安全运维培训ppt课件

汇报人：文小库

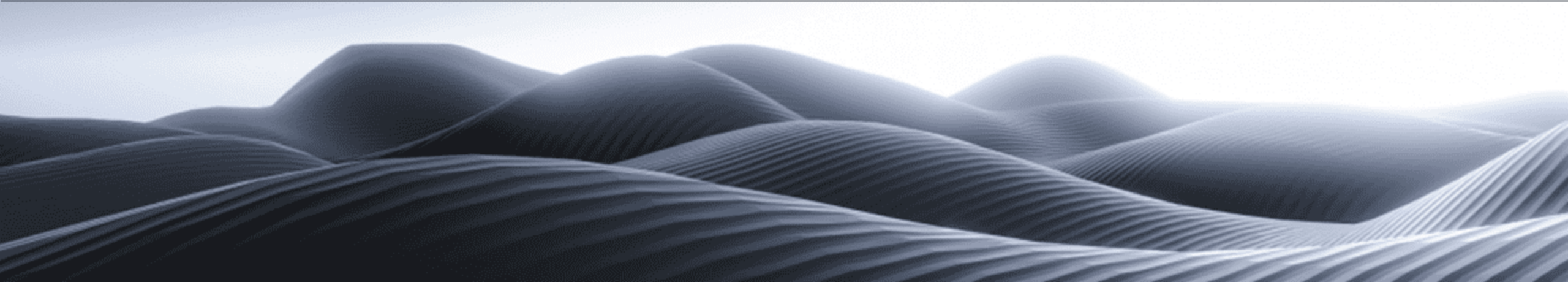
2023-12-16

contents

目录

01

安全运维概述



安全运维的定义

01

安全运维是指通过一系列技术、管理手段，确保信息系统安全稳定运行的过程。

02

安全运维包括对信息系统的监控、维护、优化以及应急响应等方面的工作。

安全运维的重要性

保障业务连续性

安全运维能够确保信息系统的稳定运行，避免因系统故障或安全事件导致业务中断。

降低安全风险

安全运维通过对信息系统的全面监控和评估，能够及时发现并解决潜在的安全风险，降低安全事件发生的概率。

防止数据泄露

通过安全运维，可以及时发现并修复潜在的安全漏洞，防止数据泄露和非法访问。

安全运维的框架

01

安全运维框架包括安全管理制度、安全技术手段、安全培训等方面。

02

安全管理制度包括信息安全政策、安全操作规程等，为安全运维提供制度保障。

