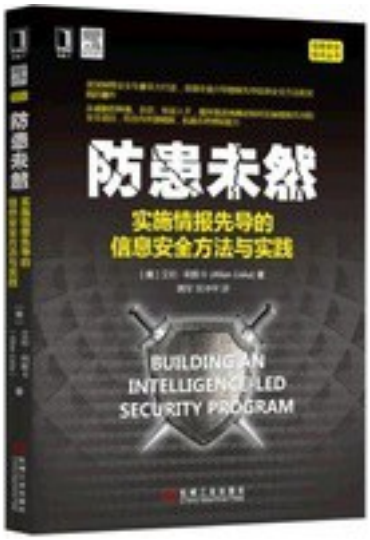
# 防患未然




防患未然_下载链接1_

著者:

出版者:机械工业出版社

出版时间:2016-1

装帧:

isbn:9787111524779

作者介绍:

目录:

防患未然_下载链接1_

## 标签

信息安全

安全

情报

情报威胁

技术

随便看看

图书馆

## 评论

面对虚拟空间安全工作的复杂性和不确定性，基于规则和功能的安全防范和措施面对越来越多的挑战，内外部情报体系的建立，实现安全威胁准实时的防范和响应是挑战也是机遇。这本书的概念、知识体系、实践值得参考。

---
网络安全在于预防、检测、响应。这本书主要讲关联各种检测指标、利用已有安全事件信息，及时发现甚至预测安全事件，并为响应团队提供分析信息。

---
还可以。不好不坏。聊天式介绍。

---
本书全面的介绍了情报先导的信息安全方法和工程实践，讨论了情报和威胁情报的定义，定义了网络威胁情报模型，持续监控获取威胁情报的安全框架，情报整合和共享方法，以及获取高级威胁情报的工具。主要阐述了内外部威胁情报收集方法，内部情报主要来源于系统日志，包括收集和监控网络中防火墙、IDS、WAF、邮件服务器、VPN、终端防护系统等的系统日志，而外部威胁情报主要来源于漏洞情报和包含IP地址、域名、文件hash等的攻击指标情报。整本书对威胁情报进行了系统的介绍，内容丰富，可以作为一本威胁情报学习的入门指导书。

---
薄薄的一本小册子，介绍威胁情报的书，对威胁情报进行了通俗性的介绍，但比较浅，可以参考下

---
孙子云“知己知彼，百战不殆”。信息安全的知己，就是建立内部安全感知分析平台，对内部的网络进行安全分析；知彼，就是有相当可靠的情报来源，时刻作为情报分析的参考。
情报先导，就是要防患于未然，结合内部安全感知和外部威胁情报，将威胁攻击扼杀在摇篮中！进而保护我们的关键核心资产！

---
防患未然_下载链接1_

# 书评

---
防患未然_下载链接1_