51CTO、CSDN、ChinaUnix、IT168、Linux中国、开源中国
六大社区联合推荐！

开源安全运维平台

Open Source Security Operation and Maintenance Platform

OSSIM Best Practices

OSSIM最佳实践

李晨光 著

清华大学出版社

开源安全运维平台

OSSIM最佳实践

李晨光 著

清华大学出版社
北京

内 容 简 介

在传统的异构网络环境中，运维人员往往利用各种复杂的监管工具来管理网络，由于缺乏一种集成安全运维平台，当遇到故障时总是处于被动“救火”状态，如何将资产管理、流量监控、漏洞管理、入侵监测、合规管理等重要环节，通过开源软件集成到统一的平台中，以实现安全事件关联分析，可从本书介绍的 OSSIM 平台中找到答案。本书借助作者在 OSSIM 领域长达 10 年开发应用实践经验之上，以大量生动实例阐述了基于插件收集日志并实现标准化，安全事件规范化分类，关联分析的精髓，书中为读者展示的所有知识和实例均来自大型企业中复杂的生产环境，并针对各种难题给出解决方案。

全书共分三篇，10 章：第一篇（第 1~2 章）主要介绍 OSSIM 架构与工作原理、系统规划、实施关键要素和过滤分析 SIEM 事件的要领。第二篇（第 3~6 章）主要介绍 OSSIM 所涉及的几个后台数据库，重点强调安全事件分类聚合、提取流程、关联分析算法、Snort 规则分析等技巧。第三篇（第 7~10 章）主要介绍日志收集方法和标准化实现思路以及在 OSSIM 中用 HIDS/NIDS、NetFlow 抓包分析异常流量的方法，深入分析了 OpenVAS 架构和脚本分析方法。

本书可以作为开源安全技术研究人员、网络安全管理人员以及高校计算机专业师生学习参考使用。

图书在版编目（CIP）数据

开源安全运维平台：OSSIM 最佳实践 / 李晨光著. - 北京：清华大学出版社，2016
ISBN 978-7-302-42385-0

I. ①开… II. ①李… III. ①Linux 操作系统－安全技术 IV. ①TP316.89

中国版本图书馆 CIP 数据核字(2015)第 296359 号

责任编辑：夏非彼
封面设计：王　翔
责任校对：闫秀华
责任印制：杨　艳

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：三河市中晟雅豪印务有限公司
经　　销：全国新华书店
开　　本：190mm×260mm　　**印　　张**：42.5　　**字　　数**：1088 千字
版　　次：2016 年 1 月第 1 版　　**印　　次**：2016 年 1 月第1 次印刷
印　　数：1～3000
定　　价：148.00 元

产品编号：062466-01

媒体推荐

51CTO 推荐

认识晨光近十年，旁观了他网络管理实践水平的日臻高超，也见证了他多年来在知识及技能的整理与传播方面的坚持和硕果累累。晨光的文章和著作特点明显：结合实践、平实厚重、干货多多，也因此受到读者的爱戴。在本书发表之前，晨光已经发表了 OSSIM 的博文六十余篇，可想而知他为本书出版的积累之深。我相信，阅读此书，您一定收获满满！

杨文飞　51CTO 总编

51CTO 推荐

李晨光老师是 51CTO 专家博主，也是 51CTO 学院知名讲师。他的文章深受同行关注和认可，荣获了多项殊荣，他的课程在学院深受学员喜爱。新书《开源安全运维平台——OSSIM 最佳实践》是李老师在 OSSIM 领域长达 10 年开发应用实战经验的总结和凝练，书中的所有知识和实例均来自大型企业中复杂的生产环境，并针对各种难题给出解决方案，相信此书一定会深受广大读者的支持。

51CTO 社区、51CTO 学院

CSDN 推荐

说来惭愧，身为机房装机工出身，竟然也是 Google 了半天才搞清楚什么叫 OSSIM。当年在机房苦哈哈地安装、调测 Nagios 和 Snort 的场景还历历在目，读起晨光老师的这本《开源安全运维平台——OSSIM 最佳实践》自然倍感亲切。

我的理解，OSSIM 是安全运维发展到一定阶段后体系化、工程化的成果，强调独立安全应用间的配合。这对使用者提出了很高的要求：不仅要熟悉系统中每个应用的用法，还要清楚安全信息在整个系统中的流转，以及出了问题后的准确定位。这不仅需要大量的实践，更需要经验的积累。这本书的内容，能更快地帮助你了解这个复杂的系统。更为难得的是，书

