管理方面：

规章制度流程建立与执行

入职安全培训

业务的安全分享。数据化量化安全问题。奖励予处罚规定。打分模式（执行与改正，积极性）

员工的评分。规范落实，分享，贡献，处罚。

技术方面：

维度以及实施方案

集团全资产获取

监控以及展示

三分技术，七分管理

参与项目规划开发

自动化测试，解放人力

运营安全平台

有根有据有人

部门负责人-项目负责人

资产（域名，服务器，应用，代码）管理划分

域名，项目-项目负责人，项目-部门，

管理域名（解析，续费）

四者之间关系

人事调动关系。

运维开发安全权力职责划分

|  |  |  |  |
| --- | --- | --- | --- |
|  | 决策权 | 管理权 | 使用权 |
| 域名 | 业务领导/部门领导 | 运维/业务 | 相关业务 |
| 服务器 | 运维 | 运维 | 相关业务 |
| 应用 | 业务 | 运维/业务 | 业务/用户 |

监管与更新

<http://www.freebuf.com/articles/neopoints/158586.html>

<http://www.freebuf.com/articles/es/184078.html>

正常运营安全：各方面互补，一环扣一环。

异常原处理：灾难备份。

SRC系统及运营

内部工单系统及跟进

安全培训

上线前渗透测试

SDLC

一个对外输出的安全平台似的东西。

知识沉淀。

展示页面工作

安全监控

态势感知：

主机态势：安装snort等客户端

网络态势：镜像流量分析

应用态势：结果是分析出服务器应用的攻击情况，不知道怎么做的

数据态势：结果是分析出服务器应用的攻击情况，不知道怎么做的

威胁情报：

CVE情报：抓取cve信息。cve.scap.org.cn

整合咨询：hackernews.cc，[www.exploit-db.com](http://www.exploit-db.com)

舆情监控：

情报交换：威胁情报搜索引擎

资产安全：

域名信息：注册使用情况

服务器信息：bash记录，syslog原始记录，开放端口

资产审计：域名信息

主机安全：

SSH登录：异常信息

系统操作：敏感操作。bash监控，数据库监控

系统运行：运行状态，长时间关机

系统检查：ossec

网络安全：

暴露端口：

流量分析：流量类型，协议划分

连接分析：？？

入侵检测：？？？

蜜罐系统：蜜罐系统

网络审计：空白的？？

应用安全：

WAF防护：

应用分析：

应用内容：

应用审计

数据安全：

注入防护：

应用配置：字典扫描目录

仓库监控：监控github等仓库

数据审计：？？

IDC流量：

关联分析：

报警事件：

主机态势：snort等

应用态势：web页面攻击次数

集团安全站点：

安全服务为安全组对业务提供哪些