1. *Ile lokalizacji (oddziałów / obiektów) obejmuje infrastruktura IT?*

Ilość lokalizacji: 4

2. *Czy środowisko obejmuje wyłącznie infrastrukturę on-premise, czy również usługi chmurowe, oraz czy rozwiązania bezpieczeństwa działają centralnie, czy osobno w poszczególnych lokalizacjach?*

Brak usług chmurowych. Zarządzanie centralne.

3. *Ilu użytkowników końcowych oraz ilu endpointów (objętych EDR/XDR) dotyczy audyt? Jaka jest skala środowiska, którego dotyczy audyt? Prosimy o orientacyjne wskazanie liczby użytkowników, stacji roboczych, serwerów, urządzeń sieciowych oraz innych istotnych elementów infrastruktury objętych zakresem.*

Ilość użytkowników: około 100 (97 AD)
Ilość stacji roboczych: około 110
Ilość serwerów: 7
UTM/Routery: 2

4. *Prosimy o informację, czy wdrożone rozwiązania bezpieczeństwa są już produkcyjnie wykorzystywane. Jeśli tak, od kiedy działają w środowisku oraz czy objęły całość infrastruktury, czy tylko jej wybrane obszary?*

Jesteśmy przed wdrożeniem podanych rozwiązań.

5. *Prosimy o informację, czy posiadają Państwo dokumentację wdrożeniową i eksploatacyjną dotyczącą analizowanych rozwiązań. W szczególności chodzi o dokumentację architektury, konfiguracji, polityk bezpieczeństwa, procedur operacyjnych, uprawnień oraz instrukcji administracyjnych.*

Nie. Pełna dokumentacja będzie tworzona podczas wdrożenia poszczególnych rozwiązań.

6. *Czy posiadają Państwo formalne polityki i procedury bezpieczeństwa powiązane z badanym zakresem? Jeśli tak, prosimy o wskazanie, jakie obszary obejmują te dokumenty oraz jak rozbudowana jest dokumentacja.*

Istniejąca dokumentacja zawiera takie elementy jak zasady bezpiecznego użytkowania sprzętu IT, dysków, programów, użytkowanie komputerów przenośnych, zarządzanie uprawnieniami, polityka haseł, zasady wynoszenia nośników z danymi poza firmę/organizację, zasady korzystania z Internetu, zasady korzystania z poczty elektronicznej i będzie przedmiotem dostosowania do nowych przepisów.

7. *W jaki sposób realizowane jest zarządzanie dostępem i uprawnieniami? Prosimy o informację, czy wykorzystywane są centralne mechanizmy uwierzytelniania, MFA, konta uprzywilejowane, rozwiązania PAM, rozdział ról administracyjnych itp.*

Zarządzanie przez serwer Active Directory. Nie wykorzystujemy dodatkowych mechanizmów uwierzytelniania.

8. *Jak wygląda obecnie obszar logowania i monitorowania zdarzeń? Prosimy o wskazanie, jakie źródła logów są zbierane, jak długo przechowywane są logi, czy działają reguły korelacyjne i alerting oraz kto operacyjnie obsługuje incydenty i alarmy.*

Aktualnie monitorujemy logi serwera AD z powiadamianiem o zdarzeniach oraz alarmy obecnego urządzenia UTM. Obsługą zajmuje się dział informatyczny – 2 osoby.

9. *Jakie konkretne rozwiązania zostały wdrożone (producenci / modele UTM, SIEM, EDR/XDR)? Prosimy o wskazanie, z jakich rozwiązań korzystają Państwo w obszarach UTM, SIEM, EDR/XDR, NAS, stacji przesiadkowych oraz infrastruktury sieciowej. Prosimy o podanie producenta, nazwy rozwiązania oraz wersji, jeśli są dostępne.*

Jesteśmy przed wdrożeniem podanych rozwiązań.

10. *Ile źródeł logów jest aktualnie podłączonych do systemu SIEM?*

Jesteśmy przed wdrożeniem podanych rozwiązań.

11. *Czy SIEM jest w pełni operacyjny (korelacja, reguły, alerty)?*

Jesteśmy przed wdrożeniem podanych rozwiązań.

12. *Czy istnieje dokumentacja architektury bezpieczeństwa (diagramy, przepływy danych)?*

Dostępne są schematy połączeń sieciowych

13. *Czy organizacja posiada SOC lub dedykowaną funkcję monitorowania bezpieczeństwa?*

Jesteśmy przed wdrożeniem podanych rozwiązań.

Czy istnieją procedury reagowania na incydenty (IR) oraz czy były one testowane?
Jesteśmy przed wdrożeniem podanych rozwiązań.

