安全加固实施标准

2019护网专项培训

NSFOCUS

CONTENTS 目 录

NSFOCUS

01

什么是安全加固

1. 安全加固目的
2. 角色与职责
3. 总体框架

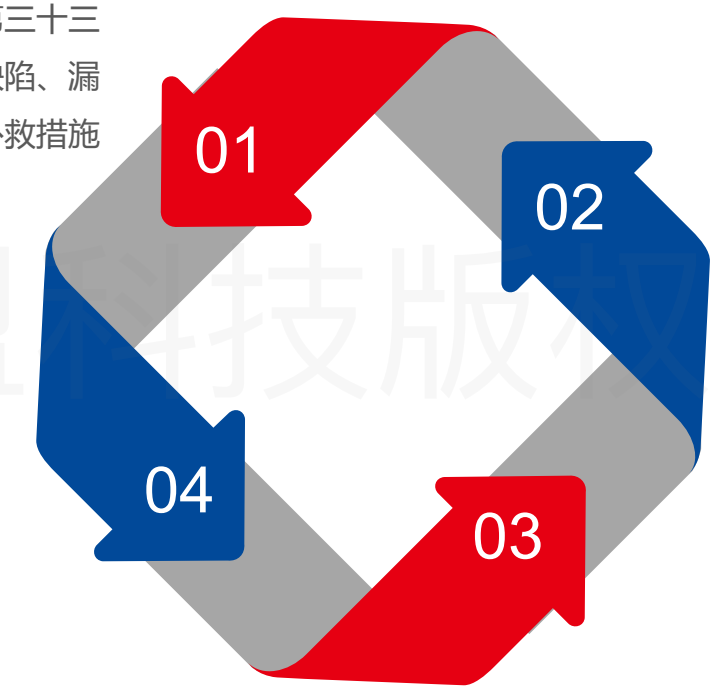
1.1

安全加固目的

为什么要做安全加固

法律法规

《中华人民共和国网络安全法》第二十二条和《关键信息基础设施安全保护条例》第三十三条，发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施



安全检查

修补加固在完成后解决掉在安全评估中发现的技术性安全问题，所有的被评估对象应不再存在高风险漏洞和中风险漏洞

利益保护

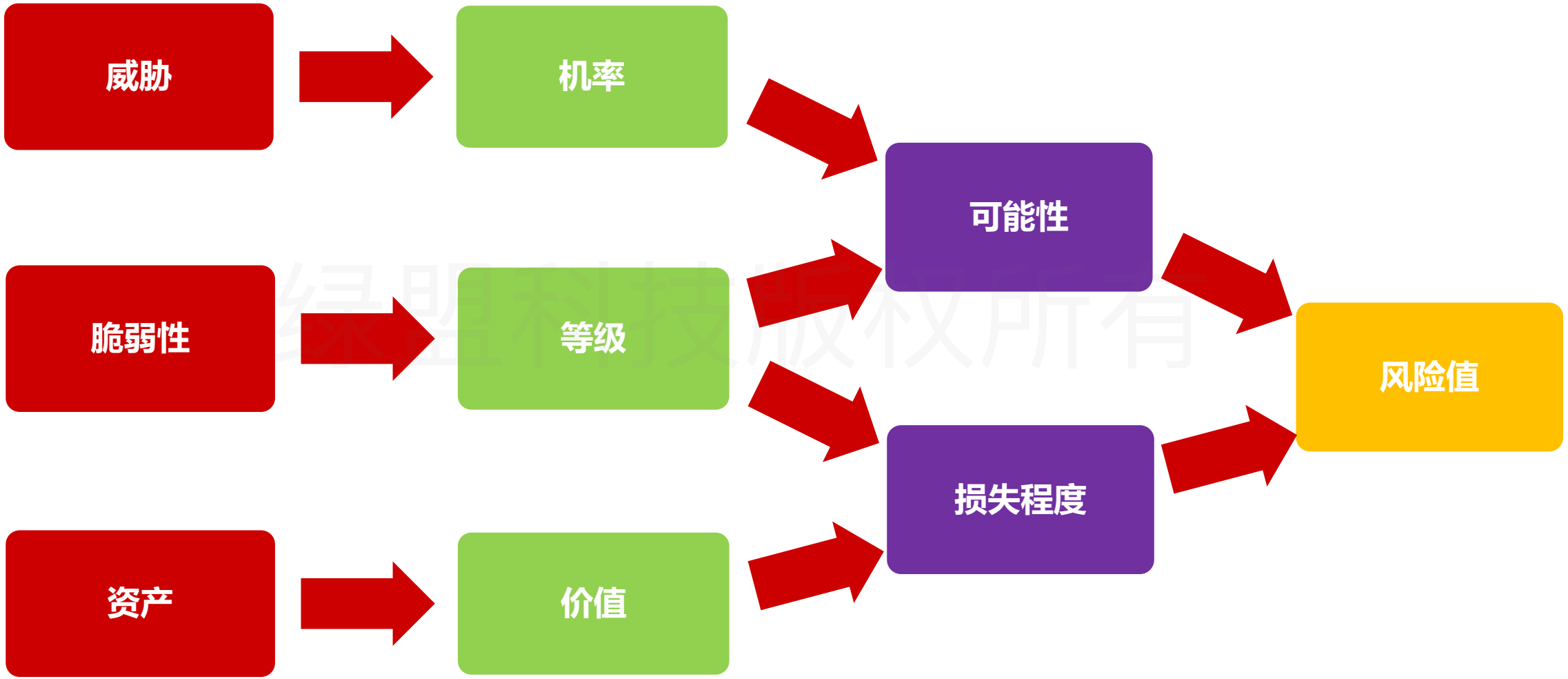
若不对自身应用进行安全防护，极易被病毒植入、广告替换、支付渠道篡改、钓鱼、信息劫持等，严重侵害企业和个人的利益。

自身安全

通过安全加固，将整个信息系统的安全状况提升到一个较高的水平，尽可能地消除或降低信息系统地安全风险

NSFOCUS

安全加固目标



目标：我们的目标是降低风险到可以接受。

1.2

角色与职责

参与加固的组织与职责

组织	职责	参与人员角色
绿盟科技服务团队	组建服务团队、制定实施方案、实施安全加固、接受用户监督、配合相关第三方的工作等	项目经理、安全加固实施工程师等
客户	确定项目负责人、配合项目实施、协调相关厂商、相关第三方的工作、对加固结果进行确认等。	项目接口人、系统管理员、配合人员
相关厂商	在客户人手不足，或客户系统由代维厂家维护情况下，由相关厂家人员配合项目实施、协助客户进行加固结果确认等	集成人员、代维人员等

要点识别

业务系统为单位

一般以“业务系统”为单位提供安全加固支持服务

相关厂商

客户并不了解待实施范围内资产的现网配置信息,依实际情况补充运维人员或外包人员的信息

明确干系人

明确各方人员的角色职责，高效沟通、提高加固效率

以实际加固项为单位

应根据加固项目的内容、范围和规模以及涉及到的组织和人员等因素确定安全加固支持服务的组织结构

1.3

安全加固总体框架

阶段划分

阶段	主要任务	主要工作成果	关键点
准备阶段	准备和落实项目所需的人员、设备、资料等资源；制定项目实施计划；制定加固方案；加固方案测试及审核；进行安全加固支持服务宣讲。	《项目实施计划》 《加固方案》 《加固清单》 《加固测试报告》	获得客户、项目经理对实施计划以及加固方案的认可
实施阶段	确认实施条件；进行安全加固并确认加固有效性。	《加固操作记录单》	安全加固实施
实施收尾阶段	交付所有的安全加固工作成果；服务汇报。	《工作成果交付清单》	服务结束

