飞络 SOC 运营服务使用手册

一、前言

本商品仅适用于飞络自有 SOC 平台或客户自建 SOC 平台，客户下单后飞络可按照客户需求提供 SOC 平台的搭建和运营服务。

二、服务介绍

本商品 SOC 服务，飞络是拥有非常丰富的安全运营能力，本服务主旨是帮助客户提供更好的安全服务，帮助客户在云端或本地在客户环境中或者在我司环境中搭建安全运营中心，进行标准化的安全运营服务，服务客户更好的解决安全问题，对已经存在的安全问题进行逐一排查和整改，对未发生的安全隐患事件进行提前预防。

1、搭建飞络 SOC 平台：统一使用 Linux 的系统，并在系统上统一安装日志接收应用软件，通过配置完成集群构建。

2、日志接入：确认提供的设备以及 IP 地址，针对不同的日志源采取相对应的日志接入方式。

3、Dashboard 制作：制作对应的搜索语句展示结果使用的 Dashboard，并在 Dashboard 界面完成数据的下钻查询，便于查看对应搜索的详细信息。

4、配置邮件告警：使用客户提供的告警邮箱，配置告警触发后邮件的发送，实现告警事件的及时发现。

5、针对提供的 usecase 模板可以进行定制化修改，以便更加适合客户的环境需求。

三、安全运营标准

1、安全运维 SLA 标准

严重等级	服务时间	响应	更新
P1-高	24*7	30 分钟	每 1 小时
P2-中	24*7	2 小时	每 4 小时
P3-低	24*7	4 小时	每 8 小时

2、针对不同 usecase 等级描述

严重等级	描述
P1-高	立即采取必要的措施来减轻当前的恶意行为
P2-中	如果不采取预防措施，很可能发生安全事故的行为
P3-低	发生安全事故可能性低的行为

3、服务请求

服务请求是指来自用户向 IT 部门提出的各种需求的通用描述，包括 IT 相关信息的获取、访问权限申请或标准变更的请求等。

SLA 标准：

严重等级	服务时间	响应	处理
配置类	7*24(L1)	2 小时	48 小时
报警类	7*24(L1)	1 小时	24 小时
咨询类	7*24(L1)	1 小时	24 小时
报告类	7*24(L1)	按需	按需

注：若非工作时间出现非紧急（P2, P3）告警事件，需 L1 运维人员与下一个工作日告知 L2 人员进行说明情况,出现紧急告警事件（P1），可立即通知 L2 人员。