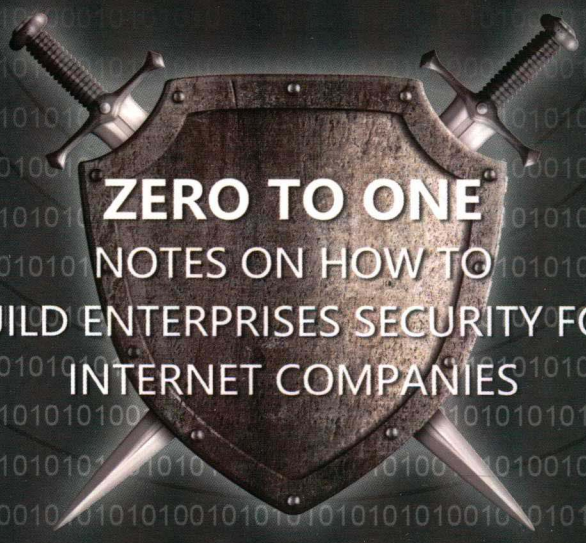
HZ BOOKS
华章IT

网络空间安全
技术丛书

- 资深网络安全专家十余年实战经验的结晶，安全领域多位专家联袂推荐。
- 从日常安全工作到建立防御系统，从抵御黑客入侵到建立风控体系，全方位介绍企业安全建设。

互联网安全建设从0到1

林鹏 编著



机械工业出版社
China Machine Press

图书在版编目（CIP）数据

互联网安全建设从 0 到 1 / 林鹏编著 . —北京：机械工业出版社，2020.5
（网络空间安全技术丛书）

ISBN 978-7-111-65668-5

I. 互… II. 林… III. 互联网络 – 网络安全 – 研究 IV. TP393.08

中国版本图书馆 CIP 数据核字（2020）第 089566 号

互联网安全建设从 0 到 1

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码：100037）
责任编辑：赵亮宇 责任校对：殷 虹
印 刷：中国电影出版社印刷厂 版 次：2020 年 6 月第 1 版第 1 次印刷
开 本：186mm × 240mm 1/16 印 张：20.25
书 号：ISBN 978-7-111-65668-5 定 价：99.00 元

客服电话：（010）88361066 88379833 68326294 投稿热线：（010）88379604
华章网站：www.hzbook.com 读者信箱：hzit@hzbook.com

内容简介

本书全面介绍企业进行互联网业务时所必备的安全技术，包含安全体系建设的方方面面，给出了作者多年亲历的案例，可供各种类型的企业建立网络安全体系时参考。

全书共分为12章：第1章介绍网络安全的基础内容，包括流量镜像、抓包、网络入侵检测系统等；第2章介绍运维涉及的常用组件、上云安全，以及一些安全建议；第3章介绍Windows、Linux系统方面的安全内容，同时也介绍了主机入侵检测系统及使用方法；第4章介绍办公网方面的一些安全技术，包括准入、隔离、DHCP Snooping等相关技术；第5章介绍与开发安全相关的内容，包括SDL、OWASP、自建扫描器等；第6章介绍日志分析相关的技术与工具，以及日志分析的一些思路和建议；第7章介绍如何组建安全平台；第8章围绕监控体系建设展开，还介绍了作者对ATT&CK的一些看法；第9章介绍GDPR及相关工作，以及数据安全方面的内容；第10章介绍账号、支付、内容等互联网常见应用的安全技术；第11章介绍设备指纹、风控系统搭建，以及与羊毛党对抗的案例；第12章介绍如何建立一个符合公司业务发展需求的安全体系，以及如何衡量安全体系的好坏。

华章图书

一本打开的书，
一扇开启的门，
通向科学殿堂的阶梯，
托起一流人才的基石。

本书赞誉

林鹏作为一名安全老兵，一直奋战在第一线，执着地探索最佳的企业安全实践。这本书也是他对企业工作的思考和经验的总结、提炼，这些经验是非常宝贵的，相信大家通过阅读此书，会有很多可以付诸于实践的收获。

