



به نام خدا

امنیت کوبرنیتیز Kubernetes

مؤلف:

شهاب مقیمی



هرگونه چاپ و تکثیر از محتویات این کتاب بدون اجازه کتبی ناشر ممنوع است. متخلفان به موجب قانون حمایت حقوق مؤلفان، مصنفان و هنرمندان تحت پیگرد قانونی قرار می‌گیرند.

◀ عنوان کتاب: امنیت کوبرنیتیز Kubernetes

◀ مولف: شهاب مقیمی

◀ ناشر: موسسه فرهنگی هنری دیباگران تهران

◀ ویراستار: نرگس مهربد

◀ صفحه آرای: نازنین نصیری

◀ طراح جلد: داریوش فرسایی

◀ نوبت چاپ: اول

◀ تاریخ نشر: ۱۴۰۱

◀ چاپ و صحافی: صدف

◀ تیراژ: ۱۰۰ جلد

◀ قیمت: ۱۸۰۰۰۰۰ ریال

◀ شابک: ۹۷۸-۶۲۲-۲۱۸-۶۲۲-۷

نشانی واحد فروش: تهران، خیابان انقلاب، خیابان دانشگاه

-تقاطع شهدای ژاندارمری-پلاک ۱۵۸ ساختمان دانشگاه-

طبقه دوم-واحد ۴ تلفن ها: ۶۶۴۹۸۱۶۸-۲۲۰۸۵۱۱۱

فروشگاههای اینترنتی دیباگران تهران :

WWW.MFTBOOK.IR

www.dibagarantehran.com

سرشناسه: مقیمی، شهاب، ۱۳۶۱-
عنوان و نام پدیدآور: امنیت کوبرنیتیز kubernetes / مولف:
شهاب مقیمی؛
ویراستار: نرگس مهربد.
مشخصات نشر: تهران: دیباگران تهران: ۱۴۰۱
مشخصات ظاهری: ۲۴۸ ص: جدول
شابک: ۹۷۸-۶۲۲-۲۱۸-۶۲۲-۷
وضعیت فهرست نویسی: فیبا یادداشت: کتابنامه: ۲۴۷-۲۴۸
موضوع: کوبرنیتیز (نرم افزار)
موضوع: Kubernetes (computer software)
رده بندی کنگره: ۷۶/۷۶ QA
رده بندی دیویی: ۰۰۵/۱۱۲
شماره کتابشناسی ملی: ۹۰۴۱۷۵۸

نشانی اینستاگرام دیبا dibagaran_publishing نشانی تلگرام: @mftbook

هر کتاب دیباگران، یک فرصت جدید علمی و شغلی.

هر گوشی همراه، یک فروشگاه کتاب دیباگران تهران.

از طریق سایتهای دیباگران، در هر جای ایران به کتابهای ما دسترسی دارید.