安全加固总体流程

项目调研集

1. 资产信息收集

制定实施方案

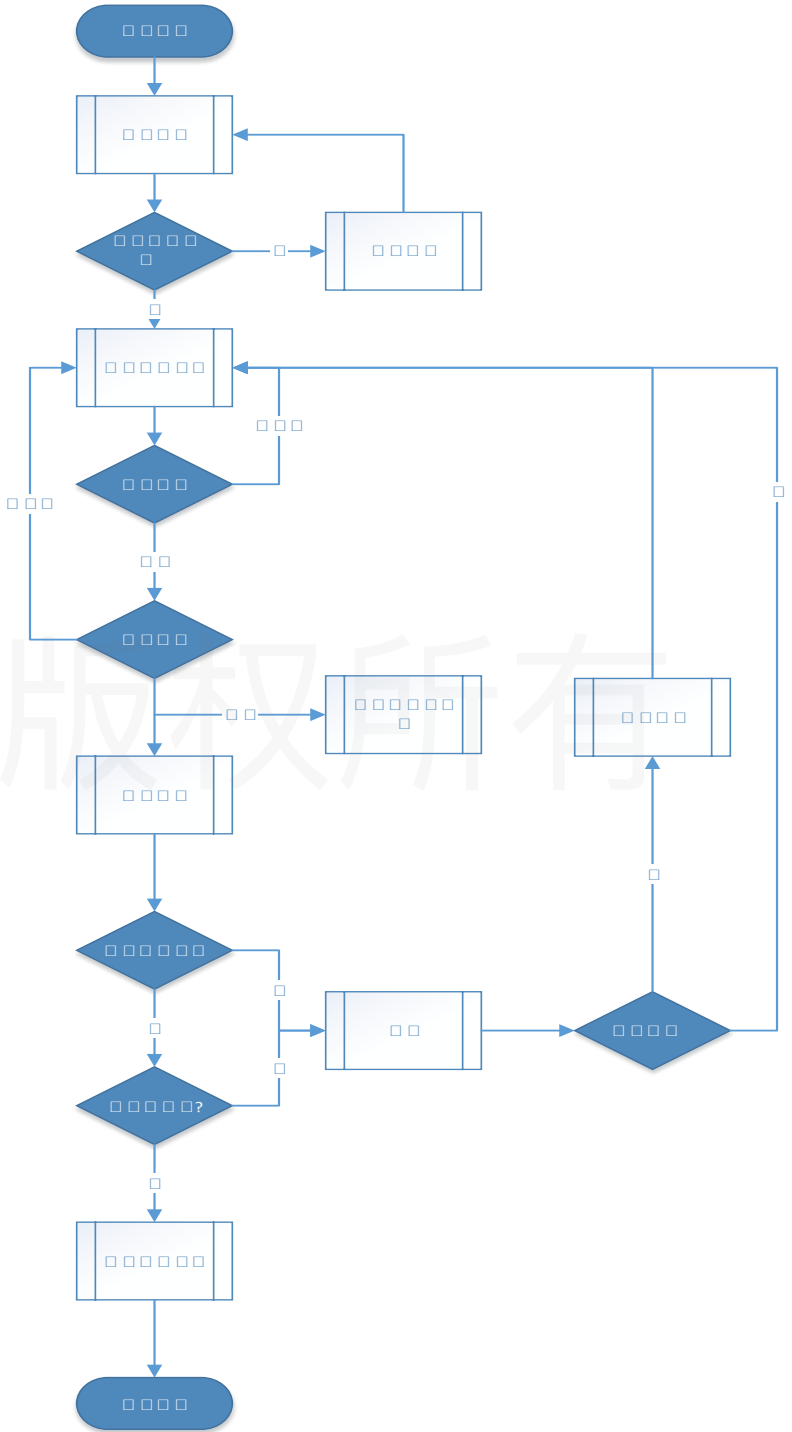
1. 加固测试
2. 方案审核
3. 数据备份

加固实施

1. 实施加固
2. 验证加固是否有效
3. 判断业务是否正常

验收汇报

1. 加固记录结果汇报



NSFOCUS

准备阶段

基础要素准备

- 确定安全加固的范围；
- 确定安全加固的时间进度；
- 确定安全加固的人力资源及沟通；

1

2

人员准备

- 确定安全加固支持的项目经理；
- 确定安全加固支持的实施人员；
- 确定安全加固支持的客户方人员；
- 确定安全加固支持的厂商支撑人员。

3

工具准备

- 确定加固工具
- 确定安全风险复测工具；
- 确定文档类工具。

4

制定加固实施方案

- 加固清单确认；
- 加固操作确认；
- 加固测试；
- 方案通过客户方审核。

5

人员培训

- 安全加固过程和方法介绍；
- 工作配合说明；
- 实施进度计划。

实施阶段

01

确认实施条件

- 实施环境、加固操作账号权限、实施申请流程、数据及配置备份、系统管理员及支撑厂商的配合

02

实施安全加固

- 按照加固方案选择不同的安全加固方法完成安全加固

03

确认加固效果

- 加固操作完成后，进行业务测试及有效性测试

04

结束安全加固

- 清理临时文件，输出安全加固操作记录单和实施报告

收尾确认

- 整理不同阶段输出的文档成果
- 提交项目成果文件

- 安全加固服务工作汇报
- 验收确认

02

安全加固准备

1. 前期准备
2. 制定安全加固实施方案
3. 安全加固测试
4. 方案审核

2.1

加固前准备

加固准备

01

目标

- 明确安全加固支持项目的客户信息、服务范围、工作计划等

02

范围

- 针对安全加固项目范围内的系统资产进行总体了解；确认工作计划、实施环境、客户接口人、流程要求、项目交付物等

03

输出

- 项目信息调研表
- 加固资产清单
- 安全加固支持服务实施计划

04

要点

- 确保加固资产无遗漏

2.2

制定安全加固实施方案

制定安全加固实施方案

01

目标

- 依据前期调研信息，确认安全加固优先级，选择恰当的安全加固方法，形成安全加固实施方案

02

方案原则

- 优先解决业务系统的高风险漏洞，其次解决中风险漏洞、低风险漏洞

03

输出

- 安全加固实施方案
- 安全加固清单
- 安全加固操作
- 配合工作清单

04

质量控制

- 项目经理对方案进行审核，确保实施质量

方案原则

版本升级

- 对于系统和应用在使用过程中暴露的安全缺陷，系统或应用厂商会及时发布解决问题的升级补丁包。升级系统或应用版本，可有效解决旧版本存在的安全风险。

关闭端口服务

- 在不影响业务系统正常运行情况下，停止或禁用与承载业务无关的服务和服务端口，可有效避免无关服务造成的安全风险。

修改配置项

- 操作系统（也包括网络设备和安全设备等）、数据库、中间件、第三方应用和业务系统可更改的配置中与安全相关的设置参数等信息，通过修改安全配置检查可以为网络和应用系统提供必要的安全保护。

方案原则

修改代码（可选）

- 修改代码一般由系统开发厂商完成。安全加固支持方仅提供加固建议及加固有效性验证。

主机/网络ACL策略

- 主机/网络ACL策略是一类临时安全加固方法。
- ACL通常应用在系统的出口控制上，可以通过实施ACL，可以有效的部署网络出网策略，控制对网内部资源的访问能力，进而来保障这些资源的安全性

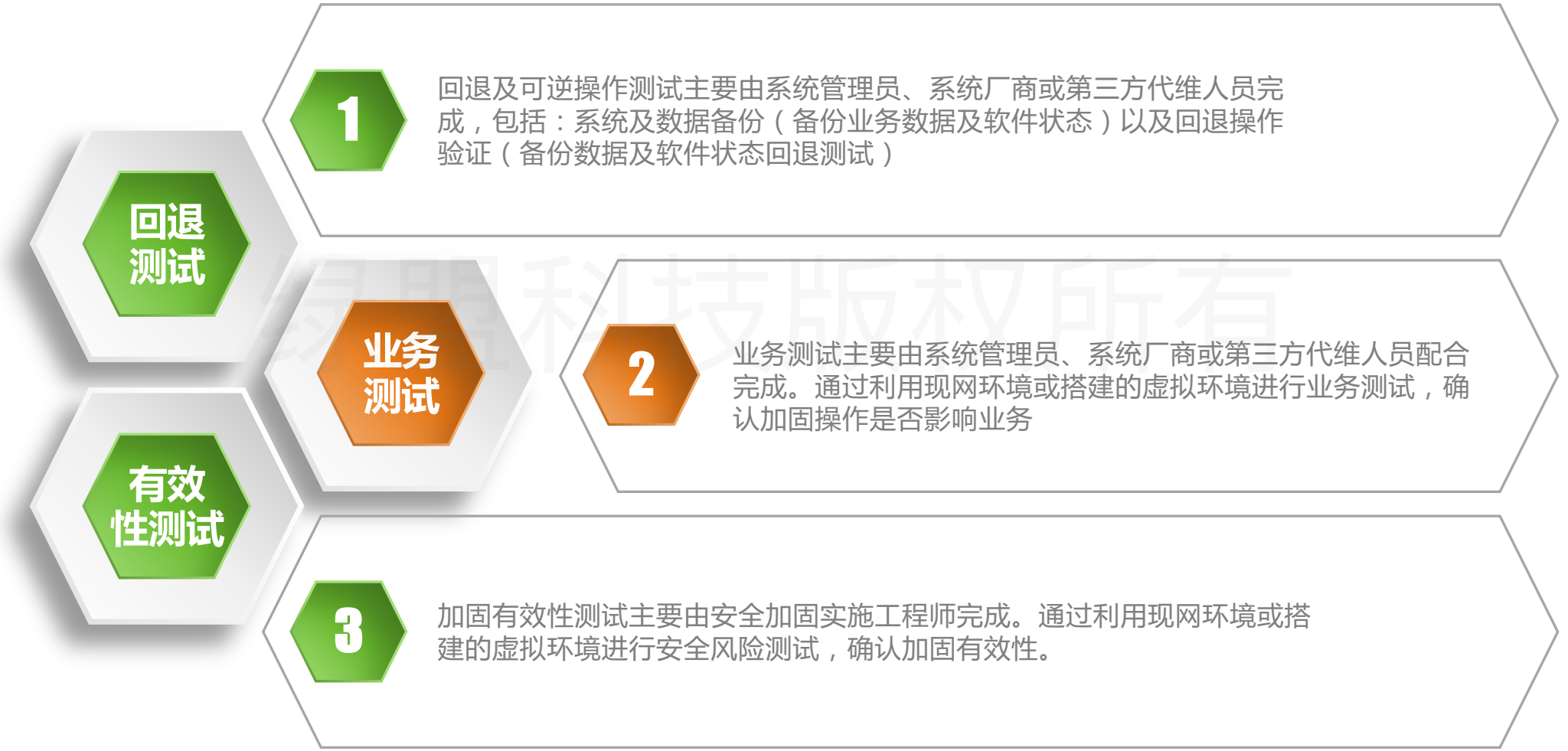
部署设备防护（可选）

- 部署设备防护是一类临时安全加固方法。
- 部署设备防护的安全加固方式一般由设备厂商完成。安全加固方仅提供防护设备策略配置建议及加固有效性验证。

2.3

安全加固测试

安全加固测试



2.4

方案审核

加固方案审核

目标

加固实施方案通过审核，
客户认可

输入

安全加固实施方案

范围

按客户方流程完成安全加固实施方案审核
由客户方接口人和主管领导对安全加固实施方案进行审核确认

输出

方案审核记录

03

安全加固操作

1. 版本升级
2. 关闭端口服务
3. 修改配置项
4. 主机/网络ACL策略

3.1

版本升级

版本升级-操作原则

一般不进行大版本升级

没有特殊情况，一般不进行大版本升级

例如MySql数据库从5.6升级到5.7

打补丁前必须做好原应用的备份工作

备份主要包括数据文件、配置文件，条件允许还要备份程序文件，确保能够完整恢复

备份操作一般由系统管理员或者系统厂商完成。应用升级前建议将旧版本以重命名的方式放在以前目录。同时注意收集旧版本目录的权限和属主设置

升级和打补丁时注意版本号和操作系统的匹配

升级包和补丁包通常有32位（i686、x86）和64位（x64）之分，需根据操作系统的版本号来确定要下载的版本；另外，对于Linux系统，部分安装包还跟Linux的发行版本有关

