从数据角度看安全运维

- 工作现状
- 数据分析处理
- 安全加固措施

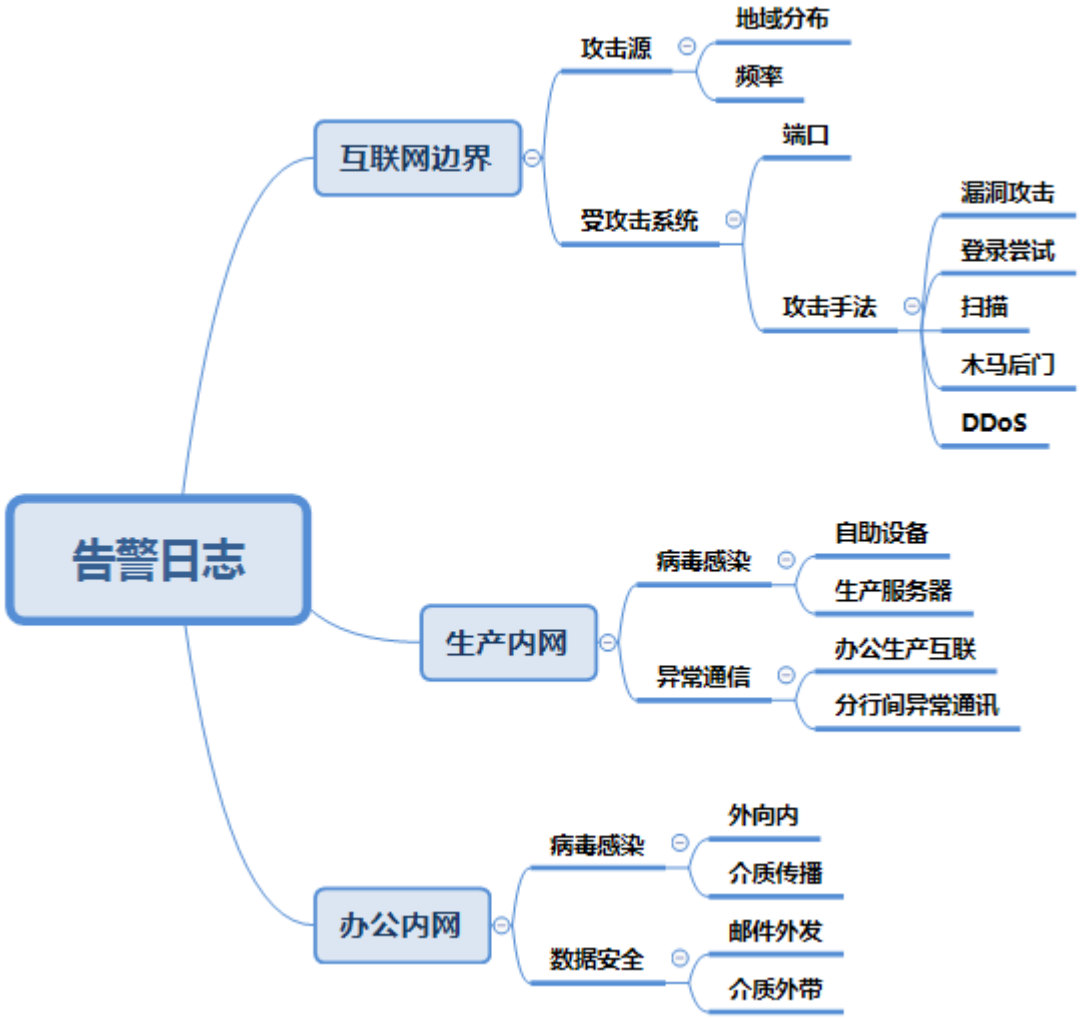
工作现状

- 项目组工作基本如下

- 工作现状
- 数据分析处理
- 安全加固措施

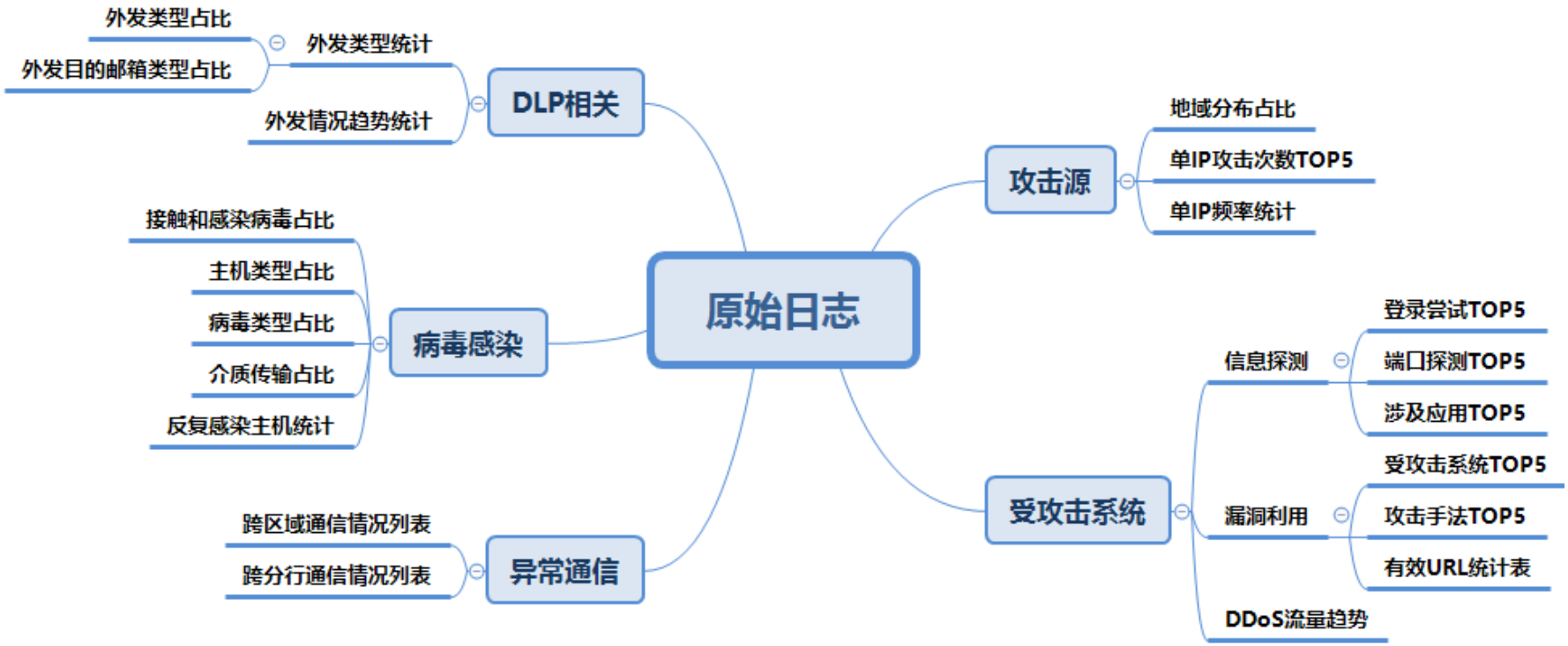
分析角度

- 面对庞杂的告警日志，我们从这些角度入手



数据处理

- 项目组现有数据处理方式如下所示



- 工作现状
- 数据分析处理
- 安全加固措施

互联网攻击防范

- 基础：监控及响应
- 主动防御：端口扫描
- http协议URL分析和验证

内网监控

- 阻断异常通信
- 联合防病毒项目组病毒传播

办公域控制

- 及时监控介质和邮件的病毒传播
- 联合控制内部资料外发

防患于未然

- 关注威胁情报
- 制定事件应急响应预案
- 定期应急演练

谢谢！