AI助力网络安全防护

深化理解，提升应对能力

Presenter name

Agenda

1. 互联网安全挑战威胁
2. 人工智能在安全中应用
3. 互联网公司安全防护
4. AI未来趋势和建议
5. AI基本原理和技术

01.互联网安全挑战威胁

网络安全威胁

网络病毒恶意软件威胁

网络病毒和恶意软件的威胁

信息窃取风险

网络病毒和恶意软件可能窃取用户的个人信息、账户密码等敏感数据，进一步被滥用或者售卖。

系统瘫痪风险

网络病毒和恶意软件可能导致系统崩溃或瘫痪，影响企业的正常运营和用户的使用体验。

数据泄露风险

网络病毒和恶意软件威胁网络安全。

数据泄露隐私问题

数据泄露与隐私问题

01

个人信息泄露

敏感信息泄露可能导致隐私和身份被窃取的风险：加强信息安全保护。

02

商业机密泄露

企业的商业机密、竞争优势等敏感信息的泄露可能导致严重的经济损失和商誉受损。

03

网络行为监控

用户在互联网上的行为轨迹被监控和记录，涉及个人隐私权的问题引发争议和担忧。

网络攻击及其影响

01

病毒攻击

通过植入恶意软件来感染系统，导致数据损坏和系统崩溃：恶意软件感染系统导致数据损坏

02

DDoS攻击

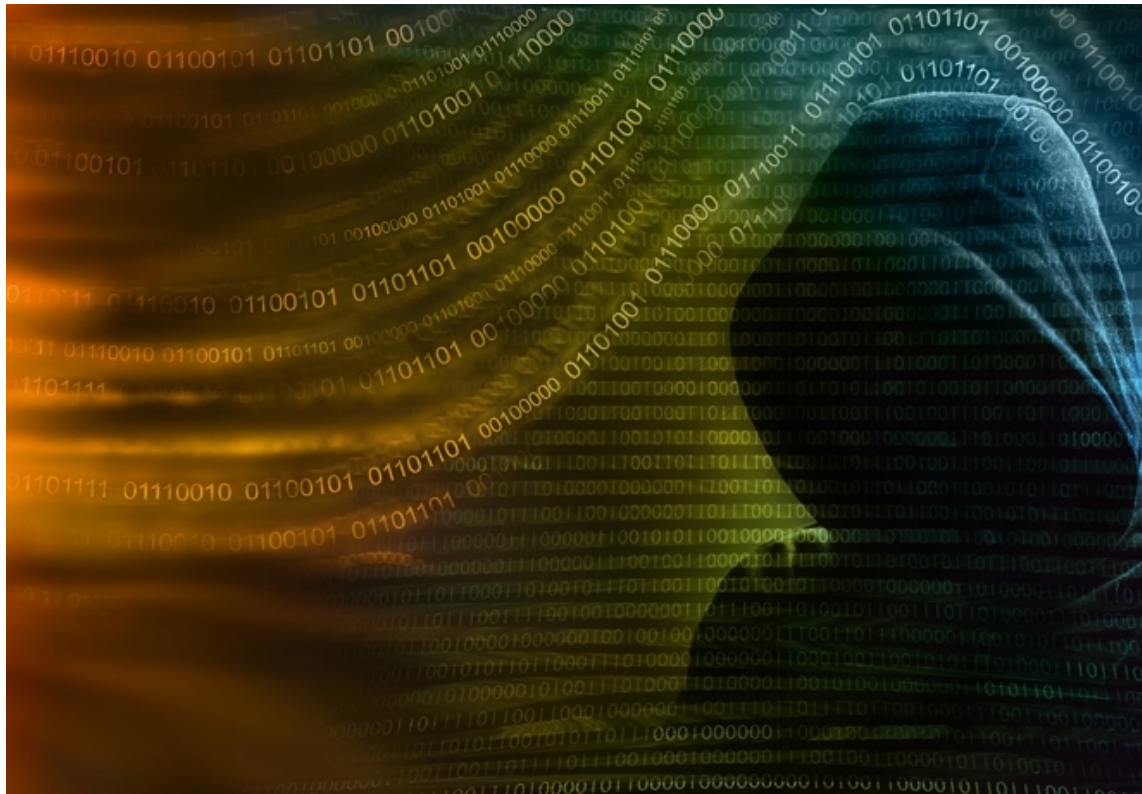
通过大量无效请求淹没目标服务器，使其无法正常工作，造成服务中断和损失。

03

社交工程攻击

利用心理和社交技巧欺骗用户，获取敏感信息或诱使其执行恶意操作。

网络攻击类型及其影响



02.人工智能在安全中应用

智能安全防护

自动化安全监测与响应

自动化安全监测和响应系统

智能化漏洞扫描

自动化扫描和识别网络漏洞

自动化事件响应

快速且准确地对安全事件进行响应

实时监测和响应

应对安全威胁

智能安全防护降误报

智能化防护和检测

智能化安全防护

利用人工智能技术提供智能防护措施: 提供智能防护。

智能化攻击检测

借助人工智能技术实现智能化的攻击检测功能

减少误报率

通过人工智能技术减少误报率，提高检测的准确性

分析网络数据发现威胁

异常检测技术

行为分析

发现用户异常活动的行为分析: 分析用户行为。

网络流量分析

监测和分析网络流量，检测异常数据包和攻击行为

日志分析

分析系统和应用程序日志，发现异常事件和威胁追踪

03.互联网公司安全防护

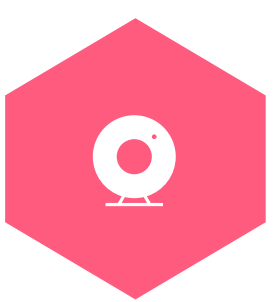
加密技术安全培训

安全培训与意识提升

提高员工安全意识

密码管理规范

加强密码强度和定期更新的意识



应急响应流程

掌握应急流程，快速响应安全事件

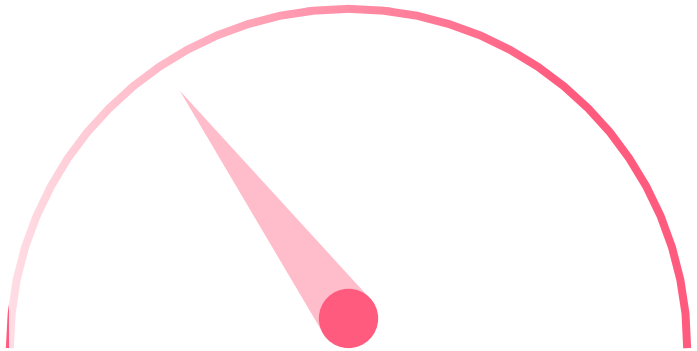
钓鱼邮件防范

提高识别和避免点击恶意链接的能力

加密技术：身份验证

加密技术和身份验证

数据加密



保护数据传输和存储的安全性

身份验证

验证用户身份以防止未授权访问

密钥管理

有效管理加密和解密所需的密钥