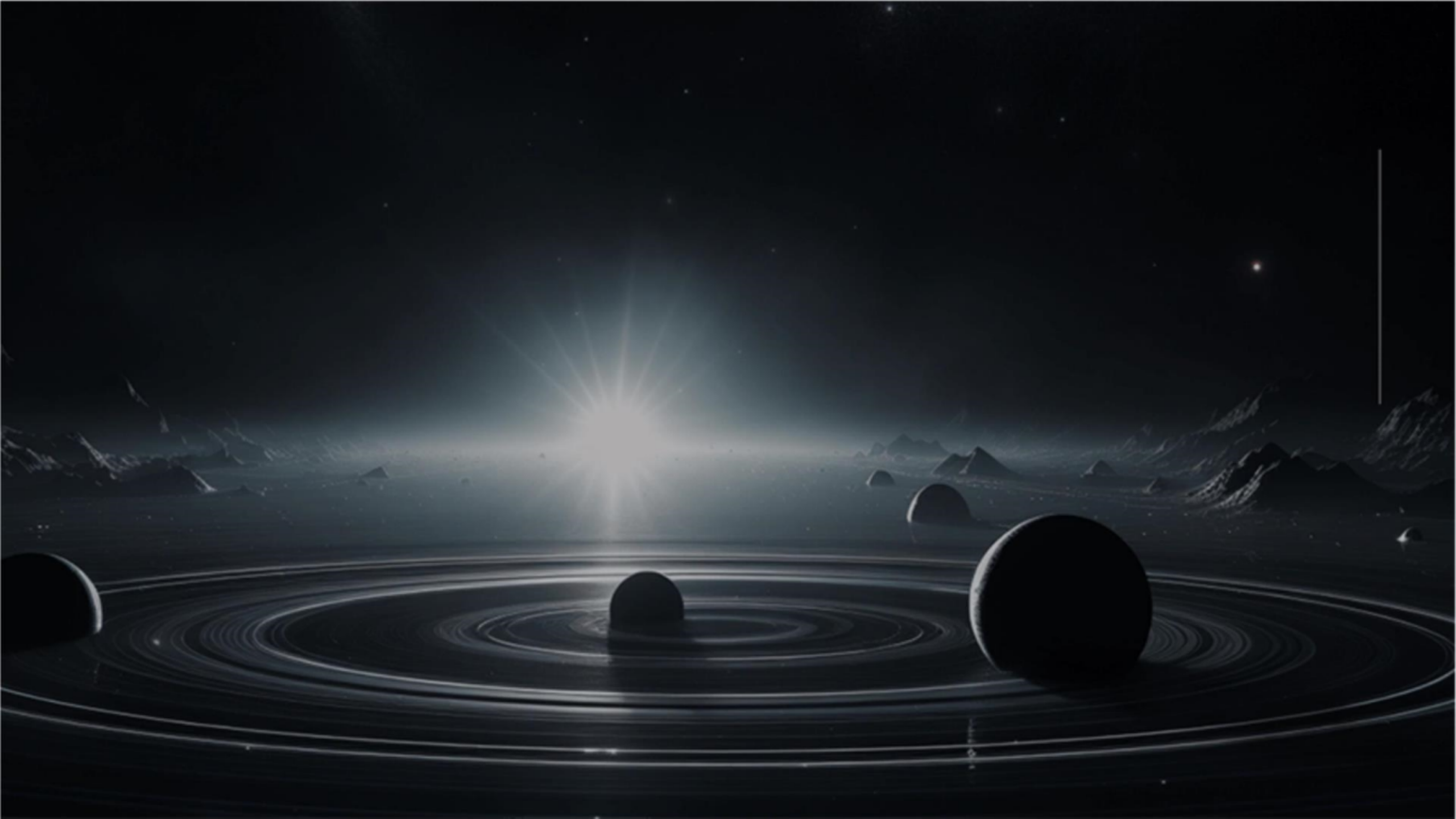
