



安全运维工程师



网络安全综合运维

序言

安全运维是对已建设好的信息系统开展安全方向的运维工作。一般外包给专业的第三方团队执行。驻场形式的运维可分为5*8和7*24两种类型；巡检形式的运维可分为月度、季度巡检模式。根据甲方的具体需求开展具体的服务工作。



目录页

01

OPTION



昨夜星辰昨夜风
项目启动

02

OPTION



今日繁花落丛中
项目规划

03

OPTION



根深蒂固百花翁
项目执行

04

OPTION



尘埃落定百家丰
项目收尾



赛博梦工厂

Cyber Works



01.昨夜星辰昨夜风-启动



进场前准备

调研模板

物理环境

网络环境

主机环境

应用环境

文档与数据

割接窗口

用户画像

启动PPT

项目目标

甲方需求

工作规划

里程碑交付

项目管理

质量保证

验收标准

组建团队

任命包括但不限于以下

岗位:

项目经理

网络工程师

系统工程师

核心专家小组

工具准备

调整模板使其成为项目专属

检查工具使其使用更加舒适

电脑杀毒使其避免带毒进场

提高性能使其执行过程顺畅

检查周边装备确保其高可用

检查备品备件库以确保跟进



赛博梦工厂

Cyber Works

工作类型

First

例行巡检一般巡检、高级巡检、策略优化、配置变更、设备升级、病毒查杀

Secede

故障处理巡检过程中发现的故障和问题要及时处理，并记录故障处理情况记录表

Third

安全审计 网络及安全设备审计服务器、存储设备审计 应用系统审计

Forth

安全通告以邮件、电话、走访等形式将安全技术和安全信息及时传递给安全运维服务的使用者。



workflow

配合部门

主流程

输出

项目组

↓
商务部门

↓
行政部门

↓
财务部门

↓
人力资源

↓
项目部

工具准备

↓
装备准备

↓
文案准备

↓
需求调研

↓
需求分析

↓
报价与成本核算

工具清单

↓
装备清单

↓
文案清单

↓
服务目录

↓
项目合同





02. 今日繁花落丛中-规划



赛博梦工厂
Cyber Works

实施方案编制

外网应用系统安全运维方案

目 录

1.	概述.....	3
1.1	背景.....	3
1.2	方案目的.....	3
1.3	工作目标.....	4
1.4	工作原则.....	4
2.	安全运维需求分析.....	6
3.	运维服务内容.....	8
3.1	日常安全检查.....	8
3.2	安全通告.....	8
3.3	安全风险评估.....	9
3.4	渗透测试.....	12
3.5	安全配置与加固.....	14
3.6	安全维护保障.....	15
3.7	安全应急响应保障.....	16
3.8	安全培训服务.....	25
4.	项目预算.....	27



赛博梦工厂

Cyber Works

workflow

配合部门

主流程

输出

项目组

商务部门

项目部

资料收集

制定服务目录

确定服务工时

编制服务方案

评审服务方案

方案提交

运维实施方案

方案评审意见

方案分发记录





03.根深蒂固百花翁-执行



一般巡检

网络设备

安全设备

服务器

存储设备

应用系统

数据库系统

机房动环

管理记录



专家巡检

设备信息

接口设置

系统信息

接口状态

设备版本

日志信息

安全配置

访问控制



策略优化

需求收集

需求确认

策略编写

策略测试

策略备份

备份验证

策略部署

部署验证



设备更新

需求收集

需求确认

更新方案

方案确认

服务备份

网络割接

设备升级

升级后验证

二次割接

割接验证



赛博梦工厂

Cyber Works

病毒管理

病毒库更新

木马库更新

按需部署节点

定期扫描

病毒发现预警

病毒防御规划

外来风险预判

内网风险管理



故障处理

故障预警

设备健康预警

故障研判

故障处理方案

故障处理记录

故障预防规划

故障预警优化

设备健康普查



安全审计

网络安全审计

服务器审计

数据库审计

存储审计

应用系统审计

需求审计

风险审计

管理审计



安全通告

全球动态

国家战略

国家政策

法律法规

漏洞通告

病毒通告

厂商通告

其他通告



赛博梦工厂
Cyber Works

workflow

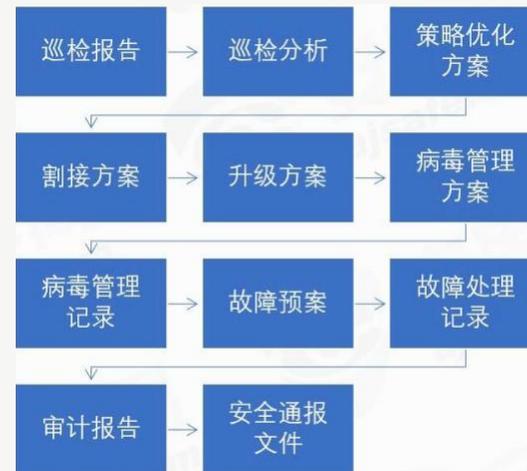
配合部门



主流程



输出





04.尘埃落定百家丰-收尾



收尾

工作

年度工作总结报告、项目总结文件、验收标准梳理

验收

准备验收会所需资料，准备一应全部交付物

售后

文件解读、应急处置培训

结束前

完善过程文档 复盘整个项目情况 总结经验教训
研讨改进计划 改进方案模拟演练 犒劳项目团队



赛博梦工厂

Cyber Works

workflow

配合部门



主流程



输出



The image features a central figure of a person wearing a black hoodie, with their right hand pressed against their forehead in a gesture of stress or contemplation. The background is a vibrant blue digital landscape. On the right side, a glowing globe is visible, surrounded by a network of white lines and nodes. Scattered across the background are several blue padlock icons, some of which are open, symbolizing security or digital access. The overall aesthetic is high-tech and futuristic.

谢谢观赏