Wstęp (5)
1. Zaczynamy (11)

- Szybko zmieniający się kształt zagrożeń (13)
- Po co monitorować? (14)
- Wyzwanie monitoringu (16)
- Zlecanie monitorowania zabezpieczeń (18)
- Monitorowanie w celu minimalizacji ryzyka (18)
- Monitorowanie sterowane regułami (18)
- Czy to zadziała w moim przypadku? (19)
- Produkty komercyjne a produkty o otwartych źródłach (19)
- Firma Blanco Wireless (19)

2. Implementowanie reguł monitorowania (21)

- Monitorowanie czarnej listy (23)
- Monitorowanie anomalii (25)
- Monitorowanie reguł (26)
- Monitorowanie z wykorzystaniem zdefiniowanych reguł (27)
- Rodzaje reguł (28)
- Reguły dla firmy Blanco Wireless (37)
- Wnioski (40)

3. Poznaj swoją sieć (41)

- Taksonomia sieci (41)
- Telemetria sieci (47)
- Sieć firmy Blanco Wireless (63)
- Wnioski (65)

4. Wybieranie celów monitorowania (67)

- Metody wybierania celów (68)
- Praktyczne porady przy wybieraniu celów (81)
- Zalecane cele monitorowania (82)
- Wybieranie komponentów w ramach celów monitorowania (83)
- Blanco Wireless: Wybieranie celów monitorowania (86)
- Wnioski (88)

5. Wybieranie źródeł zdarzeń (89)

- Zadanie źródła danych (89)
- Wybieranie źródeł zdarzeń dla firmy Blanco Wireless (102)
- Wnioski (103)

6. Dostosowywanie (105)

- Sieciowe systemy wykrywania włamań (105)
- Wdrażanie systemu NIDS (111)
- Protokoły systemowe (124)

- NetFlow (141)
- Źródła alarmów bezpieczeństwa w firmie Blanco Wireless (145)
- Wnioski (148)

7. Utrzymywanie niezawodnych źródeł danych (149)

- Utrzymywanie konfiguracji urządzeń (150)
- Monitorowanie monitorujących (155)
- Monitorowanie baz danych (165)
- Automatyczne monitorowanie systemów (169)
- Monitorowanie systemów w firmie Blanco Wireless (173)
- Wnioski (180)

8. Konkluzja: nie trać kontaktu z rzeczywistością (181)

- Co może się nie udać? (182)
- Studium przypadków (188)
- Opowieści zespołów CSIRT (194)
- Wymagania minimalne (195)
- Wnioski (201)

A: Szczegółowa konfiguracja narzędzi OSU flow-tools (203)

- Konfigurowanie serwera (203)
- Konfigurowanie eksportu danych NetFlow na routerze (205)

B: Szablon umowy o świadczenie usług (207)

- Umowa o świadczenie usług: dział sieci i dział bezpieczeństwa (207)

C: Obliczanie dostępności (211)
Skorowidz (215)