

卡巴斯基
工业网络安全

保护维系业务运转
的核心设施

关键基础设施态势感知和风险暴露控制

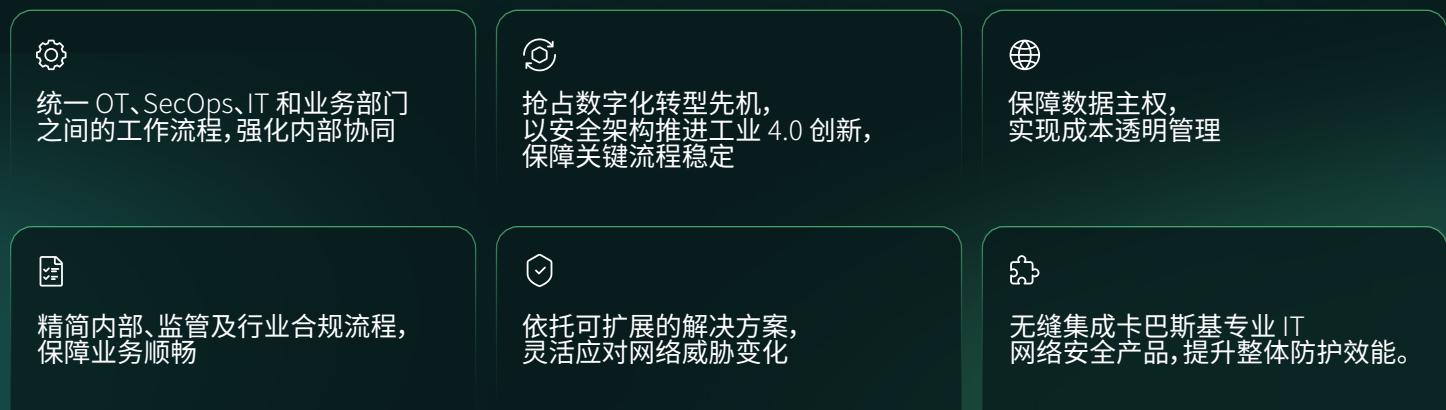
卡巴斯基工业网络安全 (KICS) 平台专用于为运营技术 (OT) 环境提供多层次防护。它可确保技术流程的连续性和控制系统的可用性。



The screenshot displays the KICS platform interface, featuring several key components:

- Dashboard:** Shows a summary of system health with three main metrics: CPU (3%), RAM (50%), and Occupied on disk (80%).
- Device by Security state:** A circular gauge showing 416 total devices, with 121 in Critical, 206 in Warning, and 89 in Normal states.
- Traffic by protocols:** A line chart showing network traffic over time across various protocols.
- Device by Status:** A circular gauge showing 416 devices, with 353 in Unauthorized, 13 in Authorized, and 50 in Archived states.
- Top application by number of events:** A bar chart showing the number of events for different applications.
- Risk scores:** A circular gauge showing a total risk score of 13600.
- GOOSE-communications statuses:** A circular gauge showing 296 GOOSE communications, with 234 Online, 12 Offline, and 50 Unknown.
- Network Map:** A diagram showing the network topology with nodes like "Blast Furnace-01", "PLC01-TM01", and "PLC02-TM02".
- PLC02-TM02 Details:** A detailed view of a specific PLC unit, showing its configuration, hardware, and software details.
- Configurations compare:** A comparison of device configurations over a 30-day period, highlighting changes and detected anomalies.

核心业务成果



The KICS platform offers the following key business outcomes:

- 统一 OT、SecOps、IT 和业务部门之间的工作流程, 强化内部协同**
- 抢占数字化转型先机, 以安全架构推进工业 4.0 创新, 保障关键流程稳定**
- 保障数据主权, 实现成本透明管理**
- 精简内部、监管及行业合规流程, 保障业务顺畅**
- 依托可扩展的解决方案, 灵活应对网络威胁变化**
- 无缝集成卡巴斯基专业 IT 网络安全产品, 提升整体防护效能。**

KICS XDR

平台能力



运营效益

占用空间小

凭借模块化部署以及灵活的可调节资源消耗设计, KICS 既不会影响系统性能与流程连通性, 还能防止软件出现膨胀现象。

兼容性

支持超过 125 个 Windows 和 Linux 系统版本, 且已完成对 200 多个工业自动化和控制系统 (IACS) 及设备的测试验证, 支持您与现有基础设置相兼容。

原生集成

卡巴斯基工业网络安全解决方案节点安全 (KICS for Nodes) 与卡巴斯基工业网络安全解决方案网络安全 (KICS for Networks) 两款解决方案紧密协作、相得益彰, 实现无阻碍集成、集中化管理以及扩展的跨产品功能, 为企业网络安全提供支撑。

解决方案架构和应用场景

具备 AI 剖析功能的高级资产管理

借助资产发现工具集与多方面的网络可见性，识别连接的设备及其交互情况，从而掌控影子基础设施，确保无未知设备隐患。

扩展检测和响应

可检测恶意或不安全活动，在威胁影响业务之前进行有效遏制。系统支持检测超 5,000 种网络攻击，对 50 多种工业协议进行深度数据包检测 (DPI)，并提供针对性的安全响应方案。

持续安全审计

借助 3,100 多条预定义审计规则和 1,300 多项 OVAL 漏洞测试，对分布式、“气隙”式及高敏感隔离环境展开安全评估，洞悉其安全态势。

③ 业务与企业

安全运营中心  卡巴斯基新一代安全 XDR 专家版

② 监测与控制

 卡巴斯基工业网络安全解决方案节点安全

站点监控系统



基于代理的资产清查



① 自动化与保护

卡巴斯基工业网络安全解决方案网络安全

被动监控 (SPAN)

变电站自动化系统
无代理轮询网络设备
交换机
BCU
主动轮询 OT 资产
IED

网络响应

主流程控
制系统
MLAD
交换机
EWS
DCS 控制
器
端点响应
来自主机与
网络的警报

KICS 网络安全被动采集以下来源的网络流量：

- 自有网络传感器
- SD-WAN 收集器
- 端点代理
- 便携扫描仪

④ 技术流程



集成案例



卡巴斯基
新一代安全 XDR 专家版

KICS 平台与卡巴斯基新一代安全 XDR 专家版结合使用，可提供统一的 IT-OT XDR 能力，并为融合基础设施提供综合防护。



卡巴斯基
异常检测机器学习

与异常检测机器学习 (MLAD) 解决方案集成后，KICS 网络安全可发送遥测数据以进行分析，并接收针对检测到的异常情况的警报。



卡巴斯基
SD-WAN

KICS 可利用 SD-WAN 基础设施收集工业流量、提供集中监控，并保护分布式工业对象和系统。



卡巴斯基
工业网络安全