

Opis przedmiotu Zamówienia

Przedmiotem zamówienia jest przeprowadzenie kompleksowej oceny zdolności i dojrzałości operacyjnej Zamawiającego w zakresie wykrywania, analizy i obsługi zdarzeń oraz incydentów bezpieczeństwa, a następnie opracowanie i optymalizacja dokumentacji scenariuszy działań oraz mechanizmów wspierających ich realizację z wykorzystaniem rozwiązań opartych na sztucznej inteligencji, w tym automatyzacji oraz implementacji algorytmów uczenia maszynowego i lokalnego modelu AI wspierającego analizę incydentów, podatności, logów i zdarzeń bezpieczeństwa.

Wymagania ogólne:

1. Realizacja zamówienia powinna umożliwić Zamawiającemu w szczególności:
 - a) ocenę aktualnego poziomu zdolności do identyfikowania i obsługi istotnych zagrożeń cyberbezpieczeństwa;
 - b) identyfikację luk w zakresie dostępności i jakości danych telemetrycznych oraz widoczności zdarzeń bezpieczeństwa;
 - c) ocenę skuteczności istniejących mechanizmów detekcji;
 - d) ocenę dojrzałości procesów monitorowania, analizy, eskalacji i zarządzania incydentami;
 - e) określenie priorytetowych kierunków rozwoju;
 - f) uporządkowanie i standaryzację dokumentacji operacyjnej;
 - g) opracowanie zoptymalizowanych scenariuszy i playbooków reagowania;
 - h) wykorzystanie mechanizmów AI do wspomaganie realizacji wybranych procesów i scenariuszy;
2. Prace powinny uwzględniać uznane standardy, modele i dobre praktyki dotyczące funkcjonowania Security Operations Center, w szczególności w zakresie oceny pokrycia zagrożeń, zdolności detekcyjnych oraz dojrzałości organizacyjnej i procesowej.
3. Ocena zdolności i dojrzałości operacyjnej powinna obejmować, w zakresie występującym w środowisku Zamawiającego, co najmniej następujące obszary:
 - a) usługi katalogowe i zarządzanie tożsamością;
 - b) pocztę elektroniczną;
 - c) stacje robocze i serwery;
 - d) mechanizmy ochrony przed złośliwym oprogramowaniem;
 - e) środowiska chmurowe;
 - f) infrastrukturę sieciową;
 - g) źródła informacji o zagrożeniach;
 - h) systemy i narzędzia wykorzystywane do monitorowania, detekcji, analizy i reagowania na zdarzenia bezpieczeństwa.
4. Analizie powinny podlegać w szczególności procesy monitorowania bezpieczeństwa, kwalifikacji i analizy alertów, eskalacji oraz zarządzania incydentami.
5. Usługa ma uwzględniać trzy zadania główne:
 - a) Zadanie 1: ATT&CK SOC Assessment – ocena dojrzałości zdolności detekcji i reakcji SOC w odniesieniu do frameworka MITRE ATT&CK oraz standardów SOC-CMM/SIM3 (Zadania: 1.1., 1.2., 1.3);
 - b) Zadanie 2: Dokumentacja i automatyzacja obsługi scenariuszy – opracowanie playbooków Security Operations Center oraz wdrożenie promptów AI wspierających analityków (Zadania: 2.1., 2.2., 2.3.);
 - c) Zadanie 3: Uczenie maszynowe i sztuczna inteligencja – implementacja algorytmów ML oraz konfiguracja lokalnego serwera AI zintegrowanego z posiadaną przez Zamawiającego platformą SecureVisio.

Zadanie 1.1.: Analiza i weryfikacja profilu zagrożeń.