比如：Red Hat Linux的程序包可能无法在Debian上运行），需要找对发行版本

版本升级-基本操作步骤

1

确定应用安装位置

针对不同系统类型对应用安装位置进行定位

2

从官网下载补丁文件

补丁文件的下载地址在风险评估报告的整改建议内会有体现

3

将加固中需要的文件上传至服务器

一般通过ssh或者ftp的方式进行上传

4

软件和补丁安装

严格按照软件和补丁的安装说明进行软件和补丁的安装工作，同步修改权限与属主

版本升级-基本操作步骤

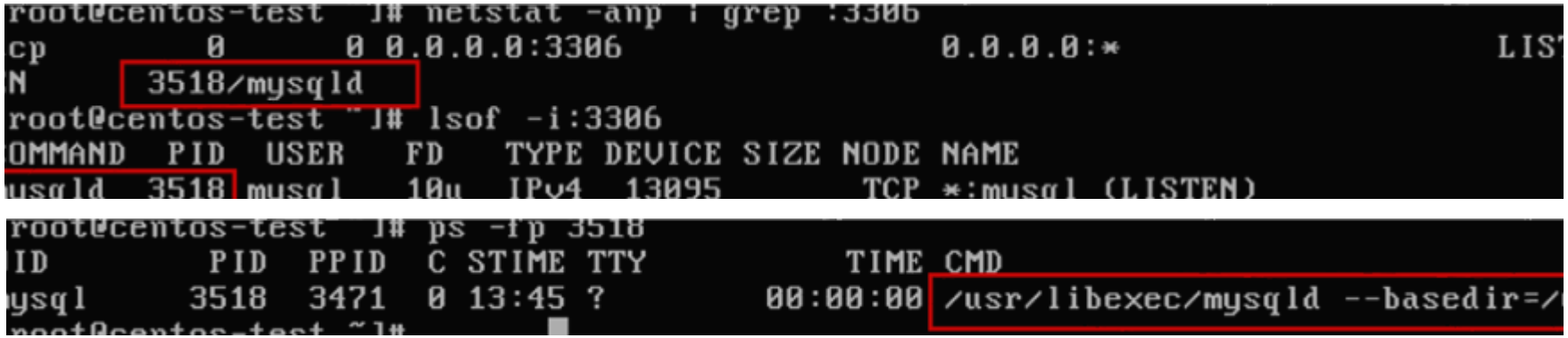
Windows系统

- 对于windows系统，可以查看应用属性的方式找到应用的安装位置

Linux类系统

- a)根据评估报告，确定应用所在端口

- b)通过端口定位web服务的根目录所在位置



3.2

关闭端口服务

关闭端口-操作原则

管理员需提供系统实际需要的服务及端口列表，将风险评估报告涉及的存在安全风险的服务端口与实际需要的服务及端口列表进行对比

应关闭或禁用的服务端口

存在安全风险的服务端口与业务应用无关，并且为不必要的服务和启动项

明确用途

无法确定

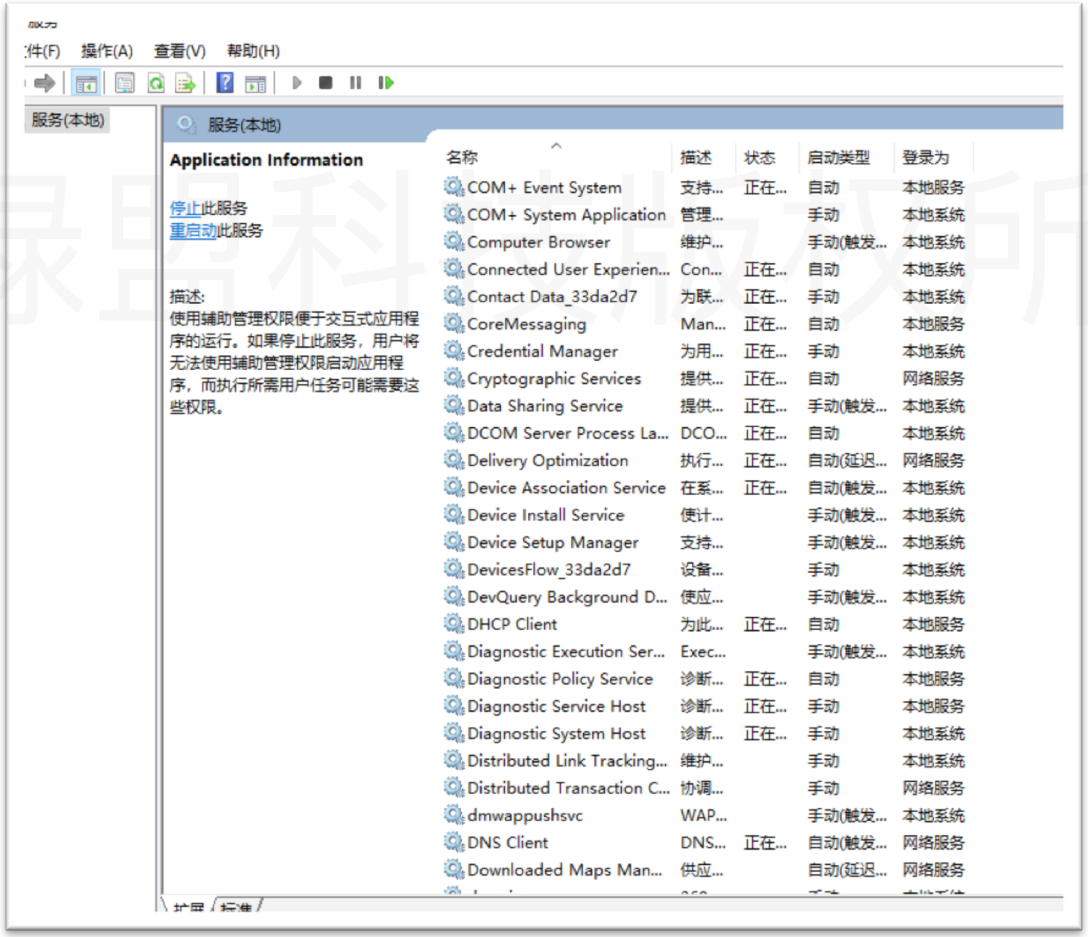
无法确定用途的端口

不建议采用关闭服务端口的方式进行加固，或者在执行服务端口关闭操作前进行严格的测试

关闭端口-基本操作步骤

Windows系统

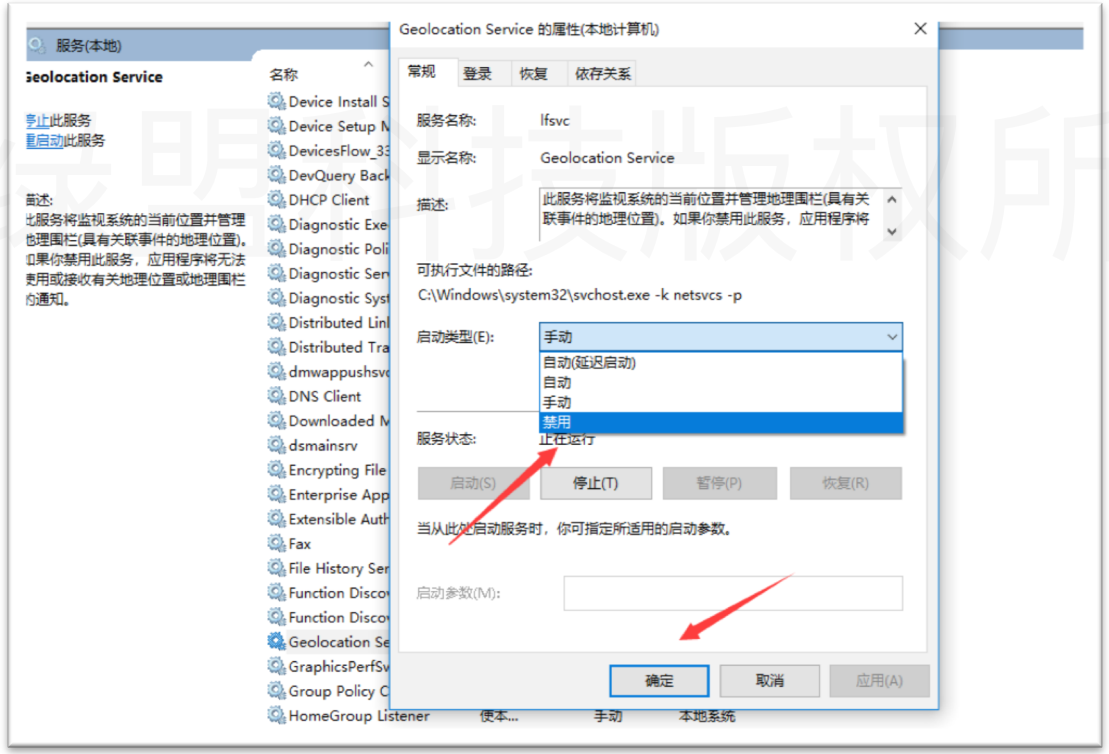
- a)开始 | 运行 | services.msc | 或者 进入“控制面板->管理工具->计算机管理”，进入“服务和应用程序”



关闭端口-基本操作步骤

Windows系统

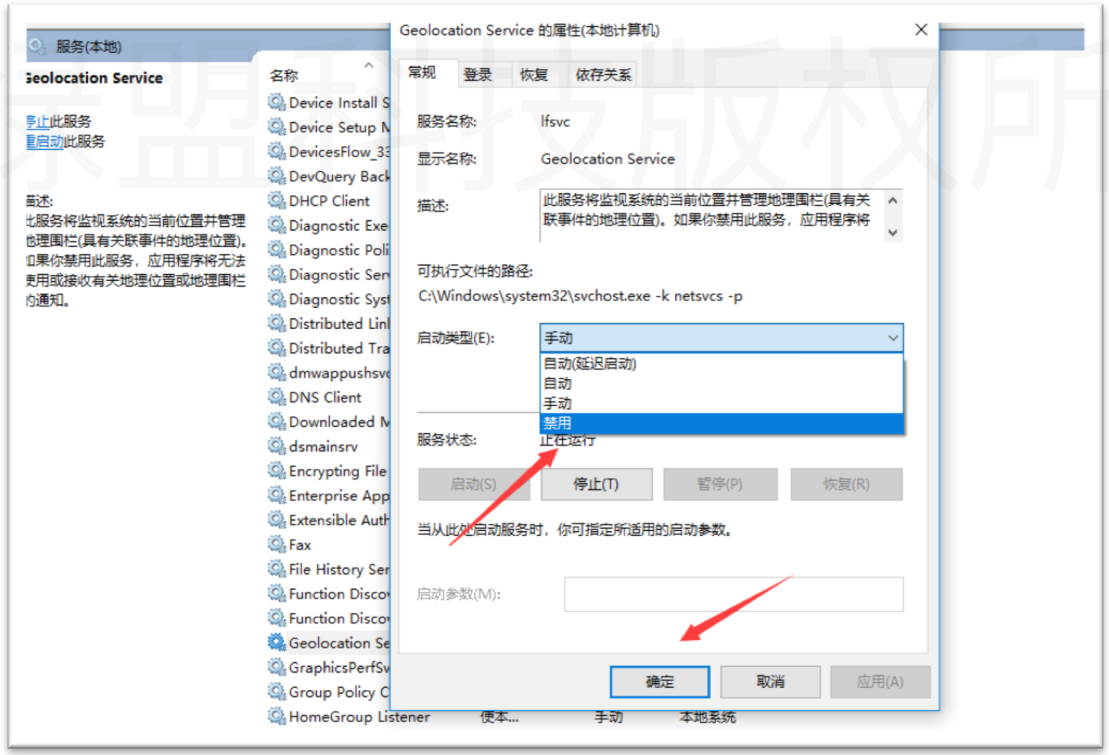
- b)选定需要关闭的服务，右键单击，在弹出的菜单中选择“属性”，会弹出属性对话框