中包含了很多最佳实践的分享，对于有一定经验的读者也有着很好的参考意义。

作者晨光老师在安全运维领域耕耘多年，书中的内容，都是在常年工作中总结出的实战经验之谈，是国内第一本系统阐述 OSSIM 理论和实践的作品，更是一个有追求的运维人员在成长路程上不可多得的资料。

然而让人觉得非常可惜的是，国内系统化安全运维的理念并不普及，提起 OSSIM 来，估计知其然的人就不多，更勿论知其所以然者。希望晨光老师的这本书能被更多的人了解和学习，能切切实实地帮到奋斗在一线的兄弟们。我想，这也是每一个 CSDN 人的愿望。

李申 CSDN 社区运营总监、CSDN 学院总监

IT168 推荐

多年来，李晨光老师一直是众多 IT 圈朋友的良师益友。文章素来结构清晰，布局平实，技术内容扎实，读后受益良多。欣闻李晨光老师将发新作，想来又是一次技术升华的历练旅程。在作者的描述下，OSSIM 这一还尚处于发端的全新安全运维架构扑面而来，读来不忍释手。原因有三：

其一，信息安全市场历来与开源没有渊源，不管是 SIEM 还是 SOC，在国内普及和实践也有些时日，但一直不温不火，搭上开源是偶然还是必然，以求甚解；其二，诚如作者所言，“本书不是神功秘籍”，只为读者铺陈经验、答疑解惑。而信息安全之于企业是个平衡问题，安全运维如何在快速变化的动态中，找到最佳平衡支撑，恰恰需要兼容并蓄；其三，想来，数据驱动的浪潮或已不远，安全威胁的全息生态掌控，玩的正是数据、事件和风险的收集和分析，要主动出击还是被动防御，不难选择。作为先睹为快者，我只能谈一些浅见，是为序。

陈毅东 IT168 企业级副总编

启明星辰专家推荐

安全信息与事件分析（SIEM）技术进入中国也有十几年了，但是就如同以 SIEM 为核心的安全运营中心（SOC）一样，由于顶着过于炫目的光环，在国内的发展始终喜忧并存。究其缘由，其中很重要的一点就在于 SIEM 是安全分析的集大成技术，涉及面广、复杂度高，对使用者要求也比较高，而国内信息安全产业的发展以及安全运维体系还未完全成熟。

但是，安全事件分析作为安全运维的核心技术无可替代，是企业和组织信息安全建设以

及安全运维的必然选择。在这种背景下，国内迫切需要一系列的相关书籍来传播和推广相关技术，本书无疑是国内安全事件分析技术领域的重要论著。

从全球范围来看，SIEM 技术发展已趋于成熟，2014 年市场规模接近 17 亿美元，商业公司占据了大部分的市场。其中，OSSIM 是唯一成功的开源 SIEM。从 2003 年发布第一个版本至今，OSSIM 已经发展了 12 年，足见其强大的生命力。而以 OSSIM 为基础成立的 AlienVault 公司也已经成为 SIEM 领域的知名公司。

OSSIM 作为一个开源安全运维和安全事件分析平台，较好地集成了各种开源的安全工具，并能够与大量商业化的安全产品进行对接，同时还具备很强的扩展能力，真正成为一个安全运维的开放式平台。

李晨光先生是国内 OSSIM 领域的权威人士，对安全运维有深刻的理解，拥有丰富的实战经验，书中汇集了他多年的实践成果，十分难得。跟随晨光学习 OSSIM，不仅能够提升自身的安全运维实战能力，也有助于理解安全运维体系和安全事件分析运作原理。

叶蓬 启明星辰泰合 SOC 产品总监、SOC 布道师

ChinaUnix 推荐

晨光是 ChinaUnix 专家博主，在 Unix/Linux 领域工作多年，在 ChinaUnix 发表了很多高质量的技术文章和 Linux 教学视频，深受广大网友喜爱。《开源安全运维平台——OSSIM 最佳实践》一书是他多年研究成果的总结，也是业界第一本关于开源安全运维的著作，书中采用了大量实例生动地讲解了 OSSIM 的安装和使用过程，深入浅出地分析了 OSSIM 关联分析等核心技术，引入了作者多年对 OSSIM 技术的研究成果和实践经验，这对于开阔读者眼界，提高技术水平将大有裨益。如果你从事系统运维，对网络安全感兴趣，我们强烈推荐此书。

