卡巴斯基 OT 网络安全

专为物理系统网络韧性提升打造的统一解决方案

kaspersky 引领未来

卡巴斯基
OT 网络安全

经验铸就韧性

工业安全解决方案
提供经严格测试、符合行业合规要求且获行业认可的稳健工业安全解决方案

威胁分析与安全培训
基于可信的威胁分析，配备完善的网络安全培训

经过实战检验的专业能力
专业安全服务，助力企业构建稳健的网络安全体系网络安全

IT XDR

卡巴斯基
新一代安全 XDR 专家版

IT-OT 融合

技术

专业解决方案

- 卡巴斯基 反无人机系统
- 卡巴斯基 异常检测机器学习
- 卡巴斯基 SD-WAN

卡巴斯基
工业网络安全

原生 OT XDR

节点安全
端点保护、检测与响应

×

网络安全
网络流量分析、检测与响应

卡巴斯基 操作系统解决方案

- 卡巴斯基 瘦客户端
- 卡巴斯基 汽车安全网关

知识

网络安全	威胁情报	培训
卡巴斯基 安全意识	卡巴斯基 ICS 威胁情报中心	卡巴斯基 ICS CERT 培训

专业知识

发现	事件响应	托管阶段保护
卡巴斯基 ICS 安全评估	卡巴斯基 事件响应	卡巴斯基 托管检测和响应

卡巴斯基
OT 网络安全

为关键任务系统提供多方面安全覆盖 - 现已实现

卡巴斯基
工业网络安全

节点安全
端点保护、
检测与响应

×

网络安全
网络流量分析、
检测与响应

原生 OT XDR

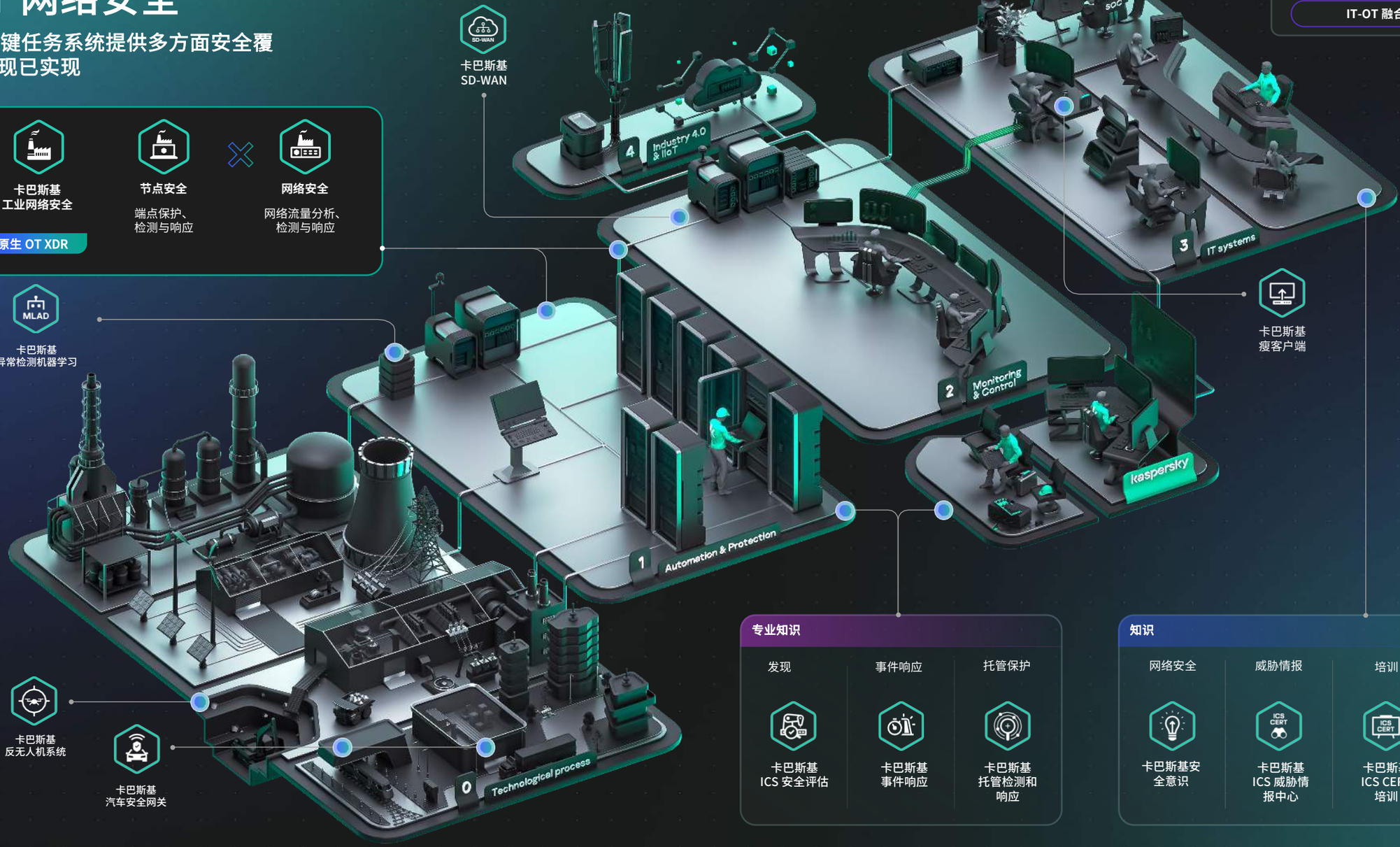
卡巴斯基
SD-WAN

卡巴斯基
新一代安全
XDR 专家版

IT-OT 融合

卡巴斯基
异常检测机器学习

卡巴斯基
瘦客户端



卡巴斯基
反无人机系统

卡巴斯基
汽车安全网关

专业知识

发现	事件响应	托管保护
卡巴斯基 ICS 安全评估	卡巴斯基事件响应	卡巴斯基托管检测和响应

知识

网络安全	威胁情报	培训
