SIEM – rozwój systemu o funkcjonalności XDR

Zamawiający posiada system SIEM (SIEM COMP Security Center), którego zakres obejmuje skonfigurowany system (realizujący wymagania równoważne: SIEM-001 - SIEM-014) wraz z instalacją i konfiguracją agentów na infrastrukturze serwerowej i końcówkach klienckich w niezbędnym zakresie.

Wymagania minimalne:

id	Treść wymagania
XDR-001	Monitorowanie infrastruktury posiadanym oprogramowaniem SIEM (SIEM COMP Security Center) należy rozszerzyć na wszystkie zasoby będące w posiadaniu Zamawiającego, tj. infrastruktura serwerowni oraz 100-200 szt. stacji roboczych. Ponadto na zasobach należy wdrożyć funkcjonalności XDR (ang. Extended detection and response).
XDR-002	Musi istnieć możliwość uruchomienia funkcjonalności XDR przynajmniej na systemach Windows, Linux, MacOS.
XDR-003	Moduł musi umożliwiać automatyczną blokadę konta użytkownika na podstawie zdefiniowanej reguły.
XDR-004	Moduł musi umożliwiać automatyczną blokadę IP na podstawie zdefiniowanej reguły zarówno w przypadku systemu z zaporą, jak i bez zapory (null route, hosts.deny).
XDR-005	Moduł musi umożliwiać automatyczny restart agenta na podstawie zdefiniowanej reguły.
XDR-006	Moduł musi umożliwiać wykrycie i zablokowanie ataków typu ransomware, celem ograniczenia ryzyk wynikających z utraty danych.
XDR-007	Moduł musi umożliwiać definiowanie własnych skryptów oraz reguł ich uruchamiania w odpowiedzi na zidentyfikowane przez SIEM zagrożenia.
XDR-008	W ramach wdrożenia Wykonawca opracuje nie więcej niż 3 dodatkowe reguły wraz ze skryptami realizujące odpowiedź systemu na wskazane przez Zamawiającego zagrożenia.
XDR-009	W przypadku braku możliwości rozwoju posiadanego przez Zamawiającego oprogramowania należy wdrożyć system SIEM spełniający wymagania równoważne (SIEM-001 – SIEM-014) oraz zrealizować wymagania XDR-001 - XDR-008 oraz XDR-010.
XDR-010	Okres utrzymanie funkcjonalności określonych wymaganiami XDR-001-XDR-009 wynosi 2 lata.

System SIEM - wymagania równoważne:

id	Treść wymagania

SIEM-001	Oprogramowanie musi pozwalać na monitorowanie sieci pod względem incydentów bezpieczeństwa (oprogramowanie typu NSM – Network Security Monitoring).
SIEM-002	Oprogramowanie musi pozwalać na pełne przechwytywanie pakietów sieciowych oraz wykrywanie sieci i punktów końcowych (endpoints).
SIEM-003	Przechwytywanie pakietów: Oprogramowanie musi pozwalać na: a) przechwytywanie całego ruchu sieciowego i jego interpretacje według zestawów predefiniowanych zasad; b) automatyczne czyszczenie starych (archiwalnych) danych przed zapełnieniem zasobów dyskowych; c) Generowanie i przechowywanie logi diagnostyczne; d) przeglądanie pakietów za pomocą kwerend.
SIEM-004	Wykrywanie sieci i punktów końcowych: Oprogramowanie musi pozwalać na: a) wykrywanie złośliwego, anomalnego lub podejrzanego ruchu w sieci na podstawie zestawu reguł (NIDS – Network-based Intrusion Detection System); b) wykrywanie włamań do sieci opartych na analizie ruchu w czasie rzeczywistym; c) wykorzystanie agentów do monitorowania punktów końcowych w sieci (HIDS – Host-based Intrusion Detection System), w tym: a. analiza dzienników systemowych; b. monitorowanie zestawów predefiniowanych zasad; c. wykrywanie rootkitów; d. alarmowanie i reagowanie na incydenty w czasie rzeczywistym.
SIEM-005	Oprogramowanie musi udostępniać graficzny interfejs WWW, który umożliwia: a) dostęp jedynie zalogowanym użytkownikom (login oraz hasło); b) podstawowy podgląd alertów bezpieczeństwa z systemów NIDS oraz HIDS; c) rozszerzony podgląd alertów z określeniem miejsca zdarzenia oraz dokładnym opisem zdarzenia wraz z jego klasyfikacją; d) wizualizację incydentów bezpieczeństwa w postaci graficznej (wykresów, diagramów); e) interfejs do pełnego przechwytywania pakietów (PCAP – packet capture); f) monitoring zasobów systemowych; g) interfejs do reagowania na incydenty bezpieczeństwa oraz zarządzania sprawami utworzonymi na podstawie alertów; h) interfejs dla narzędzia pozwalającego na operację na danych pochodzących z alertów systemu; i) dostęp publiczny do interfejsu z wykorzystaniem protokołu HTTPS z wykorzystaniem certyfikatu od CA lub lokalny oraz poprzez połączenie tunelowe VPN.