این کتاب با کاغذ حمایتی منتشر شده است

فهرست مطالب

فصل اول

۱۲.....شناسایی سطوح حملات در معماری کورنیتییز

۱۲.....مقدمه کورنیتییز

۱۳.....معماری و ساختار Cluster

۱۹.....اجزای Control Plane

۲۰.....افزونه‌ها

۲۱.....نواحی بحرانی و آسیب‌پذیر کورنیتییز

فصل دوم

۲۳.....ایمن‌سازی CI/CD Pipeline و Containaer Images

۲۳.....ایمن‌سازی Images

۲۳.....اسکن امنیتی Imageها

۲۴.....اسکن کردن Image چیست؟

۲۵.....بهترین روش‌های اسکن Image

۳۶.....معرفی ابزارهای منبع‌باز اسکن Docker Image

۳۷.....بررسی و معرفی ابزار اسکن Docker منبع‌باز Anchore Engine

۴۱.....امنیت CI/CD: اسکن امنیتی Docker با جنکینز

۴۴.....اعتبارسنجی Image از طریق یکپارچه‌سازی Anchore و کورنیتییز

۴۶.....محدود کردن Docker Image ممنوع یا Imageهای اسکن نشده

فصل سوم

۴۸.....ایمن‌سازی Control Plane

۴۸.....امنیت Kubelet

۴۹.....امنیت Kubelet - دسترسی به Kubelet API

۵۰.....امنیت Kubelet - دسترسی به kubelet API کورنیتییز

۵۰.....مثال RBAC: دسترسی به Kubelet API با curl

۵۱.....حسابرسی و لاگ امنیتی کورنیتییز API

۵۳.....سیاست‌های ثبت و حسابرسی لاگ

۵۵.....گسترش Kubernetes API با استفاده از کنترلرهای پذیرش امنیتی

۵۷.....ایمن‌سازی etc کورنیتییز

استفاده از یک رجیستری Docker قابل اعتماد ۵۹

فصل چهارم

کنترل دسترسی مبتنی بر نقش ۶۷

زمینه امنیتی کوبرنیتیز RBAC ۶۷

پیکربندی امنیتی RBAC کوبرنیتیز، احراز هویت و مجوز ۶۹

فصل پنجم

امنیت در سطح پاد: زمینه امنیتی K8s، PSP، سیاست‌های شبکه ۸۰

کنترل‌کننده‌های پذیرش کوبرنیتیز ۸۰

محتوای امنیتی کوبرنیتیز ۸۱

سیاست امنیتی کوبرنیتیز ۸۴

سیاست‌های شبکه کوبرنیتیز ۹۴

مدیریت تخصیص منابع کوبرنیتیز ۹۹

فصل ششم

ایمن کردن WORKLOADها ۱۰۱

workload ۱۰۱

ایمن‌سازی workloadها مبتنی بر VM ۱۰۲

بهبود حفاظت از Workload ابری نقطه پایانی ۱۰۳

گزینه‌هایی برای امنیت مبتنی بر کانتینر ۱۰۳

رفع عملکرد بدون سرور برای محافظت از Workload ابری ۱۰۳

محافظت از Workload در برابر حملات دنیای واقعی ۱۰۴

دید سطح پایین و هسته اهمیت دارد. ۱۰۷

برخی حملات Workload و راهکارهای امنیتی ۱۰۹

فصل هفتم

شیوه‌های امنیتی Docker ۱۱۹

شیوه‌های امنیتی Docker ۱۱۹

آسیب‌پذیری‌ها و تهدیدات امنیتی اساسی Docker ۱۲۰

Vulnerability Metadata ۱۳۶

فصل هشتم

مانیتورینگ امنیتی کوبرنیتیز ۱۴۱

۱۴۱.....	جمع‌آوری و پایش رویدادهای کوبرنیتیز - رویکردها و روش‌ها
۱۴۳.....	دلایل اهمیت نظارت بر کوبرنیتیز
۱۴۴.....	چه رویدادهایی در Kubernetes باید ثبت شود؟
۱۴۵.....	معماری و روش‌های ورود به سیستم Kubernetes
۱۴۷.....	بهترین شیوه‌های ثبت عملیات logging در Kubernetes
۱۴۸.....	ابزارهای مانیتورینگ Kubernetes چیست؟
۱۴۸.....	ابزارهای مانیتورینگ منبع‌باز Kubernetes
۱۵۳.....	پایش و مانیتورینگ با Splunk و Kubernetes
۱۵۳.....	پیکربندی Splunk
۱۶۸.....	پیکربندی جمع‌آور داده
۱۸۹.....	استخراج زمینه‌های Splunk برای لاگ‌های مربوط به کانتینر
۱۹۰.....	مانیتورینگ خوشه‌های متعدد و ACL
۱۹۲.....	جریان دادن اشیاء Kubernetes از سرور API
۱۹۹.....	سرور لایسنس

فصل نهم

ضمایم فنی ۲۰۲

۲۱۰.....	اجزای اصلی امنیت Kube System
۲۱۱.....	امنیت Kubernetes به صورت پیش‌فرض با Sysdig Secure
۲۲۴.....	فالکو در امنیت زمان اجرا
۲۲۸.....	آسیب‌پذیری‌های Docker و تمهیدات برای مقابله
۲۴۷.....	منابع اینترنتی

