Część 1 – UTM wraz z wdrożeniem

UTM – 1 komplet	
Nazwa komponentu	**Wymagane minimalne parametry techniczne**
Obudowa	Obudowa urządzenia musi być przystosowana do montażu w standardowej szafie 19" (w zestawie muszą znajdować się odpowiednie uchwyty). Obudowa urządzenia nie może być wyższa niż 1U.
Interfejsy	Minimum 12 konfigurowalnych portów 10/100/1000 Mbps RJ-45, 2 konfigurowalne porty SFP, port konsoli (DB9)
Tryby pracy	Urządzenie musi umożliwiać konfigurację trybu router, trybu bridge oraz hybrydowo (router i bridge jednocześnie). Urządzenie musi umożliwiać zdalną konfigurację i monitorowanie poprzez panel sterowania dostępny w technologii chmury, dostarczony bezpłatnie przez producenta urządzenia. Urządzenie musi mieć wbudowany kontroler do zarządzania infrastrukturą WIFI dla maksymalnie 520 punktów dostępowych.
Obsługa łączy mobilnych	Urządzenie musi posiadać co najmniej dwa porty USB 3.0 umożliwiające podłączenie modemu operatora sieci komórkowej i realizację za pośrednictwem w/w adaptera łącza zapasowego.
Protokoły Routingu	Urządzenie musi wspierać routing statyczny, protokoły RIPv1/v2 oraz OSPF, BGP
VLAN 802.1q	Urządzenie musi umożliwiać kreowanie interfejsów VLAN 802.1q. Funkcjonalność ta musi być dostępna w standardzie (bez konieczności zakupu dodatkowych licencji/modułów) Urządzenie powinno obsługiwać nie mniej niż 128 interfejsów VLAN
Sandboxing	Urządzenie musi pozwalać na aktywację co najmniej 36 miesięcznej licencji funkcjonalności sandboxing bez konieczności zakupu dodatkowych licencji/modułów
Web Security	Urządzenie musi pozwalać na aktywację co najmniej 36 miesięcznej licencji funkcjonalności web security bez konieczności zakupu dodatkowych licencji/modułów
Application Patrol	Urządzenie musi pozwalać na aktywację co najmniej 36 miesięcznej licencji funkcjonalności application patrol bez konieczności zakupu dodatkowych licencji/modułów
Anti-Malware	Urządzenie musi pozwalać na aktywację co najmniej 36 miesięcznej licencji funkcjonalności anti-malware bez konieczności zakupu dodatkowych licencji/modułów
IPS	Urządzenie musi pozwalać na aktywację co najmniej 36 miesięcznej licencji funkcjonalności IPS (bez konieczności zakupu dodatkowych licencji/modułów)
Reputation Filter	Urządzenie musi pozwalać na aktywację co najmniej 36 miesięcznej licencji funkcjonalności reputation filter (bez konieczności zakupu dodatkowych licencji/modułów)
Geo Enforcer	Urządzenie musi pozwalać na aktywację co najmniej 36 miesięcznej licencji funkcjonalność geo enforcer (bez konieczności zakupu dodatkowych licencji/modułów)
SSL (HTTPS) inspection	Urządzenie musi pozwalać na aktywację funkcji SSL (HTTPS) inspection
2-Factor Authentication	Urządzenie musi pozwalać na aktywację funkcji 2-Factor Authentication
Microsoft Azure/ Amazon VPC	Urządzenie musi pozwalać na połączenie z chmurą Microsoft Azure lub Amazon VPC
Link Aggregation (LAG)	Urządzenie musi pozwalać na aktywację funkcji Link Aggregation (LAG)

VPN	Obsługa co najmniej 1000 równoczesnych połączeń IPSec VPN/L2TP. Obsługa co najmniej 500 równoczesnych połączeń SSL VPN. Funkcjonalność ta musi być dostępna w standardzie (bez konieczności zakupu dodatkowych licencji/modułów). Przepustowość VPN nie powinna być mniejsza niż 1500 Mbps
Wysoka dostępność	Urządzenie musi wspierać tryb wysokiej dostępności. W przypadku awarii głównego urządzenia, odpowiednio skonfigurowane urządzenie zapasowe musi przejąć obsługę sieci bez ingerencji administratora. Zamawiający wymaga dostarczenia dwóch urządzeń pracujących w trybie wysokiej dostępności.
Monitorowanie oraz raportowanie zdarzeń	Musi istnieć możliwość zapisywania logów na nośniku USB lub dysku twardym podłączonym do urządzenia poprzez interfejs USB oraz wysyłania logów na zewnętrzne serwery syslog. W cenie urządzenia powinna być uwzględniona roczna licencja na aplikację chmurową przeznaczoną do analizowania logów i generowania raportów dotyczących funkcjonowania bramy.
Kształtowanie Pasma	Urządzenie musi umożliwiać elastyczne zarządzanie przepustowością, bezpośrednio na interfejsach jak i pozwalać na zdefiniowanie odpowiedniego pasma dla konkretnych portów i protokołów sieciowych. W przypadku aktywnej licencji IDS/IDP musi istnieć również możliwość definiowania pasma dla wybranych aplikacji.
Autoryzacja użytkowników	Urządzenie powinno umożliwiać autoryzację użytkowników w oparciu o wewnętrzną bazę użytkowników oraz zewnętrzne serwery RADIUS, Microsoft AD, LDAP
Wydajność	Przepustowość dla firewall'a nie powinna być mniejsza niż 8000 Mbps Przepustowość UTM (aktywowane moduły AV, IDP, Firewall) nie powinna być mniejsza niż 1900 Mbps
Maksymalna liczba równoczesnych sesji	Maksymalna liczba równolegle obsługiwanych sesji nie może być mniejsza niż 2 000 000.
Gwarancja	Minimum 36 miesięcy gwarancji na oferowane urządzenie
Serwis	W przypadku awarii urządzenia, wysyłka zastępczego produktu następuje następnego dnia roboczego po tym, w którym zgłoszona zostanie awaria. Urządzenie powinno być objęte w/w opcją serwisową w okresie nie krótszym niż 36 miesięcy.
Inne	Urządzenie musi być fabrycznie nowe i pochodzić z polskiego kanału dystrybucji

Część nr 2 - Serwer backupu wraz z wdrożeniem

Serwer backupu – 1 komplet	
NAZWA KOMPONENTU	**WYMAGANE MINIMALNE PARAMETRY TECHNICZNE**
Obudowa	Obudowa Rack o wysokości max. 2U umożliwiającą instalację min. 8 dysków 3,5" z kompletem szyn umożliwiających montaż w szafie rack.
Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	Zainstalowany minimum jeden procesor min. dwunastordzeniowy klasy x86 do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 174 punktów w teście SPECrate2017_int_base dostępnym na stronie http://www.spec.org dla konfiguracji dwuprocesorowej
RAM	Min. 64GB RDIMM 3200 MT/s