6. Wykonawca dokona analizy zagrożeń istotnych dla środowiska oraz profilu działalności Zamawiającego. Analiza powinna uwzględniać co najmniej:
 - a) zagrożenia zidentyfikowane dotychczas przez Zamawiającego;
 - b) charakter i architekturę środowiska teleinformatycznego,
 - c) dostępne informacje dotyczące wcześniejszych incydentów,
 - d) aktualne trendy dotyczące zagrożeń,
 - e) dostępne informacje Threat Intelligence,
 - f) techniki, taktyki i procedury stosowane przez współczesnych aktorów zagrożeń.
7. Wykonawca dokona weryfikacji i priorytetyzacji zagrożeń oraz odniesie je do uznanego modelu klasyfikacji taktyk i technik atakujących, np. MITRE ATT&CK lub rozwiązania równoważnego.
8. Oczekiwanym rezultatem będzie zaktualizowany i uzgodniony z Zamawiającym profil zagrożeń wraz z mapą pokrycia istotnych technik i scenariuszy ataku, stanowiący podstawę dalszej oceny zdolności Security Operations Center.

Zadanie 1.2.: Analiza źródeł danych, telemetrii i mechanizmów detekcji.

9. Wykonawca przeprowadzi ocenę dostępności, kompletności i jakości informacji wykorzystywanych przez Security Operations Center do monitorowania i wykrywania zagrożeń. Ocena powinna obejmować w szczególności:
 - a) identyfikację źródeł danych i telemetrii dostępnych dla Security Operations Center,
 - b) ocenę ich dostępności, kompletności, jakości oraz przydatności z punktu widzenia wykrywania zidentyfikowanych zagrożeń,
 - c) określenie stopnia pokrycia zidentyfikowanych zagrożeń przez dostępne źródła danych,
 - d) ocenę istniejących mechanizmów i reguł detekcji,
 - e) identyfikację obszarów o ograniczonej lub niewystarczającej widoczności,
 - f) identyfikację istotnych luk w zdolnościach detekcyjnych,
 - g) ocenę adekwatności istniejących detekcji względem aktualnego profilu zagrożeń.
10. Wykonawca powinien dokonać mapowania istniejących zdolności detekcyjnych do technik i scenariuszy zagrożeń przy wykorzystaniu uznanego modelu klasyfikacji technik ataku.
11. Oczekiwanym rezultatem będzie raport oceny źródeł danych, telemetrii oraz mechanizmów detekcji, zawierający co najmniej identyfikację luk w widoczności i pokryciu zagrożeń oraz ocenę jakości i adekwatności istniejących mechanizmów detekcji.

Zadanie 1.3.: Ocena procesów operacyjnych.

12. Wykonawca przeprowadzi ocenę dojrzałości i efektywności procesów operacyjnych związanych z obsługą zdarzeń i incydentów bezpieczeństwa. Analiza powinna obejmować co najmniej:
 - a) monitoring bezpieczeństwa,
 - b) analizę i kwalifikację alertów,
 - c) procesy triage,
 - d) eskalację zdarzeń i incydentów,
 - e) zarządzanie incydentami,
 - f) role i odpowiedzialności,
 - g) ścieżki decyzyjne,
 - h) dokumentowanie prowadzonych działań,
 - i) stosowane mierniki i wskaźniki efektywności,
 - j) istniejące procedury, scenariusze oraz playbooks operacyjne.
13. W ramach prac należy zidentyfikować potencjalne przeszkody, nieefektywności oraz obszary wymagające poprawy. Ocena powinna zostać odniesiona do uznanych modeli dojrzałości i dobrych praktyk dotyczących organizacji i funkcjonowania Security Operations Center.
14. Oczekiwanym rezultatem realizacji Zadania 1 będzie raport podsumowujący aktualny poziom zdolności i dojrzałości Security Operations Center przygotowany przez Wykonawcę. Raport powinien obejmować co najmniej:
 - a) ocenę zdolności do wykrywania i reagowania na istotne zagrożenia,

- b) ocenę pokrycia zidentyfikowanych zagrożeń przez dostępne dane i mechanizmy detekcji,
 - c) ocenę dojrzałości procesów operacyjnych,
 - d) identyfikację najważniejszych luk i ograniczeń,
 - e) rekomendacje działań naprawczych i rozwojowych,
 - f) określenie priorytetów rekomendowanych działań,
 - g) roadmapę rozwoju Security Operations Center.
15. Rekomendacje powinny obejmować co najmniej obszary danych i telemetrii, widoczności, detekcji, procesów i organizacji, metryk oraz kompetencji.
16. Ocena powinna wykorzystywać uznane standardy, modele i dobre praktyki branżowe, w szczególności MITRE ATT&CK lub rozwiązania równoważne oraz uznane modele oceny dojrzałości Security Operations Center.

