ciągłości bezpieczeństwa informacji; ▪ Weryfikowanie, przegląd i ocena ciągłości bezpieczeństwa informacji. o Nadmiarowość: ▪ Dostępność środków przetwarzania informacji. • Zgodność: o Zgodność z wymaganiami prawnymi i umownymi: ▪ Określenie stosownych zmian prawnych i umownych; ▪ Prawa własności intelektualnej; ▪ Ochrona zapisów; ▪ Prywatność i ochrona danych identyfikujących osobę; ▪ Regulacje dotyczące zabezpieczeń kryptograficznych. o Przeglądy bezpieczeństwa informacji: ▪ Niezależny przegląd bezpieczeństwa informacji; ▪ Zgodność z politykami bezpieczeństwa i standardami; ▪ Sprawdzanie zgodności technicznej.