	Min. 16 slotów dla pamięci
Gniazda PCIe	• Min. 1 slot PCI Express x16 low profile, • Min. 1 slot PCI Express x4 low profile
Interfejsy sieciowe/FC/SAS	Min. dwa interfejsy sieciowe 1GbE, Karta sieciowa dwuportowa 10GbE BASE-T
Dyski twarde	Możliwość instalacji dysków SATA, SAS, SSD, NVMe. Zainstalowane dyski: • 2 dyski 480GB SSD SATA 6Gb/s 1 DWPD Hot-Plug • 6 dysków 12TB SAS 12Gb/s min. 7200 rpm 3,5" Możliwość instalacji dwóch dysków M.2 SATA o pojemności min. 480GB oraz możliwość konfiguracji w RAID 1. Możliwość zainstalowania modułu dedykowanego dla hypervisora wirtualizacyjnego, wyposażonego w 2 nośniki typu flash o pojemności min. 32GB. Rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający min. 4GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
Wbudowane porty	min. 2 x port USB 2.0 oraz port USB 3.0, port VGA i drugi port video na przednim panelu obudowy
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900
Wentylatory	Redundantne Hot-Plug
Zasilacze	Dwa zasilacze redundantne Hot-Plug o mocy min. 800W
Diagnostyka	Serwer wyposażony w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze lub inny system diagnostyczny serwera.
Bezpieczeństwo	Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą TPM 2.0
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika • możliwość podmontowania zdalnych wirtualnych napędów • wirtualną konsolę z dostępem do myszy, klawiatury • wsparcie dla IPv6 • integracja z Active Directory • możliwość obsługi przez dwóch administratorów jednocześnie • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej • Możliwość przywrócenia poprzednich wersji firmware • Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001. Serwer musi posiadać deklarację CE. Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status

	„Certified for Windows" dla systemów Microsoft Windows 2016, Microsoft Windows 2019, Microsoft Windows 2022.
Warunki gwarancji	36 miesięcy gwarancji producenta czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez linię telefoniczną producenta. Zamawiający wymaga, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji systemu.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
System operacyjny	Zamawiający wymaga licencji Microsoft Windows Server STD 2022 lub system równoważny. Licencja Serwerowego Systemu Operacyjnego obejmująca wszystkie rdzenie procesora zainstalowanego w zaoferowanym serwerze, lecz nie mniej niż 16 core. Zamawiający dopuszcza licencje OEM lub ROK. Licencja ma umożliwiać downgrade do poprzednich wersji systemu operacyjnego oraz uprawniać do uruchamiania SSO w środowisku fizycznym lub dwóch wirtualnych środowisk systemu operacyjnego serwerze za pomocą wbudowanych mechanizmów wirtualizacji. ***Opis równoważności:*** Serwerowy system operacyjny (dalej: SSO) posiada następujące, wbudowane cechy: 1. Posiada możliwość wykorzystania 320 logicznych procesorów oraz 4 TB pamięci RAM w środowisku fizycznym 2. Posiada możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Posiada możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 7000 maszyn wirtualnych. 4. Posiada możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Posiada automatyczną weryfikację cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Posiada możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które: a) pozwalają na zmianę rozmiaru w czasie pracy systemu,

	b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c) umożliwiają kompresję „w locie” dla wybranych plików i/lub folderów, d) umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10. Posiada wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11. Posiada wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12. Posiada możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 13. Posiada możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14. Posiada wbudowaną zaporę internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15. Graficzny interfejs użytkownika. 16. Zlokalizowane w języku polskim, następujące elementy: a) menu, b) przeglądarka internetowa, c) pomoc, d) komunikaty systemowe. 17. Posiada wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 18. Posiada możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 19. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 20. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management). 21. Posiada możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: 1) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, 2) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: a) Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, b) Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, c) Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. 3) Zdalna dystrybucja oprogramowania na stacje robocze. 4) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej 5) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: a) Dystrybucję certyfikatów poprzez http b) Konsolidację CA dla wielu lasów domeny,

	6) Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen. 7) Szyfrowanie plików i folderów. 8) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). 9) Posiada możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów. 10) Serwis udostępniania stron WWW. 11) Wsparcie dla protokołu IP w wersji 6 (Ipv6), 12) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, 13) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtulne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji zapewniają wsparcie dla: a) Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, b) Obsługi ramek typu jumbo frames dla maszyn wirtualnych, c) Obsługi 4-KB sektorów dysków, d) Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, 14) Posiada możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model) 15) Posiada możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 22. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). 23. Posiada możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 24. Posiada mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 25. Posiada możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

Część nr 3 - Oprogramowanie do backupu wraz z wdrożeniem

Oprogramowanie do backupu – 1 komplet	
NAZWA KOMPONENTU	**WYMAGANE MINIMALNE PARAMETRY TECHNICZNE**
Licencje	Licencja uniwersalna pozwalająca na backup różnego rodzaju maszyn: - maszyny wirtualne (VMware, Hyper-V, Nutanix) - serwery fizyczne (Windows, Linux) - workstacje (Windows, Linux, Mac) - instancje chmurowe (Azure, AWS, Google Cloud) - udziały plikowe NAS Zamawiający wymaga dostarczenia min. 25 licencji wieczystych do backupu wraz z min. 36 miesięcznym wsparciem producenta.

Wymagania ogólne	• Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions, • Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2 i 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej • Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami. • Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manager, klastrami hostów oraz pojedynczymi hostami. • Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
Całkowite koszty posiadania	• Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej • Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków • Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental) • Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji • Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. • Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli. • Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych. • Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.

	• Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time) • Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu • Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API • Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji • Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji • Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania • Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX) • Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
Wymagania RPO	• Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej • Oprogramowanie musi wykorzystywanać mechnizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. • Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych • Oprogramowanie musi oferować ten mechanizm z dokładnością do pojedynczego datastoru • Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora • Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware i być dostępna dla następujących macierzy: HPE, Dell EMC, NetApp, Cisco, IBM, Lenovo, Fujitsu, Huawei, INFINIDAT, Pure Storage. • Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. • Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn • Oprogramowanie musi posiadać wsparcie dla NDMP • Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) • Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.

	• Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC. • Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS. • Repozytoria oparte o XFS muszą pozwalać na zmiezmienność danych przez określoną ilość czasu (tzw Immutability) • Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. • Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. • Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwośc zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO. • Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik • Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding) • Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
Wymagania RTO	• Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. • Dodatkowo dla środowiska vSphere i Hyper-V powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) • Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami • Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre • Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków • Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.

	• Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
	• Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
	• Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików:
	  o Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
	  o Mac: HFS, HFS+
	  o Windows: NTFS, FAT, FAT32, ReFS
	• Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
	• Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
	• Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.
	• Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites.
	• Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),
	• Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska
	• Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych
	• Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska
	• Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych
	• Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint.
	• Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
	• Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego
	• Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
	• Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA
	• Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

Ograniczenie ryzyka	• Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. • Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach. • Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem • Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere • Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32. • Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
Backup serwerów fizycznych oraz workstacji Windows / Linux	• Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego • Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych • Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: o Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE • Rozwiązanie musi wspierać systemy operacyjne macOS • Rozwiązanie musi wspierać wykonywanie kopi zapasowych następujących systemów plików: o NTFS, ReFS, FAT32, ext2, ext3, ext4, ReiserFS, JFS, XFS, F2FS, Brtfs (dla kernela 3.16 i nowszych), APFS, HFS, HFS+, NILFS2 • Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą) • Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów • Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na: o Lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny o Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire o Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS. o Zcentralizowanym repozytorium danych o Bezpośrednio na zasobach Chmury • Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone

	• Rozwiązanie musi wspierać technologię BitLocker • Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania • Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla: o Microsoft Exchange 2010 i nowszych o Microsoft Active Directory 2003 i nowszych o Microsoft Sharepoint 2010 i nowszych o Microsoft SQL 2005 i nowszych o Oracle 11g i nowszych • Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych • Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej • Rozwiązanie musi wspierać tworzenie wielu zadań backupowych
Monitorowanie	• System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich • System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn • System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora • System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard) • System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna • System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego • System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. • System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu. • System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach • System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów • System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych • System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych. • System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)

	• System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

Część nr 4 - SOAR/SIEM wraz z wdrożeniem

Wymagania funkcjonalne dla Systemu.

1. System musi zawierać narzędzia do zautomatyzowanego tworzenia elektronicznej, interaktywnej dokumentacji infrastruktury teleinformatycznej uwzględniając schematy architektury zabezpieczeń sieci tzn. mapy pokazującej urządzenia zabezpieczeń, strefy bezpieczeństwa, zasoby teleinformatyczne, połączenia i topologię sieci LAN/WAN), prezentującej informacje nt. bezpieczeństwa w ujęciu technicznym oraz w odniesieniu do procesów działania organizacji.

2. System musi zawierać bazę wiedzy eksperckiej (tzw. Knowledge Base) uwzględniającej wiedzę, która pozwoli ocenić poprawność projektu zabezpieczeń, identyfikując efektywność zastosowanych mechanizmów sieciowych oraz lokalnych w stosunku do potencjalnych wektorów ataków oraz w przypadku ich niezastosowania zidentyfikować ryzyka, które się z tym wiążą.

3. Dostarczone rozwiązanie musi być systemem klasy SIEM (Security Information Event Management), do którego głównych funkcji należą gromadzenie i korelacja zdarzeń przesyłanych lub pobieranych z innych systemów. Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł, agregację i wzbogacanie danych. Korelacja odbywa się na podstawie zdefiniowanych reguł określających te zależności.

4. Dostarczone rozwiązanie musi być systemem klasy SOAR (Security Orchestration, Automation And Response). Moduł obsługi incydentów może stanowić integralną część systemu SIEM lub być dostarczony w ramach odrębnego, zintegrowanego z systemem SIEM, rozwiązania.

5. Interfejs systemu elektronicznej dokumentacji musi umożliwiać wizualizację informacji o infrastrukturze teleinformatycznej. Wizualizacja musi obejmować interaktywną mapę logiczną sieci z zaznaczonymi strefami sieci, strefami bezpieczeństwa, urządzeniami sieciowymi, połączeniami, systemami zabezpieczeń IT oraz procesami.

6. System musi umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji infrastruktury IT również w formie tabelarycznej.

7. System musi prezentować techniczne informacje nt. bezpieczeństwa IT z perspektywy działalności organizacji, w tym zapisywanie, wyszukiwanie i prezentowanie co najmniej następujących informacji: procesy biznesowe organizacji oraz wspierające je usługi i powiązane z nimi zasoby IT, klasyfikacja zbiorów informacji przetwarzanych w ramach wskazanych procesów oraz przez wskazane zasoby IT, ważność zasobów IT dla organizacji ze względu na typ przetwarzanych danych oraz wspierane procesy, właścicieli zasobów (Owners) oraz zespół IT odpowiedzialny za jego obsługę (Custodians).

8. System musi umożliwiać generowanie elektronicznej dokumentacji sieci i systemów w sposób automatyczny (minimum: na podstawie danych pozyskanych z logów oraz poprzez API) lub za pomocą interfejsu graficznego I tabelarycznego.

9. Interfejs interaktywnej mapy sieci musi umożliwiać wyświetlanie i modyfikowanie szczegółowych informacji o każdym elemencie infrastruktury IT oraz posiadać mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT, który został zdefiniowany w elektronicznej dokumentacji.

10. System musi pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci.

11. System musi pozwalać na dodawanie i przechowywanie załączników powiązanych z obiektami zgromadzonymi w bazie elektronicznej dokumentacji sieci. System powinien akceptować załączniki między innymi w formatach: pdf, MS Word, MS Excel, jpg, png.

12. Dla zdarzeń zawierających adresy IP interfejs musi umożliwiać wyświetlenie dodatkowych informacji o zasobach powiązanych z tymi adresami m.in.: nazwa zasobu, rodzaj zasobu, powiązane usługi, właściciel zasobu, podatności zasobu, powiązane incydenty, lokalizacja.

13. 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.
14. Dla zarejestrowanych zdarzeń/ incydentów system automatycznie wyznaczy ścieżkę ataku i zaprezentuje ją w formie graficznej na schemacie sieci organizacji. Ścieżka ataku pokazuje wszystkie urządzenia zabezpieczeń na drodze pomiędzy celem a źródłem zdarzenia lub incydentu.

15. Dla zdarzeń zawierających adresy IP interfejs musi umożliwiać wyświetlenie dodatkowych informacji o zasobach powiązanych z tymi adresami m.in.: nazwa zasobu, rodzaj zasobu, powiązane usługi, właściciel zasobu, powiązane incydenty, lokalizacja.

16. Informacje o procesach muszą uwzględniać ważność procesów dla organizacji, typy danych przetwarzanych w ramach procesów (np. dane osobowe, informacje poufne itp.), właścicieli procesów, relacje między procesami (np. proces A zależy od procesu B, przy czym zależności powinny być prezentowane w formie graficznej) oraz czas trwania procesów (np. proces praca biurowa w organizacji jest aktywny od poniedziałku do piątku od 8:00 do 16:00).

17. Mechanizmy modułu dokumentacji elektronicznej muszą umożliwiać powiązanie danych o zasobach z informacjami pozyskanymi w rezultacie skanowania podatności.

18. 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).

19. W ramach obsługi zdarzeń/incydentów/podatności system powinien prezentować informacje o wynikach szacowania ryzyka dla zasobów związanych z incydentem oraz ocenę wpływu incydentu na organizację w przypadku materializacji zagrożenia.

20. System musi pozwalać na zautomatyzowane szacowanie ryzyka dla wszystkich systemów IT zdefiniowanych w elektronicznej dokumentacji. Szacowanie ryzyka powinno odbywać się względem zagrożeń natury informatycznej, np.: przełamanie zabezpieczeń, wyciek danych, infekcja złośliwym programem, podsłuch sieciowy.