关闭端口-基本操作步骤

Windows系统

- b)选定需要关闭的服务，右键单击，在弹出的菜单中选择“属性”，会弹出属性对话框
- c)点击“启动类型”，选择“禁用”然后点击确定按钮和应用按钮即可



关闭端口-基本操作步骤

Linux类系统

- a)查看所有开启的服务：
- #ps –ef
- #chkconfig –list
- b)在xinetd.conf中关闭不必要的服务：
- #cat /etc/xinetd.conf
- 首先复制/etc/xinetd.conf:
- #cp /etc/xinetd.conf /etc/xinetd.conf.backup
- 然后用vi编辑器编辑xinetd.conf文件，对于需要注释掉的服务在相应行开头标记"#"字符，重启xinetd服务,即可。

3.3

修改配置项

修改配置项-基本操作步骤

1）根据配置核查报告进行修改配置项加固

- 参照配置核查报告或者各行业安全配置规范进行安全加固操作

项目编号	NOMD-2013-SC-SUSE-01-02-v1
配置说明	应删除或锁定与设备运行、维护等工作无关的账号，删除过期账号。
配置指南	**1、参考配置操作** 删除用户：#userdel username; 锁定用户： 1)修改/etc/shadow 文件，用户名后加*LK* 2)将/etc/passwd 文件中的 shell 域设置成/bin/false 3)#passwd -l username 只有具备超级用户权限的使用者方可使用，#passwd -l username 锁定用户,用 #passwd –d username 解锁后原有密码失效，登录需输入新密码，修改 /etc/shadow 能保留原有密码。 **2、补充说明** 需要锁定的用户：listen,gdm,webservd,nobody,nobody4,noaccess。 对于具体系统，应基于工作相关原则，删除无用账号。
检测方法及判定依据	**1、符合性判定依据** 使用应删除或锁定账号无法登录系统 **2、参考检测方法** 分别使用应删除或锁定的与工作无关的账号登录系统，应无法登录成功。 **3、补充说明** 需要锁定的用户：listen,gdm,webservd,nobody,nobody4,noaccess。 可参考系统用户及账户登记记录，明确无关账号。
备注	

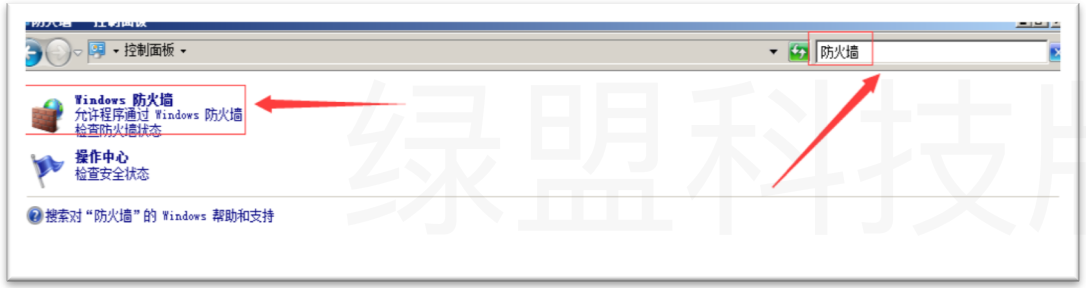
3.4

主机/网络ACL策略

ACL策略-基本操作步骤

1）Windows 系统（windows 2008）通过系统防火墙建立ACL策略

- 通过ACL策略控制特定ip才能访问服务器，屏蔽其他无关ip用户访问系统。
- a）进入服务器打开控制面板搜索防火墙



- b）选择windows防火墙——打开或关闭windows防火墙

ACL策略-基本操作步骤

- c)启用防火墙，（注意不要勾选第一个复选框，勾选之后自己也将无法连接服务器），确认

- d）选择windows防火墙——高级设置

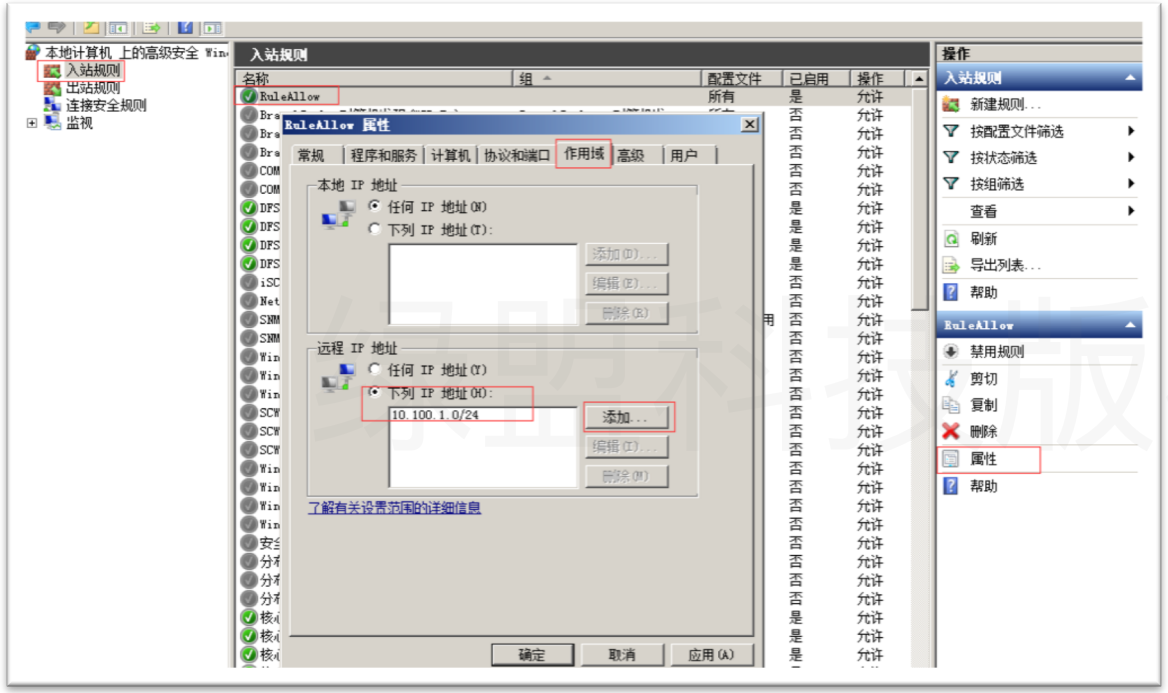
ACL策略-基本操作步骤

- e) 选择入站规则——新建规则

- f) 选择端口——下一步，依据实际情况配置对应的协议、端口、动作

ACL策略-基本操作步骤

- g)选择入站规则——RuleAllow——属性——作用域——添加需要添加的ip，完成策略配置。



ACL策略-基本操作步骤

2）华为交换机ACL策略示例

- 配置高级IPv4 ACL 3000，允许129.9.0.0网段的主机向202.38.160.0网段的主机发送端口号为80的TCP报文

配置步骤：

a) 进入系统视图：system-view
b) 创建acl 并进入acl视图：acl number 3000
c) 定义acl规则：rule permit tcp source 129.0.0.0 0.0.255.255 destination 202.38.160.0 0.0.0.255 destination-port eq 80
d) 查看acl策略配置情况：display acl 3000

