YOUR LOGO

Windows 安全与保护机制

2024

主讲人：郑冬贤

时间：2024

目 录

YOUR LOGO

Part 01

Windows 系统安全机制及设置

用户账户控制（UAC）

防止恶意软件自动安装

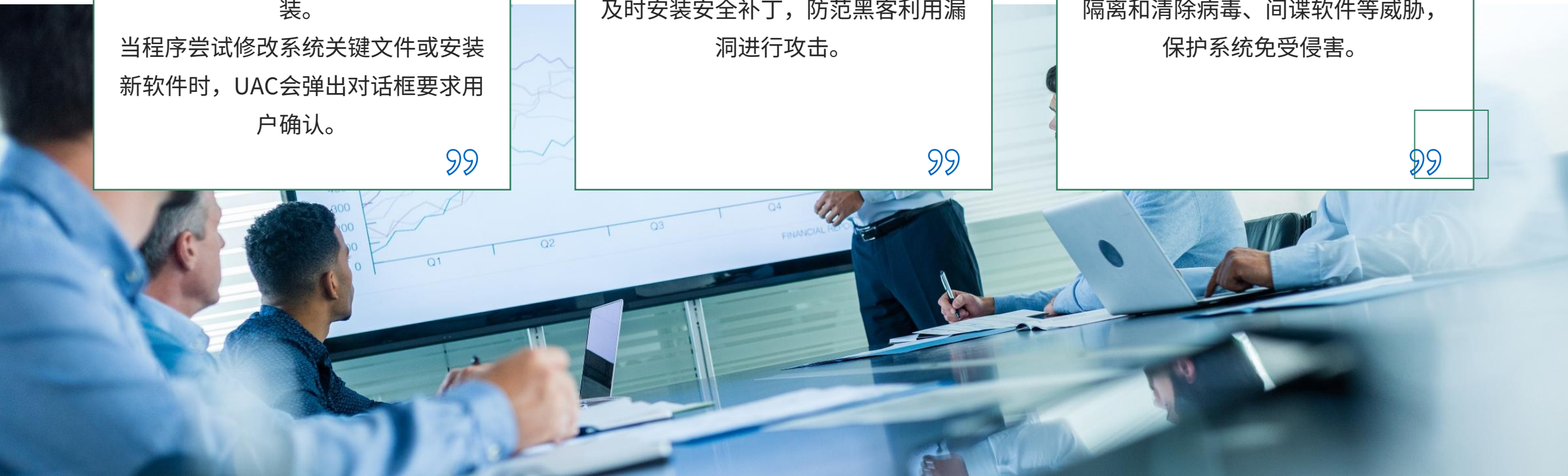
UAC通过提示用户确认来阻止未经授权的更改，有效防止恶意软件自动安装。
当程序尝试修改系统关键文件或安装新软件时，UAC会弹出对话框要求用户确认。

系统更新与补丁管理

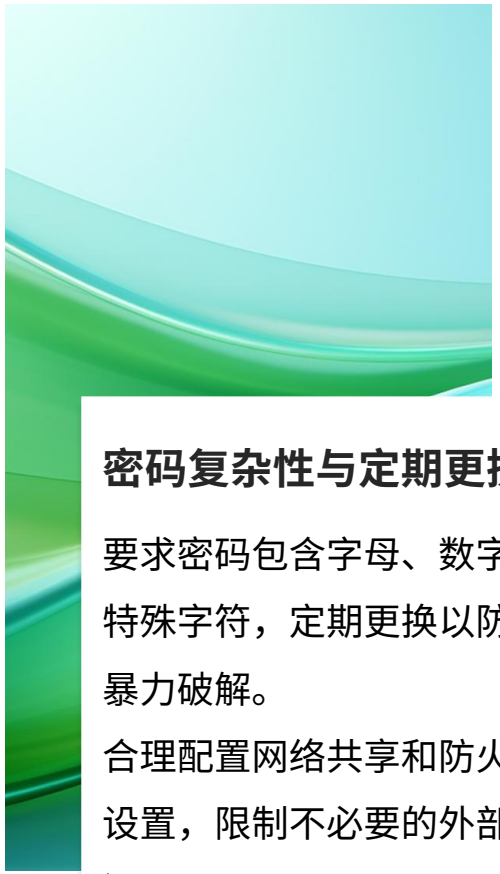
定期更新Windows系统，通过Windows Update功能修复已知漏洞。及时安装安全补丁，防范黑客利用漏洞进行攻击。

