《数据驱动的网络分析》

图书基本信息

书名：《数据驱动的网络分析》

13位ISBN编号：9787115376719

出版时间：2015-3

作者：Michael Collins

页数：264

译者：姚军

《数据驱动的网络分析》

内容概要

传统的入侵检测和日志文件分析已经不再足以保护当今的复杂网络，本书讲解了多种网络流量数据集的采集和分析技术及工具，借助这些工具，可以迅速定位网络中的问题，并采取相应的行动，保障网络的运行安全。
《数据驱动的网络分析》分为3部分，共15章，内容包括数据采集的常规过程，用于采集网络流量的传感器，基于特定系统的传感器，数据存储和分析，使用互联网层次知识系统（SiLK）分析NetFlow数据，用于安全分析的R语言简介、入侵检测系统的工作机制以及实施，确定实施攻击的幕后真凶，探索性数据分析以及数据可视化，检查通信流量和行为，获取网络映射和库存盘点的详细过程等。
《数据驱动的网络分析》适合网络安全工程师和网络管理人员阅读。

《数据驱动的网络分析》

作者简介

Michael Collins，是RedJack有限责任公司的首席科学家，该公司是华盛顿首都特区的一家网络安全和数据分析公司。在任职于RedJacak之前，Collins博士是卡内基·梅隆大学CERT/网络态势感知小组的成员。他的主要研究方向是网络测量和流量分析，特别是大流量数据集的分析。Collins博士于2008年毕业于卡内基·梅隆大学，获得电子工程博士学位。他的硕士和学士学位也来自于同一学校。

《数据驱动的网络分析》

书籍目录

《数据驱动的网络分析》

版权说明