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule permit tcp source 129.9.0.0 0.0.255.255 destination 202.38.160.0
0.0.0.255 destination-port eq 80
[Sysname-acl-adv-3000] display acl 3000
Advanced ACL  3000, named -none-, 1 rule,
ACL's step is 5
 rule  0  permit  tcp  source  129.9.0.0  0.0.255.255  destination  202.38.160.0  0.0.0.255
destination-port eq www (5 times matched)
```

04

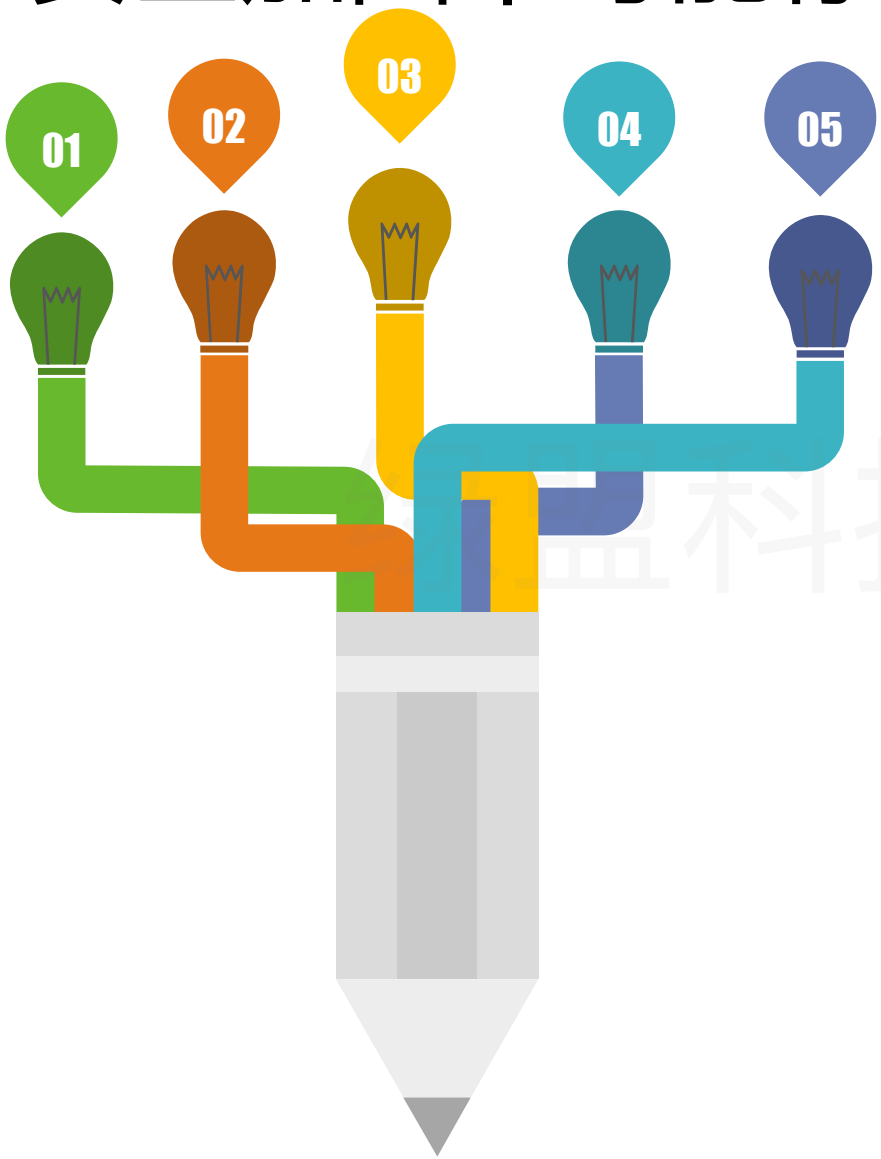
如何规避加固风险

1. 常见加固风险
2. 风险规避手段
3. 加固风险案例解析

4.1

常见加固风险

安全加固中可能存的风险



网络设备

01 升级OS

可能导致网络设备无法正常工作（事先需对OS、配置文件进行备份，一旦发现问题立即退回）

02 配置访问列表

可能导致某些用户无法访问、管理复杂度上升（改回即可恢复）

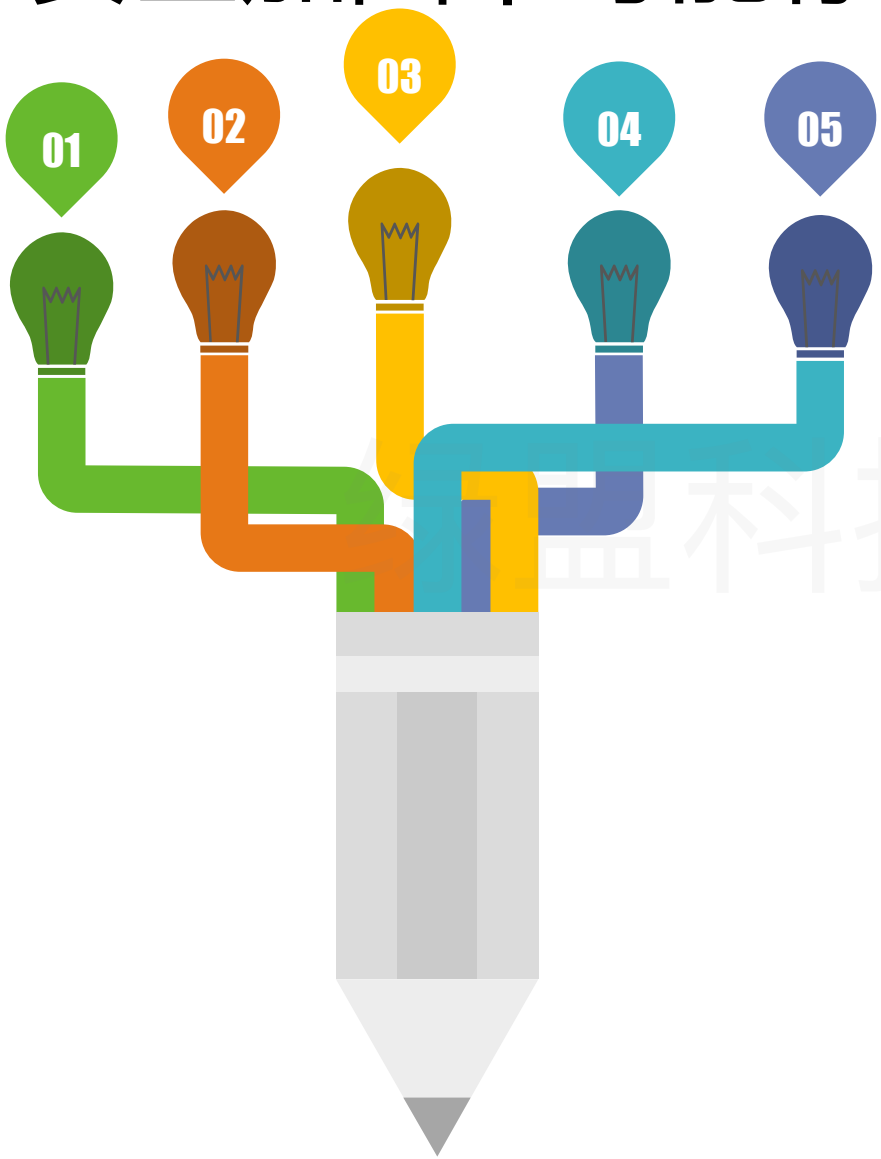
03 关闭不必要的服务

可能导致部分相关服务不可用，改动前需经网络管理员确认（改回即可恢复）

04 路由协议安全配置

可能导致网络连接不正常（改回即可恢复）

安全加固中可能存的风险



操作系统

01 **安装Patch**

能会导致某些特定的服务不可用甚至主机崩溃，尽量采用可卸载的Patch安装方式

02 **修改配置文件**

可能导致某些特定服务不可用（改回配置文件即可恢复）

03 **关闭不必要的服务**

可能导致某些应用程序不可用，需管理员事先确认（重新启动服务即可恢复）

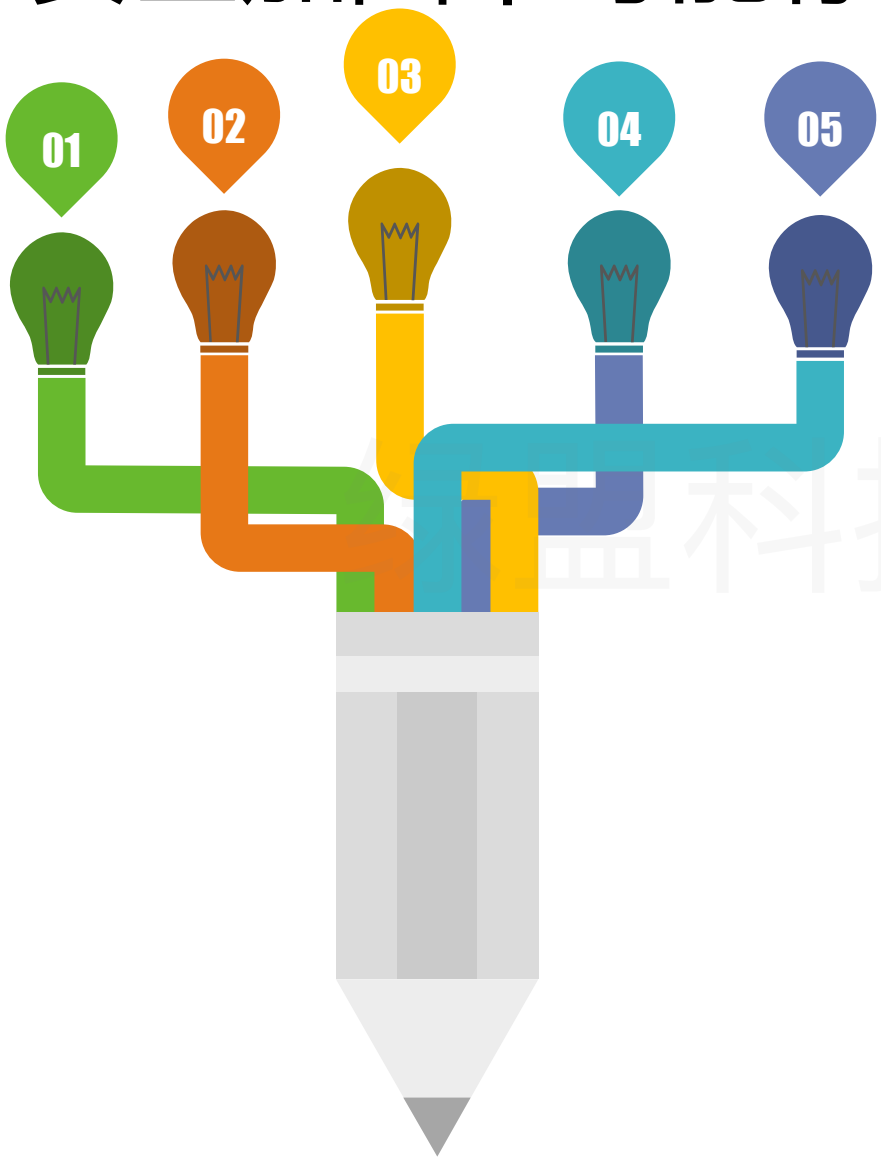
04 **应用程序升级或配置调整**

可能导致应用程序运行不正常（改回配置即可恢复）

05 **文件系统加固**

调整重要系统文件的安全属性和存取权限：可能导致某些程序无法正常运行（改回属性和权限即可恢复）

