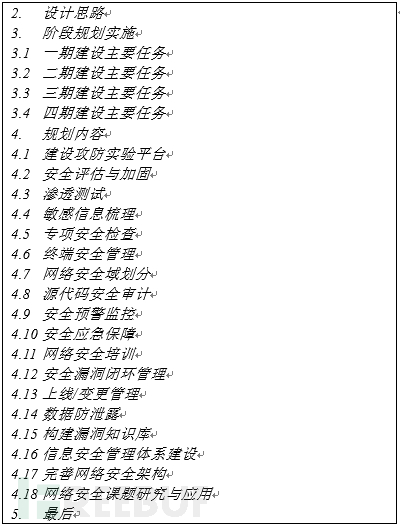
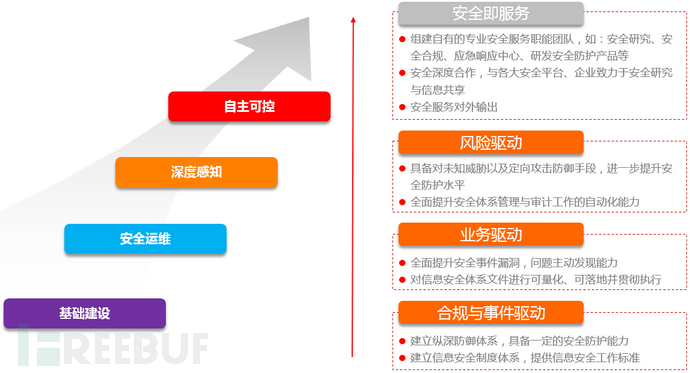
**目录架构**

[](http://image.3001.net/images/20180911/1536645232_5b975870b3ac2.png)

**二 设计思路**

信息安全规划，根据一些驱动因素进行思考，设计思路：

[](http://image.3001.net/images/20180911/1536645232_5b975870b7e1e.png)

***注：****安全规划思路，主要是用于安全建设的一个指导思想，在实际安全建设工作中，初级阶段也可能包括安全深度感知、自主可控的建设的内容。*

信息安全是由多方面组成，主要工作需要防范威胁发生的可能，以及采取风险降低措施，因此安全工作开展涉及多方面的内容：

[](http://image.3001.net/images/20180911/1536645233_5b97587110e61.png)

**三 阶段规划实施**

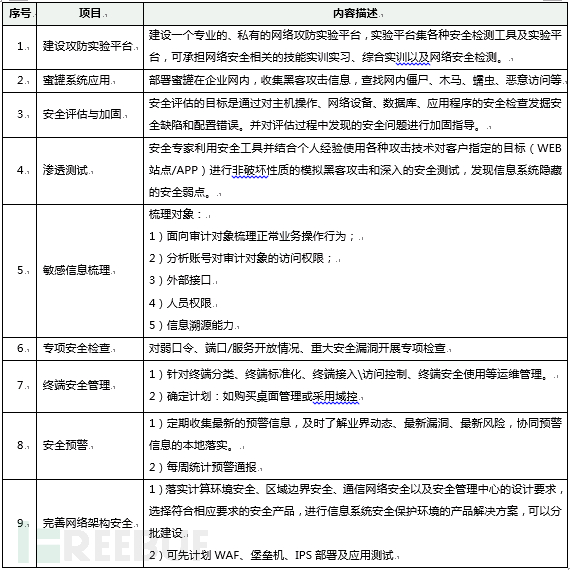
在规划实施前，会先进行安全现状了解，主要是通过对主机、应用系统、数据、终端、网络进行访谈和抽查，发现一些大致和企业共性的问题。

主要是从资产信息收集，然后分析主机、应用、网络、数据、终端方面存在的一些安全问题，由于此次企业的生产服务器均在云上，因此也就未考虑物理机房的安全。

通过前期的现状分析，**安全建设采用分期建设，主要是根据工作开展的紧迫性和易操作性进行分期规划。**

**3.1   一期建设主要任务**

**信息安全建设一期**中进行安全技术检查以及行业安全预警跟踪，尽量及时发现安全脆弱性并加固指导，为后期安全建设提供指导依据。

工作开展计划先防范风险属性由外向内，影响严重程度由高向低进行时间安排。   
[](http://image.3001.net/images/20180911/1536645232_5b975870ed153.png)

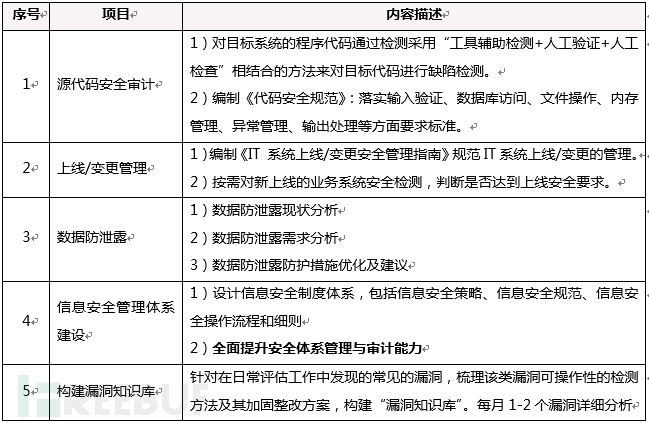
**3.2   二期建设主要任务**

在信息安全建设一期的基础上开展二期建设计划，主要针对内网安全、加强人员信息安全意识、建立安全预警和安全管理体系初级文件等工作。

[](http://image.3001.net/images/20180911/1536645233_5b97587107bce.png)

**3.3 三期建设主要任务**

在信息安全建设一期、二期的基础上开展三期建设计划，主要加强WEB安全问题早期发现、系统上线变更、数据防泄露等安全能力，全面提升安全体系管理与审计能力。

[](http://image.3001.net/images/20180911/1536645233_5b9758713df29.png)

**3.4 四期建设主要任务**

在信息安全建设一期、二期和三期的基础上开展四期建设计划，主要加强安全体系管理、审计和考核管理，更加有效的帮助软件企业降低安全问题，提升对安全问题进行集中发现、管控及处理能力，实现安全主动防御以及增强追踪能力。

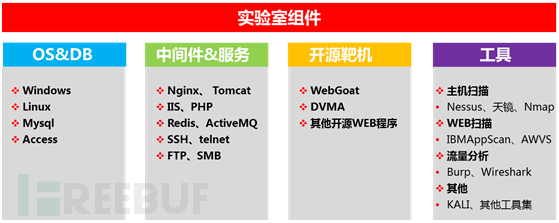
[](http://image.3001.net/images/20180911/1536645233_5b97587141da8.png)

