资产安全远程检测系统

江苏君立华域信息安全技术股份有限公司

产品概述 | Product Overview

资产安全远程检测系统围绕资产安全，对资产进行管理、探测、发现、纳管、检测与脆弱性扫描分析，并周期性检测比对预警，实现了对资产全生命周期的闭环管理。系统通过对信息资产进行远程检测和重点资产的监测，可实时了解资产安全态势。

功能特性 | Features

资产管理

系统的资产管理模块内含海量的资产指纹信息，可对企业内部资产进行有效管理。从资产发现纳管，到周期性资产检测、漏洞扫描，准确掌握资产动态、安全现状。当漏洞爆发时，可借助本系统，多维度精准定位受威胁目标，一键扫描，确认漏洞，及时修复。实现了围绕资产安全的资产全生命周期管理。

漏洞扫描

系统的漏洞扫描模块支持对主机系统、web 网站、CMS 系统、常见漏洞、中间件、数据库、框架等全系列信息资产进行漏洞扫描及安全评估。具备强大的计算、大数据分析和存储能力，可快速高效的实现多批量任务的检查监控。

子域探测

系统提供子域名信息探测功能，能及时发现企业子域名使用情况，通过周期检测比对，及时识别异常域名。可对新发现的域名进行一键纳管，避免资产管理遗漏。

口令自检

对目标系统进行弱口令自检，支持 SSH、SMB、Telnet、FTP、Mail、Nginx、MySQL、Redis 等常见系统服务、数据库服务、中间件服务的弱口令检查。

