



自顶向下
学习数据安全治理实践

目录

1、数据安全概念与安全现状

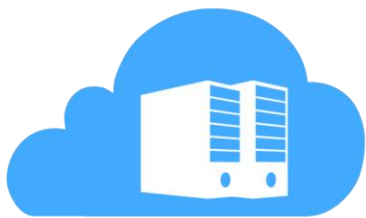
2、数据安全框架理念与安全需求

3、数据安全治理实践路径

4、数据安全常态化建设实践

5、Q&A

数据安全领域基础定义



数据

- 任何**数字形式信息**
- 任何组织都需要存储知识和数据



数据生命周期

- 数据的生命周期：**数据从产生到最终销毁的全部阶段**



数据安全

- 针对数据的生命周期提供安全保护

数据安全形势异常严峻

- 中国, 2018: 华住 (HTHT) 旗下酒店泄露了 5 亿条用户敏感数据。
- 中国, 2019: 前程无忧泄露195万个人求职信息。
- 中国, 2020: 微博 5.38 亿条数据在暗网被出售。
- 中国, 2020: 建设银行员工私下贩卖 5 万多条客户数据。
- 中国, 2021: (年度十大个人信息泄露事件之一) 淘宝进 12 亿条用户数据泄露。
- 印度, 2018: 国家身份认证系统泄露了 11 亿印度公民数据。
- 美国, 2018: 万豪旗下喜达屋酒店泄露 5 亿数据资讯。
- 美国, 2018: Facebook 公司泄露 8700 万用户数据, 被重罚 50 亿美元。
- 以色列, 2021: 网安公司 Cognyte 因错误操作泄露 50 亿个人数据。
- ...

现实痛点

机密性

- 机密数据仅仅正确的用户才可以访问
- 数据尽量不受内部或者外部的系统漏洞的影响
- 能报告谁访问了哪些数据，干了什么 (WHO / WHAT / WHEN)
- 绝密数据和法律敏感数据需特别关注