ChinaUnix 社区

Linux 中国 推荐

从 2011 年起，我就在电信系统从事网络安全方面的工作，期间接触了不少企业客户，有央企、也有中小型公司。发现很多时候，企业在应对信息化普及所带来的变化时有些力不从心。较大的企业，其企业信息化也比较完善，除了大量的服务器、终端计算机、网络设备之

外，也有各种网络安全方面的专用设备和软件，但是，随着规模的扩大设备的管理、信息的归集会越来越步入低效，往往导致各种设备资产并不能及时有效地发挥作用。

面对企业的大量的 IT 设备管理包括多个方面，从资产管理、网络监控、漏洞管理、入侵检测等都有各种管理规范和相应的软硬件设备，那么增加这些管理系统是否又进一步加剧了信息臃肿呢？过去的做法是，针对每个细分都有一套乃至几套系统来管理，而这些系统之间并不能互相协调、信息共享，往往导致自相矛盾，让管理人员无所适从。当时，似乎并没有一个可以全面地、可靠地解决这些问题的方案。

举个例子，某国有大型银行，其为了应对网络安全风险，除了防火墙之外，还专门部署了 IDS 和 IPS 设备，但是随后发现各种事件、消息如洪水般涌来，将真正有价值的信息都淹没在了各种信息噪音之中。由于并不能针对企业实际的情况有效地降低无关或常规信息的干扰，导致每天发送的例行报告，也就真的成为了“例行”，从而只是增加了收件箱中的某个文件夹的未读邮件的数字而已。

那么，如何从纷杂的信息中及时准确地将重点的信息撷取出来？如何将各个设备、功能从各个方面，一致而完整地联系起来？

有幸认识了晨光老师，听他深入浅出地介绍了 OSSIM 系统，才发现这样的一套开源解决方案，恰恰满足了大部分企业在这方面的需求。OSSIM 是开源软件，在没有接触 OSSIM 之前，很多人会对它抱有一些疑虑，担心它的健壮性不足，担心它的功能不够全面，甚至担心它一如很多开源软件那样丑陋。但是 OSSIM 让我一个在开源圈混迹了多年的老兵也很吃惊，其表现绝对可以令人眼前一亮。那么具体 OSSIM 是怎么样的呢？这个问题可不是一两句话能说明白的，想详尽了解 OSSIM 的读者，请阅读这本晨光老师的力作吧！

王兴宇 Linux 中国（https://linux.cn/）创始人、前中国电信高级专家

开源中国推荐

接到晨光让我为他的新作写序的邀请后，我诚惶诚恐，尽管已经在技术圈里瞎混了十几载。但是运维对我来说既熟悉又陌生，虽然做开发，但几乎天天都要接触运维的工作，从服务器安装、应用环境安装到应用部署，以及后期的维护、扩容和安全等等方面，特别一开始做开源中国网站时，更是事无巨细、亲力亲为；但是跟晨光接触两年来，深感自己所做的这些是多么的微不足道。

从自己的从业经验来看，运维着实是一件非常专业的工作，而且要求经验必须非常丰富，才能从各种五花八门的现象中进行问题定位，从海量日志中分析问题，从而制定行之有效的解决问题的方案。当一个系统规模不断扩大的过程中，运维工作日趋重要。

在开源领域中有大量跟运维相关的开源软件，光开源中国网站就收录了运维相关的工具

超过 400 款，而 OSSIM 就是其中非常优秀的一款。OSSIM 是目前一个非常流行和完整的开源安全架构体系。OSSIM 通过将开源产品进行集成，从而提供一种能够实现安全监控功能的基础平台。它的目的是提供一种集中式、有组织的、能够更好地进行监测和显示的框架式系统。晨光的这本书从 OSSIM 的架构原理、安装部署，再到内部架构、高性能部署以及应用场景的实战等方面进行非常详细的讲解，不仅对软件的初学者适用，而且对经验丰富的工程师都有非常高的参考价值。

