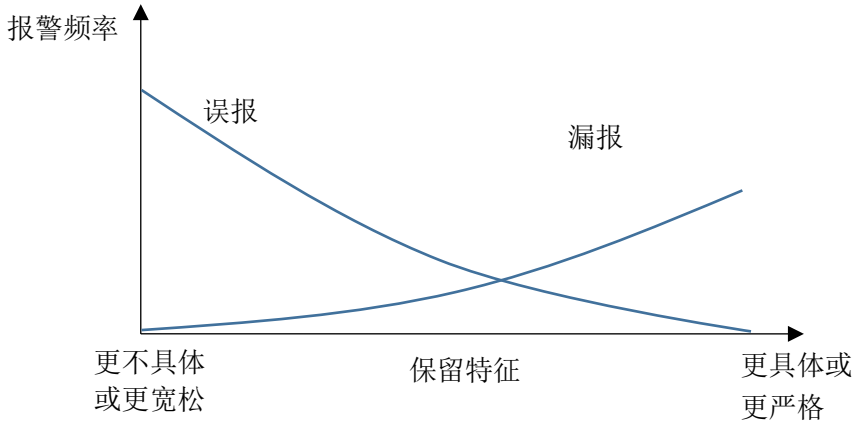
第八章 课后作业

1、在 IDS 上下文中，我们定义误报是 IDS 对于本来正常的情况产生警报。漏报是指 IDS 对于正在发生的应该报警的情况没有报警。在下图中，分别用两条曲线大致表示误报和漏报。



2、Snort 中的一个非载荷选项是 flow。此选项区分客户端和服务器，可用于指定仅匹配在一个方向上流动的数据包（客户端到服务器或者相反），并可指定仅匹配已建立的 TCP 连接。请考虑以下 Snort 规则：

```
alert tcp $EXTERNAL_NET any -> $SQL_SERVERS $ORACLE_PORTS \
( msg: “ORACLE create database attempt”; \
flow: to_server, established; content: “create database”; nocase; \
classtype: protocol-command-decode; )
```

a. 此规则是做什么的？

本规则用于检测外部网络的客户端在当前的数据库服务器创建 ORACLE 数据库。当检测到来自外部网络的客户端向数据库服务器的 ORACLE 端口发送的 TCP 内容中包含"create database"关键字时，表示该客户端试图在数据库服务器上创建数据库，当检测到该数据包时，将忽略（nocase）该数据包，并向日志中写入“ORACLE create database attempt”

b. 如果 Snort 设备放在外部防火墙的内部或外部，分别说明此规则的重要性。

如果将 Snort 设备放在外部防火墙内部：Snort 设备可以观测来自外部的所有攻击，建立入侵网络的外围防护。可以屏蔽来自网络的所有该类型攻击，

如果将 Snort 设备放在外部防火墙外部：Snort 设备需要监控所有网络流量，监控来自网络上针对内部网络的攻击数和攻击类型，并将所有相关的攻击数据包屏蔽，起到最大化的保护效果，但同时要承担更高的处理负担。