完整性

- 确保外部来源的数据格式正确
- 确保输入数据的精确性和可验证
- 数据传输符合工作流的规则
- 能报告数据的修改和授权方，以符合组织规则和隐私法律法规

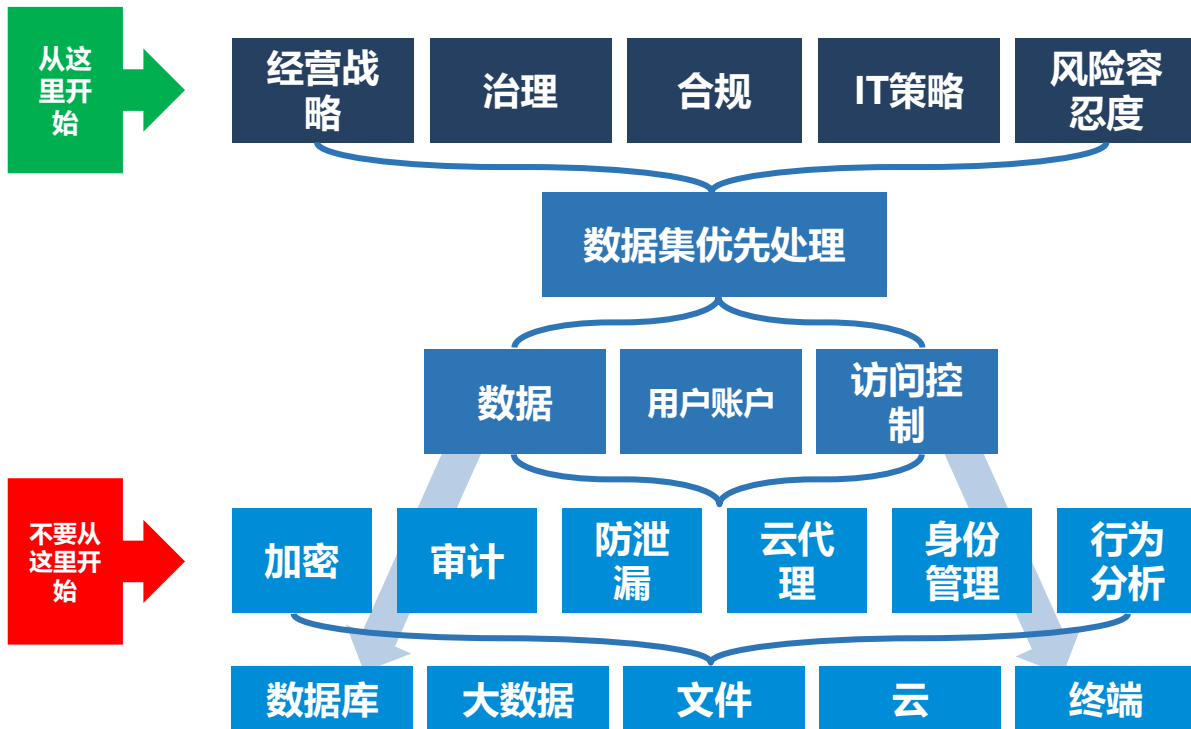
可用性

- 数据在需要时必须可用
- 数据只能给合适的用户
- 必须能跟踪谁访问了和访问过哪些数据



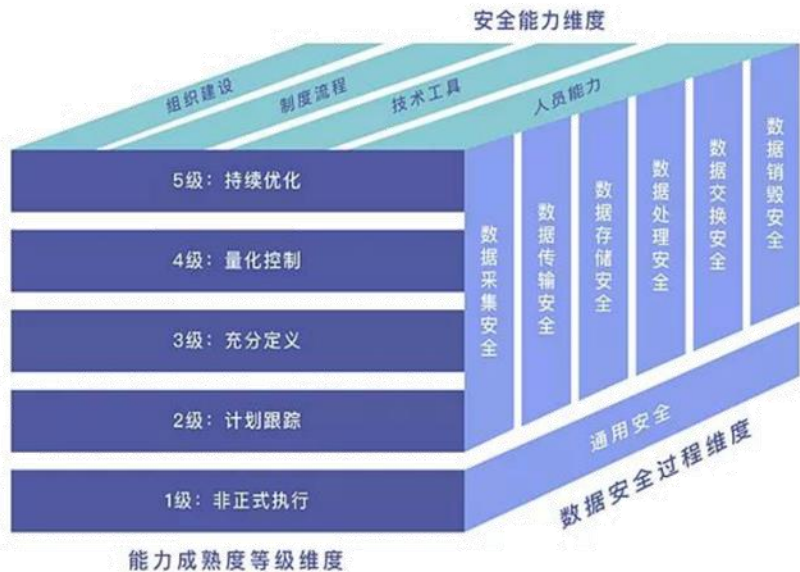
数据安全框架理念：Gartner

Gartner对数据安全治理提出了一个从上而下的整体框架，包括从治理前提、具体目标到技术支撑的完整体系。



数据安全框架理念：DSMM

- 《信息安全技术数据安全能力成熟度模型》即DSMM将数据按照其生命周期分阶段采用不同的能力评估等级
- 生命周期分为数据采集安全、数据传输安全、数据存储安全、数据处理安全、数据交换安全、数据销毁安全这6个阶段，
- DSMM从组织建设、制度流程、技术工具、人员能力这4个安全能力维度的建设进行综合考量，将数据安全成熟度划分成5个等级，依次为非正式执行级、计划跟踪级、充分定义级、量化控制级和持续优化级
- 形成一个三维立体模型，全方位地对数据安全进行能力建设。



数据安全需求

目前各组织针对数据安全治理的需求可总结为如下几个方面。

➤ 数据安全定岗定责与管理架构

✓ 组织需要在一定程度上更新自身的人员管理架构以满足数据安全建设需要。

➤ 数据安全制度流程