从此书的篇幅便知运维工作之复杂，唯有孜孜以求方能在强手之林有立锥之地，与君共勉。

红薯 开源中国办公室

前　言

为什么要写作本书

1. 现状

日常工作中，运维人员大部分时间和精力都用于处理简单、重复的问题，由于故障预警机制不完善，往往故障发生后才会进行处理，运维人员经常处于被动“救火”状态。

没有高效的管理工具支持，就很难快速处理故障。市面上有很多运维监控工具，例如商业版的 Solarwinds、ManageEngine 以及 WhatsUp 等，开源的 MRTG、Nagios、Cacti、Zabbix、OpenNMS、Ganglia 等。由于它们彼此之间没有联系，即便部署了这些工具，很多运维人员并没有从中真正解脱出来，成千上万条警告信息堆积在一起，很难识别问题的根源，结果被海量日志所淹没，无法解脱出来。

另外，在传统运维环境中，当查看各种监控系统时需要多次登录，查看繁多的界面，更新管理绝大多数工作主要是手工操作，即使一个简单的系统变更，也需要运维人员逐一登录系统，若遇到问题，管理员便会在各种平台间来回查询，或靠人肉方式搜索故障关键词，不断地重复着这种工作方式。企业需要一种集成安全的运维平台，满足专业化、标准化和流程化的需要来实现运维工作的自动化管理，通过关联分析及时发现故障隐患。

2. 手工整合的演化过程

在人工管理初期，主要依靠一些简单的 Shell 脚本完成一些基础工作，后来虽然采用 Cacti 来做性能监控，Nagios 做主机监控、PHP+SSH 等方式进行管理，但各种运维工具仍无法实现数据共享，此时整个防御体系面对网络威胁“反应迟钝”，每当故障来袭，总是“马后炮”，难以查找攻击者的踪迹，就好像一个人总被蚊子叮咬，想打蚊子可手眼又跟不上的感觉。

经过分析后，开始尝试将资产管理模块、入侵检测模块、流量监控模块、漏洞扫描模块集成到一台服务器中进行统一管理，实现了标准化日志、统一处理等任务，在系统改造中以下问题尤为突出：

- 安装时软件依赖问题难以解决。
- 各子系统界面重复验证和界面风格不统一。
- 各子系统之间数据无法共享。
- 无法实现数据之间关联分析。
- 无法生成统一格式的报表。

- 缺乏统一的仪表板以展示重要信息。
- 系统维护难度增大。

将这些开源工具集成比较困难，该方案架构并不合理，出现了性能瓶颈，对于安全事件的关联分析、合规管理及知识库查询依然无法实现。

3. 终极工具——OSSIM 集成安全运维的平台

发现一个好的管理平台并不是偶然，管理员从最原始的命令行的运维时代，进化到统一管理平台，的确要走很多弯路，其实这一过程就是普通管理员到专家的蜕变。只有经历过磨难的管理员才能深刻体会到这一点。一款优秀的安全运维平台，需要将事件与 IT 流程相关联，筛选出运维人员最关心的事件，提高工作效率。

目前能满足上述要求的开源产品只有 OSSIM 系统，它是由 AlienVault 公司开发的，现分为开源 OSSIM 和商业版 USM 两种，通过该平台实现对用户操作规范的约束和对计算机资源进行监控，包括服务器、数据库、中间件、存储备份、网络基础设施，通过自动监控管理平台实现故障综合处理和集中管理，能够为您的网络构建起一套敏感的、全方位的中枢神经系统，达到感知网络威胁的效果。

创作过程

说起来，我和 OSSIM 还是挺有缘分。研究生时曾开发过开源统一安全管理平台项目，主要目标是将不同网络设备和服务器的日志，通过标准化转化为事件，然后统一进行日志分析与设备联动。在完成这个项目过程中，主要参考 OSSIM 源代码，先后尝试了基于统计、基于距离和基于决策树的算法，攻破了网络安全事件聚合的难题。

这些年先后为几十家单位成功部署了 OSSIM 系统，并提供技术支持。在 OSSIM 项目实施过程中不断总结遇到的各种问题，经过三年的技术沉淀与积累，目前已经撰写出 600 多页的 OSSIM 应用教程，但是这些零散的手稿不成体系。从 2015 年初，开始将这些系统部署的经验进行合理组织，全书规划成三篇，共 10 章内容，这些内容包含 OSSIM 系统的各种知识和技巧，使读者今后再遇到问题能够举一反三。即使 OSSIM 更新升级后，读者也能结合书中介绍的概念和操作方法，同样能够掌握，那么本书的目标就达到了。