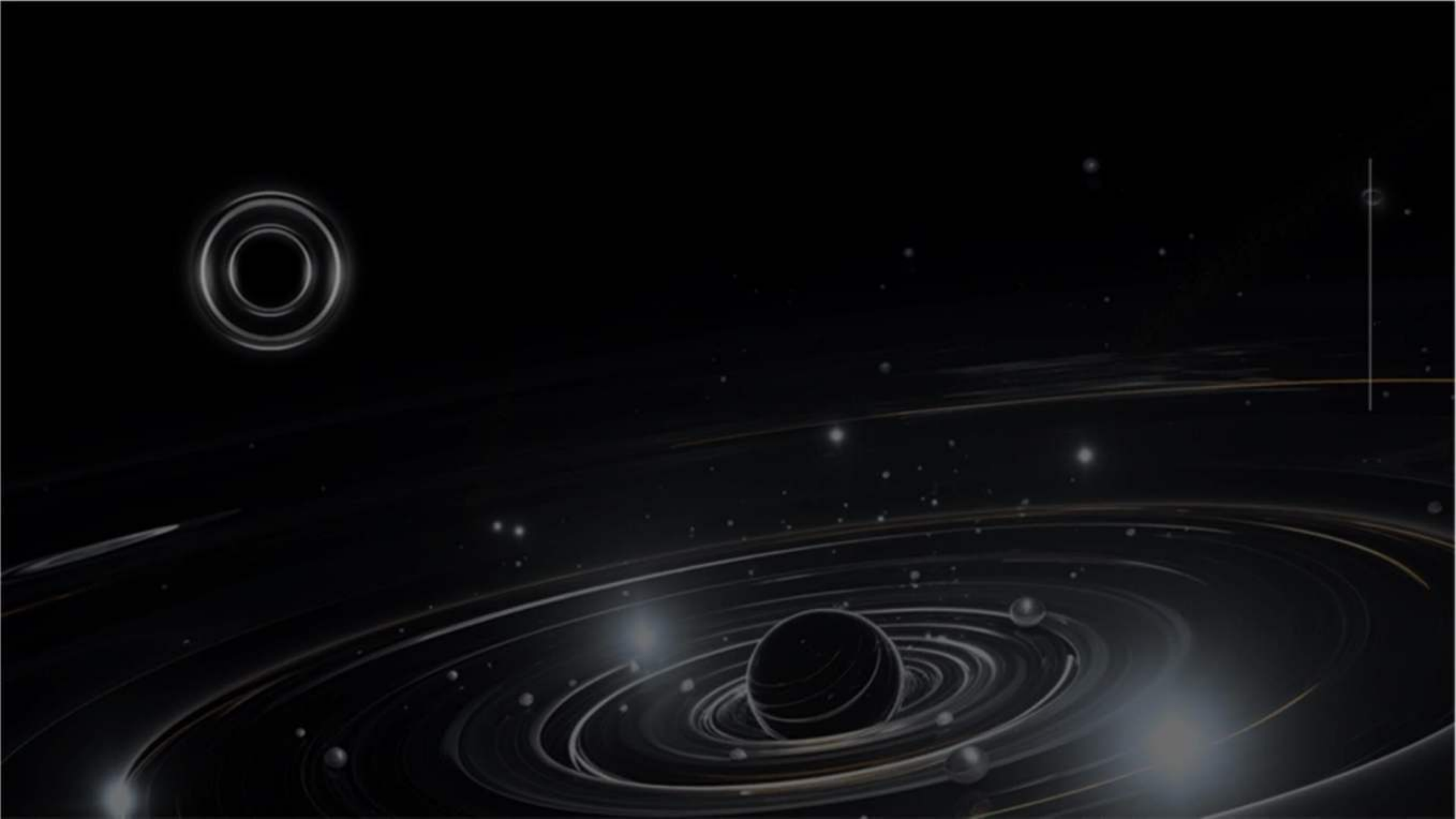


