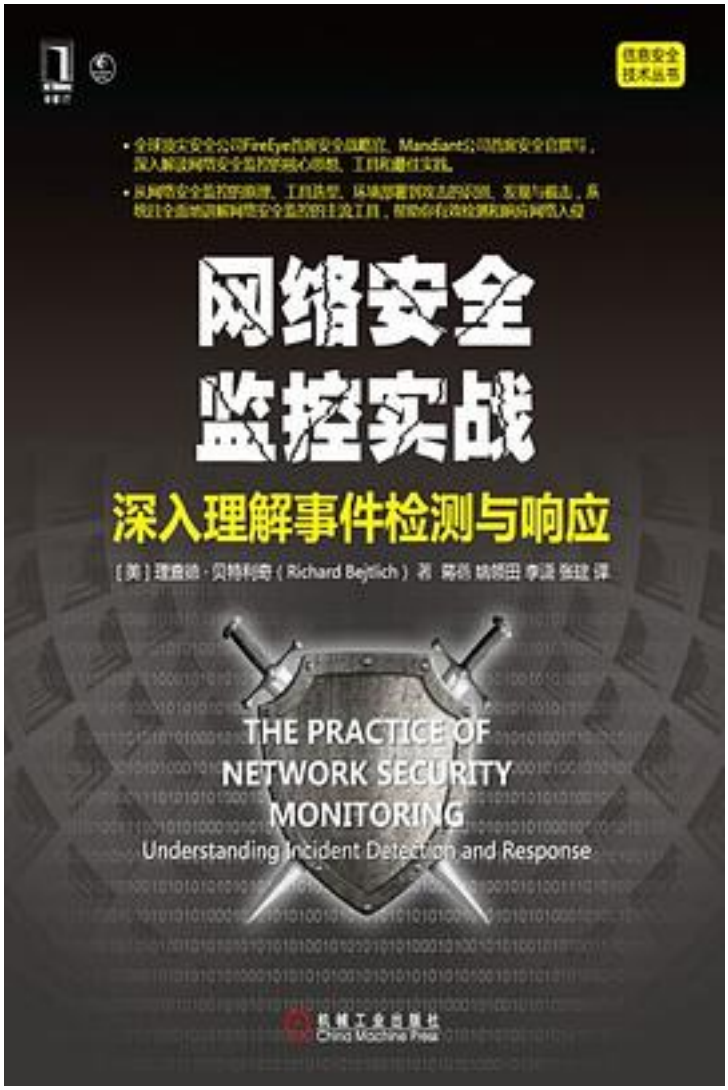
网络安全监控实战



网络安全监控实战_下载链接1_

著者:Richard Bejtlich

出版者:机械工业出版社

出版时间:2015-4

装帧:

isbn:9787111498650

作者介绍:

理查德·贝特利奇(Richard Bejtlich)现任全球顶级安全公司FireEye的首席安全战略官、美国前沿网络安全公司Mandiant的首席安全官，曾任通用电气事件响应的主管，是最早一批研究网络安全和NSM防御的践行者。他毕业于哈弗大学和美国空军学院，著有《The Tao of Network Security Monitoring》、《Extrusion Detection》和《Real Digital Forensics》。

他还在博客和推特上创作，其博客地址为http://taosecurity.blogspot.com；推特账号为@taosecurity。

目录:

网络安全监控实战_下载链接1_

标签

信息安全

网络安全

安全研究

安全

Web安全

NSM

计算机科学

计算机

评论

今年读的最好的技术书籍，专业的译者，翻译非常易读。迄今为止国内安全类别翻译书籍里面的用心之作。

本书主要讲了网络安全监控的主要原理，采用检测和响应的网络监控思想，在网络中部署NSM，对网络流量和数据进行收集、分析和预警。本书以SO作为NSM实践的工作，讲解了SO的部署，以及SO相关工具，包括Tcpdump，wireshark，networkminer等的具体实用方法，在NSM实践中的操作流程，如何监控服务器/客户端的网络检测和响应的具体案例。本书网络安全监控内容比较细致，工具的可操作性强，是一本网络安全的入门好书。

这本书看似重点讲了网络监控的工具和应用，但实际上在操作过程中则体现了当前安全趋势---由防御到检测和响应的转变。而检测和响应的关键是数据分析。本书内则是通过实践来娓娓道来分析和取证。
对于客户端监控和分析的章节，也间接地介绍了对内网的持续渗透方法和思路：）
对了，书中好多地方以apt1为例来说明。不了解的可以看下这个报告.....完全针对我军的嘛

关于网络安全监控理论方面的内容偏少，方法论也不多，大量的篇幅在介绍SO的安装部署与使用，属于工具说明书。

网络安全监控实战_下载链接1_

书评

网络安全监控实战_下载链接1_