✓ 制度流程是对人员及其岗位职责的量化约束，针对数据安全，组织往往缺乏相关可落实的制度和政策，从而引发数据安全治理过程中的稽核风险。

➤ 数据资产梳理、数据安全风险评估以及数据授权与访问管理

✓ 三者递进关系，一荣俱荣一损俱损



数据安全治理实践路径：数据策略 (Data Policy)

- 数据策略为企业或项目制定数据管理的长期战略目标；
- 数据策略是一套高阶原则，为数据管理制定指导框架；
- 数据策略用来解决一些战略问题，比如数据访问，相关法律问题，数据管理问题，数据管理责任，数据获取及其他问题；
- 安全人员在制定数据策略时需要考虑的问题包括：



数据安全治理实践路径：现状调研

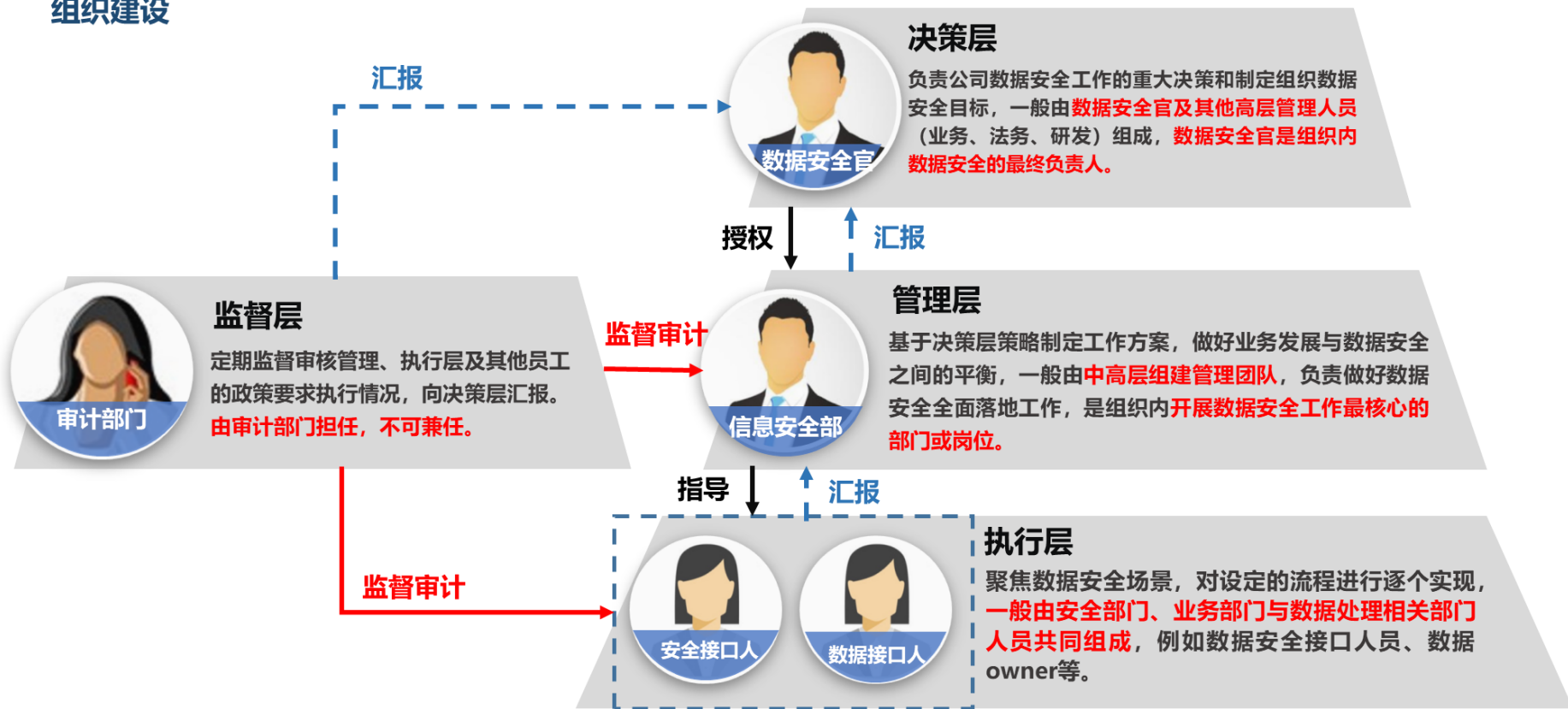
调研内容包括组织数据资产现状、管理制度流程、业务场景以及现有技术工具。

- 组织数据资产现状调研需明确组织明确业务系统状况、网络拓扑分布、并通过工具探查验证反馈信息准确性和数据资产登记完整性。
- 管理流程调研需确认组织现有人员架构、已颁布管理制度、各岗位人员系统账号权限、数据安全意识以及安全演练周期等，并通过系统演示查看各岗位人员账号权限组成。
- 业务场景调研则是研判目前组织的商业场景，确认当前管理流程和业务系统是否满足相关商业预期，并为数据安全治理差距分析提供必要因素。
- 现有技术工具调研是检测组织目前为实现数据安全已实施的工具类型，检查现有工具技术能力和需改善项目。通过系统演示实际操作相关工具功能，验证工具实际实施能力。