目录



定义与分类

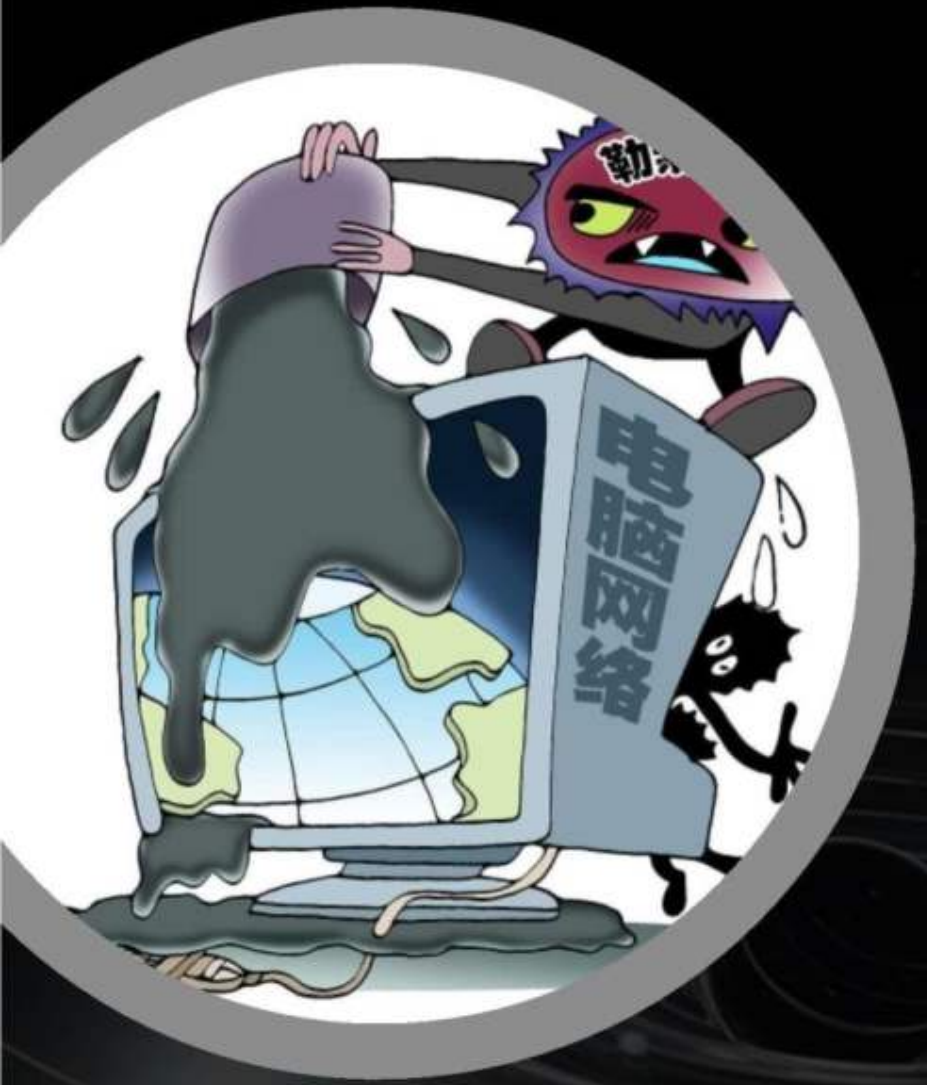
定义

网络攻击是指利用网络系统的漏洞或弱点，通过各种手段对网络及其相关设施进行窃取、破坏、篡改等行为，以达到非法目的。

分类

根据攻击方式和目标的不同，网络攻击可以分为拒绝服务攻击、恶意软件攻击、社交工程攻击、钓鱼攻击、SQL注入攻击等。

常见网络攻击手段



01

恶意软件

包括病毒、蠕虫、特洛伊木马等，通过感染用户设备或控制网络节点进行传播，对数据安全和个人隐私构成威胁。

