

SZCZEGÓŁOWY SPIS TREŚCI

PRZEDMOWA	xv
PODZIĘKOWANIA	xix
WSTĘP	xxi
○ książce	xxii
Uwagi na temat ćwiczeń umysłowych dotyczących doktryny zamku	xxiii
Przyszłe zastosowania	xxiv
Podstawy ninja	xxiv
Historyczny ninja	xxv
Zwoje ninja	xxv
Filozofia ninja	xxvi
Serce z Żelaznego Ostrza/pod Żelaznym Ostrzem	xxvii
Właściwy umysł	xxvii
Techniki ninja	xxviii
1	
MAPOWANIE SIECI	1
Czym są mapy sieci	2
Zbieranie danych wywiadowczych bez wykrycia	8
Tworzenie własnych map	10
Zalecane zabezpieczenia i środki mitygujące	14
Podsumowanie	14
2	
SZCZEGÓLNIIE STARANNY NADZÓR	15
Czym są wektory ataku	16
Koncepcja nadzoru	17
Nadzór a wytyczne NIST Cybersecurity Framework	17
Modelowanie zagrożeń	19
Wykorzystanie modelowania zagrożeń do znalezienia potencjalnych wektorów ataku	21
Zalecane zabezpieczenia i środki mitygujące	24
Podsumowanie	24

3		
BEZPIECZEŃSTWO KSENOFOBICZNE	25	
Czym jest antyuprzywilejowanie	26	
Problem z interoperacyjnością i uniwersalnymi standardami	28	
Opracowywanie unikatowych cech dla twojego środowiska	29	
Zalecane zabezpieczenia i środki mitygujące	31	
Podsumowanie	31	
4		
WYZWANIE IDENTYFIKACJI	33	
Czym jest uwierzytelnianie	35	
Uwierzytelnianie na zasadzie dopasowanych par	37	
Zalecane zabezpieczenia i środki mitygujące	39	
Podsumowanie	40	
5		
PODWÓJNIE ZAPIECZĘTOWANE HASŁO	41	
Ukryte uwierzytelnianie dwuetapowe	43	
Opracowywanie podwójnie zabezpieczonych haseł	44	
Zalecane zabezpieczenia i środki mitygujące	46	
Podsumowanie	47	
6		
GODZINY INFILTRACJI	49	
Czym jest czas i możliwości	50	
Opracowywanie zasad bezpieczeństwa oraz detektorów zdarzeń nietypowych bazujących na czasie	52	
Zalecane zabezpieczenia i środki mitygujące	54	
Podsumowanie	55	
7		
DOSTĘP DO CZASU	57	
Znaczenie czasu	59	
Utrzymanie czasu w tajemnicy	60	
Określenie własnej linii bazowej	60	
Ocena możliwości technicznych	61	
Ustalenie zasad	61	
Zalecane zabezpieczenia i środki mitygujące	61	
Podsumowanie	62	
8		
NARZĘDZIA	63	
Życie z zasobów naturalnych	65	
Zabezpieczanie narzędzi	66	
Zalecane zabezpieczenia i środki mitygujące	68	
Podsumowanie	69	

9	
CZUJNIKI	71
Identyfikowanie i wykrywanie zagrożeń za pomocą czujników	72
Lepsze czujniki	73
Zalecane zabezpieczenia i środki mitygujące	76
Podsumowanie	77
10	
MOSTY I DRABINY	79
Mosty nad granicami sieci	80
Przeciwdziałanie tworzeniu mostów	82
Zalecane zabezpieczenia i środki mitygujące	83
Podsumowanie	84
11	
ZAMKI	85
Zabezpieczenia fizyczne	87
Ulepszanie zamków	88
Zalecane zabezpieczenia i środki mitygujące	90
Podsumowanie	90
12	
KSIĘŻYC NA WODZIE	91
Socjotechnika	92
Obrona przed socjotechniką	95
Zalecane zabezpieczenia i środki mitygujące	96
Podsumowanie	97
13	
SZPIEG-ROBAK	99
Zagrożenia wewnętrzne	101
Nowe podejście do zagrożeń wewnętrznych	102
Zalecane zabezpieczenia i środki mitygujące	105
Podsumowanie	106
14	
DUCH NA KSIĘŻYCU	107
Implanty	108
Ochrona przed implantami	109
Zalecane zabezpieczenia i środki mitygujące	111
Podsumowanie	112
15	
SZTUKA ŚWIETLIKÓW	115
Atrybucja	117
Podejścia do obsługi atrybucji	118

Zalecane zabezpieczenia i środki mitygujące	120
Podsumowanie	121

16

SCHWYTANIE ŻYWCEM 123

Analiza w czasie rzeczywistym	126
Konfrontacja z żywym zagrożeniem	128
Zalecane zabezpieczenia i środki mitygujące	130
Podsumowanie	131

17

ATAK OGNIEM 133

Destrukcyjne ataki cybernetyczne	135
Zabezpieczenia przed (cyber)atakami ogniem	137
Zalecane zabezpieczenia i środki mitygujące	139
Podsumowanie	141

18

POTAJEMNA KOMUNIKACJA 143

Komunikacja dowodzenia i kontroli	145
Kontrolowanie połączeń komunikacyjnych	147
Zalecane zabezpieczenia i środki mitygujące	148
Podsumowanie	150

19

ZNAKI WYWOŁAWCZE 151

Rzemiosło operatora	152
Wykrywanie obecności znaków wywoławczych	154
Zalecane zabezpieczenia i środki mitygujące	155
Podsumowanie	155

20

DYSCYPLINA ŚWIATŁA, HAŁASU I ŚMIECI 157

Światło, hałas i śmieci w świecie cyfrowym	159
Dyscyplina wykrywania	161
Zalecane zabezpieczenia i środki mitygujące	162
Podsumowanie	163

21

OKOLICZNOŚCI INFILTRACJI 165

Okazje przeciwnika	167
Przeciwstawianie się przeciwnościom	168
Zalecane zabezpieczenia i środki mitygujące	169
Podsumowanie	169

22	
ZERO-DAY	171
Zero-day	174
Obrona przed zagrożeniami zero-day	175
Zalecane zabezpieczenia i środki mitygujące	179
Podsumowanie	180
23	
ZATRUDNIANIE SHINOBI	183
Talent w dziedzinie cyberbezpieczeństwa	185
Zarządzanie talentami	187
Zalecane zabezpieczenia i środki mitygujące	190
Podsumowanie	191
24	
FUNKCJONOWANIE WARTOWNI	193
Problemy i oczekiwania dotyczące centrum operacji bezpieczeństwa SOC	195
Oddziaływanie na zachowanie	197
Zalecane zabezpieczenia i środki mitygujące	200
Podsumowanie	201
25	
ZARZĄDZANIE ZAGROŻENIAMI NA ZASADZIE ZEROWEGO ZAUFANIA	203
Możliwości czynników zagrażających	204
Blokowanie tego, co podejrzane	206
Zalecane zabezpieczenia i środki mitygujące	208
Podsumowanie	209
26	
RZEMIOSŁO SHINOBI	211
Techniki, taktyki i procedury	214
Piramida Bólu	215
Framework ATT&CK	216
Szpiegowanie zagrożeń	218
Szpiegowanie cyberzagrożeń	219
Zalecane zabezpieczenia i środki mitygujące	221
Podsumowanie	222
PRZYPISY KOŃCOWE	223