碳泽 TANZE

碳泽千晓(CAASM)
网络资产攻击面管理系统

资产定义和收集 | 数据聚合 | 构建关系 | 攻击面呈现 | 合规管理 | 持续跟踪

为了有效解决组织资产盘点困难、安全状态模糊、攻击面不清晰等问题，碳泽信息通过长期的技术积累，研发碳泽千晓网络资产攻击面管理平台。**该系统通过从各个数据源主动收集资产数据，汇聚关联后形成资产攻击面知识图谱，从而帮助组织摸清家底、定位风险、主动缩减攻击面。**

- 云计算、虚拟化、云原生和物联网的运用，扩大了传统的网络边界；
- 云存储、云函数，容器等新型资产涌现；
- 漏洞、不安全配置等安全风险层出不穷；
- 缺乏安全视角的资产管理能力；
- 缺乏全面的攻击面管理平台；
- 资产信息和风险数据难以关联；
- 《网络安全法》、《数据安全法》、《关基条例》等法律法规合规需求。

碳泽信息始终坚持以资产为核心，自动化为纽带，风险威胁为基准，提高响应和处置效率为目标，专注于为客户构建新一代智能安全运营平台。碳泽千晓资产攻击面管理平台采用AI驱动的资产知识图谱、插件化云原生架构等技术，**帮助客户应对这些新挑战，实现全面的资产管理和攻击面管理能力，主动应对安全威胁，定位脆弱资产。**

01 产品功能特色

灵活定义资产

·IT、OT设备及各类硬件
·应用程序、站点等
·数据、用户、代码仓库
·各类云平台、容器环境

聚合并关联数据

·安全设备数据源：EDR等
·资产平台：CMDB、JIRA等
·代码仓库：Gitlab等
·插件化对接多种场景
·灵活且可自定义的数据建模
·主动的资产发现
·资产清点及关联性设定
·构建资产间的关联关系
·全面的资产知识图谱
·围绕资产的属性、关联规则、知识图谱、查询和综合呈现

攻击面管理

·全方位攻击面呈现
·漏洞与风险的统一管理及修复优先级
·DSL查询语言分析攻击面
·持续的合规监控

监控及综合报告

·持续监控资产安全状况
·高风险事件主动告警
·资产管理报告
·可定制的大屏呈现
·自定义搜索及查询规则
·全功能API

客户受益

管控所有资产
千晓的资产模型拓宽了安全管控的资产范围，并能通过多种方式收集资产数据，帮助您构建统一、去重的资产清单，确保资产管理的全面覆盖。

攻击面可视化
千晓使用贴近人类思维方式的知识图谱存储数据，借助于图可视化技术，用户可以快速对攻击面进行查询分析，实现主动防御。

自动汇聚关联
千晓通过API自动收集多种来源的资产数据，根据规则自动构建资产之间的关联关系，生成完整的资产上下文，解决数据碎片化的问题。

提升运营效率
资产是安全运营的核心，借助千晓构建的资产攻击面知识图谱，安全团队可提升应对事件响应、合规审计、重保HW等任务的安全运营效率。

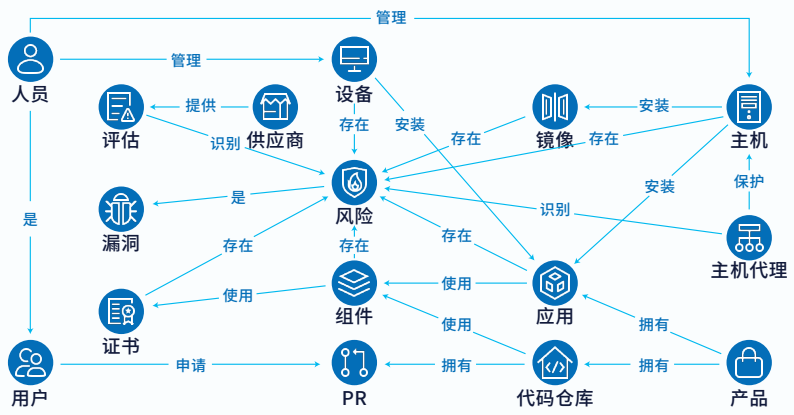
自定义面板

碳泽千晓网络资产攻击面管理系统界面

知识图谱

漏洞风险管理知识图谱示例模型

当收集的数据足够全面，就能构建完备的资产攻击面知识图谱



上海碳泽信息科技有限公司
Shanghai Tanze Info Tech Co., Ltd
电话：400-1788-258
网址：www.tanze.net.cn
销售咨询：sales@tanze.net.cn
技术支持：support@tanze.net.cn