从事 IT 工作的人都比较忙，很少有完整的时间能清闲下来，对于一般人而言没有时间就是最好的幌子，而善于利用时间的人往往能够利用各种间隙进行创作构思。在本书创作中并不是一帆风顺，有时候为了验证一个技术问题需要反复实验，为了一句话需要经过反复推敲。

初稿出炉，必须经过不断修改润色才适合阅读。本书刚刚写完时才 500 多页，但是在一遍又一遍的修改笔误和错别字之后，萌发出新的想法，每复查一遍，我都会对原稿做一些改动，数量上要数第一次改动扩充最大，以后逐渐减少，直到满意为止。

本书不是什么神功秘籍，无法让你在短时间内从一个小白变成一个牛人。书中以 OSSIM 4 平台为基础进行讲解，将各种开源软件合理地融入进来，并把本人多年 OSSIM 实施经验以案例的形式表达出来。学习 OSSIM 的道路并不是一帆风顺，希望读者朋友再遇到困难时，本书能够为您答疑解惑。

篇章结构

书的结构好比框架，而内容则是具体组成元素，本书采用了文字、图表和范例等形式，将 OSSIM 复杂的结构和工作流程直观地展现给读者。全书分为三部分，共 10 章。

1. 基础篇

第 1 章：本章从 OSSIM 起源讲起，介绍了目前运维人员现状，逐步谈到应用 SIEM 的必要性，进而介绍 OSSIM 架构与组成原理，另外还介绍了基于插件的日志采集思路，提出标准化安全事件的全新理念，详细分析了 OSSIM 的高可用架构与实现方法。

第 2 章：本章从 OSSIM 实施关键要素、安装策略、硬件选型开始，深入分析单机部署，分布式体系、传感器设置等重要安装工作。分析安装过程以图文并茂的方式，指出了系统配置过程，包括实体机、虚拟机不同环境中的安装方法及注意事项。最后重点分析了 SIEM 事件控制台的使用和事件过滤方法。

2. 提高篇

第 3 章：本章对于 OSSIM 开发人员很有帮助，除了介绍 OSSIM 数据库组成、表结构，以及系统迁移备份等技巧以外，还包括各种常见 MySQL 故障等内容。

第 4 章：本章从关联分析基础讲起，逐步深入到 OSSIM 安全事件提取过程，介绍了常用的关联分析算法。还对报警事件的聚合原理做了详细分析，并结合 OSSIM 现状采用多个实例讲解关联规则和自定义策略的使用方法。

第 5 章：本章主要介绍各种 OSSIM 系统中的监控调试工具的使用，以及系统瓶颈的诊断方法。

第 6 章：本章重点介绍 Snort 原理和预处理程序发挥的作用，包括 Snort 报警方法。深入分析 Snort 规则编写在 OSSIM 中的应用技巧以及网络异常行为分析方法。

3. 实战篇

第 7 章：本章从日志标准化和收集分析方法讲起，详细分析各种服务、网络设备所产生的日志，包括 Apache、FTP、Squid、DHCP 等，并通过实例详细介绍 OSSIM 插件开发过程。

第 8 章：本章讲解 NetFlow 进行异常流量分析的方法，包括 NetFlow 数据采集和过滤方法，介绍了分布式环境中，利用 NetFlow 监测异常流量的技巧，同时针对 OSSIM 中 Ntop、

Nagios、NetFlow 三种检测工具的使用方法进行了对比。最后还介绍了 Cacti 和 Zabbix 第三方开源监控软件集成的方法。

第 9 章：本章从 OSSIM 控制管理中心角色权限控制讲起，全面介绍了 OSSIM Web UI 的结构，讲解了 OSSEC 日志分析工具的配置使用和 Agent 的安装方法。介绍了 OSSIM 中管理网络资产的实例，并对 OpenVAS 扫描模块、脚本以及规则做了深入分析。展示了多个利用 OSSIM 进行高级攻击检测的实例，以及利用 OSSIM 进行合规管理和系统统一报表输出的方法。