02

钓鱼攻击

通过伪造信任网站或诱骗用户点击恶意链接，窃取个人信息或进行金融诈骗。

03

分布式拒绝服务攻击（DDoS）

通过大量无用的请求拥塞目标服务器或网络，导致合法用户无法访问，是一种常见的网络攻击方式。

网络攻击的危害

数据泄露

攻击者窃取敏感信息，如个人信息、企业机密等，可能导致严重后果。

系统瘫痪

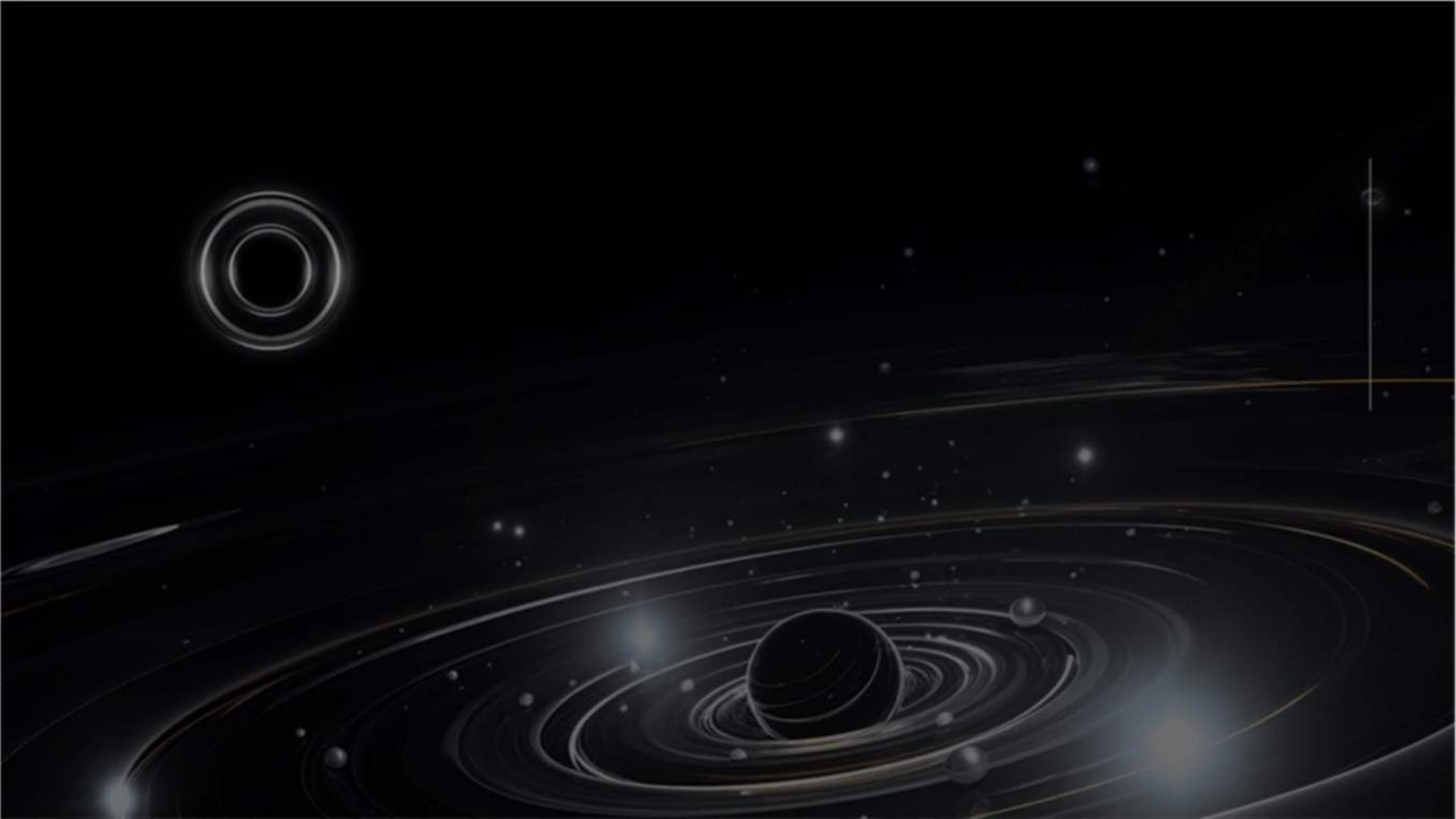
拒绝服务攻击等手段可导致网络服务中断，影响正常的生产和生活。

