



# 首届“奇安信杯”中国医院 网络安全攻防攻防比赛经验 分享

吴邦华

四川大学华西第二医院信息中心主任

## 目录

CHIMA网络安全攻防大赛经验分享

“攻防演练” 防守工作方案介绍

医院信息安全之 “我见”



7月4日：现场培训，对CTF赛制、题型等进行了集训

7月6日：正式比赛，比赛分三个轮次：

**第一轮：20分钟基础知识赛（50道题）**

各战队三名参赛选手分别进入不同的线上系统进行答题，题目各不相同，主要涉及安全运维，法律法规，linux操作系统等



### 第二轮：50分钟CTF夺旗（5道题）

各战队通过解决组委会设置的各项网络安全技术挑战题目来完成比赛，题目涵盖**密码学**（运用多种工具，如ASCII对照，古典密码，凯撒密码，栅栏密码，BASE64，莫斯解密等等对各类变形加密的符号文字等进行解密，提交答案），

**WEB题**（运用多种工具，设置本地代理抓包、改包，找出Web漏洞，如注入，XSS，文件包含等），**安全杂项**（流量分析，电子取证，数据分析等），**逆向工程**（要求使用OD进行反编译，设置断点程序破解），**隐写术**（题目的flag会隐藏到图片、视频、音频等各类数据载体中，要求选手获取提交）等等内容





1、分工明确，每人负责不同的题目，因为比赛机制为前三个做出题目的队伍有对应的分数加成。

2、比赛题目包括web注入、数据加解密、数据隐写、逆向分析等，最终我们三人共做出4道题目，最后一题作为最不常见的安卓APP逆向，我们本着不放弃的精神，一直到比赛最后一刻，一直尝试破解这个安卓APP，可惜技术欠缺，未能出结果。



第三轮：60分钟攻防混战（前20分钟windows靶机安全加固，后40分钟攻防混战）

安全加固主要是针对操作系统进行安全加固，包括修改端口号，做服务器ipsec安全策略，注册表的修改，隐藏用户的删除，webshell的查杀，防火墙的开启与设置，准备各类补丁包等等

攻防混战则是各战队模拟网络中的黑客，在防守己方服务器的同时要寻找对方的漏洞并攻击对方得分。（主办方提供一台用于生成flag的服务器，只要攻破这个服务器，就会得到一个flag字符串，我们需要找到对方靶机的漏洞，并在对方靶机上执行访问生成flag服务器的命令curl，在比赛平台上提交flag）



排名	战队名称	总分	奖项
1	四川大学华西第二医院	430	一等奖
2	郑州市中心医院	415	二等奖
3	北京友谊医院	365	二等奖
4	青海大学附属医院	364	二等奖
5	朝阳市中心医院	349	三等奖
6	西南医科大学附属医院	348	三等奖
7	陆军特色医学中心	346	三等奖
8	北京同仁医院	346	三等奖
9	江苏省中医院	325	三等奖
10	帅府校尉队	322	三等奖



## 攻防阶段：






- 1、第一时间备份服务器web代码，ssh远程上去主办方已经将代码打包好，先备份到本地，防止被其他攻击队伍删除代码。
- 2、备份好代码以后，负责攻击的队友开始审计代码，寻找漏洞
- 3、负责防御的队友开始加固，一个人负责加固服务器，修改ssh密码，修改mysql密码等；一个人负责加固web应用，修改两个web应用的后台默认口令
- 4、负责审计的队友发现web应用存在已知的web后门，随即告诉加固应用的队友删除对应的后门，防止其他人利用后门进行攻击。
- 5、发现已知后门以后，负责加固服务器的队友开始利用已知后门，使用burpsuite工具抓包对其他队伍进行攻击。
- 6、批量化攻击：原计划使用python脚本进行批量化攻击，获取对手的flag



在线工具: <http://ctf.ssleye.com/> 对于编码、杂项问题, 使用这个网站的在线工具来解决绰绰有余。

 [SSL在线工具](#) [SSL漏洞在线检测](#) [NiceTool](#) [快速导航](#)

### CTF编码

 <p><b>Base编码</b> Base64、Base32、Base16</p> <p><a href="#">ctf.ssleye.com</a> <a href="#">进入</a></p>	 <p><b>Hex编码</b> Hex, 十六进制编码转换</p> <p><a href="#">ctf.ssleye.com</a> <a href="#">进入</a></p>	 <p><b>URL编码</b> Url</p> <p><a href="#">ctf.ssleye.com</a> <a href="#">进入</a></p>	 <p><b>Quoted-printable编码</b> Quoted-printable</p> <p><a href="#">ctf.ssleye.com</a> <a href="#">进入</a></p>
 <p><b>Mimetypes</b> 获取http消息头应用类型</p> <p><a href="#">ctf.ssleye.com</a> <a href="#">进入</a></p>	 <p><b>HTML编码</b> Html</p> <p><a href="#">ctf.ssleye.com</a> <a href="#">进入</a></p>	 <p><b>Escape编码</b> Escape</p> <p><a href="#">ctf.ssleye.com</a> <a href="#">进入</a></p>	 <p><b>敲击码</b> Tap code</p> <p><a href="#">ctf.ssleye.com</a> <a href="#">进入</a></p>
 <p><b>莫尔斯电码</b> Morse code</p> <p><a href="#">ctf.ssleye.com</a> <a href="#">进入</a></p>	 <p><b>哈希计算</b> Hash</p> <p><a href="#">ctf.ssleye.com</a> <a href="#">进入</a></p>	 <p><b>AES加密</b> 支持5种模式, 5种填充</p> <p><a href="#">ctf.ssleye.com</a> <a href="#">进入</a></p>	 <p><b>DES加密</b> 支持5种模式, 5种填充</p> <p><a href="#">ctf.ssleye.com</a> <a href="#">进入</a></p>
 <p><b>Terple DES加密</b> 支持5种模式, 5种填充</p>	 <p><b>RC4加密</b> 多种字符集、Base64输出</p>	 <p><b>进制转换</b> ASCII、任意进制转换</p>	 <p><b>Base36编码</b> Base36, 支持整数</p>



CMD5: <https://www.cmd5.com/> MD5加密解密也是件极为复杂的事情, 借助一些在线工具可以使问题变得简单。

## CMD5

本站针对md5、sha1等全球通用公开的加密算法进行反向查询, 通过穷举字符组合的方式, 创建了明文密文对应查询数据库, 创建的记录约90万亿条450TB, 查询成功率95%以上, 很多复杂密文只有本站才可查询。已稳定运行十余年, 国内外享有盛誉。

密文:

类型:

自动



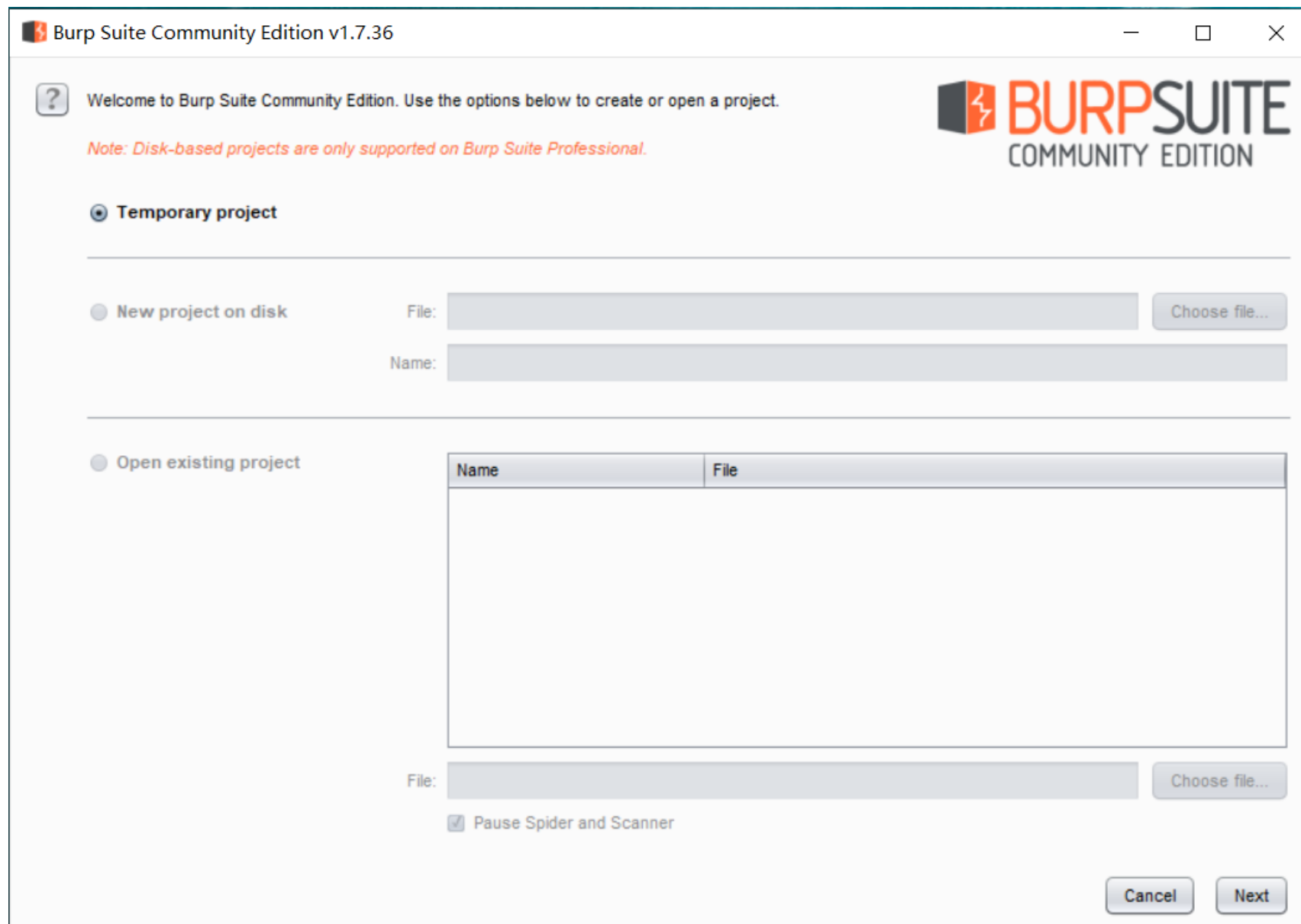
[帮助]