第 10 章：本章主要讲解基于 Web 方式下的抓包及数据包过滤方法，并采用该工具远程解决网络故障的方法，重点介绍了 tshark、tcpdump 等抓包工具的高级使用方法，最后以一个典型 IE 浏览器的 0 day 漏洞攻击的实例来检验这种工具所发挥的作用。

本书约定

（1）关于版本

本书软件的安装环境为 Debian Linux 6.0（Squeeze），内核为 2.6.32。在安装其他软件时，必须符合该版本要求。

（2）关于菜单的描述

OSSIM 的前台界面复杂，书中经常会用一串带箭头的单词表达菜单的路径，例如 Web UI 的 Dashboards→Overview→Executive，表示 Web 界面下鼠标依次经过菜单 Dashboards、Overview，最后到达 Executive 仪表板。

（3）路径问题

本书中除特别说明，所涉及路径均指在 OSSIM 系统下的路径，而不是其他的 Linux 发行版。终端控制台指通过 root 登录系统，然后输入“ossim-setup”启动 OSSIM 终端控制台的界面，如图 1 所示。

图 1　终端控制台

在终端控制台下，选择 Jailbreak System 菜单就能进入 Root shell，登录日志会保存在

/var/log/ossim/root_access.log 文件中。

（4）SIEM 事件分析控制台

书中的 SIEM 控制台是指通过 Web UI 进入系统，在菜单 Analysis→SIEM 下的界面，如图 2 所示。

图 2　SIEM 事件分析控制台

（5）关于 OSSIM Server 端与 Sensor 端的约定

本书各章中讲述的 OSSIM Server 端，是指通过 Alienvault USM 安装的系统，包括 OSSIM 四大组件，Sensor 端是通过 Alienvault Sensor 安装的系统。

（6）关于地图显示问题

所有地图信息引自谷歌地图，大家在做实验前确保能连上谷歌地图，而且使用系统中 OTX，前提条件也需要能连接到谷歌。

（7）浏览器约定

OSSIM Web UI 适合采用 Safari 7.0 以上、Google Chrome 44.0 以上、IE 10.0 以上浏览器访问。

本书读者对象

本书主要面向以下类型读者：

- 互联网和安全行业的系统安全从业人员。
- 银行、证券和保险行业 IT 运维人员。
- 政府、高校和科研机构等单位 IT 运维人员。

光盘内容

本书配套光盘包括：OSSIM 入门多媒体教程、OSSIM 安装 ISO、OSSIM 源码三部分内容，其中视频内容有以下章节：

- 第一集：OSSIM 的由来及应用部署
- 第二集：网络威胁感知技术探讨
- 第三集：OSSIM 单机部署安装与分布式安装
- 第四集：OSSIM 仪表盘操作初步
- 第五集：SIEM 控制台与 Alarm 事件告警解析
- 第六集：资产管理与漏洞扫描
- 第七集：OpenVAS 组成及升级实践
- 第八集：NetFlow 应用
- 第九集：OSSIM 权限设置与策略管理
- 第十集：用 OSSIM 发现蠕虫攻击
- 第十一集：报表合规管理
- 第十二集：命令行模式下控制台综合管理

关于作者

李晨光，毕业于中国科学院研究生院，目前就职于世界 500 强企业，资深网络架构师、51CTO 学院讲师、IBM 精英讲师、UNIX/Linux 系统安全专家，现任中国计算机学会（CCF）高级会员；在国内《计算机安全》、《程序员》、《计算机世界》、《网络运维与管理》、《黑客防线》等专业杂志发表论文六十余篇。曾独著畅销书《Linux 企业应用案例精解》、《Linux 企业应用案例精解第 2 版》，《Unix/Linux 网络日志分析与流量监控》等经典学习教程，均被中科院图书馆、国内重点高校图书馆和国立台湾大学图书馆等 200 多家图书馆收藏。《Unix/Linux 网络日志分析与流量监控》一书，于 2015 年获最受读者喜爱的本版类图书奖。

本人经常受邀在国内系统架构师大会和网络信息安全大会发表技术演讲，2012 年担任中国系统架构师大会（SACC）运维开发专场嘉宾主持人。2013 年在 IT168 举办企业内网信息安全实践沙龙活动中发表技术演讲。2014（第十届）中国网络主管论坛北京站发表技术演讲。2014 年《网络运维与管理》杂志对本人进行独家专访并刊发于 13 期杂志中、2015 年 4 月在 WOT 互联网运维与开发者大会发表技术演讲，如图 3 所示。