**四 规划内容**

**4.1 建设攻防实验平台**

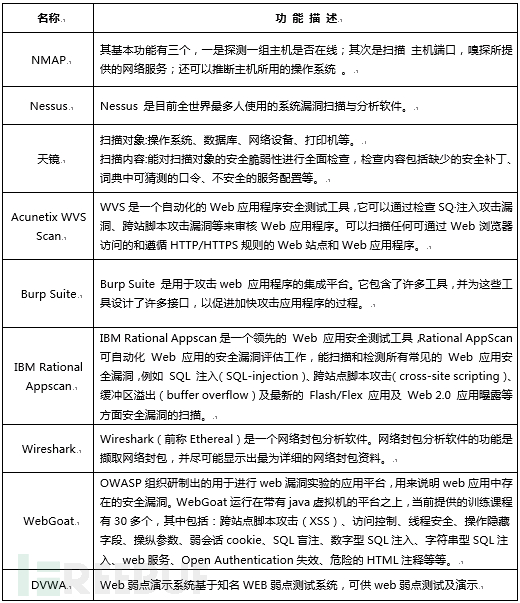
在企业内部建设一个专业的、私有的网络攻防实验平台，来满足专业网络安全实践、安全防护能力和安全意识提升、跟踪最新网络安全技术和提升企业级专业影响力等具体需要。实验平台可承担网络安全相关的技能实训实习、综合实训以及网络安全检测。

攻防实验平台主要能模拟以下的环境进行各种不同类型的攻防实验。

[](http://image.3001.net/images/20180911/1536645233_5b97587169b11.png)

为更接近一般网络的真实环境，与投入因素，后续将陆续增加的攻防实验平台套件，包括安全防护软件、中间件、数据库等。

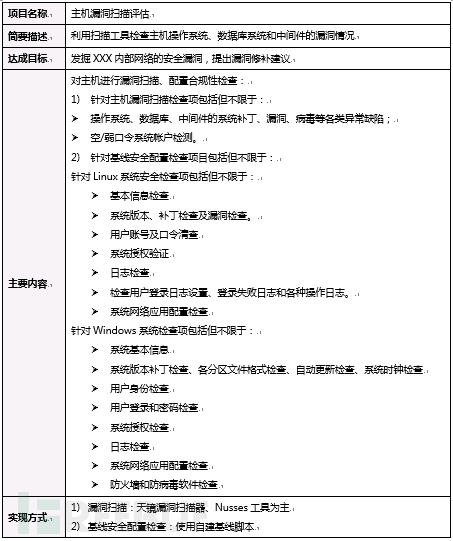
**攻防实验平台可能用到的部分工具**：

[](http://image.3001.net/images/20180911/1536645233_5b97587173a6b.png)

**4.2  安全评估与加固**

4.2.1  主机安全评估与加固

**主机安全检查：**

[](http://image.3001.net/images/20180911/1536645233_5b9758717a169.png)**主机安全加固：**

对上述范围内的主机操作系统、数据库系统和中间件等进行安全加固指导，解答各管理员在加固过程中所遇的疑难问题。

根据前期安全检查的结果，提交针对主机的安全加固方案，与相关部门讨论并认可后协助各部门进行安全加固实施。

4.2.2 应用安全评估与加固

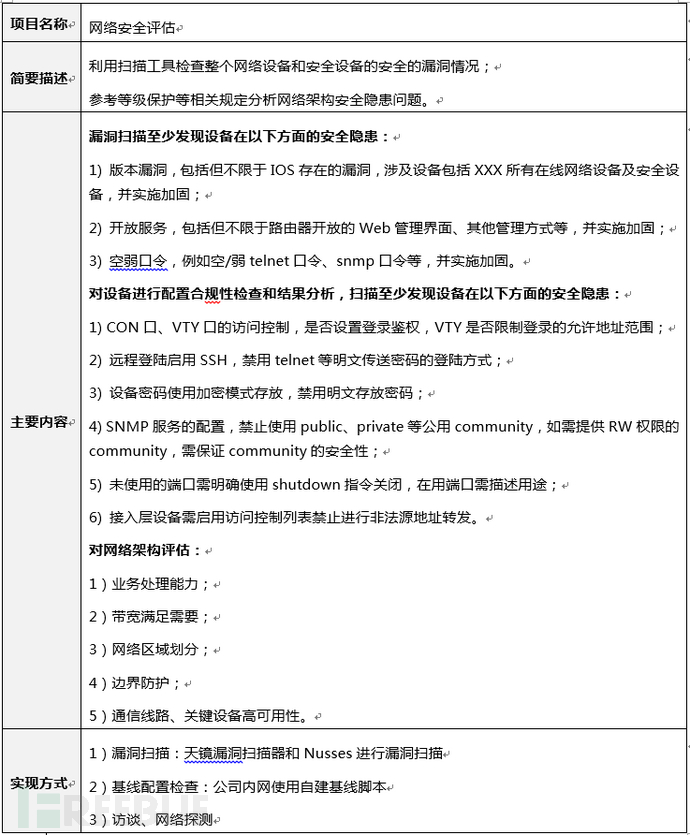
**应用安全检查：**

[](http://image.3001.net/images/20180911/1536645233_5b975871a9cd4.png)**应用安全加固：**

根据前期应用安全检查的结果，提交针对应用的安全加固方案，与各部门讨论并认可后由协助各部门进行安全加固实施。

4.2.3 网络安全评估与加固

**网络安全检查：**

[](http://image.3001.net/images/20180911/1536645234_5b975872070a1.png)**网络设备安全加固：**

根据前期网络设备安全检查的结果，提交针对网络设备的安全加固方案，与各部门讨论并认可后由协助各部门进行安全加固实施。

**4.3   渗透测试**

4.3.1  渗透测试类别

Ø  **根据测试者在测试前掌握被测对象的信息多少可分为：**

·  黑盒测试：渗透测试操作人员完全处于对系统一无所知的状态，通常这类测试的最初信息来自于DNS、Web、Email及各种公开对外的服务器，主要是模拟来自互联网的攻击者。

·  白盒测试：测试者可以通过正常渠道向被测者要求，取得各种包括网络拓扑、员工资料甚至网站或其他程序的代码片断等资料，这类测试的目的是模拟组织内部雇员的越权操作。