查询

加密

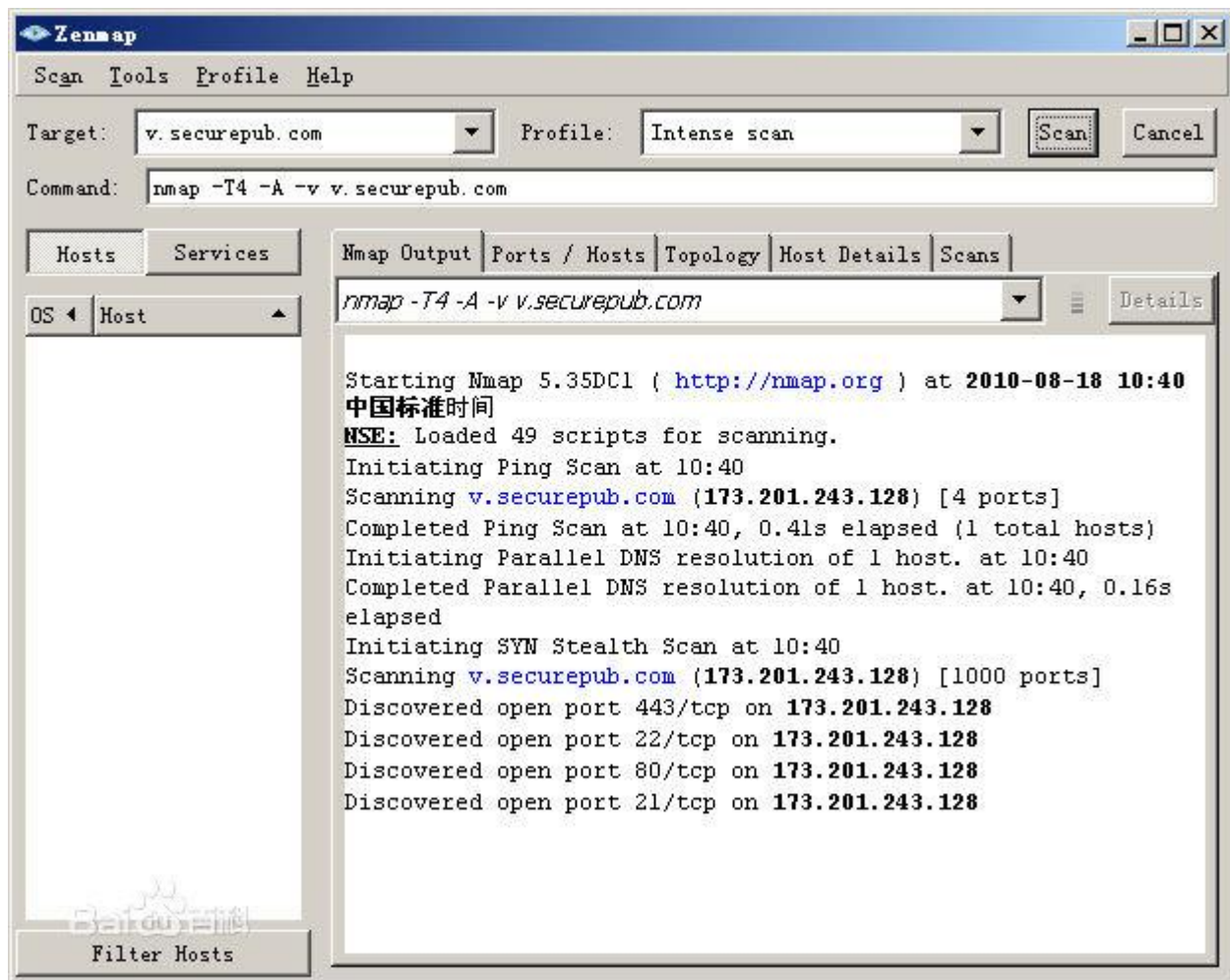
查询结果:

Burp Suite: 抓包攻击工具, 非常强大, 可以进行包分析、包伪造、包拦截等





Nmap：强大的端口扫描工具，可以探测主机是否在线、主机开了哪些端口、推断主机的操作系统等



CTF工具整合库: <http://www.ctftools.com/>

CTF国内综合练习题库:

BUGKU: <https://ctf.bugku.com/>

xctf题库网站: <https://adworld.xctf.org.cn/competition>

合天网安实验室: <http://www.hetianlab.com/CTFrace.html>

西普实验吧: <http://www.shiyanbar.com/ctf/>

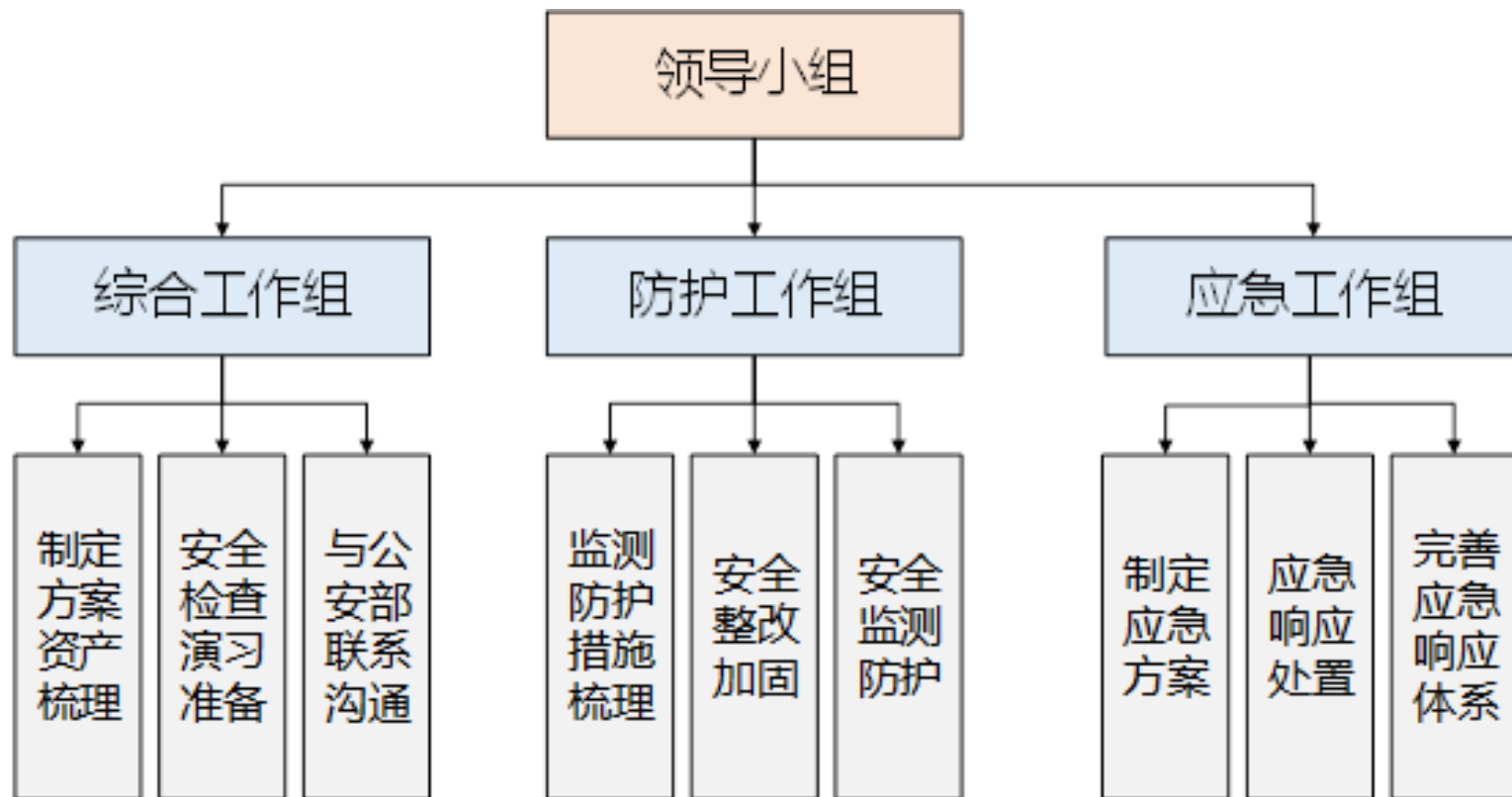
I春秋CTF: <https://www.ichunqiu.com/>

**CTF学习的目的: 发现漏洞, 修复漏洞, 防范漏洞, 做好网络安全防护工作, 而不是利用漏洞去进行违法犯罪的事情! 切记!**



作为此次攻防演习的参演单位，将通过网络安全攻防演习，进一步**检验网络安全防护能力、监测发现能力、应急处置能力**，发现可能在网络安全防护、监测和处置措施中**存在的短板**，积累有效应对网络安全攻击和威胁的经验，促进网络安全积极防御、协同处置的体系建设，促进网络安全队伍建设，**在实战中有效提升网络安全保障能力。**

为确保本次攻防演习任务的顺利完成，成立攻防演习领导小组（以下简称“领导小组”）和三个攻防演习工作组（以下简称“工作组”），组织架构如下图。





## 第一阶段：准备阶段

### 重要工作开展

#### 网络路径梳理

对目标系统相关的网络访问路径进行梳理，明确系统访问源（包括用户、设备或系统）的类型、位置和途径的网络节点，绘制准确的网络路径图。

#### 关联及未知资产梳理

梳理目标系统的关联及未知资产，形成目标系统的关联资产清单、未知资产清单。

#### 专项应急预案确认

针对本次攻防演习的目标系统进行专项应急预案的梳理，确定应急预案的流程、措施有效，针对应急预案的组织、技术、管理流程内容进行完善，确保能够有效支撑后续演习工作

#### 加强安全监测防御体系

梳理当前已有的安全监测和防御产品，对其实现的功能和防御范围进行确定，并根据已梳理的重要资产和网络路径，建立针对性的临时性（租用或借用）或者长久性（购买）的安全监测防御体系

## 第二阶段：安全自查和整改阶段

### 1、互联网暴露信息检查

互联网敏感信息暴漏将给客户网络安全带来极大的隐患。敏感信息主要有资产信息、技术方案、网络拓扑图、系统源代码、账号、口令等。可通过技术、管理和服务等方式开展互联网暴露敏感信息的发现及清理相关工作。

