

Spis treści |

O autorach	11
O recenzentach	12
Przedmowa	13
Wprowadzenie	15

CZĘŚĆ 1. Krajobraz zagrożeń i cykl cyberataku

ROZDZIAŁ 1

Wprowadzenie do krajobrazu zagrożeń	23
Krajobraz cyberzagrożeń	24
Rodzaje aktorów zagrożeń i ich motywacje	28
Zaawansowane trwałe zagrożenia	28
Cyberprzestępcy	31
Haktywiści	36
Konkurenci	36
Wewnętrzne zagrożenia	37
Grupy terrorystyczne	38
Domorośli hakerzy	38
Wnioski	38
Kształtowanie krajobrazu cyberzagrożeń	39
Podsumowanie	41

ROZDZIAŁ 2.

Cykl cyberataku	43
Faza 1. Zdobyć początkowego przyczółku	44
Uzyskiwanie dostępu do sieci	44
Ustanawianie przyczółku	47
Rozpoznawanie sieci	54
Faza 2. Utrzymanie dostępu i widoczności	59
Odkrywanie kluczowych zasobów	59
Rozprzestrzenianie się w sieci	60

Faza 3. Eksfiltracja danych i skutki	62
Eksfiltracja danych	63
Skutki	65
Podsumowanie	66

CZĘŚĆ 2. Procedury reagowania na incydenty i zbieranie dowodów kryminalistycznych z endpointów

ROZDZIAŁ 3.

Fazy efektywnego reagowania na incydenty

w infrastrukturze systemu Windows	69
Role, zasoby i problemy w reagowaniu na incydenty	70
Przygotowanie i planowanie — opracowanie skutecznego planu reagowania na incydenty	72
Wykrywanie i weryfikowanie — rozpoznawanie, ocena i potwierdzanie incydentów cyberbezpieczeństwa skierowanych przeciwko systemom Windows	76
Wykrywanie incyduentu	76
Weryfikowanie incyduentu	77
Klasyfikowanie incyduentu	79
Analizowanie i powstrzymywanie — badanie i blokowanie rozprzestrzeniania się cyberataków	80
Analizowanie incyduentu	80
Powstrzymywanie incyduentu	82
Eliminowanie i odzyskiwanie — usuwanie śladów włamania i powrót do normalnego funkcjonowania	84
Eliminowanie incyduentu	84
Odzyskiwanie	85
Podsumowanie	86

ROZDZIAŁ 4.

Pozyskiwanie dowodów z endpointów	87
Wprowadzenie do zbierania dowodów z endpointów	88
Zbieranie danych z endpointów	94
Pozyskiwanie danych trwałych	94
Pozyskiwanie danych z pamięci	96
Przechwytywanie danych o ruchu sieciowym	98
Skalowalność gromadzenia dowodów cyfrowych	101
Podsumowanie	103

CZĘŚĆ 3. Analiza incydentów i polowanie na zagrożenia w systemach Windows

ROZDZIAŁ 5.

Uzyskiwanie dostępu do sieci	107
Użycie aplikacji dostępnych publicznie	107
Wykorzystanie zewnętrznych usług zdalnych	110
Spear phishing	112
Atak typu drive-by	117
Inne metody uzyskiwania początkowego dostępu	119
Podsumowanie	120

ROZDZIAŁ 6.

Ustanawianie przyczółku	121
Metody analizy powłamaniowej	121
Utrzymywanie stałego dostępu do systemów Windows	122
Dzienniki zdarzeń	123
Rejestr systemu Windows	126
Metadane systemu plików	128
Inne źródła	129
Kanały komunikacji C2	131
Podsumowanie	133

ROZDZIAŁ 7.

Rozpoznawanie sieci i kluczowych zasobów	134
Techniki rozpoznawania środowiska Windows	134
Przypadek 1. Operatorzy ransomware'u	135
Przypadek 2. Klasyczne grupy motywowane finansowo	135
Przypadek 3. Szpiegostwo korporacyjne	136
Wykrywanie fazy rozpoznawania	139
Korzystanie z wyspecjalizowanych programów	139
Korzystanie z narzędzi systemowych	142
Dostęp do określonych lokalizacji i plików	143
Doraźna eksfiltracja danych	144
Podsumowanie	145

ROZDZIAŁ 8.

Rozprzestrzenianie się w sieci	146
Ruch boczny w środowisku Windows	146
Wykrywanie ruchu bocznego	148
Usługi zdalne	148
Narzędzia do wdrażania oprogramowania	150
Przenoszenie narzędzi między systemami	151
Wewnętrzny spear phishing	152
Cykliczność etapów pośrednich	152
Podsumowanie	153

ROZDZIAŁ 9.

Gromadzenie i eksfiltracja danych	154
Rodzaje danych będących celem ataków	154
Metody zbierania danych	156
Techniki eksfiltracji danych	157
Wykrywanie gromadzenia i eksfiltracji danych	159
Podsumowanie	162

ROZDZIAŁ 10.

Skutki	164
Rodzaje skutków	164
Ocena skutków	166
Skutki bezpośrednie	166
Ograniczanie skutków	169
Technologia	169
Ludzie	169
Procesy	170
Podsumowanie	171

ROZDZIAŁ 11.

Polowanie na zagrożenia oraz analiza taktyk, technik i procedur	172
Polowanie na zagrożenia	173
Analiza zagrożeń cybernetycznych	174
Polowanie na zagrożenia w systemach Windows	180
Częstotliwość polowania na zagrożenia	182
Przygotowanie polowania	184
Planowanie polowania	186

Wykrywanie anomalii — identyfikowanie włamań w środowiskach Windows	186
Zdobywanie uprawy w polowaniu na zagrożenia — role i umiejętności	188
Podsumowanie	191

CZĘŚĆ 4. Zarządzanie dochodzeniem w sprawie incydentów i sporządzanie raportów

ROZDZIAŁ 12.

Powstrzymywanie, eliminowanie i odzyskiwanie	195
Warunki wstępne i proces powstrzymywania incyduentu	196
Warunki wstępne powstrzymywania incyduentu	196
Planowanie powstrzymywania incydentów	199
Proces powstrzymywania incyduentu	200
Warunki wstępne i proces eliminowania incyduentu	205
Warunki wstępne i proces odzyskiwania sprawności po incydencie	206
Przygotowywanie działań naprawczych po incydencie	208
Podsumowanie	211

ROZDZIAŁ 13.

Zamykanie dochodzenia i sporządzanie raportu z incyduentu	212
Zamknięcie incyduentu	213
Analiza luk	215
Dokumentacja incyduentu	216
Podsumowujący raport techniczny	220
Podsumowujący raport dla kadry kierowniczej	222
Formularze pozyskiwania dowodów	222
Formularze łańcucha dowodowego	224
Wnioski z incyduentu	225
Zewnętrzne kanały zgłaszania incydentów cyberbezpieczeństwa	226
Podsumowanie	229