21. System w razie wykrycia incydentów o wysokim ryzyku materializacji zagrożenia natury technicznej (m.in. przełamanie zabezpieczeń, infekcja złośliwym oprogramowaniem) umożliwi automatyczne powiadamianie o incydencie wskazanych pracowników, m.in. za pomocą email i SMS.

22. System w razie wykrycia incydentów o poważnych konsekwencjach dla organizacji umożliwi automatyczne powiadamianie o incydencie wskazanych pracowników, m.in. za pomocą email i SMS.

23. System powinien umożliwiać automatyczne wyszukiwanie pojedynczych, potencjalnych punktów awarii sieci I systemów IT, których uszkodzenie może spowodować zablokowanie krytycznych usług w organizacji.

24. System ma posiadać narzędzia do modelowania zagrożeń, umożliwiając symulowanie potencjalnych scenariuszy bezpieczeństwa. Interfejs mapy sieci musi pozwalać m.in. na:

a. wyznaczenie źródła zagrożenia zasobu teleinformatycznego wraz z wynikiem analizy ryzyka dla tego zagrożenia wyliczanym w sposób automatyczny,
b. wyświetlanie zabezpieczeń zasobu teleinformatycznego przed potencjalnymi źródłami zagrożenia,
c. wyświetlanie zabezpieczeń chroniących zasoby teleinformatyczne przed określonym źródłem zagrożenia,
d. wyświetlanie lokalizacji zasobów określonego rodzaju,
e. wyświetlanie najbardziej narażonych zasobów teleinformatycznych,
f. wyświetlanie ważnych zasobów teleinformatycznych narażonych na awarie.

25. System musi umożliwiać uwzględnianie danych zgromadzonych w elektronicznej dokumentacji infrastruktury teleinformatycznej w mechanizmach korelacji zdarzeń. Wykryte zdarzenia/ incydenty będą priorytetyzowane w odniesieniu do ważności dla organizacji zasobów, których dotyczą (np.: wspomaganych procesów, przetwarzanych informacji klasyfikowanych).

26. Rozwiązanie musi umożliwić korelację zdarzeń pochodzących z różnych urządzeń, punktów końcowych i aplikacji z anomaliami wykrywanymi w przepływach sieciowych oraz podatności pozyskanych bezpośrednio ze skanerów aplikacyjnych i bazy CVE.

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

28. System musi umożliwiać wykorzystanie baz reputacyjnych w regułach korelacyjnych.

29. System musi umożliwiać automatyczne dodawanie i usuwanie list referencyjnych na podstawie reguł korelacyjnych umożliwiających zdefiniowanie warunków na podstawie których listy te będą modyfikowane. System musi umożliwiać definiowanie list referencyjnych łączących unikalne wartości w pojedynczym wierszu np: login, adres IP, aplikacja.

30. System musi być wyposażony w mechanizmy reguł opartych na mechanizmach behawioralnych z możliwością agregacji danych oraz punktowania poszczególnych zdarzeń w wyznaczonych oknach czasowych. W rezultacie działania reguł behawioralnych, system powinien tworzyć incydenty związane z przekroczeniem dozwolonych zakresów punktacji dla zdarzeń zaobserwowanych w oknie czasowym agregacji.

31. System musi umożliwiać uwzględnianie danych zgromadzonych w elektronicznej dokumentacji infrastruktury teleinformatycznej w scenariuszach obsługi incydentów. Scenariusze obsługi incydentów muszą być uzależnione od ważności dla organizacji zasobów, których dotyczą (np.: wspomaganych procesów, przetwarzanych informacji klasyfikowanych).

32. System musi umożliwiać wykorzystanie baz reputacyjnych w ramach scenariuszy obsługi incydentów (ang. Playbook).

33. System musi zapewnić graficzny interfejs wspierający proces obsługi incydentów, którego zadaniem będzie wspieranie użytkownika w realizacji zadań związanych z selekcją zdarzeń, analizą incydentów, oceną wpływu i reakcją na incydenty. Do zadań tych należą między innymi:

a. wzbogacanie danych kontekstowych,
b. gromadzenie artefaktów danych związanych z incydentem,
c. współpraca z innymi członkami zespołu,
d. komunikacja w ramach zespołu,
e. wykonywanie czynności związanych z reakcją na incydent,

f. raportowanie przebiegu incydentu.

34. System musi być wyposażony w graficzny interfejs prezentujący w formie wykresów dane statystyczne związane z procesem obsługi incydentów/podatności. Wykresy muszą umożliwiać prezentację danych uwzględniających co najmniej: ilość incydentów w czasie w podziale na priorytety, czasy reakcji i obsługi oraz bieżące ilości incydentów obsługiwanych przez poszczególnych użytkowników.

35. System powinien posiadać zestaw predefiniowanych scenariuszy obsługi (ang. Playbook).

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

37. System powinien pozwalać na przekazywanie aktywnych linków pomiędzy zintegrowanymi systemami, a otwarcie linku powinno bezpośrednio przekierowywać operatora do konsoli systemu zewnętrznego.

38. System powinien umożliwiać automatyczną zmianę statusu incydentu na podstawie informacji pobranych z innych systemów np.: identyfikacja IoC.

39. System musi umożliwiać zbieranie, przechowywanie i przypisywanie wskaźników kompromitacji (IoC) do incydentów.

40. System powinien udostępniać automatyczny raport z wszystkich podjętych działań w ramach incydentu.

41. System musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych danych przez ich podział na pola, na podstawie których może odbywać się dalsze przetwarzanie oraz wyszukiwanie danych. Mechanizm musi umożliwiać m.in. parsowanie warunkowe, parsowanie hierarchiczne, wzbogacanie zdarzeń o dodatkowe pola, mapowanie wartości, czy wykorzystanie gotowych parserów przy tworzeniu nowych.

42. Parsowanie warunkowe i hierarchiczne musi być konfigurowalne i obsługiwać następujące metody normalizacji: REGEX, JSON, XML, CEF, LEEF, SYSLOG. Musi umożliwiać wykorzystanie gotowych parserów jako elementów podrzędnych hierarchii oraz wykorzystywanie ich w warunkach.

43. Proces normalizacji musi odbywać się na bieżąco na etapie rejestrowania danych w systemie.

44. 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.

45. System musi zapewnić normalizację (parsowanie) logów protokołami Syslog, TLS Syslog, Netflow, obsługiwać pliki płaskie (ang. flat file), zapytania do bazy danych poprzez sterownik ODBC oraz odbierać wiadomości email.

46. Oferowane rozwiązanie powinno zapewniać możliwość zbierania logów z systemów Microsoft Windows poprzez mechanizm Windows Event Forwarding (WEF) bez konieczności instalowania dedykowanego oprogramowania w tych systemach.

