BIG DATA EMPOWERS
TO CREATE A NEW
ERA

运维人员安全意识培训内容

汇报人：

2024-01-31

目录

CONTENTS

BIG DATA EMPOWERS
TO CREATE A NEW
ERA

01

运维安全概述

运维安全定义与重要性

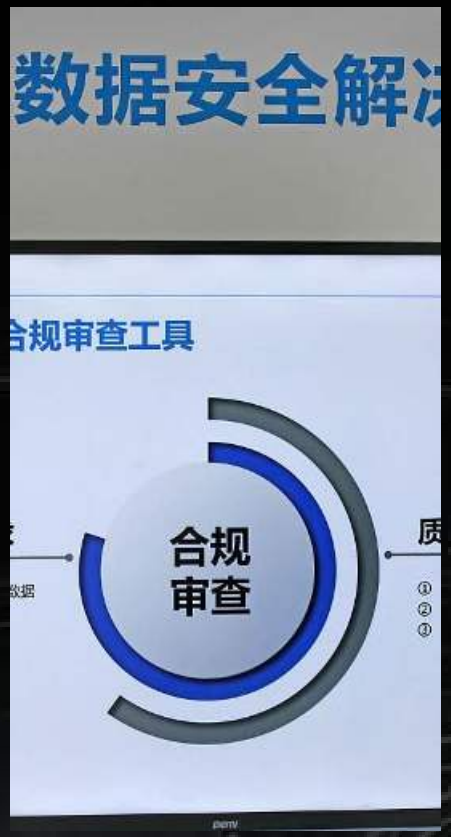
运维安全定义

运维安全是指在信息系统运维过程中，通过采取技术、管理、法律等手段，保护信息系统的机密性、完整性、可用性、可控性和可审查性，确保信息系统安全、稳定、高效运行。

运维安全重要性

运维安全是信息系统安全的重要组成部分，直接关系到企业的业务连续性和数据安全。一旦运维环节出现安全问题，可能导致系统瘫痪、数据泄露、业务中断等严重后果。

常见运维安全风险及案例分析



常见运维安全风险

包括账号与权限管理不当、恶意代码植入、未授权访问、数据泄露或篡改、拒绝服务攻击等。

案例分析

结合实际案例，分析运维安全风险产生的原因、造成的后果以及应对措施，提高运维人员对安全风险的识别和防范能力。

运维人员职责与角色定位

运维人员职责

包括系统监控、故障处理、性能优化、数据备份与恢复、安全加固等，确保信息系统稳定、高效、安全运行。

角色定位

运维人员在信息安全体系中扮演着重要角色，既是系统运行的守护者，也是安全风险的防范者。他们需要具备扎实的技术基础、敏锐的安全意识和严谨的工作态度，确保运维工作的顺利进行。

