

Spis treści |

O autorach	15
O korektorze merytorycznym	16
Wstęp	17

ROZDZIAŁ 1

Stan zabezpieczeń	21
Dlaczego higiena bezpieczeństwa powinna być priorytetem?	21
Obecny krajobraz zagrożeń	23
Ataki z wykorzystaniem łańcucha dostaw	26
Ransomware	28
Poświadczenia — uwierzytelnianie i autoryzacja	33
Aplikacje	35
Dane	36
Wyzwania dotyczące cyberbezpieczeństwa	37
Stare techniki i szersze rezultaty	38
Zmiana krajobrazu zagrożeń	39
Poprawianie stanu zabezpieczeń	41
Architektura zerowego zaufania	43
Zarządzanie stanem zabezpieczeń w chmurze	45
Środowisko wielochmurowe	47
Zespoły czerwone i niebieskie	49
Zakładanie naruszenia bezpieczeństwa	52
Podsumowanie	53
Materiały źródłowe	54

ROZDZIAŁ 2

Proces reagowania na incydenty	57
Proces reagowania na incydenty	57
Dlaczego należy wdrożyć proces IR?	58
Tworzenie procesu reagowania na incydenty	61

Zespół reagowania na incydenty	63
Cykl życia incydentu	64
Obsługa incydentu	65
Lista kontrolna dla obsługi incydentów	68
Działania po zdarzeniu	69
Scenariusz 1.	70
Wnioski ze scenariusza 1.	71
Scenariusz 2.	72
Wnioski ze scenariusza 2.	75
Kwestie związane z reagowaniem na incydenty w chmurze	76
Aktualizacja procesu IR w celu uwzględnienia charakterystyki chmury	77
Odpowiedni zestaw narzędzi	78
Proces IR z perspektywy dostawcy rozwiązań w chmurze	78
Podsumowanie	79
Materiały źródłowe	79

ROZDZIAŁ 3

Czym jest cyberstrategia?	81
Jak zbudować cyberstrategię?	81
1. Zrozumienie organizacji	82
2. Zrozumienie zagrożeń i ryzyka	82
3. Odpowiednia dokumentacja	83
Dlaczego trzeba budować cyberstrategię?	84
Najlepsze cyberstrategie ataku	86
Strategie testowania zewnętrznego	86
Strategie testowania wewnętrznego	87
Strategia testowania ślepego	87
Strategia testowania ukierunkowanego	87
Najlepsze cyberstrategie defensywne	88
Obrona w głąb	88
Obrona wszcz	89
Korzyści z posiadania proaktywnej strategii cyberbezpieczeństwa	90
Najlepsze strategie cyberbezpieczeństwa dla firm	92
Szkolenie pracowników w zakresie zasad bezpieczeństwa	93
Ochrona sieci, informacji i komputerów przed wirusami, złośliwym kodem i oprogramowaniem szpiegującym	93
Stosowanie firewalla dla wszystkich połączeń internetowych	94
Aktualizowanie oprogramowania	94
Korzystanie z kopii zapasowych	94
Zaimplementowanie ograniczeń fizycznych	94

Zabezpieczanie sieci wi-fi	95
Rotacja haseł	95
Ograniczenie dostępu dla pracowników	95
Stosowanie unikatowych kont użytkowników	95
Podsumowanie	96
Dalsza lektura	97

ROZDZIAŁ 4

Łańcuch niszczenia cyberzabezpieczeń	98
Łańcuch niszczenia cyberzabezpieczeń	99
Rekonesans	99
Uzbrajanie	101
Dostarczanie	102
Eksploatacja	102
Instalowanie	106
Dowodzenie i kontrola	106
Działania na celach	106
Maskowanie	108
Mechanizmy kontroli bezpieczeństwa stosowane do przerywania łańcucha niszczenia cyberzabezpieczeń	111
UEBA	113
Świadomość bezpieczeństwa	113
Zarządzanie cyklem życia zagrożeń	116
Gromadzenie danych kryminalistycznych	117
Wykrywanie	118
Kwalifikowanie	118
Dochodzenie	118
Neutralizacja	119
Odzyskiwanie sprawności	119
Obawy dotyczące łańcucha niszczenia cyberzabezpieczeń	120
Ewolucja łańcucha niszczenia	121
Narzędzia używane w łańcuchu niszczenia cyberzabezpieczeń	122
Metasploit	122
Twint	124
Nikto	124
Kismet	126
Sparta	127
John the Ripper	128
Hydra	129
Aircrack-ng	130