47. Normalizacja logów musi posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól o nazwę lub kod kraju korzystając z wbudowanej w produkt bazy.
48. Normalizacja musi uwzględniać możliwość nadawania kategorii zdarzeń na podstawie wartości parsowanych pól, np. logowanie, wylogowanie, zmiana uprawnień, malware, vulnerability.

49. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych.

50. System musi posiadać predefiniowany zestaw parserów.

51. System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) logów z niestandardowych źródeł danych, w oparciu o składnię wyrażeń regularnych oraz formaty JSON, XML, CIS, LEEF, Syslog. System musi umożliwiać zastosowanie wszystkich typów składni dla pojedynczego zdarzenia.

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

53. System musi umożliwiać definiowanie zakresu i czasu uczenia, np.: analiza logowania użytkowników po godzinach pracy, analiza alarmów systemu SIEM. Po wdrożeniu nie będzie wymagane żadne dostrojenie systemu.

54. System musi mieć możliwość wzbogacania kontekstu odbiegającego od normalnego zachowania użytkownika korzystając z danych zewnętrznych, minimum: Threat Intelligence, Active Directory. Przykładowe zastosowanie integracji zakłada wykorzystanie zasobów zewnętrznych, z których dane mogą podnieść skumulowaną ocenę ryzyka dla sesji użytkownika.

55. System musi posiadać funkcję „automatycznej korelacji", tzn. posiadać zaszyte mechanizmy i reguły korelacji, które po wdrożeniu i „nauce środowiska zamawiającego", będą przedstawiać właściwe incydenty dla operatorów bez dodatkowej ingerencji w reguły.

56. System musi zapewniać możliwość budowania modeli zachowania użytkowników dla zebranych danych historycznych ze skonfigurowanego (wskazanego) okresu.

57. System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych.

58. Dostarczone rozwiązanie musi być objęte 12 miesięcznym wsparciem producenta lub producentów. Wsparcie musi obejmować bezpłatne dostarczanie aktualizacji oprogramowania oraz reagowanie na zgłaszane błędy systemowe. 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).

59. Rozwiązania SIEM/UEBA, SOAR, narzędzia elektronicznej dokumentacji, narzędzie analizy ryzyka cyberzagrożeń oraz baza wiedzy mogą być dostarczone w ramach odrębnych rozwiązań, jednakże muszą być zintegrowane w sposób umożliwiający spełnienie wszystkich wymagań z poziomu jednej konsoli. Dostarczone rozwiązanie/ rozwiązania nie mogą działać w oparciu o technologię typu open-source.

60. Interfejs użytkownika Systemu musi być w języku polskim lub umożliwiać wgranie plików językowych tłumaczących interfejs na język polski. Musi być przejrzysty i konfigurowalny, poprzez pogrupowanie zawartości w bloki tematyczne, co ma umożliwić łatwe i szybkie wyszukiwanie odpowiednich danych.

61. Funkcjonowanie rozwiązania musi być oparta w całości o architekturę „on-premise", w której przetwarzane dane nie są przesyłane poza infrastrukturę Zamawiającego.

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

63. Dopuszczalne jest dostarczenie rozwiązania jako tzw. wirtualnego appliance pod warunkiem że obraz appliance jest udostępniany do pobrania przez producenta dostarczonego rozwiązania na jego oficjalnej stronie internetowej w postaci utwardzonego rozwiązania, łącznie z dedykowanym systemem operacyjnym, dla którego Producent regularnie dostarcza aktualizacje, w tym poprawki bezpieczeństwa.

64. System musi zapewniać możliwość współpracy z popularnymi bazami danych, a w tym co najmniej z: MS SQL, Oracle, DB2.

65. System powinien umożliwiać nadawanie uprawnień do obiektów/modułów systemu dla poszczególnych operatorów lub grup operatorów.

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

67. System musi dokonywać automatycznej integracji z usługą katalogową Microsoft Active Directory celem pobrania informacji o poświadczeniach i zasobach zarejestrowanych w domenie AD, minimum to: nazwa użytkownika, login, e mail, nazwa komputera, przynależność do grup, przełożonego, jednostkę organizacyjną oraz konta uprzywilejowane.

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

69. Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień do definiowalnych grup odbiorców (co najmniej: powiadamianie email oraz SMS, opcjonalnie czat).

70. System musi być dostępny z poziomu dedykowanego klienta aplikacji lub obsługiwany za pomocą dowolnej przeglądarki internetowej (Chrome, Edge, Firefox), bez konieczności instalowania jakichkolwiek dodatków dla prawidłowego jego działania.

71. System musi umożliwiać przypisanie poziomów krytyczności do monitorowanych zasobów, które będą brane pod uwagę w ewaluacji zagrożeń.

72. System musi umożliwiać mapowanie zdarzeń korelacyjnych na framework Mitre ATT&CK.

73. System musi być wyposażony w graficzny interfejs umożliwiający przeglądanie i przeszukiwanie zarejestrowanych danych 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.

74. Tworzenie raportów PDF musi posiadać opcje automatycznego harmonogramu, który w zadanym wcześniej momencie pozwoli na wysyłkę utworzonego raportu do zdefiniowanych odbiorców poczty email. Konfiguracja harmonogramu tworzenia raportów PDF i ich wysyłki powinna być dostępna poprzez graficzny interfejs użytkownika.

75. System musi rejestrować i przechowywać pozyskane dane w wersji pierwotnej oraz w wersji znormalizowanej.

76. System musi zapewniać klasyfikację zdarzeń za pomocą notacji punktowej definiującej ich poziom zagrożenia (ryzyko).

77. Interfejs systemu powinien umożliwiać z poziomu jednego okna widoku weryfikację wszystkich działań użytkownika na osi czasu, które spowodowały wzrost ryzyka. Z poziomu tego widoku system umożliwi przejście do opisu konkretnego zdarzenia.

78. System powinien w formie graficznej prezentować podsumowanie aktualnego stanu bezpieczeństwa, m.in. usługi zagrożone przez incydenty oraz podatności, średni czas obsługi incydentu lub podatności.

79. System pozwoli na prezentację danych w postaci tzw. „Dashboard", tj. dostosuje zakres i prezentacje danych do potrzeb administratora czy też zalogowanego użytkownika.

80. System musi automatycznie wyodrębnić konta użytkowników oraz ich kontekst, minimum przynależność do odpowiednich grup domenowych, konta serwisowe, użytkowników uprzywilejowanych, użytkowników w randze kierowniczej i zarejestrowane stacje robocze celem automatycznej dystrybucji tych danych do odpowiednich narzędzi systemu.

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

82. System musi umożliwiać przechowywanie teczek incydentów zawierających dowody, próbki, logi oraz inne powiązane z danym incydentem informacje.

83. System musi potrafić wczytywać informacje z innych systemów bezpieczeństwa i traktować je, jako elementy/dowody w teczkach Incydentów.

84. System musi umożliwiać powiązanie każdego zdarzenia/incydentu z odpowiednim priorytetem (definiowanym automatycznie z możliwością manualnej zmiany).