数据安全治理实践路径：组织架构设计

组织建设



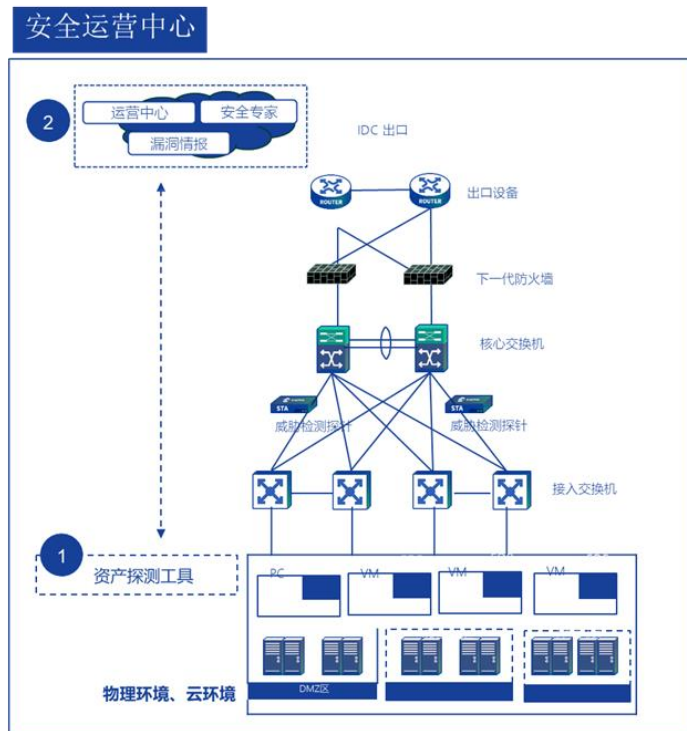
数据安全治理实践路径：数据所有者流程文档化

- 数据所有者应当建立和文档化相关策略，包括：
 - 数据所有权、知识产权、版权；
 - 业务相关的法定义务和非法定义务，确保数据合规；
 - 数据安全、防泄密控制，数据发布、价格、传播相关的策略；
 - 在数据发布前，与用户或客户签署备忘录和授权协议，明确使用的条件。
- 数据管理者的责任主要包括：
 - 遵照数据策略和数据所有权指南；
 - 确保适当用户的访问权，以及维护适当级别的数据安全；

数据安全治理实践路径：数据资产梳理

数据资产梳理包含数据资产发现、数据分类分级以及数据权限管理。

资产发现



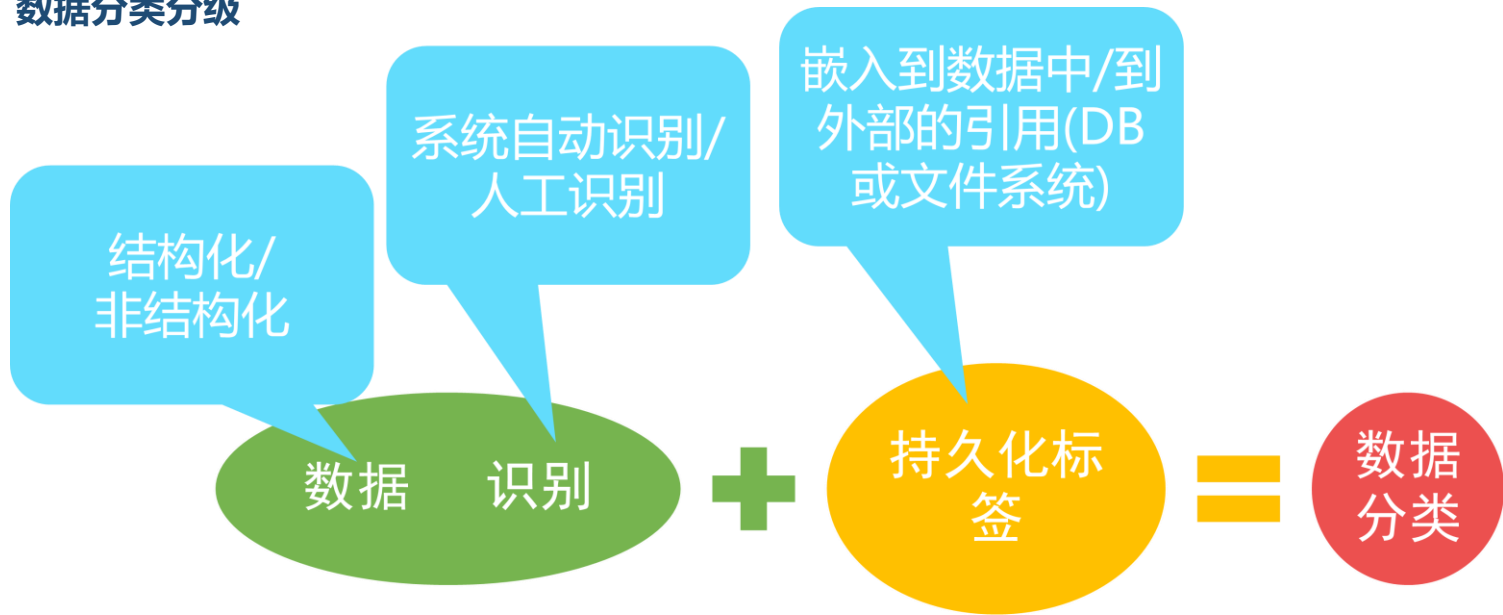
资产梳理五步法

- Step1 工具部署：本地工具+云端工具
- ↓
- Step2 云端梳理：梳理台账、主动探测
- ↓
- Step3 本地梳理：本地主动扫描探测
- ↓
- Step4 比对确认：结合出口设备和列表进行比对
- ↓
- Step5 台账输出：完善资产台账

