

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、存储分析和法规遵从性等主题，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遵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遵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

第1章 木材、树木、森林 1

1.1 概述 1

1.2 日志数据基础 2

1.2.1 什么是日志数据 2

1.2.2 日志数据是如何传输和收集的 3

1.2.3 什么是日志消息 5

1.2.4 日志生态系统 6

1.3 看看接下来的事情 12

1.4 被低估的日志 13

1.5 日志会很有用 14

1.5.1 资源管理 14

1.5.2 入侵检测 14

1.5.3 故障排除 17

1.5.4 取证 17

1.5.5 无聊的审计，有趣的发现 18

1.6 人、过程和技术 19

1.7 安全信息和事件管理（siem） 19

1.8 小结 22

参考文献 22

第2章 日志是什么 23

2.1 概述 23

2.2 日志的概念 25

2.2.1 日志格式和类型 27

2.2.2 日志语法 32

2.2.3 日志内容 35

2.3 良好日志记录的标准 36

2.4 小结 38

参考文献 38

第3章 日志数据来源 39

3.1 概述 39

3.2 日志来源 39

3.2.1 syslog 40

3.2.2 snmp 45

3.2.3 windows事件日志 48

3.3 日志来源分类 50

3.3.1 安全相关主机日志 50

3.3.2 安全相关的网络日志 52

3.3.3 安全主机日志 52

3.4 小结 54

第4章 日志存储技术 55

4.1 概述 55

4.2 日志留存策略 55

4.3 日志存储格式 57

4.3.1 基于文本的日志文件 57

4.3.2 二进制文件 59

4.3.3 压缩文件 59

4.4 日志文件的数据库存储	60
4.4.1 优点	61
4.4.2 缺点	61
4.4.3 定义数据库存储目标	61
4.5 hadoop日志存储	63
4.5.1 优点	63
4.5.2 缺点	64
4.6 云和hadoop	64
4.6.1 amazon elastic mapreduce入门	64
4.6.2 浏览amazon	64
4.6.3 上传日志到amazon简单存储服务 (s3)	65
4.6.4 创建一个pig脚本分析apache访问日志	67
4.6.5 在amazon elastic mapreduce (emr)中处理日志数据	68
4.7 日志数据检索和存档	70
4.7.1 在线存储	70
4.7.2 近线存储	70
4.7.3 离线存储	70
4.8 小结	70
参考文献	71
第5章 syslog-ng案例研究	72
5.1 概述	72
5.2 获取syslog-ng	72
5.3 什么是syslog-ng	73
5.4 部署示例	74
5.5 syslog-ng故障排除	77
5.6 小结	79
参考文献	79
第6章 隐蔽日志	80
6.1 概述	80
6.2 完全隐藏日志设置	82
6.2.1 隐藏日志生成	82
6.2.2 隐藏日志采集	82
6.2.3 ids日志源	83
6.2.4 日志收集服务器	83
6.2.5 “伪”服务器或“蜜罐”	85
6.3 在“蜜罐”中的日志记录	85
6.3.1 蜜罐网络的隐蔽shell击键记录器	86
6.3.2 蜜罐网络的sebek2案例研究	87
6.4 隐蔽日志通道简述	88
6.5 小结	89
参考文献	89
第7章 分析日志的目标、规划和准备	90
7.1 概述	90
7.2 目标	90
7.2.1 过去的问题	91
7.2.2 未来的问题	92
7.3 规划	92
7.3.1 准确性	92
7.3.2 完整性	93
7.3.3 可信性	93
7.3.4 保管	94
7.3.5 清理	94
7.3.6 规范化	94
7.3.7 时间的挑战	95