Zadanie 2.1.: Opracowanie standardu dokumentowania scenariuszy i playbooków.

17. Na podstawie wyników oceny przeprowadzonej w ramach Zadania 1 Wykonawca opracuje koncepcję standaryzacji dokumentacji scenariuszy operacyjnych Security Operations Center. Koncepcja powinna określać co najmniej:
- a) strukturę dokumentacji scenariusza lub playbooka,
 - b) wymagane elementy dokumentacji,
 - c) sposób opisu zagrożenia i mechanizmu jego detekcji,
 - d) sposób dokumentowania kolejnych etapów analizy i reagowania,
 - e) sposób prezentowania ścieżek eskalacji i odpowiedzialności,
 - f) zasady dokumentowania źródeł danych i wymaganych artefaktów,
 - g) sposób prezentacji przebiegu procesów,
 - h) zasady nazewnictwa, wersjonowania, utrzymania oraz właścicielstwa dokumentacji.
18. Wykonawca powinien również dokonać analizy możliwych sposobów tworzenia, przechowywania, utrzymywania i aktualizacji dokumentacji oraz przedstawić rekomendację rozwiązania dostosowanego do środowiska i zasobów Zamawiającego.
19. Oczekiwany rezultat będzie uzgodniona z Zamawiającym koncepcja dokumentowania scenariuszy operacyjnych Security Operations Center wraz ze standardowym szablonem playbooka oraz rekomendacją sposobu tworzenia, przechowywania i utrzymywania dokumentacji.

Zadanie 2.2.: Opracowanie zoptymalizowanych scenariuszy i playbooków.

20. Wykonawca opracuje dokumentację dla wybranych, priorytetowych scenariuszy obsługi zdarzeń i incydentów bezpieczeństwa. Wybór scenariuszy powinien wynikać z:
- a) aktualnego profilu zagrożeń,
 - b) istniejących scenariuszy Zamawiającego,
 - c) wyników oceny zdolności detekcyjnych,
 - d) zidentyfikowanych luk,
 - e) istotności poszczególnych zagrożeń dla działalności Zamawiającego.
21. Dla każdego scenariusza należy uwzględnić, odpowiednio do jego charakteru:
- a) opis zagrożenia,
 - b) wymagane źródła danych,
 - c) mechanizmy i logikę detekcji,
 - d) działania analityczne,
 - e) zasady kwalifikacji zdarzenia,
 - f) działania w zakresie triage,
 - g) ścieżki eskalacji,
 - h) działania związane z obsługą incyduentu,
 - i) role i odpowiedzialności,
 - j) diagram przebiegu procesu,
 - k) odniesienie do odpowiednich technik i dobrych praktyk bezpieczeństwa.

22. Scenariusze powinny zostać zweryfikowane wspólnie z personelem Zamawiającego odpowiedzialnym za realizację procesów Security Operations Center i uwzględniać rzeczywisty model operacyjny organizacji. Zakłada się opracowanie około 10–15 priorytetowych scenariuszy.
23. Oczekiwanym rezultatem będzie repozytorium ustandaryzowanych i zoptymalizowanych scenariuszy oraz playbooków Security Operations Center, przygotowanych w formie umożliwiającej ich praktyczne wykorzystanie przez personel Zamawiającego.
24. Wykonawca przeprowadzi również przekazanie rezultatów prac, obejmujące zasady stosowania, utrzymywania i aktualizacji opracowanej dokumentacji.

Zadanie 2.3.: Wsparcie realizacji scenariuszy z wykorzystaniem AI.