Windows Defender 实时监控

开启Windows Defender实时扫描和检测系统中的恶意软件。
隔离和清除病毒、间谍软件等威胁，保护系统免受侵害。



强密码策略与网络共享设置



密码复杂性与定期更换

要求密码包含字母、数字和特殊字符，定期更换以防止暴力破解。

合理配置网络共享和防火墙设置，限制不必要的外部访问。

01

防火墙与网络端口管理

关闭不必要的网络端口，只允许特定应用程序或服务通过防火墙通信。

减少系统暴露在网络攻击下的风险，提高系统安全性。

02

YOUR LOGO

Part 02

Windows Server 账户管理

创建不同权限的用户账户

根据职责分配最小化权限

创建不同权限的用户账户，根据员工职责分配权限，降低安全风险。
普通员工账户仅给予基本权限，管理员账户保留高级权限。

定期审查账户活动

审查账户活动，如登录时间、地点，发现异常使用情况。
及时采取措施，如锁定账户或更改密码，防止账户被盗用。

多因素身份验证（MFA）

增强账户登录安全性

即使密码泄露，攻击者也难以在没有其他认证因素的情况下登录系统。

采用多因素身份验证，如密码、短信验证码或硬件令牌。

YOUR LOGO

Part 03

Windows Server 注册表与组策略

注册表访问权限管理

防止未经授权的注册表修改

01

限制对注册表关键区域的访问权限，避免系统故障或安全漏洞。

02

将注册表中涉及系统启动项的键值设置为只读权限，防止恶意软件添加自启动项。

组策略集中管理配置

统一安全设置

通过组策略对域内的计算机和用户进行统一的安全设置。

快速、高效地将安全策略应用到大量计算机上，确保网络环境的安全性和一致性。

YOUR LOGO

Part 04

Windows Server 系统

进程与服务管理

识别系统进程和服务

注册表是 Windows Server 系统的核心数据库，存储了系统和应用程序的各种配置信息。合理管理注册表可以优化系统性能和安全性。通过限制对注册表关键区域的访问权限，防止未经授权的修改，避免因注册表被篡改而导致系统故障或安全漏洞。例如，将注册表中涉及系统启动项的键值设置为只读权限，防止恶意软件添加自启动项，随系统启动而运行。

组策略则提供了集中管理和配置 Windows 系统的功能。管理员可以通过组策略对域内的计算机和用户进行统一的安全设置，如设置密码策略、限制特定软件的运行、配置网络访问规则等。利用组策略可以快速、高效地将安全策略应用到大量的计算机上，确保整个网络环境的安全性和一致性，减少因人为配置错误或遗漏而产生的安全隐患。

