

Spis treści

O autorce	8
O recenzentach	9
Wstęp	10

Część I. Informatyka wywiadowcza 15

Rozdział 1. Czym jest informatyka wywiadowcza?	17
--	----

Informatyka wywiadowcza	17
Poziom strategiczny	19
Poziom operacyjny	19
Poziom taktyczny	19
Cykl działań wywiadowczych	22
Planowanie i wyznaczanie celów	24
Przygotowywanie i gromadzenie danych	25
Przetwarzanie i wykorzystywanie danych	25
Analiza i wytwarzanie informacji	25
Rozpowszechnianie i integracja wiedzy	25
Ocena i informacje zwrotne	25
Definiowanie Twojego zapotrzebowania na informacje wywiadowcze	27
Proces gromadzenia danych	28
Wskaźniki naruszenia bezpieczeństwa	29
Zrozumieć złośliwe oprogramowanie	29
Wykorzystanie źródeł publicznych do gromadzenia danych — OSINT	31
Honeypoty	31
Analiza złośliwego oprogramowania i sandboxing	31

Przetwarzanie i wykorzystywanie danych	32
Cyber Kill Chain®	33
Model diamentowy	34
Framework MITRE ATT&CK™	35
Tendencyjność a analiza informacji	35
Podsumowanie	37
Rozdział 2. Czym jest polowanie na zagrożenia?	38
Wymogi merytoryczne	38
Czym jest polowanie na zagrożenia?	39
Rodzaje polowań na zagrożenia	40
Zestaw umiejętności łowcy zagrożeń	41
Piramida bólu	42
Model dojrzałości w procesie polowania na zagrożenia	44
Określenie naszego modelu dojrzałości	44
Proces polowania na zagrożenia	45
Pętla polowania na zagrożenia	46
Model polowania na zagrożenia	47
Metodologia oparta na danych	48
TaHiTI — polowanie ukierunkowane integrujące informatykę wywiadowczą	51
Tworzenie hipotezy	54
Podsumowanie	56
Rozdział 3. Z jakich źródeł pozyskujemy dane?	57
Wymogi merytoryczne i techniczne	57
Zrozumienie zebranych danych	57
Podstawy systemów operacyjnych	58
Podstawy działania sieci komputerowych	61
Narzędzia dostępne w systemie Windows	74
Podgląd zdarzeń w systemie Windows	74
Instrumentacja zarządzania systemem Windows (WMI)	78
Śledzenie zdarzeń dla Windows (ETW)	78
Źródła danych	80
Dane z punktów końcowych	80
Dane sieciowe	84
Dane zabezpieczeń	91
Podsumowanie	96
Część II. Zrozumieć przeciwnika	97
Rozdział 4. Jak mapować przeciwnika	99
Wymogi merytoryczne	99
Framework ATT&CK	100
Taktyki, techniki, subtechniki i procedury	100
Macierz ATT&CK	102
Nawigator ATT&CK	105

Mapowanie za pomocą frameworka ATT&CK	107
Przetestuj się!	109
Odpowiedzi	113
Podsumowanie	115
Rozdział 5. Praca z danymi	116
Wymogi merytoryczne i techniczne	116
Używanie słowników danych	117
Metadane zdarzeń zagrażających bezpieczeństwu typu open source	118
Używanie narzędzia MITRE CAR	121
CARET	122
Używanie Sigmy	124
Podsumowanie	126
Rozdział 6. Jak emulować przeciwnika	127
Stworzenie planu emulacji przeciwnika	127
Czym jest emulacja przeciwnika?	127
Plan emulacji zespołu MITRE ATT&CK™	128
Jak emulować zagrożenie	130
Atomic Red Team	130
Mordor (Security Datasets)	131
CALDERA	133
Pozostałe narzędzia	134
Przetestuj się!	136
Odpowiedzi	138
Podsumowanie	138
Część III. Jak pracować z wykorzystaniem środowiska badawczego	139
Rozdział 7. Jak stworzyć środowisko badawcze	141
Wymogi merytoryczne i techniczne	142
Konfigurowanie środowiska badawczego	142
Instalowanie środowiska wirtualnego VMware ESXI	143
Tworzenie sieci VLAN	144
Konfigurowanie zapory (firewalla)	146
Instalowanie systemu operacyjnego Windows Server	152
Konfigurowanie systemu operacyjnego Windows Server w roli kontrolera domeny	156
Zrozumienie struktury usługi katalogowej Active Directory	159
Nadanie serwerowi statusu kontrolera domeny	161
Konfigurowanie serwera DHCP	163
Tworzenie jednostek organizacyjnych	168
Tworzenie użytkowników	169
Tworzenie grup	172
Obiekty zasad grupy	175