——杨勇（coolc） 腾讯安全平台部负责人

万物互联时代，企业网络的暴露面在不断增加，新的威胁层出不穷，网络安全问题可能造成的损失也越来越大。虽然网络安全防护产品也在随之增长，但网络安全产品就像是一支支不同兵种的部队，最终还是需要企业的网络安全工程师排兵布阵，结合企业业务构建安全体系。作者在书中将自身多年从事安全攻防与构建企业网络安全体系的经验与心得完整地呈现在读者面前，深入浅出，对于安全新人来说，可以一览安全行业全貌，不再无从下手，对于有经验的安全从业人员，也可以查漏补缺，并了解未来业务安全、AI 安全的演进方向。希望本书可以帮助安全行业培养更多优秀的从业人员，共同守护生命和资产的安全。

——马坤 四叶草安全创始人

感谢林鹏先生邀请我阅读此书。这些年我的主要精力都花在“以攻促防”的安全体系建设上，过去两年多创建的慢雾科技虽然是在区块链生态安全领域，但服务的许多项目方实际上都非常需要这部分的安全体系落地经验。这本书给了我一个成体系的安全建设指引与启发——从 0 到 1 地构建，很值得大家阅读。

——余弦（cos） 慢雾科技创始人

从网络安全行业的无序时代开始，林鹏先生差不多与我们一起成长了 15 年，在这 15 年里我们这群人中也出现了很多技术专家或组成了顶尖的攻防团队。其中，林鹏先生是一个非常特殊的存在，他是唯一一个研究防御性技术的专家，经历了轮番上阵的磨练，也从一败涂地到一夫当关。

与防御技术相比，攻击技术的复杂度要低得多，信息化安全建设是一个体系性、周期性、长期性的工程，内容繁杂且耦合性强，本书在多个方面提供了从 0 到 1 的技术及方法论，有助于读者尽早发现安全隐患，尽快发现威胁事件，尽速避免资产受损。

——苗盛茂（Miao）梦之想科技创始人

有幸提前拜读了林总著作中风控相关的章节，感觉这对业务安全从业者是很有帮助的，我自己也有不少收获。

本书风控章节介绍了典型的黑产事件、黑产作弊工具和常见的攻击手段，从攻击者视角介绍了黑产的危害。在此基础上，进一步介绍包括设备指纹和各类数据画像在内的风控系统建设思路，并通过实战案例对风控系统的作用和价值进行了展示。

本书是作者多年实战经验的总结和升华，是一本不可多得的诚意之作。

——马传雷（Flyh4t） 同盾反欺诈研究院负责人

欣闻林鹏（lion_00）同学出书了，第一时间拜读了一下。书如其人，朴实无华，是一本互联网企业信息安全管理实操方面很好的参考手册。作为业内知名的白帽黑客出身的企业信息安全负责人，林鹏结合他在不同规模及不同形态的互联网业务中的经验和教训，完整、全面地阐述了互联网企业在不同的发展阶段，在信息安全方面面临的各种问题与挑战，并给出了可操作的建议。本书对于各类企业人员，尤其是从初创型互联网企业发展到中大型企业的信息安全管理人员和技术人员来说，是一本可供借鉴的不可多得的好书。林鹏不仅是工程师，也是程序员，再加上近几年来打怪升级到企业信息安全负责人的角色，使他写的这本书非常适合各类技术人员阅读。

——王雷 万达集团信息安全负责人

作者是我多年的老同事，其本身在安全行业深耕细作近十年，在共事的两家公司均实现了安全团队、安全业务的从无到有，并且通过自身敏锐的洞察力、卓越的专业能力为公司多次规避相关风险、挽回损失。

本书是其多年知识的积累、精华，相信通过阅读本书，可以使读者更好地了解安全相关的知识，更好地规避安全风险。

——张宏勇 丙晟科技平台支撑部总监

本书完整地将业务风控与攻防对抗的关键技术一一进行了讲解，能够很好地帮助读者学习和理解安全技术及安全业务上的必备技能，是安全体系建设方向非常不错的必读

书之一。在当前纷繁复杂的网络安全背景下，一本纲领完善的安全学习材料对从业者在技术学习、深入研究和体系建设上有着非常大的帮助，林鹏将多年在安全技术研究和安全业务对抗中总结的大量实践经验凝聚在本书中，非常值得大家学习。