### 2、互联网资产发现

互联网资产发现服务通过数据挖掘和调研的方式确定资产范围，之后基于IP或域名进行互联网资产进行扫描发现，通过对发现的资产进行确认，将遗漏的资产纳入保护范围。



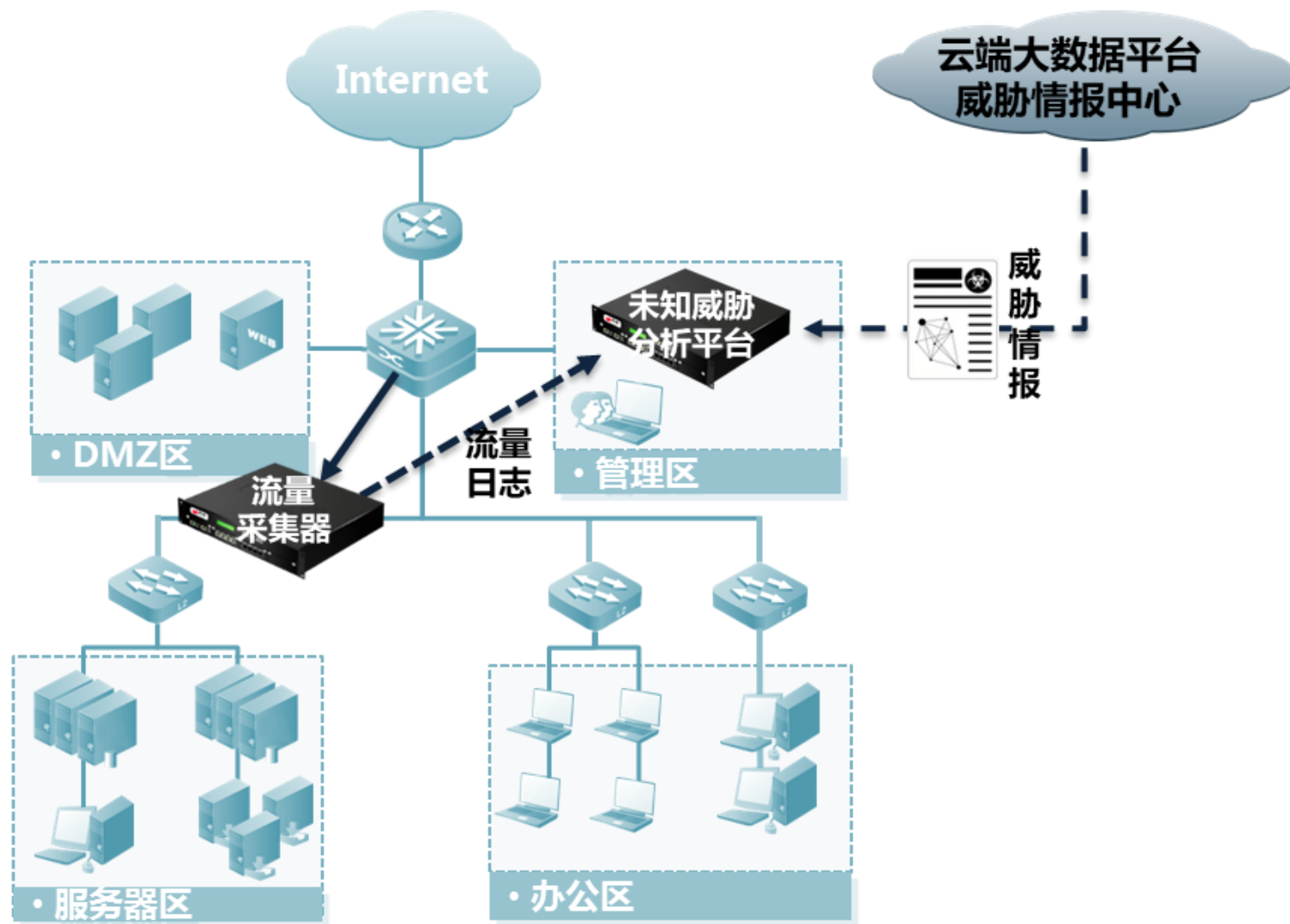
## 第二阶段：安全自查和整改阶段

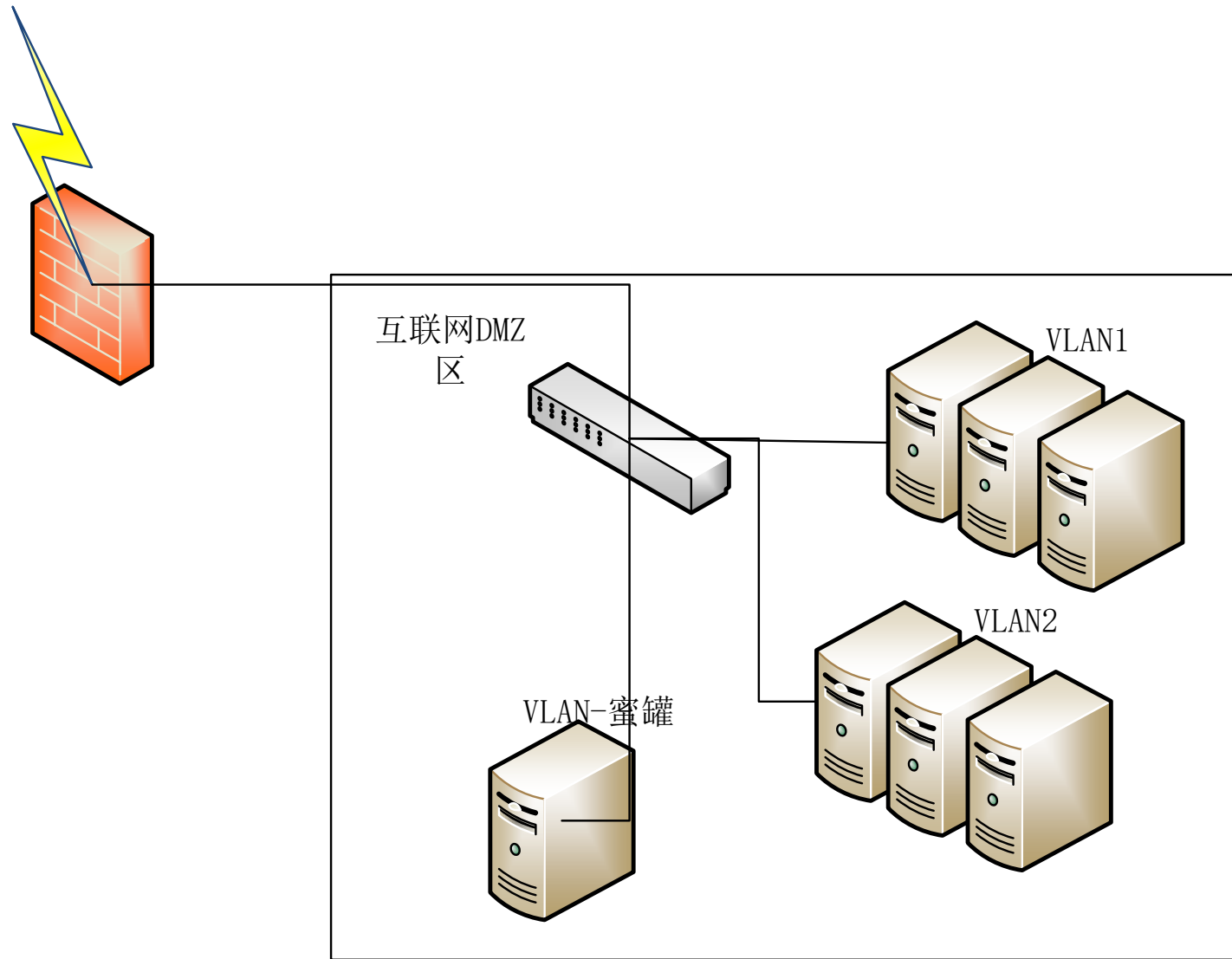
### 3、威胁感知系统部署

威胁感知系统可基于自有的多维度海量互联网数据，进行自动化挖掘与云端关联分析，提前洞悉各种安全威胁。同时结合部署本地的大数据平台，进行本地流量深度分析。

### 4、蜜罐系统部署

互联网资产发现服务通过数据挖掘和调研的方式确定企业资产范围，之后基于IP或域名进行互联网资产进行扫描发现，通过对发现的资产进行确认，将遗漏的资产纳入保护范围。







## 第二阶段：安全自查和整改阶段

### 5、主机加固实施

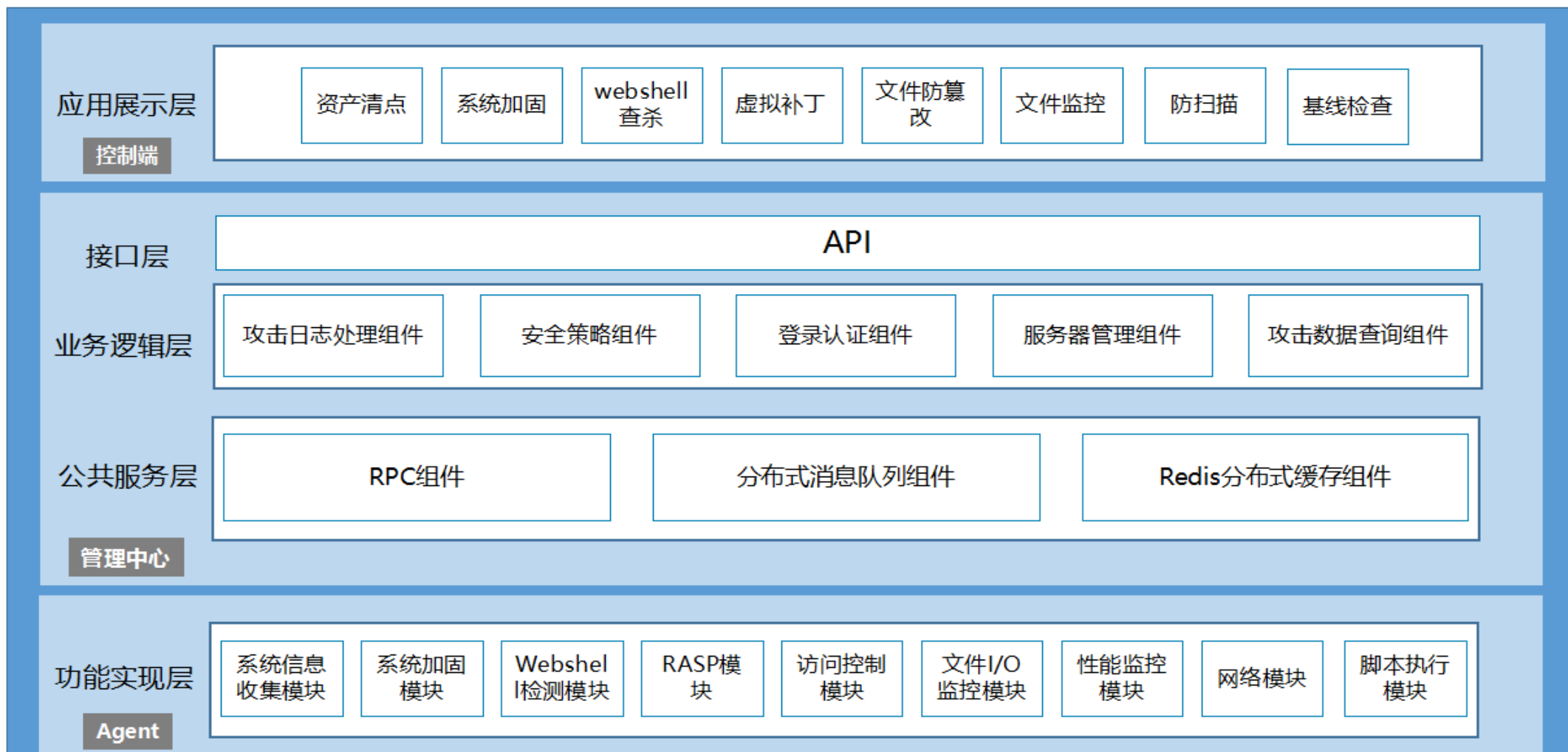
在内部业务服务器上安装部署监控服务端，实现网络及系统层攻击拦截，攻击方式捕获、漏洞发现，漏洞修复，补丁管理，系统加固，访问控制，应用隔离，威胁感知，系统资源监控，应用性能监控等功能。

**6、网络安全检查：网络架构评估、网络安全策略检查、网络安全基线检查、安全设备基线检查；**

**7、主机安全检查：操作系统、数据库、中间件安全基线，主机漏洞扫描；**

**8、应用安全检查：应用系统合规性检查、漏洞扫描、渗透测试**

**9、运维终端安全检查：运维终端安全策略、基线，漏洞扫描；**



## 第二阶段：安全自查和整改阶段

### 10、日志审计：网络、主机（操作系统、数据库、中间件）、应用、安全设备

针对本次目标系统中网络设备的日志记录进行检查，确认能够对访问和操作行为进行记录；明确日志开通级别和记录情况，并对未能进行日志记录的情况进行标记，明确改进措施。

### 11、备份有效性检查：备份策略检查、备份系统有效性检查；

12、安全意识培训：针对本次演习参与人员进行安全意识培训，明确演习工作中应注意的安全事项；

### 13、安全整改加固

基于以上安全自查发现的问题和隐患，及时进行安全加固、策略配置优化和改进，切实加强系统的自身防护能力和安全措施效能，减少安全隐患，降低可能被外部攻击利用的脆弱性和风险。



## 第三阶段：攻防预演习阶段

攻防预演习是为了在正式演习前，检验安全自查和整改阶段的工作效果以及防护小组否能顺利开展防守工作，而组织攻击小组对目标系统开展真实的攻击。

通过攻防预演习结果，及时发现目标系统还存在的安全风险，并对遗留（漏）风险进行分析和整改，确保目标系统在正式演习时，所有发现的安全问题均已得到有效的整改和处置。

## 第四阶段：正式护网阶段

在正式防护阶段，重点加强防护过程中的安全保障工作，各岗位人员各司其职，从攻击监测、攻击分析、攻击阻断、漏洞修复和追踪溯源等方面全面加强演习过程的安全防护效果。

### 1、安全事件实时监测

借助安全防护设备（全流量分析设备、Web防火墙、IDS、IPS、数据库审计等）开展攻击安全事件实时监测，对发现的攻击行为进行确认，详细记录攻击相关数据，为后续处置工作开展提供信息。

## 第四阶段：正式护网阶段

### 2、事件分析与处置

根据监测到安全事件，协同进行分析和确认。如有必要可通过主机日志、网络设备日志、入侵检测设备日志等信息对攻击行为进行分析，以找到攻击者的源IP地址、攻击服务器IP地址、邮件地址等信息，并对攻击方法、攻击方式、攻击路径和工具等进行分析研判。