SIEM-006	Oprogramowanie musi pozwalać na niezależne wykorzystanie przynajmniej dwóch interfejsów sieciowych, w tym: a) interfejs do zarządzania; b) interfejs do nasłuchu ruchu sieciowego.
SIEM-007	Oprogramowanie musi pozwalać na zarządzanie jego komponentami i przegląd zdarzeń systemowych za pomocą interfejsu konsolowego (CLI).
SIEM-008	W zakresie zarządzania agentów HIDS oprogramowanie musi pozwalać na: a) instalację agentów na urządzeniach z systemami Windows, MacOS, AIX, HP-UX, Oracle Solaris oraz Linux; b) instalację agentów w postaci kontenerów (np. Docker); c) rejestracja agentów poprzez REST API; d) zarządzanie agentami poprzez interfejs konsolowy oraz REST API; e) zabezpieczenie REST API z wykorzystaniem połączenia HTTPS; f) tworzenie grup agentów i zdalne zarządzanie nimi; g) zdalna aktualizacja agentów.
SIEM-009	W zakresie HIDS oprogramowanie musi pozwalać na: a) zbieranie danych z dzienników systemowych urządzenia agenta; b) zbieranie informacji o systemie i jego zasobach; c) monitorowanie integralności plików systemowych; d) audyt zmian danych w systemie oraz przez kogo zostały dokonane; e) wykrywanie anomalii i malware w systemie; f) monitorowanie polityk bezpieczeństwa; g) monitorowanie wykonywanych poleceń systemowych; h) aktywne reagowanie na incydenty bezpieczeństwa – blokowanie dostępu do urządzenia dla intruzów; i) „bezagentowy” monitoring urządzeń sieciowych poprzez SSH; j) wykrywanie podatności w aplikacjach zainstalowanych na urządzeniu; k) skanowanie monitorowanych plików z wykorzystaniem VirusTotal.
SIEM-010	Oprogramowanie musi pozwalać na wizualizację zbieranych danych o incydentach bezpieczeństwa w postaci wykresów oraz posiadać predefiniowane zestawienia / kokpity (dashboards) i umożliwiać ich tworzenie z poziomu interfejsu graficznego WWW.
SIEM-011	Oprogramowanie musi posiadać moduł do zarządzania sprawami pozwalający na: a) szybki podgląd sprawy z dostępem do pełnej jej treści; b) okno edycji sprawy pozwalające przynajmniej na: i. zdefiniowanie tytułu sprawy; ii. zdefiniowanie syntetycznego opisu sprawy; iii. zdefiniowanie szczegółowego opisu sprawy; iv. umożliwianie dołączania załączników;

	v. gromadzenie historii sprawy; vi. przypisanie sprawy do osoby odpowiedzialnej; vii. określenie parametrów sprawy min. w zakresie: status sprawy, ocena wpływu na organizację, priorytet sprawy.
SIEM-012	Moduł sprawy musi być dostępny dla wszystkich pracowników organizacji.
SIEM-013	Oprogramowanie musi posiadać moduł do zarządzania zgłoszeniami pozwalający na: a) szybki podgląd zgłoszenia z dostępem do pełnej jego treści; b) okno edycji zgłoszenia pozwalające przynajmniej na uzupełnienie formularza zgłoszenia właściwego dla danego CSIRT obejmującego minimum: i. tytuł zgłoszenia; ii. syntetyczny opis zgłoszenia; i. dane teleadresowe; iii. opis incydentu; iv. załączniki; v. przypisanie zgłoszenia do osoby odpowiedzialnej; vi. określenie statusu zgłoszenia; c) gromadzenie historii sprawy; d) wydruk formularza zgłoszenia przynajmniej do pliku w formacie pdf.
SIEM-014	Wykonawca dostarczy dokumentację użytkownika i przeprowadzi instruktaż dla administratorów (maksymalnie 3 osoby) z obsługi wdrożonych funkcjonalności.