经济损失

网络攻击可能导致企业遭受经济损失，如修复系统、赔偿用户损失等。

声誉损害

企业遭受网络攻击可能导致公众对其信任度降低，影响企业形象和声誉。



防火墙技术

防火墙概述

防火墙是网络安全的重要组件，用于隔离内部网络和外部网络，防止未经授权的访问和数据泄露。

防火墙类型

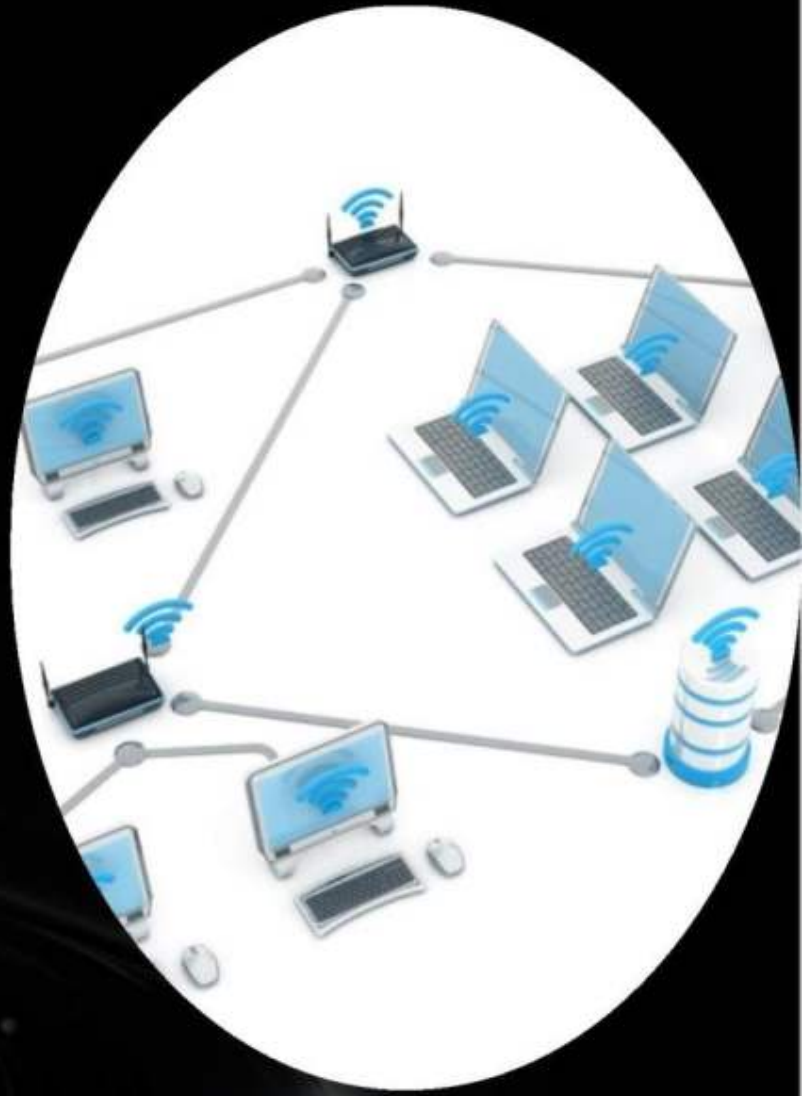
根据实现方式和功能，防火墙可分为包过滤防火墙、代理服务器防火墙和有状态检测防火墙等。

