Spis treści

O autorach ... 11

O recenzentach ... 12

Przedmowa ... 13

CZĘŚĆ 1. Stworzenie zespołu niebieskiego

ROZDZIAŁ 1

Tworzenie strategii obrony ... 19

Sposób, w jaki organizacje odnoszą korzyści z utworzenia zespołu niebieskiego ... 20

Ocena ryzyka ... 20

Monitorowanie i nadzorowanie ... 20

Kontrola bezpieczeństwa ... 21

Raportowanie i rekomendacje dla kierownictwa ... 21

Skład zespołu niebieskiego ... 22

Analityk ... 22

Cyberratownik ... 22

Łowca zagrożeń ... 23

Konsultant do spraw bezpieczeństwa ... 24

Administrator bezpieczeństwa ... 24

Administrator zarządzania tożsamością i dostępem ... 24

Analityk zgodności ... 24

Zespół czerwony ... 25

Zespół fioletowy ... 26

Zbieranie danych o cyberzagrożeniach ... 27

Umiejętności wymagane do pracy w zespole niebieskim ... 27

Chęć do nauki i zorientowanie na szczegóły ... 28

Dogłębna znajomość sieci i systemów ... 28

Nieszablonowe i innowacyjne myślenie ... 28

Umiejętność przekraczania barier w wykonywaniu zadań ... 28

Wykształcenie, kwalifikacje i certyfikaty ... 29

Rozwój i utrzymanie talentów ... 29
Laboratoria cybernetyczne ... 29
Capture-the-Flag i hackathony ... 30
Projekty badawczo-rozwojowe ... 30
Zasięg społeczności ... 30
Mentoring ... 30
Ciągła, nieograniczana nauka ... 31
Podsumowanie ... 31

ROZDZIAŁ 2
Zarządzanie zespołem bezpieczeństwa obronnego ... 32
Dlaczego organizacje powinny rozważyć pomiary poziomu cyberbezpieczeństwa ... 32
Kluczowe wskaźniki bezpieczeństwa zespołu niebieskiego ... 33
W jaki sposób zespół niebieski wybiera KRI dla swojej firmy ... 34
Wybór kluczowych wskaźników w zakresie cyberbezpieczeństwa ... 36
W jakim celu i w jaki sposób organizacje mogą zautomatyzować ten proces ... 40
Jakich pułapek należy unikać podczas automatyzacji przepływów pracy zespołu niebieskiego ... 40
Automatyzacja zbierania i prezentowania KRI ... 41
Podsumowanie ... 42

ROZDZIAŁ 3
Ocena ryzyka ... 43
Metodologia NIST ... 43
Metodologia oceny ryzyka NIST ... 45
Inwentarze zasobów ... 46
Metody zarządzania ryzykiem ... 49
Identyfikacja zagrożeń ... 49
Obliczanie ryzyka ... 51
Obowiązki w zakresie zarządzania ryzykiem ... 53
Podsumowanie ... 55
Bibliografia ... 55

ROZDZIAŁ 4
Działania zespołu niebieskiego ... 57
Zrozumienie strategii obrony ... 57
Działania zespołu niebieskiego — infrastruktura ... 59
Działania zespołu niebieskiego — aplikacje ... 60
Działania zespołu niebieskiego — systemy ... 62
Działania zespołu niebieskiego — punkty końcowe ... 63

Działania zespołu niebieskiego — chmura ... 65
Planowanie obrony przed osobami z organizacji ... 68
Zakres odpowiedzialności zespołów niebieskich ... 71
Podsumowanie ... 72

ROZDZIAŁ 5
Zagrożenia ... 73
Czym są cyberzagrożenia ... 73
Cyber Kill Chain ... 75
Faza 1. Rekonesans ... 76
Faza 2. Zbrojenie ... 78
Faza 3. Dostarczanie ... 81
Faza 4. Eksploitacja ... 81
Faza 5. Instalowanie ... 82
Faza 6. Dowodzenie i kontrola ... 82
Faza 7. Działanie ... 83
Ataki wewnętrzne ... 89
Różne rodzaje napastników ... 91
Skutki cyberprzestępczości ... 92
Proaktywne, a nie reaktywne podejście do bezpieczeństwa ... 93
Podsumowanie ... 94

ROZDZIAŁ 6
Ład korporacyjny, zgodność, regulacje i dobre praktyki ... 95
Określenie interesariuszy i ich potrzeb ... 95
Konstruowanie wskaźników ryzyka ... 97
Potrzeba zgodności i identyfikacja wymagań zgodności ... 99
Zapewnienie zgodności legislacyjnej i odpowiedniego poziomu ładu korporacyjnego ... 103
Podsumowanie ... 105

