网络安全运维管控平台

汇报人：

2024-02-06

目录

contents

01

平台概述与目标

网络安全运维背景

网络安全威胁日益严重

随着网络技术的快速发展，网络安全威胁不断增多，攻击手段日趋复杂，对企事业单位的网络安全构成了严重威胁。

运维管理面临挑战

传统的网络安全运维管理方式存在效率低下、响应速度慢、缺乏统一管控等问题，难以满足当前网络安全保障的需求。

管控平台功能与定位

01

集中化安全管理

提供统一的安全管理平台，实现对各类网络安全设备和系统的集中管理、监控和响应。

02

智能化运维支持

借助人工智能、大数据分析等技术手段，提供智能化的安全运维支持，提高运维效率和质量。

03

全方位风险防控

从网络层、系统层、应用层等多个层面出发，提供全方位的安全风险防控措施。

业务目标与价值体现

提高安全运维效率

通过自动化、智能化的安全运维手段，大幅提高安全运维效率，降低运维成本。

提升安全防护能力

通过集中化、全方位的安全管理，有效提升网络的整体安全防护能力。

保障业务稳定运行

确保网络安全与业务稳定运行，避免因安全问题导致的业务中断和损失。

技术架构与部署环境

01

模块化设计

采用模块化设计理念，方便功能扩展和升级维护。

02

分布式部署

支持分布式部署方式，可根据实际需求灵活调整部署架构。

03

高可用性保障

采用冗余设计、负载均衡等技术手段，确保平台的高可用性。

04

兼容性考虑

兼容主流操作系统、数据库、中间件等基础设施，降低部署难度。

02

核心功能模块介绍

资产管理模块

01

资产发现与识别

自动发现网络中的各类资产，包括硬件设备、软件系统、网络设备等，并识别其基本信息和属性。

02

资产分类与标签

对发现的资产进行分类管理，添加标签以便于后续管理和查询。

03

资产变更追踪

实时监控资产变更情况，包括新增、删除、修改等操作，确保资产信息的准确性和完整性。

漏洞管理模块

漏洞扫描与检测

定期对网络中的资产进行漏洞扫描，发现潜在的安全隐患和漏洞。

漏洞评估与定级

对扫描发现的漏洞进行评估，确定其危害程度和紧急程度，并进行定级处理。

漏洞修复与验证

提供漏洞修复建议和方案，并对修复后的漏洞进行验证，确保漏洞得到彻底解决。

配置管理模块

配置项识别与提取

自动识别网络中的各类配置项，包括系统参数、网络配置、安全策略等。

配置基线管理与审核

建立配置基线，对配置项进行管理和审核，确保配置项符合安全要求和标准。

配置变更追踪与审计

实时监控配置项的变更情况，包括修改、删除、新增等操作，确保配置信息的完整性和可追溯性。

日志审计模块

日志采集与存储

实时采集网络中的各类日志信息，包括系统日志、安全日志、操作日志等，并进行集中存储和管理。

日志审计与追溯

对日志信息进行审计和追溯，还原事件真相，为事后分析和追责提供依据。

日志分析与查询

对采集的日志进行分析和查询，发现异常事件和行为，并提供相应的报警和处置建议。

03

平台优势与特点分析

高效自动化运维能力

自动化监控

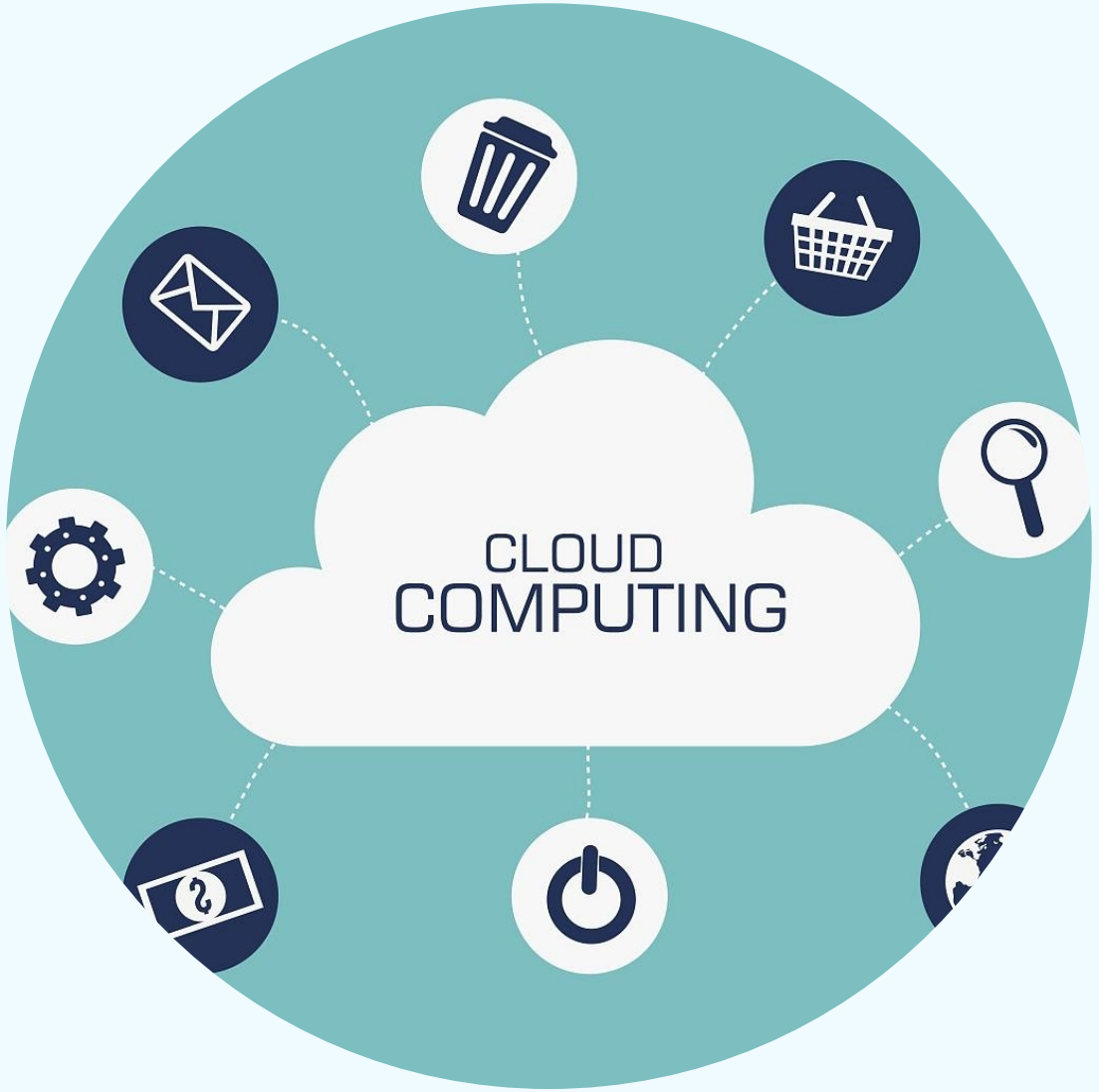
实时监控网络设备和系统状态，及时发现潜在问题。

自动化部署

快速部署和更新应用，提高运维效率。

自动化故障处理

智能分析故障原因，自动修复或提供解决方案。



全面安全防护策略部署

1

多层次安全防护

结合网络隔离、入侵检测、数据加密等多种技术，确保系统安全。

2

实时安全监控

对系统进行全面监控，及时发现并处理安全威胁。

3

定期安全漏洞扫描

定期扫描系统漏洞，及时修补，防止潜在安全风险。