

Spis treści |

O autorze	13
O recenzencie	14
Przedmowa	15

CZĘŚĆ 1. Podstawy reagowania na incydenty i kryminalistyki cyfrowej

ROZDZIAŁ 1

Czym jest reagowanie na incydenty	23
Proces reagowania na incydenty	24
Rola kryminalistyki cyfrowej	27
Ramy reagowania na incydenty	28
Karta reagowania na incydenty	28
Zespół CSIRT	30
Plan reagowania na incydenty	36
Klasyfikowanie incydentów	38
Podręcznik reagowania na incydenty	39
Proces eskalacji	41
Testowanie ram reagowania na incydenty	44
Podsumowanie	46
Pytania	46
Literatura uzupełniająca	47

ROZDZIAŁ 2

Zarządzanie incydentami cyberbezpieczeństwa	48
Angażowanie zespołu reagowania na incydenty	49
Modele angażowania zespołów CSIRT	49
Badanie incydentów	54
Centrum operacyjne zespołu CSIRT	56

Komunikacja	57
Rotowanie personelu	57
SOAR	58
Uwzględnianie komunikacji kryzysowej	60
Komunikacja wewnętrzna	60
Komunikacja zewnętrzna	61
Powiadomienie publiczne	62
Uwzględnianie strategii powstrzymania	62
Powrót do normalności — likwidacja, odtworzenie i działania po incydencie	65
Podsumowanie	68
Pytania	69
Lektura uzupełniająca	69

ROZDZIAŁ 3

Podstawy kryminalistyki cyfrowej	70
Rozwój kryminalistyki	70
Zasada wymiany Locarda	71
Zagadnienia prawne w kryminalistyce cyfrowej	72
Regulacje prawne	73
Zasady postępowania z dowodami	74
Procedury kryminalistyczne w reagowaniu na incydenty	75
Krótka historia kryminalistyki cyfrowej	75
Proces kryminalistyki cyfrowej	76
Laboratorium kryminalistyki cyfrowej	84
Podsumowanie	94
Pytania	95
Lektura uzupełniająca	95

ROZDZIAŁ 4

Metoda dochodzeniowa	96
Studium przypadku analizy włamań: kukułka jajo	97
Rodzaje dochodzeń cyfrowych	99
Funkcjonalna metoda dochodzenia cyfrowego	102
Identyfikacja i określanie zakresu	103
Zbieranie dowodów	103
Wstępna analiza incydentu	104
Wstępna korelacja	104
Normalizacja incydentu	105

Dekonfliktowanie zdarzenia	105
Druga korelacja	106
Oś czasu	106
Analiza kill chain	106
Raportowanie	106
Łańcuch kill chain	107
Model diamentowy analizy włamań	110
Aksjomaty modelu diamentowego	114
Kombinacja modelu diamentowego i analizy włamań łańcucha kill chain	115
Atrybucja	117
Podsumowanie	117
Pytania	118

CZĘŚĆ 2. Pozyskiwanie dowodów

ROZDZIAŁ 5

Zbieranie dowodów sieciowych	121
Przegląd dowodów sieciowych	121
Przygotowanie	124
Schemat sieci	124
Konfiguracja	125
Zapory ogniowe i dzienniki proxy	125
Zapory sieciowe	126
Zapory aplikacji internetowych	126
Internetowe serwery proxy	127
NetFlow	127
Przechwytywanie pakietów	128
tcpdump	129
WinPcap i RawCap	132
Wireshark	134
Zbieranie dowodów	137
Podsumowanie	139
Pytania	140
Lektura uzupełniająca	140

ROZDZIAŁ 6

Pozyskiwanie dowodów opartych na hoście	141
Przygotowania	141
Hierarchia ulotności	142

Pozyskiwanie dowodów	143
Procedury zbierania dowodów	144
Pozyskiwanie z pamięci ulotnej	146
FTK Imager	147
WinPmem	150
RAM Capturer	151
Systemy wirtualne	154
Pozyskiwanie dowodów nieulotnych	155
Pozyskiwanie plików chronionych za pomocą programu FTK	155
Narzędzie CyLR	156
Kroll Artifact Parser and Extractor	157
Podsumowanie	162
Pytania	162
Lektura uzupełniająca	163