·  灰盒测试：对测试目标有一定的了解，主要是模拟离职的员工或合作伙伴，他们对组织的结构比较了解，但不在公司内部，没有访问权限。

Ø  **根据渗透者所处的位置可以分为：**

·  内网测试：渗透测试人员由内部网络发起测试，这类测试能够模拟组织内部违规操作者的行为。最主要的“优势”是绕过了防火墙的保护。

·  外网测试：渗透测试人员完全处于外部网络（例如拨号、ADSL或外部光纤），模拟从组织外部发起的攻击行为，模拟可能来自于对组织内部信息一无所知的攻击者，或者对组织内部信息一清二楚的攻击者。

Ø  **根据渗透内容深度和广度可以分为：**

· 普通渗透测试：仅对特定业务系统的WEB站点进行模拟黑客攻击，使用黑客工具、测试工具、特制shell工具，自动化、手工测试单个WEB站点的安全隐患；

·  深入渗透测试：以特定业务系统的WEB站点为起点，（1）横向测试同网段的相应WEB站点安全性，重点在于核查攻破单个站点后，对同网段的WEB站点整体危害。（2）纵向测试，从外网跳转攻击到内网，或者内部不同子网间跳转攻击，重点在于测试边界防火墙、防护措施的有效性，尽力获取内部有价值的信息。

**4.3.2  WEB网站渗透测试**

4.3.2.1   渗透测试范围

针对WEB网站进行渗透测试，重要网站系统每半年做一次渗透测试，普通网站系统每年做一次渗透测试，选择一个网站为始点进行深度渗透测试。

4.3.2.2   渗透测试内容

WEB网站渗透测试内容主要以OWASP TO10与常见重大WEB漏洞为主，如：   


**4.3.3  手机客户端渗透测试**

4.3.3.1   渗透测试范围

针对手机客户端APP进行渗透测试：



4.3.3.1  渗透测试内容

手机客户端APP渗透测试内容，如：



**4.4    敏感信息梳理**

4.4.1  梳理目标

1)   建立以系统平台数据为管理对象的敏感信息防护，根据敏感数据内容、属性、承载载体、使用方式和频率进行数据分类、分级管理，全局展现敏感数据的分布及防护级别。

2)   加强对数据访问使用中的权限控制、二次授权管理，支持数据访问控制流程、执行、审批的流程管理，实现数据交互中控制管理。

3)   数据交互、下载中的对于信息内容防护措施，实现数据下载的专区控制，增加安全防护措施，包括模糊化处理、加密和数字水印管理，分离数据下载执行过程与下载范围的控制管理。

4)   实现全面的数据操作审计管理，集中管理敏感数据操作日志，包括应用系统数据操作日志、堡垒主机操作日志、同时应包括数据库操作行为审计系统的日志信息，对数据实现补全、筛选以及关联分析。

5)   明确敏感信息存在载体、数据使用场景、系统数据交互接口、人员操作权限等信息，用于敏感信息防护策略配置和管理。

6)   将敏感数据访问建立独立的访问入口，与其他安全管控系统独立工作，只有数据管控区访问才能访问核心域的主机和数据库，从管控区导出敏感数据需要经过申请审批，从物理上提高核心工作区安全性，确保各业务系统平台系统维护和操作的安全性及确保运维操作人员身份合法性，防止敏感数据外泄，保证敏感数据的有效管控。

4.4.2  梳理对象

1)   面向审计对象梳理正常业务操作行为

根据业务系统的审计对象，调研分析针对审计对象的正常业务操作：如后台进程和前台调用。操作行为必须包括：由谁（账号）执行进程、以何种方式操作、操作哪个实体、输入何种参数、形成何种结果、操作频率等等）。对于不在梳理的正常业务操作行为范围内的操作，都是不合法，需要重点审计。

2)   分析账号对审计对象的访问权限

收集业务系统主机、数据库所有操作账号。主机系统账号包括资源帐号和自然人账号。数据库账号应包括：自然人账号、生产账号，其中自然人账号对应三个角色。结合审计对象，确认各种账号对审计对象所具有的权限，形成自然人账号与资源账号对应关系、资源帐号与实体操作权限对应表。

3)   外部接口

收集业务系统各子系统之间互访接口的访问关系，包括接口发起方IP地址，接口使用的进程、接口类型、开放端口、数据流向、访问频率等内容。

4)   人员权限

在明确重点敏感保护对象的情况下，梳理相应访问权限对应的资源帐号，以及资源帐号对应的角色，使用该帐号的自然人情况。

5）信息溯源能力

在明确重点敏感保护对象的情况下，梳理用户行为、信息发布、内容操作记录的保存、传输、销毁流程。

**4.5  专项安全检查**

4.5.1  弱口令检查

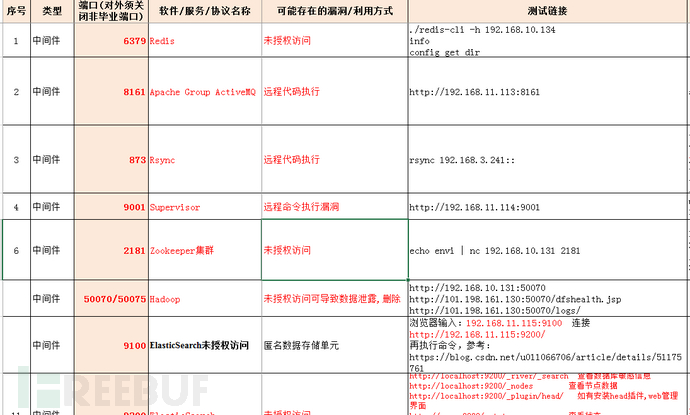
通过分析行业内常见口令字典，形成弱口令检查字典，对各平台操作系统、应用、中间件、数据库进行全面检测的弱口令检查。

4.5.2  端口专项检查

梳理所属各平台的设备所开放的端口对应服务与软件版本，关闭不必要要端口，对维护端口进行访问限制，形成产品信息表并定期更新。

4.5.3  重大漏洞专项检查

根据最新安全趋势，选取风险级别高，威胁大，可能造成极严重后果的典型安全漏洞，对所有系统平台进行全面检测，如：



**4.6  终端安全管理**

4.6.1  终端安全目标

**主要目标包括：**

1、根据各终端的访问需求，进行分类管理和合适的访问控制；

2、对终端的防病毒、入侵防范策略进行统一管控，更加快捷有效的进行安全防护措施实施；

3、对终端的接入\访问进行控制，避免非授权访问及外部威胁引入；

4、严格控制终端外设的使用，监控并防止用户USB口、光驱、软驱的使用情况，以及上网行为监控，严防信息泄密和外网威胁引入。

4.6.2  终端安全规划

制定《终端安全管理规定》，对终端安全管理的要求，可参考如下：   


**4.7 网络安全域划分**

4.7.1  安全域划分目标

1)   根据行业安全标准关于安全域划分和边界整合的精神，对现有信息系统及网络结构进一步优化和调整进行建议。

2)   对现存的一些不合理的边界、系统互联方式进行清理，将其纳入到安全域划分和边界整合的体系；但需要充分考虑实施成本、可行性、对现有业务的影响，做阶段性的目标规划建议。