Airgeddon	131
Deauther Board	132
HoboCopy	133
EvilOSX	134
Platforma Dragon rozwiązania Comodo AEP	135
Podsumowanie	141
Dalsza lektura	142
Materiały źródłowe	143

ROZDZIAŁ 5

Rekonesans	145
Rekonesans zewnętrzny	146
Skanowanie mediów społecznościowych celu	146
Nurkowanie w śmietnikach	148
Inżynieria społeczna	149
Rekonesans wewnętrzny	157
Narzędzia używane do rekonesansu	158
Narzędzia do rekonesansu zewnętrznego	159
Narzędzia rekonesansu wewnętrznego	177
Airgraph-ng	177
Wardriving	187
Hak5 Plunder Bug	188
Porównanie rekonesansu pasywnego i rekonesansu aktywnego	191
Metody walki z rekonesansem	191
Metody zapobiegania rekonesansowi	192
Podsumowanie	193
Materiały źródłowe	194

ROZDZIAŁ 6

Włamywanie się do systemów	196
Analizowanie aktualnych trendów	197
Ataki z wymuszeniem	197
Ataki z manipulowaniem danymi	201
Ataki na urządzenia IoT	204
Backdoory	206
Hakowanie urządzeń codziennego użytku	208
Hakowanie chmury	209
Phishing	220
Ekspluotowanie luki w zabezpieczeniach	222
Zero-day	224

Wykonywanie kroków mających na celu złamanie zabezpieczeń systemu	232
Wdrażanie ładunków	232
Włamywanie się do systemów operacyjnych	236
Włamywanie się do systemu zdalnego	239
Włamywanie się do systemów internetowych	241
Ataki na urządzenia mobilne z systemami iOS i Android	248
Exodus	249
SensorID	251
Zhakowanie iPhone'ów przez Cellebrite	252
Man-in-the-disk	253
Spearphone (przechwytywanie danych głośnika na Androidzie)	254
Tap 'n Ghost	254
Narzędzia zespołów czerwonych i niebieskich dla urządzeń mobilnych	256
Podsumowanie	258
Dalsza lektura	260
Materiały źródłowe	260

ROZDZIAŁ 7

W pogoni za tożsamością użytkownika	263
Tożsamość to nowe granice	263
Poświadczenia i automatyzacja	266
Strategie hakowania tożsamości użytkownika	267
Uzyskanie dostępu do sieci	268
Zbieranie poświadczeń	269
Hakowanie tożsamości użytkownika	271
Brute force	271
Inżynieria społeczna	273
Pass the hash	279
Kradzież tożsamości za pośrednictwem urządzeń mobilnych	282
Inne metody hakowania tożsamości	282
Podsumowanie	283
Materiały źródłowe	283

ROZDZIAŁ 8

Ruch boczny	285
Infiltracja	286
Mapowanie sieci	286
Przeskanuj, zablokuj i napraw	289
Blokowanie i spowalnianie	291

Wykrywanie skanów Nmapa	292
Wykorzystanie sprytnych sztuczek	293
Wykonywanie ruchu bocznego	295
Etap 1. — zhakowany użytkownik (działanie użytkownika)	295
Etap 2. — dostęp administratora stacji roboczej (użytkownik = administrator)	296
Myśl jak haker	297
Unikanie alertów	298
Skanowanie portów	299
Sysinternals	300
Udziały plików	302
Windows DCOM	304
Pulpit zdalny	305
PowerShell	307
Windows Management Instrumentation	309
Zaplanowane zadania	311
Kradzież tokenów	311
Skradzione poświadczenia	312
Nośniki wymienne	313
Skażone treści udostępniane	313
Rejestr zdalny	313
TeamViewer	314
Wdrażanie aplikacji	315
Sniffing sieci	315
Spoofing ARP	315
AppleScript i IPC (OS X)	316
Analiza zhakowanego hosta	317
Centralne konsole administracyjne	317
Płądrowanie poczty elektronicznej	317
Usługa Active Directory	318
Udziały administratora	320
Pass the Ticket	320
Pass-the-Hash (PtH)	320
Winlogon	322
Proces lsass.exe	322
Podsumowanie	326
Dalsza lektura	326
Materiały źródłowe	327