03

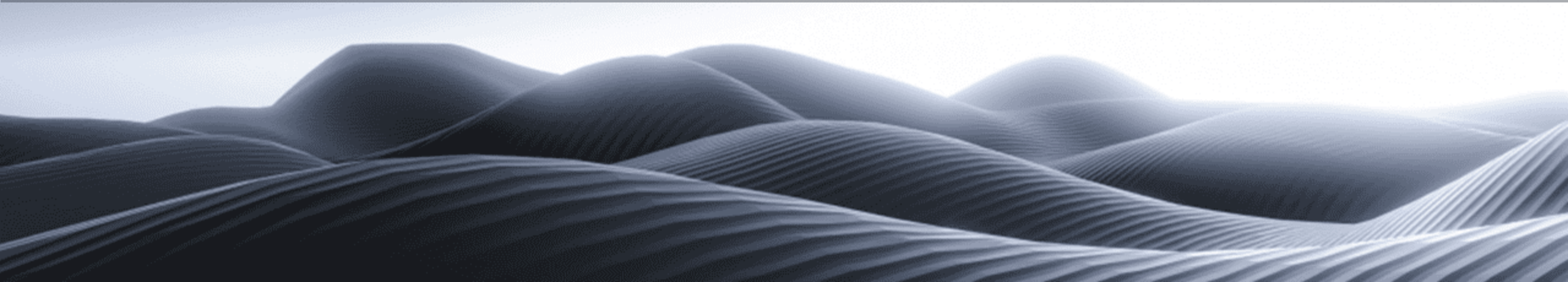
安全技术手段包括漏洞扫描、入侵检测、安全审计等，为安全运维提供技术支持。

04

安全培训包括安全意识培训、技能培训等，提高运维人员的安全意识和技能水平。

02

安全运维基础知识



网络安全概述

01

网络安全定义

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，确保系统连续可靠正常地运行，网络服务不中断。

02

网络安全重要性

随着互联网的普及，网络安全问题日益突出，网络安全已成为国家安全、社会稳定和经济发展的重要保障。

03

网络安全威胁

网络攻击、病毒传播、黑客攻击、数据泄露等是常见的网络安全威胁。

系统安全概述

系统安全定义

系统安全是指在操作系统、数据库、网络设备等系统层面采取必要的安全措施，确保系统的稳定性和安全性。

系统安全重要性