卡巴斯基安全意识	卡巴斯基 ICS 威胁情报中心	卡巴斯基 ICS CERT 培训

卡巴斯基
工业网络安全

态势感知及风险暴露控制

- **资产清单与网络可视化：**追踪所有已连接设备及其配置构建网络拓扑图，分析数据流。
- **消除威胁并定位安全症结：**发现并缓解主机与网络中的各类威胁，深入剖析威胁产生的根本原因，并采取针对性安全响应措施。
- **评估风险并监控安全变更：**评估主机、网络设备及控制器的潜在漏洞，监控其安全设置变更情况。

核心优势

- 经过测试与验证，可与 200 多个工业自动化系统及设备实现兼容
- 提供无缝集成的 OT XDR 平台，专为关键基础设施打造，以应对多重安全挑战
- 低资源占用，不影响系统性能或流程连续性

KICS 及其核心技术均经过行业权威审计

ISA/IEC 62443-4-1　SOC 2 Type 2　ISO/IEC 27001　GB 42250-2022

卡巴斯基
新一代安全 XDR 专家版

面向工业与企业层面，提供端到端安全防护

卡巴斯基工业网络安全平台与卡巴斯基新一代安全 XDR 专家版深度集成，全面拓展安全防护场景——支持与第三方解决方案协同联动，增强威胁调查与应急响应能力。该集成有助于在工业环境与企业环境的交叉点为您的业务运营提供安全防护。

安全团队可掌握事件发展的整体图景，确定其根本原因，以防止类似事件的再次发生。

核心优势

- 面向融合的、资产密集型的 IT/OT/IoT 基础设施的安全与数据主权
- 卡巴斯基产品组合的原生互操作性提供无缝且专业的集成能力

MLAD

卡巴斯基
异常检测机器学习

早期异常检测和预测分析

- 在设备故障与人为操作失误酿成严重后果之前实现早期预警与识别，有助于规避生产中断与安全事故的发生。
- 捕捉非典型员工行为或异常设备操作，识别潜在的定向攻击与蓄意破坏意图。
- 识别由多个过程参数微小偏差所引发的、在网络物理系统运行中极难察觉的隐蔽异常。

