**Wdrożenie systemu SIEM**

**Dostawa i wdrożenie Systemu Zbierania i Analizy Logów, Systemu SIEM (Security Information and Event Management) wraz z modułami EDR, NDR oraz wsparciem na 36 miesięcy dla 900 adresów IP.**

1. **Wymagania dla Systemu Zbierania i Analizy Logów oraz Systemu SIEM.**

## Wymagania dla Systemu Analizy Logów

### W ramach systemu logowania i raportowania musi zostać dostarczone rozwiązanie monitorujące, gromadzące logi, korelujące zdarzenia i generujące raporty na podstawie danych z systemów bezpieczeństwa.

### Rozwiązanie musi zostać wdrożone na stanowiskach zarządzania systemu SIEM (poz. 17 formularza cenowego, załącznik A12) w środowisku VMware Workstation, w taki sposób aby umożliwiały administratorowi zarządzanie systemem.

### Pozostałe elementy rozwiązania muszą zostać dostarczone w postaci maszyn wirtualnych instalowanych w środowisku Windows Hyper-V, vSphere oraz VMware Workstation uruchomionych na istniejącej infrastrukturze Zamawiającego.

### Dane zbierane przez rozwiązanie powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach i zagrożeniach.

### Rozwiązanie musi umożliwiać obsługę incydentów na podstawie reguł wyszukujących automatycznie zdarzenia z logów.

### Rozwiązanie musi mieć możliwość synchronizacji z serwerami czasu NTP.

### Rozwiązanie musi mieć predefiniowane panele w postaci graficznej prezentacji zebranych informacji wykonane przez producenta.

### Rozwiązanie musi umożliwiać gromadzenie zdarzeń za pomocą protokołów TCP oraz UDP.

### Rozwiązanie musi umożliwiać bezpieczne gromadzenie danych przy pomocy protokołu TLS.

### Rozwiązanie musi umożliwiać przesyłanie logów do innego serwera logów (funkcja syslog forwarder).

### Rozwiązanie jest lokalne i wymaga instalacji w środowisku klienta.

### Rozwiązanie musi posiadać narzędzie dla łatwego przeszukiwania logów zebranych z podłączonych firewalli. Logi muszą być filtrowane na podstawie zapytań, które można stosować wielokrotnie. –

### Rozwiązanie musi być wyposażone w wyszukiwanie zaawansowane w oparciu o wiele kryteriów (rodzaj logu, czas, itd.).

### Rozwiązanie musi być wyposażone w funkcjonalność wyświetlania rezultatów wyszukiwania co najmniej jako logi proste i graficzne.

### Rozwiązanie musi umożliwiać wykorzystanie zewnętrznych źródeł (CSV, IPtoHost, LDAP, GeoIP).

### Rozwiązanie musi umożliwiać nawigację na podstawie czasu (minut, godzin, dni, okresów)

### Rozwiązanie musi umożliwiać eksport wyników wyszukiwania w formacie CSV.

### Rozwiązanie musi umożliwiać tworzenie statycznych raportów.

### Musi istnieć możliwość zapisania stworzonych raportów do plików w formatach: PDF.

### Rozwiązanie musi umożliwiać zaplanowanie wykonania raportów.

### Rozwiązanie musi umożliwiać tworzenie własnych raportów.

### Rozwiązanie musi umożliwiać na podstawie kryteriów przeszukiwania logów utworzenie reguły alarmującej administratora. Reguła zostaje uaktywniona, gdy wszystkie kryteria zapytania zostaną spełnione. Powiadomienie musi mieć formę minimum wiadomości email. -

### Rozwiązanie musi mieć funkcjonalność tworzenia incydentów z kryteriów zapytań i zarządzanie incydentami poprzez możliwość przypisywania osób do obsługi incydentów, komentowania incydentów, podejrzenia logów źródłowych które zawarte są w incydencie.

