# 日志管理

## 前置知识

记录日志的目录是为了进行回溯和分析，通过对日志的综合分析来识别出用户的操作过程行为，并分析出异常行为或攻击行为，以便于系统能够对这样的非法行为采取阻止措施

**威胁描述：**

如果日志信息没能恰当的保存和处理导致被修改或破坏，这将失去通过日志还原用户过去操作行为的能力，导致记录的日志失去意义。

**涉及功能点：**

登录

## 修复方案

1. 在系统记录了日志后，应定时将记录的日志发送到SIEM系统中进行存储和分析处理。
2. 在SIEM系统中要进行恰当的配置，确保日志不能被修改。只分配給审计员查询日志信息的权限，所有人都不能有修改或删除日志的权限。定时对日志记录进行备份。