3)   针对各业务系统安全域的划分，根据风险不同及防护重点不同，建议给出合理的监视、测量、清理、审计等技术手段，以实现安全域内安全事件的及时响应和清除。

4)   对现存的一些不合理的终端使用策略、内部访问关系进行清理，参照现有的系统规划技术方案，提出合理的整改、实施建议开展安全域划分工作。

4.7.2  安全域划分及设计思路

安全域的划分必须要基于对网络与业务的充分理解，在保证业务正常开展的同时实现对安全域的有效隔离。

**具体的规划方案需要根据业务需求、现有网络架构进行规划**：

为了方便理解安全域划分，把网络环境划分成4个安全域（仅供参考）：

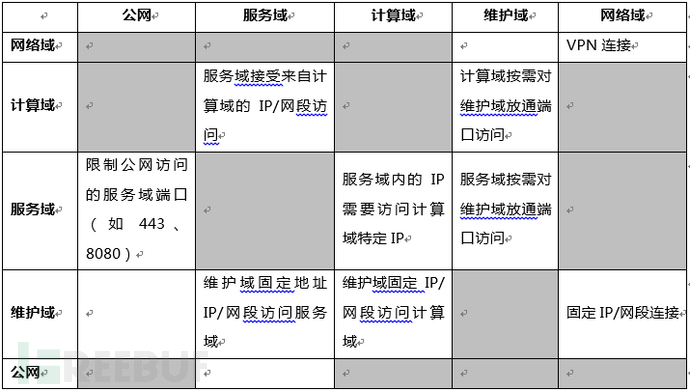
**计算域：**数据库服务器，数据库服务器提供数据存储和访问服务。

**服务域：**WEB服务器，负责处理终端发出的各种请求，并将处理结果以Web的方式返回。

**网络域：**网络域是由连接具有相同安全等级的计算域、维护域和服务域的网络设备和网络拓扑组成，访问必须通过VPN才能接入。

**维护域：**所有需要登录系统平台进行日常维护的终端。

访问控制参考，如：



1) 计算域（固定源IP）à服务域（固定目标IP、端口）；

2)  服务域（固定源IP）à计算域（固定目标IP、端口）；

3) 维护域（固定源IP/段）à计算域（固定目标、端口）、服务域（固定目标、端口）；

4) 计算域内不同系统服务器进行网络隔离；

**5)**服务域内不同系统服务器进行网络隔离；

6) 生产环境与测试环境、开发环境网络隔离；

7) 维护域（固定源IP/段）才可以跨网络域访问云平台服务器；

8) 网络域之间采用VPN连接。

4.7.3  网络结构分析

分析网络结构着重于分析目前网络架构是否既能实现平台数据交换功能又能保证系统安全，目的是为了找到在系统建设初期单纯为了实现功能而未考虑的安全的环节，从而在解决方案中补充缺少的安全环节，找到能够同时满足功能实现和安全要求，并且和现有**网络结构结合最紧密**、**对现有网络结构改动最小**、**不至于影响业务的解决方案**。

4.7.4  平台数据流分析

在调研、访谈的结果基础上对第一手资料进行分析与整理，由大到小，获得各系统平台之间的访问关系及子系统之间的联系，最终获得完整清晰的平台数据流图，在这个平台数据流图上进行平台单元、集群的划分和平台单元接口的界定。并根据这个平台数据流图总结整个系统面临的安全隐患和外来威胁，为下一步的安全解决方案确定方向。

4.7.5  网络优化和边界整合

针对各系统平台进行网络结构分析和业务数据流分析的结果，结合各系统平台对于安全威胁、安全防护要求的定义，对安全域边界进行整合、加强边界的互联互访控制，以帮助对现有的网络系统进行模块化划分，进行层次化的保护，以有效保证系统和信息安全，同时也为未来系统的建设和规划提供了依据。

**4.8   源代码安全审计**

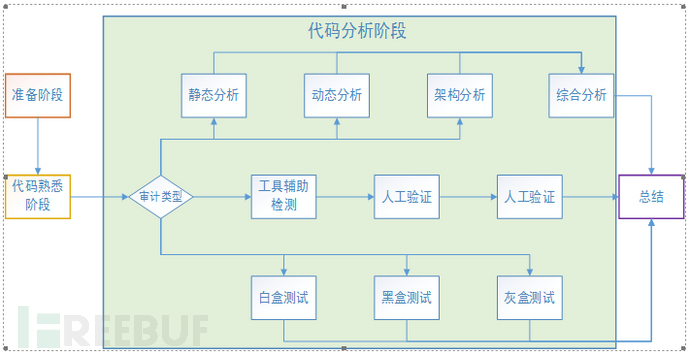
4.8.1  代码安全审计综述

由于业务平台的复杂性、交互性增加多，代码编写不规范带来了更多不安全因素，需要进行白盒与黑盒安全测试，发现并指导解决WEB上的应用安全问题。

代码审计属于白盒测试，白盒测试因为可以直接从代码层次看漏洞，所以能够发现一些黑盒测试发现不了的漏洞，比如二次注入，反序列化，xml实体注入等可能的0day漏洞。

4.8.2  代码审计方法

对目标系统的程序代码通过检测采用“工具辅助检测+人工验证+人工检查”相结合的方法来对目标代码进行缺陷检测。通过工具辅助和人工结合的方法，能够有效的发现代码中存在的缺陷。



**4.8.3  代码审计内容**

主要包括三种类型的分析审核：

一、动态分析

主要包括平台系统外部接口的获取、面向安全漏洞发现的畸形注入数据生成、注入测试与系统响应监控等技术环节：



1、外部接口的获取

通过前期的分析，得到应用外部接口信息，为下一步的检测提供目标。需获取的信息包括：

Ø 地址、访问方法、调用方法

Ø 接口参数、类型

Ø 响应机制

2、畸形输入数据生成

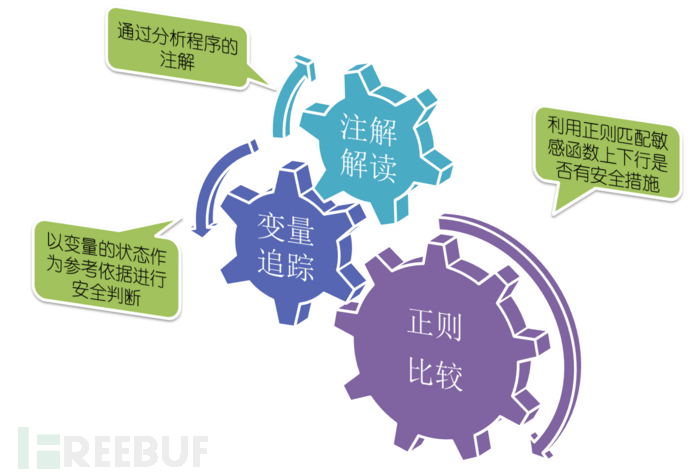
本部分工作将根据获取的接口信息（参数类型等），基于黑客技术知识生成相应的畸形输入测试数据。