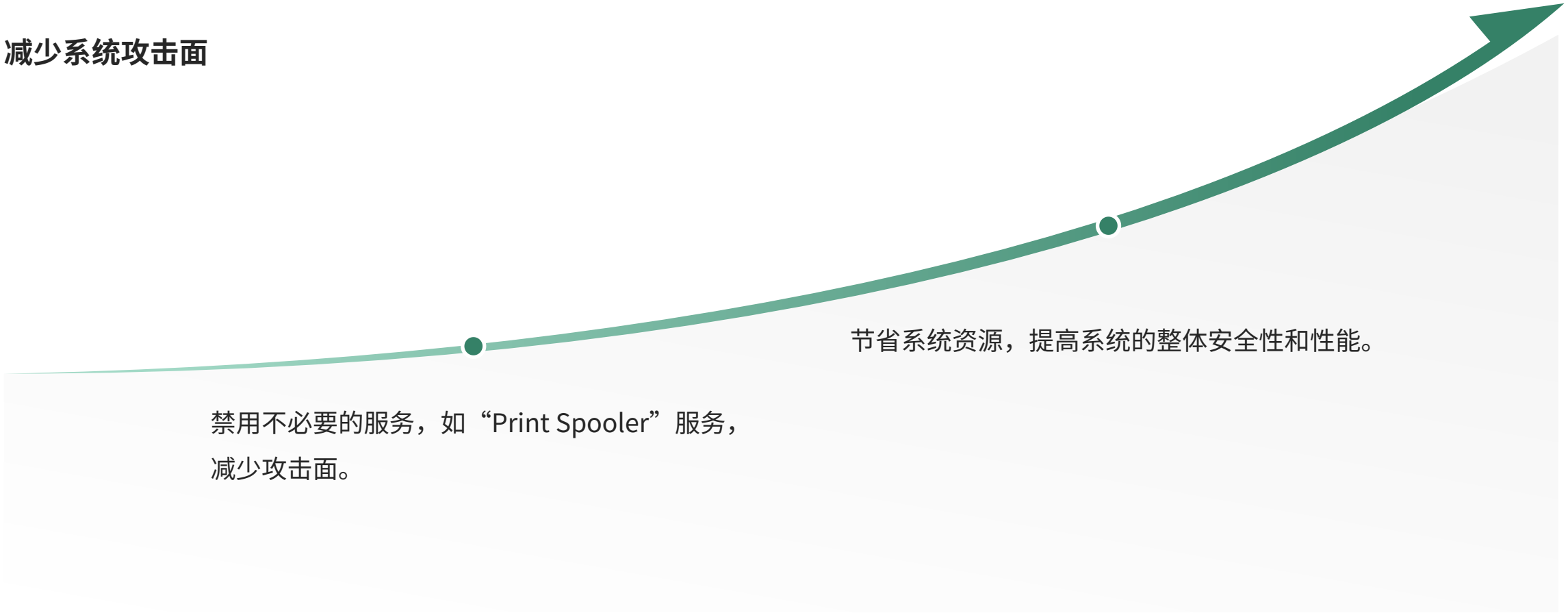
了解系统进程的功能和行为模式

熟悉系统进程和服务，识别潜在的安全问题。

及时发现异常进程，如多个同名进程或路径异常可能意味着系统被恶意软件感染。

禁用不必要的服务

减少系统攻击面



禁用不必要的服务，如“Print Spooler”服务，减少攻击面。

节省系统资源，提高系统的整体安全性和性能。

YOUR LOGO

Part 05

Windows Server 日志管理

启用详细日志记录

Windows Server 的日志记录了系统、应用程序和安全事件的详细信息，是安全分析和故障排查的重要依据。启用详细的日志记录功能，包括登录事件、文件访问事件、系统错误事件等，确保能够全面捕捉系统活动信息。
定期检查和分析日志文件，通过查看登录失败记录，可以发现潜在的暴力破解攻击尝试；分析文件访问日志，能够追踪敏感文件的访问情况，及时发现数据泄露风险。同时，合理设置日志存储位置和保留期限，防止日志被攻击者篡改或删除，确保日志数据的完整性和可用性，以便在发生安全事件时能够进行有效的追溯和调查，明确事件的发生原因、时间和涉及的账户等关键信息，为采取相应的安全措施提供有力支持。

全面捕捉系统活动信息

启用详细日志记录功能，包括登录事件、文件访问事件、系统错误事件等。

确保能够全面捕捉系统活动信息，为安全分析和故障排查提供依据。

定期检查和分析日志文件

发现潜在的安全威胁

定期检查和分析日志文件，发现潜在的暴力破解攻击尝试。

分析文件访问日志，追踪敏感文件的访问情况，及时发现数据泄露风险。

YOUR LOGO

谢谢大家

2024

主讲人：郑冬贤

时间：2024