ROZDZIAŁ 7

Zdalne gromadzenie dowodów	164
Wyzwania związane z reagowaniem na incydenty w organizacji	164
Wykrywanie w punktach końcowych i reagowanie	165
Omówienie i implementacja narzędzia Velociraptor	166
Serwer narzędzia Velociraptor	168
Moduł zbierający narzędzia Velociraptor dla systemu Windows	170
Velociraptor a scenariusze	171
Zbieranie dowodów z użyciem narzędzia Velociraptor	172
CyLR	173
WinPmem	174
Podsumowanie	181
Pytania	181

ROZDZIAŁ 8

Obrazowanie kryminalistyczne	183
Czym jest obrazowanie kryminalistyczne	184
Obraz kontra kopia	184
Woluminy logiczne i fizyczne	184
Rodzaje plików obrazów	186
SSD kontra HDD	186
Narzędzia do obrazowania	188
Przygotowanie dysku do przechowywania obrazów	189
Korzystanie z blokad zapisu	193

Techniki obrazowania	194
Obrazowanie przy wyłączonym systemie	194
Obrazowanie na żywo	202
Systemy wirtualne	203
Obrazowanie w systemie Linux	205
Podsumowanie	210
Pytania	211
Lektura uzupełniająca	211

CZĘŚĆ 3. Badanie dowodów

ROZDZIAŁ 9

Badanie dowodów sieciowych	215
Przegląd dowodów sieciowych	215
Analiza dzienników zapory sieciowej i proxy	217
Narzędzia SIEM	218
Elastic Stack	219
NetFlow	220
Analizowanie przechwyconych pakietów	221
Narzędzia wiersza poleceń	222
Real Intelligence Threat Analytics	223
NetworkMiner	226
Arkime	228
Wireshark	232
Podsumowanie	239
Pytania	240
Lektura uzupełniająca	240

ROZDZIAŁ 10

Badanie pamięci systemowej	241
Omówienie analizy pamięci	242
Metodyka analizy pamięci	242
Sześćoetapowa metodyka SANS	243
Metodyka połączeń sieciowych	244
Narzędzia do badania pamięci	244
Analiza pamięci z wykorzystaniem Volatility	245
Volatility Workbench	255
Badanie pamięci z wykorzystaniem Strings	256
Instalowanie Strings	257
Typowe wyszukiwania w Strings	257

Podsumowanie	258
Pytania	258
Lektura uzupełniająca	259

ROZDZIAŁ 11

Analiza systemowej pamięci masowej	260
Platformy kryminalistyczne	261
Autopsy	263
Instalowanie Autopsy	264
Zakładanie nowego dochodzenia	264
Dodawanie dowodów	266
Poruszanie się w Autopsy	270
Badanie dochodzenia	272
Analiza głównej tablicy plików	284
Analiza prefetch	286
Analiza rejestru	287
Podsumowanie	292
Pytania	292
Lektura uzupełniająca	293

ROZDZIAŁ 12

Analizowanie plików dziennika	294
Dzienniki i zarządzanie nimi	294
Korzystanie z systemów SIEM	296
Splunk	299
Elastic Stack	299
Security Onion	300
Dzienniki systemu Windows	301
Dzienniki zdarzeń systemu Windows	301
Analiza dzienników zdarzeń systemu Windows	305
Pozyskiwanie dzienników	305
Triaż	307
Szczegółowa analiza dziennika zdarzeń	309
Podsumowanie	319
Pytania	319
Lektura uzupełniająca	320

ROZDZIAŁ 13

Tworzenie raportu o incydencie	321
Przegląd dokumentacji	322
Co należy dokumentować	322
Rodzaje dokumentacji	323
Źródła danych	325
Odbiorcy	325
Raport wykonawczy	327
Raport z dochodzenia w sprawie incydentu	328
Raport kryminalistyczny	331
Przygotowanie raportu kryminalistycznego z incydentu	336
Sporządzanie notatek	336
Język raportu	340
Podsumowanie	341
Pytania	341
Lektura uzupełniająca	342