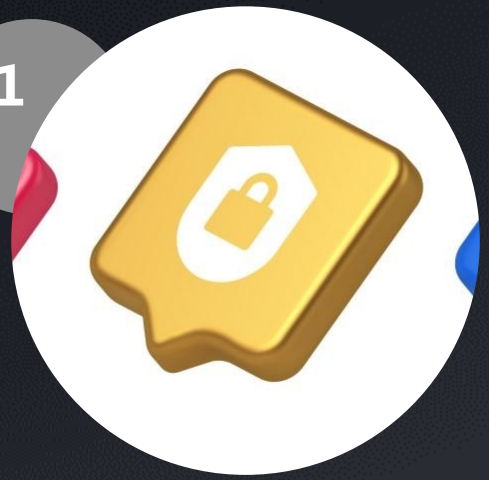
系统是支撑业务运行的基础设施，系统安全直接关系到业务的正常运行和数据的安全。

系统安全威胁

系统漏洞、恶意软件、病毒等是常见的系统安全威胁。

应用安全概述

01



应用安全定义

应用安全是指在应用程序和软件层面采取必要的安全措施，确保应用程序的稳定性和安全性。

02

应用安全重要性

应用程序是业务运行的核心，应用安全直接关系到业务的安全和数据的保密性。

03

应用安全威胁

SQL注入、跨站脚本攻击、恶意文件上传等是常见的应用安全威胁。

数据安全概述

数据安全定义

数据安全是指在数据的产生、传输、存储和使用过程中采取必要的安全措施，确保数据不被未经授权的访问、泄露、篡改或破坏。

数据安全重要性

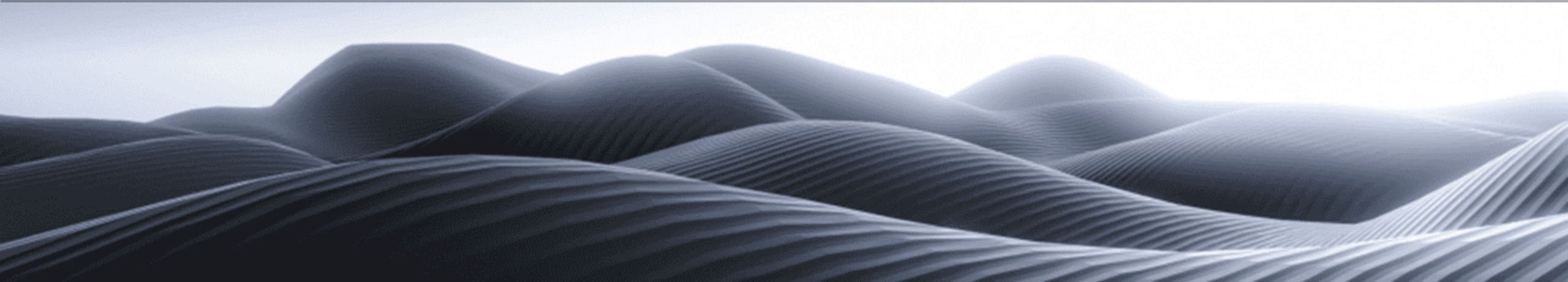
数据是企业的核心资产，数据安全直接关系到企业的生存和发展。

数据安全威胁