### 3、威胁情报共享

对于经过分析已经确认的攻击事件，将攻击事件涉及的IP地址、攻击方式，攻击行为和相关威胁情报等整理后进行共享，可根据提供的IP地址等信息进行针对性的日志或流量查询和分析，判断本地是否发生此类攻击行为，共同打造攻击防护情报网。



## 第四阶段：正式护网阶段

### 4、防护总结与整改

全面总结本次攻防演习各阶段的工作情况，包括组织人员、攻击情况、防守情况、安全防护措施、监测手段、响应和协同处置等，形成总结报告并向有关单位汇报。

针对演习结果，对在演习过程中还存在的脆弱点，开展整改工作，进一步提高目标系统的安全防护能力。

应按“事件监测—初步处置—反查—处置—恢复上线”的基础思路开展防护工作，能力强者，在此基础上扩展。

## 事件监测、初步处置、攻击行为反查、应用及主机处置；

1) 事件监测：通过各类监测设备对安全事件进行监测(FW、waf、IPS等安全设备)，发现攻击行为或疑似攻击行为；

2) 初步处置：在发现疑似攻击行为时，不管是否已经攻击成功，直接协调FW或WAF维护人员，进行IP（端口）封堵处理，避免进一步攻击行为发生；(发现攻击IP及时群里发出，验证后就“先封禁”再上报给公安。如果公安确认该IP为攻击队IP，要求不允许封IP，安全拦截措施转为通过WAF 建立特殊IP组建立高防护策略并按照攻击情况进行人工添加策略如特定路径禁止访问策略。)

3) 攻击行为反查：在初步处置的同时，我方人员利用IPS对攻击行为进行反查，确认攻击事件及影响范围，以协调进一步处理线索，并协调人员将事件上报网安；

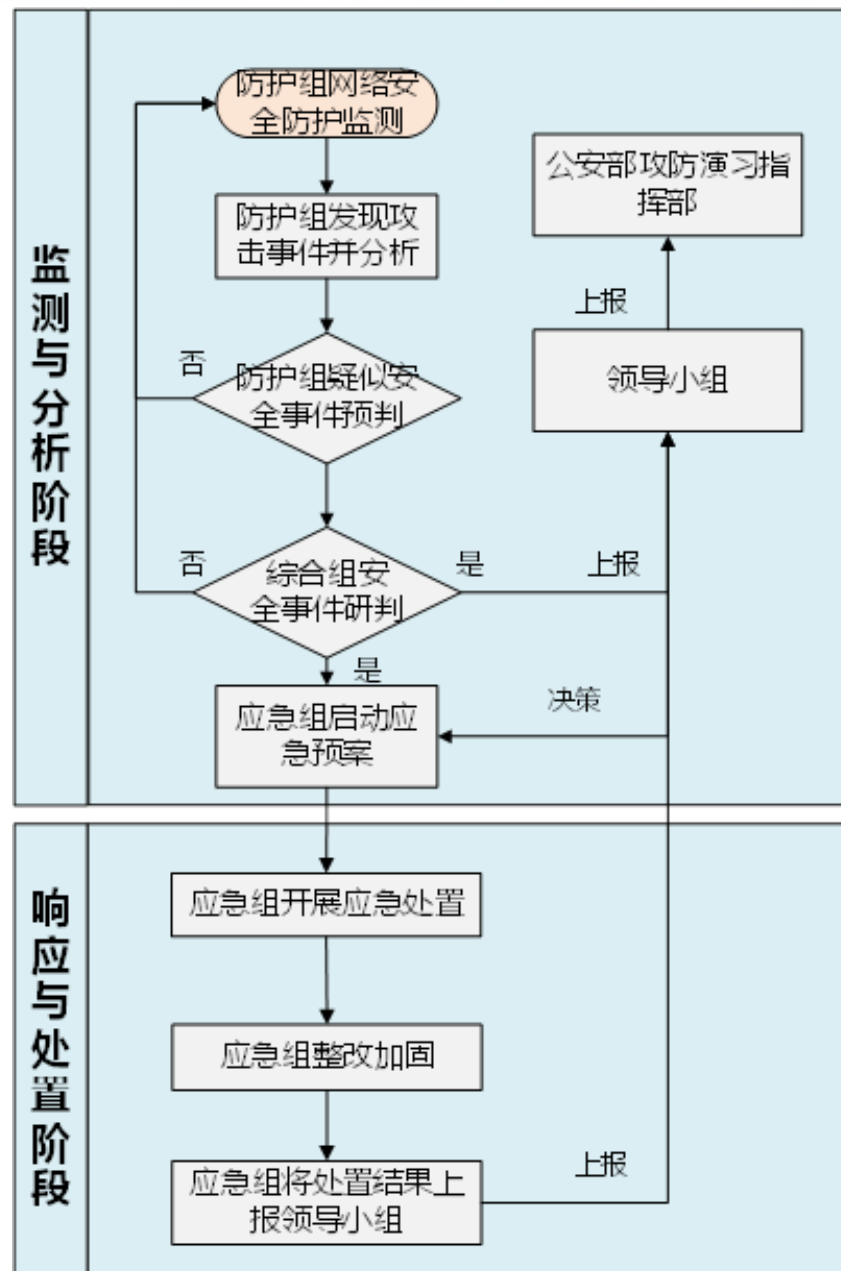
4) 应用及主机处置：如通过反查确认有主机或应用被攻击，第一时间应用和主机下线，通采用人员分析或失陷监测工具分析的方式确认系统被攻击的情况，协调相关责任人进行进一步处置；