防火墙部署

防火墙的部署应根据网络结构和安全需求进行合理配置，包括选择合适的部署位置、配置安全策略等。

防火墙发展趋势

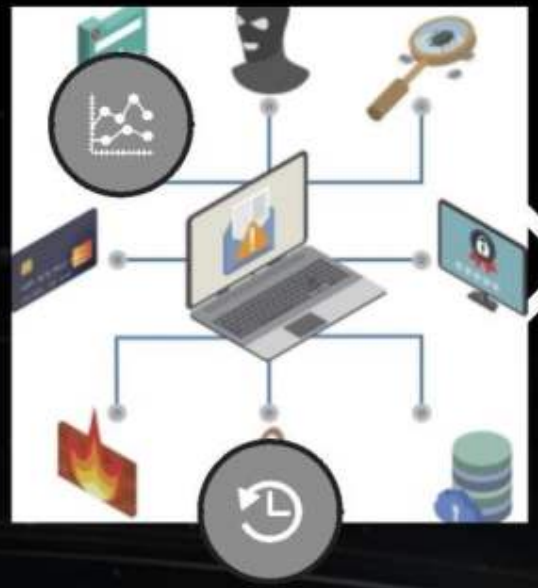
随着网络安全威胁的不断变化，防火墙技术也在不断发展，出现了下一代防火墙、云防火墙等新型防火墙。