14. *Czy audyt ma obejmować:*

- *tylko przegląd konfiguracji (review),*
- *czy również testy praktyczne (np. weryfikacja reguł, symulacje zdarzeń)?*

Bez przeprowadzenia testów nie jest możliwa ocena wymieniona w zakresie zapytania. Oczekujemy takich działań, w wyniku których otrzymamy rezultaty sformułowane w zapytaniu. Wierzymy w profesjonalizm i doświadczenie oferentów, którzy dobiorą odpowiednie narzędzia do osiągnięcia rezultatów.

10. *Czy wymagane jest sprawdzenie skuteczności detekcji (np. testowe zdarzenia w SIEM/EDR)?*

Bez przeprowadzenia testów nie jest możliwa ocena wymieniona w zakresie zapytania. Oczekujemy takich działań, w wyniku których otrzymamy rezultaty sformułowane w zapytaniu. Wierzymy w profesjonalizm i doświadczenie oferentów, którzy dobiorą odpowiednie narzędzia do osiągnięcia rezultatów.

11. *Czy dostępna jest dokumentacja powdrożeniowa systemów (konfiguracje, polityki, procedury)? Jeżeli tak, jaka jest orientacyjna liczba stron dokumentacji?*

Jesteśmy przed wdrożeniem podanych rozwiązań.

12. *Czy audyt ma być realizowany zdalnie, na miejscu, czy w modelu mieszanym? Jeśli wymagane są prace on-site, prosimy o wskazanie liczby lokalizacji oraz miast, w których miałyby być prowadzone działania.*

Audyt nie może zostać zrealizowany zdalnie. 4 lokalizacje w mieście Głogów. Dopuszczamy audyt w trybie hybrydowym.

13. *Jaki poziom dostępu zostanie zapewniony audytorom? Prosimy o informację, czy możliwy będzie dostęp do konsol administracyjnych, konfiguracji, logów, dokumentacji oraz do osób odpowiedzialnych za wdrożenie i utrzymanie poszczególnych systemów.*

Zostanie zapewniony dostęp do konsol administracyjnych, konfiguracji, logów tylko w obecności pracowników działu informatycznego. Niezbędny kontakt z pracownikami będzie zapewniony.

14. *Czy poza oceną poprawności wdrożenia oczekują Państwo również praktycznej weryfikacji skuteczności wybranych mechanizmów bezpieczeństwa? Na przykład poprzez testy konfiguracji, przegląd scenariuszy detekcyjnych, weryfikację reakcji na zdarzenia, analizę przypadków użycia lub warsztaty z administratorami.*

Bez przeprowadzenia testów, nie jest możliwa ocena wymieniona w zakresie zapytania. Oczekujemy takich działań, w wyniku których otrzymamy rezultaty sformułowane w zapytaniu. Wierzymy w profesjonalizm i doświadczenie oferentów, którzy dobiorą odpowiednie narzędzia do osiągnięcia rezultatów.

15. *Czy istnieją konkretne wymagania lub standardy, względem których ma być prowadzona ocena (CIS Benchmarks, ISO 27001, wymogi branżowe, wewnętrzne polityki)?*

Ocena w zakresie technicznym powinna być prowadzona z wykorzystaniem uznanych dobrych praktyk i standardów, umożliwiających weryfikację konfiguracji, skuteczności zabezpieczeń oraz poziomu wdrożenia mechanizmów ochronnych.

Zamawiający dopuszcza zastosowanie m.in.:

CIS Critical Security Controls oraz CIS Benchmarks w zakresie oceny konfiguracji i zabezpieczeń technicznych,

NIST Cybersecurity Framework w zakresie oceny zdolności organizacji do monitorowania, wykrywania oraz reagowania na incydenty bezpieczeństwa, w szczególności w kontekście funkcjonowania systemów SIEM oraz EDR/XDR

16. *Czy audyt obejmuje również weryfikację backupu i odtwarzania? NAS jest w zakresie, ale nie jest jasne czy chodzi tylko o konfigurację urządzenia, czy też politykę kopii zapasowych, separację od produkcji (anty-ransomware), testy odtworzeniowe.*

Tylko w zakresie separacji od produkcji i zabezpieczeń samego serwera NAS.

17. *Czy w zakresie są również urządzenia końcowe użytkowników (konfiguracja stacji roboczych, hardening, GPO), czy tylko infrastruktura centralna?*

Tak. Głównie konfiguracja centralna przez GPO z wybraną grupą urządzeń końcowych, maksymalnie 10 urządzeń.

18. *Kto aktualnie administruje wdrożonymi systemami - zespół wewnętrzny, outsourcing, mieszany model?*

Obecnie administruje wewnętrzny zespół: dział informatyczny – 2 osoby

19. *Ilu pracowników / działów będzie zaangażowanych w wywiady?*

Około 8 - 10 (2 ujęcie wody, 2 oczyszczalnia ścieków, 2 centrala, 2 dział informatyczny, 2 inne)

20. *Czy przewidziane są warsztaty lub spotkania podsumowujące?*

Spotkanie podsumowujące