全流程安全管控方案

# 目前现状

在G20审计期间，发现目前我们在安全整体上确实存在较大的不足，与业内的差距较明显。主要体现如下几个方面：

1. 资产梳理不清晰，造成很多安全监视盲点
2. 安全体系建设上进度还偏慢，在管理制度推行上很多都在评审或者试运行阶段，也缺少明确的发文
3. 安全培训覆盖面不足，造成公司整体安全意识偏弱
4. 抓生产而忽视了办公网整体安全的环节，造成了部分的短板
5. 配套安全设备未发挥最大价值
6. 运维安全管理制度缺少，导致暴露了较多运维不当导致的安全问题（原注重应用安全和基线安全）
7. 缺少整体安全监视平台，就是所谓的威胁情报和安全风险。这些都未纳入整体安全管控，造成有风险未及时处理
8. 缺少定期的安全巡检和定期的外围渗透制度
9. 子公司的资产未纳入安全管控，造成部分的安全监视盲点

所以针对上面的问题，我们安全测试部制定了全流程的安全管控方案同时配合SDL流程整体推进，从而将安全覆盖到每一环节，而非只局限在软件研发生命周期内。

# 恒生电子安全管控

## 安全团队建设

任何制度的落地执行都离不开人，安全也是如此。所以第一就是要打造高效的安全团队。总体建设目标是将团队分为SDL工程师团队和攻防团队。

SDL工程师团队指定接口人对接各业会或子公司，与实际的业务结合，总结出适用于各业务会的安全保障方法。他们的职责是保障各自所负责各业委会或子公司的安全。

攻防团队的职责负责定期的巡检和渗透，通过外围渗透从而发现安全执行不到位和安全遗留问题。从黑客的角度保障公司的外围安全。通过巡检发现一些安全不合规项，从而促进改进。也可以二者相结合。

短期目标：攻防团队从目前SDL工程师中抽取（2-3名）有较高水准的人组成。 SDL工程师团队需要继续补充。标准是各业委会一个对接人（因需8人，实缺4人）

## SDL流程建设

目的是为了将安全开发过程融入到传统的项目开发流程中，在需求分析，设计，编码，测试，发布加入安全管控。从而降低系统的安全漏洞上线率，提供系统的整体安全。

目前急需制定相应配置制度，界定每个阶段的输入输出，并发文，从而让SDL工程师有依执行。

该章节具体可参考与蚂蚁共同制定的《软件开发管理制度》

短期目标：尽快整理和发布SDL相关流程和制度并与各业委会首架协商制定SDL推行试点产品（项目）

## 运维安全管理

目的是为了规范相关产品发布后，在运维阶段的安全管控。从权限，运维数据，账号，密码，补丁，应急等多角度制定相关的安全规范制度，让运维有依可循。

短期目标：整理和发布《恒生运维安全管理制度》

## 线上资产统一管理

对线上的IP、域名等相关资产进行定期梳理，并将数据同步到对应安全团队；

针对公司使用框架、对应组件、第三方代码等进行安全测试。同时跟踪最新安全资讯，做好安全预警。

短期目标：尽快督促技术管理部完成该资产信息搜集

## 安全风险监控&威胁情报收集平台

目的是收集乌云唐朝巡检，魔方，IDS，IPS，Github，阿里云盾，漏洞预警等有的安全风险和威胁信息的收集，通过自身制定的过滤机制，有效地推送到安全工程师手中进行分析，然后根据风险情况，及时通知相关处理单元。

首先要整理公司包含子公司相关资产。其次开发平台对各信息来源进行数据分析，并推送到安全工程师手中

短期目标：需建立相关制度，目前通过半自动或者人工预警的方式处理。

* Github敏感信息泄露监控

使用脚本或开源监控系统对Github上可能存在的敏感信息就进行扫描查找。

使用关键字如：hundsun、smtp hundsun、vpn hundsun、mail hundsun、ftp hundsun

* 各类社工库信息检索

搭建社工库，对社工库信息进行检索，对使用hundsun工作邮箱注册各类网站的邮箱进行安全风险提醒；

对各类数据泄露事件进行安全风险预警，同时对相关数据进行深度分析，整理hundsun邮箱，更新及添加top常用密码。

* 阿里云盾安全告警信息及时监控响应

使用脚本工具对公司生产网络中云盾报警信息进行处理。做到对紧急事件能够进行第一时间预警处理。对安全威胁事件，进行数据存储整理，并进行验证分析。进行月度的安全威胁分析。

* IDS及IPS告警日志监控分析

对IDS及IPS日志进行监控分析。同时对高危告警进行第一事件通知、处理验证。月度进行日志分析总结。

## 定期外围渗透

整理相关资产，定期对公司外网进行安全渗透，从而提高整体信息安全。过程中需制定渗透测试规范指南以及整理子公司外网资产信息列表。拟计划每季度集合公司安全专家进行一轮外网渗透，同时也要保障不影响实际线上业务。

## 定期安全巡检

根据相关规范每季度一次对恒生公司进行规范性的检查，查找各环节安全执行的不合规项

## 定期攻防演练

每半年与安全相关单元，信息中心，系统基础部，安全管理部，安全技术部等合作组织攻防演练，已检验我们公司整体安全应急处理情况，和不断提供的我们安全的战备能力

## 建立恒生安全应急响应中心

通过建立私有SRC或借助外部的安全测试平台，通过赏金的方式来鼓励更多的白帽子挖掘我们的漏洞，从而帮忙我们提高整体的信息安全。不过前提要保障我们各安全设备运行有序和相应措施基本落实到位，可控制因此带来的安全风险。

# 子公司安全管控

## 资产统一申报

子公司的资产统一申报登记。将安全相关制度延伸到各子公司，将其纳入恒生整体信息安全。

## 定期外围渗透

通过申报的资产和外部的信息搜集定期子公司的外网进行安全渗透，从而保障子公司整体信息安全。过程中需制定渗透测试规范指南以及整理恒生子公司外网资产信息列表。拟计划每季度集合公司安全专家进行一轮外网渗透，同时也要保障不影响实际的业务生产。

## 定期安全巡检

根据相关规范每季度一次对恒生所属子公司进行规范性的检查，查找各环节安全执行的不合规项。