入侵检测系统

入侵检测概述

入侵检测系统用于实时监测网络流量和系统行为，发现异常行为并及时报警。



入侵检测技术

入侵检测涉及多种技术，如流量分析、协议分析、系统日志分析等。

入侵检测类型

根据检测方式，入侵检测可分为基于特征的检测和基于异常的检测两类。

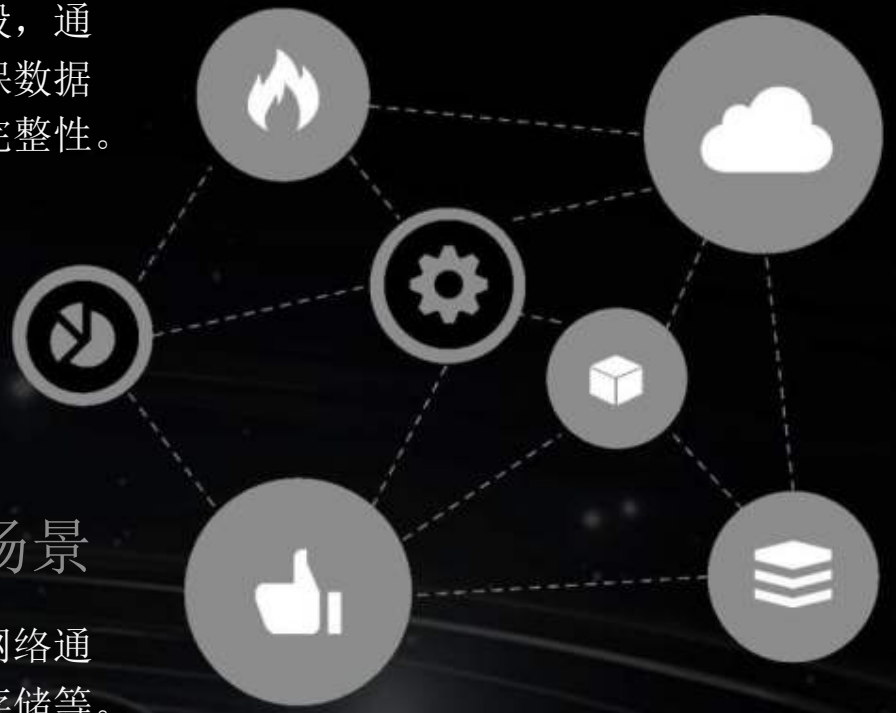
入侵检测发展趋势

随着威胁的不断演变，入侵检测系统也在不断发展，出现了基于人工智能的入侵检测等新技术。

数据加密技 术

数据加密概述

数据加密是保护数据安全的重要手段，通过加密算法将明文转换为密文，确保数据在传输和存储过程中的机密性和完整性。



数据加密算法

常见的数据加密算法包括对称加密算法（如AES、DES）和非对称加密算法（如RSA）。

数据加密应用场景

数据加密广泛应用于各类场景，如网络通信、数据库存储、云存储等。

数据加密发展趋势

随着技术的不断发展，数据加密算法也在不断演进，出现了量子加密等新型加密技术。

安全审计与日志分析

安全审计概述

安全审计是对网络系统进行全面或局部的检查、监测和评估，以发现潜在的安全隐患和威胁。

日志分析

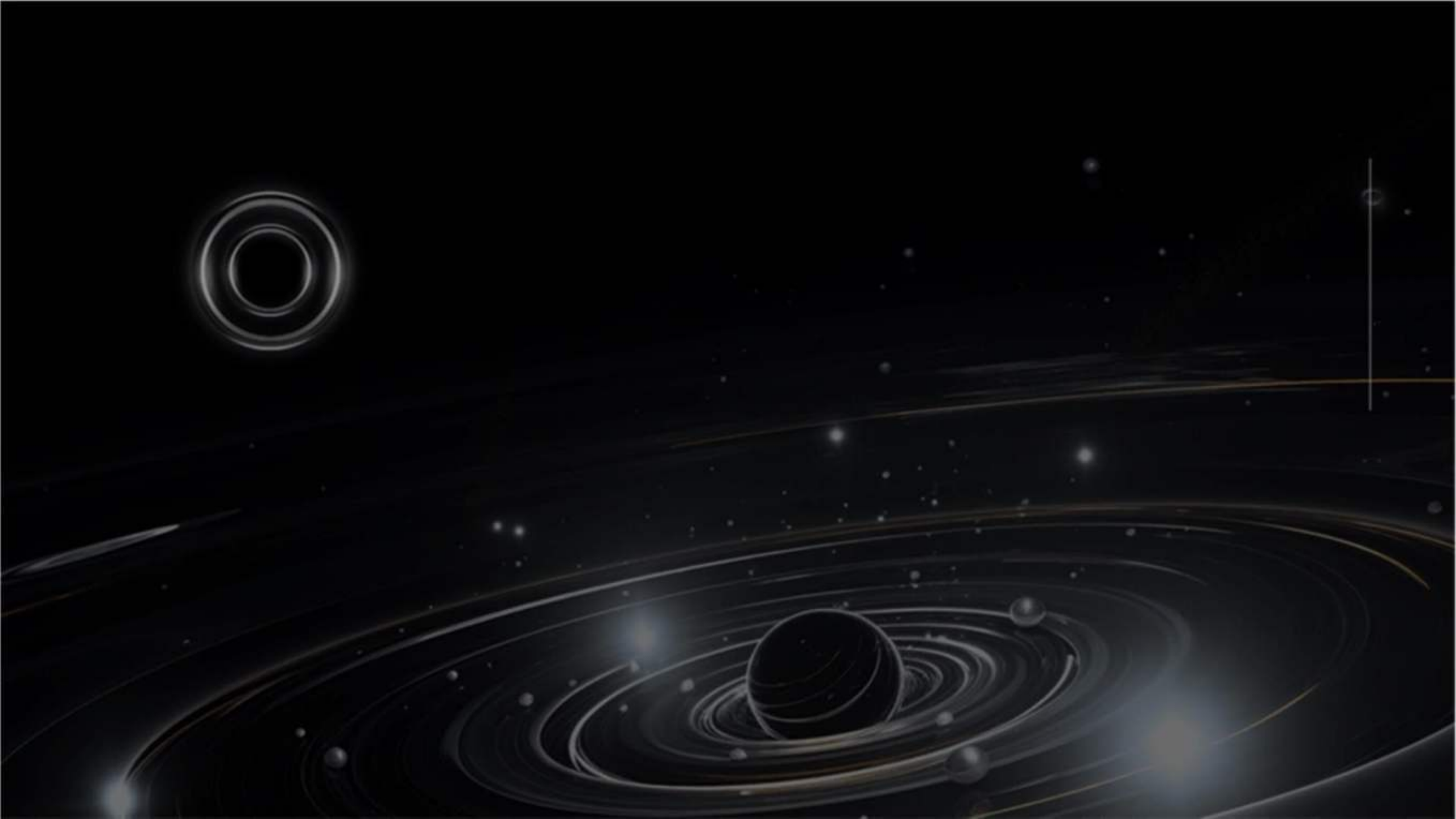
日志分析是对系统日志、网络流量日志等数据进行收集、处理和分析，以发现异常行为和安全事件。