3、输入测试与系统响应监控

由安全分析人员在相关输入工具的辅助下向目标系统注入畸形数据驱动目标系统运行，并根据接口信息监控系统的反应，以期发现目标系统中可能存在的安全漏洞。

**二、静态分析**

静态分析部分的工作主要包括利用静态分析工具在代码中查找固定的模式或规则集合。静态分析工具的输出仍然需要人为判断。



1、工具分析

使用工具自动检查所有应用程序源代码，发现代码中的问题。

2、人工代码分析阶段

基于应用知识标识出安全关键点，即有可能引发安全问题的系统实现模块或语句，包括系统程序判断、重要函数的调用、重要的程序执行、外部数据流分析其所有可能的流路径，当路径中出现安全关键点时进一步对数据的合法性检验的实现进行检验。若其合法性检验的实际实现存在缺漏，则预示着发现了一个可能的安全漏洞等进行人工的审计。

三、综合分析

结合以上分析中的可疑点进行深入的分析测试，由代码审核小组人员通过模拟攻击的方式对代码问题进行测试，避免误报。

**4.9  安全预警监控**

定期收集最新的预警信息，及时了解业界动态、最新漏洞、最新风险，协同预警信息的本地落实。

4.9.1  内网实时监控

通过安全检测设备、安全防护设备，对各类安全事件进行安全预警监控、安全分析并下发安全事件处理工单，协助相关部门进行安全事件应急处理。

4.9.2  公网实时监控

实时监测洞响应平台、CNCERT、CNVD等网络安全事件处置平台以及各大安全论坛披露的漏洞信息，通过筛选、过滤相关关键字实施动态安全监控，发现与公司系统相关的安全漏洞立即开展信息推送与处置协作

4.9.3  每周安全预警

每周从互联网应急中心（CNCERT）、CNVD、CVE、防病毒厂家、操作系统厂家的通告、告警信息、大型资信网站，汇总成每周安全预警报告及安全知信，并给出相应的修复、整改指导意见。

4.9.4  安全预警跟踪

每周协同相关工作人员，对上周安全预警信息进行跟踪落实，主要工作包括了：针对预警信息，给出检查漏洞的方法和解决办法，并行资产关联，指出存在风险的资产。

4.10    安全应急保障

4.10.1  应急预案

**一、应急预案目标**

建立健全的恢复应急工作机制，提高对突发事件的组织协调能力和应急处置能力，满足突发情况下通信保障和通信恢复工作的需要，最大程度地降低重大灾害、事件、故障等对通信业务的损害。

二、应急预案内容

建立应急预案，预案内容不限于以下：

1、安全攻击：DDOS攻击、网页篡改、网页挂马、恶意代码、域名劫持等。

2、设备故障：平台瘫痪、平台过载、应用进程异常故障、数据备份及恢复故障、服务器硬件故障等。

4.10.2  应急演练

每年1次应急演练。

应急演练和攻防演练的开展，现场技术支持扮演攻击方，提供安全扫描工具、攻击工具、测试脚本。

应急演练的目的在于：

1. 验证应急预案的有效性；

2. 测试各防护设备及策略的有效性；

3. 理顺安全事件上报及处理流程；

4. 校验各工作人员安全事件处理技能熟练度。

4.10.3  应急响应

**一、应急响应目标**

安排具有网络安全攻防经验和应急响应工作经历的技术人员完成实施工作解决安全事件问题。根据每次应急响应的具体情况，在必要时将会聘请外部安全顾问协助进行安全事件的分析和处置。

二、应急响应范围

应急响应服务启动条件如下：

Ø 系统管理员通过评估、检查等方式发现了安全问题（如主机已被入侵、系统存在后门、网络蠕虫正在蔓延等情况），且可能对业务造成加大影响，无法自行解决或无法在短时间内自行解决时，可以启动应急响应；

Ø 系统安全管理员在解决一般安全事件的过程中，由于处理不当或无法解决，造成安全事件的影响扩大或蔓延（如病毒向骨干网络中蔓延等情况），在一定时间内没有解决的情况下，可以启动应急响应；

Ø 当发生以上情况启动应急响应，因技术或事件等限制需要安全厂商提供对安全事件应急响应的知识经验、技术手段和产品支持，启动本应急响应服务。

**三、应急响应内容**



**4.11  网络安全培训**

根据需求制定详细的培训计划，从技术和管理两个纬度进行网络与信息安全的培训。同时，采取“分阶段，分层次”的形式，落实培训计划，强化培训效果。

通过培训希望能够达到这样几个目的：

Ø 普及网络安全知识和黑客的一些常用攻击手法，帮助员工提高安全意识保障组织网络安全。

Ø 提升漏洞扫描、渗透测试等所发现的共性问题的认识与理解，包括工具使用问题、漏洞原理、利用方式、加固方法等；

Ø 在统一的应急预案框架下制定不同事件的应急演练和培训，锻炼实际操作技能及应变能力，提高了应急处理的信心；

Ø 提升信息技术人员、管理人员等相关人员的安全意识，提高安全技术人员的安全技能，了解目前的安全技术现状、安全体系的发展趋势。

**员工安全意识培训案例，如：**

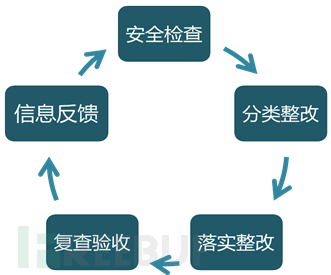


**4.12  安全漏洞闭环管理**

1、建立漏洞闭环管理制度，指导规范安全整改工作，为安全整改工作提供制度依据；

2、安全风险治理“闭环管理”，是以安全漏洞治理为主线，从漏洞排查治理到漏洞消除的“闭环”管理流程，即安全检查→分类整改→落实整改→复查验收→信息反馈→新的漏洞排查。

