

Wprowadzenie	9
1. Zagrożenia związane z kontenerami	15
Ryzyko, zagrożenie i środki ostrożności	16
Model zagrożenia kontenera	16
Granice bezpieczeństwa	20
Wielodostępność	21
Maszyny współdzielone	21
Wirtualizacja	22
Wielodostępność w przypadku kontenerów	23
Egzemplarze kontenera	24
Zasady dotyczące zapewnienia bezpieczeństwa	24
Najmniejsze możliwe uprawnienia	24
Głęboka defensywa	24
Ograniczenie płaszczyzny ataku	25
Ograniczenie pola rażenia	25
Podział zadań	25
Stosowanie zasad bezpieczeństwa w kontenerach	25
Podsumowanie	26
2. Wywołania systemu Linux, uprawnienia i właściwości jądra	27
Wywołania systemowe	27
Uprawnienia plików	28
setuid i setgid	30
Mechanizm właściwości jądra systemu Linux	33
Podniesienie uprawnień	35
Podsumowanie	36

3. Grupy kontrolne	37
Hierarchia grup kontrolnych	37
Tworzenie grup kontrolnych	38
Definiowanie ograniczeń dla zasobów	40
Przypisanie procesu do grupy kontrolnej	41
Używanie grup kontrolnych z Dockerem	42
Grupy kontrolne — wersja druga	43
Podsumowanie	44
 4. Izolacja kontenera	 45
Przestrzenie nazw systemu Linux	46
Izolacja nazwy hosta	47
Izolowanie identyfikatorów procesów	49
Zmiana katalogu głównego	52
Połączenie przestrzeni nazw i zmiany katalogu głównego	55
Przestrzeń nazw punktów montowania	55
Przestrzeń nazw sieci	57
Przestrzeń nazw użytkownika	59
Ograniczenia przestrzeni nazw użytkownika w Dockerze	61
Przestrzeń nazw IPC	62
Przestrzeń nazw grup kontrolnych	63
Proces kontenera z perspektywy systemu komputera gospodarza	64
Maszyny gospodarza kontenera	65
Podsumowanie	67
 5. Maszyna wirtualna	 69
Uruchomienie komputera	69
Poznaj VMM	70
Typ 1. VMM — hipernadzorca	71
Typ 2. VMM	72
Maszyny wirtualne oparte na jądrze	73
Przechwycić i emulować	73
Obsługa instrukcji niewirtualizowanych	74
Izolacja procesu i zapewnienie bezpieczeństwa	75
Wady maszyny wirtualnej	76
Izolacja kontenera w porównaniu do izolacji maszyny wirtualnej	77
Podsumowanie	77

6. Obrazy kontenera	79
Główny system plików i konfiguracja obrazu	79
Nadpisanie konfiguracji w trakcie działania obrazu	80
Standardy OCI	80
Konfiguracja obrazu	81
Tworzenie obrazu	82
Niebezpieczeństwa związane z poleceniem docker build	82
Tworzenie obrazu kontenera bez użycia demona	83
Warstwy obrazu	84
Przechowywanie obrazów kontenera	86
Identyfikowanie obrazów kontenera	86
Zapewnienie bezpieczeństwa obrazowi kontenera	88
Zapewnienie bezpieczeństwa podczas tworzenia obrazu	89
Pochodzenie pliku Dockerfile	89
Najlepsze praktyki związane z zapewnieniem bezpieczeństwa pliku Dockerfile	89
Ataki na komputer, w którym są tworzone obrazy	92
Zapewnienie bezpieczeństwa podczas przechowywania obrazów	92
Utworzenie własnego rejestru obrazów	92
Podpisywanie obrazów	93
Zapewnienie bezpieczeństwa podczas wdrażania obrazów	93
Wdrożenie właściwego obrazu	93
Definicja wdrożenia zawierającego kod o złośliwym działaniu	94
Sterowanie dopuszczeniem	94
GitOps i zapewnienie bezpieczeństwa podczas wdrożenia	95
Podsumowanie	96
 7. Luki w zabezpieczeniach oprogramowania umieszczonego w obrazie kontenera	 97
Szukanie luk w zabezpieczeniach	97
Luki w zabezpieczeniach, poprawki bezpieczeństwa i dystrybucje	98
Luki w zabezpieczeniach na poziomie aplikacji	99
Zarządzanie ryzykiem związanym z lukami w zabezpieczeniach	99
Skanowanie pod kątem luk w zabezpieczeniach	100
Zainstalowane pakiety	100
Skanowanie obrazu kontenera	101
Kontenery niemodyfikowalne	101
Regularne skanowanie	102
Narzędzia skanowania	103
Źródła informacji	103
Nieaktualne źródła danych	104
Luki w zabezpieczeniach, które nie zostaną usunięte	104