安全审计工具

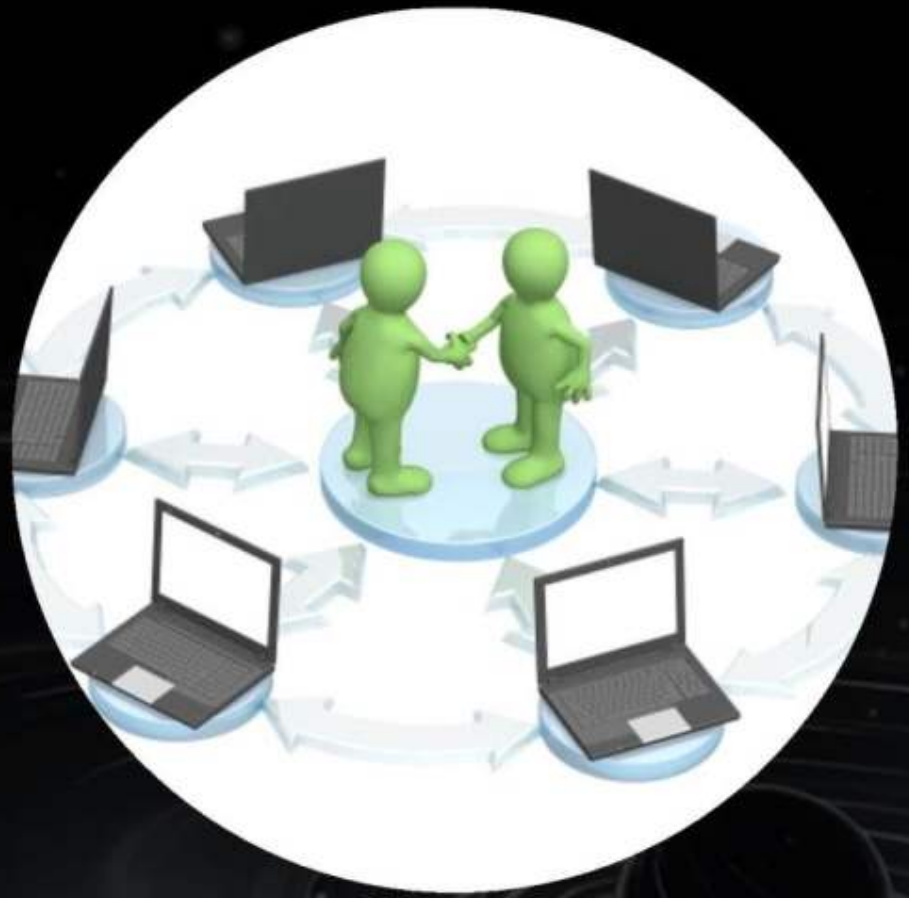
安全审计涉及多种工具，如漏洞扫描器、渗透测试工具等。

安全审计发展趋势

随着威胁的不断演变，安全审计技术也在不断发展，出现了基于大数据的安全审计等新技术。



网络安全策略制定



确定网络安全目标

根据组织的需求和风险评估，明确网络安全的目标和优先级。

制定安全策略

基于安全目标，制定相应的网络安全策略，包括数据保护、访问控制、事件响应等。

策略实施计划

为确保安全策略的有效实施，制定详细的实施计划，包括时间表、责任人及所需资源。

安全管理制度建 设

- 建立安全管理制度

  制定全面的安全管理制度，明确各部门和人员的安全职责。

- 定期安全培训

  组织定期的安全培训，提高员工的安全意识和技能。

- 安全审计与监控

  实施安全审计和监控，确保安全管理制度得到有效执行。