与外部系统集成

卡巴斯基 MLAD 可从 KICS 网络安全、工业自动化系统及 IoT/IIoT 设备接收过程遥测数据

MLAD 事件处理器与外部源（SIEM 系统、IIoT 及网络设备）交换 CEF 消息

IACS – 工业自动化和控制系统
SIEM – 安全信息和事件管理

IIoT – 工业物联网
IoT – 物联网

卡巴斯基
SD-WAN

确保分布式工业网络可靠性的统一解决方案

卡巴斯基 SD-WAN 助力工业企业能构建具备集中管理能力的弹性地理分布式网络，保障工业生产流程的持续稳定运行。

卡巴斯基工业网络安全平台依托 SD-WAN 基础设施，实现工业流量的采集与集中监控，为分布式工业设施及系统提供统一的安全防护。

核心优势

- 便捷的可扩展性
- 成本优化
- 便捷高效管理
- 集中安全

技术

卡巴斯基
反无人机系统

无人机监控和防御解决方案

卡巴斯基反无人机系统通过阻止未经授权的无人机侵入工业企业空域，降低因空域入侵导致的生产中断风险。
该系统具备空域自动扫描、无人机探测与分类能力，并通过可视化网页界面显示空域态势信息。当监测到威胁且符合法规要求时，操作员可即时启动反制措施，消除无人机安全隐患。

卡巴斯基反无人机系统是一个模块化解决方案，可部署于任意规模的工业场所。该解决方案还支持“敌我识别”工作模式，在保障组织自有无人机正常作业的同时，拦截并驱离未经授权的无人飞行器，实现安全防护与业务运营的协同。

核心优势

- 卡巴斯基反无人机系统支持将来自不同厂商的雷达、射频扫描仪、摄像头及干扰器组合并编排到统一的系统中。
- 基于多传感器融合技术，提高了在杂乱、嘈杂或低能见度条件下的检测可靠性。

技术

卡巴斯基
瘦客户端

安全的远程与虚拟桌面基础设施

风险

用户工作站是最常见的网络攻击目标之一

解决方案

卡巴斯基瘦客户端基于卡巴斯基自研的微内核卡巴斯基 OS 操作系统打造，用于构建可管理且功能完善的瘦客户端基础设施。

瘦客户机无主动散热装置、无机械运动部件，可在生产环境中提供可靠的性能表现。

核心优势

- 设计即安全
- IS 和 IT 的单一管理平台
- 基础设施集成仅需两分钟

卡巴斯基
汽车安全网关

为互联汽车构建可靠的 IT 系统

- 安全的互联汽车软件网关，同时提供车载远程信息处理单元 (TCU) 的功能
- 从操作系统层面提供安全保障
- 符合保障车辆网络安全与安全性的最新要求（ISO 26262、ISO/SAE 21434、UN R155、UN R156、Uptane）
- 保障 E/E 架构电子单元之间以及这些单元与网联汽车云平台、诊断设备之间的安全可靠通信
- 实现远程诊断、安全的空中下载 ECU 更新及其他远程信息处理服务

核心优势

为高信息安全要求行业提供专业的安全性与网络免疫能力

将安全网关与远程信息处理控制单元集成于单一解决方案中，有助于降低成本

专用协议有助于优化蜂窝网络流量费用

知识

卡巴斯基 ICS 威胁情报中心

深入了解工业网络安全威胁与漏洞，以支持有效的风险评估、攻击检测、事件调查与响应。

依托卡巴斯基 ICS CERT（工业网络安全领域的首个私营 CERT）深厚的专业沉淀与实战经验为您提供支持。

核心优势

- 快速威胁检测和广泛的分析能力
- 提升调查与主动威胁搜索的效率
- 丰富的威胁和漏洞信息，助力做出明智决策

卡巴斯基威胁情报解决方案和服务

机器可读的威胁情报

- 卡巴斯基 威胁数据源 — ICS
- 卡巴斯基 网络追踪

威胁情报专家支持

- 卡巴斯基 下线服务
- 卡巴斯基 询问分析师 — ICS

人工可读的威胁情报

- 卡巴斯基 威胁查找
- 卡巴斯基 数字足迹情报
- 卡巴斯基 威胁分析 — 沙盒 | 归因 | 相似性
- 卡巴斯基 威胁 情报报告 — APT | 犯罪软件 | ICS
- 卡巴斯基 威胁基础设施跟踪