* 1. **Wymagania systemowe**

### Liczba zdarzeń na sekundę (EPS): min. 9 500

### Zarządzanie logami: min 3 lata

### Liczba obsługiwanych urządzeń min. 600

### Liczba zapisu zdarzeń na dobę: min 12000 MB

### System logów musi wspierać hiperwizory: Vmware ESXi, Proxmox oraz Microsoft HyperV

* 1. **Lista systemów, z których system musi zbierać i przechowywać Logi:**

1. Serwer fizyczny – 6 sztuk
2. Macierz - 4 sztuki,
3. UTM – do 6 sztuk
4. Przełącznik Fibre Channel – 4 sztuki
5. Przełącznik rdzeniowy, agregacyjny – do 8 sztuk
6. Przełącznik dostępowy (LAN) – do 60 sztuk
7. Macierz NAS – do 20 sztuk
8. Zasilacz awaryjny (UPS) – do 6 sztuk
9. Serwer bazodanowy – 1 sztuka
10. Serwer poczty elektronicznej – 1 sztuka
11. Serwer wirtualizacji (Host, hypervizor) - 3 sztuki
12. Serwer wirtualizacji (konsola zarządzająca) – 3 sztuki
13. Serwer Backupu - 1 sztuka
14. maszyna wirtualna – do 50 sztuk
15. serwer AD - 2 sztuki
16. Serwery plików Windows / Synology – do 4 sztuk
17. **Wymagania dla Systemu SIEM.**

### W ramach systemu logowania i raportowania musi zostać dostarczone rozwiązanie monitorujące incydenty na urządzeniach sieciowych Zamawiającego

### Rozwiązanie musi w pełni realizować swoją funkcjonalność lokalnie (instalacja on-prem)

### Architektura rozwiązania musi być oparta o fizyczne lub wirtualne sondy monitorujące, których rolą jest odbieranie kopii ruchu sieciowego, generowanie alarmów oraz/lub metadanych o zdarzeniach, przygotowanie przechwyconych plików do dalszej analizy oraz przekazywanie przetworzonych danych do urządzenia administracyjnego.

### Architektura rozwiązania musi być oparta także o fizyczne lub wirtualne urządzenie administrujące, którego rolą jest zarządzanie sondami, włącznie z regułami detekcji, sygnaturami i nadzorem stanu, dogłębna analiza odebranych plików, prezentacja wyników detekcji, a także przekazywanie danych do rozwiązań stron trzecich

### Platformy muszą obsługiwać szyfrowanie dysków w standardzie LUKS.

### Rozwiązanie musi wspierać implementację na środowisku wirtualnym takim jak m.in. VMWare, Hyper-V, Proxmox, KVM, OVM, OVF.

### Sonda fizyczna lub wirtualna musi być w stanie przetworzyć dane dla maksymalnego odbieranego ruchu sieciowego na poziomie 4Gb/s.

### Rozwiązanie musi umożliwiać obsługę do 3 900 zdarzeń na sekundę, musi umożliwiać przechowywanie do 9 milionów zdarzeń, musi mieć możliwość detekcji malware, a także musi analizować przy pomocy silnika detekcji shellcode/powershell do 3 na sekundę.

### Licencja na zakup i serwis oprogramowania musi bazować na ilości aktywnie występujących w ruchu sieciowym adresów IP. Ilość adresów, objętych monitorowaniem: 900.

### Musi posiadać moduły zabezpieczone połączeniem (HTTPS) w przeglądarce

### Konsola rozwiązania musi zawierać informacje o kluczowych z punktu widzenia bezpieczeństwa detekcjach, uwzględniając adresy IP, adresy MAC, porty sieciowe, protokoły sieciowe, wyniki skanów plików, payload, sygnatury czasowe.

### Konsola rozwiązania musi szacować poziom ryzyka dla każdego wykrytego zagrożenia oraz musi dawać możliwość tagowania zdarzeń i załączania opisu (notatek).