安全加固中可能存的风险



数据库

01 安装Patch

可能导致数据库无法正常工作，其他依赖于数据库的应用程序也将受到影响（根据我司的实施经验由实施工程师提出建议，由数据库管理员进行确认，必要时可咨询厂商技术人员）

02 修改数据库账户密码

可能导致某些登陆数据库的应用程序需要重新设置（加固前通知相关应用系统管理员，同时设置应用程序）

03 禁用数据库系统不必要的网络协议

可能导致某些依赖于相关协议的应用程序无法正常工作（改动前需由数据库管理员进行确认）

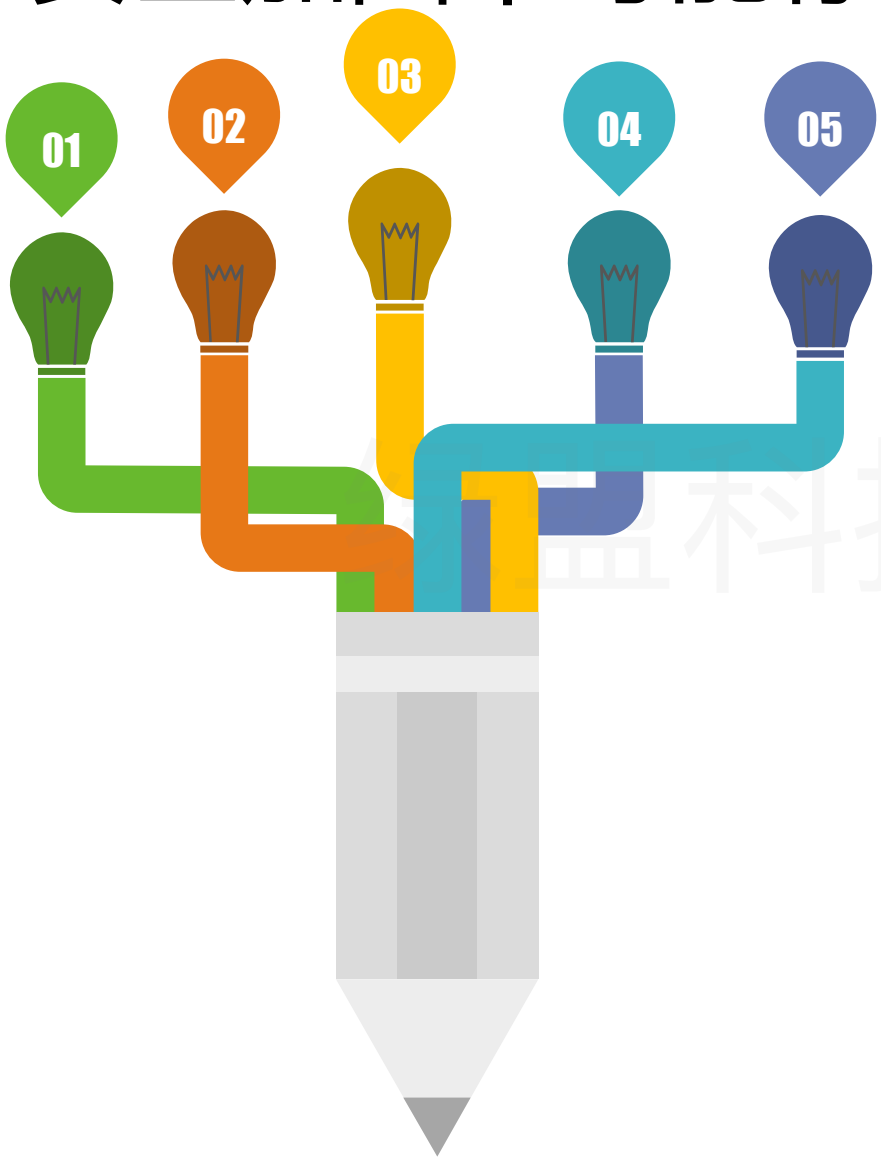
04 分配数据库文件访问权限

可能导致被遗漏的用户无法访问相关文件（重新设置即可）

05 删除无用的/扩展存储过程

可能导致数据库的某些功能无法使用，实施前需经数据库管理员确认

安全加固中可能存的风险



中间件及常见网络服务

01

安装Patch

可能导致中间件或网络服务无法正常工作，其他依赖于这些中间件的应用程序也将受到影响（根据我司的实施经验由实施工程师提出建议，由系统管理员进行确认，必要时可咨询厂商技术人员）

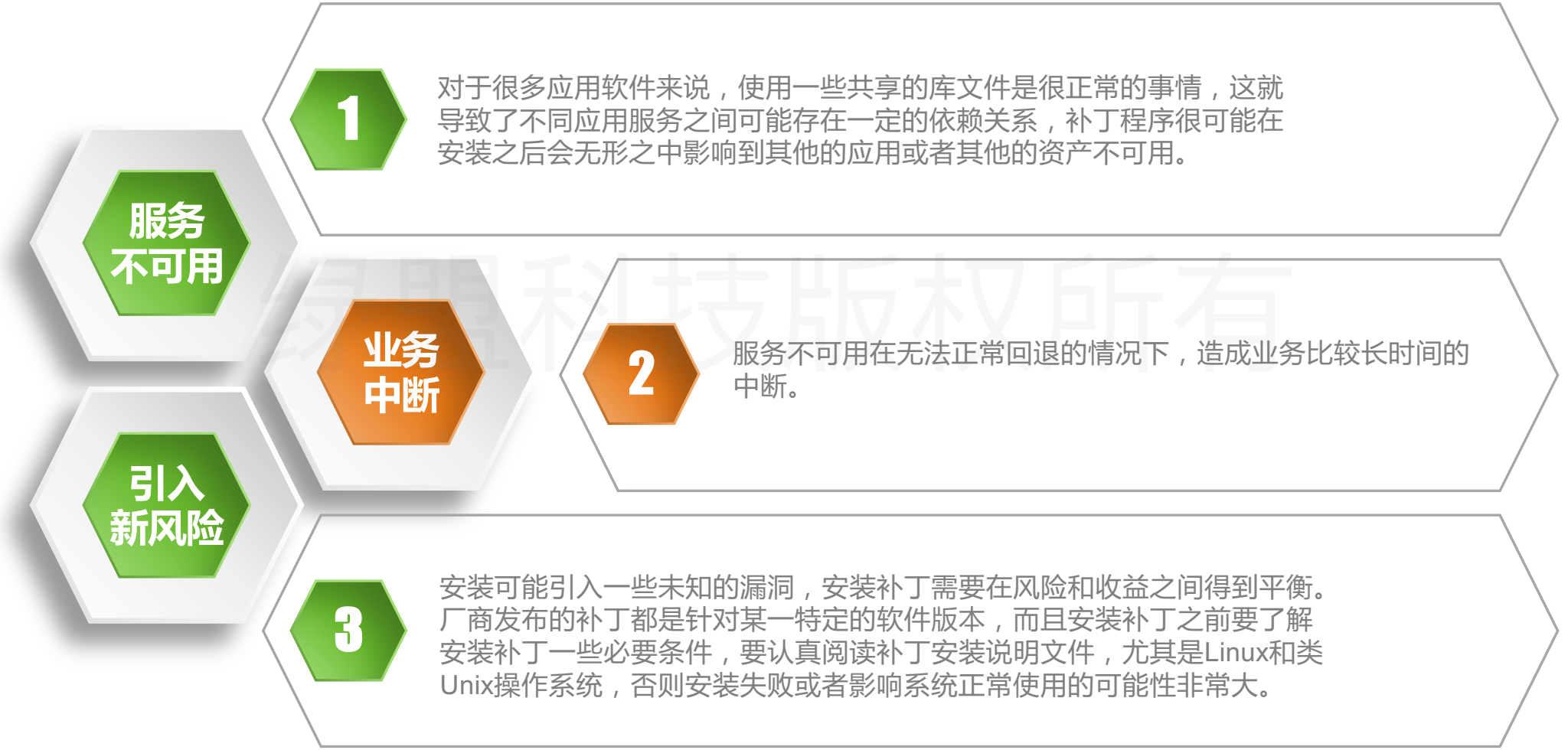
02

修改某些默认的安全配置

可能导致某些关联的程序不可用，需管理员事先确认（修改回原来的配置即可恢复）

NSFOCUS

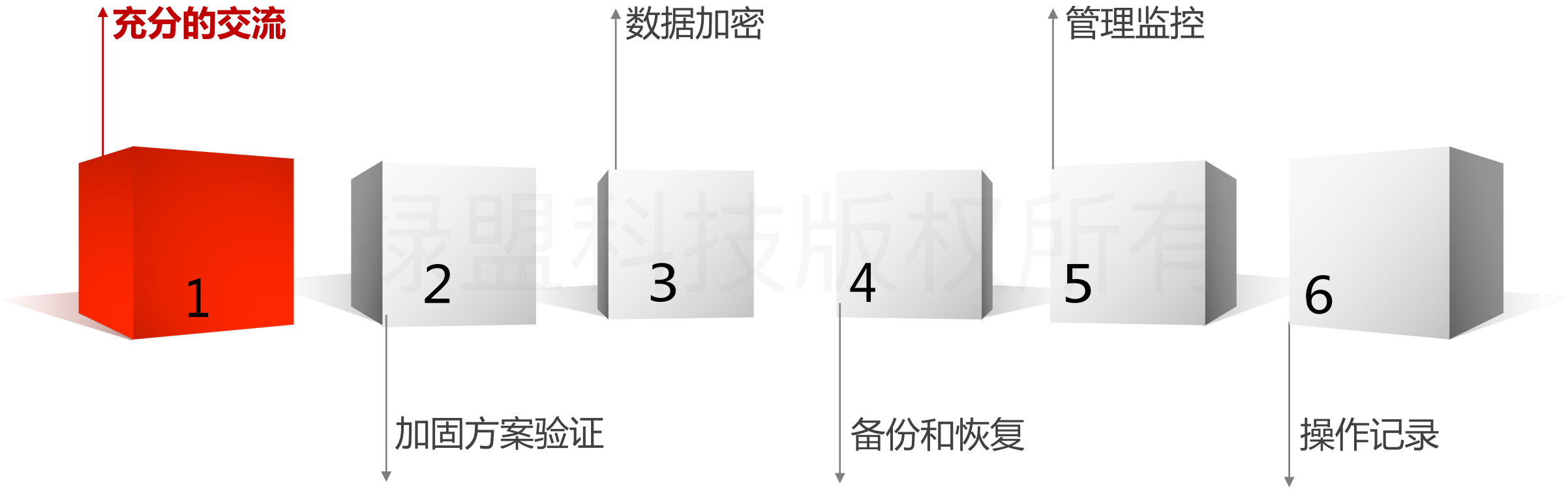
常见加固风险



4.2

风险规避手段

风险规避手段



加固方案验证

加固有效性测试

1. 利用现网环境或搭建的虚拟环境进行安全风险测试，确认加固有效性。

回退及可逆操作测试

1. 系统及数据备份（备份业务数据及软件状态）以及回退操作验证（备份数据及软件状态回退测试）

业务测试

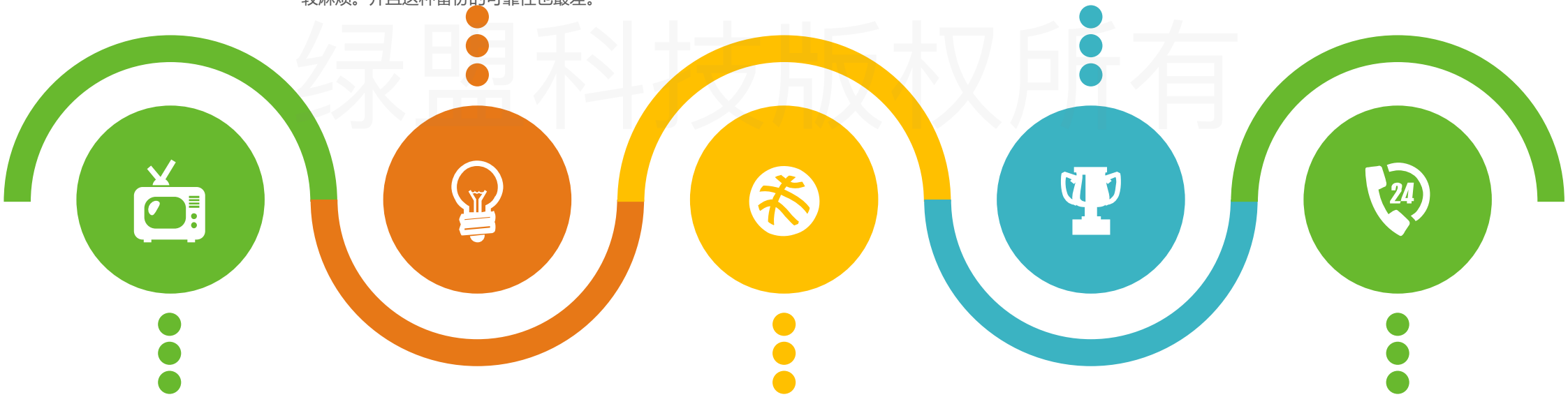
1. 通过利用现网环境或搭建的虚拟环境进行业务测试，确认加固操作是否影响业务。

备份和恢复

无论采用何种备份方式，系统备份的数据一定要进行了有效验证和妥善保管。

增量备份：备份的数据只是相对于上一次备份后新增加的和修改过的数据。这种备份的优点很明显：没有重复的备份数据，既节省了存储空间，又缩短了备份的时间。但它的缺点在于当发生灾难时，恢复数据比较麻烦。并且这种备份的可靠性也最差。