85. System powinien posiadać możliwość rejestracji zgłoszeń i przekształcenia ich w incydenty bezpieczeństwa z możliwością rozdzielenia uprawnień dla obu tych czynności.

86. System powinien mieć logikę automatycznego przypisywania zgłoszeń, minimum na podstawie dostępności operatora, jego obciążenia, oraz cech zasobu którego dotyczy incydent, minimum typ zasobu (np.: serwer lub stacja robocza), krytyczność oraz realizowane z jego udziałem usługi z katalogu usług.

87. System musi umożliwiać grupowanie manualne w jeden incydent bezpieczeństwa zdarzenia podobne/powiązane np. wielokrotnie raportowane, przez systemy źródłowe, wielokrotnie zgłoszone przez użytkowników.
88. System powinien grupować automatycznie w jeden incydent bezpieczeństwa zdarzenia podobne/powiązane np. wielokrotnie raportowane, przez systemy źródłowe, wielokrotnie zgłoszone przez użytkowników.

89. System powinien umożliwiać obsługę tzw. lawinowych incydentów (incydenty takie same, lecz pochodzące od różnych użytkowników lub systemów) poprzez podłączanie ich do jednego głównego incydentu oraz nadanie odpowiedniego priorytetu tego typu zdarzeniom. Zamkniecie głównego incydentu/zdarzenia powinno umożliwiać zamykanie powiązanych z nim incydentów/zdarzeń w trybie manualnym (operator) lub automatycznym (system). W podglądzie incydentu powinna się pojawić informacja o podpiętych incydentach.

90. System musi pozwalać na określenie automatycznych oraz inicjowanych przez operatora reakcji na incydenty bezpieczeństwa i/lub zdarzenia, polegających na integracji z systemami zewnętrznymi w celu uzyskania dodatkowych informacji, dotyczących incydentu/zdarzenia lub podjęcia akcji zapobiegawczych.

91. System musi umożliwiać wykonywanie działań remediacyjnych na stacjach roboczych/serwerach (pobieranie logów, uruchamianie skryptów, weryfikacja rejestrów, itp.).

92. System musi umożliwiać przypisywanie i przekazywanie incydentów do operatorów lub grup operatorów

93. System musi pozwalać na zbieranie danych i reputacji z systemów klasy Threat Intelligence minimum to IP, FQDN, URL, Hash.

94. System powinien pozwalać, przy użyciu języków skryptowych ogólnie dostępnych (np. Python lub/i PowerShell), na skonfigurowanie nowych, nie uwzględnionych przez producentów rozwiązania możliwości integracyjnych z zewnętrznymi systemami.

95. System powinien umożliwiać przeglądanie listy zasobów (urządzeń, systemów, osób, itp.) pod kątem poziomu

I ilości incydentów, które są z nimi powiązane.

96. System musi mieć możliwość automatycznego informowania o zmianie statusu incydentu (minimum: wygenerowaniu, przypisaniu, przekroczeniu czasu SLA oraz zamknięciu karty incydentu).

97. System powinien umożliwiać ustawienie parametrów SLA bazując na ustalonym automatycznie priorytecie zdarzania/incydentu/podatności. System musi dokonywać automatycznego pomiaru tych czasów i weryfikacji ich do zdefinowanych wymagań SLA. Wyniki pomiaru czasu powinny być stale aktualizowane i prezentowane w interfejsie systemu.

98. System powinien umożliwiać dodawanie, modyfikację i usuwanie umów SLA, które zawierają co najmniej następujące parametry: data rozpoczęcia i zakończenia obowiązywania umowy, jednostka organizacyjna (struktura jednostek), której dotyczy umowa, lista usług z katalogu usług, których dotyczy umowa.

99. System musi zawierać mechanizm integracji ze skanerami podatności co najmniej dwóch producentów oraz co najmniej jednym skanerem podatności dostępnym na zasadach open source. W ramach integracji system musi mieć możliwość uruchamiania skanowania podatności i importowania jego wyników. Silnik skanujący, będący źródłem podatności musi zostać dołączony do oferty systemu bezpieczeństwa.
100. Interfejs modułu obsługi incydentów musi prezentować listę podatności zasobów związanych z incydentem.

101. System musi automatycznie ustalać priorytety podatności w odniesieniu do ważności podatnych systemów IT dla organizacji oraz oceny technicznej zagrożenia bazującej na wartości CVSS lub wartości pozyskanej bezpośrednio z silnika skanera.

102. System powinien uwzględniać w ocenie zdarzeń i incydentów, informacje o podatnościach technicznych wykrytych przez narzędzia do zarządzania podatnościami zarówno przez import raportu jak i integrację przez API.

103. System musi zawierać mechanizm definiowania harmonogramów skanowania podatności oraz na ich podstawie automatycznie uruchamiać procesy skanowania i analizowania uzyskanych raportów.

104. System musi umożliwiać obsługę podatności w ramach scenariuszy obsługi (playbook).

105 . System SIEM oraz wszystkie moduły towarzyszące muszą umożliwiać równoczesną pracę co najmniej 10 operatorów oraz objąć monitoringiem min. 300 zasobów IT. Przez zasób IT rozumie się serwery fizyczne lub serwery wirtualne oraz komputery użytkowników. Ilość danych przekazywanych do systemu, tj. EPS (Events Per Second) oraz ilość kolektorów agregujących i parsujących nie może powodować zmian w zakresie licencjonowania. Wykonawca udzieli Zamawiającemu wieczystej, nieograniczonej czasowo licencji na zakupiony System.

106. System ma gwarantować możliwość elastycznej rozbudowy o dalsze zasoby IT, które w przyszłości zostaną objęte jego działaniem.

107. Po zakończonym wdrożeniu należy zapewnić bezpłatne 3-dniowe certyfikowane szkolenia (3 x 8h) zakresie użytkowania i administrowania wdrożonego systemu lub systemów dostarczonych w ramach zamówienia. Szkolenie ma zostać przeprowadzone dla maksymalnie 10 osób i uwzględniać informacje z zakresu wdrożonego systemu SIEM i SOAR (m.in. zarządzanie incydentami bezpieczeństwa; kompletowanie informacji potrzebnych do opracowania raportu o incydencie; szacowanie ryzyka itp.). Szkolenia muszą być zakończone certyfikatem potwierdzającym wspomniane umiejętności wydanym przez producenta systemu. Szkolenia mogą odbyć się w formie zdalnej.

108. Wykonawca przekaże Zamawiającemu wszelkie, niezbędne do poprawnego korzystania z wdrożonego rozwiązania, informacje o specyfice systemu oraz informacje techniczne na temat jego prawidłowej eksploatacji (tj. dokumentację powdrożeniową oraz instrukcję/instrukcje obsługi).

109. Wykonawca zainstaluje i skonfiguruje oprogrmowanie na dostarczonym w postępowaniu serwerze lub dostarczy dodatkowe urządzenie do uruchomienia oprogramowania SOAR/SIEM.