BIG DATA EMPOWERS
TO CREATE A NEW
ERA

02

系统安全基础知识

操作系统安全配置与加固

1

了解操作系统的基本安全机制

包括用户认证、访问控制、安全审计等。

2

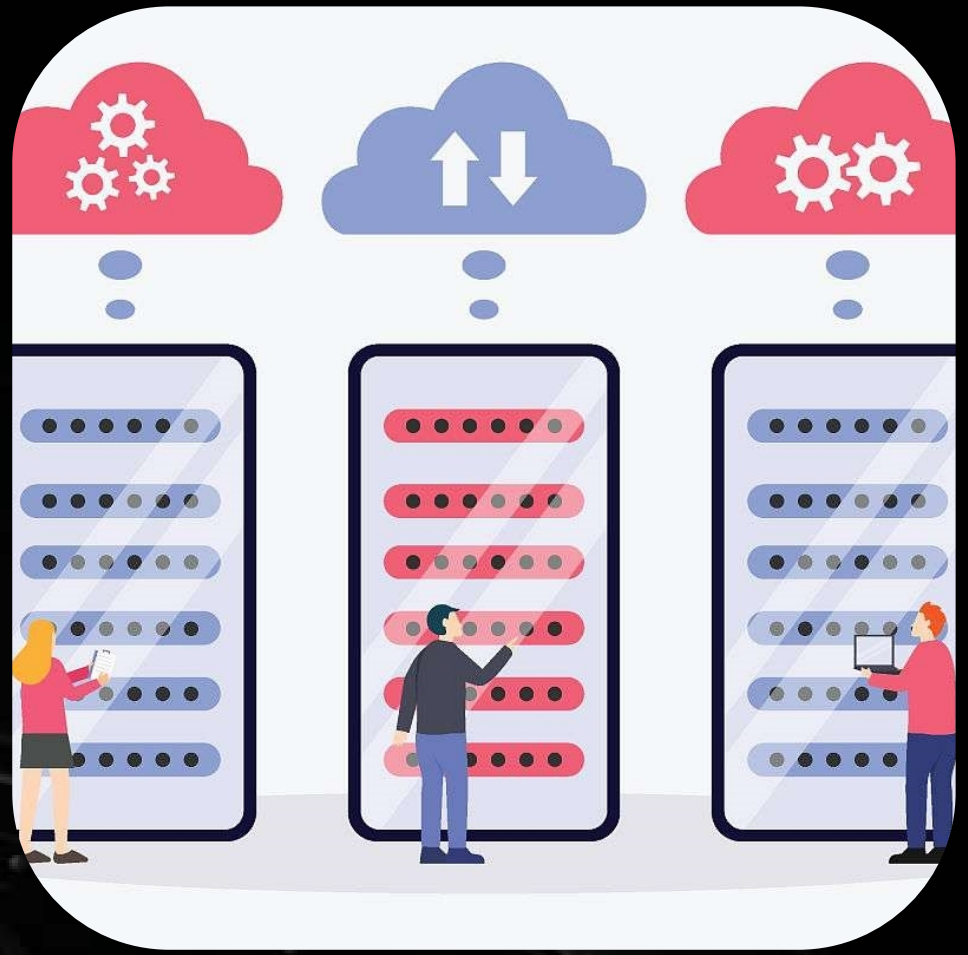
掌握操作系统的安全配置方法

如关闭不必要的服务、设置强密码策略、配置防火墙等。

3

熟悉操作系统的加固措施

包括安装安全补丁、升级系统版本、使用安全工具等。



网络设备安全策略部署

01

了解网络设备的安全威胁

如DDoS攻击、ARP欺骗、中间人攻击等。

02

掌握网络设备的安全配置方法

如配置访问控制列表（ACL）、启用加密技术、设置安全管理员权限等。

03

熟悉网络设备的安全策略部署

包括网络隔离、VPN技术、入侵检测系统等。

数据库管理系统安全防护

了解数据库管理系统的安全威胁

如SQL注入、数据泄露、权限提升等。

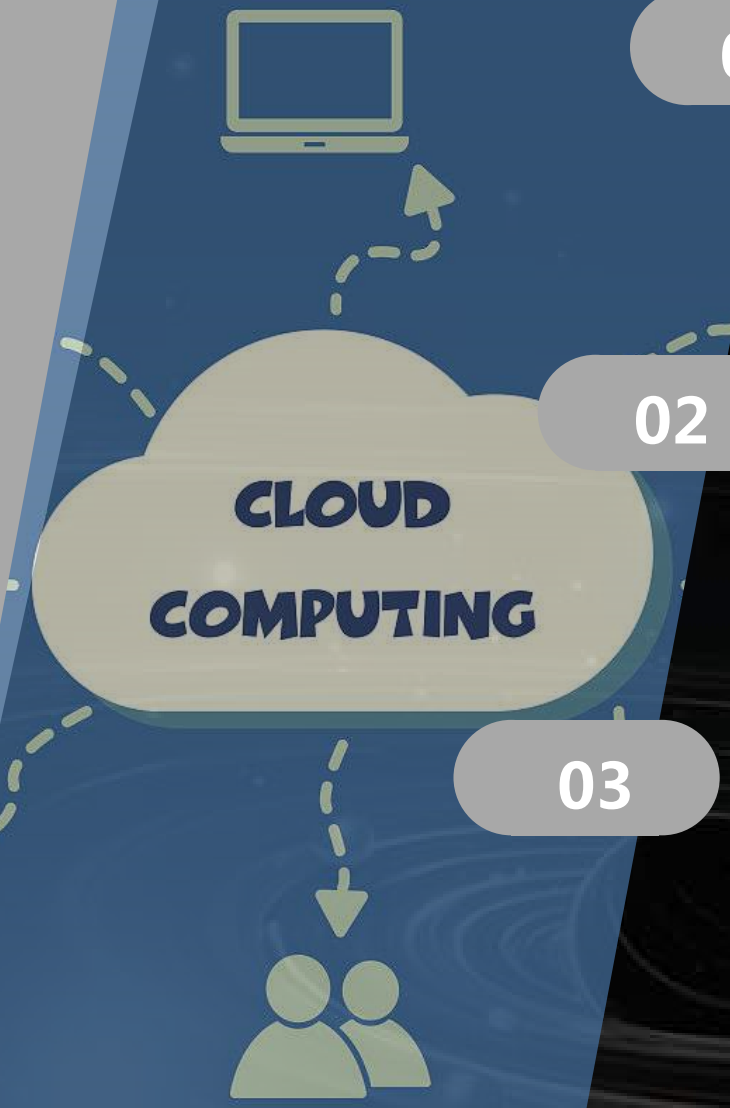
掌握数据库管理系统的安全配置方法

如设置强密码、限制用户权限、开启审计功能等。

熟悉数据库管理系统的安全防护措施

包括数据加密、备份恢复、安全漏洞修补等。

应用软件漏洞修复及更新



01

了解应用软件的安全漏洞类型

如缓冲区溢出、跨站脚本攻击、文件上传漏洞等。

02

掌握应用软件漏洞的修复方法

如升级软件版本、安装安全补丁、修改配置文件等。

03

熟悉应用软件的更新策略

包括定期更新、紧急更新、灰度更新等，以确保软件的安全性和稳定性。

BIG DATA EMPOWERS
TO CREATE A NEW
ERA

03

网络安全防护技能提升

防火墙配置与管理实践

防火墙基本原理与功能

了解防火墙的作用、分类及工作原理，掌握包过滤、代理服务等核心技术。

常见防火墙产品配置

熟悉市场上主流防火墙产品的配置方法，如Cisco、Juniper、华为等。

防火墙策略优化

根据业务需求和安全风险，制定并优化防火墙访问控制策略，提高安全防护效果。

防火墙日志分析与故障排除

掌握防火墙日志分析方法，及时发现并处理安全事件和故障。

入侵检测与响应机制建设

入侵检测系统（IDS）原理与部署

了解IDS的工作原理、分类及部署方式，掌握签名检测、异常检测等核心技术。

入侵防御系统（IPS）应用与实践

熟悉IPS的功能、特点及与IDS的区别，掌握IPS在网络安全防护中的应用。

安全信息与事件管理（SIEM）技术

了解SIEM的基本概念、功能及架构，掌握其在入侵检测与响应中的作用。

应急响应流程与演练

制定应急响应流程，组织定期的应急演练，提高应对网络安全事件的能力。