**领导小组：**负责指挥协调开展应急响应工作，及时向攻防演习指挥部上报应急处置情况。

**综合工作组：**负责与演习指挥部联系沟通，综合分析研判安全事件，报领导小组启动相应应急预案。

**防护工作组：**利用监测技术手段对网络攻击进行监测、分析、预警和处置，将初步判定为安全事件的分析结果反馈综合工作组。

**应急工作组：**接到安全事件应急处置通知，立即启动应急预案开展应急处置工作，将处置完成后将处置结果上报领导小组。





## 信息安全的三要素CIA

**C**

**保密性 (Confidentiality)** —— 确保信息在存储、使用、传输过程中不会泄漏给非授权用户或实体。

**I**

**完整性 (Integrity)** —— 确保信息在存储、使用、传输过程中不会被非授权篡改，防止授权用户或实体不恰当地修改信息，保持信息内部和外部的 consistency。

**A**

**可用性 (Availability)** —— 确保授权用户或实体对信息及资源的正常使用不会被异常拒绝，允许其可靠而及时地访问信息及资源。

CIA三元组是信息安全的目标，也是基本原则，与之相反的是DAD三元组：

泄  
露

**D**

isclosure

篡  
改

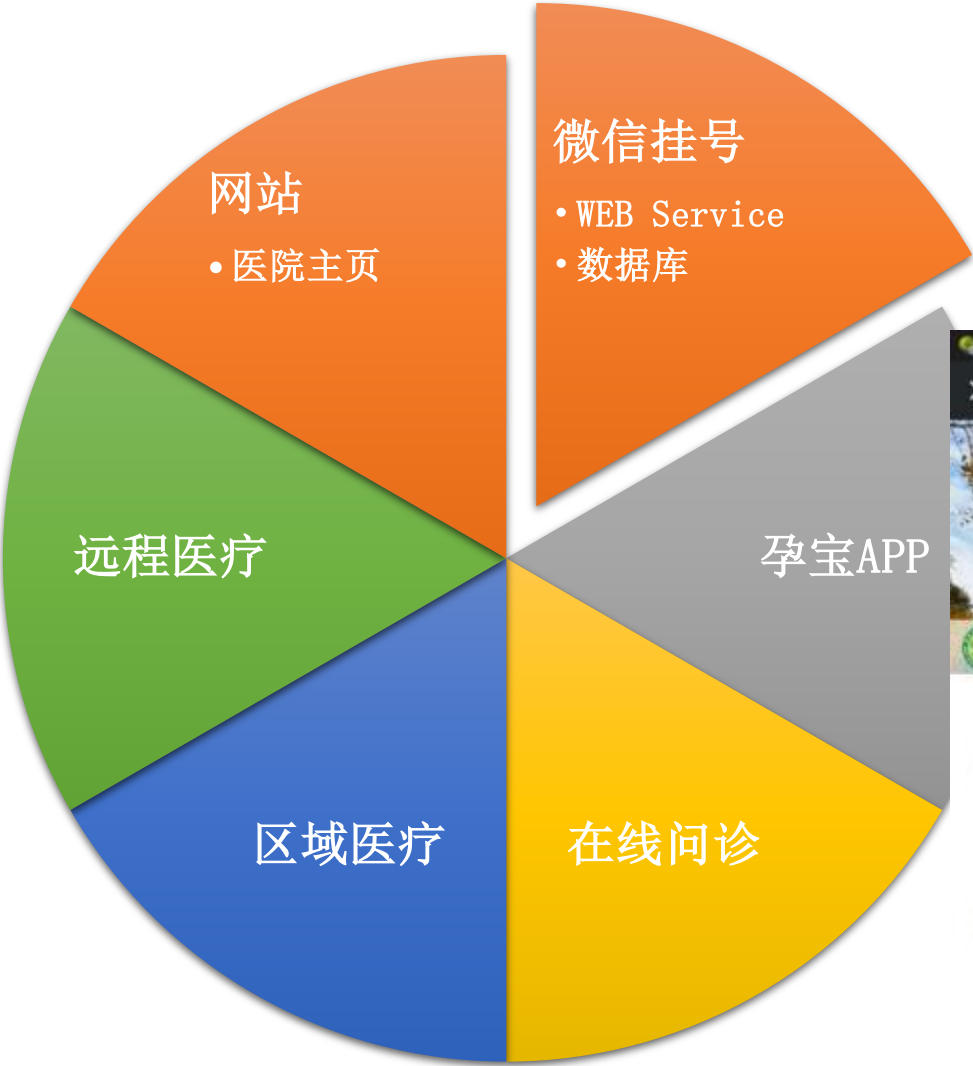
**A**

literation

破  
坏

**D**

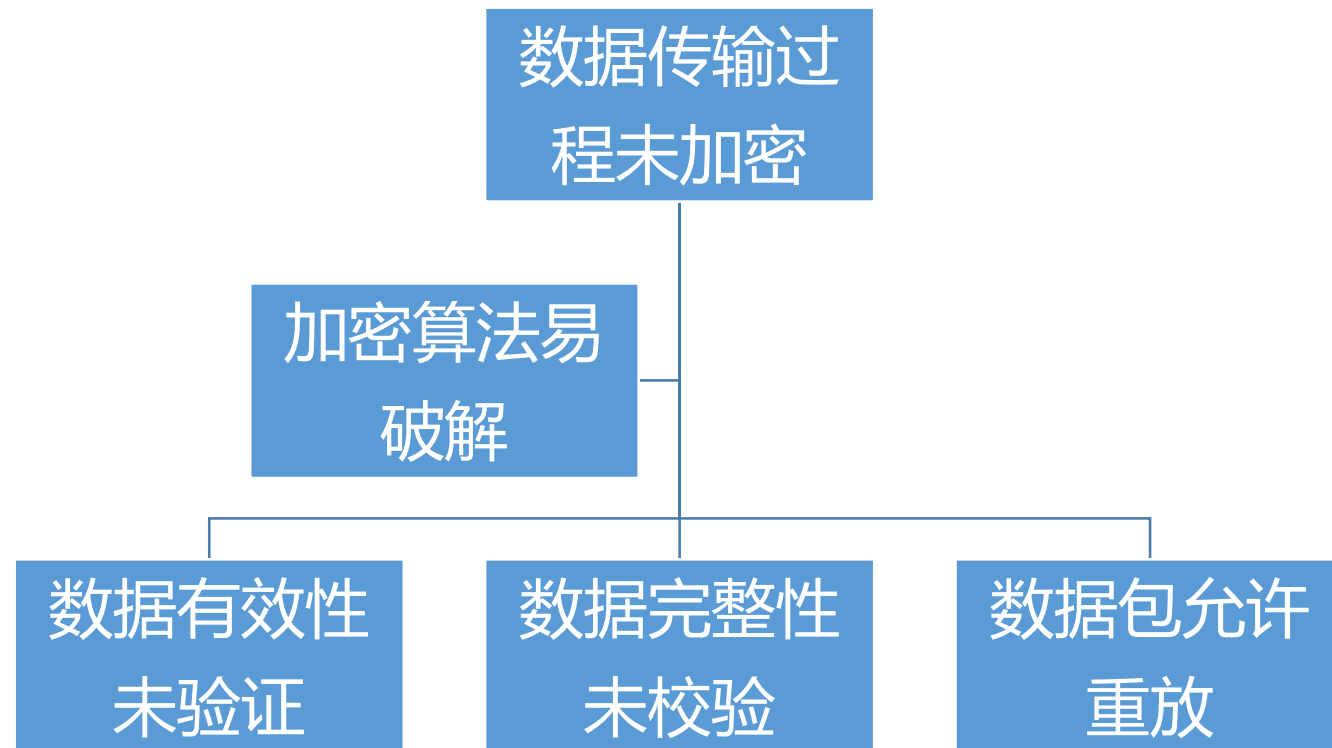
estruction





- 操作系统漏洞  
Win2000/2003/2008, Linux
- Web应用系统漏洞  
ASP/PHP/JSP/CGI
- 服务器应用软件漏洞  
Web中间件、数据库软件、运维工具