ROZDZIAŁ 9

Podnoszenie poziomu uprawnień	328
Infiltracja	329
Poziome podnoszenie uprawnień	329
Pionowe podnoszenie uprawnień	331
Jak działa podnoszenie poziomu uprawnień?	331
Eksploatacja poświadczeń	332
Błędne konfiguracje	333
Luki w zabezpieczeniach i eksploity podnoszenia uprawnień	334
Inżynieria społeczna	336
Złośliwe oprogramowanie	337
Unikanie alertów	337
Podnoszenie uprawnień	339
Eksploatacja niezaktualizowanych systemów operacyjnych	341
Manipulacja tokenami dostępu	342
Eksploatacja funkcjonalności ułatwień dostępu	344
Shimming aplikacji	346
Omijanie kontroli konta użytkownika	349
Luka w zabezpieczeniach podnoszenia uprawnień i ucieczki z kontenera (CVE-20220492)	352
Wstrzyknięcie biblioteki DLL	352
Zhakowanie kolejności przeszukiwania bibliotek DLL	354
Przejęcie biblioteki dynamicznej	355
Eksploracja luk w zabezpieczeniach	355
Demon startowy	357
Praktyczny przykład podnoszenia uprawnień w docelowym systemie Windows	358
Zrzucanie pliku SAM	360
Rootowanie Androida	361
Korzystanie z pliku /etc/passwd	361
Wstrzyknięcie EWM	362
Stosowanie zaczepów	362
Zaplanowane zadania	363
Nowe usługi	364
Elementy startowe	364
Buforowanie sudo	365
Dodatkowe narzędzia do podnoszenia uprawnień	365
0xsp Mongoose v1.7	366
0xsp Mongoose RED dla systemu Windows	367
Hot Potato	367

Wnioski	368
Podsumowanie	369
Materiały źródłowe	369

ROZDZIAŁ 10

Reguły bezpieczeństwa	371
Przegląd reguł bezpieczeństwa	371
Przesunięcie w lewo	373
Edukacja użytkownika końcowego	375
Wytyczne dla użytkowników w zakresie bezpieczeństwa mediów społecznościowych	375
Szkolenie w zakresie świadomości bezpieczeństwa	377
Egzekwowanie reguł	378
Reguły w chmurze	380
Biała lista aplikacji	382
Zwiększanie zabezpieczeń	385
Monitorowanie zgodności	387
Automatyzacja	389
Ciągła poprawa stanu zabezpieczeń dzięki regułom bezpieczeństwa	390
Podsumowanie	392
Materiały źródłowe	393

ROZDZIAŁ 11

Bezpieczeństwo sieciowe	394
Obrona w głąb	394
Infrastruktura i usługi	395
Przesyłane dokumenty	397
Punkty końcowe	399
Mikrosegmentacja	399
Fizyczna segmentacja sieci	400
Wykrywanie sieci za pomocą narzędzia do mapowania	402
Zabezpieczanie zdalnego dostępu do sieci	404
VPN site-to-site	406
Segmentacja sieci wirtualnej	407
Sieć zerowego zaufania	409
Planowanie wdrożenia sieci zerowego zaufania	411
Bezpieczeństwo sieci hybrydowej w chmurze	412
Widoczność sieci w chmurze	414
Podsumowanie	418
Materiały źródłowe	418

ROZDZIAŁ 12

Aktywne czujniki	419
Funkcjonalności wykrywania	419
Wskaźniki naruszenia bezpieczeństwa	420
System wykrywania włamań	425
System zapobiegania włamaniom	428
Wykrywanie na podstawie reguł	428
Wykrywanie na podstawie anomalii	429
Analityka behawioralna w infrastrukturze lokalnej	429
Umiejscowienie urządzenia	433
Analityka behawioralna w chmurze hybrydowej	433
Microsoft Defender for Cloud	434
Analityka dla obciążeń roboczych PaaS	436
Podsumowanie	438
Materiały źródłowe	439