CZĘŚĆ 2. Działania na polu walki

ROZDZIAŁ 7
Środki prewencyjne ... 113
Czym są środki prewencyjne ... 113
Korzyści ... 113
Rodzaje środków prewencyjnych ... 114
Środki administracyjne ... 114
Środki fizyczne ... 115
Środki techniczne/logiczne ... 115

Warstwy środków prewencyjnych ... 116
Kontrola polityk ... 116
Bezpieczeństwo na styku i środki fizyczne ... 118
Kontrola sieci ... 119
Środki do ochrony bezpieczeństwa danych ... 121
Środki bezpieczeństwa w odniesieniu do aplikacji ... 121
Środki bezpieczeństwa dla punktów końcowych ... 123
Zabezpieczanie użytkownika ... 124
Podsumowanie ... 125

ROZDZIAŁ 8
Środki wywiadowcze ... 126
Czym są środki wywiadowcze ... 126
Rodzaje środków wywiadowczych ... 127
SOC ... 128
Jak działa SOC ... 128
Jakie są korzyści z SOC ... 129
Testowanie pod kątem występowania podatności ... 130
Testy penetracyjne ... 132
Zespoły czerwone ... 132
Bug bounty ... 133
Skanowanie kodu źródłowego ... 133
Skanowanie pod kątem zgodności lub w celu „utwardzenia" ... 134
Narzędzia do środków wywiadowczych ... 135
Platforma analizy zagrożeń ... 135
Narzędzia do orkiestracji, automatyzacji i reagowania na zagrożenia ... 136
Narzędzia do zarządzania informacjami i zdarzeniami dotyczącymi bezpieczeństwa ... 136
Informatyka śledcza ... 137
Podsumowanie ... 138

ROZDZIAŁ 9
Przeprowadzanie dochodzenia w przypadku cyberzagrożeń ... 139
Czym jest CTI ... 139
Jakość CTI ... 140
Rodzaje informacji o zagrożeniach ... 141
Strategiczne informacje o zagrożeniach ... 141
Taktyczne informacje o zagrożeniach ... 142
Informacje operacyjne o zagrożeniach ... 143

Korzystanie z analityki wywiadowczej ... 144
1. Opracowanie planu ... 144
2. Zbieranie informacji ... 144
3. Przetwarzanie ... 145
4. Analiza ... 145
5. Rozpowszechnianie ... 146
6. Informacje zwrotne ... 146
Polowanie na zagrożenia ... 146
Znaczenie polowania na zagrożenia ... 146
Efektywne wykorzystanie CTI ... 148
Framework MITRE ATT&CK ... 149
Macierz MITRE ATT&CK ... 150
Jak wykorzystać schemat ATT&CK ... 151
Podsumowanie ... 152

ROZDZIAŁ 10
Reagowanie na incydenty i odzyskiwanie po awarii ... 153
Planowanie reagowania na incydenty ... 153
Testowanie planów reagowania na incydenty ... 155
Podręczniki reagowania na incydenty ... 158
Podręcznik ataku ransomware ... 158
Podręcznik ataków związanych z utratą/kradzieżą danych ... 163
Podręcznik ataków phishingowych ... 168
Planowanie odzyskiwania po awarii ... 172
Ubezpieczenie cybernetyczne ... 177
Podsumowanie ... 180

ROZDZIAŁ 11
Ustalanie priorytetów i wdrażanie strategii zespołu niebieskiego ... 181
Pojawiające się technologie i techniki wykrywania włamań oraz zapobiegania im ... 181
Symulowanie działań przeciwnika ... 182
Usługi VCISO ... 182
Bezpieczeństwo zależne od kontekstu ... 183
Defensywna sztuczna inteligencja ... 183
Extended Detection and Response ... 184
Opis użytkowania zgodnie z zaleceniami producenta ... 184
Zerowe zaufanie ... 185
Pułapki, których należy unikać podczas powoływania zespołu niebieskiego ... 187
Rozpoczęcie przygody z zespołem niebieskim ... 188
Podsumowanie ... 189

CZĘŚĆ 3. Zapytaj ekspertów

ROZDZIAŁ 12
Spostrzeżenia ekspertów 193
Antoni Desvernois 193
William B. Nelson 194
Laurent Gerardin 196
Peter Sheppard 197
Pieter Danhieux 199