——张作裕（bk7477890）阿里安全

本书介绍了网络安全的方方面面，穿插了作者大量的实践工作经验和案例，对企业安全建设从业者具有非常好的学习借鉴意义。

——聂君　奇安信网络安全部总经理

企业安全建设是一个系统化的工程，从安全管理、安全研发甚至安全研究，几乎会涉及安全行业的各个领域。相对于传统企业，互联网企业的环境更加复杂。另外，互联网企业普遍掌握大量的用户数据，成为黑灰产觊觎的对象。面对风险大、基础差、任务重的环境，建设互联网公司的安全体系更是任重道远。林鹏的这本书系统地介绍了安全建设的各个领域，内容由浅入深，是一本难得的指导手册。

——兜哥　国内著名安全专家

百度安全高级架构师《AI 安全之对抗样本入门》作者

我们开始了移动支付，开始了直播带货，各种业务都开始高度依赖互联网。然而互联网给企业带来的不仅仅是机遇，也会带来诸多新的问题与挑战，安全问题便是其中之一。虽然网络安全越来越受到关注与重视，但是对于大多数企业而言，该怎么开始做安全，怎么做才能实现安全，却是十分模糊的。本书给我们提供了一个很好的解读与参考。不论是企业管理者，或是甲方安全建设的实践者，均可成为此书的读者。粗读可解大惑，细品可答小疑。

——童永鳌（gainover）　无糖信息 CTO

认识鹏哥好多年了，或许是因为我们两个年龄相仿，也或许是因为我们都有着一颗骚动的心，不管怎样，我们彼此惺惺相惜。就在前些日子，我们还聊过以后退休了写本书。没想到，他的书都已经要出版了。

这是一本蓝队技术方面的专著，可以说是作者从业多年来智慧和经验的结晶。从运维安全、办公网安全到安全日志分析、体系建设，作者用 12 章的篇幅涵盖了蓝队技术的方方面面。也许你会说，我一个红队选手为何立蓝队的 flag？好吧，虽然我跟鹏哥一红一蓝、一矛一盾，看似毫无关联、针锋相对，但没有盾焉有矛，没有矛又何来盾？攻与

防本来就是对立统一的，没有纯粹的攻，也没有纯粹的防。所以，我不仅要把这本书推荐给蓝队选手，还要把它推荐给红队选手，因为知己知彼，方能百战不殆。这个浅显的道理大家既然知道，那就赶紧开始阅读吧！

——Moriarty　网络安全自由职业者

在安全领域有着丰富安全体系建设实践经验的鹏鹏，终于将自己的心得写了出来，为安全事业贡献了力量，帅气！有幸拜读此书，深感这本书内容深入浅出，理论与实践、技术与管理相结合，让安全从业者有了相应的参考，对于建立正确的安全价值观，同时根据实践形成自己的安全知识体系有着很大的启发与帮助。

——马金龙　新浪网网络安全部经理　安全架构师

如果想要一本拿来就用的安全建设类书籍，我想就是这本《互联网安全建设从0到1》了。企业安全建设工作千头万绪，有了这本书会让读者少走很多弯路。作者凝练十余年的安全建设经验，打造了一本非常实用的工具书，给我们带来很大的帮助和启发，值得每位安全从业者拥有。

——黄乐　央视网　网络安全部副总监

这是一本适合从安全小白到企业安全负责人阅读的全阶段的安全书籍，作者将自己多年丰富的安全经验融入此书，通俗易懂，雅俗共赏，既可以作为安全工程师的工具手册解决各类常见安全问题，也可以指导安全负责人如何从0到1系统地建设企业安全体系，非常值得推荐。

——王任飞（avfisher）　公众号“安全小飞侠”作者

林鹏于我是哥们，更是良师益友，他拥有十余年甲方安全体系建设经验，长期从事金融安全、电商安全领域工作，本书凝聚了作者十余年来企业安全建设成果的精华，为推动企业安全建设提供有力支撑，也为安全从业者提供了更广阔的视野，我既是安全从业者，也是受益者，推荐这本书，希望更多的企业团队及个人能从本书获益。