CZĘŚĆ 4. Reagowanie na incydenty związane z oprogramowaniem ransomware

ROZDZIAŁ 14

Przygotowanie i reagowanie na oprogramowanie ransomware	345
Historia oprogramowania ransomware	346
CryptoLocker	346
CryptoWall	346
CTB-Locker	346
TeslaCrypt	348
SamSam	348
Locky	348
WannaCry	349
Ryuk	349
Analiza przypadku oprogramowania ransomware Conti	349
Kontekst	350
Ujawnienie operacyjne	351
Taktyki i techniki	352
Eksfiltracja	358
Wpływ	358

Właściwe przygotowanie na ransomware	359
Odporność na oprogramowanie ransomware	359
Przygotowanie zespołu CSIRT	361
Likwidacja i odzyskiwanie	362
Powstrzymywanie	362
Likwidacja	364
Odzyskiwanie	364
Podsumowanie	367
Pytania	368
Informacje uzupełniające	368

ROZDZIAŁ 15

Dochodzenie w sprawie ransomware	369
Początkowy dostęp i wykonanie oprogramowania ransomware	369
Uzyskanie początkowego dostępu	370
Wykonanie	377
Uzyskiwanie dostępu do danych uwierzytelniających i ich kradzież	380
ProcDump	381
Mimikatz	381
Badanie działań poeksploatacyjnych	383
Dowodzenie i kontrola	388
Security Onion	389
RITA	390
Arkime	391
Badanie technik ruchu bocznego	393
Podsumowanie	397
Pytania	397
Lektura uzupełniająca	398

CZĘŚĆ 5. Analiza i polowanie na zagrożenia

ROZDZIAŁ 16

Analiza złośliwego oprogramowania w reagowaniu na incydenty	401
Przegląd analizy złośliwego oprogramowania	402
Klasyfikacja złośliwego oprogramowania	405
Konfigurowanie piaskownicy na potrzeby złośliwego oprogramowania	407
Piaskownica lokalna	407
Piaskownica w chmurze	408
Analiza statyczna	408
Analiza właściwości statycznych	410

Analiza dynamiczna	413
Eksplorator procesów	414
Process Spawn Control	415
Zautomatyzowana analiza	417
ClamAV	422
YARA	424
yarGen	426
Podsumowanie	429
Pytania	429
Lektura uzupełniająca	430

ROZDZIAŁ 17

Korzystanie z analizy cyberzagrożeń	431
Czym jest analiza cyberzagrożeń	431
Rodzaje analiz cyberzagrożeń	434
Piramida bólu	435
Metodyka analizy cyberzagrożeń	437
Pozyskiwanie informacji o cyberzagrożeniach	438
Źródła opracowywane wewnętrznie	439
Źródła komercyjne	439
Źródła open source	440
Baza MITRE ATT&CK	441
Korzystanie z IOC i IOA	448
Analiza cyberzagrożeń w reagowaniu na incydenty	452
Autopsy	452
Maltego	454
YARA i Loki	459
Podsumowanie	462
Pytania	462
Lektura uzupełniająca	463

ROZDZIAŁ 18

Polowanie na cyberzagrożenia	464
Czym jest polowanie na zagrożenia	465
Cykl wykrywania zagrożeń	465
Raportowanie działań związanych z polowaniem na zagrożenia	469
Model dojrzałości polowania na zagrożenia	471
Stawianie hipotezy	472
MITRE ATT&CK	473
Planowanie polowania na zagrożenia	474

Cyfrowe techniki kryminalistyczne w polowaniu na zagrożenia	476
EDR w polowaniu na zagrożenia	477
Podsumowanie	480
Pytania	480
Lektura uzupełniająca	481
Dodatek	483
Odpowiedzi	487
Skorowidz	489