7.4 准备	96
7.4.1 分解日志消息	96
7.4.2 解析	96
7.4.3 数据精简	96
7.5 小结	98
第8章 简单分析技术	99
8.1 概述	99
8.2 一行接一行：绝望之路	100
8.3 简单日志查看器	101
8.3.1 实时审核	101
8.3.2 历史日志审核	102
8.3.3 简单日志操纵	103
8.4 人工日志审核的局限性	105
8.5 对分析结果做出响应	105
8.5.1 根据关键日志采取行动	106
8.5.2 根据非关键日志的摘要采取行动	107
8.5.3 开发行动计划	109
8.5.4 自动化的行动	109
8.6 示例	110
8.6.1 事故响应的场景	110
8.6.2 例行日志审核	110
8.7 小结	111
参考文献	111
第9章 过滤、规范化和关联	112
9.1 概述	112
9.2 过滤	114
9.3 规范化	115
9.3.1 ip地址验证	116
9.3.2 snort	116
9.3.3 windows snare	117
9.3.4 通用cisco ios消息	117
9.3.5 正则表达式性能考虑因素	118
9.4 关联	119
9.4.1 微观关联	121
9.4.2 宏观关联	122
9.4.3 使用环境中的数据	125
9.4.4 简单事件关联器	126
9.4.5 状态型规则示例	127
9.4.6 构建自己的规则引擎	132
9.5 常见搜索模式	139
9.6 未来	140
9.7 小结	140
参考文献	140
第10章 统计分析	141
10.1 概述	141
10.2 频率	141
10.3 基线	142
10.3.1 阈值	145
10.3.2 异常检测	145
10.3.3 开窗	145
10.4 机器学习	146
10.4.1 knn算法	146
10.4.2 将knn算法应用到日志	146
10.5 结合统计分析和基于规则的关联	147

10.6 小结	148
参考文献	148
第11章 日志数据挖掘	149
11.1 概述	149
11.2 数据挖掘简介	150
11.3 日志数据挖掘简介	153
11.4 日志数据挖掘需求	155
11.5 挖掘什么	155
11.6 深入感兴趣的领域	157
11.7 小结	158
参考文献	158
第12章 报告和总结	159
12.1 概述	159
12.2 定义最佳报告	160
12.3 身份认证和授权报告	160
12.4 变更报告	161
12.5 网络活动报告	163
12.6 资源访问报告	164
12.7 恶意软件活动报告	165
12.8 关键错误和故障报告	166
12.9 小结	167
第13章 日志数据可视化	168
13.1 概述	168
13.2 视觉关联	168
13.3 实时可视化	169
13.4 树图	169
13.5 日志数据合成	170
13.6 传统日志数据图表	175
13.7 小结	176
参考文献	176
第14章 日志法则和日志错误	177
14.1 概述	177
14.2 日志法则	177
14.2.1 法则1——收集法则	178
14.2.2 法则2——留存法则	178
14.2.3 法则3——监控法则	178
14.2.4 法则4——可用性法则	179
14.2.5 法则5——安全性法则	179
14.2.6 法则6——不断变化法则	179
14.3 日志错误	179
14.3.1 完全没有日志	180
14.3.2 不查看日志数据	181
14.3.3 保存时间太短	182
14.3.4 在收集之前排定优先顺序	183
14.3.5 忽略应用程序日志	184
14.3.6 只搜索已知的不良条目	184
14.4 小结	185
参考文献	185
第15章 日志分析和收集工具	186
15.1 概述	186
15.2 外包、构建或者购买	186
15.2.1 构建一个解决方案	187
15.2.2 购买	187
15.2.3 外包	188