——杨蔚（301）　北京众安天下科技有限公司创始人

序　一

好友林鹏约我为他的新书作序，诚惶诚恐，犹豫再三，才落笔写下这段文字。不是别的原因，而是从业十余年，一直作为一个默默无闻的后台工作者，从未有过动笔的念头。也正因如此，一些书约都被我婉拒。而恰有一天，在停车场偶遇林鹏兄弟，他详细介绍了本书的内容，从国家大势到企业利弊给我一番“洗脑”，竟让我想起曾经所经历的企业动荡和各种暗流中的“腥风血雨”，一阵触动，晚上到家落笔作成这段小序。

近几年，新技术不断崛起：公有云、私有云、大数据、无人车、人工智能、区块链……每一项创新似乎都给企业发展带来了新的机会。但每次技术革新带来的机会背后，总是出现新的黑天鹅事件：各种交易所被盗，某全球领先社交网站涉嫌数据滥用，Deepfake（AI 换脸）……如果认真去分析，这些事件绝大部分都属于信息安全大学科范畴。这些信息安全问题正给各类企业带来巨大的挑战，全球的互联网公司都想斥巨资解决。而近几年，各国更是从国家角度出发，自上而下推动一系列的立法。欧盟的 GDPR 甚至牺牲了一成以上的商业效率去保护用户的数据隐私。

而信息安全本身的发展也是从原先单点攻击防守发展到了大到政策落实，小到业务落实的层层逻辑和流程。如果说原先是黑白帽、安全技术之争，今天则是不同公司、不同组织的安全意识之争。企业主没有安全意识，就有可能要承受黑天鹅事件的打击；技术人员没有安全意识，就有可能要承担被攻击、被追责的风险；销售人员没有安全意识，就有可能要承担预算、标书泄露的风险。当今时代，信息安全比的是意识。

林鹏兄弟作为数家大型企业整体信息安全的负责人，有着丰富的经历和知识。所涉面也极广：从技术攻防到政策理解，从产品部署到攻防数据分析，从攻击溯源到国际级调查项目，从公司流程制定到各类安全标准认证。相信本书不仅能让专业人士查漏补缺，也能给当今获取新领域竞争力的各位同行开启一扇门。

最后想说，没有绝对的安全，只有步步为营、小心谨慎、开放学习，在不断的攻防实践中升级自己的安全手段、安全装备，提升自己的安全意识，这样才能在未来的信息安全之争中立于不败之地。

孙明焱　猎豹移动高级副总裁

序　二

随着 5G、AIoT、区块链等新技术的发展和普及，未来不仅仅是电脑和手机在线，而是有更多的智能设备在线。这些智能设备打通了物理世界和虚拟世界的边界，我们面临的不再是信息安全而是网络空间安全，未来的黑客攻击影响是真正可以从网络边界落地到现实世界的。

时代的发展催生新的产品形态，越来越多的企业将要或者正在开展面向互联网的业务，这些业务 24 小时在线，可以被互联网上的任何 IP 访问，这些业务面临比过去更大的安全风险。业务的发展迅猛，但是一些企业的安全保障能力却没有跟上，于是产生了各类见诸报端的安全问题，给企业自身和用户带来严重影响。

以上情况势必将让网络安全行业更加蓬勃地发展，网络安全从业者显得更加重要。那么，作为一个网络安全从业者，应该从何处入手来保障企业安全？在我看来，从业者应该有扎实的一线技术，知道黑客是如何攻击的，进而理解如何防御，逐渐积累经验和能力，提高防御水平。

本书就很好地阐述了企业安全建设的方方面面，基本涵盖了企业安全所涉及的网络、运维、主机、研发、办公及业务等领域的安全风险和防御手段，既有可落地的技术实践指导，也有宏观的安全方法论，实在是不可多得的网络安全工作的案头必读之物。作者林鹏本身是一位资深的白帽子，精通各类黑客攻击手法，又主导过多家企业的安全防护工作，攻防视角兼备，其集十余年功力写成的本书是多年企业安全建设经验的总结，大力推荐。