### Rozwiązanie musi obsługiwać silniki detekcji takie jak Analiza Shellcode i Powershell, tj. detekcja technik wykorzystywanych przez cyberprzestępców w postaci specyficznego kodu służącego do wywoływania podatności oprogramowania zainstalowanego na stacjach roboczych czy serwerach.

### Rozwiązanie musi umożliwiać analizowanie całego ruchu sieciowego w oparciu o dostarczone reguły opisujące charakter niebezpiecznych połączeń.

1. Powiadomienia Push UP o wykrytym incydencie powyżej zdefiniowanego priorytetu wysyłane na urządzenie mobilne z system Android lub iOS.
2. Powiadomienia SMS o wykrytym incydencie powyżej określonego priorytetu wysyłane na zdefiniowane numery telefonów.
3. Możliwość integracji zewnętrznego systemu z oferowanym systemem SIEM poprzez dedykowane API
4. Możliwość zablokowania podejrzanego, potencjalnie niebezpiecznego ruchu sieciowego (LAN, WAN) do danych adresów IP na zarządzanych hostach (serwery, stacje robocze)
5. Możliwość obserwacji w czasie rzeczywistym lub wyznaczonych interwałach czasowych określonych plików (np. systemowych) generując alerty, gdy te pliki zostaną zaatakowane lub zmodyfikowane.
6. Zintegrowana z modułem zarządzania incydentami baza przetworzonych incydentów, znanych zagrożeń, regularnie aktualizowana o nowe incydenty, zagrożenia.
7. Możliwość porównania nowo utworzonego incydentu z posiadaną bazą opracowanych incydentów, znanych zagrożeń w wyniku czego administrator otrzymuje listę podobnych incydentów oraz listę incydentów zawierających zmienne obserwacyjne zawarte w nowym incydencie.
8. Możliwość przeszukiwania bazy incydentów pod kątem konkretnej zmiennej obserwacyjnej.
9. Możliwość klasyfikacji wykrytych zdarzeń na podstawie min. 16 stopniowej skali oraz możliwość modyfikacji poziomów skali wg potrzeb administratora.
10. Możliwość klasyfikacji utworzonych incydentów na podstawie kryteriów:
11. waga, min. 4 poziomy
12. poufność, możliwość nadania incydentowi parametru poufny czyli incydent zawierający dane wrażliwe wymagające szczególnej ochrony
13. tagi, możliwość przypisania tagu dla incydentu
14. zadanie, możliwość tworzenia zadań w ramach incydentów oraz przypisywania operatora dla zadania
15. Możliwość integracji SOAR z usługą katalogową Windows Active Directory.
16. Możliwość automatycznego uruchamiania zdefiniowanych działań w odpowiedzi na wykryty incydent, na przykład izolacja hosta, zablokowanie ruchu sieciowego lub zatrzymanie procesu.
17. Możliwość integracji z różnymi narzędziami bezpieczeństwa, takimi jak systemy antywirusowe, firewalle, czy też narzędzia do monitorowania ruchu sieciowego.
18. Możliwość wykorzystania algorytmów heurystycznych do automatycznego analizowania podejrzanych zachowań lub wzorców w systemie.
19. Możliwość dostosowania filtrów, które pomagają w identyfikacji istotnych zdarzeń oraz redukcji fałszywych alarmów, zwiększając ciągłość przepływu pracy.
20. Możliwość tworzenia dynamicznych skryptów i reguł reakcji na incydenty, umożliwiających dostosowanie się do zmieniających się warunków i nowych rodzajów zagrożeń.
21. Wsparcie dla integracji z platformami chmurowymi oraz możliwość monitorowania i zarządzania w środowisku chmurowym.