25. Wykonawca zaprojektuje i wdroży mechanizmy wykorzystujące rozwiązania oparte na sztucznej inteligencji, wspierające realizację wybranych scenariuszy operacyjnych Security Operations Center. Mechanizmy powinny wspierać analityków co najmniej w wybranych obszarach:
 - a) analizie alertów i zdarzeń,
 - b) klasyfikacji zdarzeń i incydentów,
 - c) analizie i wzbogacaniu informacji dotyczących zdarzenia,
 - d) identyfikacji istotnych informacji i artefaktów,
 - e) generowaniu rekomendacji dotyczących dalszych działań,
 - f) wspieraniu realizacji kolejnych kroków wynikających z playbooka,
 - g) przygotowywaniu dokumentacji dotyczącej obsługi zdarzeń i incydentów.
26. Zakres scenariuszy objętych mechanizmami AI powinien zostać ustalony na podstawie ich priorytetu, możliwości automatyzacji oraz wyników Zadania 1.
27. Opracowane mechanizmy powinny zostać zweryfikowane z personelem Security Operations Center pod kątem poprawności merytorycznej i zgodności z procesami operacyjnymi Zamawiającego.
28. Wykonawca powinien zapewnić możliwość dalszego utrzymywania, rozwijania i aktualizowania przygotowanych mechanizmów przez Zamawiającego.
29. Oczekiwanym rezultatem będzie repozytorium przygotowanych i zweryfikowanych mechanizmów wspierających realizację scenariuszy Security Operations Center z wykorzystaniem AI, wraz z dokumentacją umożliwiającą ich użytkowanie, utrzymanie oraz dalszy rozwój.

Zadanie 3.1.:Opracowanie i wdrożenie algorytmów uczenia maszynowego.

30. Wykonawca dokona weryfikacji parametrów sprzętowych związanych z wymaganiami ML wraz z rekomendowanym planem działania w dwóch scenariuszach:
 - gdy zasoby sprzętowe nie mogą być rozszerzone,
 - gdy zasoby sprzętowe zostaną zwiększone.
31. Wykonawca przeprowadzi analizę kontekstu organizacji względem potrzeb algorytmów uczenia maszynowego, w tym:
 - identyfikację koniecznych zmian reguł kontekstowych zasobów,
 - identyfikację zmian związanych z kontami użytkowników.
31. Wykonawca dokona selekcji profili, które mają podlegać algorytmom uczenia, w tym w przypadku zbyt ogólnych profili – podział z wygenerowaniem nowych profili.
32. Wykonawca we współpracy z Zamawiającym przygotowuje parametry zbioru danych:
 - wielkość zbioru,
 - zakresy nauczania,
 - okresy treningowe i walidacyjne.
33. Wykonawca musi wykonać selekcję zbiorów reguł:
 - wykluczanie ze zbioru ogólnego,
 - przygotowanie zbiorów dodatkowych,

- wybór adekwatnych profili.
- 34. Wykonawca przygotowuje reguły uczenia maszynowego (selekcja danych do nauki).
- 35. Wykonawca dokona mapowania zbioru reguł na przygotowane reguły oraz algorytmy.
- 36. Wykonawca wykona strojenie (fine-tuning) algorytmów.
- 37. Produktem etapu ma być implementacja działających algorytmów uczenia maszynowego dostosowanych do specyfiki organizacji. Algorytmy mają zapewniać ochronę przed zagrożeniami ukrytymi w ruchu legitymowanym.

Etap 3.2.: Przygotowanie i skonfigurowanie lokalnego modelu AI.

- 38. Wykonawca zainstaluje i skonfiguruje serwer AI.
- 39. Wykonawca przeprowadzi instalację środowiska dla modelu AI.
- 40. Wykonawca przygotowuje, zainstaluje model AI oraz dokona jego integracji z posiadaną przez Zamawiającego platformą SecureVisio.
- 39. Wykonawca dokona instalacji i uruchomienia komponentów SecureVisio:
 - SecureVisio LLM (Large Language Model),
 - SecureVisio RAG (Retrieval-Augmented Generation),
 - SecureVisio MCP (Model Context Protocol / Multi-agent Control Platform).
- 40. Wykonawca zrealizuje przeszkolenie oraz implementację modelu w obszarach:
 - obsługi incydentów,
 - obsługi podatności,
 - analizy logów,
 - analizy zdarzeń.
- 41. Produktem etapu ma być w pełni działający lokalny serwer AI zintegrowany z platformą SecureVisio. Model AI ma być przeszkolony i gotowy do wsparcia operacyjnego Security Operations Center.
- 42. Na potrzeby przygotowania i skonfigurowania lokalnego modelu AI, Wykonawca dostarczy urządzenie fizyczne wraz z niezbędnym oprogramowaniem o następujących wymaganiach:
 - Wymagania sprzętowe: CPU – 32 rdzeni, RAM 128GB, GPU 1x NVIDIA Blackwell 6000, dysk 2TB NVMe SSD, Sieć – 10GbE.
 - Wymagania programowe:
 - System operacyjny: Linux (Ubuntu 22.04 LTS lub nowszy),
 - Środowisko konteneryzacji: Docker + Kubernetes,
 - Frameworki ML: PyTorch, TensorFlow, Hugging Face Transformers,
 - Narzędzia MLOps: MLflow, Kubeflow lub równoważne,
 - Integracja API: REST z SecureVisio,
 - Wymagania bezpieczeństwa:
 - Szyfrowanie danych w spoczynku i w tranzycie (TLS 1.3+),
 - Autentykacja wieloskładnikowa (MFA),
 - Izolacja sieciowa (VLAN, firewall),
 - Audyt logów dostępu,