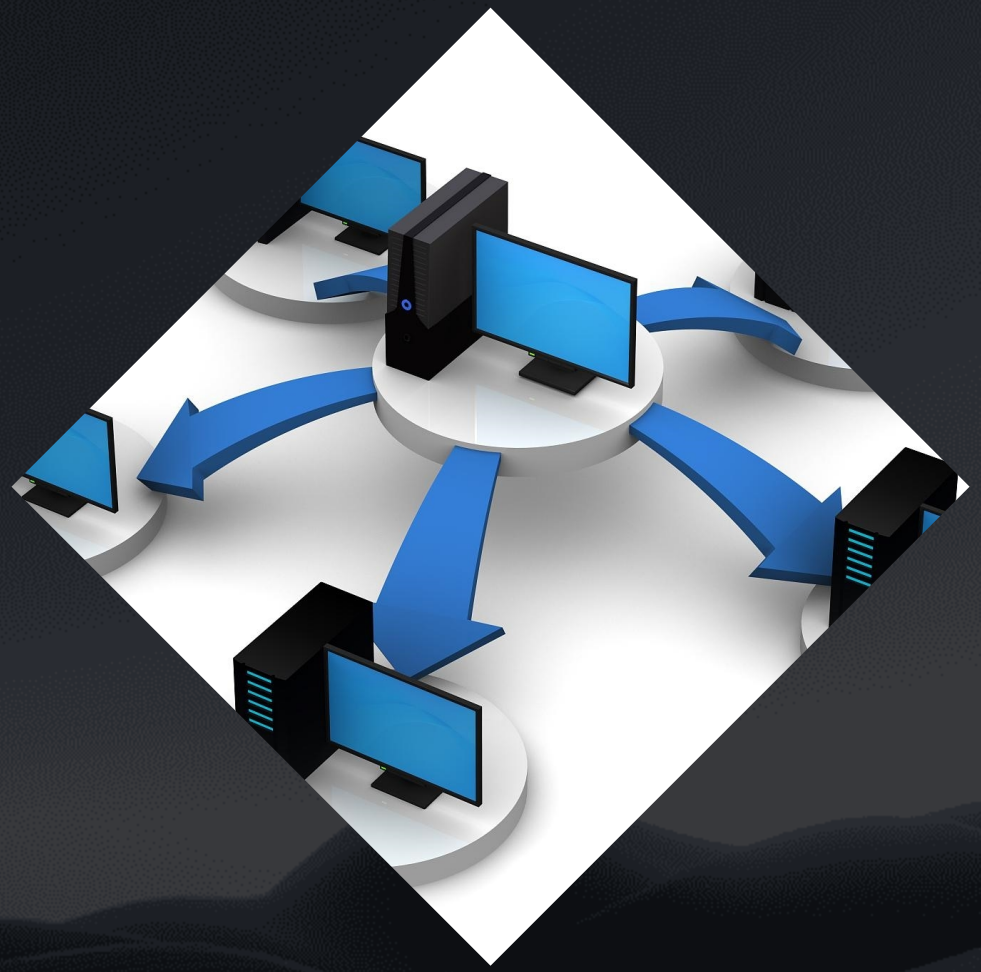
数据泄露、数据篡改、数据丢失等是常见的数据安全威胁。

03

安全运维技术



防火墙技术



防火墙定义

防火墙是用于保护网络免受未经授权访问的设备或系统，通常位于内部网络和外部网络之间。

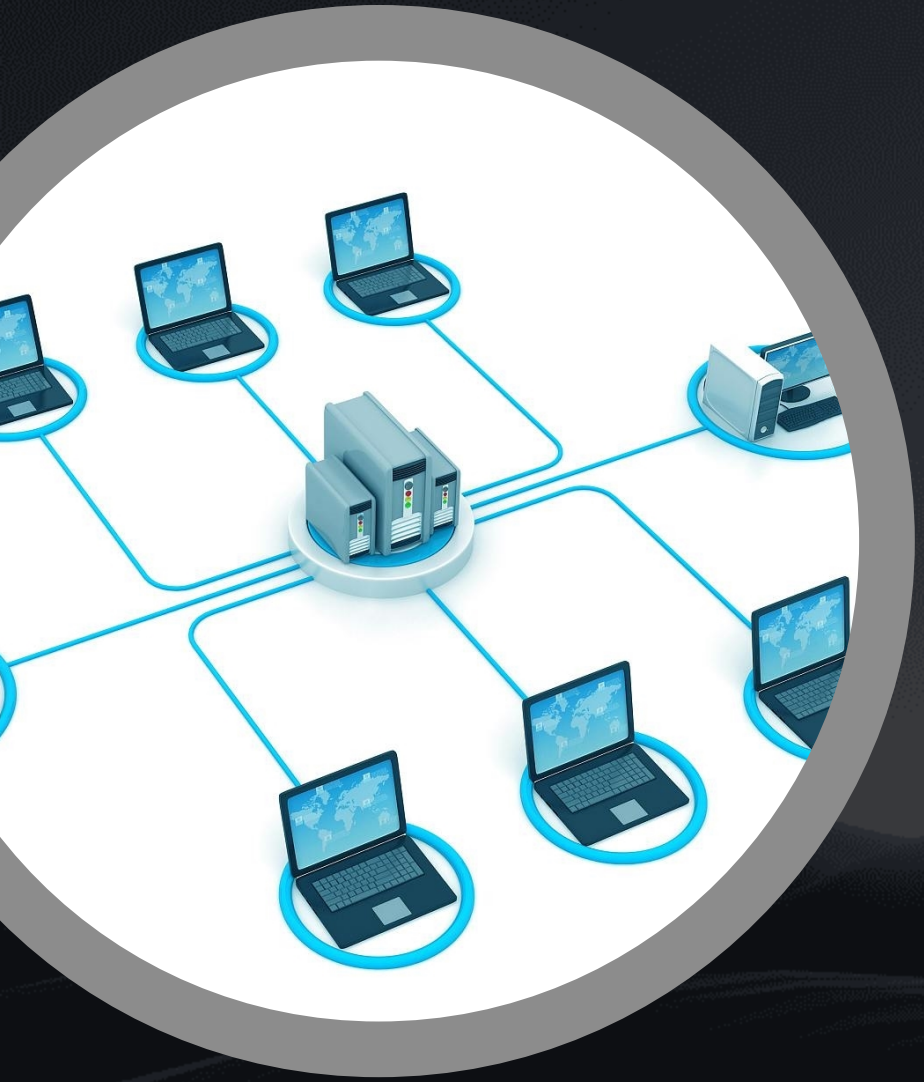
防火墙功能

防火墙可以过滤掉恶意流量和未经授权的访问，同时还可以限制网络流量和数据传输。

防火墙类型

根据实现方式，防火墙可分为软件防火墙和硬件防火墙，根据部署位置可分为边界防火墙和内部防火墙。

入侵检测技术



01

入侵检测定义

入侵检测是通过对网络流量和系统行为进行分析，检测出潜在的攻击行为并及时响应的技术。

02

入侵检测功能

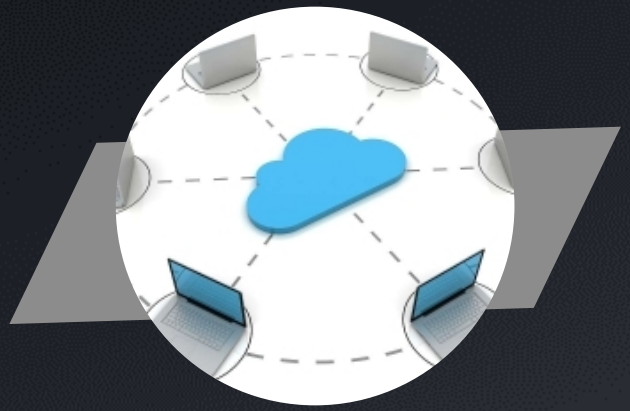
入侵检测系统可以实时监控网络流量和系统行为，发现异常情况并及时报警，同时还可以对攻击行为进行分析和溯源。