Szczegółowy zakres i wytyczne procesu wdrożenia systemu

1. Proces wdrożenia systemu powinien zostać zrealizowany zgodnie z opisanymi niżej wytycznymi oraz zatwierdzonym harmonogramem, umożliwiając efektywne wdrożenie rozwiązania.
2. Proces wdrożeniowy podzielony zostanie na obszary:
   a. Obszar Analizy, zakładający stworzenie elektronicznej dokumentacji organizacji wraz z podłączeniem I skonfigurowaniem mechanizmów szacowania ryzyka pod kątem kluczowych zasobów IT i procesów organizacji (budowa kontekstu organizacji);
   b. Obszar Detekcji, zakładający podłączenie i konfigurację narzędzi odpowiedzialnych za wykrywanie zdarzeń I incydentów bezpieczeństwa w ramach zainstalowania modułu SIEM;
   c. Obszar Reakcji, zakładający podłączenie i konfigurację mechanizmów wspomagających proces automatyzacji reakcji na wykryte zdarzenia, incydenty bezpieczeństwa i podatności w ramach zainstalowania modułu SOAR;

3. Obszar Analizy ma na celu identyfikację potencjalnych cyber zagrożeń oraz możliwych konsekwencji na jakie narażona jest organizacja. Zakres prac powinien uwzględniać kolejno:
   a. Pracę z konsultantem (w zakresie m.in. wprowadzenia do metodyki, uzupełnienia ankiety przedwdrożeniowej oraz przygotowania i zatwierdzenia harmonogramu prac);
   b. Uruchomienie systemu w infrastrukturze zamawiającego, w tym:
      • konsultacje w przygotowaniu infrastruktury Zamawiającego do instalacji systemu,
      • przygotowanie przez Zamawiającego połączenia zdalnego,
      • instalację lub import maszyny wirtualnej typu „software appliance”,
      • aktywację licencji,
      • wstępną konfigurację,
      • import/wprowadzenie tabeli adresacji znaczących stref bezpieczeństwa, wymaganych przez mechanizmy wykrywania (np.: sieci serwerów, sieci DMZ, sieci LAN);
   c. Podłączenie głównego źródła zdarzeń opisującego komunikację sieciową, w tym:
      • przekierowanie logów opisujących transmisje sieciową (traffic) z zapór sieciowych (Firewall) na kolektor systemu,
      • uruchomienie reguł wykrywania;
   d. Prace audytowe, w tym:
      • pasywną analizę transmisji sieciowej:
         o ruch z/do serwerów webowych i aplikacyjnych,
         o ruch z/do serwerów baz danych,
         o ruch z/do serwerów pocztowych,
         o ruch z/do kontrolerów domenowych,
         o ruch z/do serwerów usług podstawowych (m.in. DNS/NTP),
         o ruch z/do zasobów zidentyfikowanych na bazie charakterystyki i wolumenu ruchu oraz możliwości identyfikacji aplikacji,
      • konsultacje w ramach otrzymanych wyników;
      • zebranie danych audytowych wymaganych do sporządzenia raportu;
   e. Analizę podatności, w zakresie:
      • integracji po API ze wskazanym przez zamawiającego komercyjnym skanerem/ skanerami podatności lub zainstalowanie skanera podatności typu open source;
      • przygotowanie reguł priorytetów i importu krytycznych podatności;
   f. Przygotowanie dynamicznego raportu audytowego w oparciu o dostępne w systemie narzędzia elektronicznej dokumentacji i szacowania ryzyka obejmującego analizę prawdopodobieństwa przełamania zabezpieczeń organizacji. Raport powinien zawierać:

- zidentyfikowane zagrożenia oraz prawdopodobieństwo ich wystąpienia;
- potencjalne wektory ataków dla wykrytych zagrożeń;
- wizualizacja graficzna wykrytych źródeł zagrożeń oraz wektorów ataków;
- rekomendacja zabezpieczeń;
- zidentyfikowane zagrożenia związane z podatnościami oraz prawdopodobieństwo wykorzystania ich do przełamania zabezpieczeń;

4. Obszar Detekcji ma na celu uruchomienie i dostrojenie mechanizmów wykrywania zagrożeń. Zakres prac powinien uwzględniać kolejno:

a. Podłączenie (przekierowanie przez Zamawiającego do systemu) źródeł zdarzeń i ich dalszą konfigurację w systemie. Kluczowe źródła zdarzeń obejmują:

- zapory sieciowe w punkach styku z siecią Internet (Firewall brzegowy);
- sieciowe systemy bezpieczeństwa dedykowane do wykrywania incydentów bezpieczeństwa (np.: Sandbox, IDP/IPS, AntySpam)
- centralne systemy, dedykowane do kontroli złośliwego oprogramowania na stacjach końcowych/Serwerach, umożliwiające wykrywanie aktywności złośliwego oprogramowania (np.: AntyWirus, EDR);
- kontroler domenowy oraz system zarządzania dostępem uprzywilejowanym;
- systemy detekcji anomalii w przepływach lub zdarzeniach (np.: NBA);
- system SIEM
- źródła, muszą zostać powiązane z parserami, pozwalającymi na detekcję zgodną z wbudowanymi w system regułami korelacji;

b. Adaptację reguł profilowych, pozwalających na dostosowanie zdarzeń do zasobów, których dotyczą;

c. Podłączenie reguł detekcji;

d. Podłączenie i konfiguracja mechanizmów UEBA:

- integracja z Active Directory
- adaptacja profili użytkowników UBA
- adaptacja profili hostów EBA
- import reguł bezpieczeństwa UEBA, uruchomienie procesu uczenia

5. Obszar Reakcji ma na celu uruchomienie i dostrojenie mechanizmów automatyzacji w działaniach reagowania na wykryte zagrożenia bezpieczeństwa. Zakres prac powinien uwzględniać:

a. import gotowych scenariuszy obsługi

b. Konfigurację zespołów obsługi, celem właściwej adresacji podatności oraz zdarzeń wymagających obsługi

c. Konfigurację mechanizmów powiadamiania

Część nr 5 - Szkolenia dla kadry zarządzającej max. dla 10 osób

Część I

- Zakres przedmiotowy i podmiotowy obowiązywania przepisów dotyczących cyberbezpieczeństwa.
- Obowiązki podmiotów publicznych, w tym jednostek samorządu terytorialnego.
- Obowiązki podmiotu publicznego uznanego za operatora usługi kluczowej.
- Struktura krajowego systemu cyberbezpieczeństwa.
- Zadania i rola CSIRT NASK - Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego.

Część II

- Wprowadzenie do wymagań Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).
- Omówienie założeń wdrożenia (SZBI).
- Zakres i granice (SZBI).
- Polityka bezpieczeństwa informacji (SZBI).
- Cele bezpieczeństwa informacji (SZBI).