胡珀（lake2）　腾讯安全平台部总监

序　三

和林鹏没见过，但不算陌生，毕竟，他作为安在的“座上宾”，曾上过我们的“人物”报道。所以，印象里他是个牛人，而现在，牛人百忙中居然出了一本书，那就更牛了。我是写过书的，深知其味，与林鹏也就有了更多共鸣。

其实，当他让我写推荐序时，我是很为难的，毕竟，一没仔细读过，二是脱离专业工作日久，怕说得不妥而带偏读者也错会了作者。等到林鹏给我发来大纲，以及他的一些用意和心得，我说，这推荐序我写定了。

很多时候，一本书你未必要通读正文，只看摘要和目录，就大概能领会一二了。那么我对林鹏新书的这一二领会在哪呢？

其一，这是真正来自“甲方”一线从业者实打实的经验之谈。我们知道，从事网络安全的，向来“低调”，自己做一分，便不多说半分，尤其是在企业中做内部安全的，很多时候就像扫地僧，本事不小，可从不张扬，甚至都很少表达。有人问，那市面上那么多网络安全的书都哪来的？这几年的我不了解，但至少多年前，比如我写书那会儿，厂商居多，高校居多，职业攒书者居多，来自企业一线专家的著作太少。这导致一个问题，就是诸多的网络安全书籍，大多还是沿用传统的攻防思维和技术脉络，很少有从企业最佳实践和日常运营角度去展现和表达的。而在林鹏新书的大纲中，安全平台建设、安全部门组建和日常工作、监控体系建设以及工作开展、数据和隐私安全，尤其是业务安全和风控、安全体系和度量，恰恰都是企业安全工作最核心的部分。由此可见，此书多干货，用户尤可鉴。

其二，当我和林鹏从他的新书引申开去聊得更多时，我才知道，林鹏不是突然间以写一本书的方式来做分享的，在他长达十年的一线工作中，他经常在一些著名的国际会议上做议题演讲和技术分享，写过大量文章，也录过视频课程，是个名副其实的知识“网红”。一个人只有乐于分享，他才能把分享当成习惯乃至日常，而只有当分享成为习惯和日常，才能将分享打磨成真正的擅长。这样一个乐于分享、习惯分享又擅长分享的人，所写的书是否值得一读，自然明了。

如上两点，权作我对林鹏新书的一二领会。

期待林鹏新书早日付梓并出品面世，届时，我会第一时间讨来研读，看看是否能够印证此刻判断。

话说，迄今为止，在选书和读书这件事上，我大抵是没有看错过的。

张耀疆　安在创始人

前　言

笔者从事安全行业工作近 10 年了，也参加过大大小小的安全会议，并担任过一些会议的演讲嘉宾，听到最多的问题是如何在甲方进行安全工作。确实，笔者刚加入当当网进行安全工作时，也是一头雾水，不知道该从哪里下手。对于一个刚进入安全行业，尤其是加入甲方工作的安全从业者来说，该怎么去做，该从哪里开始，是一件比较棘手的事情。因此笔者才想借此机会，将自己的工作经验写出来，也希望给安全行业做点微小的贡献。

笔者认为，安全行业有一个特别之处：直接与人对抗，不仅需要非常扎实的技术及理论基础，而且需要对人性有所认识。因此需要不断地学习，不断地实践。对于理论知识的学习而言，现在互联网十分发达，可以非常容易地找到需要学习的内容（不过网上内容良莠不齐，需要通过实践进行辨别）；对于实践，网上也有很多靶机，亦可以很方便地使用。除此之外，笔者也推荐使用 VMware 和 dynamps 等模拟器，灵活使用这两个工具，几乎可以组建所有类型的网络环境，本书里的实验内容大多用到了以上两个工具。