3、式发布之后对相关岗位人员进行制度宣贯、培训，规范漏洞加固流程，提升人员安全管理意识及管理水平。



**4.13 上线/变更管理**

4.13.1  建立上线变更管理

加强IT系统建设过程中安全控制，规范IT系统上线验收的管理。

4.13.2  上线/变更安全检测

对新上线的业务系统安全检测内容包括：

1. 提供接入网络的系统的安全相关文档；

2. 对接入网络进行漏洞检测，包括主机漏洞和应用漏洞；

3. 对接入网络的网站/APP进行渗透测试；

4. 对接入网络的系统的安全配置进行基线检查。

**4.14    数据防泄露**

4.14.1  数据防泄露目标

企事业的机密文档，研发源代码，图纸等核心技术机密资料，很容易经内部员工的主动泄密流转到外面，甚至落到竞争对手手中，给企业造成极大的经济与声誉损失。

常见的泄密的途径包括：

- 内部人员将机密电子文件通过U盘等移动存储设备从电脑中拷出带出；

- 内部人员将自带笔记本电脑接入公司网络，把机密电子文件复制走；

- 内部人员通过互联网将机密电子文件通过电子邮件、QQ、微信等发送出去；

- 内部人员将机密电子文件打印、复印后带出公司；

- 内部人员通过将机密电子文件光盘刻录或屏幕截图带出公司；

- 内部人员把含有机密电子文件的电脑或电脑硬盘带出公司；

- 含有机密电子文件的电脑因为丢失，维修等原因落到外部人员手中。

- 外部电脑接入公司网络，访问公司机密资源盗取机密电子文件泄密

- 内部人员将通过Internet网络存储，进行保存。

……

为保障公司机密资料不至于泄露，企业数据防泄露建设目标，如下：

1、对核心技术文档（office，设计图纸，源代码等）进行全生命周期加密保护。

2、核心文档只能在受控范围内被指定授权人员使用，非授权用户不能篡改文档内容，不能随意打印，不能随意拷贝，不能截屏，未授权外带禁止使用；

3、核心机密文档受控后，文档所有使用行为均可审计；

4、不改变用户原有工作习惯、不增加用户工作负担、不限制用户的正常操作行为，在保证用户原有业务模式的情况下，不影响用户的工作效率，让用户在安全的环境中无感知的处理各种研发业务。

5、实现对OA，ERP等应用系统数据安全防护。

4.14.2  数据防泄露规划

针对数据防泄露的常见方式，分为技术与管理、产品部署两种方式实现，如下：

一、技术与管理措施实现：

1）通过终端安全规划的落地，实现部分防控措施；

2）通过管理制定如：安全管理制定、保密协议等进行约束。

**二、产品部署实现方式：**



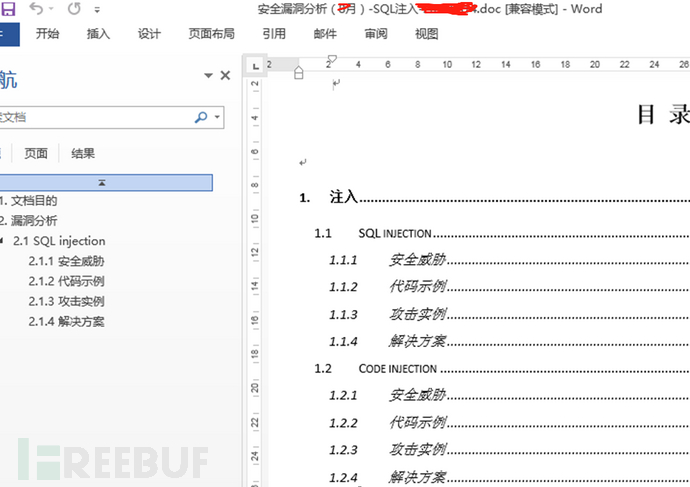
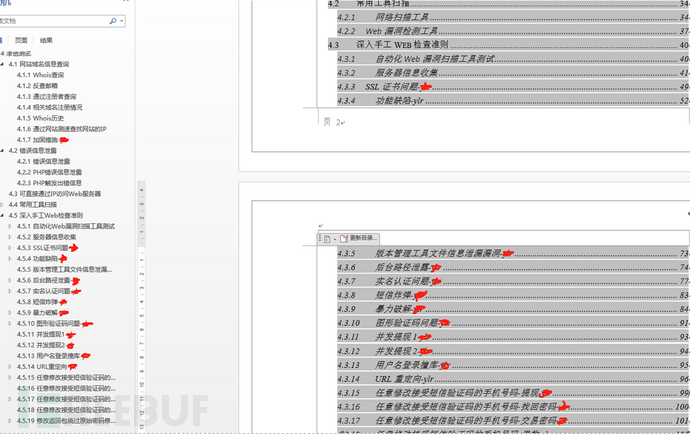
虽然从技术上网络访问控制、设备接入等方面进行控制能起到一定的防泄露，但存在一些局限性或影响工作效率。

**综合考虑，**建议从**技术、安全产品、管理**三个层面进行防泄露管控。

**4.15   构建漏洞知识库**

针对在日常评估工作中发现的常见的漏洞，梳理该类漏洞可操作性的检测方法及其加固整改方案，构建“漏洞知识库”。

下面这些只是个人工作中整理的，有点乱，基本是自己看：



**4.16    信息安全管理体系建设**

4.16.1  建设目标

信息安全策略与标准体系是信息安全组织、运作、技术体系标准化、制度化后形成的一整套对信息安全的管理规定。该标准体系包括信息安全策略、信息安全规范、信息安全操作流程和细则，涉及管理要素和技术要素，覆盖信息系统的终端层、物理层、网络层、系统层、应用层五个层次以及通用信息安全管理规范。

4.16.2  建设内容

4.16.2.1   信息安全方针制定

陈述信息安全的管理意图，提出企业或组织的信息安全目标，为今后目标明确、有组织、有计划的信息安全建设给出总体方向。

4.16.2.2   安全组织体系职责设计

建立整个信息管理体系相吻合的信息安全管理组织体系。

设计专门进行信息安全建设和管理的组织管理体系。在体系中包括安全决策组织、决策人，安全管理组织、管理岗位和技术岗位等。设计安全组织和其他组织、部门中接口和协调关系，并对不同层次的组织和人员制定安全职责。

4.16.2.3   信息安全规范文档制定

制定全面和适用的信息安全标准和规范。

《信息安全标准文档》是企业实施信息安全管理和技术工作的指导性标准文件，作为信息安全建设和管理的内部标准和规范。一般包括各个网络设备、主机操作系统和应用程序的应遵守的安全配置和管理的技术标准和规范；安全建设和日常管理和维护的规范。标准和规范将作为信息系统和安全系统的安装、配置、采购、项目评审、日常安全管理和维护时必须遵照的标准，从而成为信息安全建设和管理的内部标准和规范。