فهرست تصاویر

شکل ۱- اجزای یک خوشه Kubernetes.....	۱۳
شکل ۲- معماری کلان کوبرنتس.....	۲۱
شکل ۳- لایه‌های Image با یک شناسه هش واحد.....	۲۳
شکل ۴- گردش کار امنیت DevOps.....	۲۵
شکل ۵- افزودن مرحله اسکن Image در گردش کار CI/CD.....	۲۷
شکل ۶- اسکن درون خطی.....	۲۸
شکل ۷- قرار دادن اسکن Image در رجیستری.....	۲۸
شکل ۸- استفاده از کنترل‌کننده پذیرش.....	۲۹
شکل ۹- بین کردن imageها.....	۳۰
شکل ۱۰- آلودگی parent image.....	۳۱
شکل ۱۱- بررسی آسیب‌پذیریهای سیستم عامل.....	۳۲
شکل ۱۲- بررسی آسیب‌پذیریهای یک Image بدون توزیع.....	۳۲
شکل ۱۳- علامت‌گذاریهای آسیب‌پذیریها.....	۳۵
شکل ۱۴- گزارش آسیب‌پذیریهای image.....	۳۶
شکل ۱۵- منابع و نقاط پایانی Anchore Engine.....	۳۸
شکل ۱۶- معماری Anchore Engine.....	۳۹
شکل ۱۷- گردش کار ایجاد Container Image.....	۴۱
شکل ۱۸- پیکربندی Engine API.....	۴۲
شکل ۱۹- ثبت مشخصات Image در Anchore.....	۴۲
شکل ۲۰- فراخوانی اسکنر Anchore container image.....	۴۳
شکل ۲۱- شناسایی فرآیند ساخت متوقف‌شده در Anchore engine.....	۴۳
شکل ۲۲- ارتباطات Kubelet.....	۴۸
شکل ۲۳- ایجاد لیست سفید Container image.....	۶۱
شکل ۲۴- سیاست‌های امنیتی کوبرنیتییز.....	۸۵
شکل ۲۵- سیاست‌های امنیتی پاد.....	۸۶
شکل ۲۶- امتیازات کنترلر.....	۹۲
شکل ۲۷- تعریف نام منبع.....	۹۲
شکل ۲۸- پنل weave cloud برای مشاهده پادها.....	۹۷
شکل ۲۹- بررسی موضوعات امنیت زمان اجرا.....	۱۰۵
شکل ۳۰- اسکن فوری آسیب‌پذیری.....	۱۰۶
شکل ۳۱- قرار گرفتن در معرض زمان اقامت.....	۱۰۷
شکل ۳۲- سیاست‌های کانتینر.....	۱۰۸
شکل ۳۳- داشبورد - تشخیص - پاسخ.....	۱۰۹
شکل ۳۴- ایجاد Repo در Quay.....	۱۳۳

۱۳۳.....	شکل ۳۵- اسکن امنیتی Quay در Image
۱۳۴.....	شکل ۳۶- انتخاب Interrogation Services
۱۳۴.....	شکل ۳۷- وارد کردن آدرس API هدف
۱۳۵.....	شکل ۳۸- انتخاب نحوه اتصال به اسکنر
۱۳۵.....	شکل ۳۹- تست صحت اتصال
۱۳۶.....	شکل ۴۰- تنظیمات Timestamp
۱۴۹.....	شکل ۴۱- داشبورد کوبرنیتیز
۱۵۰.....	شکل ۴۲- داشبورد Prometheus
۱۵۱.....	شکل ۴۳- تعبیه نمای ردیابی با جزئیات مخفی و مخفی کردن minimap
۱۵۲.....	شکل ۴۴- داشبوردهای کیبانا خارج از جعبه
۱۵۶.....	شکل ۴۵- آخرین وضعیت استقرار
۱۶۶.....	شکل ۴۶- اسکن فعالیت کوبرنیتیز
۱۶۷.....	شکل ۴۷- نتایج اسکن کوبرنیتیز
۱۶۸.....	شکل ۴۸- نتایج اسکن
۱۸۵.....	شکل ۴۹- فهرست‌های splunk به طور پیش فرض جستجو شده‌اند.
۱۸۶.....	شکل ۵۰- نظارت بر ماکروه‌های kubernetes
۱۹۷.....	شکل ۵۱- ارسال اشیاء
۱۹۸.....	شکل ۵۲- جستجو در داده‌ها
۲۰۲.....	شکل ۵۳- جریان کاری Anchore Jenkins
۲۰۳.....	شکل ۵۴- انتخاب Manage Jenkins
۲۰۴.....	شکل ۵۵- انتخاب Manage Plugins
۲۰۴.....	شکل ۵۶- انتخاب افزونه Anchore Container Image Scanner
۲۰۵.....	شکل ۵۷- تنظیمات سیستم
۲۰۵.....	شکل ۵۸- پیکربندی Anchore
۲۰۷.....	شکل ۵۹- اضافه کردن Image برای اسکن
۲۰۷.....	شکل ۶۰- اضافه شدن Anchore Build Option
۲۰۸.....	شکل ۶۱- مشخصات Build
۲۰۹.....	شکل ۶۲- گزارش خلاصه سیاست‌ها
۲۱۲.....	شکل ۶۳- نقض سیاست
۲۱۳.....	شکل ۶۴- امنیت- قانون سیستم kube
۲۱۴.....	شکل ۶۵- فید هشدار امنیتی kubernetes
۲۱۷.....	شکل ۶۶- مدیریت کاربر امنیت kubernetes
۲۲۵.....	شکل ۶۷- نحوه کار فالتکو
۲۲۵.....	شکل ۶۸- سلسله‌مراتب کاری فالتکو
۲۳۸.....	شکل ۶۹- ایجاد Repository جدید
۲۳۸.....	شکل ۷۰- نمونه گزارش CVE