Luki w zabezpieczeniach podpakietów	104
Różne nazwy pakietu	104
Dodatkowe funkcje skanowania	105
Błędy narzędzi skanowania	105
Skanowanie w trakcie procesu ciągłej integracji i ciągłego wdrożenia	105
Uniemożliwianie uruchamiania obrazów zawierających luki w zabezpieczeniach	108
Luki w zabezpieczeniach dnia zerowego	108
Podsumowanie	109
8. Wzmocnienie izolacji kontenera	111
seccomp	111
AppArmor	113
SELinux	114
gVisor	116
Kontener Kata	118
Firecracker	119
Unijądro	119
Podsumowanie	120
9. Złamanie izolacji kontenera	121
Kontener domyślnie działa z uprawnieniami użytkownika root	121
Nadpisanie identyfikatora użytkownika	122
Wymaganie uprawnień użytkownika root wewnątrz kontenera	123
Kontener niewymagający uprawnień użytkownika root	125
Właściwości jądra systemu Linux i opcja --privileged	128
Montowanie zawierających dane wrażliwe katalogów systemu gospodarza	130
Montowanie gniazda Dockera	131
Współdzielenie przestrzeni nazw między kontenerem i gospodarzem	131
Kontener przyczepy	132
Podsumowanie	133
10. Zapewnienie bezpieczeństwa sieci kontenera	135
Zapora sieciowa kontenera	135
Model OSI	137
Wysyłanie pakietu IP	138
Adres IP kontenera	139
Izolacja sieci	140
Reguły i routing na warstwach 3. i 4.	141
iptables	141
IPVS	143

Polityki sieciowe	143
Rozwiązania w zakresie polityki sieciowej	145
Najlepsze praktyki związane z polityką siecią	146
Architektura Service Mesh	147
Podsumowanie	148
11. Bezpieczna komunikacja między komponentami przy użyciu TLS	149
Bezpieczne połączenie	149
Certyfikat X.509	150
Para kluczy publicznego i prywatnego	151
Urząd certyfikacji	152
Żądanie podpisania certyfikatu	153
Połączenie TLS	154
Bezpieczne połączenia między kontenerami	155
Unieważnienie certyfikatu	156
Podsumowanie	157
12. Przekazywanie danych poufnych do kontenera	159
Właściwości danych poufnych	159
Przekazywanie informacji do kontenera	160
Przechowywanie danych poufnych w obrazie kontenera	161
Przekazywanie danych poufnych przez sieć	161
Przekazywanie danych poufnych w zmiennych środowiskowych	162
Przekazywanie danych poufnych za pomocą plików	163
Dane poufne w Kubernetes	163
Dane poufne są dostępne dla użytkownika root	164
Podsumowanie	165
13. Zabezpieczanie środowiska uruchomieniowego kontenera	167
Profile obrazów kontenera	167
Profile ruchu sieciowego	168
Profile plików wykonywalnych	168
Profile dostępu do plików	170
Profile identyfikatorów użytkowników	170
Inne profile używane w środowisku uruchomieniowym	171
Narzędzia zapewnienia bezpieczeństwa kontenera	171
Unikanie różnic	173
Podsumowanie	174

14. Kontenery i przygotowana przez OWASP lista Top 10	175
Wstrzyknięcie kodu	175
Złamanie mechanizmu uwierzytelnienia	175
Ujawnienie danych wrażliwych	176
Zewnętrzne encje XML	176
Nieprawidłowa kontrola dostępu	176
Błędna konfiguracja zabezpieczeń	177
XSS	177
Niebezpieczna deserializacja	178
Używanie komponentów zawierających znane luki w zabezpieczeniach	178
Niewystarczający poziom rejestrowania danych i monitorowania	178
Podsumowanie	179
Zakończenie	181
Dodatek A. Lista rzeczy do sprawdzenia w zakresie zapewnienia bezpieczeństwa	182