4.16.2.4   信息安全流程文档制定

开发和制定适用的信息安全操作流程(Procedure)和执行手册(Manual)必要文档。

《信息安全标准文档》是指导企业具体使用安全实施、安全管理、日常安全操作和维护的文件，详细规定主要业务应用和事件处理的流程和步骤，和相关注意事项。可以作为安全管理和操作人员具体工作时的详细指导和参考。此部分必须具有可操作性，而且应该得到有效推行和实施。

4.16.2.5   信息安全制度制定

完成各类管理制度、管理规定、管理办法和暂行规定等具体安全管理文档，作为具体安全管理的详细规定。

信息安全制度和管理办法相关文档主要包括各类管理制度、管理规定、管理办法和暂行规定等。根据安全方针中规定的安全各个方面所应遵守的原则方法和指导性策略，引出的具体安全管理规定、管理办法和实施办法，这些文档必须具有可操作性，而且必须得到有效推行和实施的。

4.16.2.6   文档输出介绍

安全制度参考模板

**总纲方针：**

《IT安全管理策略》

**安全管理体系：**

《内部审计管理办法》

《人员信息安全策略》

《网络安全管理办法》

《物理安全管理办法》

《信息安全符合性管理办法》

《信息安全组织架构》

《信息交换安全管理办法》

《信息对外发布管理办法》

《系统安全补丁管理指南》

《网络安全域划分指南》

《员工信息安全手册》

《WEB安全编程技术规范》

《访问控制管理办法》

《信息系统上线验收安全管理指南》

《信息系统运维管理办法》

《信息资产管理办法》

《运维安全管理规范》

《IT安全事件管理指南》

《IT安全监控与预警管理指南》

**安全标准：**

《安全产品选择》

《信息安全管理岗位及其职责》

《第三方人员管理办法》

《介质安全管理规定》

《网络设备配置标准》

《防火墙管理规定》

《机房安全管理制度》

《系统日志管理办法》

《系统数据备份管理规定》

《系统用户和口令管理规定》

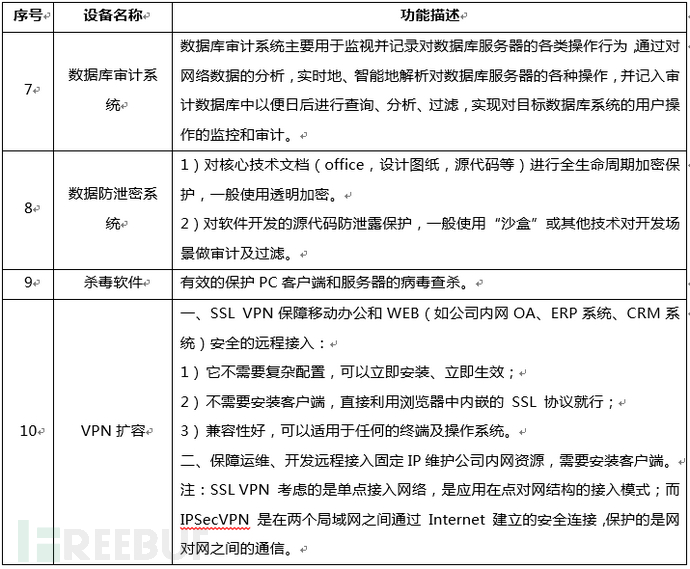
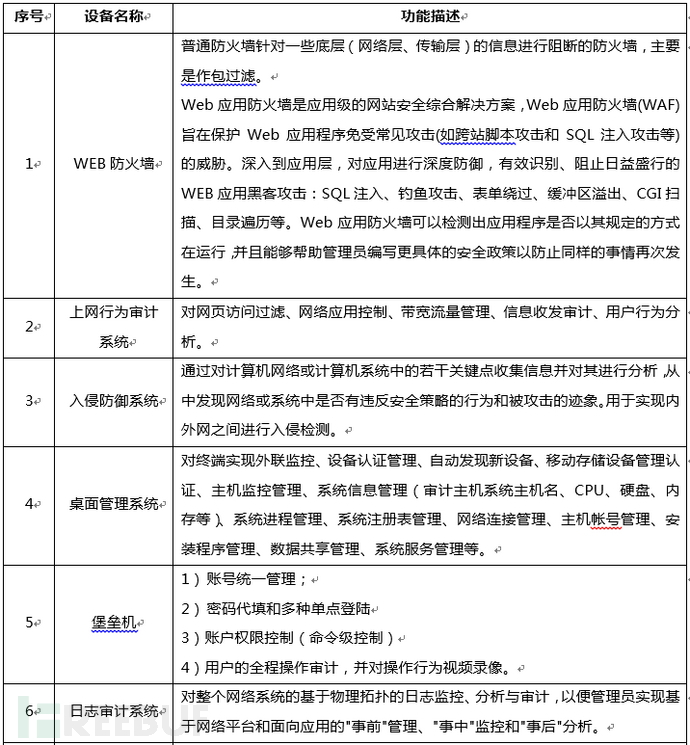
《病毒恶意代码防范管理办法》

《电子邮件使用安全管理规定》

《远程办公管理办法》

**完善网络安全架构**

根据等级保护及行业安全需求分析和设计策略，选择符合相应要求的安全产品，进行信息系统安全保护环境的产品解决方案，可以分批建设，产品如：



**4.18    网络安全课题研究与应用**

针对安全威胁的防护，传统的防火墙/UTM、IDS/IPS、防病毒系统、多种信息安全审计系统和安全管理平台等安全防护手段大多都采用基于特征、规则或关联分析的方式被动的保护网络安全。随着网络入侵手段的日新月异，0day漏洞层出不穷的被发现，这些静态的保护手段已经渐渐显露出不足之处。

为了加强网络安全的及时性、有效性，开展网络安全课题研究与应用。

**一、安全挑战**

1. 资产的信息安全管控难度大

2. 网络攻击的恶意样本文件检测识别效率低

3. 新的攻击技术手段难以预防

4. 难以进行信息安全事件取证

**二、安全需求**

1. 资产安全主动监测管控能力

2. 实时安全监控及攻击源快速定位能力

3. 最新真实的攻击信息库，新型攻击检测及防护能力

4. 攻击行为取证、攻击样本捕获能力

4.18.1  蜜罐系统应用

4.18.1.1   建设目标

蜜罐（HoneyPot），是一种供攻击者攻击从而产生价值的安全设施。与用户通常使用的安全防御设施不同，蜜罐只有在受到攻击的情况下才能展现出价值。

安全领域的专家及用户通过蜜罐系统，可以了解到攻击者通过什么方法、使用什么工具展开攻击、以及他们攻击的出发点，并能够从中发现规律和趋势，为安全防御工作的有效进行提供了很好的基础。