فهرست جداول

جدول ۱- جنبه‌های کنترلی مختلف کلاستر.....	۸۷
جدول ۲- قابلیت‌های لینوکس و امتیاز زمان اجرا.....	۱۲۴
جدول ۳- لیست محصولات و ابزارهای برتر اصالت‌سنجی خودکار Image.....	۱۲۶
جدول ۴- لیست پورت‌های کوپرنیتییز.....	۱۴۳
جدول ۵- حاشیه‌نویسی کلی و عمومی.....	۱۷۱
جدول ۶- حاشیه‌نویسی برای لاگ‌های کانتینر.....	۱۷۲
جدول ۷- حاشیه‌نویسی برای آمار کانتینر.....	۱۷۷
جدول ۸- حاشیه‌نویسی برای آمار پردازش کانتینر.....	۱۷۷
جدول ۹- حاشیه‌نویسی برای آمار شبکه کانتینر.....	۱۷۸
جدول ۱۰- حاشیه‌نویسی برای جدول سوکت شبکه کانتینری.....	۱۷۹
جدول ۱۱- حاشیه‌نویسی رویدادها.....	۱۷۹
جدول ۱۲- حاشیه‌نویسی برای لاگ‌های مربوط به برنامه.....	۱۸۰
جدول ۱۳- گزینه‌های اسکن.....	۲۰۷
جدول ۱۴- لیست ابزارهای امنیتی داکر.....	۲۳۲

خط‌مشی انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب‌هایی با کیفیت عالی است که بتواند
خواسته‌های به‌روز جامعه فرهنگی و علمی کشور را تا حد امکان پوشش دهد.
هر کتاب دیباگران تهران، یک فرصت جدید شغلی و علمی

حمد و سپاس ایزد منان را که با الطاف بی‌کران خود این توفیق را به ما ارزانی داشت تا بتوانیم در راه ارتقای دانش عمومی و فرهنگی این مرز و بوم در زمینه چاپ و نشر کتب علمی و آموزشی گام‌هایی هرچند کوچک برداشته و در انجام رسالتی که بر عهده داریم، مؤثر واقع شویم.

گسترده‌گی علوم و سرعت توسعه روزافزون آن، شرایطی را به وجود آورده که هر روز شاهد تحولات اساسی چشمگیری در سطح جهان هستیم. این گسترش و توسعه، نیاز به منابع مختلف از جمله کتاب را به عنوان قدیمی‌ترین و راحت‌ترین راه دستیابی به اطلاعات و اطلاع‌رسانی، بیش از پیش برجسته نموده است.

در این راستا، واحد انتشارات مؤسسه فرهنگی هنری دیباگران تهران با همکاری اساتید، مؤلفان، مترجمان، متخصصان، پژوهشگران و محققان در زمینه‌های گوناگون و مورد نیاز جامعه تلاش نموده برای رفع کمبودها و نیازهای موجود، منابعی پُر بار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهد.

کتابی که در دست‌دارید تألیف "جناب آقای مهندس شهاب مقیمی" است که با تلاش همکاران ما در نشر دیباگران تهران منتشر گشته و شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

با نظرات خود مشوق و راهنمای ما باشید

با ارائه نظرات و پیشنهادات و خواسته‌های خود، به ما کمک کنید تا بهتر و دقیق‌تر در جهت رفع نیازهای علمی و آموزشی کشورمان قدم برداریم. برای رساندن پیام‌هایتان به ما از رسانه‌های دیباگران تهران شامل سایتهای فروشگاهی و صفحه اینستاگرام و شماره‌های تماس که در صفحه شناسنامه کتاب آمده استفاده نمایید.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران
dibagaran@mftplus.com

مقدمه مؤلف

امروزه با سرویس‌های وب مدرن، کاربران انتظار دارند برنامه‌ها ۷/۲۴ در دسترس باشند و توسعه‌دهندگان انتظار دارند که نسخه‌های جدید آن برنامه‌ها را چندین بار در روز اجرا کنند. کانتینری‌سازی^۱ کمک می‌کند تا این اهداف را برآورده کند و برنامه‌های کاربردی را قادر می‌سازد بدون زمان توقف منتشر و به‌روز شوند.