- Podejścia do szacowania ryzyka.
- Audyty (SZBI).
- Przegląd zarządzania – rola w procesie doskonalenia (SZBI).
- Kluczowe czynniki skutecznego spełnienia wymagań bezpieczeństwa informacji.

1.1. **Szkolenia dla osób zatrudnionych u świadczeniodawcy w wymiarze 2h.**

- Polityka haseł – praktyczne podejście i narzędzia wspomagające.
- Vhishing / ID Call Hijacking – aspekty bezpieczeństwa telefonów.
- Zagrożenia związane z nieznanym sprzętem – jak np. nieznany pendrive może zaszkodzić całej instytucji.
- Spear Phishing – wszystko co „powiesz" (w sieci) może zostać użyte przeciwko Tobie
- – praktyczne aspekty „zachowania" w sieci.
- Ataki Bruteforce / Ataki Słownikowe – podstawowe metody łamania haseł;
- Web Archive – Internet nie zapomina.
- Pliki Cookies – czym są popularne „ciasteczka".
- Metadane – czyli dane o danych.
- Phishing / Spoofing – nigdy nie wiesz kto jest po drugiej stronie.
- Socjotechniki – podstawowe definicje i przykłady użycia.
- Data Leak – czym jest i jakie zagrożenia niesie.
- Dobre praktyki - kilka zasad podnoszących bezpieczeństwo.

Część nr 1, 2, 3 - Wdrożenie

- Wykonawca zobowiązany jest dostarczyć i uruchomić wymienioną powyżej platformę Infrastruktury serwerowej (UTM, serwer backupu oraz oprogramowanie do backupu) dla prawidłowego funkcjonowania Szpitalnego Systemu Informatycznego.
- Jeżeli zajdzie potrzeba, wraz z dostarczoną Infrastrukturą Serwerową, Wykonawca zobowiązany jest dostarczyć niezbędne elementy np. urządzenia i wyposażenie – kable połączeniowe, elementy mocujące, uznane przez Wykonawcę za niezbędne i umożliwiające prawidłowe działanie całego Systemu. Dostarczona Infrastruktura Serwerowa musi zapewniać bezproblemową pracę po podłączeniu jej do sieci informatycznej Zamawiającego.
- Wykonawca jest zobowiązany dokonać montażu dostarczonej Infrastruktury Serwerowej oraz oprogramowania w miejscach wskazanych przez Zamawiającego.
- Wszystkie elementy Infrastruktury serwerowej powinny zostać zamontowane w szafie serwerowej rack, w sposób umożliwiający ich prawidłową wentylację.
- W zakresie części serwerowej w ramach postępowania wymagane jest wykonanie następujących usług:

1. Instalacja fizyczna dostarczonej Infrastruktury
   a) Przygotowanie planu instalacji:
      - zestawienie dostarczanych urządzeń,
      - propozycja rozmieszczenia elementów w istniejących szafach rackowych,
      - propozycja testów odbiorczych,
   b) Instalacja, montaż i uruchomienie serwera kopii zapasowej:
      - montaż serwera w istniejącej szafie rackowej,
      - podłączenie serwera do sieci LAN i SAN do istniejących przełączników LAN i SAN,
      - podłączenie serwera do zasilania,
      - inicjalne uruchomienie serwera backupu,
      - testy działania serwera oraz weryfikacja parametrów,
   c) Instalacja, montaż i uruchomienie UTM-ów:
      - montaż UTM-ów w szafie rack,
      - podłączenie UTM-ów do sieci LAN do istniejących przełączników LAN,

- podłączenie UTM-ów do zasilania,
- inicjalne uruchomienie UTM-ów,
- testy działania UTM-ów oraz weryfikacja parametrów,

2. Instalacja oprogramowania systemowego oraz backupowego:
   a) Inwentaryzacja stanu obecnego:
      - zestawienie nazewnictwa poszczególnych elementów istniejącego systemu,
      - zestawienie zainstalowanych wersji oprogramowania,
   b) Przygotowanie projektu technicznego:
      - zestawienie stosowanej nomenklatury,
      - rysunki logicznej struktury systemu,
      - propozycję nazewnictwa poszczególnych elementów systemu wirtualizacji,
      - zestawienie wymaganych wersji oprogramowania,
      - propozycje konfiguracji polityk bezpieczeństwa dla UTM-ów – uzgodnienia polityk bezpieczeństwa z Zamawiającym,
      - propozycje konfiguracji systemu backupu,
   c) Implementacja zgodna z projektem:
      - Instalacja oprogramowania systemowego i backupowego,
      - Konfiguracja oprogramowania systemowego i backupowego,
      - Konfiguracja UTM-ów zgodnie z wytycznymi Zamawiającego,
      - Aktywacja dostarczonego oprogramowania,
   d) Przygotowanie dokumentacji powykonawczej. Winna ona zawierać:
      - zestawienie stosowanej nomenklatury,
      - rysunki logicznej struktury systemu produkcyjnego i backupu,
      - zestawienie nazewnictwa poszczególnych elementów systemu,
      - zestawienie konfiguracji UTM-ów,
      - zestawienie konfiguracji systemu backupu,
      - zestawienie wersji zainstalowanego oprogramowania.

- Po zakończonym montażu Wykonawca przekaże Zamawiającemu wszystkie hasła dostępowe do kont „super użytkowników" oraz dokumentację do wszystkich oferowanych urządzeń, oprogramowania narzędziowego (systemowego, backupowego itd.) wraz z dokumentami potwierdzającymi nabycie dla Zamawiającego licencji oraz dostępami do zainstalowanego oprogramowania.
- Wykonawca wykona również instruktaże użytkowe dla wskazanych przez Zamawiającego dwóch administratorów, z zakresu konfiguracji, obsługi i prawidłowej eksploatacji zainstalowanego Sprzętu ze szczególnym uwzględnieniem obsługi i zaawansowanego systemu kopii zapasowych w środowisku Zamawiającego.

Część nr 6 – Wykonanie audytu bezpieczeństwa – 1 audyt

Audyt ma w szczególności wykazać podniesienie poziomu bezpieczeństwa teleinformatycznego w odniesieniu do poziomu wynikającego z ankiety lub jego brak. Raport winien zawierać jasne stanowisko audytora w zakresie wykazania, że spożytkowane środki wpłynęły na podniesienie poziomu bezpieczeństwa. Zaleca się również dokonanie audytu w zakresie ustawowych obszarów działalności podmiotu w tym w szczególności:
- weryfikacja struktury organizacyjnej oraz przepływu dokumentów elektronicznych,
- analizy zewnętrznej i wewnętrznej sieci komputerowej,
- analizy serwerów,
- testów dostępu do sieci wenętrznej i zewnętrznej,
- analizy stacji roboczych,
- analizy kopii zapasowych,
- analizy poczty email,
- analizy ogólnego bezpieczeństwa danych i mechanizmów kontroli w podmiocie

- opracowanie dokumentacji audytowej – raprtu z wytycznymi do podniesienia doskonalenia poziomu bezpieczeństwa wraz z rekomendacjami.