

## Spis treści

Przedmowa .....	13
Wprowadzenie .....	15
1. Zarządzanie aktywami .....	21
Fizyczne i mobilne zarządzanie aktywami .....	22
Aktywa IoT konsumenta .....	23
Aktywa programistyczne .....	24
Zarządzanie aktywami w chmurze .....	25
Środowiska wielochmurowe .....	25
Hybrydowe środowiska chmury .....	26
Oprogramowanie innych firm oraz oprogramowanie open source (OSS) .....	27
Oprogramowanie innych firm (i związane z nim ryzyko) .....	28
Uwzględnianie oprogramowania open source .....	29
Inwentaryzacja aktywów lokalnych i w chmurze .....	29
Lokalne centra danych .....	30
Oprządkowanie .....	31
Narzędzia do zarządzania aktywami .....	31
Narzędzia do sprawdzania podatności .....	32
Narzędzia do zarządzania inwentarzem w chmurze .....	32
Aktywa efemeryczne .....	33
Źródła prawdy .....	34
Ryzyko zarządzania aktywami .....	35
Log4j .....	35
Brakujące i nieuwzględnione aktywa .....	36
Nieznane niewiadome .....	36
Zarządzanie łańcuchem .....	37
Zalecenia dotyczące zarządzania aktywami .....	38
Odpowiedzialność przy zarządzaniu aktywami .....	38
Wykrywanie aktywów .....	39
Uzyskanie odpowiedniego oprządkowania .....	39

Transformacja cyfrowa .....	41
Standardowe procedury działania przy wprowadzaniu i wycofywaniu .....	41
Podsumowanie .....	42
6 Efektywne zarządzanie podatnościami na zagrożenia	
2. Zarządzanie łataniami .....	43
Podstawy zarządzania łataniami .....	43
Ręczne zarządzanie łataniami .....	44
Ryzyko ręcznego łatania .....	44
Oprzysiężenie do ręcznego łatania .....	46
Zarządzanie automatycznym łataniami .....	47
Zalety łatania automatycznego w porównaniu z ręcznym .....	48
Kombinacja łatania automatycznego i ręcznego .....	49
Ryzyko przy automatycznym łataniu .....	49
Zarządzanie łataniami w środowiskach deweloperskich .....	50
Łatanie oprogramowania open source .....	51
Niecałe oprogramowanie jest sobie równe .....	52
Wewnętrzne zarządzanie łataniami .....	52
Odpowiedzialność zespołów ds. infrastruktury i zespołów operacyjnych .....	52
Kto jest właścicielem zarządzania łataniami? .....	53
Podział obowiązków .....	54
Narzędzia i raportowanie .....	55
Łatanie przestarzałych systemów .....	55
Przestarzałe oprogramowanie .....	56
Niezałatane oprogramowanie open source .....	57
Ryzyko szczątkowe .....	58
Powszechne ataki na niezałatane systemy .....	58
Ustalanie priorytetów działań związanych z łataniami .....	59
Zarządzanie ryzykiem i łataniami .....	60
Tworzenie programu zarządzania łataniami .....	60
Ludzie .....	61

Proces .....	61
Technologia .....	62
Podsumowanie .....	62
3. Bezpieczna konfiguracja .....	63
Regulacje, ramy i prawa .....	63
Pierwsza dziesiątka wadliwych konfiguracji według NSA i CISA .....	64
Domyślna konfiguracja oprogramowania i aplikacji .....	65
Niewłaściwa separacja uprawnień użytkownika i administratora .....	65
Niedostateczny monitoring sieci wewnętrznej .....	66
Brak segmentacji sieci .....	67
Słabe zarządzanie łańcuchem .....	67
Omijanie systemu kontroli dostępu .....	69
Słabe lub źle skonfigurowane wieloskładnikowe metody uwierzytelniania .....	69
Brak MFA odpornych na phishing .....	69
Niewystarczające listy kontrolne do udziałów i usług sieciowych .....	69
Słaba higiena poświadczeń .....	70
Nieograniczone wykonywanie kodu .....	70
Ograniczanie zagrożeń .....	70
Wzorce CIS (CIS Benchmark) .....	73
Techniczne wytyczne implementacji zabezpieczeń DISA .....	74
Podsumowanie .....	75
4. Ciągłe zarządzanie podatnościami .....	76
Kontrola CIS 7 — ciągłe zarządzanie podatnościami .....	76
Ustanowienie i utrzymanie procesu zarządzania podatnościami .....	77
Ustanowienie i obsługa procesu naprawczego .....	77
Zautomatyzowane zarządzanie poprawkami systemu operacyjnego .....	78
Zautomatyzowane zarządzanie łańcuchem aplikacji .....	78
Zautomatyzowane skanowanie wewnętrznych aktywów przedsiębiorstwa pod kątem podatności na zagrożenia .....	79
Zautomatyzowane skanowanie podatności na zagrożenia	

zewnątrznych aktywów przedsiębiorstwa .....	79
Eliminowanie wykrytych podatności .....	80
Praktyki ciągłego monitorowania .....	80
Podsumowanie .....	82
5. Ocena podatności i identyfikacja oprogramowania .....	83
Powszechny system oceny podatności .....	83
CVSS 4.0 w skrócie .....	84
Miary bazowe .....	87
Miary możliwości wykorzystania .....	87
Miary zagrożenia .....	89
Miary środowiskowe .....	90
Miary dodatkowe .....	91
Jakościowa skala oceny wagi .....	93
łańcuch wektorowy .....	94
System oceny przewidywania exploitów .....	94
EPSS 3.0 — ustalanie priorytetów przez przewidywanie .....	94
EPSS 3.0 .....	96
8 Efektywne zarządzanie podatnościami na zagrożenia	
Posuwamy się do przodu .....	97
Kategoryzacja podatności na zagrożenia według interesariuszy .....	98
Przewodnik CISA po SSVC .....	100
Przykład drzewa decyzyjnego .....	106
Formaty identyfikacji oprogramowania .....	107
Schemat nazewnictwa (CPE) .....	107
Package URL .....	109
Znaczniki identyfikacyjne oprogramowania .....	110
Lista podatności (CWE) .....	111
Podsumowanie .....	113
6. Zarządzanie bazą danych podatności i exploitów .....	114
Baza danych podatności NVD .....	114
Indeks Sonatype oprogramowania open source .....	116