کوبرنیتیز^۲ به شما کمک می‌کند، مطمئن شوید که آن برنامه‌های کانتینری در هر کجا و زمانی که شما می‌خواهید می‌شوند و به آن‌ها کمک می‌کند منابع و ابزارهایی را که برای کار کردن نیاز دارند، پیدا کنند. کوبرنیتیز یک پلتفرم متن‌باز و آماده تولید است، که با تجربه انباشته گوگل در ارکستراسیون کانتینر طراحی شده و با بهترین ایده‌های جامعه ترکیب گردیده است.

از سویی ایمن کردن کوبرنیتیز ممکن است یک کار مبهم به نظر برسد. کوبرنیتیز به عنوان یک سیستم بسیار پیچیده متشکل از مجموعه‌ای از اجزای مختلف، چیزی نیست که بتوانید به سادگی با فعال کردن یک ماژول امنیتی یا نصب یک ابزار امنیتی، ایمن کنید.

در عوض، امنیت کوبرنیتیز به تیم‌هایی نیاز دارد که به هر نوع خطر امنیتی که ممکن است بر لایه‌ها و سرویس‌های مختلف در یک خوشه کوبرنیتیز تأثیر بگذارد، رسیدگی کنند؛ به عنوان مثال، تیم‌ها باید بدانند که چگونه گره‌ها، شبکه‌ها، پادها، داده‌ها و غیره کوبرنیتیز را ایمن کنند.

تیم‌های Cloud/DevOps/DevSecOps معمولاً مسئول امنیت و انطباق با حرکت برنامه‌های ابری حیاتی به سمت تولید هستند. این به برنامه شلوغ آن‌ها می‌افزاید تا زیرساخت ابر و سلامت برنامه را در شکل خوبی نگه دارند. کوبرنیتیز به یک رویکرد جدید برای امنیت نیاز دارد. به هر حال، ابزارها و فرآیندهای قدیمی با ناتوانی در ایجاد دید در محیط‌های کانتینر پویا، از برآوردن نیازهای بومی ابری کوتاهی می‌کنند. پنجاه و چهار درصد کانتینرها به مدت پنج دقیقه یا کم‌تر عمر می‌کنند، که بررسی رفتارهای غیرعادی و رخنه‌ها را بسیار چالش‌برانگیز می‌کند.

علاوه بر این، مدیران کوبرنیتیز باید بدانند، کوبرنیتیز چه ابزارهایی را به صورت بومی برای رفع نگرانی‌های امنیتی ارائه می‌دهد و چه نوع ابزارهای امنیتی شخص ثالث را برای پر کردن شکاف‌ها باید با خوشه‌های^۳ خود ادغام کنند. هدف از تدوین این کتاب تهیه و گردآوری مطالبی است که دربرگیرنده و پوشش‌دهنده شیوه استاندارد مناسب به منظور بررسی جنبه‌های مختلف امنیت کوبرنیتیز و اصول هر یک است و بهترین روش‌ها برای امنیت کوبرنیتیز را در هر لایه و سطح خدمات توضیح می‌دهد. مزید امتنان است با ارسال نظرات و رهنمودهای ارشادی خود از طریق رایانامه moghimi.shahab@gmail.com این حقیر را در تدوین بهینه‌تر مطالب آتی بهره‌مند سازید.

¹ Containerization

² Kubernetes

³ Clusters

سپاسگزار کسانی هستم که سرآغاز تولد من هستند، از یکی زاده می‌شوم و از دیگری جاودانه، استادی که سپیدی را بر تخته سیاه زندگی‌ام نگاشت و مادری که تار مویی از او به پای من سیاه نماند.

تقدیم به همسرم؛ به پاس قدردانی از قلبی آکنده از عشق و معرفت که محیطی سرشار از سلامت، امنیت، آرامش و آسایش برای من فراهم آورده‌است.

تقدیم به دل‌بندم؛ امیدبخش‌ترینم که آسایش او آرامش من است.

تقدیم به دوستان عزیزم؛ هیچ دوستی تصادفی نیست. دوستی که اشک‌های شما را درک می‌کند بسیار ارزشمندتر از دوستان زیادی است که تنها لب‌خند شما را می‌شناسند.

ارادتمند شما

شهاب مقیمی

بهار ۱۴۰۱