

Spis treści |

O autorach	11
O recenzentach	12
Przedmowa	13

CZĘŚĆ 1. Wprowadzenie do inżynierii detekcji

ROZDZIAŁ 1

Podstawy inżynierii detekcji	19
Podstawowe pojęcia	19
Unified Kill Chain	20
Framework MITRE ATT&CK	22
Piramida bólu	24
Rodzaje cyberataków	25
Motywacja dla inżynierii detekcji	28
Definicja inżynierii detekcji	30
Ważne cechy wyróżniające	32
Wartość programu inżynierii detekcji	32
Potrzeba zapewnienia lepszej wykrywalności	33
Cechy dobrego wykrywania zagrożeń	33
Korzyści z programu inżynierii detekcji	35
Przewodnik korzystania z tej książki	37
Struktura książki	37
Ćwiczenia praktyczne	38
Podsumowanie	39

ROZDZIAŁ 2

Cykl życia inżynierii detekcji	40
Faza 1. Odkrywanie wymagań	41
Charakterystyka kompletnego wymagania mechanizmu detekcji	42
Źródła wymagań dla mechanizmów detekcji	43

Ćwiczenie. Źródła wymagań dotyczących mechanizmów detekcji w Twojej organizacji	48
Faza 2. Selekcja	49
Dotkliwość zagrożenia	50
Dopasowanie mechanizmu detekcji zagrożenia do organizacji	50
Pokrycie zagrożeń mechanizmami detekcji	50
Aktywne eksploity	51
Faza 3. Analiza	52
Określenie źródła danych	52
Ustalenie typów wskaźników wykrycia	53
Kontekst badawczy	53
Ustalenie kryteriów walidacji	55
Faza 4. Programowanie	55
Faza 5. Testowanie	56
Rodzaje danych testowych	57
Faza 6. Wdrażanie	58
Podsumowanie	59

ROZDZIAŁ 3

Budowa laboratorium testowego inżynierii detekcji	60
Wymagania techniczne	61
Elastic Stack	61
Wdrażanie systemu Elastic Stack za pomocą Dockera	63
Konfiguracja Elastic Stack	68
Konfiguracja narzędzia Fleet Server	72
Instalacja i konfiguracja systemu Fleet Server	73
Dodatkowe konfiguracje dla komponentu Fleet Server	75
Dodawanie hosta do laboratorium	77
Zasady komponentu Elastic Agent	83
Tworzenie pierwszego mechanizmu detekcji	85
Dodatkowe zasoby	87
Podsumowanie	88

CZĘŚĆ 2. Tworzenie mechanizmów detekcji

ROZDZIAŁ 4

Źródła danych inżynierii detekcji	91
Wymagania techniczne	92
Źródła danych i telemetrii	92
Nieprzetworzona telemetria	92
Narzędzia zabezpieczeń	100

Źródła danych MITRE ATT&CK	101
Identyfikacja źródeł danych	102
Analiza problemów i wyzwań związanych ze źródłami danych	104
Kompletność	104
Jakość	105
Terminowość	105
Pokrycie	106
Ćwiczenie. Więcej informacji o źródłach danych	106
Dodawanie źródeł danych	107
Ćwiczenie. Dodawanie źródła danych serwera WWW	107
Podsumowanie	116
Lektura uzupełniająca	117

ROZDZIAŁ 5

Analiza wymagań dla mechanizmów detekcji	118
Przegląd faz wymagań dla mechanizmów detekcji	118
Odkrywanie wymagań dla mechanizmów detekcji	119
Narzędzia i procesy	120
Ćwiczenie. Odkrywanie wymagań w organizacji	122
Selekcja wymagań dla mechanizmów detekcji	124
Dotkliwość zagrożenia	124
Dopasowanie zagrożenia do organizacji	125
Pokrycie wymagań dla mechanizmów detekcji	126
Aktywne exploity	126
Obliczanie priorytetu	127
Analiza wymagań dla mechanizmów detekcji	130
Podsumowanie	132

ROZDZIAŁ 6

Tworzenie mechanizmów detekcji przy użyciu wskaźników naruszeń zabezpieczeń	133
Wymagania techniczne	134
Wykorzystanie wskaźników naruszenia zabezpieczeń	134
Przykładowy scenariusz. Identyfikacja kampanii IcedID przy użyciu wskaźników	137
Ćwiczenie	146
Instalacja i konfigurowanie systemu Sysmon jako źródła danych	146
Wykrywanie skrótów	148
Mechanizmy detekcji wskaźników sieciowych	151
Podsumowanie ćwiczenia	155