数据安全治理实践路径：数据资产梳理

数据资产梳理包含数据资产发现、数据分类分级以及数据权限管理。

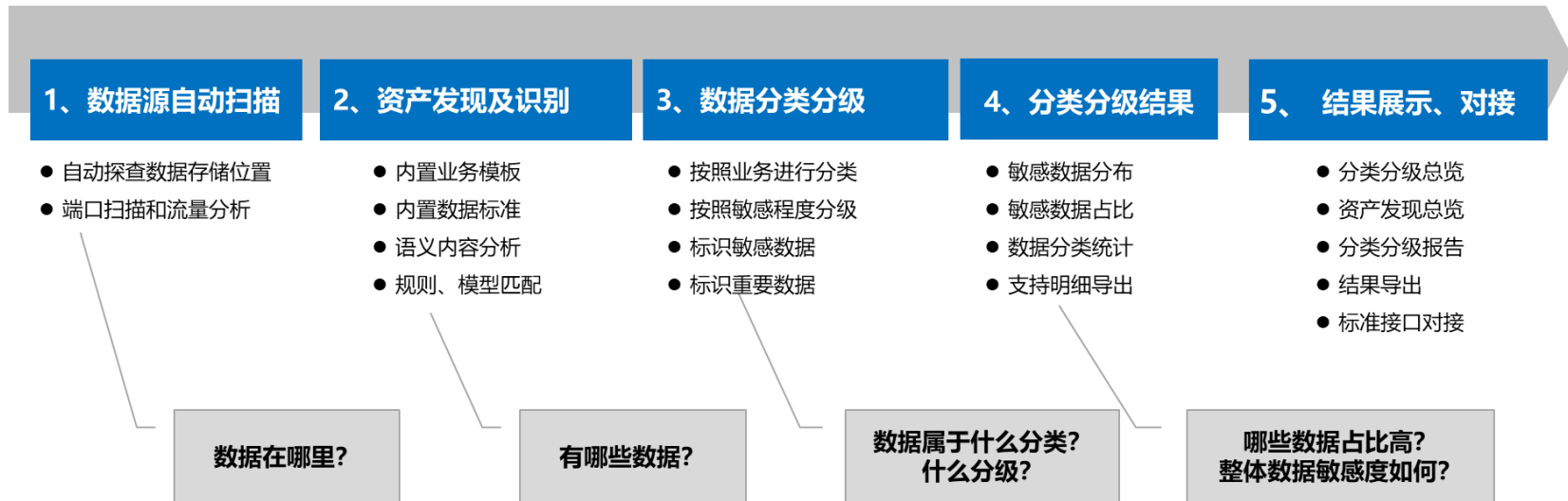
数据分类分级



数据安全治理实践路径：数据资产梳理

数据资产梳理包含数据资产发现、数据分类分级以及数据权限管理。

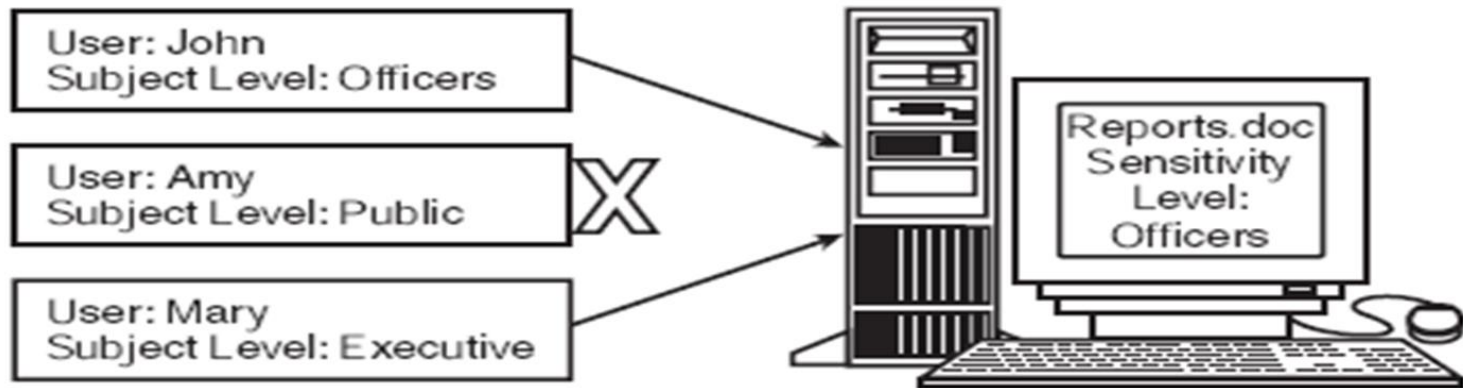
数据分类分级



数据安全治理实践路径：数据资产梳理

数据资产梳理包含数据资产发现、数据分类分级以及数据权限管理。

数据权限管理



Security Policy:

- Public: has access only to public level
- Officers: has access only to officers and public level
- Executive: has access only to public, officers, and executive

数据安全治理实践路径：数据安全风险评估

数据安全风险评估包含数据基础风险评估、数据安全合规风险评估以及数据全生命周期风险评估。

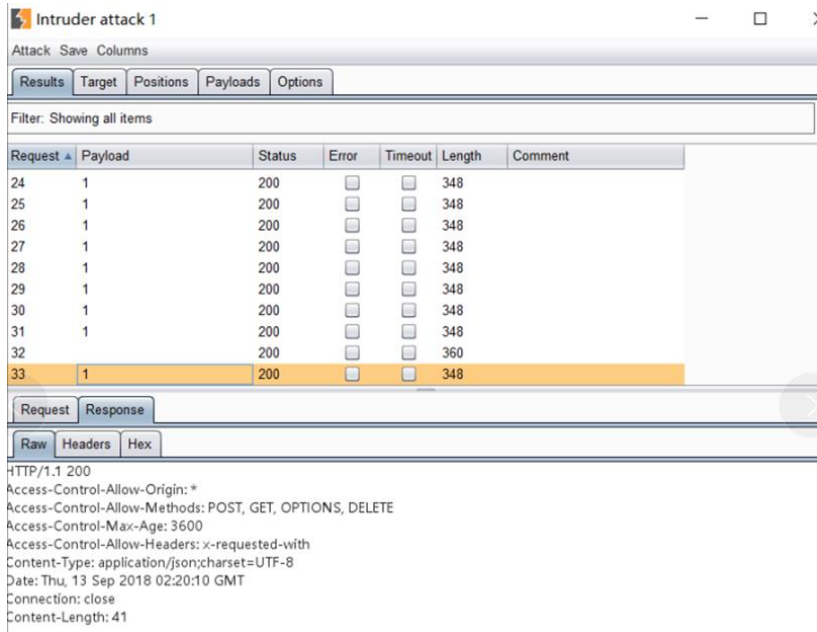
数据基础风险评估



数据安全治理实践路径：数据安全风险评估

➤ web应用弱口令

web应用弱口令指web应用前台或后台登录处存在可猜解的、不符合密码策略的口令，应用前台或后台一般存在大量的敏感数据或存在漏洞的功能点，web应用弱口令可用burpsuite中的intruder模块等方式进行自动化发现。