资产安全远程检测系统

监测预警

目标系统进行风险监测预警，扫描检测目标系统的相关信息及可能存在威胁的文件，监测核查内容包括：安全基线、挖矿后门、系统配置。

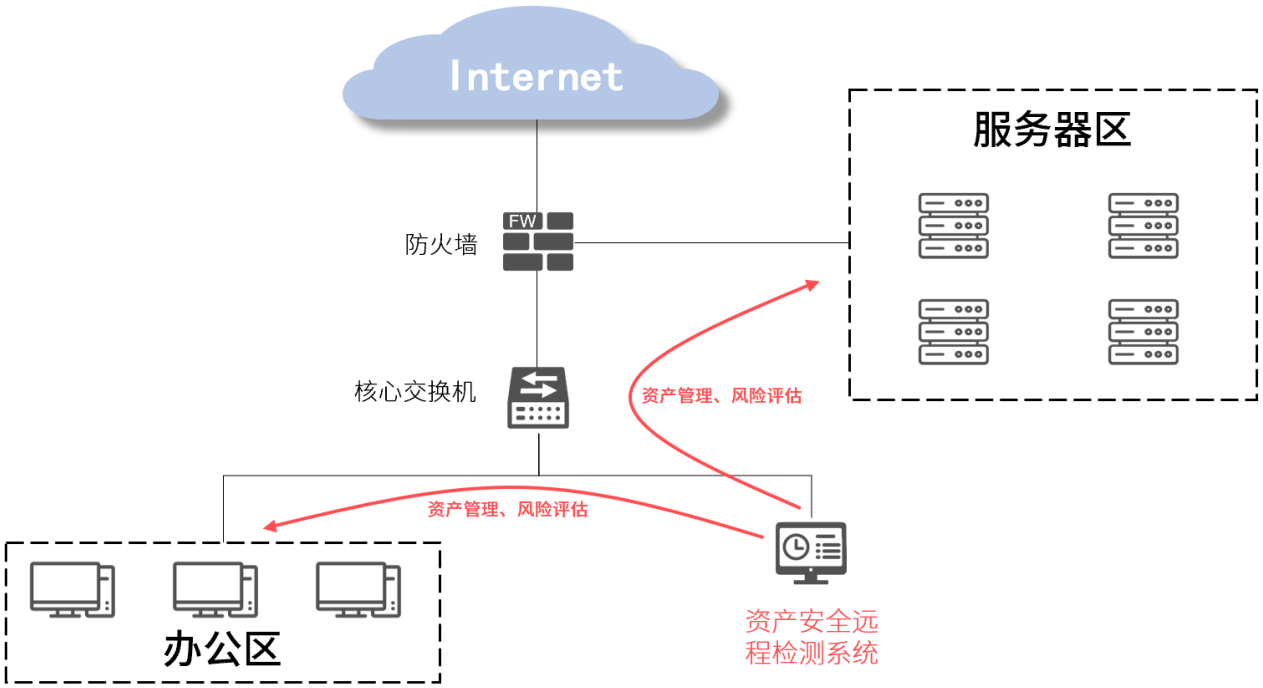
代理中心

系统提供大量高匿代理,系统流量可通过代理转发，有效绕过目标的安全防护策略，实现对目标的安全评估。

开放融合

系统开放资产检测指纹库、敏感词库、口令破解字典库等接口，用户可添加相应内容实现平台能力扩充；同时平台开放 API 接口，可与其他安全产品（如 SOC、SIEM 等）整合，实现优势互补，多设备联动。

典型应用 | Typical scene



资产安全远程检测系统

技术参数 | Technical Parameter

产品型号	君立华域资产安全远程检测系统
资产管理	支持主机资产、URL 资产管理，可识别资产 IP、主机 MAC、主机名、主机状态、资产分类、设备类型、设备厂商、主机系统、系统厂商、支撑脚本、服务组件、应用框架、地理位置、地理坐标、检测时间、端口矩阵、端口服务等；
	支持手工录入、表格导入、自主探测等方式纳管资产；支持定时检测、周期检测、任务重扫、任务结果对比、结果导出；
	支持资产标签管理，包括部门标签、系统标签、负责人标签、地区标签、行业标签等；支持多种资产检索方式，检索条件包括：资产状态、资产是否已检测、资产是否已扫描、资产来源、资产纳管时间、资产标签（归属地、负责人、归属部门、归属系统、归属行业、备注信息）、资产漏洞（漏洞类型、漏洞名称、漏洞等级）、资产属性（开放端口、开放服务、端口状态、资产分类、设备类型、设备厂商、主机系统、系统厂商、支撑脚本、服务组件、应用框架）；
漏洞扫描	支持定时扫描、登录扫描、周期扫描、任务重扫、任务暂停、代理扫描；支持扫描任务比对，及时发现漏洞变化；
	支持主机漏洞扫描、弱口令扫描、敏感信息社工扫描、数据库漏洞扫描、CMS 识别扫描、Web 漏洞扫描、中间件漏洞扫描、框架漏洞扫描等；支持漏洞自动化验证；
	安全评估报告包括目标基本信息、漏洞危害等级、漏洞描述、漏洞验证详情、漏洞路径、解决方案等；支持在线编辑报告；
子域探测	支持顶级域名扫描检测，快速准确地定位子域名，并判断有效性。可以进行资产的纳管和安全的管理；
	支持探测扫描任务比对，发现缺省或新增子域名；
	支持备案管理，从单位名称、单位性质、备案证号、网站域名、网站名称、系统定级等多个纬度进行域名管理；
暗链扫描	支持扫描目标 URL 中的暗链接，避免网站被人挂上违法链接，可设置扫描的深度；
安全工具	支持弱口令本地自检，支持 SSH、SMB、Telnet、FTP、Mail、Nginx、MySQL、Redis 等常见系统服务、数据库服务、中间件服务的弱口令检查；
	支持基线合规检查、挖矿后门检测、应急响应分析；
	提供大量 HTTP 代理,平台流量可通过代理转发，有效绕过目标的安全防护策略，实现对目标的渗透测试；
报表能力	可展示资产总量、存活量、安全资产量、存在风险资产量、存在风险资产排行、资产量变化折线图、资产分类统计、指纹与插件总量；可展示资产端口、服务、设备类型、厂商、系统和网站组件统计 Top10；
	可展示最新漏洞排行榜，支持自动关联存在相同漏洞的资产，通过资产链接可跳转至漏洞扫描报告页面，进而查看漏洞详情；
	可展示资产检测报表、漏洞扫描报表、子域探测报表、暗链扫描报表、基线核查报表等；
开放融合	开放 API 接口，用户可扩充资产指纹库、敏感词库、弱口令字典等，同时能够与其他平台（如 SOC、SIEM、扫描器等）整合；
安全策略	支持设置网络访问控制策略；
备份升级	支持备份/恢复系统数据；