# Prezentacja z zakresu administracji Systemem Analizy Logów:

### Wykonawca będzie odpowiedzialny za przeprowadzenie prezentacji/instruktarzu dla Zamawiającego w zakresie:

### Wykrywania awarii Systemu Analizy Logów, mogących uniemożliwić poprawne działanie systemów informacyjnych Zamawiającego i/lub świadczenie usług,

### Samodzielnej zmiany zasobów takich jak: vCPU, vRAM, pamięć masowa.

### Optymalizacji konfiguracji Systemu Analizy Logów w celu nieprzekraczania wartości licencji Systemu posiadanego przez Zamawiającego

### Konfiguracji Systemu Analizy Logów w celu gromadzenia i normalizowania logów ze wskazanych systemów Zamawiającego

### Weryfikacji czy System Analizy Logów prawidłowo analizuje logi

### Tworzenia wymagań dla systemów Zamawiającego wysyłających logi w zakresie poziomu logowania zdarzeń.

### Przygotowania i uzyskania aprobaty Zamawiającego dla scenariuszy testów Systemu Analizy Logów,

1. **Moduł EDR (Endpoint Detection and Response).**

Wykonawca wraz z system SIEM dostarczy system klasy Endpoint Detection and Response wraz z centralną konsolą zarządzającą w postaci licencji bezterminowej dla 600 użytkowników wraz z wsparciem technicznym na okres min. 36 miesięcy. Minimalne wymagania dla systemu EDR:

1. Rozwiązanie musi posiadać moduł EDR dla systemów Windows oraz MacOS umożliwiające bezproblemową współpracę z systemem antywirusowym do ochrony stacji roboczych, użytkowanym przez Zamawiającego firmy ESET.
2. Rozwiązanie musi zawierać centralną konsolę administracyjną umożliwiającą monitorowanie oraz wizualizację zebranych danych z zarządzanych urządzeń.
3. Rozwiązanie musi posiadać serwer administracyjny z możliwością wysyłania zdarzeń do konsoli administracyjnej.
4. Rozwiązanie musi posiadać serwer administracyjny z możliwością wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
5. Rozwiązanie musi umożliwiać utworzenie wykluczenia automatycznie rozwiązujące alarmy, pasujące do utworzonego wykluczenia.
6. Rozwiązanie musi zapewniać kryteria wykluczeń konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, nazwę komputera, grupę, użytkownika.
7. Rozwiązanie musi umożliwić administratorowi weryfikację uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, rozmiar pliku.
8. Rozwiązanie musi umożliwiać administratorowi, w ramach plików wykonywalnych oraz plików DLL, możliwość oznaczenia ich jako bezpieczne lub niebezpieczne.
9. Rozwiązanie musi posiadać konsolę administracyjną z możliwością audytowania innych administratorów konsoli.
10. Rozwiązanie musi posiadać konsolę administracyjną z możliwością połączenia się do stacji roboczej i wykonywania komend zdalnych.
11. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.
12. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.
13. Rozwiązanie musi umożliwiać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.
14. Rozwiązanie musi zapewniać integrację z przynajmniej takimi systemami jak: konsola programu antywirusowego, moduł EDR.
15. Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: numer seryjny, informacje o systemie, procesor, pamięć RAM, karty sieciowe.
16. Serwer administracyjny musi posiadać możliwość tworzenia grup komputerów.
17. Rozwiązanie musi zapewniać korzystanie z min. 100 szablonów raportów, przygotowanych przez producenta lub własnych raportów tworzonych przez administratora.
18. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email oraz do dziennika syslog.
19. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami.
20. Rozwiązanie musi informować administratora o niezainstalowanych aktualizacjach systemowych.
21. **Moduł NDR (Network Detection and Response).**

Wykonawca wraz z system SIEM dostarczy system klasy Network Detection and Response wraz z centralną konsolą zarządzającą w postaci licencji bezterminowej dla 900 adresów IP wraz z wsparciem technicznym na okres min. 36 miesięcy. Minimalne wymagania dla systemu NDR:

1. Wielowątkowy silnik detekcji umożliwiający obsługę ruchu liczonego w dziesiątkach Gigabitów

* Możliwość obsługi wielu podsieci VLAN
* Możliwość obsługi wielu fizycznych połączeń sieciowych do różnych segmentów sieci LAN
* Obsługa biblioteki wyrażeń regularnych HyperScan
* Możliwość aktualizacji reguł bez wyłączania/ponownego uruchamiania silnika detekcji

1. Obsługa wielowątkowości procesora
2. Możliwość analizy kopii ruchu w sieci LAN w czasie rzeczywistym bez ingerencji w ruch sieciowy
3. Rejestracja żądań HTTP
4. Rejestracja i przechowywanie certyfikatów TLS
5. Możliwość wyodrębnienia plików z analizowanego ruchu sieciowego i zapisania ich na dysku do późniejszej analizy
6. Możliwość przechwytywania pakietów danych przesyłanych w sieci LAN i zapisywanie ich dla późniejszej analizy offline
7. Tworzenie raportów w przypadku wykrycia ruchu opisanego regułami jako ruch niebezpieczny
8. Rejestrowanie i dogłębna analiza ruchu szyfrowanego TLS/SSL
9. Rejestrowanie wszystkich kluczy wymiany do analizy oraz w celu zapobiegania podmianie
10. Rejestrowanie, zapisywanie ruchu HTTP z dowolnego portu do pliku w celu późniejszej analizy
11. Możliwość identyfikacji, wyodrębniania i rejestrowania plików w ruchu HTTP
12. Rejestracja wszystkich zapytań i odpowiedzi DNS
13. Funkcja wykrywania włamań sieciowych
14. Funkcja zapobiegania włamaniom sieciowym
15. funkcja monitorowania bezpieczeństwa sieci LAN
16. Pełne wsparcie dla protokołu IPv6
17. Możliwość dekodowania tuneli: IP-IP, IP6-IP4, IP4-IP6, GRE, VXLAN, Geneve, Teredo
18. Silnik strumienia TCP: śledzenie sesji, stream reassembly (pakietowe sprawdzanie strumieni według Jarka), target based stream reassembly
19. IP Defrag engine: target based reassembly
20. Możliwość obsługi wielu podsieci VLAN
21. Możliwość obsługi wielu fizycznych połączeń sieciowych do różnych segmentów sieci LAN
22. Możliwość modyfikacji reguł
23. Możliwość zdefiniowania niebezpiecznych plików przez parametry: wielkość, nazwa, rozszerzenie
24. Możliwość wykrywania złośliwego oprogramowania w oparciu o odcisk palca JA3, JA3S
25. Możliwość wykrywania złośliwego oprogramowania w oparciu o metodę HASSH
26. Obsługa dekodowania pakietów: IPv4, IPv6, TCP, UDP, SCTP, ICMPv4, ICMPv6, GRE, Ethernet, PPP, PPPoE, Raw, SLL, VLAN, QINQ, MPLS, ERSPAN, VXLAN
27. Dekodowanie warstwy aplikacji: HTTP, HTTP/2, SSL, TLS, SMB, DCERPC, SMTP, FTP, SSH, DNS, ENIP/CIP, DNP3, NFS, NTP, DHCP, TFTP, KRB5, IKEv2, SIP, SNMP, RDP, RFB
28. Możliwość tworzenia raportów zgodnych z standardem JSON, SYSLOG,
29. Możliwość filtrowania alertów z podziałem na wagę/priorytet
30. Możliwość filtrowania alertów dla wybranej reguły z podziałem na wagę/priorytet
31. Wspierane systemy operacyjne: Windows, Linux, FreeBSD, OpenBSD, MacOS, Mac OS X
32. Obsługa przekazywania alertów „dalej” do systemów takich jak: syslog, eve.log, JSON, Unified 2
33. Filtrowanie alertów na poziomie: reguł, hostów, sieci