日志管理与分析权威指南

日志管理与分析权威指南_下载链接1_

著者:Anton A. Chuvakin

出版者:机械工业出版社

出版时间:2014-6

装帧:平装

isbn:9787111469186

日志是计算机系统中一个非常广泛的概念，磁盘系统、内核操作系统、应用服务器等任何设备和程序都可能输出日志，其内容、形式、规模和用途等各不相同。面对如此庞大的日志，我们如何处理和分析日志数据，从中获取有用信息？

《日志管理与分析权威指南》由日志管理与分析领域资深安全专家亲笔撰写，从日志的基本概念开始，循序渐进讲解整个日志生命期的详细过程，涵盖日志数据收集、存储分析和法规依从性等主题，并通过丰富的实例，系统阐释日志管理与日志数据分析的实用技术和工具，既包括传统的syslog，也涵盖云计算和大数据环境下新兴的日志分析技术。此外，本书从整个运营规程、策略上形成完整的系统，突破行业和具体软硬件配置的限制，不管读者身处何种规模、何种软硬件配置，均能从本书介绍的概念和思路中获益，并通过自己的努力，形成基于标准、适合自身特点的日志运营架构。

作者介绍:

Anton A. Chuvakin博士是日志管理、SIEM和PCI DSS依从性领域公认的安全专家，他参与撰写了《Security Warrior》(ISBN: 978-0-596-00545-0)和《Know Your Enemy: Learning About Security Threats》第2版（ISBN: 978-0-321-16646-3）、《Information Security Management Handbook》第6版（ISBN: 978-0-8493-7495-1）、《Hacker’s Challenge 3:20 Brand-New Forensic Scenarios & Solutions》（ISBN: 978-0-072-26304-6）、《OSSEC Host-Based Intrusion Detection Guide》（Syngress，ISBN: 978-1-59749-240-9）等书籍。

Anton已经发表了数十篇有关日志管理、关联分析、数据分析、PCI DSS、安全管理等安全主题的文章。他的博客www.securitywarrior.org是该领域中最受欢迎的博客之一。此外，Anton在全球的许多安全会议上发表演讲，包括美国、英国、新加坡、西班牙、俄罗斯等地。他参与新兴的安全标准的制定，并且担任多家安全领域创业公司的顾问。

目前，他运营自己的顾问公司Security Warrior。在此之前，他曾经是Qualys的PCI依从性解决方案主管和LogLogic的首席日志管理者，任务是为全世界提供关于安全、标准化和运营日志的重要性的培训。在LogLogic之前，他曾经受雇于一家安全供应商，担任战略产品管理职务。Anton拥有Stony Brook大学的博士学位。

Kevin J. Schmidt是Dell SecureWorks公司的高级经理，这家业界领先的安全托管服务提供商（MSSP）是Dell的下属公司。他负责公司SIEM平台主要部分的设计和开发，包括数据获取、关联分析和日志数据分析。就职于SecureWorks之前，Kevin为Reflex Security工作，致力于IPS引擎和反病毒软件。在此之前，他是GuradedNet公司的首席开发人员和架构师，该公司构建了行业最早的SIEM平台之一。他还是美国海军预备队（USNR）的军官。Kevin在软件开发和设计领域有19年的经验，其中11年从事网络安全领域的研发工作。他持有计算机科学学士学位。

Christopher Phillips是Dell SecureWorks的经理和高级软件开发人员，负责公司Threat Intelligence服务平台的设计和开发。他还负责一个团队，致力于集成来自许多第三方提供商的日志和事件信息，帮助客户通过Dell SecureWorks系统和安全专业人士分析信息。在就职于Dell SecureWorks之前，他为McKesson和Allscripts工作，帮助客户进行HIPAA标准化、安全性和保健系统集成方面的工作。他在软件开发和设计领域有18年以上的经验，持有计算机科学学士学位和MBA学位。

技术编辑简介

Patricia Moulder（CISSP、CISM、NSA-IAM）是一位高级安全主题专家和顾问。她持有东卡罗莱纳大学科学硕士学位。她在网络安全评估、Web应用审计、商用及美国政府客户无线

网络技术方面有超过19年的经验。她在辛克莱尔社区学院担任网络安全助理教授5年之久，她在SDLC应用安全审计和数据隐私标准化方面也有大量跨平台经验。

目录: 译者序
作者简介
序言
前言

日志管理与分析权威指南_下载链接1_

标签

日志管理

计算机

日志分析

日志

运维

信息安全

编程

架构

评论

偏理论的译本工具书，国外安全大牛所著，可get的点全藏在空泛的理论中，来甲方后颇有这种认识，日志数据的核心价值不仅是为了定位攻击，他更大的作用在于大数据建模，由攻击模型在实时性的日志系统中预防/预判攻击，这才是日志数据的功能所在。

介绍了不少平时被大家忽略的基础日志.技术的东西少点.比如没有rsyslog(某人的最爱)logstash(另一个人的最爱)
看完之后,才发现日志管理刨去技术,剩下60%还应该是设计规划,以及审计等非技术方面的事情.真心不应该重业务,轻基础.喜图表,忽流程.

讲太多系统日志，实用的东西不多。

安全分析、soc从业人员必读。

最近在做一个日志分析可视化的项目，无意中在图书馆看到这本书，拿回来翻了一下，过的很快，走马关灯的翻了一遍，适合运维人员对服务器日志等数据有个框架性的理解，篇幅内容很广，不算很深入。

作为基础入门知识了解还行

列举基础介绍型

书的内容很专业，但是比较适合大型的软件和网络应用场景。

真的只是本指南。感觉syslog和CEE标准要多关注下。

从安全角度阐述日志管理与分析，非常多的实例，虽然不深入，但覆盖面广，对新手可扩充眼界，对老鸟会起到“对，说到点子上的”提醒作用

全面介绍了什么是安全日志分析，是一本很好的入门读物，具有很强的指导性。但是具体细节不够清楚，需要继续参考其他的资料。

偏理论的安全日志采集分析类丛书，覆盖面广，但多泛泛而谈。适合新手的日志类书籍入门，以及有相关经验的从业者查漏补缺。

没有想象中的那么强大

讲的都是一些概念行的东西，获得较少

让我怀疑翻译是不是机翻？？？

介绍日志不详进，空泛。

我怀疑是机器翻译的，生硬的很，词不达意！！！
另外，原书的内容显得组织性不够，不够深入。

翻译的看不太懂。

日志管理与分析权威指南_下载链接1_

书评

Anton在相关领域的多年浸淫，就已经确保了足够的含金量。特别是作为负责Gartner SIEM领域MQ评估的研究员，所以很欣喜的看到这本书的中文出版，拿到书之前就充满期待。
刚拿到书没多久，刚开始跳着看(不到5%)，从章节来看，覆盖非常广泛，这就注定了不可能非常深入，也不可能纠...

书中一共写了22章内容，多数章节安排的内容为12~15页，第5章，最逗了，一共7页，三张半纸张，介绍了5.1～5.6
一共6个小节，每个小节平均1页内容，这还包括图，表在里面，根本没有吧syslog-ng讲清楚，如果你是一般的linux工程师看了这部分内容估计会云里雾里，在第13章，写日志...

日志管理与分析权威指南_下载链接1_