● 战术 ● 操作 ● 战略
○ 可通过卡巴斯基威胁情报门户获取

专业中心

- 卡巴斯基 全球研究和分析团队
- 卡巴斯基 AI 技术研究
- 卡巴斯基 ICS CERT
- 卡巴斯基 威胁研究
- 卡巴斯基 安全服务

● 威胁研究 ● 事件调查

知识

卡巴斯基威胁数据源

卡巴斯基威胁数据源服务提供近乎实时的威胁情报，助力工业组织防御网络安全威胁。其中，ICS 数据源涵盖已知恶意文件及经证实可在工业控制系统中被利用的最新漏洞信息。在具体情境下，这些数据有助于揭示全局，回答“人物、事件、地点、时间”等问题，从而确定攻击来源、加速安全决策并做出有效应急响应。

核心优势

- 改进并加速事件响应与取证能力
- 增强的安全解决方案
- 防止敏感资产和知识产权泄露

您将获得：

卡巴斯基 ICS 哈希数据源

最新的威胁情报，用于 ICS（以及 OT 中使用的其他系统）简化和自动执行及时的攻击检测和调查

防御 # 检测 # 的 IoC

卡巴斯基 ICS 漏洞数据源

面向工业环境中的 ICS 系统及其他系统，以机器可读格式提供经严格核验与深度精炼的软件及硬件漏洞数据。

防御 # 检测 # 的 IoC

OVAL 格式的 ICS 漏洞数据源

定期更新包含 OVAL 定义的数据源，用于自动检测 SCADA 系统以及其他工业软件中的已知漏洞

检测

知识

卡巴斯基 ICS 情报报告阶段

卡巴斯基 ICS 威胁情报报告对针对工业组织面临的恶意活动提供深度情报与前瞻性洞察，同时涵盖主流工业控制系统及基础技术中已发现漏洞的详细分析。为工业组织量身定制的详细信息可帮助客户保护关键资产（包括软件和硬件组件），并确保技术过程的安全性和连续性。**保障技术过程的安全性和连续性**。

核心优势

- 检测并防范已报告的威胁，保护关键资产，保障技术流程的安全与连续性
- 将检测到的恶意或可疑活动与卡巴斯基研究成果进行关联，以将事件归因于特定攻击活动并识别威胁

您将获得：

APT 报告

聚焦针对工业组织的新型 APT 攻击及大规模攻击活动，并同步追踪当前活跃威胁的最新态势。

发现的漏洞

聚焦工业控制系统、工业物联网及各行业关键基础设施中广泛部署的主流产品已知漏洞。

威胁环境

剖析工业控制系统威胁态势的重大演变，揭示影响 ICS 安全水平的新兴关键因素及当前面临的核心威胁，并提供覆盖地区、国家及行业维度的专项分析。

漏洞分析和缓解

我们的咨询服务依托卡巴斯基资深专家团队，提供专业、可落地的定制化建议，助力企业识别并抵御安全威胁。

卡巴斯基分析师咨询

卡巴斯基分析师咨询服务是对卡巴斯基威胁情报产品组合的有力补充。通过这项服务，为您提供与资深分析师直接对接的专属通道。您可就当前面临或重点关注的特定威胁与漏洞，获取针对性的专业研判与深度洞察，强化防御能力，抵御针对企业及工业基础设施的安全威胁。

核心优势

- 联系专业的威胁情报专家，包括卡巴斯基 ICS CERT 的工业安全专家
- 个性化的详细背景信息，有助于有效调查
- 我们的专家详细说明如何对威胁和漏洞做出快速有效的响应

