风险评估工程师

风险评估前的那点事儿（一）

CONTENTS


PART01
工作范围
37:12

资 产 识 别

Asset Identification

开展对资产的识别，将帮助我们实现网络安全资产范围界定，有效识别资产边界，将会为网络安全部署提供界限。从成本管理和网络安全有效性中获取当前较为合理的一种平衡。

资产分类
Assets classification

物理环境包括：机房、建筑、空调、电力、动力等
网络环境包括：路由、交换、防火墙、网闸等
主机环境包括：Windows、Linux等
应用环境包括：ERP、OA、PMIS、动环等
数据环境包括：数据库、数据分析、审计等

资 产 评 估 对 象

P 服务器

检查服务器健康状况、安全防御状况、历史访问情况、应用服务情况、数据存储情况等。

D 网络设备

检查网络健壮性、连通性、稳定性，分析网络吞吐情况、流量分布情况、安全防御情况等。

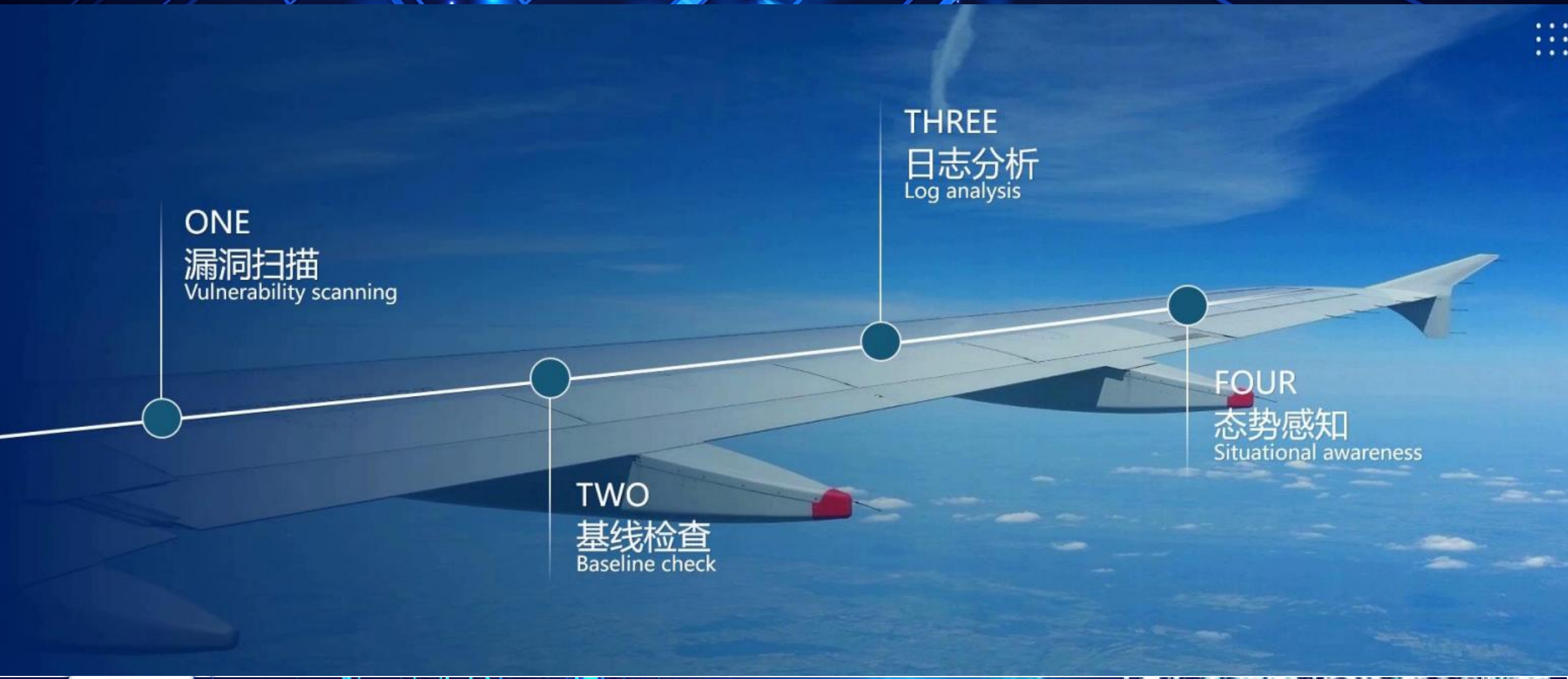
A 安全态势分析

多角度分析安全态势，梳理和识别安全风险，规划风险和威胁应对方法，提出应对建议。

C 安全设备

检查安全设备的健壮性、连通性、稳定性，分析安全设备权限、策略状态，判断攻击情况等。

辅 助 评 估


ONE
漏洞扫描
Vulnerability scanning
TWO
基线检查
Baseline check
THREE
日志分析
Log analysis
FOUR
态势感知
Situational awareness

谢谢观赏