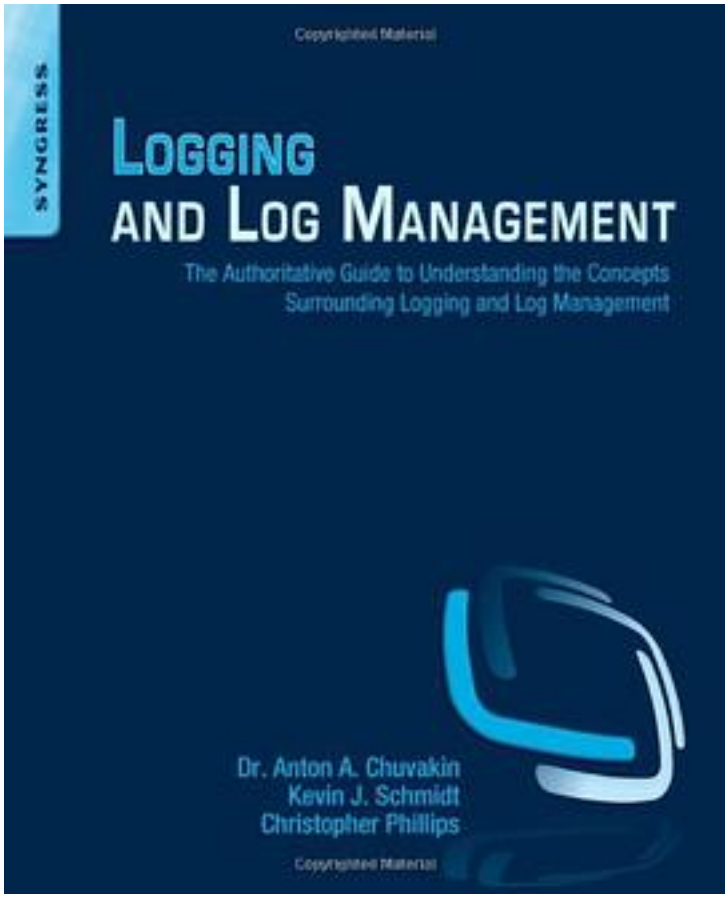
Logging and Log Management



Logging and Log Management_下载链接1_

著者:Anton A. Chuvakin

出版者:Syngress

出版时间:2012-12-13

装帧:Paperback

isbn:9781597496353

Effectively analyzing large volumes of diverse logs can pose many challenges. "Logging and Log Management" helps to simplify this complex process using practical guidance and real-world examples. Packed with information you need to know for system, network and security logging. Log management and log analysis methods are covered

in detail, including approaches to creating useful logs on systems and applications, log searching and log review. It is a comprehensive coverage of log management including analysis, visualization, reporting and more. It includes information on different uses for logs - from system operations to regulatory compliance. It features case Studies on syslog-ng and actual real-world situations where logs came in handy in incident response. It provides practical guidance in the areas of report, log analysis system selection, planning a log analysis system and log data normalization and correlation.

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:

标签

计算机

Log

系统管理

检查日志信息

英文版

互联网

评论

比较入门

基础的太基础，可深入的没展开，开阔视野用

Logging and Log Management_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...

Logging and Log Management_下载链接1_