Wymagania dotyczące produktów końcowych zamówienia:

- 43. W ramach realizacji zamówienia Wykonawca dostarczy co najmniej:
 - Zaktualizowany profil zagrożeń dla środowiska Zamawiającego;
 - Mapę pokrycia zidentyfikowanych zagrożeń przez zdolności Security Operations Center ;
 - Analizę źródeł danych i telemetryi wraz z identyfikacją luk w widoczności;
 - Ocenę istniejących mechanizmów i reguł detekcji;
 - Ocenę dojrzałości procesów operacyjnych Security Operations Center;
 - Raport z kompleksowej oceny zdolności i dojrzałości Security Operations Center;
 - Rekomendacje oraz roadmapę rozwoju Security Operations Center z określeniem priorytetów;

- Standard i szablon dokumentowania scenariuszy/playbooków Security Operations Center;
- Repozytorium około 10–15 zoptymalizowanych scenariuszy/playbooków Security Operations Center;
- Repozytorium mechanizmów wykorzystujących AI do wspomagania realizacji wybranych scenariuszy;
- Repozytorium reguł uczenia maszynowego i algorytmów dostrojonych do pracy zespołu Security Operations Center i specyfiki organizacji;
- Lokalny serwer AI z zainstalowanymi i dostrojonymi komponentami LLM, RAG, MCP w zakresie obsługi incydentów, podatności, logów oraz zdarzeń;
- Dokumentację dotyczącą utrzymania i aktualizacji opracowanych materiałów i mechanizmów;
- Sesję przekazania wiedzy dla personelu Zamawiającego z zakresu wdrożonych rozwiązań i wykonanych zadań (minimum 2 sesje).

44. Zamawiający wymaga by zadania zostały zrealizowane w następującej pracochłonności zespołów:

Zadanie	(pracochłonność dni robocze)	Zadanie	(pracochłonność dni robocze)
Zadanie 1.1.	8	Zadanie 3.1.	25
Zadanie 1.2.	10	Zadanie 3.2.	25
Zadanie 1.3.	12		
Zadanie 2.1.	8		
Zadanie 2.2.	10		
Zadanie 2.3.	12		

45. Realizacja zamówienia musi odbywać się w ścisłej współpracy z przedstawicielami Zamawiającego, w szczególności personelem odpowiedzialnym za monitoring bezpieczeństwa, analizę zdarzeń i reagowanie na incydenty.
46. Wykonawca powinien zastosować metodykę zapewniającą możliwość oceny zarówno technicznych zdolności detekcyjnych, jak i organizacyjno-procesowej dojrzałości Security Operations Center.
47. Wykonawca powinien zapewnić spójność rezultatów poszczególnych zadań, w szczególności poprzez wykorzystanie wyników oceny zdolności i dojrzałości Security Operations Center jako podstawy do wyboru, priorytetyzacji i optymalizacji scenariuszy operacyjnych.
48. Wszelkie rekomendacje dotyczące wykorzystania konkretnych technologii lub narzędzi powinny wynikać z przeprowadzonej analizy oraz uwzględniać istniejące środowisko, zasoby i uwarunkowania Zamawiającego.