- 15.2.4 问题 189
- 15.3 日志分析基本工具 189
 - 15.3.1 grep 189
 - 15.3.2 awk 191
 - 15.3.3 microsoft日志解析器 192
 - 15.3.4 其他可以考虑的基本工具 193
 - 15.3.5 基本工具在日志分析中的作用 194
- 15.4 用于集中化日志分析的实用工具 195
 - 15.4.1 syslog 195
 - 15.4.2 rsyslog 196
 - 15.4.3 snare 197
- 15.5 日志分析专业工具 197
 - 15.5.1 ossec 198
 - 15.5.2 ossim 200
 - 15.5.3 其他值得考虑的分析工具 201
- 15.6 商业化日志工具 202
 - 15.6.1 splunk 202
 - 15.6.2 netiq sentinel 203
 - 15.6.3 ibm q1labs 203
 - 15.6.4 loggly 204
- 15.7 小结 204
- 参考文献 204
- 第16章 日志管理规程 205
 - 16.1 概述 205
 - 16.2 假设、需求和预防措施 206
 - 16.2.1 需求 206
 - 16.2.2 预防措施 207
 - 16.3 常见角色和职责 207
 - 16.4 pci和日志数据 208
 - 16.4.1 关键需求10 208
 - 16.4.2 与日志记录相关的其他需求 211
 - 16.5 日志记录策略 213
 - 16.6 审核、响应、升级规程 初始基线 217
 - 16.6.3 人工构建初始基线 219
 - 16.6.4 主要工作流程：每天日志审核 220
 - 16.6.5 异常调查与分析 222
 - 16.6.6 事故响应和升级 225
 - 16.7 日志审核的验证 225
 - 16.7.1 日志记录的证据 226
 - 16.7.2 日志审核的证据 226
 - 16.7.3 异常处理的证据 226
 - 16.8 日志簿——异常调查的证据 227
 - 16.8.1 日志簿推荐格式 227
 - 16.8.2 日志簿条目示例 228
 - 16.9 pci遵从性证据包 230
 - 16.10 管理报告 230
 - 16.11 定期运营任务 231
 - 16.11.1 每日任务 231
 - 16.11.2 每周任务 232
 - 16.11.3 每月任务 232
 - 16.11.4 季度任务 233
 - 16.11.5 年度任务 233
 - 16.12 其他资源 233
 - 16.13 小结 233

参考文献	234
第17章 对日志系统的攻击	235
17.1 概述	235
17.2 各类攻击	235
17.2.1 攻击什么	236
17.2.2 对机密性的攻击	236
17.2.3 对完整性的攻击	241
17.2.4 对可用性的攻击	245
17.3 小结	252
参考文献	252
第18章 供程序员使用的日志	253
18.1 概述	253
18.2 角色与职责	253
18.3 程序员所用的日志记录	254
18.3.1 日志应该记录哪些信息	255
18.3.2 程序员使用的日志记录api	256
18.3.3 日志轮转	257
18.3.4 不好的日志消息	259
18.3.5 日志消息格式	259
18.4 安全考虑因素	261
18.5 性能考虑因素	262
18.6 小结	263
参考文献	263
第19章 日志和依从性	264
19.1 概述	264
19.2 pci dss	265
19.3 iso 2700x系列	269
19.4 hipaa	271
19.5 fisma	276
19.6 小结	281
第20章 规划自己的日志分析系统	282
20.1 概述	282
20.2 规划	282
20.2.1 角色和职责	283
20.2.2 资源	284
20.2.3 目标	284
20.2.4 选择日志记录的系统和设备	285
20.3 软件选择	285
20.3.1 开源软件	285
20.3.2 商业化软件	286
20.4 策略定义	287
20.4.1 日志记录策略	287
20.4.2 日志文件轮转	288
20.4.3 日志数据收集	288
20.4.4 留存/存储	288
20.4.5 响应	289
20.5 架构	289
20.5.1 基本模型	289
20.5.2 日志服务器和日志收集器	290
20.5.3 日志服务器和具备长期存储的日志收集器	290
20.5.4 分布式部署	290
20.6 扩展	291
20.7 小结	291
第21章 云日志	292

21.1 概述	292
21.2 云计算	293
21.2.1 服务交付模型	293
21.2.2 云部署模型	294
21.2.3 云基础设施特性	295
21.2.4 标准？我们不需要讨厌的标准	295
21.3 云日志	296
21.4 监管、依从性和安全问题	300
21.5 云中的大数据	301
21.6 云中的siem	303
21.7 云日志的优缺点	304
21.8 云日志提供者目录	305
21.9 其他资源	305
21.10 小结	305
参考文献	306
第22章 日志标准和未来的趋势	307
22.1 概述	307
22.2 从今天推知未来	308
22.2.1 更多的日志数据	308
22.2.2 更多动力	309
22.2.3 更多分析	310
22.3 日志的未来和标准	310
22.4 渴望的未来	314
22.5 小结	314
• • • • •	(收起)

[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](#)