除了学习外，笔者还认为做安全应深入一线，在对抗中发现问题，这样才能保持对安全的敏感度。

另外，在安全的攻防对抗中，尽管攻方容易成为耀眼的明星，但防守方也可以非常出色。既然选择了防守，便意味着担当了守卫的责任，我的身后便是信任我的人、我的公司，我当尽全力去守护。本书结合了笔者多年的防御经验，从各个方面讲述了如何做好防守工作。

全书共 12 章：第 1 ~ 8 章为基础安全部分，主要介绍日常的安全工作，建立防御系统，抵御黑客入侵；第 9 ~ 11 章为业务安全部分，主要介绍互联网常见业务安全相关内容；第 12 章介绍如何构建安全体系。

每章内容简介如下：

第 1 章　网络安全，介绍运维涉及的网络安全的基础内容，包括流量镜像、抓包、网络入侵检测系统等。

第 2 章　运维安全，介绍运维涉及的常用组件、云上安全，以及一些安全建议。

第 3 章　主机安全，包括 Windows、Linux 系统方面的安全内容，同时也介绍了主机入侵溯源分析、入侵检测系统及使用方法。

第 4 章　办公网安全，介绍办公网方面的一些安全技术，包括准入、隔离、DHCP Snooping 等相关技术。

第 5 章　开发安全，介绍与开发安全相关的内容，包括 SDL、OWASP、自建扫描器等。

第 6 章　日志分析，介绍日志分析相关的技术与工具，以及日志分析的一些思路和建议。

第 7 章　安全平台建设，介绍如何组建安全平台部门及部门的日常工作内容。

第 8 章　安全监控，围绕监控体系建设展开，还介绍了个人对 ATT&CK 的一些看法。

第 9 章　隐私与数据安全，介绍 GDPR 及相关工作，以及数据安全方面的内容。

第 10 章　业务安全，主要介绍账号、支付、内容等互联网常见应用的安全技术。

第 11 章　风控体系建设，介绍设备指纹、风控系统搭建，以及与羊毛党对抗的案例。

第 12 章　企业安全体系建设，介绍如何建立一个符合公司业务发展需求的安全体系，以及如何衡量安全体系的好坏。

由于笔者在移动安全方面涉及不深，本书内容缺少了这个部分，也算是一个小小的遗憾。

致谢

在这里要衷心地感谢我的领导、我很敬佩的安全圈前辈孙明焱（CardMagic），他在日常工作中给了我很大的信任并提供了很多帮助与支持，在百忙之中，还给本书写了序。感谢胡珀（lake2）@ 腾讯，腾讯安全在业内称得上是行业标杆，也是我学习的榜样，感谢他给本书写了序。感谢张耀疆 @ 安在为本书作序，我们虽然暂未谋面，但可以看到安在在他的带领下不断为安全领域输出各种有价值的内容，祝愿他的平台越来越好。感谢饶琛琳（三斗室）@ 日志易，在我初学 Logstash 时，不厌其烦地解答我提出的很多问题，也算是我学习 ELK 的启蒙老师。感谢我的 CCIE 老师秦柯（现任明教教主）@ 乾颐堂，我在网络安全方面的技术，很多都是跟他学的，同时他也被誉为“CCIE 制造机”。

感谢机械工业出版社的吴怡编辑，她非常仔细地修改了我写的每一个字，提出了很多修改建议，她是一位非常认真负责的好编辑，感谢赵亮宇编辑对本书进行编辑工作，

也感谢出版流程中的所有工作人员。

感谢所有我任职过的公司以及我的团队，是他们给了我锻炼、学习、成长的机会，也给了我帮助与支持。

还要感谢同行对我的帮助，他们分别是（排名不分先后）：郑昀炜（Cnhawk）、马传雷（Flyh4t）@同盾、张坤（bloodzer0）@毕马威、黄乐（企业安全工作实录）@央视网、靳小飞@vipkid、聂君（君哥的体历）@奇安信、赵弼政（职业欠钱）@美团、王永涛（Sanr）、马金龙（吗啡）@新浪、秦波（大波哥）@滴滴、王任飞（avfisher）@华为、王昱（猪猪侠）@阿里、游小波@西海龙湖、黄梦娜（Mils）@兴业银行、凌云（linkboy）@携程、张迅迪（教父）@阿里、杨勇（coolc）@腾讯，等等。