## 程序安全

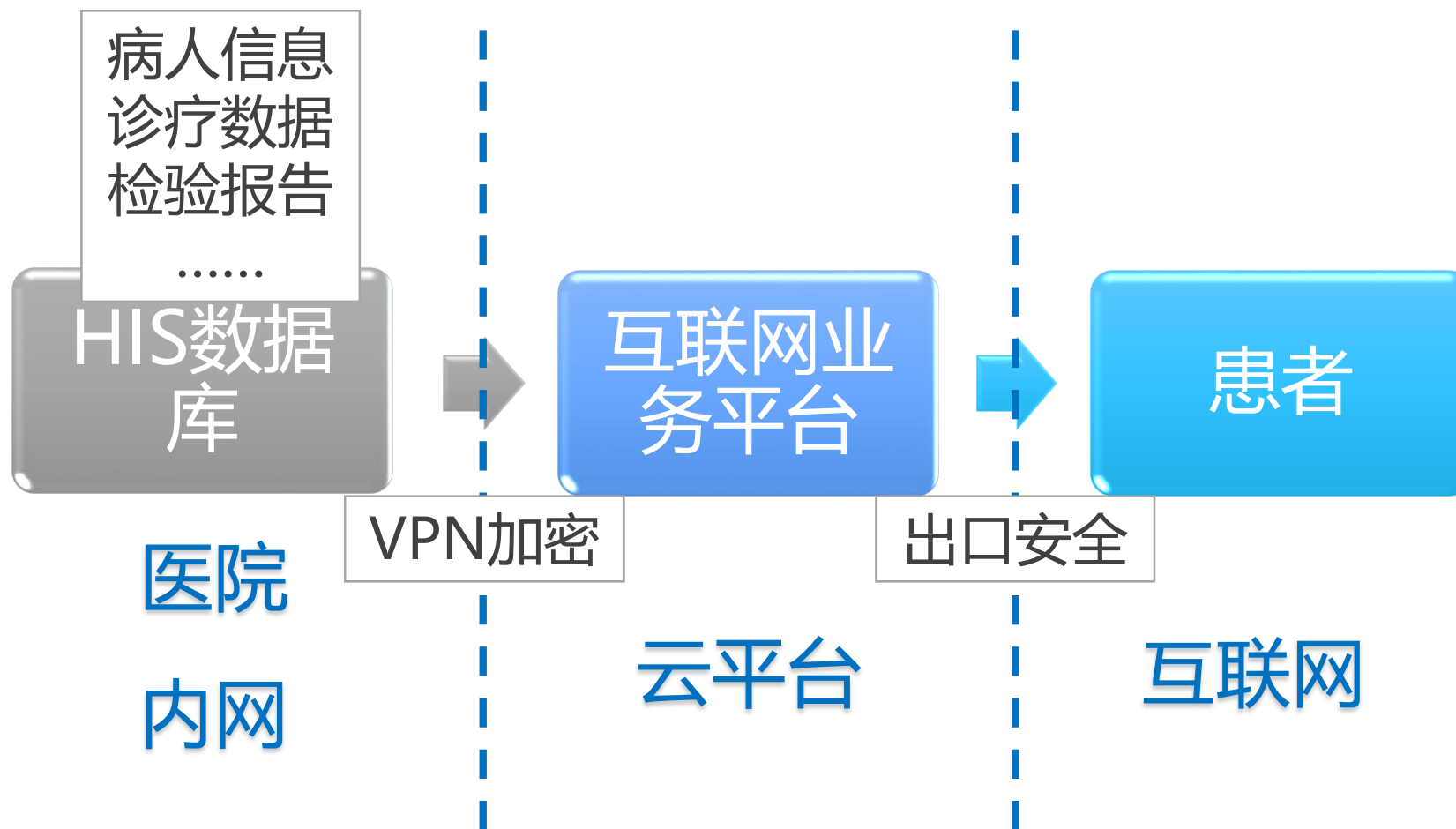
反编译导致源代码、接口信息和敏感数据暴露。

程序被重新打包(盗版), 嵌入广告、恶意代码或进行钓鱼攻击等。

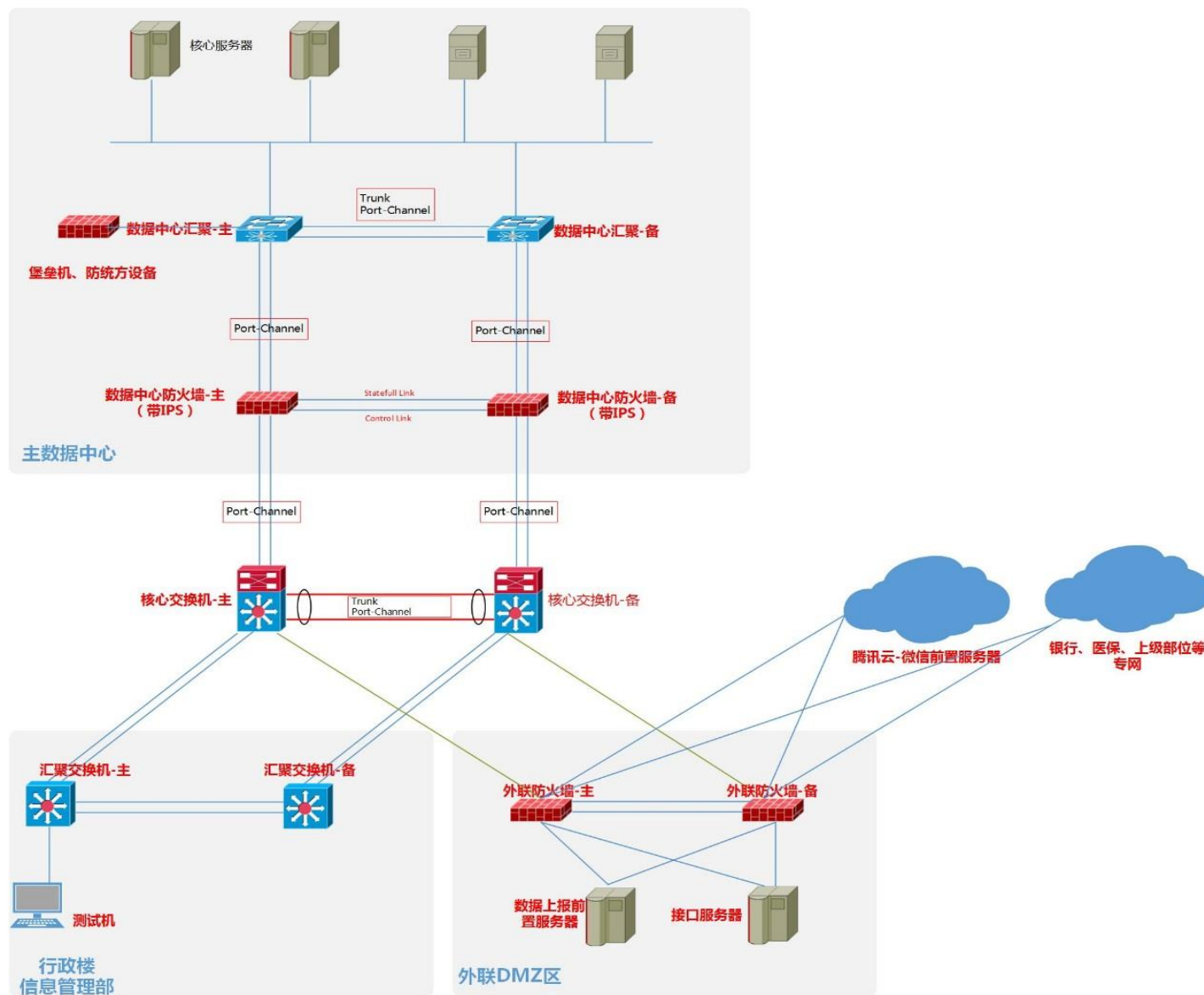
## 数据安全

配置文件被非法读取或篡改。

用户数据文件被非法读取或篡改。







- 边界加强防范
  - 尽可能使用专线或VPN接入
  - 采用防火墙、网闸等
  - 自行研发对接系统（接口）
  - 出口部署抗DDOS、WAF等安全设备
- 严格的端口映射审核
  - 关闭非必要的映射端口
  - 定期进行渗透测试、漏洞扫描

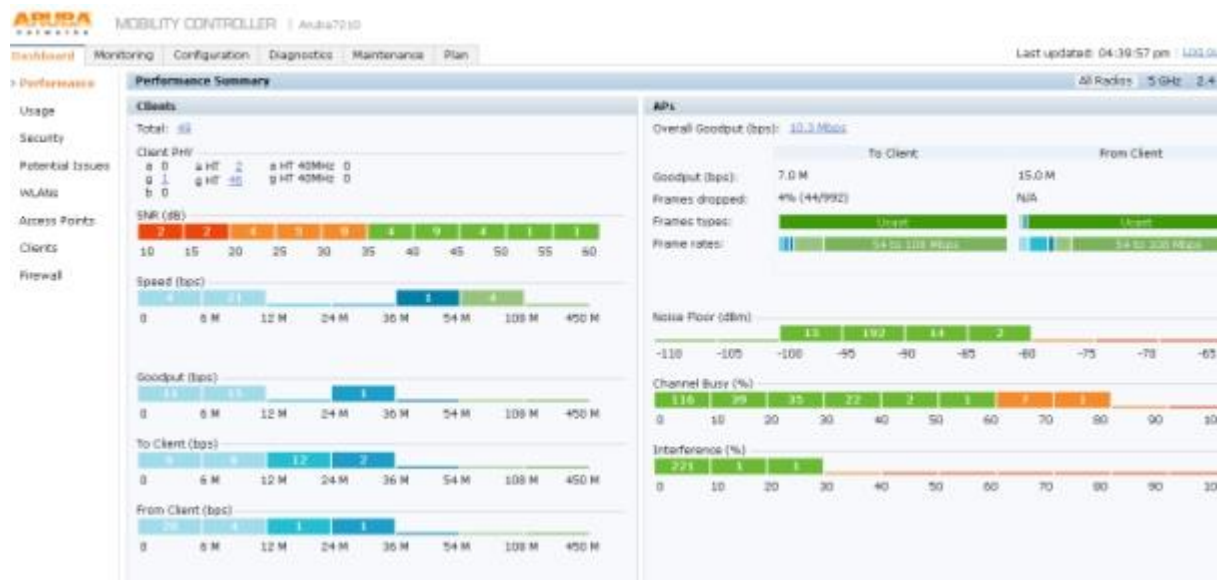


- 机房远程监控
  - 红外摄像
  - 智能传感
  - 自动报警
- 定期巡查
  - 指纹进入
  - 巡查与奖惩制度





- 控制无线接入
  - MAC地址绑定
  - 防火墙策略控制访问IP
- 控制系统访问权限
  - 通过堡垒机进行服务器操作管控，行为记录
  - 核心数据库密码由双人管理
- 数据审计（防统方）
  - 审计数据库操作，敏感操作溯源



- 用户授权的最小化
  - 足够你用，但仅够你用
  - 做好审核与备案
- 特定用户指定IP
  - Webservice用户限定IP来源
  - 开发人员指定IP
  - 特定系统指定IP与用户

The screenshot displays a web application interface with two main sections: 'USER LOGIN DETAILS' and 'REGISTER AS A CARE PROVIDER'. The 'USER LOGIN DETAILS' section includes fields for User ID, Username, Password, Confirm Password, Security Code, and Activation Date. The 'REGISTER AS A CARE PROVIDER' section includes fields for Care Provider Name, Care Provider ID, Care Provider Type, Care Provider Group, and Activation/Deactivation Dates. Below these sections is a 'CARE PROVIDER DETAILS' section with a table listing various care providers and their associated hospitals. The table has columns for 'Care Provider Name', 'Security Code', and 'Hospital'. The table lists several care providers, including '产科AS-产房室', '产科AS-产房室', '产科AS-产房室', '产科AS-产房室', '产科AS-产房室', and '产科AS-产房室'. The interface is in Chinese and appears to be a web-based system for managing healthcare providers.