文件系统备份：对主机系统而言，要进行文件系统的备份。应根据具体需求对此次加固过程中可能所产生的不稳定情况制定良好的备份策略，从而确保业务系统的正常稳定运行。



全备份：对整个系统进行完全备份，包括系统和数据。这种备份方式的好处就是很直观，容易被人理解。而且当发生数据丢失时，只要用全备份就可以恢复丢失的数据。不足之处：如果需要备份的数据量相当大，备份所需时间较长。

差分备份：备份的数据是相对于上一次全备份之后增加的和修改过的数据。差分备份在避免了另外两种策略缺陷的同时，又具有了它们的所有优点。

冗于备份：系统的所有模块均可以进行冗余分布式配置，安装相同模块的主机之间互为备份。

NSFOCUS

备份和恢复

恢复总是与一定类型的失效相对应的。在系统加固过程中如果出现被加固系统没有响应的情况，应当立即停止加固工作，与被加固系统管理员一起分析情况，在确定原因后，由被加固系统管理员或厂商对系统进行正确恢复。

4.3

加固风险案例解析

加固风险案例解析

OpenSSL漏洞(CVE-2014-0160)安全加固

信息收集

1. 明确漏洞存在的资产
2. 明确漏洞受影响的版本(OpenSSL 1.0.1f、OpenSSL 1.0.2-beta)
3. 收集漏洞修复的方法：版本升级和禁用Heartbleed模块

制定加固方案

1. 确认安全加固优先级：先备后主
2. 选择恰当的安全加固方法：单机可以禁用Heartbleed模块，集群升级无漏洞的SSL版本

加固测试

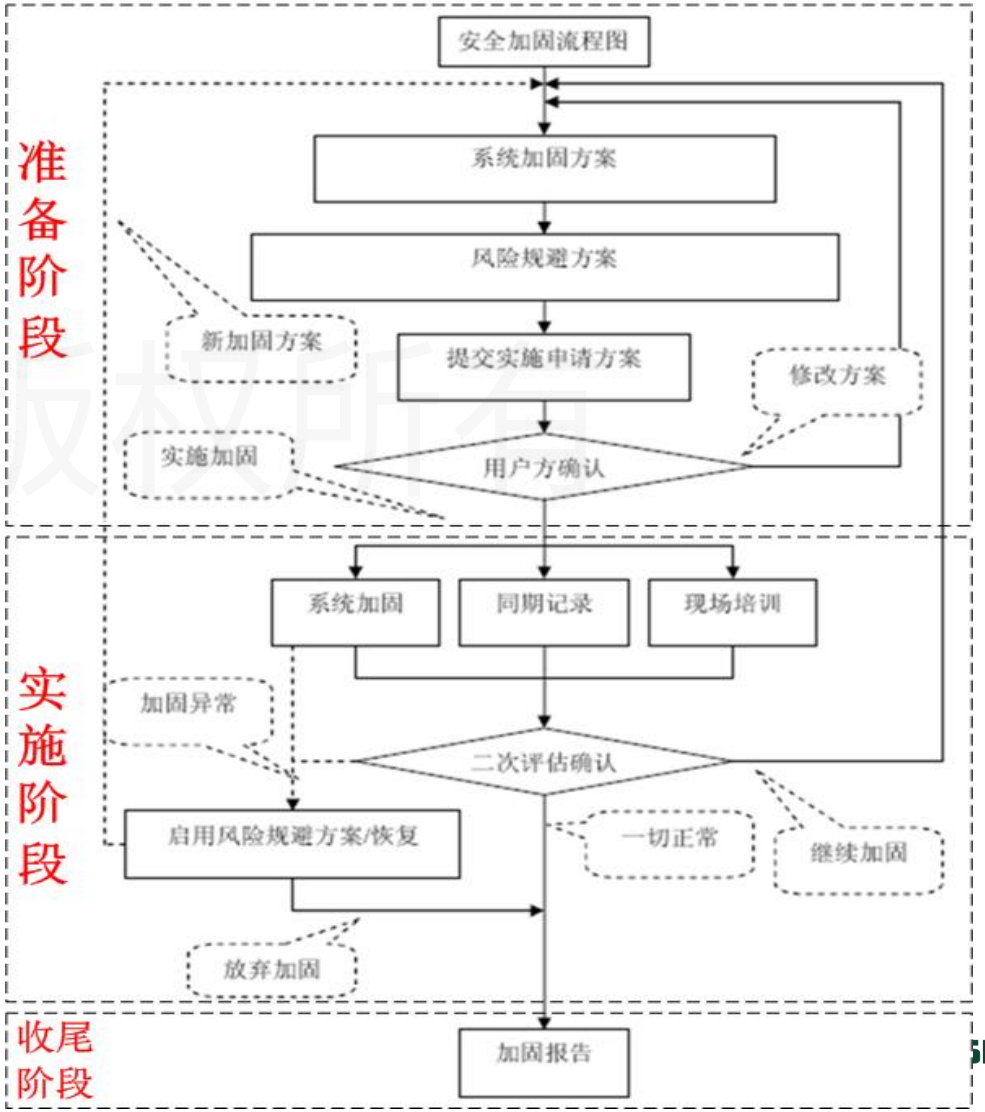
1. 搭建测试环境或准生产环境进行加固测试
2. 回退及可逆操作测试
3. 业务可用性测试

方案审核

1. 对安全加固实施方案进行审核
2. 确认风险规避手段
3. 确认安全加固的时间、人员、帐号权限等

实施加固

1. 依据加固方案和加固清单完成SSL版本的升级
2. 确认加固的有效性和对业务的影响。



加固风险案例解析

Memcached服务器UDP反射放大攻击安全加固

信息收集

1. 明确漏洞存在的资产
2. 明确漏洞受影响的端口 UDP：11211
3. 收集漏洞修复的方法：关闭端口、访问控制、绑定监听IP、启用认证

制定加固方案

1. 确认安全加固优先级：先备后主
2. 选择恰当的安全加固方法：业务端口进行访问控制、非业务端口进行关闭

加固测试

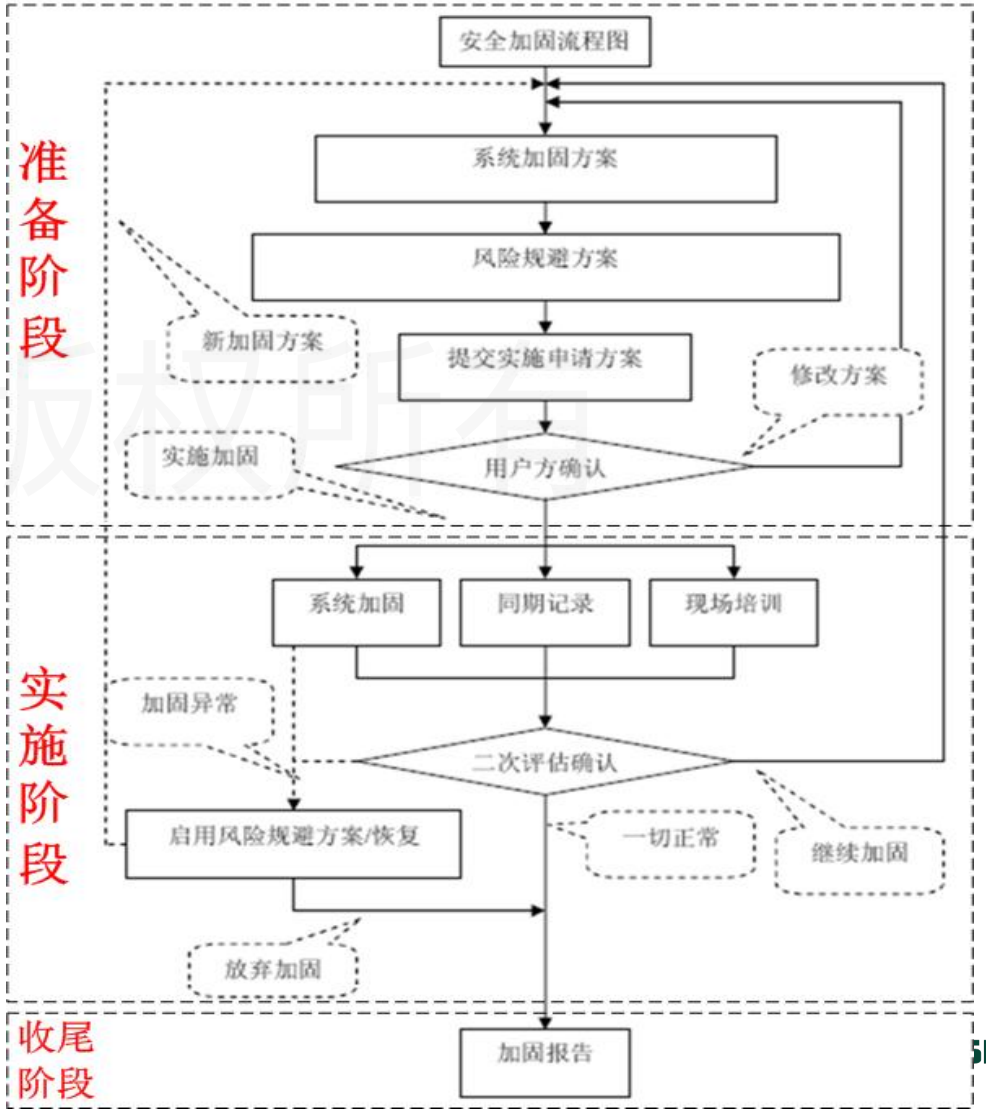