另外，感谢北洋舰队的朋友，在我刚入门安全领域时，他们把攻击的经验分享给我，我才可以从防御角度思考问题出在哪里，如果是我做防御该去如何应对。感谢“蓝星最强技术扯淡公益群”的所有群友及所有给过我帮助的朋友们。同时要声明，本书的一些素材来源于互联网，在此对原作者一并表示感谢。

最后感谢我的家人，尤其是我的妻子，在我写书的漫长时间里承担了繁重的家务，默默地支持着我，让我可以专心写完此书，兑现了我要写一本书的承诺。也感谢我的女儿，小家伙在我写书的过程中很乖巧、听话，为我提供了良好的写书环境。

尽管笔者尽量保证书中不出现错误，书中每个实验都是自己完成后再编写内容，但是由于技术水平和能力有限，难免会有错漏之处，在此，笔者恳请读者不吝指正。关于错误内容可以反馈至 lion_00@163.com 中，笔者也会通过微信公众号“安全防御”（anquanfangyu）发布勘误。欢迎读者与笔者一起交流安全技术。

献给特别的朋友们

2017 年，我组建了一个梦之队，这个团队的成员几乎都是安全行业内的高手，我们一起完成了一个又一个挑战——从无到有建立了安全防御系统、风控系统，在一次活动中挽回了 9 亿活动币，避免了近百万元的损失，等等。但是，由于公司业务不佳，大家最后各奔东西，这也让我深刻地理解到安全团队的定位——为业务服务，否则一切都失去了意义。虽然目前梦之队的队员们分散在不同的公司，但是在我写这本书时他们都非常支持我，给了我很多帮助，感觉又一次在一起合作了。本书中也包含了这个团队的实战经验，因此我将这段回忆写在这里，献给这群特别的朋友们。

2017 年还有一天就结束了，这也是我发的第一个朋友圈，是为了我的团队兄弟们发的。你们每个人在我看来都是非常棒的！大牛（宗悦：rootsecurity@ 京东），就好比一个屏障，在运维安全和系统配置方面独当一面；董川，以前只写运维脚本，现在是 Storm、Spark、实时处理大数据全能；土豪（陈锋卫 @ 民生），优秀的前端和超级的 PHPer，每个系统都有你的功劳；奇哥（陈奇 @ 宜信），没有你就没有我们的基础数据，一再地改善抓包性能，使丢包率更少，你功不可没；超哥（吴业超 @360）的贡献为我们创造了非常大的便利，也让咱们的漏洞平台看起来很专业；感谢小侯（侯芳芳），从没入职的时候到现在一直帮我改 PPT，还有 27000 的项目也非常尽责；神奇的猫爷（王振飞：加菲猫 @ 道享）总能给我们带来非常实用的工具，比如扫描器、扫码登录；神一样存在的梁大神（梁宛生：花生 @ 道享）简直就是漏洞发掘专家，你对飞凡的贡献我不会忘记；马老板（马鑫 @ 锦江），优秀的产品经理加数据分析师，你的 PRD 写得非常专业；玄妹子（玄银星 @ 道享）的月报写得也是越来越好，跟踪漏洞也不让我操心；还有吴总（吴淳 @ 百度），虽然你的 Kibana 是后学的，但也发现了很多异常，在对刷单的识别方面已经算火眼金睛了，希望有机会还能一起打球；小妹（王小妹 @ 京东云）和小杨（杨智 @ 政采云），你们虽然来的时间短，但是也能很快适应工作，发挥自己的作用，为咱们补了短板；还有邱大神（邱永永 @ 华为）也算是飞凡盾的创始人了，一个人完成了那么复杂的逻辑功能；当然也感谢县长（张宏勇 @ 丙晟）对我们的帮助和照顾。虽然我们受到一些众所周知的情况影响，但和大家在一起共事真的非常开心。你们任何一个人的离开都是公司的损失。感谢你们每个人的付出。感谢你们每个人对我的支持和理解，不管将来怎样，我都会永远记得大家。

目　录