The screenshot shows the 'Intruder attack 1' window in Burp Suite. It displays a table of attack results with columns for Request, Payload, Status, Error, Timeout, Length, and Comment. The table shows 13 rows of data, with the 13th row (Request 33) highlighted in orange. Below the table, there are tabs for 'Request' and 'Response', and sub-tabs for 'Raw', 'Headers', and 'Hex'. The 'Response' tab is selected, showing the following text:

```
HTTP/1.1 200
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, DELETE
Access-Control-Max-Age: 3600
Access-Control-Allow-Headers: x-requested-with
Content-Type: application/json;charset=UTF-8
Date: Thu, 13 Sep 2018 02:20:10 GMT
Connection: close
Content-Length: 41
```

数据安全治理实践路径：数据安全风险评估

➤ 数据库弱口令/未授权访问

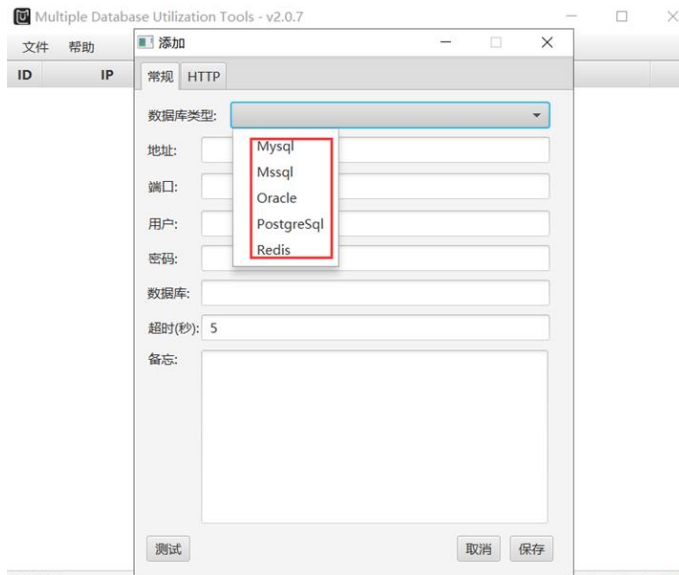
数据库管理员为了管理数据库方便，可能会将数据库口令设置为root/root、root/123456、sa/123456、sys/123456、null之类不符合密码安全策略(8位以上并存在3中不同类型的字符)的口令，这些口令被称为弱口令。如果某数据库存在弱口令，攻击者通过弱口令字典能够很容易的猜解出数据库口令。下图为一款弱口令爆破工具，该工具能够发现mysql、sqlserver、oracle、mongodb、postgresql、redis数据库中存在的弱口令或未授权访问漏洞。

The screenshot shows a web-based interface for a weak password cracking tool. On the left, there is a list of services with checkboxes: SSH, RDP, SMB, MySQL (checked), SQLServer (checked), Oracle (checked), FTP, MongoDB (checked), Memcached, PostgreSQL (checked), Telnet, SMTP, SMTP_SSL, POP3, POP3_SSL, IMAP, IMAP_SSL, VNC, and Redis (checked). The main area contains input fields for '目标:' (Target), '账户:' (Account), and '密码:' (Password), along with buttons for '导入地址' (Import Address), '导入账户' (Import Account), and '导入密码' (Import Password). There are also checkboxes for '只破解一个账户' (Only crack one account), '扫描端口' (Scan ports), and '不根据检查服务自动选择密码字典' (Do not automatically select password dictionary based on check service). Dropdown menus for '超时:' (Timeout: 15), '线程:' (Threads: 50), and '重试:' (Retries: 0) are present. A '开始检查' (Start Check) button and a '停止检查' (Stop Check) button are also visible. Below the input fields is a table titled '弱口令列表' (Weak Password List) with columns: 序号 (Serial Number), IP地址 (IP Address), 服务 (Service), 端口 (Port), 帐户名 (Account Name), 密码 (Password), BANNER, and 用时[毫秒] (Time [ms]).

数据安全治理实践路径：数据安全风险评估

➤ 数据库提权

某些数据库中可能存在能够提升权限的组件或漏洞，如mysql可利用udf.dll进行提升权限操作；sqlserver数据库中可利用xp_cmdshell、sp_oacreate组件进行提升权限操作；postgresql可利用某些版本中的漏洞进行提权操作。



数据安全治理实践路径：数据安全风险评估

➤ 安全控制

网络流量的加密保护 (TLS)

数据存储/系统数据的加密

数据使用中的加密保护

数据库中敏感内容的加密保护

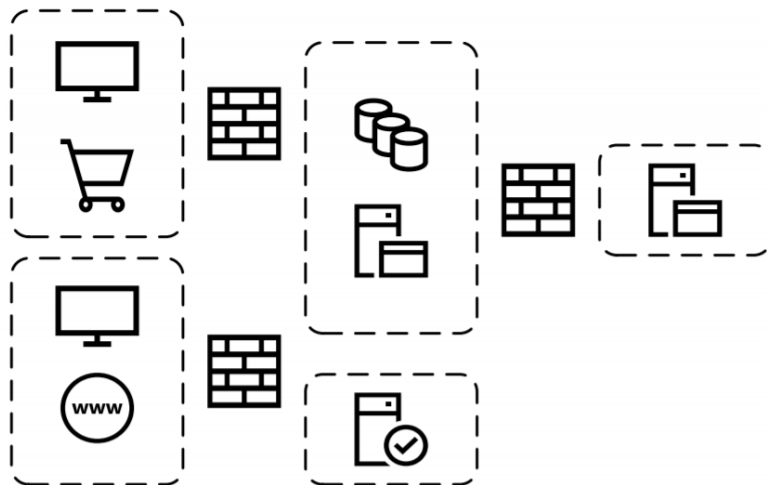
加密密钥和证书的防护

授权和鉴权机制的加密

WAF

数据库防火墙

.....