03

入侵检测类型

根据实现方式，入侵检测可分为基于主机的入侵检测和基于网络的入侵检测。

加密技术

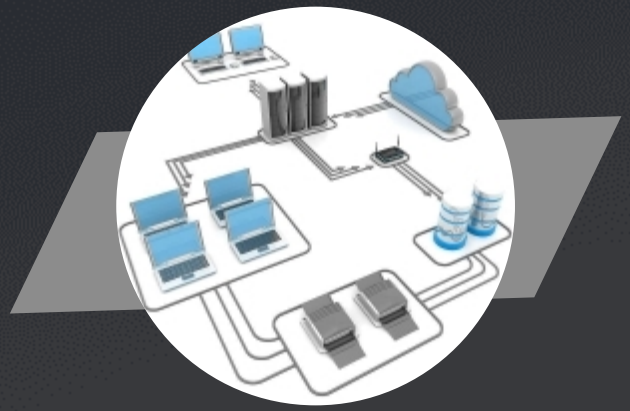


加密定义

加密是通过特定的算法将明文转换为密文，以保护数据的机密性和完整性。

加密功能

加密可以防止数据在传输过程中被窃取或篡改，同时还可以保证数据的机密性和完整性。



加密类型

根据实现方式，加密可分为对称加密和非对称加密，根据应用场景可分为数据加密和通信加密。

身份认证技术

身份认证定义

身份认证是用于验证用户身份的机制，以确保只有合法用户才能访问受保护的资源。

身份认证功能

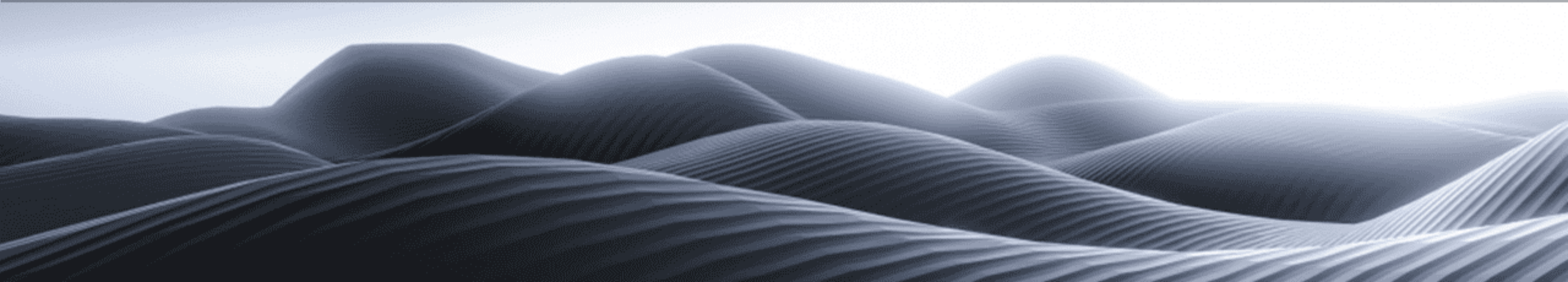
身份认证系统可以验证用户的身份和权限，防止未经授权的用户访问受保护的资源。

身份认证类型

根据实现方式，身份认证可分为基于密码的身份认证和基于生物特征的身份认证。

04

安全运维流程



安全漏洞扫描流程

选择合适的扫描工具

根据扫描目标和范围，选择合适的漏洞扫描工具。

漏洞分析

对收集到的漏洞信息进行分析，识别漏洞的危害程度和影响范围。

确定扫描目标和范围

明确需要扫描的资产、系统和应用，以及可能存在的漏洞。

实施扫描

对目标资产、系统和应用进行漏洞扫描，收集漏洞信息。

漏洞报告

生成漏洞报告，记录漏洞信息、危害程度和修复建议。

安全事件应急响应流程

事件发现与报告

通过监控系统、日志分析等手段发现安全事件，并及时报告给安全运维团队。

初步分析

对事件进行初步分析，了解事件的性质、来源和影响范围。

应急响应

启动应急响应计划，组织人员对事件进行处理，包括隔离、止损、溯源等。

事件处理

对事件进行处理，包括修复漏洞、加固系统、清理恶意代码等。

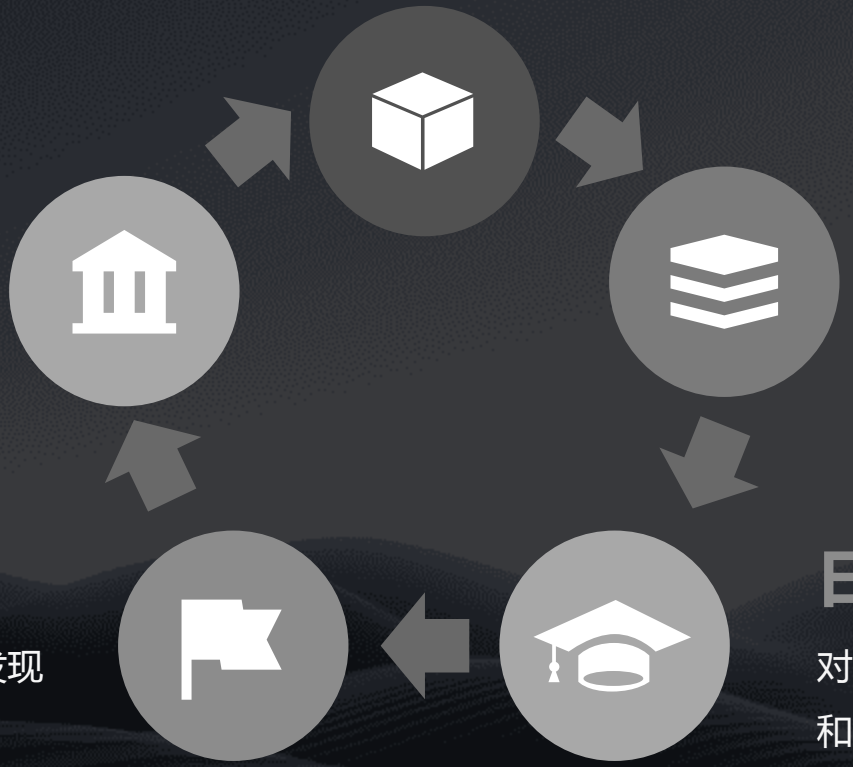
事件总结与报告

对事件处理过程进行总结，生成事件报告，记录事件处理过程和结果。

安全日志分析流程

日志收集

通过各种手段收集系统、应用和网络日志。



日志筛选

对收集到的日志进行筛选，去除无关信息和重复信息。

日志分析

对筛选后的日志进行分析，识别异常行为和潜在的安全威胁。

威胁预警

根据分析结果，生成威胁预警，及时发现和处理潜在的安全威胁。

日志存储与备份

将分析后的日志进行存储和备份，以备后续分析和审计使用。