Help Instance

关于ASO产品现在以及未来若干个问题

Last modified: 11 六月 2024

希望通过这篇文章能帮助我和大家理清产品, 帮助我们把ASO成功渡过商业化验证.

如果你有时间先阅读 PingCAP CTO 黄东旭： 关于基础软件产品价值的思考 ↗ ,那就再好不过了.

> PS: TiDB 虽然是数据库跟 ASO 这种产品本质上不同, 但是有很多共性, 文章中提到的问题, 我们在做数审产品的时候就遇到了, 到现在也没有好的解决方案.

产品定位

在思考 `迭代方向` 之前我们需要对 `ASO` 有明确的产品定位:

```
ASO 是 `A Security Infrastructure PaaS Platform`.
```

基于这个定位, ASO 从业务侧看有三个模块组成:

1. ASO Core, 负责基础 `日志(log)` `指标(metrics)` `流量(traffic)` 收集, 解析以及格式化成固定结构, 我们把这种已经被预处理过的叫做 `Message` . (60%)

2. ASO Pipeline Script Engine, 负责解析 `Message`, 并且分析解析结果 转化成 `安全指标` `安全事件`. (45%)
3. ASO API 提供基础的`DSL`查询接口. `DSL` 理论上非常灵活, 基本满足 99% 产品查询需求. (70%)
4. ASO Graph Library 提供图表库. (可通过 ASO Pipeline Script Engine 自定义的 脚本策略, 灵活生成图表) (TODO)
5. ASO Event 事件订阅机制, `ASO Pipeline Script Engine` 安全事件 或者 安全指标, 通过这个机制可以生成 工单, 自定义报警策略等 (TODO).

这样拆分是我们从规划开始就已经确定的, 原因很简单, 我们希望:

1. 所有基础能力由 ASO Core 提供, 屏蔽复杂的底层技术, 开发人员只用关注 安全产品自身的业务.
2. 99% 安全产品的复杂开发业务都会映射到 API 这一侧, 所以我们在技术选型的时候 API 组件提供了灵活的 `DSL` 查询接口, 所以基于ASO Core 开发安全产品的开发人员不需要特别关注 `API` 这个业务.
3. 提供灵活的 Rule Script Engine 选择:
    1. Javascript (70%)
    2. Expr-Lang (@TODO) 来帮助开发人员处理 `Message`.

当我们完成这些功能, 那么:

开发人员只需要 将 ASO Core 处理过后的特定结构日志`Message` 通过 `ASO Pipeline Script Engine` 处理成自身安全业务想要的数据结构, 就能完成业务.

ASO 未来 迭代方向

我们希望 10月份 是我们 第一个 里程碑, 所以近期迭代策略:

暂时不会去扣产品细节, 而是完成我们列出的业务功能.

商业化验证

在做商业化验证之前, 会有几个前置问题亟须解决:

1. 如何重建 研发 与 BD 已经崩坏的信任问题.
2. 人员配置问题

在销售驱动类型的公司, 做新的产品按我个人的理解是相对比较容易对新产品做商业验证的, 因为大部分需求都来自于客户真实的需求, 但是上述两个问题, 导致内部资源协调沟通阻塞, 进而导致产品商业验证难产.

我最近听到最多的是, 无论是公司售前还是技术都不愿意销售公司自研产品, 包括但不限于 `数审`