数据安全治理实践路径：数据安全风险评估

➤ 数据库加密

应用层加密

姓名	身份证号
张三	112233***
李四	234567***



姓名	身份证号
张三	ARnP%1***
李四	x@~j1***

格式保留加密(FPE)

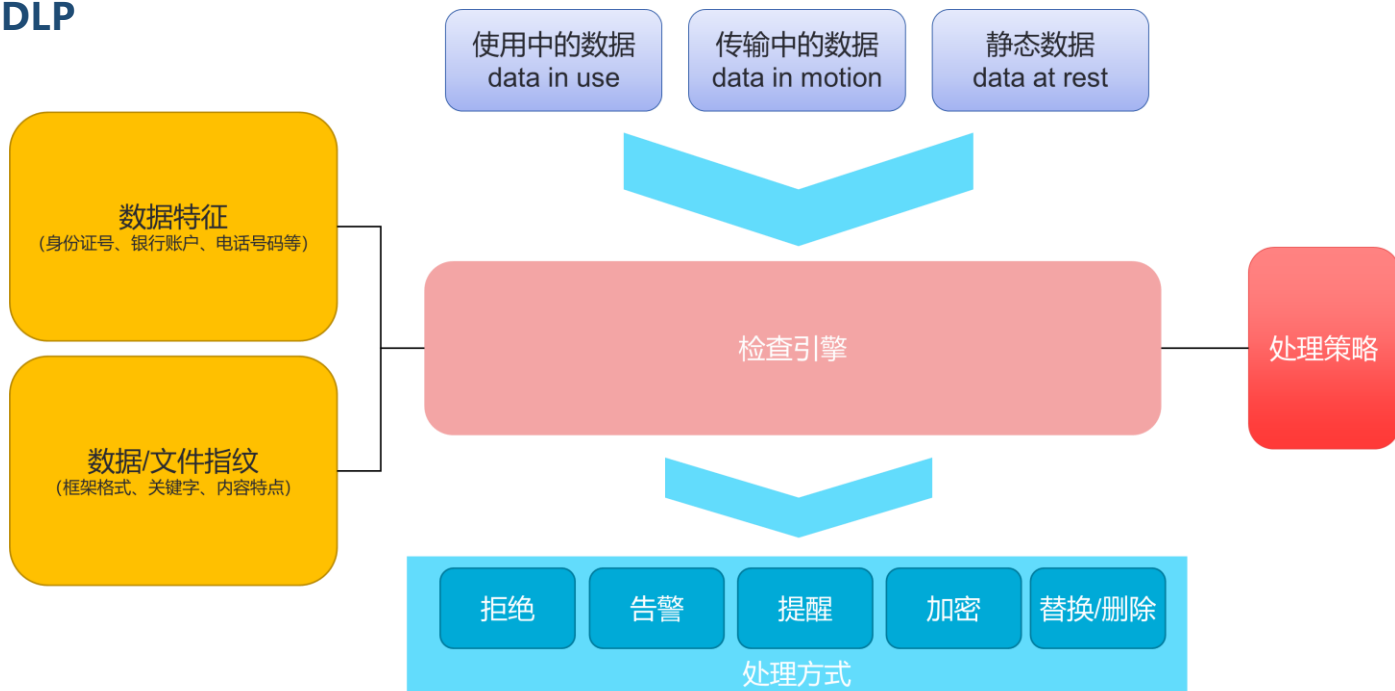
姓名	身份证号
张三	112233***
李四	234567***



姓名	身份证号
张三	621791***
李四	183563***

数据安全治理实践路径：数据安全风险评估

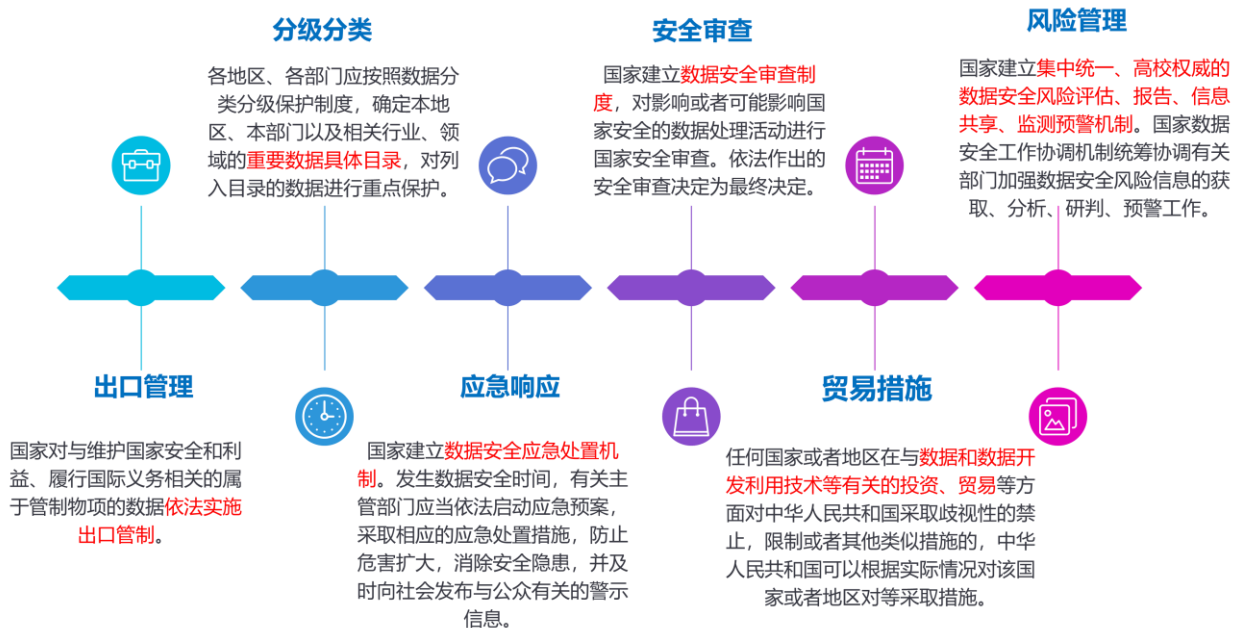
➤ DLP



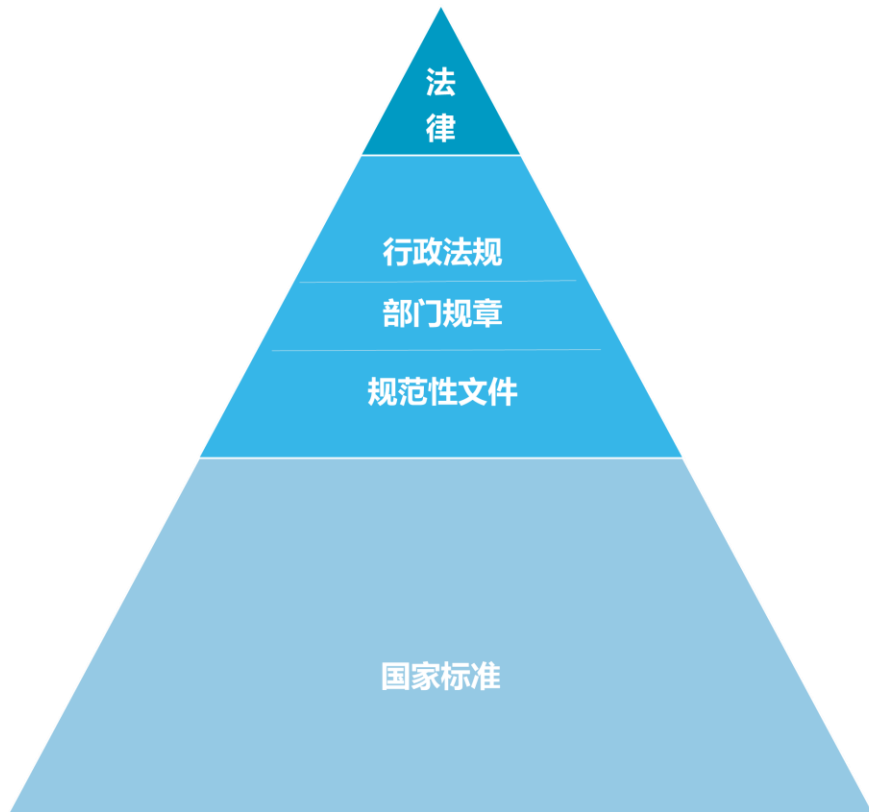
数据安全治理实践路径：数据安全风险评估

数据安全风险评估包含数据基础风险评估、数据安全合规风险评估以及数据全生命周期风险评估。

数据安全合规风险评估 – 以数据安全法为例



中国数据安全领域法律法规体系



- ◆ 《网络安全法》
- ◆ 《数据安全法》
- ◆ 《个人信息保护法》

- ◆ 《儿童个人信息网络保护规定》
- ◆ 《网络安全审查办法》
- ◆ 《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》
- ◆ 《常见类型移动互联网应用程序必要个人信息范围》
- ◆ 《个人信息出境安全评估办法（征求意见稿）》
- ◆ 《互联网个人信息安全保护指南》
- ◆ 《App违法违规收集使用个人信息自评估指南》
- ◆

- ◆ 《GB/T 31500-2015 信息安全技术 存储介质数据恢复服务要求》
- ◆ 《GB/T 15843.6-2018信息技术 安全技术 实体鉴别 第6部分：采用人工数据传递的机制》
- ◆ 《GB/T 37025-2018 信息安全技术 物联网数据传输安全技术要》
- ◆ 《GB/T 37973-2019信息安全技术 大数据安全管理指南》
- ◆ 《GB/T 35273-2020 信息安全技术 个人信息安全规范》
- ◆ 《GB/T 39335-2020 信息安全技术 个人信息安全影响评估指南》
- ◆ 《GB/T 39276-2020 信息安全技术 网络产品和服务安全通用要求》
- ◆ 《GB/T 39725-2020 信息安全技术 健康医疗数据安全指南》
- ◆ 《信息安全技术 数据出境安全评估指南（征求意见稿）》
- ◆

数据安全治理实践路径：数据安全风险评估

数据安全风险评估包含数据基础风险评估、数据安全合规风险评估以及数据全生命周期风险评估。

数据全生命周期风险评估

数据安全法



数据安全能力成熟度模型



数据安全常态化安全运营

数据安全常态化运营包括常态化安全治理、安全自动化响应建设、数据安全意识培训与攻防演练。

常态化安全治理在上述现有数据安全治理成果之上，定期进行现状调研与业务分析，确认当前数据安全持续性落实程度以及业务变化，若业务变化导致数据分类分级、数字资产等出现更新，则需要根据新的数据资产情况和新产生数据类别进行梳理和分类分级，确保数据安全治理成果与业务变化与时俱进。