* 有关已发布报告的补充信息：

- 有关 ICS 漏洞的信息
- 按地区与行业维度划分的工控系统威胁态势统计及最新演变趋势
- 针对 ICS 的恶意软件的分析
- 有关法规要求和标准的信息

卡巴斯基
安全意识

将员工转换为人力防火墙

卡巴斯基安全意识产品组合助力企业从决策层到执行层，构建坚实的网络安全文化体系：

- **卡巴斯基 交互 保护 模拟 (KIPS)** – 专为发电、石油天然气、石油化工等工业场景量身定制的游戏化模拟平台。通过沉浸式体验直观展现网络安全事件对业务绩效的深远影响，使管理层切身感受战略决策的实际后果。
- **卡巴斯基自动化安全意识平台 (ASAP)** – 依托互动式培训与仿真钓鱼攻击演练，面向全体员工系统培育安全行为习惯，确保全员掌握必要的工业网络安全知识与实操技能。
- **卡巴斯基高管培训** – 面向企业决策者及各职能部门负责人的实战型课程，助力高层管理者深入洞察网络安全态势，提升战略决策能力。

涵盖的主要主题

- 电子邮件安全
- 网站和互联网
- 密码和帐户
- 社交媒体和即时消息
- 工业网络安全
- PC 安全
- 移动设备管理
- 机密数据
- GDPR
- 物理数据安全
- 银行卡安全和 PCI DSS
- 人工智能和神经网络
- 个人数据

卡巴斯基
ICS CERT 培训

运用学到的知识

我们的 ICS 培训计划旨在帮助 IT、OT 和信息安全专业人员以及管理人员和其他员工扩展工业网络安全知识并培养专业实践技能。

卡巴斯基专家传授的实用技巧

- 数字取证和事件响应
- 探索 OT/IoT 设备和工业软件中的漏洞
- 面向 IT、OT 和 IS 专家的跨职能培训课程

专业知识

卡巴斯基
ICS 安全评估

确保 OT 环境中的网络韧性

风险

只需一个漏洞，网络犯罪分子就可能完全控制整个工业系统

解决方案

一种识别工业基础设施安全漏洞和弱点的综合方案

核心优势

- 加强安全控制措施，保护操作员、工程师及其他员工
- 识别黑客可能利用的安全漏洞，防范针对装配线、制造设备及机器人系统的潜在攻击与运行干扰
- 保护制造设计、项目及方案免遭窃取
- 防止可能导致产品质量或安全性受损的入侵事件

卡巴斯基工业安全评估方法

外部渗透测试
黑盒或灰盒

互联网

工业（OT）基础设施

- 网络架构和设备
- 行业解决方案、工作站和服务器
- 设备和组件

设备和组件

OT 安全分析
- 白盒测试
- 攻击模拟
- 成效评估

企业局域网、MES

内部渗透测试
黑盒或灰盒

测试环境

硬件和软件组件的安全分析
- 白盒测试
- 零日漏洞
- 硬化指南

卡巴斯基
托管检测和响应

AI 赋能人类精进

- 持续搜寻、检测和消除工业企业面临的威胁
- 无需雇用新的网络安全专家，降低安全成本
- 无需在内部建立 SOC，即可享有 SOC 的核心能力与运营价值

我们所保护的客户中有 22% 来自工业领域

查看 MDR 分析师 报告 了解更多信息

核心优势

主动威胁检测：获得专利的攻击指标有助于识别控制系统内的隐藏威胁

自动化、引导式的响应（可提供完整的取证调查和恶意软件分析）

ICS 网络安全专业知识：由行业经验丰富的主动威胁检测专家团队提供有力支持

专业知识

了解更多　　报告事件

卡巴斯基
事件响应

管理安全违规造成的后果

风险

针对关键基础设施的安全事件，响应处置须依托具备工业现场实战能力的专业团队。错误和不合时宜的操作可能会显著加剧攻击造成的损害。

解决方案

- 卡巴斯基全球应急响应团队 快速消除事件后果
- 覆盖事件调查与响应全周期的支持
- 基于我们自研创新工具的情报、收集与修复
- 按需提供专业知识并可与您的团队进行知识共享