图 3　作者在各种全国大会中发表技术演讲

支持与勘误

由于 OSSIM 本身结构复杂，知识点众多，在本书撰写过程中难免有所疏漏，希望广大读者能把问题反馈给笔者，本人不胜感激。为了方便读者学习实践，书中涉及所有软件和实验环境都已发布在作者博客 http://chenguang.blog.51cto.com/350944/1679097，在此博客中的 OSSIM 专栏包含了大量实战经验，大家可以一边阅读本书，一般参考博客，互为印证，如有问题大家可以留言，我将定期为读者解答。

也欢迎读者加作者的微博：http://weibo.com/cgweb。

致谢

首先感谢我的父母多年来养育之恩，感谢我在各个求学阶段的老师们，感谢每一位读者，你们将是本书继续完善的新动力，尤其要感谢我的妻子，有了她精心的照顾，我才能全身心投入到创作中。最后要感谢清华大学出版社的编辑们，为了提升本书质量他们花费了大量心血。本书若有不足之处，敬请读者不吝指正。

李晨光

2016 年 1 月

目 录

第一篇 基础篇

第 1 章 OSSIM 架构与原理 3

1.1 OSSIM 概况 3

1.1.1 从 SIM 到 OSSIM 4

1.1.2 安全信息和事件管理（SIEM） 5

1.1.3 OSSIM 的前世今生 6

1.2 OSSIM 架构与组成 13

1.2.1 主要模块的关系 14

1.2.2 安全插件（Plugins） 15

1.2.3 采集与监控插件的区别 17

1.2.4 检测器（Detector） 20

1.2.5 代理（Agent） 20

1.2.6 报警格式的解码 21

1.2.7 OSSIM Agent 22

1.2.8 代理与插件的区别 26

1.2.9 传感器（Sensor） 26

1.2.10 关联引擎 28

1.2.11 数据库（Database） 30

1.2.12 Web 框架（Framework） 31

1.2.13 Ajax 创建交互 32

1.2.14 归一化处理 32

1.2.15 标准的安全事件格式 33

1.2.16 OSSIM 服务端口 37

1.3 基于插件的日志采集 39

1.3.1 安全事件分类 39

1.3.2 采集思路 39

1.4 Agent 事件类型 44

1.4.1 普通日志举例 45

1.4.2 plugin_id 一对多关系 45

1.4.3 MAC 事件日志举例 47

1.4.4 操作系统事件日志举例 47

1.4.5 系统服务事件日志举例 47
1.5 RRDTool 绘图引擎 48
1.5.1 背景 49
1.5.2 RRD Tool 与关系数据库的不同 49
1.5.3 RRD 绘图流程 49
1.6 OSSIM 工作流程 50
1.7 缓存与消息队列 50
1.7.1 缓存系统 50
1.7.2 消息队列处理 51
1.7.3 RabbitMQ 53
1.7.4 选择 Key/Value 存储 54
1.7.5 OSSIM 下操作 Redis 54
1.7.6 Redis Server 配置详解 57
1.7.7 RabbitMQ、Redis 与 Memcached 监控 58
1.8 OSSIM 高可用架构 60
1.8.1 OSSIM 高可用实现技术 60
1.8.2 安装环境 62
1.8.3 配置本地主机 62
1.8.4 配置远程主机 62
1.8.5 同步数据库 63
1.8.6 同步本地文件 63
1.9 OSSIM 防火墙 64
1.9.1 理解 Filter 机制 64
1.9.2 规则匹配过程 66
1.9.3 iptables 规则库管理 67
1.10 OSSIM 的计划任务 68
1.10.1 Linux 计划任务 68
1.10.2 OSSIM 中的计划任务 70
1.11 小结 72

第 2 章 OSSIM 部署与安装 73

2.1 OSSIM 安装策略 73
2.1.1 未授权行为 74
2.1.2 传感器位置 75
2.2 分布式 OSSIM 体系 75
2.2.1 特别应用 76
2.2.2 多 IDS 系统应用 76
2.3 安装前的准备工作 77
2.3.1 软硬件配备 77
2.3.2 传感器部署 78
2.3.3 分布式 OSSIM 系统探针布局 80