了解入侵者的攻击方式、攻击目标、攻击工具、攻击漏洞等信息，对于网络安全研究，网络数据防范来说是非常重要的。同时，对于重要的网络服务器，应该对其加强防护，加强监控，降低安全隐患。蜜网管理系统可以很好的完成这一目标。

**蜜网系统有作用,如：**

Ø 捕获木马和僵尸网络样本；

Ø 挖掘已知漏洞利用方式。通过对网络数据包和样本的分析可以了解黑客更新的漏洞利用方式甚至是沟通方式；

Ø 预警未知漏洞(0day)，提供未知漏洞信息供研究人员分析可以获得更加具体的0day信息。

**可关注本地网络安全：**

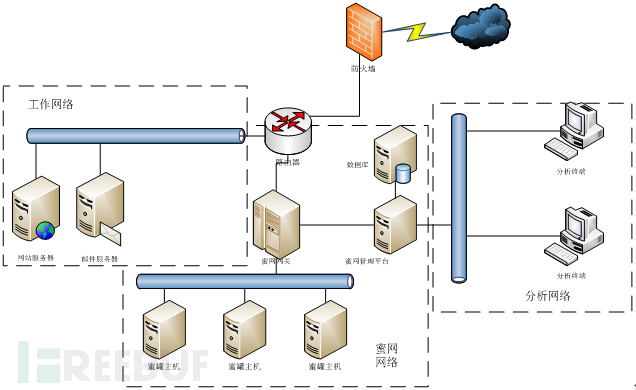
Ø 蜜网系统为网络提供了真实可靠的预警机制；

Ø 大量部署蜜罐可以有效的迷惑入侵者，从而能够及时的预警并为本地及时反应留出足够的时间；

Ø 蜜网系统捕获的数据可使用户更有效的了解网络安全状况，从而有针对性的提高薄弱环节安全措施。

4.18.1.2   功能实现

蜜网管理系统的部署必须能够获取入侵者的操作，并保证工作网络的安全。为了保证工作网络的安全，应将**工作网络**与**蜜网网络**划分为两个网络。同时，为了分析蜜网管理系统获取的数据，还必须有分析人员操作的主机来分析数据。显然，分析人员也应当是一个独立的网络，我们称之为**分析网络**。因此，从安全方面和工作方面考量，蜜罐的部署环境应该是工作网络、蜜网网络、分析网络隔离的。如下图所示。



蜜网网络中，可以根据需求，配置任意多数量的蜜罐主机。这些主机可以放在一台或多台服务器上。

研究蜜罐技术，部署蜜罐在企业网内，收集黑客攻击信息，查找网内僵尸、木马、蠕虫、恶意访问等。**计划先部署蜜罐系统的功能如下所示：**



4.18.1  SDL应用

4.18.2.1  建设目标

SDL是安全软件开发生命周期，是一套完整的，面向Web和APP开发厂商的安全工程方法。帮助软件企业降低安全问题，提升软件安全质量。

项目目标：

（1）制定面向Web和APP开发企业的安全开发流程

制定动态的安全开发流程，对安全活动及活动要求进行分级，不同类型的软件，可以根据产品的风险及可用的投入资源来确定开发过程中要执行的安全活动，明确活动的输入，输出，执行者及依赖关系；

（2）制定及开发安全基础培训课程

制定安全培训体系，确定不同的角色需要接受的培训内容及培训的周期；开发基础性的培训课程；

（3）根据实践经验，输出各个安全活动的方法指导及模板，主要的安全活动有：安全风险评估、SDL安全要求设计、威胁建模、基于威胁建模的测试

（4）制定WEB应用/移动应用安全设计指南

（5）制定安全编码（JAVA、PHP）

（6）将OWASP现有项目，如开发指南、测试指南融合到软件全开发体系中；

4.18.2.2   SDL实现

安全软件开发的流程，以及各个阶段需要进行的安全活动，包括活动指南，工具、模板等，主要包括：

Ø 培训：提供安全培训体系，包含安全意识培训，安全基础知识培训，安全开发生命周期流程培训和安全专业知识培训

Ø 需求阶段：如何对软件产品的风险进行评估，建立基本的安全需求

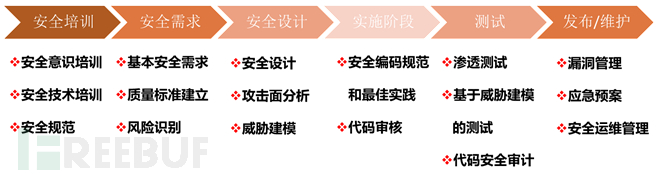
Ø 设计阶段：提供安全方案设计及威胁建模

Ø 实现阶段：提供主流编程语言的安全编码规范，安全函数库以及代码审计方法

Ø 测试阶段：基于威胁建模的测试设计，渗透测试

Ø 发布/维护阶段：建立漏洞管理体系

**SDL流程介绍示意图：**

***注：****当系统数量多，对系统安全性要求非常高的时候，严格按照SDL流程是很有必要。*

4.18.3  SOC平台应用

4.18.3.1   建设目标

SOC（安全管理中心）是实现网络安全管理的技术支撑平台，它以风险管理为核心，为安全运营和管理提供支撑，用于企业网络、设备、应用、数据等安全对象的安全保护。

**设计思路：**

将安全管理员从复杂的设备配置和海量日志信息中解脱出来，把精力专注于发现和处理各种重要安全事件；同时又将各自独立的安全设备组成为一个有机的整体，通过基于资产管理的事件关联分析和管理，及时发现安全风险、安全事件和业务安全隐患，并结合安全策略和安全知识的管理，提供多种安全响应机制，从而使得客户能够实时掌控网络的安全态势。

安全管理中心与已经部署的各类安全设备形成一个完整的安全保障体系，从而实现了高效、全面的网络安全防护、检测和响应。具备监控、预警、响应、追踪等功能，并具备可审计功能，即对内部安全管理人员的相关操作进行日志记录。

**设计目标：**



**实现价值：**

Ø 统一日志管理

Ø 统一配置管理

Ø 统一威胁管理

Ø 各安全产品和系统的统一协调和处理

Ø 设备的自动发现

Ø 风险分析自动化

Ø  KPI考核等

SOC的功能架构图这里就不放了