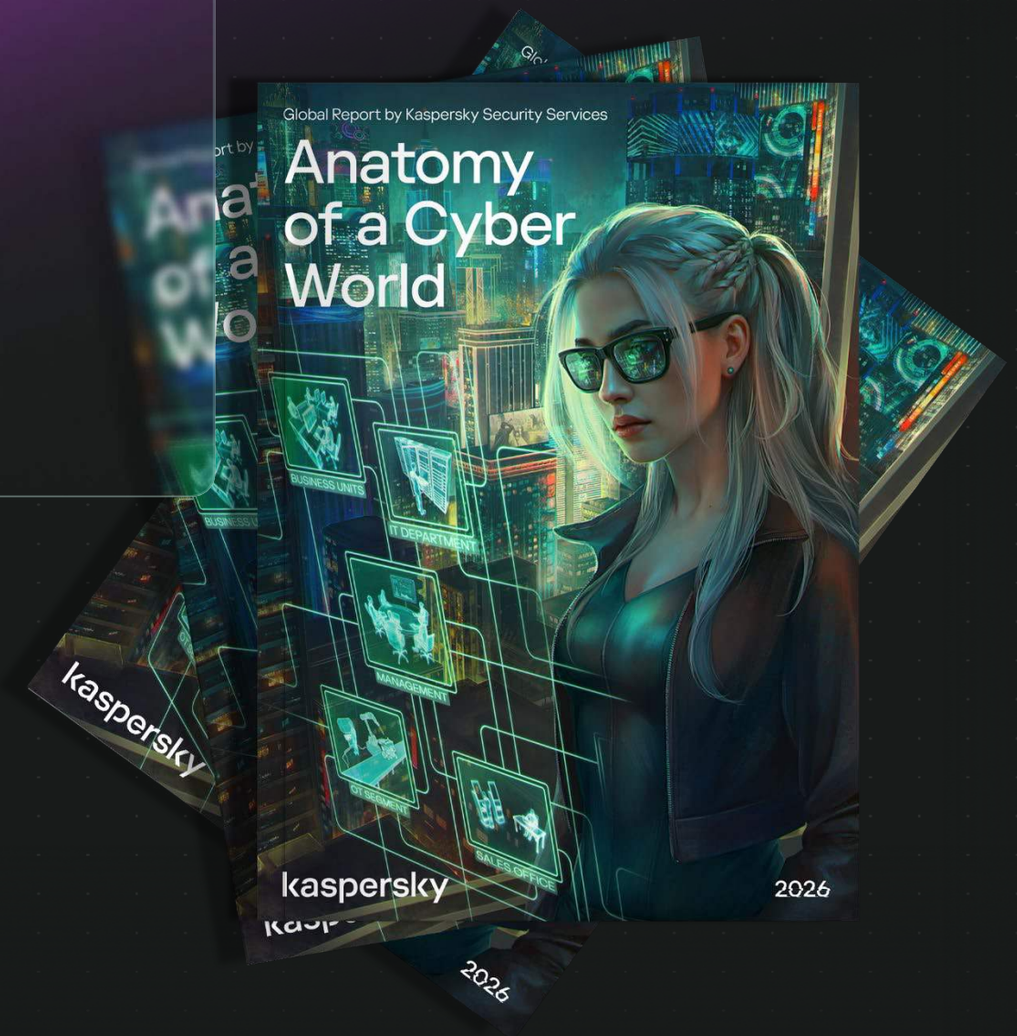
服务组合

事件 响应
威胁调查与清除

数字取证
数字证据的分析

恶意软件分析
获取攻击中使用
的文件的详细视图

通过卡巴斯基安全服务发布的
全球报告，深入剖析网络世界的内在结构



值得信赖的合作伙伴

近 30 年安全实践经验与 PB 级威胁情报数据

ICS-CERT – 我们自有的国际 OT/IoT 安全研究部

拥有 IT/OT 安全行业积累的久经验证的专业知识，斩获众多奖项与成就

已通过超过 200 项认证，可与自动化供应商解决方案实现互操作

技术方案经严格验证，符合行业标准与合规要求

更多 OT 解决方案　　更多 IT 解决方案　　联系我们