注册科室	安全码	医院
产科AS-产房室	产房管理	
产科AS-产房室	便民门诊医生	
产科AS-产房室	产科门诊医生	
产科AS-产房室	产科门诊医生(1)	
产科AS-产房室	产科门诊医生(2)	
产科AS-产房室	产科住院医生(副高以上)	

- 终端准入与管控

- 禁止修改IP
- 禁用USB，光驱，带存储的输出设备
- 禁止双网卡、非法进程
- 安全准入、授权、备案

- 终端杀毒、补丁

- 病毒库定期更新
- 定期扫描漏洞，安装补丁



完备的终端准入流程

1. 进一步加固基础安全，建设符合高性能，高可用的弹性架构，管理资产风险；
2. 围绕数据，建设全方位全视角安全数据监控感知体系。
3. 结合自身能力加固业务与应用安全，明确业务红线，加强业务管控。
4. 通过安全管理为技术体系赋能，管理为本，细化流程，确保绩效
5. 根据实际情况将安全体系融入医院信息化大数据整体体系。

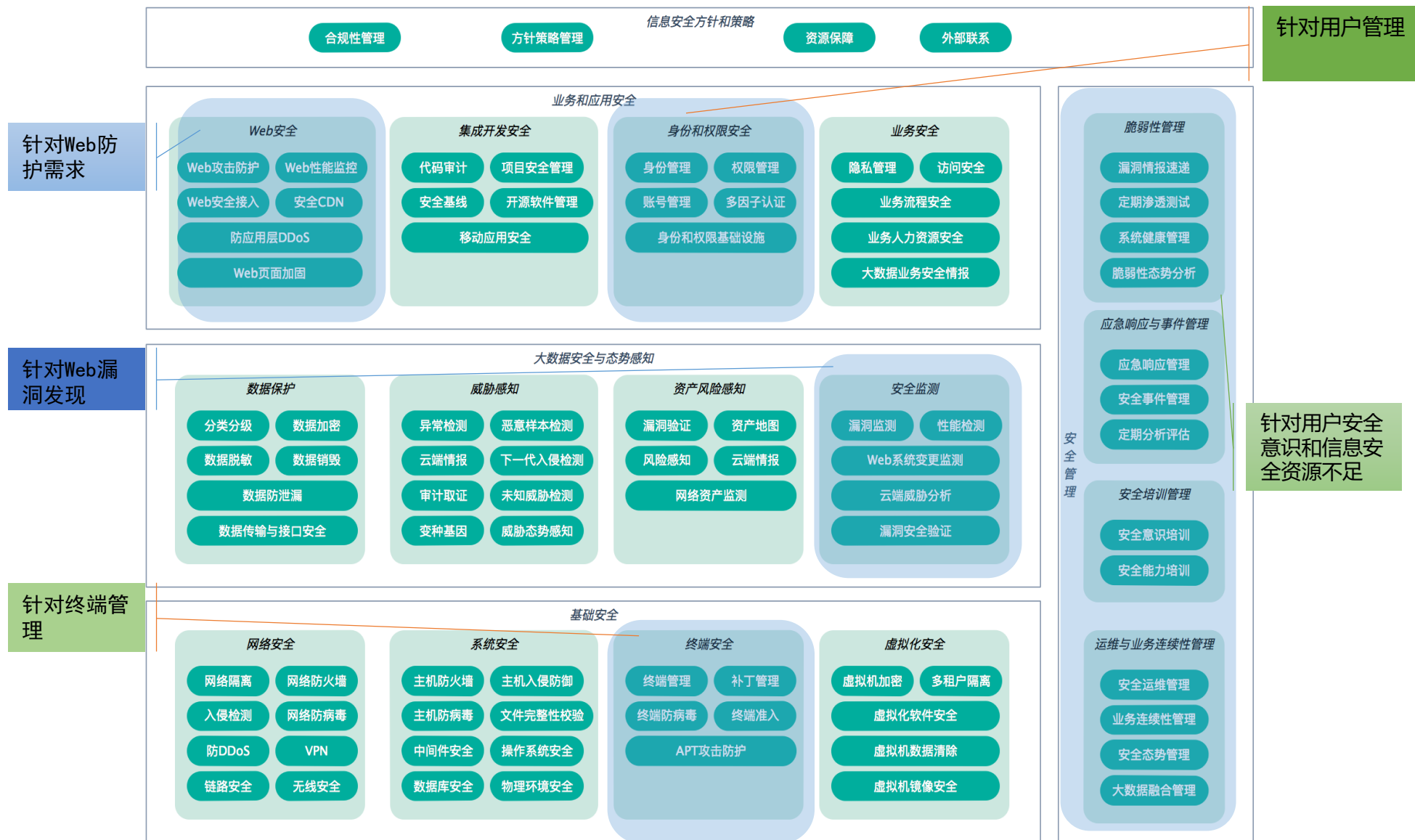




# 分阶段分重点进行建设

2019 北京网络安全大会  
2019 BEIJING CYBER SECURITY CONFERENCE

根据自身的薄弱点进行分阶段建设  
一定要有侧重





**总结!**



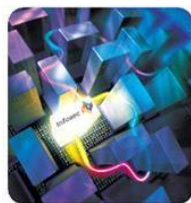
**信息安全就是防泄露**



**信息安全就是网络安全**



**信息安全就是防黑客**



**信息安全就是技术问题**



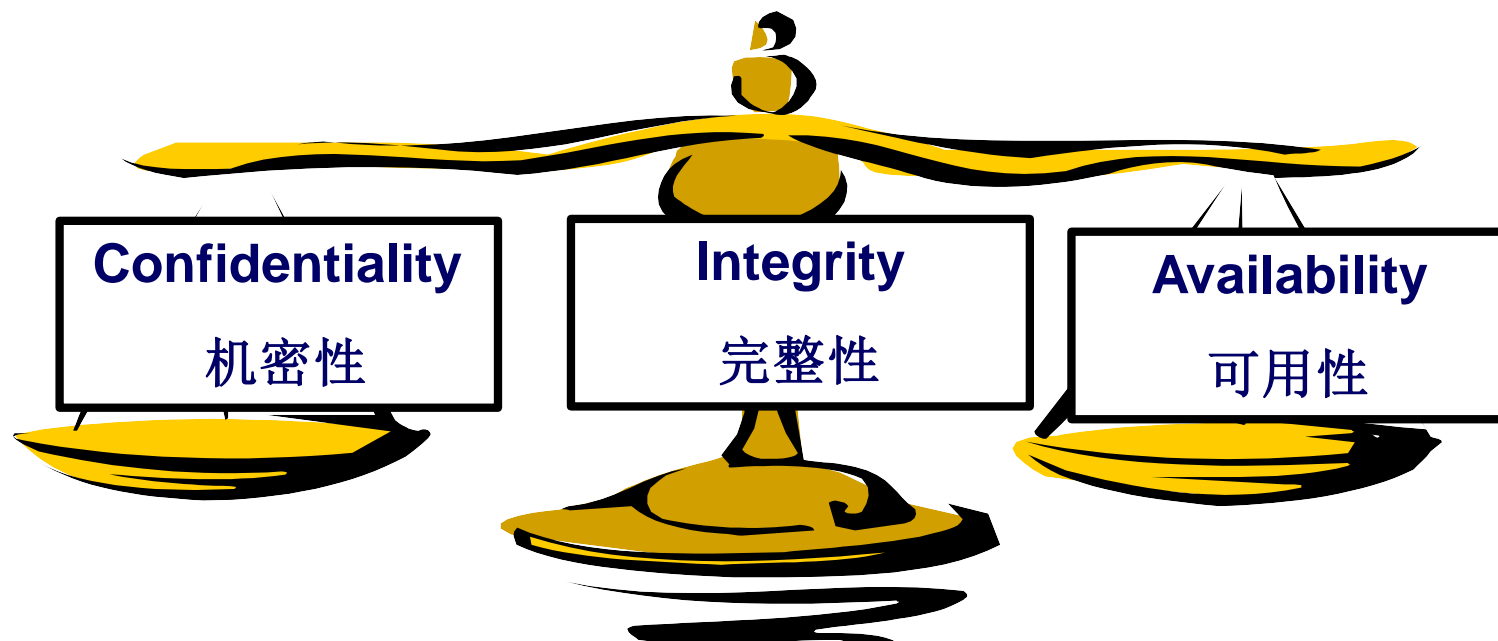
**信息安全就是一场运动**



**信息安全就是麻烦**

## ❖ 信息安全就是网络安全

- 只要防止黑客入侵和病毒就可以了
- 信息安全只要保证公司的机密信息不被泄露，即保证信息的保密性





## ❖ 解决安全问题搞运动

- 问题严重了，搞个运动
- 运动过了，可以歇歇


## ❖ 信息安全与业务无关

- 信息安全事务上的投入是没有价值的，只会给工作带来麻烦
- 信息安全是业务之外多余的工作，日常的业务流程无须考虑信息安全
- 系统或者网络安全失效，不会造成业务上的财务损失

- ❖ **七分管理、三分技术，技术是基础，管理才是关键**
- ❖ **网络安全是信息安全的一部分**
- ❖ **信息安全是一项长期的工作，贯穿在日常的工作中**
- ❖ **信息安全的任务就是保障业务的持续性，信息安全  
是业务持续的必要条件**

- 1. 信息安全是信息化建设的基础工程，做的好不显，做不好遭殃**
- 2. 安全不看你做了什么，关键看没有做什么**
- 3. 安全工作要平衡，投入产出要平衡，方便麻烦要平衡**
- 4. 安全是1，其他都是0**
- 5. 人人都是安全员**
- 6. 未来的几年如果安全不做重点，其他重点都将成为痛点！**



The background is a solid blue color with a subtle, abstract pattern of thin, light blue lines that form a grid-like structure, possibly representing a network or data flow. The pattern is more dense in some areas and more sparse in others, creating a sense of depth and movement.

# THANKS

**2019 北京网络安全大会**  
2019 BEIJING CYBER SECURITY CONFERENCE