ossec[编辑](javascript:void(0))

本词条缺少**名片图**，补充相关内容使词条更完整，还能快速升级，赶紧来编辑吧！

OSSEC是一款[开源](http://baike.baidu.com/view/9664.htm" \t "_blank)的多平台的[入侵检测系统](http://baike.baidu.com/view/20936.htm)，可以运行于Windows, Linux, OpenBSD/FreeBSD, 以及 MacOS等操作系统中。包括了日志分析，全面检测，root-kit检测。作为一款HIDS，OSSEC应该被安装在一台实施监控的系统中。另外有时候不需要安装完全版本得OSSEC，如果有多台电脑都安装了OSSEC，那么就可以采用[客户端](http://baike.baidu.com/view/930.htm" \t "_blank)/服务器模式来运行。客户机通过客户端程序将数据发回到服务器端进行分析。在一台电脑上对多个系统进行监控对于企业或者家庭用户来说都是相当经济实用的。

**书    名**

OSSEC Host-Based Intrusion Detection

**作    者**

Hay, Andrew

**ISBN**

9781597492409

**类    别**

[图书](http://baike.baidu.com/view/5214.htm)  > 英文原版书 > Computers & Internet（计算机与网络）

**定    价**

￥613.00

**出版社**

Syngress Publishing

**出版时间**

2008-02-28

**上架时间**

2013-10-25

**语    言**

英文

[](http://baike.baidu.com/picture/1348667/1348667/0/cbc17b3802eed73097ddd8e9.html?fr=lemma&ct=single)

主要功能

主要功能有日志分析、完整性检查、rootkit检测、基于时间的警报和主动响应。除了具有入侵检测系统功能外，它还一般被用在SEM/SIM（安全事件管理（SEM： Security Event Management）/安全信息管理（SIM：SecurityInformation Management））解决方案中。因其强大的日志分析引擎，ISP（Internet service provider）（网络服务提供商）、大学和数据中心用其监控和分析他们的防火墙、[入侵检测系统](http://baike.baidu.com/view/20936.htm)、网页服务和验证等产生的日志。[1]

OSSEC是一款开源的入侵检测系统，包括了日志分析，全面检测，rook-kit检测。作为一款HIDS，OSSEC应该被安装在一台实施监控的 系统中。另外有时候不需要安装完全版本得OSSEC，如果有多台电脑都安装了OSSEC，那么就可以采用客户端/服务器模式来运行。客户机通过客户端程序 将数据发回到服务器端进行分析。在一台电脑上对多个系统进行监控对于企业或者家庭用户来说都是相当经济实用的。

OSSEC最大的优势在于它几乎可以运行在任何一种操作系统上，比如Windows, Linux, OpenBSD/FreeBSD, 以及 MacOS。不过运行在Windows上的客户端无法实现root-kit检测，而其他系统上的客户端都没有问题。OSSEC的手册上说OSSEC目前还 不支持Windows系统下得root-kit检测，估计是正在开发中。