数据安全常态化安全运营

数据安全常态化运营包括常态化安全治理、安全自动化响应建设、数据安全意识培训与攻防演练。

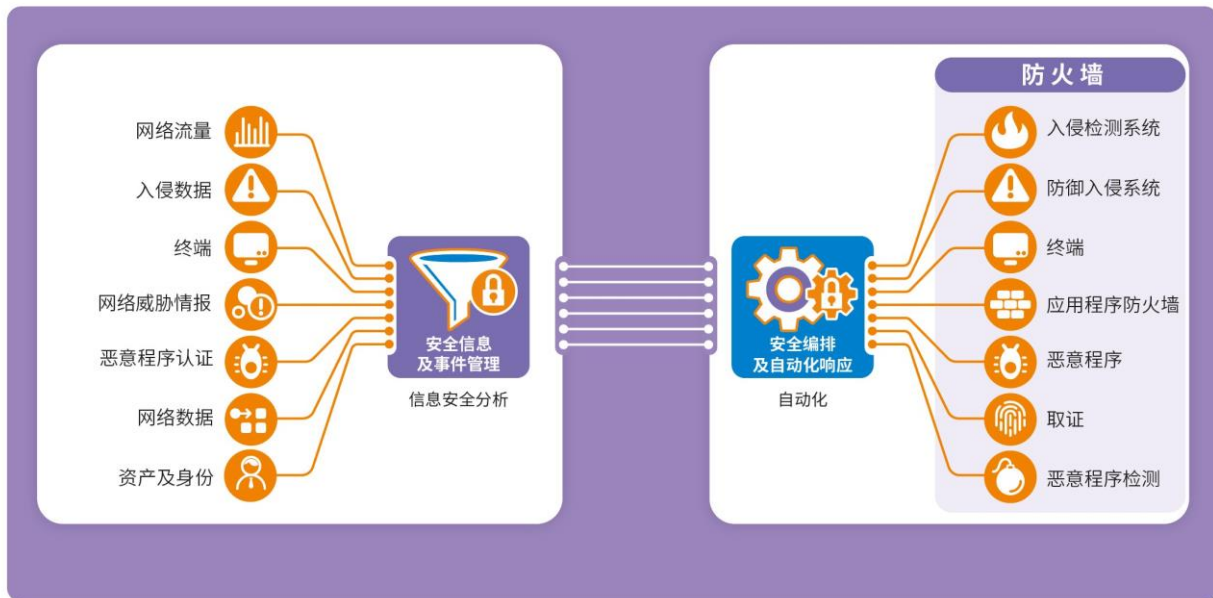
安全自动化响应建设



数据安全常态化安全运营

数据安全常态化运营包括常态化安全治理、安全自动化响应建设、数据安全意识培训与攻防演练。

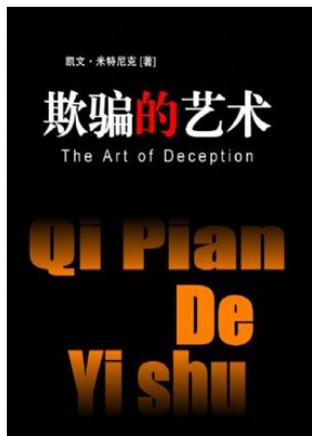
安全自动化响应建设



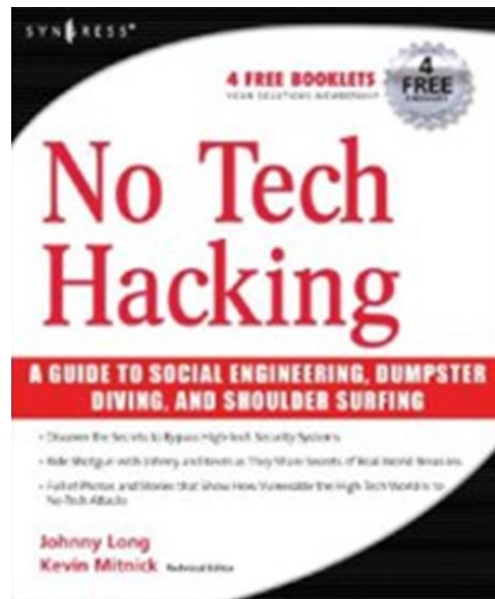
数据安全常态化运营包括常态化安全治理、安全自动化响应建设、数据安全意识培训与攻防演练。

数据安全意识

社会工程学是一门综合艺术，结合社会学、心理学、人际关系学和行为学，用于达到技术上难以达到的目的。



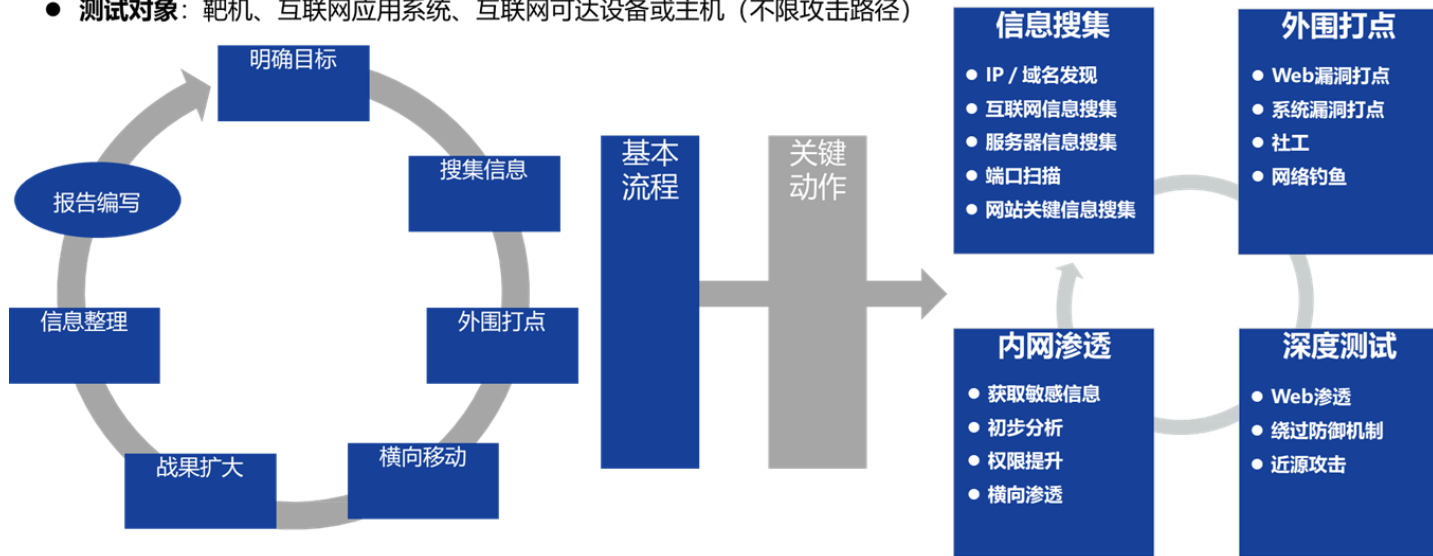
利用人的心理弱点（如人的本能反应、好奇心、信任、贪婪）、规章制度的漏洞进行诸如欺骗、伤害等手段，以期获得所需的信息（如计算机口令、银行账户信息）。



数据安全常态化运营包括常态化安全治理、安全自动化响应建设、数据安全意识培训与攻防演练。

攻防演练

- **工作目标:** 全面验证脆弱点，明确测试对象的安全隐患，并检视安全加固后的安全防御能力，最大限度削减脆弱性
- **测试对象:** 靶机、互联网应用系统、互联网可达设备或主机（不限攻击路径）



对目标单位和靶机进行**多轮外围打点**，**攻击路径不限**，深度挖掘脆弱性问题

1

数据安全导论

- 数据安全基础知识
- 数据安全法律法规和标准
- 数据安全模型和框架
- 数据分类与访问控制

2

数据安全风险挑战与响应

- 数据风险和挑战
- 数据风险管理
- 数据风险缓解措施

3

数据安全治理与架构

- 数据安全治理
- 数据安全管理体系
- 数据安全架构

4

密码学与加密基础

- 密码学基础
- 密钥管理基础
- 密码学国际国内标准
- 最佳实践

5

隐私保护理念与实践

- 隐私基本概念
- 法律法规和监管要求
- 隐私保护原则

6

新兴技术的数据安全挑战

- 大数据、AI区块链等新兴场景与数据安全
- 隐私保护技术

数据安全框架学习 - CDSP

主要面向安全领域有相关经验的管理者和专业人士、相关研究人员、开发技术人员，以及其它有志于从事数据安全领域咨询、管理和架构设计的人士。

- 首席数字官/首席数据官
- 首席安全官/首席信息安全官
- 首席信息官/首席隐私官
- 信息技术总监/信息安全总监/经理
- 安全顾问/分析师/审计师
- 安全架构师/设计师
- 产品架构师/领域架构师/系统设计师
- 安全系统工程师
- 对数字安全和隐私保护有兴趣的人士
- 有直接面向个人客户的线下和线上业务的金融行业企业



Q&A环节



谢谢
Thank you