1. 搭建测试环境或准生产环境进行加固测试
2. 回退及可逆操作测试
3. 业务可用性测试

方案审核

1. 对安全加固实施方案进行审核
2. 确认风险规避手段
3. 确认安全加固的时间、人员、帐号权限等

实施加固

1. 依据加固方案和加固清单完成端口的关闭。
2. 确认加固的有效性和对业务的影响。



加固风险案例解析

Oracle提权漏洞安全加固

信息收集

1. 明确漏洞存在的资产
2. 明确漏洞受影响的版本：10g
3. 收集漏洞修复的方法：版本升级和数据库防火墙虚拟补丁

制定加固方案

1. 确认安全加固优先级：先备后主
2. 选择恰当的安全加固方法：数据库防火墙虚拟补丁
   （1）解析出会话的用户名：证明不是sys用户，可能会是一种越权行为。
   （2）对语句进行进一步验证：证明语句中包含有常被用来的攻击的字段名：dbms_metadata，并且含有函数get_ddl。
   （3）满足上述条件，可以猜测为攻击行为。
   （4）最后验证语句并非查询类型select ....，排除正常行为。

加固测试

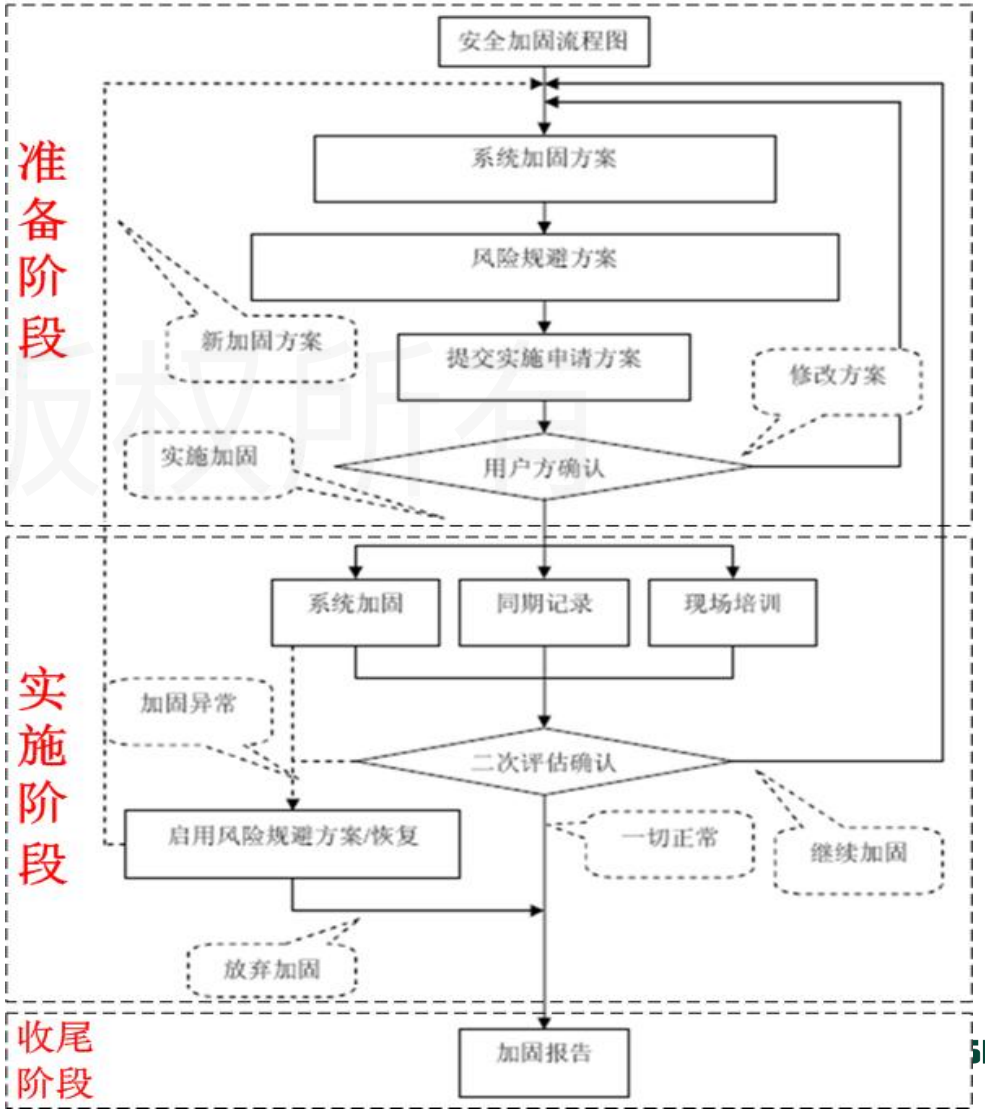
1. 搭建测试环境或准生产环境进行加固测试
2. 回退及可逆操作测试
3. 业务可用性测试

方案审核

1. 对安全加固实施方案进行审核
2. 确认风险规避手段
3. 确认安全加固的时间、人员、帐号权限等

实施加固

1. 依据加固方案完成虚拟补丁，并在数据库防火墙完成部署。
2. 确认加固的有效性和对业务的影响。



加固风险案例解析

安全域安全加固

信息收集

1. 明确网络面临的风险
2. 行业合规要求
3. 各个区域之间通信受到限制，区域内部通信多不进行限制

制定加固方案

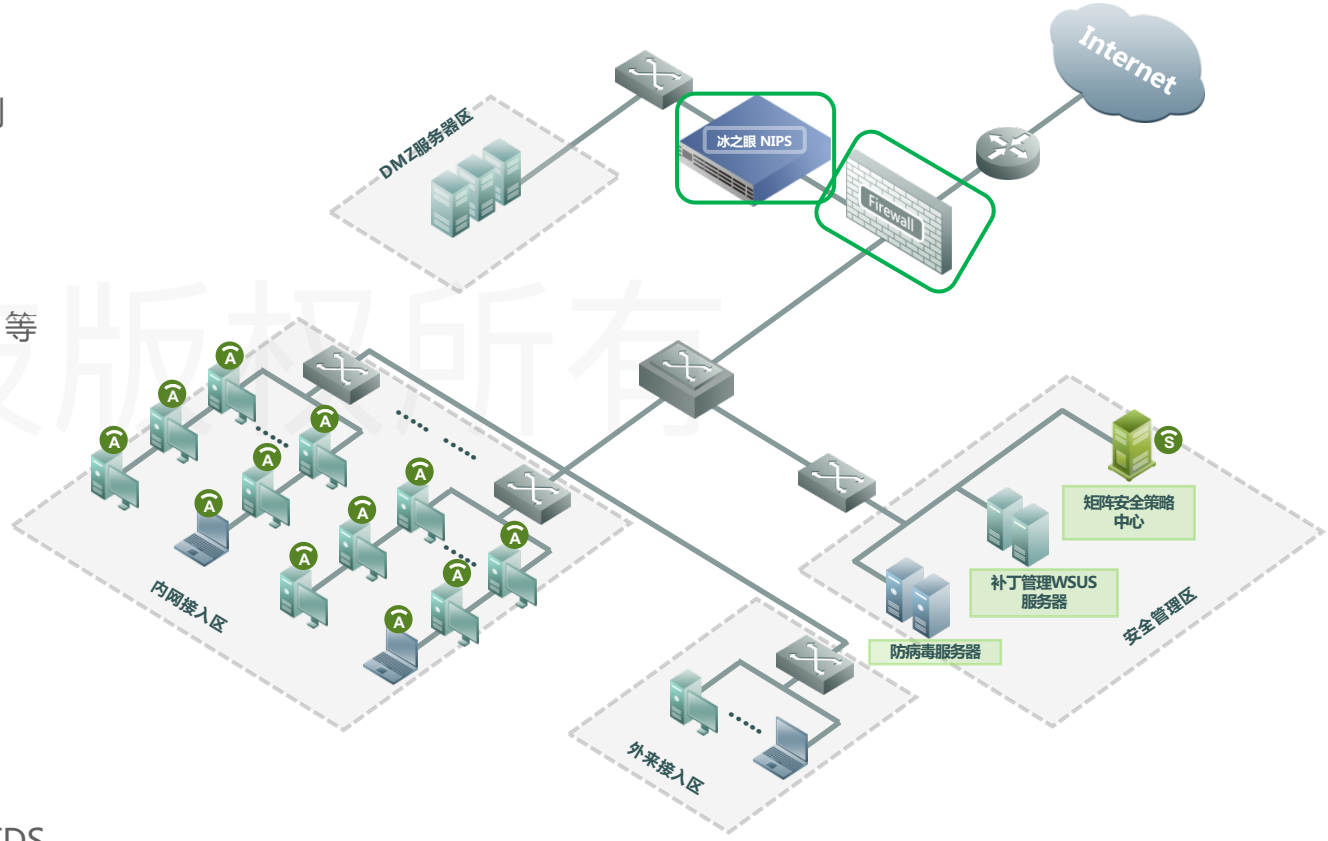
1. 面临的风险部署防护设备
2. 行业合规要求：双层异构防火墙、日志审计（等保三级）等
3. 按照业务安全需求进行安全域划分，区域之间隔离

方案审核

1. 对安全加固实施方案进行审核
2. 确认风险规避手段
3. 确认安全加固的时间、人员、帐号权限等

实施加固

1. 网络改造一般在生产环境进行加固测试
2. 依据加固方案在各个高风险安全域的核心交换机上部署IDS，做好网络安全监控，并且在安全域出入口处部署防火墙。
3. 确认加固的有效性和对业务的影响。



NSFOCUS

谢谢！

NSFOCUS