ROZDZIAŁ 13

Analiza zagrożeń	440
Analiza zagrożeń	440
Narzędzia do analizy zagrożeń udostępniane na licencji open source	445
Bezpłatne źródła informacji o zagrożeniach	449
MITRE ATT&CK	452
Analiza zagrożeń oferowana przez Microsoft	458
Microsoft Sentinel	458
Podsumowanie	461
Materiały źródłowe	461

ROZDZIAŁ 14

Badanie incydentu	462
Ustalanie zakresu problemu	462
Kluczowe artefakty	463
Badanie włamania do systemu lokalnego	469
Badanie włamania do systemu w chmurze hybrydowej	473
Integracja Defender for Cloud z systemem SIEM w celu przeprowadzania badań	479
Proaktywne badanie (polowanie na zagrożenia)	482
Wnioski	485
Podsumowanie	486
Materiały źródłowe	486

ROZDZIAŁ 15

Proces odzyskiwania sprawności	487
Plan odzyskiwania sprawności po katastrofie	488
Proces planowania odzyskiwania sprawności po katastrofie	489
Wyzwania	493
Odzyskiwanie sprawności bez przestojów	494
Planowanie awaryjne	495
Proces planowania awaryjnego IT	496
Narzędzia zarządzania ryzykiem	502
Plan ciągłości działania	504
Planowanie ciągłości działania	505
Jak opracować plan ciągłości działania?	506
Siedem kroków do utworzenia skutecznego planu ciągłości działania	507
Najlepsze praktyki w zakresie odzyskiwania sprawności po katastrofie	509
Najlepsze praktyki lokalne	510
Najlepsze praktyki w chmurze	510
Najlepsze praktyki w środowisku hybrydowym	511
Podsumowanie	512
Dalsza lektura	512
Materiały źródłowe	513

ROZDZIAŁ 16

Zarządzanie lukami w zabezpieczeniach	514
Tworzenie strategii zarządzania lukami w zabezpieczeniach	515
Inwentaryzacja zasobów	516
Zarządzanie informacjami	517
Ocena ryzyka	519
Ocena luk w zabezpieczeniach	524
Raportowanie i śledzenie procesu remediacji	525
Planowanie reagowania	526
Elementy strategii zarządzania lukami w zabezpieczeniach	528
Różnice między zarządzaniem lukami w zabezpieczeniach a przeprowadzaniem ich oceny	529
Najlepsze praktyki zarządzania lukami w zabezpieczeniach	530
Strategie usprawniające zarządzanie lukami w zabezpieczeniach	533
Narzędzia do zarządzania lukami w zabezpieczeniach	535
Narzędzia do inwentaryzacji zasobów	536
Narzędzia do zarządzania ryzykiem	538
Narzędzia do oceny ryzyka	541
Narzędzia do oceny luk w zabezpieczeniach	541

Narzędzia do raportowania i śledzenia remediacji	543
Narzędzia do planowania reagowania	543
Intruder	544
Patch Manager Plus	545
Windows Server Update Services (WSUS)	546
Platforma Comodo Dragon	547
InsightVM	548
Azure Threat and Vulnerability Management	548
Implementowanie zarządzania lukami w zabezpieczeniach za pomocą narzędzia Nessus	549
OpenVAS	556
Qualys	556
Acunetix	558
Wnioski	559
Podsumowanie	559
Dalsza lektura	560
Materiały źródłowe	560

ROZDZIAŁ 17

Analiza dzienników	562
Korelacja danych	562
Dzienniki systemów operacyjnych	564
Dzienniki systemu Windows	564
Dzienniki systemu Linux	566
Dzienniki firewalla	567
Dzienniki serwera WWW	569
Dzienniki platformy AWS	570
Dostęp do dzienników AWS z poziomu usługi Microsoft Sentinel	572
Dzienniki Azure Activity	574
Dostęp do dzienników Azure Activity z poziomu usługi Microsoft Sentinel	575
Dzienniki platformy GCP	577
Podsumowanie	579
Materiały źródłowe	580

Skorowidz	581
------------------------	------------