Konfigurowanie zasad inspekcji	178
Dodawanie nowych klientów	186
Konfigurowanie stosu ELK	188
Konfigurowanie usługi systemowej Sysmon	193
Pobieranie certyfikatu	195
Konfigurowanie aplikacji Winlogbeat	196
Szukanie naszych danych w instancji stosu ELK	199
Bonus — dodawanie zbiorów danych Mordor do naszej instancji stosu ELK	200
HELK — narzędzie open source autorstwa Roberto Rodriguez	201
Rozpoczęcie pracy z platformą HELK	202
Podsumowanie	204
 Rozdział 8. Jak przeprowadzać kwerendę danych	 205
Wymogi merytoryczne i techniczne	205
Atomowe polowanie z użyciem bibliotek Atomic Red Team	206
Cykl testowy bibliotek Atomic Red Team	207
Testowanie dostępu początkowego	208
Testowanie wykonania	216
Testowanie zdolności do przetrwania	218
Testy nadużywania przywilejów	220
Testowanie unikania systemów obronnych	223
Testowanie pod kątem wykrywania przez atakującego zasobów ofiary	224
Testowanie taktyki wysyłania poleceń i sterowania (C2)	225
Invoke-AtomicRedTeam	227
Quasar RAT	227
Przypadki użycia trojana Quasar RAT w świecie rzeczywistym	228
Uruchamianie i wykrywanie trojana Quasar RAT	230
Testowanie zdolności do przetrwania	234
Testowanie dostępu do danych uwierzytelniających	237
Badanie ruchów poprzecznych	238
Podsumowanie	239
 Rozdział 9. Jak polować na przeciwnika	 240
Wymogi merytoryczne i techniczne	240
Oceny przeprowadzone przez MITRE	241
Importowanie zbiorów danych APT29 do bazy HELK	242
Polowanie na APT29	243
Używanie frameworka MITRE CALDERA	271
Konfigurowanie programu CALDERA	272
Wykonanie planu emulacji za pomocą programu CALDERA	277
Reguły pisane w języku Sigma	287
Podsumowanie	290
 Rozdział 10. Znaczenie dokumentowania i automatyzowania procesu	 291
Znaczenie dokumentacji	291
Klucz do pisania dobrej dokumentacji	292
Dokumentowanie polowań	294

Threat Hunter Playbook	297
Jupyter Notebook	298
Aktualizowanie procesu polowania	299
Znaczenie automatyzacji	300
Podsumowanie	301
Część IV. Wymiana informacji kluczem do sukcesu	303
Rozdział 11. Jak oceniać jakość danych	305
Wymogi merytoryczne i techniczne	305
Jak odróżnić dane dobrej jakości od danych złej jakości	306
Wymiary danych	307
Jak poprawić jakość danych	308
OSSEM Power-up	310
DeTT&CT	310
Sysmon-Modular	312
Podsumowanie	315
Rozdział 12. Jak zrozumieć dane wyjściowe	316
Jak zrozumieć wyniki polowania	316
Znaczenie wyboru dobrych narzędzi analitycznych	320
Przetestuj się!	321
Odpowiedzi	323
Podsumowanie	323
Rozdział 13. Jak zdefiniować dobre wskaźniki śledzenia postępów	324
Wymogi merytoryczne i techniczne	324
Znaczenie definiowania dobrych wskaźników	325
Jak określić sukces programu polowań	328
Korzystanie z frameworka MaGMA for Threat Hunting	329
Podsumowanie	331
Rozdział 14. Jak stworzyć zespół szybkiego reagowania i jak informować zarząd o wynikach polowań	332
Jak zaangażować w działanie zespół reagowania na incydenty	333
Wpływ komunikowania się na sukces programu polowania na zagrożenia	336
Przetestuj się!	339
Odpowiedzi	341
Podsumowanie	341
Dodatek. Stan polowań	343