Podatności oprogramowania open source .....	117
Baza danych zaleceń GitHub .....	118
Bazy danych exploitów .....	119
Exploit-DB .....	119
Metasploit .....	120
GitHub .....	120
Podsumowanie .....	120
7. Łączenie podatności w łańcuch .....	121
Ataki z użyciem łańcucha podatności .....	121
łańcuchy exploitów .....	123
łańcuchy podatności .....	123
łańcuchy podatności publikowane przez sprzedawców .....	124
łączenie i ocena podatności .....	126
CVSS .....	126
EPSS .....	127
Luki w branży .....	127
Niedostrzeżenie łączenia podatności .....	129
Terminologia .....	129
Wykorzystanie w programach zarządzania podatnościami .....	130
Ludzki aspekt łączenia podatności na zagrożenia .....	132
Phishing .....	132
Naruszenie biznesowej poczty e-mail .....	133
Inżynieria społeczna .....	133
Integracja z VMP .....	134
Zasady przywództwa .....	135
Integracja z praktykiem ds. bezpieczeństwa .....	135
Wykorzystanie IT i rozwoju .....	136
Podsumowanie .....	136
8. Analiza zagrożeń związanych z podatnościami .....	137
Dlaczego analiza zagrożeń jest ważna dla programu zarządzania podatnościami (VMP)? .....	137

Od czego zacząć? .....	138
Techniczne informacje o zagrożeniach .....	138
Taktyczna analiza zagrożeń .....	139
Strategiczna analiza zagrożeń .....	139
Operacyjna analiza zagrożeń .....	140
Polowanie na zagrożenia .....	141
Integracja analizy zagrożeń z systemami VMP .....	142
Ludzie .....	142
Proces .....	143
Technologia .....	144
Podsumowanie .....	144
9. Chmura, DevSecOps i bezpieczeństwo łańcucha dostaw .....	145
Modele usług chmurowych i współdzielona odpowiedzialność .....	145
Środowiska hybrydowe i wielochmurowe .....	147
Kontenery .....	148
Kubernetes .....	153
Przetwarzanie bezserwerowe .....	156
DevSecOps .....	157
Oprogramowanie open source .....	160
Oprogramowanie jako usługa .....	166
Ryzyko systemowe .....	167
Podsumowanie .....	170
10. Czynniki ludzkie w zarządzaniu podatnościami .....	171
Inżynieria czynników ludzkich .....	172
Inżynieria bezpieczeństwa czynników ludzkich .....	174
Przełączanie kontekstu .....	174
Pulpity podatności .....	176
Raporty o podatności .....	177
10 Efektywne zarządzanie podatnościami na zagrożenia	
Poznanie i metapoznanie .....	178
Poznanie podatności .....	179

Sztuka podejmowania decyzji .....	179
Zmęczenie decyzyjne .....	180
Zmęczenie alertami .....	180
Liczba ujawnionych podatności .....	181
Wymagane poprawki i konfiguracje .....	181
Zmęczenie zarządzaniem podatnościami .....	183
Psychiczne obciążenie pracą .....	183
Integracja czynnika ludzkiego z VMP .....	184
Zacznij od małych kroków .....	184
Rozważenie skorzystania z pomocy konsultanta .....	185
Podsumowanie .....	186
11. Secure-by-design, czyli oprogramowanie bezpieczne	
już na etapie projektu .....	187
Bezpieczne już na etapie projektu/domyślnie .....	188
Bezpieczne już na etapie projektu .....	189
Domyślnie bezpieczne .....	190
Zasady bezpieczeństwa oprogramowania .....	190
Zasada 1. Przejęcie odpowiedzialności za wyniki w zakresie	
bezpieczeństwa klientów .....	190
Zasada 2. Przyjęcie radykalnej przejrzystości i odpowiedzialności .....	193
Zasada 3. Kierowanie od góry .....	194
Taktyka bezpieczeństwa już na etapie od projektu .....	195
Taktyka domyślnego bezpieczeństwa .....	196
Przewodniki utwardzania kontra luzowania .....	197
Zalecenia dla klientów .....	197
Modelowanie zagrożeń .....	198
Tworzenie bezpiecznego oprogramowania .....	199
Szczegóły SSDF .....	200
Bezpieczeństwo, inżynieria chaosu i odporność .....	206
Podsumowanie .....	207
12. Model dojrzałości zarządzania podatnościami .....	208

Krok 1. Zarządzanie aktywami .....	209
Krok 2. Bezpieczna konfiguracja .....	210
Krok 3. Ciągłe monitorowanie .....	212
Krok 4. Zautomatyzowane zarządzanie podatnościami .....	214
Krok 5. Integracja czynników ludzkich .....	215
Krok 6. Analiza podatności na zagrożenia .....	216
Podsumowanie .....	217
Podziękowania .....	219
O autorach .....	221
O korektorze merytorycznym .....	223