目录

产品概述

金山云安全管理中心(Kingsoft Cloud Security Management，KSM)是集网络入侵威胁检测，安全弱点发现，攻击统计分析和威胁情报为一体的综合态势感知管理平台，通过安全态势实时感知及数据挖掘分析技术，帮助云上用户发现网络层、主机层、业务层等各层面的网络安全问题，实时大屏展现安全态势，实现对云上安全的有效统一管理。

产品优势

云安全管理中心基于安全大数据聚合分析，从网络层、主机层、业务层全面感知各类网络安全风险，帮助你实现对云上安全的统一运营和管理，产品具备以下优势：

安全统一管理 云安全管理中心汇聚各类安全设备和安全产品数据，实现对云上安全的统一管理

发现未知威胁 实时检测各类云上网络入侵行为，及时发现网络入侵威胁

威胁情报联动 协同威胁情报关联分析，有效降低告警误报，提升攻击发现能力

安全可视运营 实时安全态势大屏，多层面多维度展现网络安全态势，助力安全可视运营

产品功能

借助云安全管理中心可以实现以下功能：

- **入侵威胁** 在网络入口部署分光设备，基于数据包深度分析技术对进出流量进行全面的安全检测，可发现网络病毒、主机失陷、恶意流量、APT攻击等各类网络入侵威胁，对未知威胁进行提前发现和预警。
- **弱点发现** 可发现WEB应用和服务器存在的安全弱点，包括OWASP、CNNVD各类常见WEB漏洞类型以及服务器信息泄露、高危端口等安全问题，并提供修复处置建议。
- **实时大屏** 提供安全态势总览、主机安全态势、业务安全态势、业务运行态势（二期）、威胁情报中心（二期）、应急响应中心（二期）六块大屏，实时展现网络安全态势情况。
- **攻击分析** 提供详细的DDoS攻击和WEB应用攻击明细记录及统计信息，包括详细攻击起始时间、来源IP、攻击IP、攻击类型、攻击数据、风险等级等。
- **威胁情报** 默认集成威胁情报模块，对风险来源、样本等数据通过威胁情报进行协同分析以提高识别率，二期将开放威胁情报查询功能，输出威胁情报服务能力

各模块详细功能列表如下：

模块	子模块	说明
实时大屏	实时大屏	提供安全态势总览、主机安全态势、业务安全态势、业务运行态势（二期）、威胁情报中心（二期）、应急响应中心（二期）六块大屏，实时展现安全态势情况。
安全总览	安全总览	提供网络入侵、DDoS攻击、WEB应用攻击、漏洞情况、主机告警5个维度的统计情况及趋势，提供DDoS攻击和WEB应用攻击的详细攻击统计，支持EIP和高防IP的DDoS受攻击情况及黑洞状态展现。
入侵威胁	网络防病毒	通过内置防病毒检测引擎对HTTP协议流量进行文件还原。提取文件类型及特征码信息进行病毒分析检测，实时发现网络僵尸、蠕虫、木马、勒索、挖矿等恶意软件传播，支持对常见文件格式分析和检测，包括不限于docx、PDF、压缩文件等。
入侵威胁	主机失陷检测	通过主机网络连接的IP、域名等对外连接信息与在线IOC情报进行自动碰撞精准检测内网主机失陷行为并进行威胁告警，威胁告警信息包括攻击事件、黑客团伙、恶意软件家族等。
入侵威胁	恶意流量检测	基于特征签名对网络流量进行行为特征检测以发现恶意流量并进行告警。
入侵威胁	APT攻击发现	通过对威胁事件进行时间行为关联与大数据分析进行APT攻击发现。
入侵威胁	未知威胁检测	针对网络的未知威胁，通过机器学习方法对恶意软件行为特征建模学习，基于威胁模型检测发现未知威胁并及时告警。
入侵威胁	威胁事件告警	支持所有网络威胁事件的列表展示及查询，告警主机列表展示告警主机信息，针对威胁事件进行详情展示包括威胁描述、处置建议以及威胁发现过程。
弱点发现	漏洞发现	支持WEB和服务器漏洞扫描，覆盖OWASP、CNNVD常见WEB漏洞类型，发现服务器信息泄露、高危端口、匿名登录、越权访问和缓冲区溢出等各种常见的低危到高危的服务器漏洞，支持第三方应用漏洞检测。
弱点发现	服务器安全问题	支持服务器及数据库登录检测，弱密码检测、异地登录告警，服务器本地webshell及病毒检测，远程桌面及FTP暴力破解防护，自定义防护配置，检测SQL注入、XSS跨站脚本攻击，主动拦截webshell上传，检测服务器高危漏洞，Windows高危漏洞补丁自动升级。

攻击分析	攻击分析	提供详细的DDoS攻击和WEB应用攻击明细记录及统计信息，包括详细攻击起始时间、来源IP、攻击IP、攻击类型、攻击数据、风险等级等。