

Spis treści

O autorze	13
O recenzentach	14
Podziękowania	15
Wprowadzenie	17
Rozdział 1. Pierwsze kroki z DevOps	19
Struktura	19
Cele	20
Czym jest DevOps?	20
Obszary metodyki DevOps	25
Zarządzanie i planowanie	26
Tworzenie i kompilowanie kodu	26
Ciągła integracja i testy	27
Automatyczne wdrażanie	27
Zapewnianie poprawnego działania oprogramowania w środowisku produkcyjnym	28
Monitorowanie	28
Ciągła integracja i ciągłe dostarczanie oprogramowania	28
Kanał dostarczania oprogramowania	30
Narzędzia DevOps	32
Automatyzacja za pomocą narzędzi Jenkins i Drone	38
Zarządzanie infrastrukturą i konfiguracją	39
Narzędzia monitorujące	40
Pakiet ELK	41
Kontenery i orkiestracja	42
DevOps a bezpieczeństwo	42
Wprowadzenie do DevSecOps	43
Podsumowanie	45
Rozdział 2. Platformy kontenerowe	47
Struktura	47
Cele	48

Kontenery Dockera	48
Czym jest Docker?	48
Nowe funkcjonalności platformy Docker i zarządzanie kontenerami	49
Architektura platformy Docker	50
Silnik	50
Rejestr	52
Klient	52
Testowanie platformy Docker w chmurze	54
Orkiestracja kontenera	56
Docker Compose	56
Kubernetes	57
Instalacja platformy Kubernetes i kluczowe pojęcia	58
Docker Swarm	61
Swarm w praktyce	63
Platforma OpenShift	66
Platforma OpenShift jako usługa	66
Metodyka DevOps z platformą OpenShift	66
Najważniejsze elementy platformy OpenShift	69
Scenariusze szkoleniowe	72
Podsumowanie	72
Rozdział 3. Zarządzanie kontenerami i obrazami Dockera	75
Struktura	76
Cele	76
Zarządzanie obrazami Dockera	76
Wprowadzenie do obrazów Dockera	76
Warstwy obrazu	77
Etykiety obrazu	78
Projektowanie obrazów kontenerów	80
Polecenia Dockerfile	80
Czym jest plik Dockerfile?	81
Tworzenie obrazu za pomocą pliku Dockerfile	81
Dobre praktyki tworzenia pliku Dockerfile	85
Zarządzanie kontenerami	86
Wyszukiwanie i uruchamianie obrazu	86
Uruchomienie kontenera w tle systemu	88
Badanie kontenera	88

Optymalizacja obrazów	91
Pamięć podręczna platformy Docker	92
Optymalizacja kompilacji obrazu	94
Tworzenie aplikacji dla środowiska Node.js	94
Zmniejszanie obrazu	96
Zmniejszanie obrazów za pomocą obrazu Alpine Linux	97
Okrojone obrazy	98
Podsumowanie	101
Rozdział 4. Wprowadzenie do bezpieczeństwa platformy Docker ...	103
Struktura	104
Cele	104
Zasady bezpieczeństwa platformy Docker	104
Podatność głównego procesu platformy Docker na ataki	106
Dobre praktyki bezpieczeństwa	107
Uruchamianie kontenera jako nie-administratora	108
Uruchamianie kontenera w trybie tylko do odczytu	110
Blokowanie uprawnień SETUID i SETGID	111
Weryfikowanie wiarygodności obrazów	112
Ograniczanie wykorzystania zasobów	112
Kompetencje kontenera	113
Wyświetlenie wszystkich kompetencji	115
Nadawanie i odbieranie kompetencji	116
Blokowanie polecenia ping w kontenerze	118
Nadawanie kompetencji do zarządzania siecią	120
Uruchamianie uprzywilejowanych kontenerów	121
Wiarygodność kontenerów	123
Podpisywanie obrazów	124
Bezpieczne pobieranie obrazów z wykorzystaniem pliku Dockerfile	126
Narzędzie notary do zarządzania obrazami	126
Rejestr Dockera	127
Czym jest rejestr?	127
Rejestr Dockera w serwisie Docker Hub	127
Tworzenie lokalnego rejestru	128
Podsumowanie	131
Pytania	131

Rozdział 5. Bezpieczeństwo hosta platformy Docker	133
Struktura	134
Cele	134
Bezpieczeństwo procesu platformy Docker	134
Audyt plików i katalogów	137
Bezpieczeństwo jądra systemu Linux i moduł SELinux	138
Profile AppArmor i Seccomp	139
Instalacja modułu AppArmor w systemie Ubuntu	140
Moduł AppArmor w praktyce	142
Domyślny profil AppArmorDocker	142
Uruchamianie kontenera bez profilu AppArmor	143
Uruchamianie kontenera z profilem Seccomp	144
Zmniejszanie podatności kontenera na ataki	145
Testowanie bezpieczeństwa platformy Docker	146
Przykłady użycia narzędzia Docker Bench for Security	149
Kod źródłowy narzędzia Docker Bench for Security	152
Audyt hosta platformy Docker za pomocą narzędzi Lynis i dockscan	155
Audyt pliku Dockerfile	156
Narzędzie dockscan skanujące luki w bezpieczeństwie i sprawdzające podatność platformy Docker na ataki	161
Podsumowanie	163
Pytania	163
Rozdział 6. Bezpieczeństwo obrazów Dockera	165
Struktura	166
Cele	166
Repozytorium Docker Hub	166
Skanowanie bezpieczeństwa obrazów Dockera	166
Proces skanowania obrazów Dockera	167
Otwarte narzędzia do analizy zagrożeń	169
Ciągła integracja oprogramowania na platformie Docker	169
CoreOS Clair	171
Dagda — pakiet testów bezpieczeństwa	171
OWASP Dependency-Check	175
MicroScanner	179
Skaner Clair i repozytorium Quay.io	180
Repozytorium GitHub i odnośniki do narzędzia Clair	187

