**Załącznik nr 2 do Umowy nr …………………………..**

**z dnia ………………………… roku**

**Przeprowadzenie audytu konfiguracji ESET Inspect**

Niniejszy załącznik ustala zasady przeprowadzenie audytu konfiguracji ESET Inspect

1. Audytu systemu ESET Inspect dokonany jest przez certyfikowanego przez producenta ESET inżyniera z minimum 3 letnim doświadczeniem oraz posiadającego m.in. certyfikaty z :
2. Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z normą ISO 27001;
3. CISA (Certified Information Systems Auditor);
4. CISSP (Certified Information Systems Security Professional);
5. (C)ISM (CIS Information Security Manager);
6. OSCP (Offensive Security Certified Professional);
7. CEH (Certified Ethical Hacker);
8. eWPT (Web Application Penetration Tester);
9. eWPTX (Web Application Penetration Tester eXtreme).
10. Audyt przeprowadzany jest w formie zdalnej bez uczestnictwa klienta.
11. Wykonawca uzyska połączenie do konsoli ESET Inspect oraz ESET Protect.
12. W trakcie audytu następuje:
13. Weryfikacja ilości wdrożonych konektorów XDR i łączących się do serwera ESET Inspect;
14. Weryfikacja dzienników serwera ESET Inspect;
15. Weryfikacja poprawności konfiguracji zbierania dzienników;
16. Weryfikacja uruchomionych reguł;
17. Weryfikacja statusu bazy danych;
18. Weryfikacja procesów generujących największą ilość danych.
19. Audyt kończy się przekazaniem raportu wraz z rekomendacjami w formie elektronicznej.