Podsumowanie	155
Lektura uzupełniająca	155

ROZDZIAŁ 7

Opracowywanie mechanizmów detekcji opartych na wskaźnikach

behawioralnych	156
Wymagania techniczne	156
Wykrywanie narzędzi przeciwnika	156
Przykładowy scenariusz. Użycie narzędzia PsExec	157
Wykrywanie taktyk, technik i procedur (TTP)	173
Przykładowy scenariusz. Technika omijania kontroli znacznika sieci	174
Podsumowanie	179

ROZDZIAŁ 8

Tworzenie dokumentacji i potoki mechanizmów detekcji

Dokumentowanie mechanizmu detekcji	181
Ćwiczenie. Dokumentowanie mechanizmu detekcji	184
Analiza repozytorium mechanizmów detekcji	187
Mechanizm detekcji jako kod	190
Wyzwania związane z tworzeniem potoku mechanizmu detekcji	199
Ćwiczenie. Publikowanie reguły przy użyciu projektu mechanizmów detekcji Elastic	200
Podsumowanie	209

CZĘŚĆ 3. Walidacja mechanizmów detekcji

ROZDZIAŁ 9

Walidacja mechanizmów detekcji

Wymagania techniczne	214
Czym jest proces walidacji?	214
Na czym polegają ćwiczenia zespołu purple team?	216
Symulowanie aktywności przeciwnika	217
Atomic Red Team	218
CALDERA	219
Ćwiczenie. Walidacja mechanizmów detekcji dla pojedynczej techniki z wykorzystaniem Atomic Red Team	220
Ćwiczenie. Walidacja mechanizmów detekcji dla wielu technik z wykorzystaniem systemu CALDERA	226

Korzystanie z wyników walidacji	232
Pomiar pokrycia zagrożeń mechanizmami detekcji	234
Podsumowanie	241
Lektura uzupełniająca	241

ROZDZIAŁ 10

Wykorzystanie wiedzy o zagrożeniach	242
Wymagania techniczne	242
Przegląd zagadnień związanych z wiedzą o zagrożeniach	243
Wiedza o zagrożeniach typu open source	243
Wewnętrzne źródła wiedzy o zagrożeniach	245
Zbieranie wiedzy o zagrożeniach	245
Wiedza o zagrożeniach w cyklu życia inżynierii detekcji	246
Odkrywanie wymagań	246
Selekcja	246
Analiza	248
Wiedza o zagrożeniach na potrzeby inżynierii detekcji w praktyce	248
Przykład. Wykorzystywanie na potrzeby inżynierii detekcji wpisów na blogach z informacjami o zagrożeniach	249
Przykład. Wykorzystanie systemu VirusTotal na potrzeby inżynierii detekcji	252
Ocena zagrożeń	255
Przykład. Wykorzystanie oceny zagrożeń na potrzeby inżynierii detekcji	256
Zasoby i dalsza lektura	262
Źródła i pojęcia związane z wiedzą o zagrożeniach	262
Skanery online i piaskownice	263
MITRE ATT&CK	263
Podsumowanie	263

CZĘŚĆ 4. Metryki i zarządzanie

ROZDZIAŁ 11

Zarządzanie wydajnością	267
Wprowadzenie do zarządzania wydajnością	267
Ocena dojrzałości mechanizmu detekcji	268
Pomiar wydajności programu inżynierii detekcji	270
Pomiar skuteczności programu inżynierii detekcji	272
Priorytetyzacja prac związanych z detekcją	274
Trafność, hałaśliwość i czułość	276

Obliczanie skuteczności mechanizmu detekcji	280
Metryki pokrycia o niskiej wierności	280
Automatyczna walidacja	282
Metryki pokrycia o wysokiej wierności	282
Podsumowanie	296
Lektura uzupełniająca	296

CZĘŚĆ 5. Kariera w inżynierii detekcji

ROZDZIAŁ 12

Wskazówki dotyczące kariery w inżynierii detekcji	301
Zdobycie pracy w branży inżynierii detekcji	301
Oferty pracy	302
Rozwijanie umiejętności	303
Inżynier detekcji jako zawód	307
Role i obowiązki inżyniera detekcji	309
Przyszłość inżynierii detekcji	310
Powierzchnie ataku	310
Widoczność	311
Możliwości urządzeń zabezpieczeń	311
Uczenie maszynowe	312
Współdzielenie metodologii ataków	313
Przeciwnik	313
Człowiek	313
Podsumowanie	314