Repozytorium obrazów Quay.io	188
Rejestracja w repozytorium Quay.io	189
Analiza obrazów Dockera za pomocą silnika i interfejsu CLI	
narzędzia Anchore	193
Uruchomienie silnika Anchore	195
Podsumowanie	200
Pytania	200

Rozdział 7. Audyt i analiza podatności kontenerów Dockera

na ataki	201
Struktura	202
Cele	202
Zagrożenia i ataki na kontenery	202
Zagrożenie Dirty COW (CVE-2016-5195)	207
Zapobieganie zagrożeniu Dirty COW	
przy użyciu mechanizmu AppArmor	210
Zagrożenie jack in the box (CVE-2018-8115)	210
Najbardziej zagrożone pakiety	211
Analiza zagrożeń obrazów Dockera	212
Klasyfikacja zagrożeń	213
Zagrożenia obrazu Alpine	215
Zagrożenia platformy Docker	217
Zagrożone obrazy w serwisie Docker Hub	219
Uzyskiwanie szczegółowych informacji o zagrożeniach CVE	
za pomocą interfejsu vulners API	220
Podsumowanie	222
Pytania	222

Rozdział 8. Bezpieczeństwo platformy Kubernetes

Struktura	224
Cele	224
Wprowadzenie do bezpieczeństwa platformy Kubernetes	224
Zabezpieczanie kontenerów na platformie Kubernetes	224
Konfigurowanie platformy Kubernetes	225
Dobre praktyki bezpieczeństwa na platformie Kubernetes	226
Zarządzanie poufnymi informacjami	230
Bezpieczeństwo silnika platformy Kubernetes	231

Kontrola bezpieczeństwa platformy Kubernetes	231
Zwiększanie bezpieczeństwa kontenerów na platformie Kubernetes	232
Narzędzie Kube Bench i zagrożenia	234
Zalecenia CIS Benchmark dla platformy Kubernetes	234
Weryfikacja węzłów roboczych	235
Weryfikacja węzła głównego	235
Zagrożenia platformy Kubernetes	236
Projekty zabezpieczeń platformy Kubernetes	238
kube-hunter	238
kubesecc	238
Wtyczki do zarządzania klastrem Kubernetesa	239
Podsumowanie	242
Pytania	242
Rozdział 9. Sieć kontenerów Dockera	245
Struktura	245
Cele	246
Typy sieci kontenerów	246
Typy sieci na platformie Docker	246
Tryb mostu	248
Tryb hosta	253
Zarządzanie siecią na platformie Docker	255
Sieć na platformie Docker	255
Komunikacja między kontenerami i wiązanie portów	258
Wiązanie portów kontenera i portów hosta	258
Ekspozowanie portów	259
Tworzenie sieci na platformie Docker i zarządzanie nimi	260
Polecenia sieciowe	260
Sieć mostowa	261
Dołączenie kontenera do sieci	262
Łączenie kontenerów	265
Łączenie kontenerów wewnątrz hosta za pomocą parametru --link	265
Zmienne środowiskowe	266
Podsumowanie	268
Pytania	269

Rozdział 10. Monitorowanie kontenerów	271
Struktura	271
Cele	272
Wydajność kontenerów, wskaźniki i zdarzenia	272
Zarządzanie dziennikami	272
Wskaźniki kontenerów	275
Odczytywanie wskaźników za pomocą polecenia <code>docker inspect</code>	278
Zdarzenia w kontenerach Dockera	278
Inne narzędzia monitorujące	280
Narzędzia do monitorowania wydajności	283
cAdvisor	283
dive	286
Falco	289
Monitorowanie działania	290
Monitorowanie serwisu WordPress	290
Uruchomienie kontenera z narzędziem Falco	291
Filtry	294
Analiza wywołań systemowych za pomocą narzędzia Csysdig	296
Podsumowanie	296
Pytania	297
Rozdział 11. Administrowanie kontenerami Dockera	299
Struktura	300
Cele	300
Wprowadzenie do administrowania kontenerami	300
Zarządzanie kontenerami Dockera za pomocą narzędzia Rancher	302
Wdrożenie platformy Kubernetes za pomocą narzędzia Rancher	306
Zarządzanie kontenerami za pomocą narzędzia Portainer	310
Wdrożenie narzędzia Portainer w klastrze Docker Swarm	320
Zarządzanie klastrem Docker Swarm za pomocą narzędzia Portainer	323
Podsumowanie	326
Pytania	326